FORO NACIONAL DE CIBERSEGURIDAD

FORO NACIONAL DE CIBERSEGURIDAD

MOTOR DE LA COLABORACIÓN PÚBLICO-PRIVADA

2023

- Brújula de la ciberseguridad del ciudadano
- Código de buen gobierno de la ciberseguridad
- Impulso a la industria y a la I+D+i. Resumen de propuestas y trabajos de la fase 2
- Marco de competencias para programas superiores de formación especializada en ciberseguridad
- Informe sobre las necesidades, capacidades y retos para la colaboración público-privada en materia de ciberdefensa en las empresas del sector de la defensa y la seguridad

Catálogo de publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

NIPO (edición on-line): 089-23-015-X
Fecha de edición: junio 2023

FORO NACIONAL DE CIBERSEGURIDAD

MOTOR DE LA COLABORACIÓN PÚBLICO-PRIVADA

2023

Prólogo

La vulnerabilidad del ciberespacio es uno de los riesgos para la Seguridad Nacional que se percibe con mayor deterioro en un horizonte temporal de cinco años, según el resultado de la encuesta de percepción de riesgos del Informe Anual de Seguridad Nacional 2022.

España, al igual que el resto de países de nuestro entorno, se enfrenta a numerosos retos en el ámbito de la ciberseguridad, propiciados en gran medida por los elevados y crecientes niveles de conectividad de entidades públicas, empresas y ciudadanía. Las ciber amenazas han evolucionado muy rápidamente en los últimos años, los ciber atacantes han perfeccionado sus técnicas y los ciberataques son cada vez más frecuentes, persistentes, más graves y más difíciles de detectar. Los ciberdelitos siguen aumentando, en especial los fraudes informáticos, uno de los fenómenos con mayor incidencia en el ciberespacio.

El actual escenario geopolítico, la competencia por la soberanía tecnológica, la demanda sobre la propiedad y gestión de los datos que se obtienen y mercantilizan en el ciberespacio, así como tecnologías antes emergentes y ahora ya presentes, como el 5G o la inteligencia artificial, son algunos de los elementos que sin duda marcan la actualidad y marcarán la tendencia en ciberseguridad en el futuro más próximo.

Hacer frente a los retos presentes y futuros en el ámbito de la ciberseguridad no es posible sin el elemento clave de la colaboración público privada. Desde el Departamento de Seguridad Nacional se asume el compromiso se potenciar, facilitar y materializar la mencionada **colaboración público-privada** a través del **Foro Nacional de Ciberseguridad**. Este espacio de encuentro es creado en julio de 2020, con el objetivo de *proponer iniciativas para desarrollar la Estrategia Nacional de Ciberseguridad a través de sinergias público-privadas que permitan dotar de una mayor protección a la sociedad española en toda su amplitud*. Los trabajos desarrollados en la primera etapa del Foro salieron a la luz en febrero de 2022 y abordaron: la cultura de la ciberseguridad en España, el apoyo a la Industria e I+D+i y la definición de un Esquema nacional de certificación para responsables de esta materia.

En esta segunda etapa del Foro 2023, tengo el placer de presentar el resultado de los nuevos trabajos de los distintos grupos que, en esta etapa, se han centrado en la ciberseguridad del ciudadano, la responsabilidad social corporativa, el impulso a la industria y a la I+D+i, la formación especializada en ciberseguridad, así como en las necesidades de ciberdefensa, y que son los siguientes:

— Brújula de la ciberseguridad del ciudadano

— Código de buen gobierno de la ciberseguridad

— Marco de competencias para programas superiores de formación especializada en ciberseguridad

— Impulso a la industria y a la I+D+i. Resumen de propuestas y trabajos de la fase 2

— Informe sobre las necesidades, capacidades y retos para la colaboración público-privada en materia de ciberdefensa en las empresas del sector de la defensa

Agradezco a todos los expertos que, de forma desinteresada, han contribuido con su experiencia y conocimientos a la elaboración de estos trabajos que hoy conforman este libro de ciberseguridad. Una obra, modelo de colaboración publico privado, imprescindible para avanzar en este sector. Un trabajo de colaboración que contribuirá a la concienciación de la sociedad y al refuerzo de las capacidades de España para afrontar los riesgos y amenazas en el ciberespacio.

Miguel Ángel Ballesteros Martín

Director del Departamento de Seguridad Nacional
Presidencia del Gobierno

ÍNDICE GENERAL

FORO NACIONAL DE CIBERSEGURIDAD

BRÚJULA DE LA CIBERSEGURIDAD DEL CIUDADANO

Propuestas para afrontar los principales riesgos en diez ámbitos

Hacia un Plan estratégico de ciberseguridad ciudadana

2023

LA BRÚJULA DE LA CIBERSEGURIDAD DEL CIUDADANO

La **Estrategia Nacional de Ciberseguridad** de 2019 señala la necesidad de una mayor implicación de toda la sociedad, mediante el fomento de una cultura de ciberseguridad, para evolucionar desde la concienciación al compromiso, en el entendimiento de que **el ciudadano es corresponsable de la ciberseguridad nacional**.

Asimismo, como indica la **Carta de Derechos Digitales, los poderes públicos deben velar por el derecho a la ciberseguridad de los ciudadanos**, además de promover la sensibilización y formación en materia de ciberseguridad, para lo que podrán contar con la colaboración de la sociedad civil.

Con el objetivo de abordar desde ambas perspectivas la necesidad de aumentar la concienciación de la sociedad sobre los ciberriesgos que implica el uso de la tecnología, **la Brújula para la ciberseguridad del ciudadano** se concibe como un instrumento orientativo en el que se **analizan diez ámbitos que el Foro Nacional de Ciberseguridad ha considerado que están entre los que representan en la actualidad un riesgo mayor** para la ciudadanía o que necesitan una especial atención.

Para cada ámbito analizado se ha incluido: una introducción a los retos planteados, las necesidades percibidas que pueden tener los ciudadanos en ese ámbito; algunas iniciativas existentes de referencia, a modo de ejemplo, para ayudar a afrontar los riesgos y finalmente, una selección de propuestas dirigidas a los agentes impulsores de la cultura de la ciberseguridad.

Complementando lo anterior, de manera visual a través de un código de semáforo, se presentan, para cada ámbito y por segmentos de la población que se han considerado más vulnerable, el estado de la situación y las recomendaciones principales. Finaliza la Brújula con unas conclusiones y recomendaciones dirigidas a las Administraciones Públicas, con la propuesta de elaboración de un **Plan estratégico de ciberseguridad ciudadana y una Estrategia de protección de menores online.**

Los ámbitos objeto de análisis han sido los siguientes:

1. Redes sociales
2. Contraseñas y credenciales
3. Ingeniería Social
4. Primer acceso a las TIC
5. Trámites y compras online
6. Privacidad e información personal
7. Internet de las cosas
8. Protección del dispositivo
9. Inteligencia artificial
10. Denuncia, soporte y ayuda

Esperamos que esta Brújula cumpla su misión y sirva de orientación en el camino hacia una mayor cultura en ciberseguridad en España.

PORQUE LA CIBERSEGURIDAD ES RESPONSABILIDAD DE TODOS

FORO NACIONAL DE CIBERSEGURIDAD

Autores

Coordinadora sociedad civil:

Ana Isabel Borredá Caballero (Presidenta de la Fundación Borredá)

Coordinadora institucional:

Elena de la Calle Vian (Departamento de Seguridad Nacional)

Autores y colaboradores:

Adrián Capdevila Dueñas

Félix Gómez Mármol

Enrique González Herrero

Eugenia Hernández Sánchez

Mar López Gil

Juan José Martínez Pagán

Casimiro Nevado Santano

Ramón Ortiz González

Antonio Ramos García

Arturo Ribagorda Garnacho

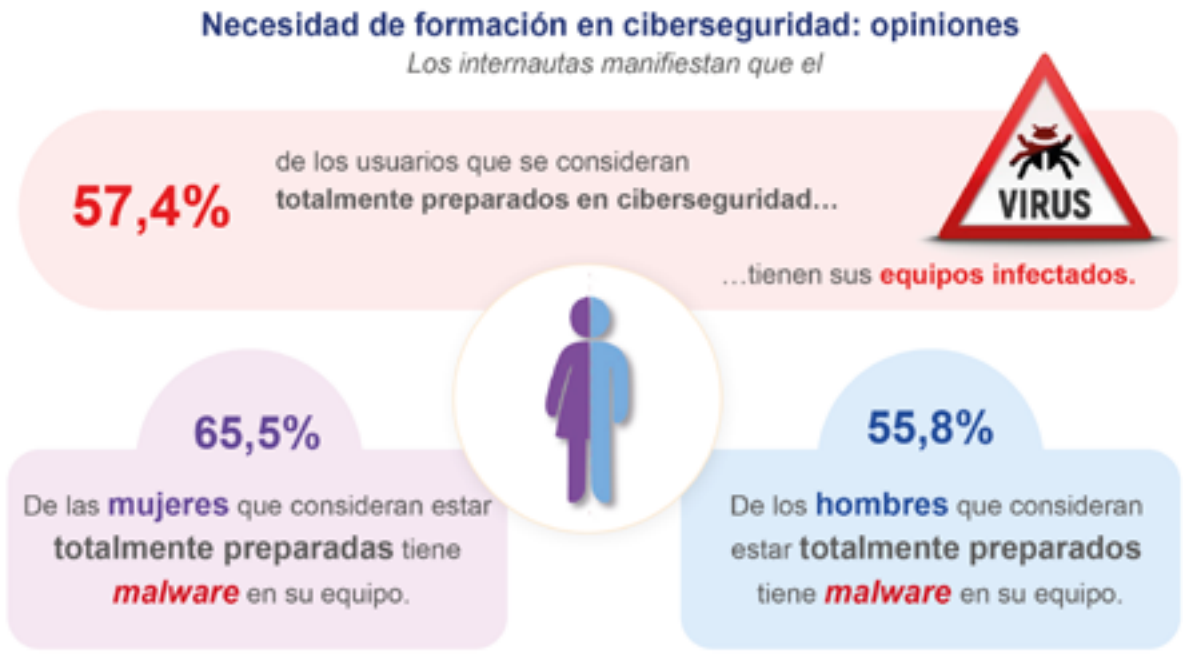
ÍNDICE

1. LA CIBERSEGURIDAD: UN DESAFÍO PARA LA CIUDADANÍA

La tecnología forma parte de la realidad cotidiana de toda la ciudadanía. Especialmente en los últimos años asistimos a una verdadera transformación digital de nuestra sociedad que ha contribuido, sin duda, a mejorar la vida de la población. El desarrollo de nuevas tecnologías permite hoy, por ejemplo, conectar a las personas a grandes distancias, solicitar multitud de servicios desde un teléfono móvil, recibir información de interés en tiempo real o desempeñar acciones cotidianas en el hogar de manera más confortable.

Sin embargo, a pesar de esos avances, es indudable que el **uso de la tecnología también entraña grandes retos, entre los cuales destaca la ciberseguridad**. En este sentido, la implicación del propio usuario resulta imprescindible para poder hacer frente a los riesgos, amenazas y vulnerabilidades que pueden derivarse de los dispositivos y servicios digitales que utiliza. **Conocimientos y habilidades como el establecimiento de medidas de seguridad básicas o el uso responsable de los dispositivos deberían ser cuestiones asumidas por los ciudadanos de manera mayoritaria,** como ocurre en la actualidad en otros ámbitos, por ejemplo, en el de la seguridad vial, **pero la realidad muestra que no es así en términos generales**.

Esa falta de concienciación y corresponsabilidad se aprecia en estudios como el que lleva a cabo periódicamente el **Observaciber**, el observatorio de ciberseguridad dependiente de la Secretaria de Estado de Digitalización e Inteligencia Artificial, cuyo objetivo es fomentar la cultura de la ciberseguridad en España. En su informe titulado ***Cómo se protege la ciudadanía de los ciberriesgos*** (en su edición de abril de 2022) señala que el 41,1% de los participantes declara realizar conscientemente alguna conducta de riesgo en el empleo de sus dispositivos. Por ejemplo, el 39,6% navega sin tener las actualizaciones al día, el 33% pulsa en enlaces de Internet que no saben a dónde le dirigen o el 34,6% descarga aplicaciones de *markets* o páginas no oficiales.



> También resulta reveladora la cantidad de usuarios que consideran estar suficientemente protegidos sin que así sea (según el citado estudio, un 57,4% de los participantes que afirma sentirse totalmente preparado tienen sus equipos infectados) y el desconocimiento que existe de los vectores de ataque o los riesgos reales a los que se enfrentan cuando navegan por Internet o utilizan dispositivos conectados. En consecuencia, desconocen cómo deben actuar ante las diferentes amenazas que existen en este ámbito.

Dada esta carencia de concienciación y conocimientos en torno a los riesgos que existen en el ciberespacio, **los expertos del Grupo de Cultura de Ciberseguridad del Foro Nacional de Ciberseguridad** han llevado a cabo un análisis de algunos de los principales ámbitos en los que los riesgos y amenazas asociados a las tecnologías, o servicios más extendidos o en desarrollo, requieren una especial concienciación y corresponsabilidad por parte de la sociedad, así como de los segmentos de la población más vulnerables a ellos.

2. SEGMENTOS DE POBLACIÓN MÁS VULNERABLES

En cuanto al perfil y los segmentos de población que se pueden considerar más vulnerables a los riesgos y amenazas que conlleva el uso de la tecnología, en relación con la ciberseguridad destacan los siguientes:

Menores de edad

Los menores de edad constituyen uno de los segmentos más vulnerables, especialmente, a partir del momento en el que tienen independencia en el uso de sus propios dispositivos y consumo de contenidos. Es entonces cuando comienzan a registrarse en diferentes servicios, juegos, redes sociales, etc., sin la madurez suficiente y sin el conocimiento apropiado de los riesgos y peligros que existen en el ámbito digital. Coincide, además, con un momento vital en el que puede que cuestionen la autoridad de los adultos y, además, tengan cierta disponibilidad de recursos económicos propios que pueden gastar, por ejemplo, en compras o juegos online.

Dentro de este conjunto de población, es de vital importancia centrarse en los **adolescentes:** menores que empiezan a utilizar la tecnología como vehículo social, académico, laboral, de ocio y económico y que, frecuentemente, pueden mostrar comportamientos impulsivos, inmadurez o poca cultura de ciberseguridad. En este caso, es fundamental que la familia y los educadores, con el apoyo de las autoridades, les ayuden a tomar conciencia del potencial de la tecnología, tanto para lo bueno como para lo malo, hacerles partícipes de los auténticos riesgos a los que están expuestos y acompañarlos en la adquisición de criterio, conocimientos y habilidades.

Personas mayores

Las personas de edad avanzada suelen presentar mayores dificultades a la hora de acceder y utilizar las tecnologías, si bien muchas de ellas se ven abocadas a emplearlas en actividades cotidianas para las que no siempre están capacitadas (por ejemplo, banca online o trámites administrativos en general). Son vulnerables porque, aunque suelen ser muy precavidas, muchas veces son víctimas de estafas por desconocimiento de las técnicas empleadas por los ciberdelincuentes. Otras muchas rechazan directamente la tecnología precisamente porque no la consideran segura y les "da miedo", a pesar de que para ciertas actividades no tengan otra alternativa. Son especialmente vulnerables a acciones en las que se combina una acción cibernética maliciosa con un contacto personal, por ejemplo, a través de una llamada telefónica.

Este segmento no se define exclusivamente por la edad, sino también por la falta de conocimiento y de personas en su entorno familiar en las que apoyarse y a las que poder consultar en caso de necesidad.

Población en edad laboral no concienciada

Este segmento se refiere a las personas que disponen de los conocimientos mínimos necesarios para desenvolverse con la tecnología, sin llegar a ser usuarios avanzados, ni ser plenamente conscientes de los riesgos a los que se enfrentan. El uso de la tecnología tiene un impacto en su vida personal, pero también en el **ámbito laboral,** sea presencial o teletrabajo, dado que algunas acciones individuales pueden tener repercusión en su empresa. Es el caso de los usuarios que no son conscientes de las vulnerabilidades de sus dispositivos y de su red doméstica, pero los utilizan para teletrabajar y conectarse a la red corporativa, con el riesgo de que pueda afectar a su organización si el usuario descarga *malware*, le roban las credenciales, etc. En este marco se encuentran los trabajadores de cualquier organismo, organización y empresa, siendo de particular importancia la atención especial a aquellos que trabajan en infraestructuras críticas y para operadores de servicios esenciales.

Colectivos en riesgo de exclusión

Se han identificado tres colectivos considerados en riesgo de exclusión tecnológica. Sería el caso de los desconectados por su imposibilidad de acceso a la tecnología (sea por cuestiones económicas, escasez de infraestructuras en su lugar de residencia, etc.), las personas con discapacidad y la población extranjera e inmigrantes.

- **Desconectados:** Personas habitualmente desconectadas o sin recursos. En este sentido, es especialmente relevante el subsegmento de habitantes de **zonas rurales** por no estar tan familiarizados, a priori, con nuevas tecnologías, que suelen tener más presencia en las ciudades, y viven en lugares donde existe brecha digital.

- **Personas con discapacidad:** Las personas con discapacidad merecen una atención especial por el efecto multiplicador del riesgo que puede suponer la dificultad de uso si la tecnología no reúne las características de accesibilidad necesarias. Asimismo, las personas con discapacidad intelectual presentan una mayor vulnerabilidad para las acciones de ingeniería social.

- **Población extranjera e inmigrantes**: La falta de concienciación en este caso estaría favorecida por dificultades relacionadas con el idioma, así como por el distinto contexto cultural.


WORLD

3. RIESGOS DE CIBERSEGURIDAD PARA EL CIUDADANO

TOP 1: REDES SOCIALES

Las redes sociales forman ya parte del día a día de millones de personas. Sin embargo, la elevada frecuencia de su uso no siempre viene acompañada de una mayor concienciación sobre los riesgos a las que están expuestas, en especial, el relacionado con la pérdida de la privacidad.

Compartir una publicación, subir una foto o un vídeo, comentar una noticia, crear nuevas amistades, pasar tiempo en ciertos entornos de conexión en tiempo real... Todas estas acciones deberían estar acompañadas de comportamientos ciberseguros, pero no todos los usuarios lo consideran imprescindible hasta que experimentan, de alguna u otra manera, las consecuencias de no haberle dado la importancia debida. En ocasiones, incluso, se difuminan y llegan a traspasarse los límites del entorno personal hacia el mundo laboral.

Cuanto más tiempo pasan las personas en las redes sociales más expuestas están a sus riesgos, y dado que está tendencia sigue aumentando, es necesaria una mayor concienciación sobre las prácticas y comportamientos ciberseguros en estos entornos.

Retos y amenazas que plantea

Esta conexión cada vez más permanente es, en términos de ciberseguridad, un vector de incidentes y exposición de privacidad y, en numerosos casos, también de actividades fraudulentas y criminales. Su utilización constante expone información sobre la vida en el ámbito personal y profesional.

Por otro lado, las redes sociales se extienden como uno de los mecanismos más utilizados para ataques relacionados con la ingeniería social y otras conductas delictivas como el ciberacoso o el *ciberbullying*.

Necesidades de los ciudadanos

- Una formación más específica sobre los temas relacionados con los riesgos existentes en el uso de las redes sociales, tanto en lo que se refiere al control de la información publicada, como a la configuración de la privacidad.

- Una mayor exigencia normativa sobre el aspecto más técnico de la configuración de privacidad.

- Un control más exhaustivo del acceso para los menores de edad, haciendo respetar las condiciones de uso de cada red social y activando mecanismos en otros portales (juego, cripto, banca) para verificar la documentación acreditativa de edad antes del acceso.

- Crear conciencia sobre los riesgos inherentes que supone la utilización de redes sociales. Por ejemplo:

    - Qué supone compartir información (usuarios, claves, contraseñas, pin, claves de la Seguridad Social, Clave Tokens, DNI o identificaciones oficiales, teléfono, correo, mensajes).

    - Vulnerabilidades a las que se expone al navegar en equipos públicos, o de terceras personas, wifis y redes no autorizadas.

    - La importancia de crear contraseñas seguras, actualizar software, usar antivirus.

    - Cómo detectar perfiles legítimos y falsos, enlaces fraudulentos, técnicas de ingeniería social, estafas virtuales.

- Dotar al usuario de hábitos y recursos para incorporarlos en todos los niveles: desde cómo proteger la privacidad de sus datos personales, información

confidencial profesional o cualquier dato sensible, hasta cómo adoptar buenas prácticas para el uso de redes sociales, sitios y plataformas digitales.

Algunas iniciativas de referencia

- Curso presencial para personas con discapacidad y nuevos usuarios sobre el manejo básico de las redes sociales y aplicaciones de videollamada[1].

- Talleres online gratuitos de ciberseguridad, que incluyen un curso específico sobre riesgos y fraudes en redes sociales[2]. Buenas prácticas. Políticas de seguridad para las pymes desarrolladas por el Instituto Nacional de Ciberseguridad. Proporciona las herramientas de seguridad adecuadas para proteger las redes sociales, así como concienciar sobre la necesidad de formar a los administradores antes de desempeñar esta labor[3]:

Propuestas a los actores impulsores de la cultura de la ciberseguridad

Algunas de las actuaciones en las que deben trabajar los actores impulsores de la cultura de ciberseguridad para promocionar un uso más seguro de las redes sociales deberían apoyarse en mensajes más contundentes tales como:

- Clarificación sobre las opciones de privacidad ofrecidas por las redes sociales y el establecimiento de opciones restrictivas en el uso del perfil personal.

- Concienciación y uso del sentido común en el comportamiento ante los desconocidos y sus planteamientos de enlace (*match*) en la red del mismo modo que lo haríamos en el mundo real.

- La no publicación ni facilitación de datos propios que abran la puerta a la identificación de conductas o hábitos que puedan derivar en caer víctimas de un delito.

- Atención a la publicación de imágenes o contenidos de terceros y, especialmente, en el caso de menores.

- Impulsar la implantación efectiva de controles de acceso para los menores de edad.

---

[1] https://plenainclusionmadrid.org/formacion/formacion-redes-sociales-y-videollamada/

[2] https://www.osi.es/es/talleres-ciberseguridad

[3] https://www.incibe.es/protege-tu-empresa/blog/buenas-practicas-redes-sociales-aumenta-tu-popularidad-sacrificar-seguridad

TOP 2: CREDENCIALES Y CONTRASEÑAS

Las credenciales son documentos físicos o digitales que garantizan nuestra identidad. Tienen una relación estrecha con la autenticación, que es el proceso de comprobar nuestras credenciales y gracias al cual es posible verificar que somos quien decimos ser. Las contraseñas, por su parte, son uno de los tipos de credenciales más frecuentes que se usan para comprobar nuestra identidad en los medios digitales.

El uso de contraseñas como único mecanismo de autenticación está desaconsejado en determinados entornos. Son numerosos los métodos que pueden utilizar los actores maliciosos en Internet para conseguirlas[4] y, por ello, para autenticarnos de manera segura, se suele utilizar una combinación de, al menos, dos tipologías diferentes de credenciales, dando lugar a la llamada autenticación de dos factores o a autenticación de factor múltiple. Por ejemplo: una contraseña más una clave única enviada a mi dispositivo; una contraseña más un dispositivo o el reconocimiento facial (característica biométrica) más dispositivo, etc.

La autenticación de usuarios es el primer proceso básico en la cadena de la ciberseguridad de los usuarios. Es de vital importancia, ya que un actor malintencionado que consiguiera nuestras credenciales podría suplantar nuestra identidad a todos los efectos, desde el acceso a nuestras cuentas bancarias, hasta cometer un delito con nuestro nombre[5].

[4] MITRE ATTCK matrix: Credential Access (*The adversary is trying to steal account names and passwords*) https://attack.mitre.org/tactics/TA0006/

[5] Fiscalía general del Estado. Unidad de criminalidad informática. Comunicación usurpación identidad https://www.fiscal.es/documents/20142/fa2280e1-e5ed-b37f-dc3f-6fc3aa3dd6b7

Retos y amenazas que plantea

El primer reto que se plantea es la concienciación de los usuarios. Los procesos de autenticación de factor múltiple, y con tiempos de caducidad de sesión por inactividad, no son percibidos por los usuarios como mecanismos beneficiosos que ayudan a proteger sus activos digitales, sino más bien como mecanismos perturbadores, ante los cuales sienten incomodidad. Es por ello que existe la tendencia a sortearlos por cualquier método y a usar contraseñas inseguras que, en la práctica, vienen a ser lo mismo que no utilizar ninguna[6].

El segundo reto se produce como consecuencia de la alta cantidad de aplicaciones y servicios digitales que utiliza el ciudadano medio que, según recientes estudios, es de 30 diferentes en un mes[7]. El desafío consiste en la dificultad para crear y custodiar de manera segura tantas contraseñas, diferentes para cada una de las aplicaciones o servicios, que además hay que actualizar periódicamente.

Otro reto es la compartición de credenciales con terceras personas. Suele producirse por una causa puntual y, una vez compartida, no se tiene la precaución de cambiar la contraseña.

Además, el *phishing,* junto con el SMS *spoofing* son dos métodos utilizados habitualmente por los ciberdelincuentes para robar credenciales y controlar dispositivos, que a su vez pueden ser usados como credencial. Por ello, la concienciación y el entrenamiento de los usuarios para que sepa reconocerlos y evitar caer en ellos es un reto adicional.

Necesidades de los ciudadanos

La complejidad para el usuario en la gestión segura de credenciales, unida a la sofisticada ingeniería de los cibercriminales, convierten a la gran mayoría de los ciudadanos en personas altamente vulnerables a este riesgo.

Por ello, una parte importante de la responsabilidad de proteger la identificación de los ciudadanos cuando acceden a servicios digitales debe recaer en aquellos que tienen los recursos para implementar los mecanismos adecuados de control de acceso. Por ejemplo, la adopción de mecanismos de autenticación multifactorial y de contraseñas complejas, el uso de la biometría, etc[8]. Esto debe ser considerado como una responsabilidad

[6] https://unaaldia.hispasec.com/2022/12/las-contrasenas-mas-utilizadas-de-2022.html

[7] Mobile App Download Statistics & Usage Statistics (2022) https://buildfire.com/app-statistics/

[8] Four user authentication issues developers and admins struggle with (solved). https://www.smseagle.eu/2020/01/27/4-user-authentication-issues-developers-and-admins-struggle-with-solved/

importante de las empresas que ofrecen servicios críticos al ciudadano y también de las administraciones públicas.

En este sentido, cabe destacar como ejemplo el uso del certificado digital y el DNI electrónico, que proporcionan a los ciudadanos accesos de alto nivel de seguridad a los servicios públicos. En este sentido, sería conveniente facilitar más tutoriales y guías de ayuda a los usuarios, como las que ofrece la página del DNI electrónico[9] para configurar el uso de dichos mecanismos.

Asimismo, sería necesario el incremento de tutoriales y contenidos audiovisuales para concienciar a los usuarios y enseñarles cómo configurar factores de autenticación múltiple en los servicios digitales que utilizan.

Algunas iniciativas de referencia

- INCIBE, la opción de documentos para el empleado de la sección "Protege tu empresa" ofrece una guía muy completa y detallada sobre la gestión de contraseñas[10].

- La Oficina de Seguridad del Internauta (OSI) ha lanzado una campaña con el nombre "Contraseñas seguras", que presenta una serie de artículos sobre las contraseñas. En ellos cubre aspectos como la concienciación, buenas prácticas y el uso de gestores de contraseñas[11].

- El CCN-PYTEC ofrece una guía completa sobre autenticación multifactor en la que se definen los requisitos mínimos para cumplir con el Esquema Nacional de Seguridad (ENS)[12].

---

[9]Ejemplo de uso del DNI electrónico: https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_1079&id_menu=%5B17

[10]https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/contrasenas.pdf

[11]https://www.osi.es/es/campanas/contrasenas-seguras

[12]https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/boletines-pytec/353-pildorapytec-oct2020-autenticacion-multifactor/file

Propuestas a los actores impulsores de cultura de ciberseguridad

- Programas de concienciación y educación en ciberseguridad. Con eslóganes como “tu contraseña es la llave de tu casa, ¿la dejarías en un lugar donde cualquiera la pudiera coger?”.

- Cybervoluntarios en las escuelas, asociaciones de vecinos y centros de mayores que ayuden a las personas con pocos conocimientos a utilizar el certificado digital.

- Facilitar el acceso a gestores de contraseñas, con una subvención si fuera necesario (al igual que existe una subvención para el Kit Digital).

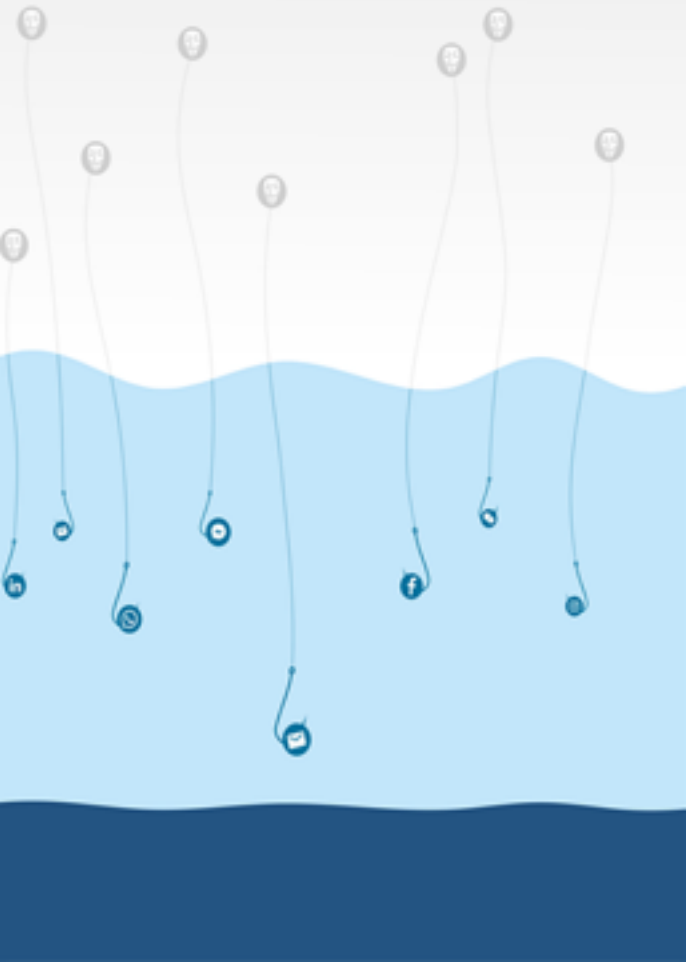
- Impulso del uso de biometría como mecanismo de autenticación, sin menoscabo de su consideración como dato personal sensible.

- Fomento de la responsabilidad compartida entre proveedores y usuarios en el uso de credenciales y la gestión de la autenticación, para evitar las malas prácticas de los dueños de los sistemas si, por ejemplo, no disponen de autenticación de factor múltiple o permiten contraseñas débiles.

TOP 3: ATAQUES DE INGENIERÍA SOCIAL

La ingeniería social consiste en la manipulación psicológica de los usuarios para acceder a sus datos sensibles. Incluye la suplantación, el engaño, la manipulación y, en general, el abuso de la confianza de las personas para que revelen información o realicen acciones perjudiciales para ellas mismas o para terceros sin que sean conscientes de ello. Entre estas acciones se incluye el acceso a las cuentas bancarias de la víctima, el robo de su identidad en redes sociales, el acceso a información privada, como fotos y vídeos, el uso de su dispositivo para atacar a otras víctimas, etc.

Cualquier persona puede ser víctima de un ataque de ingeniería social, pero las personas con menos dominio de la tecnología están más expuestas, tardan más tiempo en darse cuenta y, en muchas ocasiones, no saben a quién recurrir si son víctimas de este tipo de ataque.



La ingeniería social puede entrar en la vida de los ciudadanos por varias vías:

- A través del teléfono, haciéndose pasar por una persona o entidad de confianza y pidiendo que se entreguen contraseñas, dinero o acceso remoto al ordenador. En los casos de v*ishing,* los ciberdelincuentes imitan voces mediante el uso de Inteligencia Artificial.

- Por email, a través de un correo con un enlace o un archivo adjunto malicioso, dando lugar al *ransomware* o secuestro de datos.

- A través de un dispositivo externo como un USB que, entregado como obsequio, contenga *malware* con el objetivo de entrar en sistemas de la competencia y poder espiarles.

- Por Internet, a través de la nueva técnica *deep-fake*, que es como se conoce a las alteraciones en el rostro y la voz de una persona mediante el uso de un software con Inteligencia Artificial.

Retos y amenazas que plantea

La ingeniería social sirve para llevar a cabo diversos tipos de ataques, que suponen el verdadero reto de esta amenaza:

- *Phishing*: consiste en el envío de correos electrónicos o mensajes de texto falsos que simulan provenir de instituciones, bancos, tiendas online, etc., proporcionando enlaces a páginas no oficiales que emulan perfectamente la estética de las páginas oficiales de dichas entidades donde se le solicita ingresar credenciales como nombres de usuario y contraseñas.

- Duplicación de la tarjeta SIM: consiste en la solicitud al operador de telecomunicaciones de una nueva tarjeta, suplantando la identidad de la víctima y así utilizarla para validar transacciones bancarias.

- Interceptación de mensajes SMS: es la interceptación mediante ingeniería de comunicaciones de los mensajes SMS enviados a un número de teléfono, para validar transacciones bancarias y robar dinero.

- Lectura de códigos QR: consiste en insertar un archivo infectado o una URL maliciosa en un código QR con la finalidad de llevarnos a una página de pagos falsa que emule a la del comercio u organismo oficial al que están suplantando, o descargue el archivo malicioso en nuestro dispositivo.

Necesidades de los ciudadanos

Es necesario empoderar a los ciudadanos a través del **autoconocimiento y la formación** en esta temática. Son los sesgos cognitivos y tipo de personalidad que tenemos los que están al mando de la mayor parte de nuestros pensamientos y acciones. Los cibercriminales conocen esos sesgos cognitivos y analizan los tipos de personalidad que existen, saben a qué reacciona cada cual, qué les llama la atención, a qué les resulta irresistible dar click. Nuestra personalidad nos hace vulnerables.

Para formar adecuadamente (en cantidad y calidad) a los usuarios en materia de ciberseguridad, es necesario reducir la vulnerabilidad que podría encarnar cada elemento humano en la sociedad, precisamente por la impredecibilidad que tienen las personas en su comportamiento. La **neurociberseguridad** es una forma de empoderar a los usuarios a través del autoconocimiento, donde se debe facilitar un diálogo entre la neurociencia a través de los procesos cognitivos y la seguridad en el ámbito digital. Así entenderán y serán conscientes de los procesos cognitivos que explican el éxito de los ciberataques y podrán evitarlos.

También se requiere **concienciación y divulgación atractiva a través de campañas de comunicación masivas** para generar nuevos hábitos en el ámbito digital en la ciudadanía:

Algunas iniciativas de referencia

Phishing:

- INCIBE protege tu empresa. Sección dedicada al *phishing* con ejemplos y descripciones detalladas y consejos para evitarlo[13].
- El CCN-CERT, en la sección de su web "Defensa contra amenazas", ofrece dos *hashtags* de Twitter en los que publica regularmente información y alertas actualizadas sobre campañas de *phishing* y *malware*[14]:
- La Universidad Veracruzana (México) ha creado una página de concienciación a la que llegas después de clicar en un enlace engañoso originado por ellos mismos. Sirve como entrenamiento[15].

SIM-Swaping:

- La Oficina de Seguridad del Internauta ofrece en su blog un artículo muy detallado con instrucciones precisas para evitarlo y un video explicativo[16].

Códigos QR:

- INCIBE, en la sección de su web "Protege tu empresa", cuenta con una página explicando los riesgos y ofrece consejos a las empresas para evitar que sus códigos QR sean manipulados o suplantados con fines maliciosos[17].

---

[13] https://www.incibe.es/protege-tu-empresa/tematicas/phishing

[14] #NoTeinfectesConElMail y #CiberCOVID19

[15] https://www.uv.mx/csirt/concientizacion-phishing/

[16] https://www.osi.es/es/actualidad/blog/2022/06/09/sim-swapping-como-evitar-esta-estafa

[17] https://www.incibe.es/protege-tu-empresa/blog/protege-los-codigos-qr-y-no-pongas-riesgo-seguridad-tus-clientes

Propuestas a los actores impulsores de cultura ciberseguridad

- Lanzamiento de enlaces engañosos que lleven a una página que sirva como concienciación y educación a los ciudadanos, como lo hace la Universidad Veracruzana, o lo hacen algunas empresas con sus empleados.

- Campañas de concienciación masivas basadas en el autoconocimiento para el empoderamiento de la ciudadanía, aportando más valor e información, más allá de los hábitos.

- Aplicaciones gratuitas para lectura de código QR, que permitan visualizar la URL antes de acceder a ella.

- Mensajes más contundentes sobre la amenaza del *phishing*, de los QR maliciosos y cómo darnos cuenta de que hemos sido víctimas.

TOP 4: PRIMER ACCESO A LAS TIC

La iniciación a las TIC se produce a edades cada vez más tempranas, hasta el punto de que utilizamos el apelativo de nativos digitales para describir las destrezas de las nuevas generaciones.

En paralelo, hay personas que comienzan a aprovechar las posibilidades que ofrecen las tecnologías conectadas a edades tardías, lo que requiere un esfuerzo importante de capacitación para poder utilizar con confianza y seguridad los servicios digitales.

En ambos casos, el primer acceso a las TIC es un proceso que merece especial atención, así como mayores esfuerzos de concienciación y formación.

Retos y amenazas que plantea

El uso de las TIC supone un reto para toda la sociedad debido a los riesgos y amenazas que existen en el ámbito digital, pero más si cabe para las personas que comienzan a utilizar dispositivos conectados, como podrían ser los teléfonos móviles, las tabletas o los ordenadores. Los riesgos a los que se enfrentan los colectivos de menores y personas de avanzada edad que comienzan a utilizar las TIC son comunes con el resto de los ciudadanos, con el añadido de un acentuado desconocimiento, *a priori*, tanto del uso de los dispositivos como de las amenazas que habitan en la red.

El robo de información personal, la suplantación de identidad, el fraude, el acoso en sus diferentes modalidades o la difamación en redes sociales son algunas de las amenazas más comunes para los menores y, en su mayor parte, también para los ciudadanos de edad avanzada. En el caso de los menores, debido a la inmadurez propia de la edad, el uso de la tecnología les vuelve más vulnerables a la adicción o futura ludopatía.

Necesidades de los ciudadanos

En el caso de los menores y adolescentes, que van introduciéndose en el uso de dispositivos móviles, vemos cómo utilizan especialmente los teléfonos o las tabletas para acceder a servicios como las redes sociales, aplicaciones de comunicación o a los juegos en línea. Esta iniciación requiere una educación adaptada a los más pequeños para que hagan un uso responsable de dichos servicios y estén preparados para detectar y evitar los riesgos y amenazas que afectan a su uso. Es importante sensibilizar a los adultos de la necesaria supervisión en virtud del especial deber de vigilancia, como pueden ser los padres o tutores respecto de sus hijos o pupilos o los titulares de un centro docente respecto de los alumnos.

Igualmente, las personas mayores que hasta ahora estaban desconectadas se ven abocadas al uso de tecnologías para llevar a cabo determinadas operaciones de la Administración o de las entidades financieras, que les obligan a hacer uso de dispositivos y procesos informáticos hasta entonces desconocidos para ellos. Por ello, es necesario que también los mayores que están aprendiendo a utilizar estas herramientas conozcan y tomen conciencia de los riesgos que entraña su utilización.

Algunas iniciativas de referencia

- La extinta Agencia de Protección de Datos de la Comunidad de Madrid puso en marcha hace dos décadas charlas para adolescentes en los colegios en las que estaban involucrados los propios profesores de informática.

- Internet Segura 4 Kids (is4K): esta iniciativa de INCIBE es el Centro de Seguridad en Internet para menores de edad en España[18].

- Experiencia Senior: se trata de un programa de concienciación para mayores de 60 años, también lanzado por INCIBE. Su objetivo es impulsar y potenciar las habilidades digitales de los usuarios mayores de 60 años con materiales específicos y formativos, que les permitan adquirir las nociones básicas necesarias para desenvolverse con confianza y seguridad cuando naveguen por Internet[19].

Propuestas a los actores impulsores de cultura de la ciberseguridad

- Elaborar una hoja de ruta de formación que se plasme en iniciativas de todo tipo adaptadas a la edad de los más jóvenes, como pueden ser la grabación de contenidos audiovisuales infantiles, charlas en los centros educativos, aplicaciones o juegos que les permitan aprender mientras se entretienen. En definitiva, es necesario adaptar formatos y mensajes a los menores para poder llegar a ellos de manera eficaz. En ese sentido, es fundamental contar con los educadores, quienes realmente conocen esas necesidades.

- Por otro lado, son los padres quienes tendrán que desempeñar un papel principal en la educación y el cuidado del acceso a las TIC de sus hijos. En ese sentido, han de ser conscientes y transmitir la corresponsabilidad que supone utilizar las tecnologías. El primer acceso a las TIC requiere también acciones orientadas a

[18] https://www.is4k.es/necesitas-saber

[19] https://www.osi.es/es/experiencia-senior

los padres, como puedan ser campañas de sensibilización o actividades lúdico-educativas que puedan llevar a cabo conjuntamente progenitores y menores.

- El ámbito educativo también debe estar implicado en la formación y concienciación de los menores cuando comienzan a utilizar las tecnologías. Convendría alcanzar acuerdos y convenios al más alto nivel para que los colegios incorporen actividades destinadas a dicho fin, en las que estén involucrados tanto los educadores, como los padres, expertos en la materia y, evidentemente, los menores.

- En el caso de las personas mayores, igualmente requiere que los mensajes y contenidos que contribuyan a su formación estén adaptados a su edad e intereses. Uno de los aspectos clave al respecto es evitar provocar miedo a la hora de utilizar sus dispositivos, sino todo lo contrario, confianza y herramientas para que estos usuarios sepan reaccionar ante los retos que se les planteen.

- Las campañas de concienciación son una herramienta muy útil, pero insuficiente si no van acompañadas de otras acciones. En este sentido, se deben identificar las vías de acceso a ese segmento de población, localizando sus centros de encuentro, en ciudades y zonas rurales, o los medios de comunicación más populares entre los mayores, para que las actividades formativas lleguen al público objetivo.

- Al igual que los jóvenes, resultaría interesante involucrar a los descendientes de las personas mayores, ya sean sus hijos, nietos, sobrinos o cualquier otro familiar que pueda ayudarles, por ejemplo, mediante actividades compartidas lúdico-formativas.

- Las entidades financieras, la Administración y todas aquellas organizaciones que requirieran el uso de la tecnología para poder beneficiarse de sus servicios, deberían participar en iniciativas que ayudasen a entender y conocer cómo protegerse en la Red.

TOP 5: TRÁMITES Y COMPRAS ONLINE

La tecnología digital nos ha traído grandes beneficios, pero también ha generado nuevos riesgos para los usuarios en el comercio electrónico, la navegación web y la realización de gestiones online. El fraude en el comercio electrónico ha aumentado más rápido que la cifra de ventas, alcanzando un importe a nivel mundial de 41.400 millones de euros[20].

El fraude puede producirse de muchas maneras, como la suplantación de identidad, el robo de credenciales de una tarjeta de crédito o la publicación de ofertas falsas por las que el usuario nunca recibirá el producto adquirido. Es perjudicial tanto para los usuarios finales, como para las empresas, siendo particularmente sensibles las pymes por su menor capacidad de inversión para dotarse de los medios de protección.

Retos y amenazas que plantea

Los vectores de ataque y métodos utilizados por los ciberdelincuentes para perpetrar sus ataques son múltiples. Citamos algunos:

- Observación visual si introducimos nuestras claves en un lugar público.
- Interceptación del tráfico para robar contraseñas si estamos en una WiFi pública y no estamos utilizando una VPN.
- Introducción de las claves de mi tarjeta de crédito en un sitio web o una pasarela de pagos fraudulenta, si no somos capaces de verificar el grado de confianza del sitio.
- Interceptación de nuestras claves y de nuestra tarjeta de crédito por *malware* que se haya introducido en nuestro equipo si no tenemos actualizado el antivirus.
- Interceptación de nuestras claves y nuestra tarjeta de crédito por *malware* que se haya introducido en un sitio de *e-commerce* si la empresa que gestiona el sitio no ha parcheado las vulnerabilidades.

[20] Juniper Research: Online payment fraud: markets forecast, emerging threats & Segment analysis 2022-2027 https://www.juniperresearch.com/researchstore/fintech-payments/online-payment-fraud-research-report

- Ciberanzuelos o *phishing* vía *email*, SMS o ingeniería social. Un engaño mediante el cual nosotros mismos estamos facilitando nuestras claves al cibercriminal sin ser conscientes de ello.

- Duplicación fraudulenta de nuestro módulo SIM por el ciberdelincuente para interceptar los códigos de validación SMS.

- Falta de disciplina en la custodia de nuestras contraseñas, registrándolas en algún sitio desde donde puedan ser robadas, no actualizándolas periódicamente o utilizando una misma contraseña para varios servicios.

- Introducir nuestras credenciales en un sitio web que no tiene implementado el protocolo https (el candadito verde del navegador), permitiendo así que la comunicación pueda ser interceptada por un ciberdelincuente.

Con tantas posibles vías de ataque, el mayor reto es la concienciación y formación del ciudadano, para que sea capaz de elaborar sus propias estrategias y rutinas, adaptadas a las circunstancias personales que le permitan utilizar los servicios de la manera más segura posible.

El segundo reto es la disponibilidad y conocimiento del uso de herramientas, siendo imprescindibles los antivirus o EDR en todos los dispositivos, y su correcta configuración y actualización.

Necesidades de los ciudadanos

El ciudadano de a pie necesita conocer aspectos básicos de ciberseguridad como, por ejemplo, saber identificar si un sitio web es seguro y quién es el titular de este; las recomendaciones básicas de seguridad y buenas prácticas para operar en la red y realizar compras y gestiones; los riesgos a que se enfrenta y sus posibles consecuencias; los métodos de ataque o engaño más comunes y evitarlos. Si es una pyme o un autónomo, además necesita conocer qué tiene que hacer para ofrecer sus servicios digitales de manera segura para sus clientes y para sí mismo. En cualquier caso, en consonancia con lo anterior, la necesidad más primordial del ciudadano como consumidor o profesional es la formación en ciberseguridad.

Por otro lado, es necesario contar con una normativa clara que delimite las responsabilidades entre proveedores y usuarios de servicios digitales en caso de ataque cibernético o fraude.

Finalmente, cabe destacar que incluso con la mejor concienciación y educación se hace difícil gestionar todas las prácticas necesarias para una ciberseguridad personal sin apoyarse en herramientas. El ciudadano necesita una caja de herramientas de

ciberseguridad, a ser posible integrada y de fácil acceso, que incluya como mínimo lo más básico: antivirus o EDR, verificador de URL y gestor de contraseñas, además de un lector para el DNI electrónico.

Iniciativas de referencia

- La Asociación Española de Banca dispone de un portal con contenido formativo para usar de forma segura sus plataformas[21].
- OSI-INCIBE: Compra segura en internet[22].
- Guía de Ciberseguridad en el comercio electrónico[23].
- Cursos y tutoriales sobre compras online[24].

Propuestas a los actores impulsores de cultura ciberseguridad

- Inclusión de la ciberseguridad personal como materia en los ciclos de enseñanza obligatoria.
- Creación de una caja de herramientas de seguridad digital, conteniendo, al menos, los elementos mencionados en la sección anterior. Esto se podría proveer como un Kit Digital gratuito para los ciudadanos.
- Promover la elaboración de guías de consejos y seguridad para el uso de aplicaciones comerciales de pagos online, para que los ciudadanos puedan utilizarlas de forma segura.
- Promover la elaboravión de Kit de Consejos y configuración en las entregas de tarjetas y/o integración de medios de pagos en móviles (tecnología NFC) por parte las entidades financieras.
- Promover la emisión y popularización, por parte de los bancos y entidades de crédito, de tarjetas de crédito con numeración virtual o tarjetas de pago recargables.

---

[21] https://www.aebanca.es/category/ciberseguridad/

[22] https://www.osi.es/sites/default/files/docs/guia_compra_segura_internet_web_vfinal.pdf

[23] https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_comercio_electronico_metad.pdf

[24] https://concienciat.gva.es/cursos/compras-online-seguras/; https://www.osi.es/es/pagos-online

- Promover el aprovechamiento de los recursos de los fabricantes de sistemas operativos de los principales móviles para ofrecer consejos de seguridad a los usuarios.
- Divulgar el conocimiento de los sellos de confianza de las páginas web y su significado.
- Delimitar las responsabilidades en caso de fraude, así como las consecuencias si no se han adoptado las medidas de seguridad necesarias por las distintas partes.

TOP 6: PRIVACIDAD E INFORMACIÓN PERSONAL

Desde la antigüedad, los individuos han percibido el valor de sus datos personales, pero no es hasta que el uso de las tecnologías de la información y las comunicaciones se generaliza cuando esta percepción se torna en preocupación por las capacidades de estas tecnologías para capturar, procesar, almacenar y transmitir datos e información personal.

Este derecho a la privacidad está regulado por el *Reglamento europeo 679/2016* de protección de datos personales y su adaptación a nuestro entramado legal, *la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales Personales.*

Estas disposiciones instituyen, entre otras, un conjunto de deberes para los responsables del tratamiento de estos datos, otorgan unos derechos a las personas físicas, prevén para cada Estado miembro una o varias autoridades de control independientes y establecen un conjunto de sanciones administrativas para los responsables en caso de incumplimiento.

Retos y amenazas que plantea

El principal reto es concienciar a las personas físicas en la importancia de sus datos personales y la necesidad de ser muy cautelosos cuando se ceden a terceros ante la enorme capacidad de las tecnologías de la información para recopilar, procesar, almacenar, transmitir datos, en especial en lo referente a datos sensibles, como los

relativos a la salud, ideología, opiniones políticas, vida u orientación sexual, origen étnico o racial, convicciones religiosas o filosóficas, la afiliación sindical, etc.

Mención aparte merecen las *cookies* que almacenan los datos de navegación en una web para transmitirlos después al responsable de esta, lo que puede permitirle conocer nuestros hábitos, preferencias, aficiones, idioma, etc.

Necesidades de los ciudadanos

Para afrontar estos retos y desafíos, los ciudadanos precisan, básicamente, conocer:

- Qué es un dato de carácter personal.
- Los derechos que les asisten según las disposiciones legales: acceso, rectificación, supresión, limitación de tratamiento, oposición y portabilidad de los datos.
- Las condiciones de licitud del tratamiento de sus datos:
    - El interesado dio su consentimiento expreso, informado, libre, específico e inequívoco (consentimiento que debe poder ser retirado en cualquier momento tan fácilmente como se otorgó).

Que dicho tratamiento sea necesario para:

    - La ejecución de un contrato.
    - El cumplimiento de una obligación legal.
    - Proteger intereses vitales del interesado o de terceros.
    - El cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos.
    - La satisfacción de intereses legítimos del responsable del tratamiento o de un tercero.
- Ante quién y cómo proceder si considera conculcados sus derechos, el tratamiento de sus datos no se ha ejecutado bajo los principios de protección de datos o sin una base legitimadora adecuada.

Algunas iniciativas de referencia

- Educar en seguridad y privacidad digital: Curso organizado por la AEPD, el INCIBE y el INTEFP[25].

Propuestas a los actores impulsores de cultura ciberseguridad

- Identificar a los colectivos cuyos miembros están especialmente expuestos y realizar acciones de divulgación dirigidas específicamente a ellos.

- Impulsar acciones de divulgación en los colegios a través de las asociaciones de padres y madres (CEAPA, CONCAPA, AMPA, etc.) y las consejerías de educación de las comunidades autónomas.

- En el caso de personas mayores, canalizar las acciones a través de asociaciones de pensionistas, uniones de jubilados, asociaciones de mayores, etc., y las consejerías con competencias en el bienestar de los mayores. Así como ONGs como Cruz Roja, Cáritas, etc.

- Fomentar la corresponsabilidad de los ciudadanos, que pasa por conocer en primer lugar qué se entiende por datos personales, las categorías especiales de datos personales, los derechos que le asisten y los canales de denuncia, además del seguimiento de una serie de consejos en su navegación por internet. Por lo que respecta a los consejos en la navegación por Internet, se encuentran, entre otros:

    - No facilite información personal salvo que sea informado, al menos, de la identidad del responsable o encargado del tratamiento, la finalidad del tratamiento, los derechos que le asisten y ante quién ejercitarlos, la dirección electrónica u otro medio donde acceder al resto de informaciones obligadas por la normativa de protección de datos.

    - No proporcione información personal de terceros excepto que se haya obtenido su consentimiento.

    - Revise periódicamente la configuración de privacidad de sus cuentas en redes sociales.

    - Sea muy cauto con las informaciones personales que publique procurando que sean las mínimas, así como con las informaciones personales almacenadas en el móvil.

[25] https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-aepd-incibe-e-intef-lanzan-un-nuevo-curso-de-formacion

- Desconfíe de los correos de desconocidos con faltas de ortografía, de ofertas muy atractivas que transmitan premura, *phishing*, ya que suelen solicitar datos personales como números de cuentas bancarias o instan al usuario a conectarse a páginas web con el mismo propósito.

- Si guarda información personal en la nube, configure adecuadamente las opciones de privacidad, asegurándose de que el canal de transferencia de datos trabaje bajo https, cifrando sus datos (aunque ya lo haga el proveedor del servicio) y manteniendo copias de seguridad en un soporte convencional.

- Si usa un sensor para monitorizar su actividad física, compruebe los ajustes del dispositivo para preservar su privacidad y no comparta la información registrada en las redes sociales.

TOP 7: INTERNET DE LAS COSAS

Hoy en día existen multitud de dispositivos cotidianos que están conectados a Internet y que recaban, tratan, almacenan y transmiten información del usuario, que puede ser de carácter básico o, incluso, en algunos casos de especial protección, como los datos relacionados con la salud. Se trata de tecnologías que tienen el objetivo de hacer más sencillas y eficientes determinadas actividades y que proporcionan, además, información de valor al usuario. Por ejemplo, a la hora de cocinar, hacer deporte, ver la televisión, etc. Es lo que conocemos como Internet de las Cosas (IOT).

El 16 de julio de 2020, la Comisión puso en marcha una investigación sectorial sobre el Internet de las Cosas de consumo[26] en la UE. Las conclusiones de la investigación confirmaron que, en general, cada vez más dispositivos y servicios se están convirtiendo

[26] https://competition-policy.ec.europa.eu/system/files/2022-01/internet-of-things_final_report_2022_es.pdf

en «inteligentes», lo que permite a los usuarios acceder a una gama cada vez más amplia de dispositivos y servicios interconectados dentro y fuera de sus hogares.

Según la Comisión Europea se espera el despliegue de más de 41.000 millones de dispositivos IoT para 2025. Uno de los principales retos del IoT tiene que ver con la capacidad de manejar volúmenes diversos y muy grandes de dispositivos conectados, así como con la necesidad de identificarlos de forma segura para que puedan conectarse a las redes de IoT[27].

En este sentido, se hace una especial alusión a los asistentes de voz que permiten a los usuarios acceder a una amplia gama de funciones, como reproducir música, escuchar la radio, noticias o podcasts, controlar dispositivos domésticos inteligentes, brindar información o ayudar en la planificación y ejecución de rutinas diarias, así como a las aplicaciones móviles inteligentes o las aplicaciones complementarias, interfaces de usuario para acceder a dispositivos inteligentes y servicios de IoT para consumidores.

Las soluciones de IoT se utilizan también dentro del contexto de las llamadas ciudades inteligentes o *smart cities*, con el objetivo de crear un entorno interconectado en las ciudades en el que se mejore el uso de los recursos y se proporcionen servicios de manera más inteligente, tanto en el transporte urbano como en el suministro de agua o en los sistemas de calefacción, entre otros muchos ámbitos.

Retos y amenazas que plantea

Los dispositivos asociados al IOT pueden contener vulnerabilidades, ya sea por su configuración, infraestructura o características. Teniendo en cuenta que esta tecnología recoge y procesa información de los usuarios, es fundamental poner atención en su protección y uso.

A esto hay que sumar que los dispositivos IoT están relacionados o conectados cada vez más con otras tecnologías como el Big Data, 5G o la Inteligencia Artificial, lo que incremente los riesgos a los que están sujetos estos dispositivos.

Los usuarios deben conocer los riesgos y las medidas de seguridad básicas cuando adquieren dispositivos que tengan la capacidad de conectarse a Internet para evitar que los ciberdelincuentes se hagan con su control, invadiendo la privacidad del usuario o generando situaciones de riesgo. En este sentido, es destacable lo señalado por la propuesta de Reglamento Europeo de Ciberresiliencia[28] , en el que se pone de manifiesto la insuficiente comprensión de la información y del acceso a ella por parte de los usuarios

[27] https://digital-strategy.ec.europa.eu/en/policies/internet-things-policy

[28] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52022PC0454&from=ES

lo que les impide elegir productos con las características de ciberseguridad adecuadas o utilizarlos de manera segura.

Tal y como apunta el INICIBE[29], a menudo el usuario no es consciente del tratamiento de datos llevado a cabo por los dispositivos sensorizados. Los mecanismos convencionales utilizados para obtener el consentimiento de los usuarios son considerados consentimientos de baja calidad debido a que en muchos casos se basan en la falta de información que recibe el usuario sobre el posterior tratamiento de los datos personales que está proporcionando. Además, esta información puede llegar a manos de terceros sin que el usuario sea consciente de su difusión.

En el día a día pueden encontrarse con la inutilización de los dispositivos conectados, la perdida de privacidad, vigilancia no autorizada, problemas para la salud o participación en actividades ilícitas por la utilización de los dispositivos conectados para formar parte de una red zombi para lanzar ciberataques a gran escala.

Necesidades de los ciudadanos

Conocer:

- Qué es el IoT, para qué sirve y en que les afecta desde el punto de vista de la seguridad.
- Aspectos relativos a la protección de datos y a la privacidad en el uso del IoT.
- Configuraciones de seguridad que pueden implementarse en dispositivos conectados.

Algunas iniciativas de referencia

- La Oficina de Seguridad del Internauta del Instituto Nacional de Seguridad, contempla un espacio específico sobre el IoT, los riesgos de un mundo hiperconectado[30].
- Informe de buenas prácticas en el IoT del CCN CERT[31].

---

[29] https://www.incibe-cert.es/blog/riesgos-y-retos-ciberseguridad-y-privacidad-iot

[30] https://www.osi.es/es/campanas/iot-los-riesgos-de-un-mundo-hiperconectado

[31] https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/2258-ccn-cert-bp-05-internet-de-las-cosas/file.html

Propuestas a los actores impulsores de cultura ciberseguridad

- **Guía Básica de Seguridad IoT**: las guías actuales están orientadas a las empresas, pero no tanto a la concienciación y buen uso por parte de la sociedad en general.

- **Concienciar sobre las obligaciones existentes** de informar a los consumidores de los riesgos de los dispositivos conectados a Internet si no se toman medidas de seguridad y se hace un uso responsable de ellos.

- **Acciones de concienciación** sobre un uso higiénico de los dispositivos IoT, para que los usuarios implementen medidas básicas necesaria, como las siguientes: cambiar las contraseñas por defecto que traen de fábrica estos dispositivos; crear contraseñas seguras para el acceso a las aplicaciones de los dispositivos IoT; instalación de antivirus o la configuración adecuada de la red doméstica, entre otras.

TOP 8: PROTECCIÓN DEL DISPOSITIVO

La capacidad de procesamiento y conexión con la que cuentan los dispositivos actuales (ordenadores, móviles, tabletas, *wearables*, aparatos conectados, etc.) tiene como consecuencia que los usuarios estén cada vez más expuestos a los riesgos que entraña el mal uso o funcionamiento incorrecto de los mismos.

Las consecuencias de esta situación pueden ir desde una simple molestia (por ejemplo, no saber cuántos pasos ha contabilizado nuestro *smartwatch* esta semana) hasta restricciones operativas muy serias, como robos de información, suplantación de identidad, sustracción de dinero y un largo etcétera.

Por este motivo, es esencial que los usuarios implementen medidas de protección de sus dispositivos y de la información que contienen, de manera que se minimicen en lo posible las amenazas a las que están sujetos. A esto se une la necesidad de hacer un uso correcto de los dispositivos, evitando prácticas que faciliten que los riesgos mencionados se materialicen.

Retos y amenazas que plantea

Nuestra sociedad tiene una cada vez mayor dependencia de los dispositivos conectados, especialmente, de teléfonos móviles, equipos informáticos y tabletas. Dicha dependencia es tal que estos aparatos se han vuelto en muchas ocasiones imprescindibles para realizar algunas actividades cotidianas, tanto en el ámbito personal como en el profesional.

El principal reto es proteger adecuadamente tanto los dispositivos en sí como la información que contienen. Es preciso concienciar de que es necesario implementar en los dispositivos medidas de seguridad tales como establecer claves de acceso al aparato, instalar antivirus, actualizar el software periódicamente, realizar copias de seguridad, utilizar aplicaciones de detección en caso de pérdida, mantener activo el *firewall*, navegar a través de VPN y así hasta cubrir las distintas necesidades en función del uso que haga de ellos. De lo contrario, el usuario estará dejando la puerta abierta a accesos no deseados que no solo socaven su privacidad, sino que les causen un perjuicio significativo como pudiera ser el robo de claves o acceso a información sensible.

Evitar las amenazas conlleva asumir la responsabilidad de aplicar medidas como las mencionadas y además llevar a cabo buenas prácticas durante la utilización de sus dispositivos. Esto supone, en muchos casos, aplicar el sentido común y la cautela para evitar situaciones –lamentablemente habituales– como escribir las claves de acceso o contraseñas y pegarlas al propio dispositivo, descargar archivos de páginas web no verificadas como seguras, dejar acceso libre a sus ordenadores o móviles, conectarse a redes abiertas sin protección, etc. En definitiva, otro de los retos actuales es concienciar a la población de la importancia de emplear la tecnología de manera adecuada, esto es, minimizando los riesgos de manera activa.

Necesidades de los ciudadanos

La protección de los dispositivos implica una participación proactiva de los usuarios, pues son ellos quienes habrán de adoptar la mayor parte de medidas destinadas a su seguridad. No obstante, es necesario que los propios dispositivos incorporen medidas de seguridad de la información y las comunicaciones, y además permitan una configuración sencilla para obtener un nivel de protección óptimo.

Los usuarios hoy en día son conocedores de la existencia de algunas soluciones que proporcionan seguridad a sus dispositivos, como, por ejemplo, los antivirus. Sin embargo, se produce una doble necesidad en cuanto que, por un lado, desconocen otras muchas herramientas destinadas a mejorar su protección y, por otro, no las instalan por desconfianza o por pensar que su configuración puede ser compleja. En ese sentido, los ciudadanos necesitan concienciarse sobre la importancia de las soluciones y configuraciones de seguridad y, a la vez, hace falta facilitarles la tarea a la hora de implementarlas.

Los ciudadanos también han de comprender que las medidas de seguridad, incluso cuando suponen un coste económico, son tan necesarias como lo son en otros ámbitos de la vida, véase la vivienda. Han de entender que las amenazas de la Red pueden ser tan peligrosas como algunas del ámbito físico, por ejemplo, un robo de claves bancarias puede suponer el robo de dinero de la cuenta.

Algunas iniciativas de referencia

- Oficina de Seguridad del Internauta de INCIBE: la OSI proporciona información y soporte al usuario final para evitar y resolver los problemas de seguridad que le pueden surgir al navegar por Internet, sobre todo, en sus primeros pasos en las nuevas tecnologías. Esta página cuenta, por un lado, con una sección de herramientas gratuitas[32] que los usuarios pueden descargar para instalar en sus dispositivos del tipo que sean. Por otro lado, contiene campañas para,

[32] https://www.osi.es/es/herramientas

por ejemplo, saber configurar dispositivos móviles[33] para establecer unas capacidades mínimas de seguridad.

- El CSIRT-GV ha puesto en marcha una campaña[34] centrada en la protección de los dispositivos móviles frente a ciberataques. En ella se facilitan consejos prácticos, orientaciones e incluso la descarga de antivirus para que los usuarios tomen conciencia y establezcan medidas mínimas de seguridad.

Propuestas a los actores impulsores de cultura ciberseguridad

- Impulso de la fabricación de soluciones y dispositivos con ciberseguridad por diseño, de manera que aumente el nivel de protección mínimo adecuado para el usuario.

- Involucración de los propios fabricantes de tecnologías en la protección de los dispositivos que ponen a la venta, ya sea fomentando campañas conjuntas con organismos de concienciación al ciudadano o elaborando materiales con contenidos que ayuden al usuario a proteger esos dispositivos o soluciones.

- Desarrollar actividades de vigilancia tecnológica junto con el Ministerio de Consumo para comunicar a los fabricantes los problemas de seguridad en sus dispositivos, con la finalidad de que estos las subsanen a través de actualizaciones y para futuros desarrollos.

- Promocionar los programas de *bug bounty* (recompensas por encontrar vulnerabilidades) para dispositivos dirigidos al consumo mayoritario (y en especial para los públicos más desprotegidos).

- Enfatizar el enfoque de responsabilidad compartida de los propios usuarios, con el objetivo de que adopten las medidas oportunas para proteger sus dispositivos. En este sentido, tanto los conocimientos como los mensajes han de estar adaptados a los diferentes perfiles poblacionales y mediante los medios de comunicación más utilizados por dichos segmentos.

- Facilitar herramientas gratuitas de ciberseguridad a los ciudadanos, promocionando iniciativas similares o impulsando la que lleva a cabo la OSI.

- Subvenciones para dispositivos con seguridad por diseño.

---

[33] https://www.osi.es/es/campanas/dispositivos-moviles

[34] https://concienciat.gva.es/tips_de_seguridad/protege-tu-movil-de-ciberataques/

TOP 9: INTELIGENCIA ARTIFICIAL

La Estrategia Nacional de Inteligencia Artificial (ENIA)[35] señala que, del mismo modo que la inteligencia humana es muy compleja de definir, no existe aún una definición formal y universalmente aceptada de inteligencia artificial (IA), y se remite a la definición dada por la Comisión Europea que se ha referido a la IA como "sistemas de software (y posiblemente también de hardware) diseñados por humanos que, ante un objetivo complejo, actúan en la dimensión física o digital: percibiendo su entorno, a través de la adquisición e interpretación de datos estructurados o no estructurados, razonando sobre el conocimiento, procesando la información derivada de estos datos y decidiendo las mejores acciones para lograr el objetivo dado". La inteligencia artificial incluye el aprendizaje automático y el procesamiento del lenguaje natural[36].

El estudio elaborado por el Observatorio Nacional de Tecnología y Sociedad[37] (ONTSI), dirigido a analizar analiza la percepción de la opinión pública en relación con la implantación de elementos de IA, expone que "la población valora positivamente la aplicación de la IA en todas aquellas aplicaciones que suponen una ayuda en muchas actividades cotidianas y contribuyen a mejorar o facilitar nuestra vida". En este sentido, la IA puede aportar múltiples aplicaciones y oportunidades en diversos campos como la salud, la educación, el transporte y la gestión de la movilidad, el apoyo a la toma de decisiones o en el ámbito de la ciberseguridad para prevenir y detectar ciberataques o ayudarnos a la detección de noticias falsas y de patrones de comportamiento manipulativos.

Retos y amenazas que plantea

En cuanto a los riesgos relacionados con el uso de la IA para los ciudadanos, existen numerosos documentos que alertan sobre la necesidad de evaluar el posible impacto para los derechos humanos, tal y como asevera también la Comisión Europea. En este sentido, se debe considerar el posible sesgo de los algoritmos utilizados por la IA, que se puede producir cuando los datos manejados para su entrenamiento no son representativos en el contexto en el que se aplican. Además, se ha de ser consciente de que la inteligencia artificial puede utilizarse para la modificación de imágenes y videos con el objetivo de generar contenidos falsos

[35] https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/ENIA2B.pdf

[36] ¿Qué es la inteligencia artificial? | Accenture

[37] Estudio sobre aplicación de la inteligencia artificial (ontsi.es)

o amplificar artificialmente determinadas informaciones, así como para facilitar la suplantación de la identidad a través de los denominados *deep fakes*.

Dado que la inteligencia artificial se basa en tener una gran cantidad de datos de los usuarios para poder entrenar a los algoritmos, uno de los mayores retos es la privacidad. Así, la IA combinada con Internet de las cosas (IoT) podría detectar patrones de comportamiento en el hogar o hábitos de navegación y compras por internet, a través de la captura y procesamiento de audio, video u otra información disponible a través de dispositivos conectados.

Nuestro país, sin duda, ha hecho una apuesta decidida por el desarrollo de la IA como parte de la *Estrategia España Digital 2025*, de la cual han derivado distintas medidas, como la publicación de la citada Estrategia Nacional de Inteligencia Artificial , que incluye como una de sus líneas de actuación la creación de confianza en la IA. Sin embargo, la IA está aún lejos de la ciudadanía, sin que esta sea consciente de los beneficios, que esta tecnología aporta ni de los riesgos[38].

Necesidades de los ciudadanos

Es necesario que los ciudadanos conozcan qué es la IA y para qué sirve, de una manera clara, concisa y sencilla.

En la misma línea, los ciudadanos deben conocer los riesgos y amenazas derivados de esta tecnología, en especial, aquellos aspectos relativos a la protección de datos.

Asimismo, los ciudadanos deben prestar atención a la configuración de seguridad de los dispositivos conectados que utilicen técnicas de IA.

Algunas iniciativas de referencia

- La Agencia de Protección de Datos en el documento de "Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial"[39] hace referencia a los derechos que tienen los ciudadanos con relación a la toma de decisiones automatizadas.

- En el marco de la planificación del Programa Nacional de Inteligencia Artificial de Finlandia, AuroraAI es un programa que aglutina es una serie de cursos gratuitos en línea creados por Reaktor y la Universidad de Helsinki. Los cursos combinan la teoría con ejercicios prácticos. En la iniciativa también ha participado el Gobierno

[38] Una inteligencia artificial ética y confiable para la ciudadanía europea - Retina (https://retinatendencias.com/)

[39] https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf

de España y su contenido (una introducción a la Inteligencia Artificial, en línea y gratis, para no expertos) se encuentra en español[40] .

- La Oficina de Seguridad del Internauta (OSI) del Instituto Nacional de Ciberseguridad (INCIBE), en el espacio Ponte al Día, incluye un artículo sobre los **riesgos que pueden suponer los asistentes inteligentes**[41]. Además, proporciona un espacio sobre cómo realizar configuraciones seguras para altavoces inteligentes con el asistente Alexa[42].

- Asimismo, Amazon y Google, por su parte, han diseñado espacios específicos dirigidos a ayudar a implementar la seguridad de Alexa[43] y de Google Nest[44].

- Destacar también Hackers vs. Cybercrook[45], una aventura gráfica de la OSI en la que el usuario debe ayudar a un personaje a proteger su casa inteligente, amenazada por Cybercrook. El jugador debe ir resolviendo los problemas que le plantea el juego para poder avanzar en la aventura.

Propuestas a los actores impulsores de la cultura de la ciberseguridad

- Actualización de los recursos existentes e implementación de otros nuevos más concretos para impulsar las previsiones contempladas la *Ley 15/2022*, de 12 de julio, integral para la igualdad de trato y la no discriminación, en los que se alerte sobre los riesgos de la IA.

- Concienciar a la ciudadanía sobre el funcionamiento básico de la IA y cómo puede afectarles, en especial, en cuanto a la protección de sus datos personales, como establece la Estrategia Nacional de Inteligencia Artificial en su Línea de Actuación 6.1–Crear confianza en la IA.

- Implicar a fabricantes y desarrolladores, inclusive científicos y centros de investigación, para el desarrollo de acciones conjuntas de concienciación sobre la IA, sus usos y riesgos y, específicamente, sobre la utilización segura de los asistentes personales.

- Estas acciones deberían desarrollarse de manera articulada y conjunta a fin de alcanzar un mayor impacto a través de mensajes contundentes.

---

[40] https://www.elementsofai.com/es

[41] https://www.osi.es/es/actualidad/blog/2018/05/30/que-riesgos-pueden-suponer-los-asistentes-inteligentes

[42] https://www.osi.es/es/actualidad/blog/2020/07/24/configuraciones-seguras-para-altavoces-inteligentes-con-el-asistente

[43] https://www.amazon.es/Portal-de-privacidad-de-Alexa/b?node=17136920031

[44] https://landing.google.com/advancedprotection/

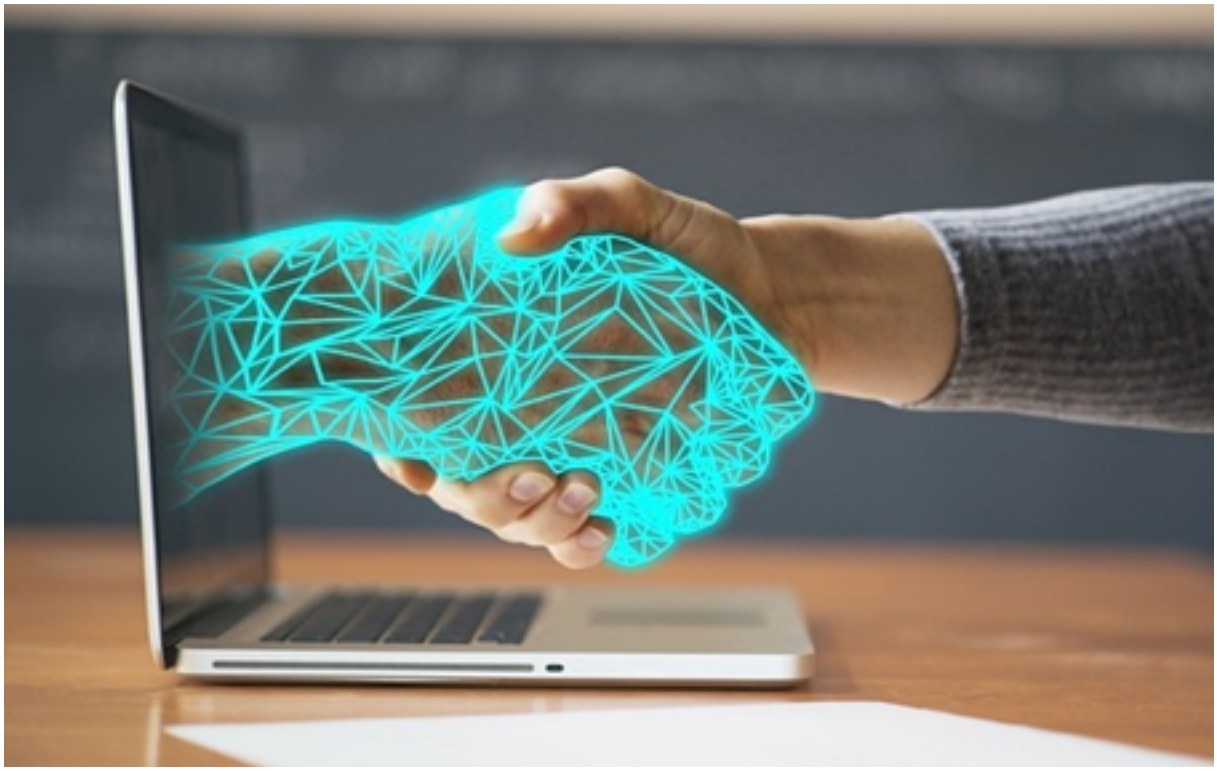
[45] https://www.osi.es/es/hackers

TOP 10: DENUNCIA, SOPORTE Y AYUDA

Saber a quién acudir para consultar dudas de ciberseguridad y recibir ayuda, así como conocer los canales de denuncia existentes si se ha sido víctima de un ciberdelito, constituyen necesidades esenciales para todos los ciudadanos que, en muchos casos, desconocen a quien dirigirse para recibir información, o cómo poner en conocimiento de las autoridades competentes los fraudes o ciberdelitos de los que han sido víctimas.

El soporte y la ayuda de terceros tienen un efecto tanto preventivo como reactivo, capacitando al ciudadano para hacer frente a las ciberamenazas, así como ayudando a la recuperación tras sufrir un ciberincidente.

Por otra parte, la denuncia del hecho delictivo es esencial para avanzar en la lucha contra la cibercriminalidad, que en los últimos años ha alcanzado un gran crecimiento[46].



[46] https://www.europapress.es/nacional/noticia-cibercriminalidad-mantiene-tendencia-alza-subir-89-pandemia-20230122112547.html

Retos y desafíos que plantea

A pesar de que el conocimiento y el recurso a los canales de ayuda ha ido aumentado progresivamente, se constata que aún no serían conocidos por la mayoría de la población, como pone de manifiesto el estudio "Cómo se protege la ciudadanía ante los ciberriesgos" [47], en el que se indica que el servicio proporcionado por el INCIBE a través del teléfono 017, en el que se brinda ayuda sobre ciberseguridad a la ciudadanía y empresas, es conocido por el 15,4% de las personas encuestadas.

Por otro lado, es importante que el ciudadano sepa que, a pesar de que todo intercambio de información u operatividad en Internet deja un rastro digital, los datos son volátiles, susceptibles de ser duplicados, fácilmente modificables e incluso eliminados, por lo que, ante la presencia de un posible delito o incidente, hay que actuar y ponerlo en conocimiento de las autoridades a la mayor brevedad, facilitándole el conocimiento de los canales de denuncia y su acceso. En este sentido, la posibilidad de la denuncia online, particularmente, ampliando la posibilidad de hechos delictivos que se pueden denunciar, facilitaría que el ciudadano pusiera en conocimiento los hechos de manera más rápida y eficiente.

Necesidades de los ciudadanos

Conocer los canales de ayuda, tanto los ofrecidos por las Administraciones Públicas como los que ponen a su disposición otras entidades con las que se relacionan de manera telemática, como los bancos.

Conocer y facilitar el acceso a los canales de denuncia proporcionados por las Fuerzas y Cuerpos de Seguridad del Estado y la Agencia Española de Protección, entre otros.

Concienciación sobre qué medidas tomar si se está siendo o se ha sido víctima de un ciberdelito. Por ejemplo[48]:

- Cómo hacer una denuncia y qué documentación se debe aportar.
- Acciones para evitar la progresión del ataque y para tratar de bloquear operaciones fraudulentas, alertando rápidamente, en su caso, al banco.
- Acciones para facilitar la investigación:

[47] https://observaciber.es/sites/observaciber/files/media/documents/ciudadaniaciberriesgos_abril2022_1.pdf

[48] Información más detallada en el ANEXO

- información que se ha de recopilar, cómo hacerlo y cómo conservarla (correos electrónicos, conversaciones, páginas web, videos, perfiles de redes sociales etc.);

- uso de los servicios de terceros de confianza o testigos online, que certifican el contenido publicado y público en la Red y pueden garantizar su validez en un proceso penal;

- acudir a un notario, a un perito forense o a las autoridades policiales que puedan certificar el contenido en cuestión.

Algunas iniciativas de referencia

- Concurso lanzado por INCIBE para dar a conocer el teléfono 017 entre todos los centros educativos de España[49].

- Campaña Europol EC3 sobre cómo hacer de tu hogar un lugar ciberseguro[50].

- Campaña de Policía Nacional destinada al uso seguro de Internet por parte de menores, en colaboración con Telefónica[51].

- Campaña "YO DENUNCIO" de la Guardia Civil (iniciativa de 2010).

- Campaña de la Agencia Española de Protección de Datos y del Ministerio de Consumo con consejos para actuar ante una suplantación de identidad en redes sociales, incluyendo la denuncia[52].

Propuestas a los actores impulsores de cultura ciberseguridad

- Explicar mediante mensajes más claros y contundentes las diferentes vías y canales disponibles de ayuda para la ciudadanía, respuesta a incidentes, soporte especializado y denuncia. En el caso de la denuncia los canales serían los siguientes:

---

[49] https://www.incibe.es/sala-prensa/notas-prensa/incibe-lanza-concurso-dar-conocer-el-telefono-017-todos-los-centros

[50] https://www.europol.europa.eu/cms/sites/default/files/documents/safe-at-home_es.pdf

[51] ttp://www.ciberexperto.org/

[52] https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-ministerio-consumo-campana-suplantacion-identidad

    - Brigada Central de Investigación Tecnológica (BCIT) de la Policía Nacional; Grupo de Delitos Telemáticos (DT) de la Guardia Civil; Sección Central de Delitos en Tecnologías de la Información (SCDTI) de la Ertzaintza; Unidad Central de Delitos Informáticos de los Mossos y Grupo de Apoyo Tecnológico de la Policía Foral de Navarra.

    - En el caso concreto de contenidos sensibles, la Agencia Española de Protección de datos pone a disposición de la ciudadanía un canal prioritario de retirada de contenidos sensibles.

    - Fiscal de Sala de Criminalidad Informática.

    - Defensor del Pueblo.

- Sería positivo que existiera una forma alternativa y segura de presentar las denuncias para optimizar el tiempo de atención al ciudadano, que incluyese, por ejemplo, la firma electrónica con doble factor de autenticación en las Sedes Electrónica de la Guardia Civil y de la Policía Nacional.

- Nuevas campañas en prensa y medios de comunicación para difundir estos canales.

- Repositorio común con las vías de denuncia y canales públicos puestos a disposición de los ciudadanos.

ANEXO

DECÁLOGO DE RECOMENDACIONES SI VAS A DENUNCIAR

La investigación tecnológica se basa en datos, muchas veces, intangibles. No obstante, todo intercambio de información u operatividad en Internet deja un rastro digital.

> Todos los datos en la Red son volátiles, susceptibles de ser duplicados, fácilmente modificables e incluso eliminados, por lo que, ante la presencia de un posible delito o incidente, hay que actuar y ponerlo en conocimientos de las autoridades a la mayor brevedad.

Por todo ello, es recomendable que sigas los siguientes pasos:

1. Si se han realizado pagos a terceros o se han ejecutado transferencias fraudulentas, además de denunciarlo, debes contactar y alertar rápidamente a tu banco para tratar de bloquear la operación si fuera posible.

2. Si estás sufriendo un delito en ese momento y no puedes controlar el dispositivo, se te ha bloqueado, ves que se mueve el ratón por su cuenta o aparecen ventanas o caracteres raros de bloqueo, desenchufa el cable de alimentación del ordenador y del router y apaga el móvil. De esta manera, sin conexión, si están actuando de forma remota, no podrán seguir operando.

3. Si ya hemos sufrido el delito, no alteres el soporte original: no toques las aplicaciones que ya puedan estar abiertas, no sigas interactuando con los autores del delito si has mantenido conversaciones con ellos por algún medio como Whatsapp, correo electrónico u otras aplicaciones de intercambio de información.

4. Recopila conserva y no borres toda la información disponible que tengas sobre el hecho: correos electrónicos conversaciones, páginas web donde hayas operado, documentación como supuestas facturas, justificantes de pago, así como las cuentas de usuario que puedas tener. Ten en cuenta que si borras o pierdes alguna de la información de la que dispones, nunca se podrá volver a recuperar.

5. Si has sufrido un cargo fraudulento o inesperado que no has realizado, tienes que acudir a tu banco para que verifique la operación y te aporte un comprobante sobre la operaciones fraudulentas que deberás adjuntar en el momento de la denuncia.

6. No modifiques claves ni contraseñas. Imagínate que cierras la cuenta de una red social, por ejemplo, Facebook, y estuviste hablando por mensaje privado con un sospechoso. Ya no se podrá acceder a sus contenidos salvo que tenga la contraseña guardada en el dispositivo.

7. Los pantallazos no tienen validez en un proceso penal. Es habitual presentar capturas de pantalla mal detalladas, impresas en un papel o pantallazos imprecisos de la información. Las capturas de pantalla son fácilmente modificables y no serán admitidas en un proceso judicial. Si tienes que recoger cualquier comentario, perfil en redes o páginas web existen los denominados terceros de confianza o testigos online, webs que certifican automáticamente el contenido publicado y público en la Red. Estos servicios te permiten realizar una copia exacta del contenido de la página que te interese reportar y certifican que no ha sido alterado. Solo tienes que introducir la URL (la dirección en la Red que te he mostrado) de la página que desees y posteriormente te lo envían al correo que desees en formato PDF.

   Si no sabes emplearlos o los contenidos son de carácter privado, como mensajes directos en redes sociales o sistemas de mensajería, será necesario que acudas a un notario, a un perito forense o a las autoridades policiales que puedan certificar el contenido en cuestión.

8. Si dispones de información como cuentas de perfiles en redes sociales, emails, conversaciones en plataformas de segunda mano, etc. debes ser muy cauteloso porque puedes aportar esa información de forma parcial, incompleta o ilocalizable.

9. Si tienes que reportar o denunciar perfiles, no es suficiente con el *nick* o seudónimo. Debes saber que cada uno de los usuarios de las redes sociales tiene su propio identificador. Si no sabes cómo obtenerlo, puedes ir a la página principal o de inicio del perfil o cuenta que te interese reportar y copiar la URL (nombre de la página web) de la barra de direcciones que estés visionando del perfil. No obstante, el *nick* también es fundamental (aunque ya venga implícito en el identificador).

10. Si has comprado en un anuncio sospechoso, los datos clave que deberás aportar son, como mínimo, la URL de la barra de direcciones del navegador y todos los datos que puedan ayudar a situar el anuncio: sección, usuario/referencia de publicación, fecha y hora y cualquier otro dato concreto.

11. Si tienes que denunciar o aportar la referencia a algún vídeo que esté publicado, no aportes capturas a modo de fotograma. Lo ideal sería, si sabes, que descargues inmediatamente el vídeo y lo aportes como un archivo por separado. Existen programas gratuitos que te permiten descargarte el archivo de vídeo. SI no sabes

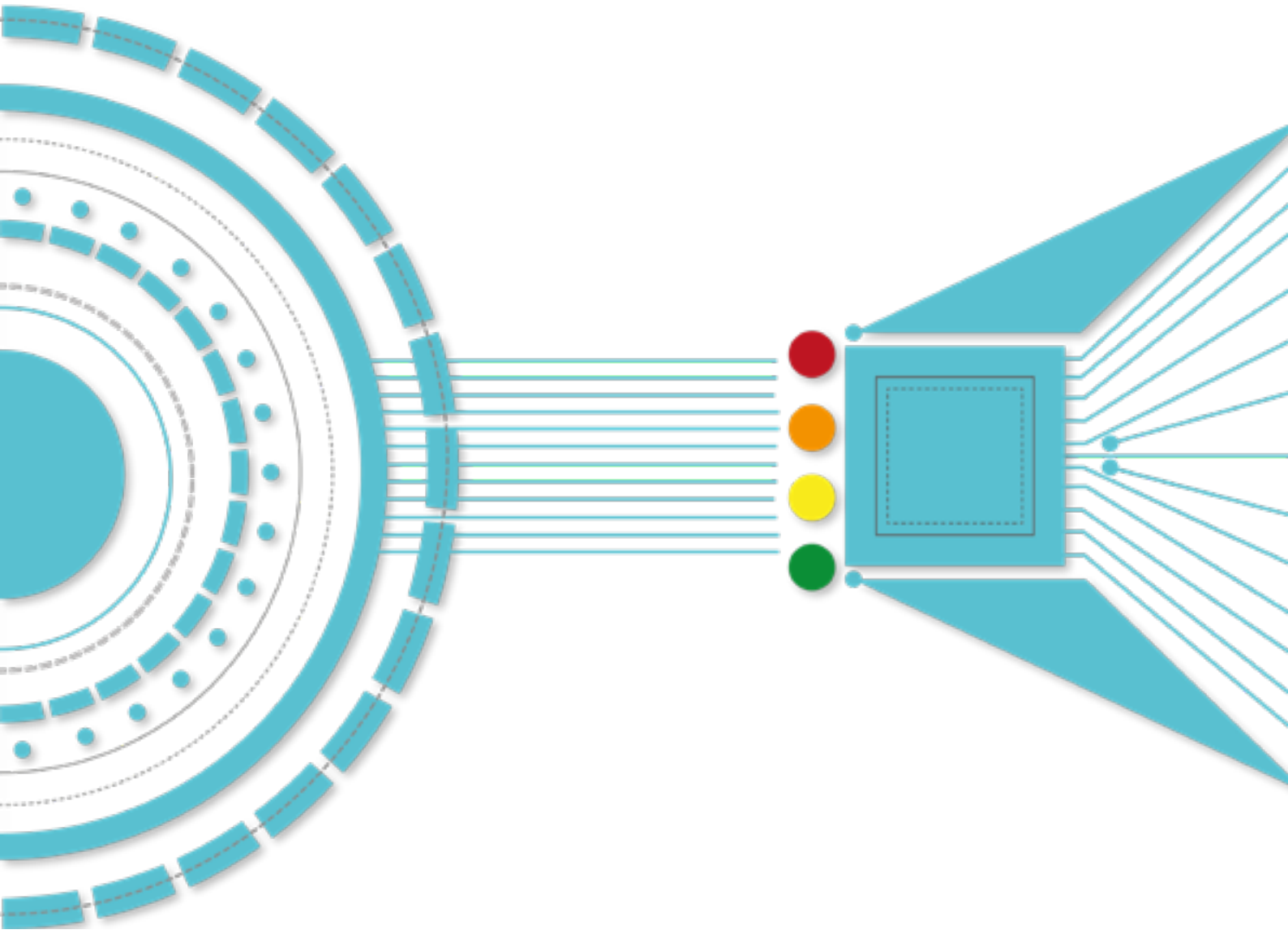
realizar este proceso, es suficiente con que aportes la URL o la dirección web del vídeo y el nombre del canal del usuario que lo publica.

12. Si ha sido tu empresa la que ha sufrido un ataque, sería conveniente que realizaras un informe pericial informático forense de cara a presentar las evidencias del ataque sufrido y hacerlo valer en un juicio para asumir las responsabilidades que correspondan frente a otros u los clientes.

13. Conserva toda la información y las evidencias digitales que hayas aportado o se te hayan solicitado hasta el final del proceso.

14. Debes saber que puedes ampliar la información de la que dispones en cualquier momento ante las autoridades si dispones de nuevos datos o de nueva documentación.

4. SEMÁFORO DE RIESGOS Y SECTORES MÁS VULNERABLES



	MENORES DE EDAD	PERSONAS MAYORES	POBLACIÓN EN EDAD LABORAL	COLECTIVOS EN RIESGO DE EXCLUSIÓN	RECOMENDACIONES
REDES SOCIALES	🔴	🟠	🔴	🔴	• Clarificación sobre las opciones de privacidad ofrecidas por las redes sociales y el establecimiento de opciones restrictivas en el uso del perfil personal. • Concienciación y uso del sentido común en el comportamiento ante los desconocidos y sus planteamientos de enlace (match) en la red del mismo modo que lo haríamos en el mundo real. • La no publicación ni facilitación de datos propios que abran la puerta a la identificación de conductas o hábitos que puedan derivar en caer víctimas de un delito. • Atención a la publicación de imágenes o contenidos de terceros y especialmente en el caso de menores. • Impulsar la implantación efectiva de controles de acceso para los menores de edad.
	Se trata de uno de los medios más utilizados para ataques de ingeniería social y otras conductas delictivas como el ciberacoso o el ciberbullying Es una puerta de entrada para incidentes y exposición de privacidad y, en numerosos casos, también de actividades fraudulentas y criminales				
USO DE CONTRASEÑAS Y CREDENCIALES	🟠	🔴	🔴	🔴	• Programas de concienciación y educación en ciberseguridad. Con eslóganes como “Tu contraseña es la llave de tu casa, ¿la dejarías en un lugar donde cualquiera la pudiera coger?” • Cybervoluntarios en las escuelas, asociaciones de vecinos y centros de mayores que ayuden a las personas con pocos conocimientos a utilizar el certificado digital. • Facilitar el acceso a gestores de contraseñas, con una subvención si fuera necesario (al igual que existe una subvención para el Kit Digital). • Impulso del uso de la biometría como mecanismo de autenticación, sin menoscabo de su consideración como dato personal sensible. • Fomento de la responsabilidad compartida entre proveedores y usuarios en el uso de credenciales y la gestión de la autenticación, para evitar las malas prácticas de los dueños de los sistemas si, por ejemplo, no disponen de autenticación de factor múltiple o permiten contraseñas débiles.
	El robo de contraseñas es un vector de ataque habitual y muy exitoso para todo tipo de atacantes				
ATAQUES DE INGENIERÍA SOCIAL	🟠	🔴	🔴	🔴	• Lanzamiento de links engañosos que lleven a una página que sirva como concienciación y educación a los ciudadanos, como lo hace la Universidad Veracruzana, o como lo hacen algunas empresas con sus empleados. • Campañas de concienciación masivas basadas en el autoconocimiento para el empoderamiento de la ciudadanía, aportando más valor e información, más allá de los hábitos. • Aplicaciones gratuitas para lectura de código QR, que permitan visualizar la URL antes de acceder a ella. • Mensajes más contundentes sobre la amenaza del *phishing*, de los QRs maliciosos y cómo darnos cuenta de que hemos sido víctimas.
	Se trata de medios no técnicos para conseguir de manera fraudulenta el acceso a información o sistemas o para llevar a cabo un fraude.	Incluye la suplantación, el engaño, la manipulación y, en general, el abuso de la confianza de las personas para que revelen información o realicen acciones perjudiciales sin buscar esos efectos o ser conscientes de ellos.			

	MENORES DE EDAD	PERSONAS MAYORES	POBLACIÓN EN EDAD LABORAL	COLECTIVOS EN RIESGO DE EXCLUSIÓN	RECOMENDACIONES
PRIMER ACCESO A LAS TIC					• Elaborar una hoja de ruta de formación que se plasme en iniciativas de todo tipo adaptadas a la edad de los más jóvenes, como pueden ser la grabación de contenidos audiovisuales infantiles, charlas en los centros educativos, aplicaciones o juegos que les permitan aprender mientras se entretienen. En definitiva, es necesario adaptar formatos y mensajes a los menores para poder llegar a ellos de manera eficaz. En ese sentido, es fundamental contar con los educadores, quienes realmente conocen esas necesidades. • Los padres deben desempeñar un papel principal en la educación y el ciudadano del acceso a las TIC de sus hijos. En ese sentido, han de ser conscientes y transmitir la corresponsabilidad que supone utilizar las tecnologías. El primer acceso a las TIC requiere también acciones orientadas a los padres, como puedan ser campañas de sensibilización o actividades lúdico-educativas que puedan llevar a cabo conjuntamente progenitores y menores. • El ámbito educativo también debe estar implicado en la formación y concienciación de los menores cuando comienzan a utilizar las tecnologías. Convendría alcanzar acuerdos y convenios al más alto nivel para que los colegios incorporen actividades destinadas a dicho fin, en las que estén involucrados tanto los educadores, como los padres, expertos en la materia y, evidentemente, los menores. • En el caso de las personas mayores, igualmente requiere que los mensajes y contenidos que contribuyan a su formación estén adaptados a su edad e intereses. Uno de los aspectos clave al respecto es evitar provocar 'miedo' a la hora de utilizar sus dispositivos, sino todo lo contrario, confianza y herramientas para que estos usuarios sepan reaccionar ante los retos que se les planteen. • Las campañas de concienciación son una herramienta muy útil, pero insuficiente si no van acompañadas de otras acciones. En este sentido, se deben identificar las vías de acceso a ese segmento de población, localizando sus centros de encuentro, en ciudades y zonas rurales o los medios de comunicación más populares entre los mayores, para que las actividades formativas lleguen al público objetivo. • Al igual que los jóvenes, resultaría interesante involucrar a los descendientes de las personas mayores, ya sean sus hijos, nietos, sobrinos o cualquier otro familiar que pueda ayudarles, por ejemplo, mediante actividades compartidas lúdico-formativas. • Las entidades financieras, la Administración, y todas aquellas organizaciones de cualquier tipo que requirieran el uso de la tecnología para poder beneficiarse de sus servicios, deberían participar en iniciativas que ayudasen a entender y conocer cómo protegerse en la Red.
	Se produce, por un lado, a edades cada vez más tempranas y, por otro, a edades tardías en las que los ciudadanos se ven obligados a utilizar herramientas que nunca habían empleado enfrentándose a riesgos y amenazas para los que no están preparados ni formados.				

	MENORES DE EDAD	PERSONAS MAYORES	POBLACIÓN EN EDAD LABORAL	COLECTIVOS EN RIESGO DE EXCLUSIÓN
				
TRÁMITES Y COMPRAS ON LINE	Durante el acceso online a plataformas de compras, adquisición de servicios o trámites con las administraciones, los ciudadanos se enfrentan a situaciones de riesgo para los que no siempre han recibido una formación que les permita proteger sus datos y su patrimonio.			

RECOMENDACIONES

- Inclusión de la ciberseguridad personal como materia en los ciclos de enseñanza obligatoria.
- Creación de una caja de herramientas de seguridad digital. Esto se podría proveer como un Kit Digital gratuito para los ciudadanos.
- Promover la elaboración de guías de consejos y seguridad para el uso de aplicaciones comerciales de pagos online, para que los ciudadanos puedan utilizarlas de forma segura.
- Promover la elaboración de Kit de Consejos y configuración en las entregas de tarjetas y/o integración de medios de pagos en móviles (tecnología NFC) por parte las entidades financieras.
- Promover la emisión y popularización, por parte de los bancos y entidades de crédito, de tarjetas de crédito con numeración virtual o tarjetas de pago recargables.
- Promover el aprovechamiento de los recursos de los fabricantes de sistemas operativos de los principales móviles para ofrecer consejos de seguridad a los usuarios.
- Divulgar el conocimiento de los sellos de confianza de las páginas web y su significado.
- Delimitar las responsabilidades en caso de fraude, así como las consecuencias si no se han adoptado las medidas de seguridad necesarias por las distintas partes.

	MENORES DE EDAD	PERSONAS MAYORES	POBLACIÓN EN EDAD LABORAL	COLECTIVOS EN RIESGO DE EXCLUSIÓN	RECOMENDACIONES

PRIVACIDAD E INFORMACIÓN PERSONAL	●	●	●	●	• Identificar a los colectivos cuyos miembros están especialmente expuestos y realizar acciones de divulgación dirigidas específicamente a cada colectivo.
					• Impulsar acciones de divulgación en los colegios a través de las asociaciones de padres y madres (CEAPA, CONCAPA, AMPA, etc.) y las consejerías de educación de las comunidades autónomas.
					• En el caso de personas mayores, canalizar las acciones a través de asociaciones de pensionistas, uniones de jubilados, asociaciones mayores, etc., y las consejerías con competencias en el bienestar de los mayores. Así como ONGs como Cruz Roja, Caritas.
					• Fomentar la corresponsabilidad de los ciudadanos, que pasa por conocer en primer lugar qué se entiende por datos personales, las categorías especiales de datos personales, los derechos que le asisten y los canales de denuncia, además del seguimiento de una serie de consejos en su navegación por internet. Por lo que respecta a los consejos en la navegación por internet, se encuentran, entre otros:
					  • No facilite información personal salvo que sea informado, al menos, de: la identidad del responsable o encargado del tratamiento, la finalidad del tratamiento, los derechos que le asisten y ante quien ejercitarlos, la dirección electrónica u otro medio donde acceder al resto de informaciones obligadas por la normativa de protección de datos.
					  • No proporcione información personal de terceros excepto que se haya obtenido su consentimiento.
					  • Revise periódicamente la configuración de privacidad de sus cuentas en redes sociales.
					  • Sea muy cauto con las informaciones personales que publique procurando que sean las mínimas, así como con las informaciones personales almacenadas en el móvil.
					  • Desconfíe de los correos de desconocidos con faltas de ortografía, de ofertas muy atractivas, que transmiten premura, etc. (*phising*), pues a menudo solicitan datos personales, como números de cuentas bancarias, o instan a conectarse a páginas web con los mismos propósitos.
					  • Si guarda información personal en la nube, configure adecuadamente las opciones privacidad, asegurándose de que el canal de transferencia de datos trabaje bajo https, cifrando sus datos (aunque ya lo haga el proveedor del servicio) y manteniendo copias de seguridad en un soporte convencional.
					  • Si usa un sensor para monitorizar su actividad física, compruebe los ajustes del dispositivo para preservar su privacidad y no comparta la información registrada en las redes sociales.

Preocupación por las capacidades de la tecnología para capturar, procesar, almacenar y transmitir datos e información personal.

	MENORES DE EDAD	PERSONAS MAYORES	POBLACIÓN EN EDAD LABORAL	COLECTIVOS EN RIESGO DE EXCLUSIÓN	RECOMENDACIONES
INTERNET DE LAS COSAS					• Guía Básica de Seguridad IoT: las guías actuales están orientadas a las empresas, pero no tanto a la concienciación y buen uso por parte de la sociedad en general. • Concienciar sobre las obligaciones existentes de informar a los consumidores de los riesgos de los dispositivos conectados a Internet si no se toman medidas de seguridad y se hace un uso responsable de ellos. • Acciones de concienciación sobre un uso higiénico de los dispositivos IoT, para que los usuarios implementen las medidas básicas necesaria como las siguientes: cambiar las contraseñas por defecto que traen de fábrica estos dispositivos; crear contraseñas seguras para el acceso a las aplicaciones de los dispositivos IoT; instalación de antivirus o la configuración adecuada de la red doméstica, entre otras.
	Existen multitud de dispositivos cotidianos que están conectados a Internet y que recaban, tratan, almacenan y transmiten información del usuario, que puede ser básica o de especial protección Estos dispositivos suelen contener vulnerabilidades, ya sea por su configuración, infraestructura o características				
PROTECCIÓN DE LOS DISPOSITIVOS					• Impulso de la fabricación de soluciones y dispositivos con ciberseguridad por diseño, de manera que aumente el nivel de protección mínimo adecuado para el usuario. • Involucración de los propios fabricantes de tecnologías en la protección de los dispositivos que ponen a la venta, ya sea fomentando campañas conjuntas con organismos de concienciación al ciudadano o elaborando materiales con contenidos que ayuden al usuario a proteger esos dispositivos o soluciones. • Desarrollar actividades de vigilancia tecnológica junto con el Ministerio de Consumo para comunicar a los fabricantes los problemas de seguridad en sus dispositivos, con la finalidad de que estos las subsanen a través de actualizaciones y para futuros desarrollos. • Promocionar los programas de *bug bounty* (recompensas por encontrar vulnerabilidades) para dispositivos dirigidos al consumo mayoritario (y en especial para los públicos más desprotegidos). • Enfatizar el enfoque de responsabilidad compartida de los propios usuarios, con el objetivo de que adopten las medidas oportunas para proteger sus dispositivos. En este sentido, tanto los conocimientos como los mensajes han de estar adaptados a los diferentes perfiles poblacionales y mediante los medios de comunicación más utilizados por dichos segmentos. • Facilitar herramientas gratuitas de ciberseguridad a los ciudadanos, promocionando iniciativas similares o impulsando la que lleva a cabo la Oficina de Seguridad del Internauta. • Subvenciones para dispositivos con seguridad por diseño.
	La capacidad de procesamiento y de conexión con la que cuentan los dispositivos actuales (teléfonos inteligentes y tabletas, más allá de los típicos portátiles, y a los que podemos sumar todo tipo de wearables) hace que las personas estemos, cada vez, más expuestas a los riesgos de un mal uso o un mal funcionamiento de los mismos.				

	MENORES DE EDAD	PERSONAS MAYORES	POBLACIÓN EN EDAD LABORAL	COLECTIVOS EN RIESGO DE EXCLUSIÓN	RECOMENDACIONES
INTELIGENCIA ARTIFICIAL	🟠	🟠	🔴	🟠	• Actualización de los recursos existentes e implementación de otros nuevos más concretos para impulsar las previsiones contempladas la Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación, en los que se alerte sobre los riesgos de la IA. • Concienciar a la ciudadanía sobre el funcionamiento básico de la IA y cómo puede afectarles, en especial, en cuanto a la protección de sus datos personales, como establece la Estrategia Nacional de Inteligencia Artificial en su Línea de Actuación 6.1 Crear confianza en la IA . • Implicar a fabricantes y desarrolladores, inclusive científicos y centros de investigación, para el desarrollo de acciones conjuntas de concienciación sobre la IA, sus usos y riesgos y, específicamente, sobre la utilización segura de los asistentes personales. • Estas acciones deberían desarrollarse de manera articulada y conjunta a fin de alcanzar un mayor impacto a través de mensajes contundentes.
	Esta tecnología no presenta una flexibilidad como la de la inteligencia humana, que permite adaptarse a cualquier situación, lo que puede llevar a un comportamiento erróneo que podría conllevar una vulneración de la protección de datos e incluso suplantar la identidad de una persona.				

DENUNCIA, SOPORTE Y AYUDA	🔴	🔴	🔴	🔴	• Explicar mediante mensajes más claros y contundentes las diferentes vías y canales disponibles de ayuda para la ciudadanía, respuesta a incidentes, soporte especializado y denuncia. En el caso de la denuncia, los canales serían los siguientes:
					  • Brigada Central de Investigación Tecnológica (BCIT) de la Policía Nacional; Grupo de Delitos Telemáticos (DT) de la Guardia Civil; Sección Central de Delitos en Tecnologías de la Información (SCDTI) de la Ertzaintza; Unidad Central de Delitos Informáticos de los Mossos y Grupo de Apoyo Tecnológico de la Policía Foral de Navarra.
					  • En el caso concreto de contenidos sensibles, la Agencia Española de Protección de Datos pone a disposición de la ciudadanía un canal prioritario de retirada de contenidos sensibles.
					  • Fiscal de Sala de Criminalidad Informática.
					  • Defensor del Pueblo.
					• Sería positivo que existiera una forma alternativa y segura de presentar las denuncias para optimizar el tiempo de atención al ciudadano, que incluyese, por ejemplo, la firma electrónica con doble factor de autenticación en las Sedes Electrónica de la Guardia Civil y de la Policía Nacional.
					• Nuevas campañas en prensa y medios de comunicación para difundir estos canales.
					• Repositorio común con las vías de denuncia y canales públicos puestos a disposición de los ciudadanos.

	Actualmente, se pueden realizar múltiples trámites con las Administraciones Públicas a través de las TIC, principalmente haciendo uso del certificado electrónico o de otros mecanismos, esto no se ve reflejado cuando el ciudadano tiene la necesidad de presentar una denuncia ante las Fuerzas y Cuerpos de Seguridad, ya que esta únicamente puede presentarse en casos concretos, siendo obligatorio el desplazamiento físico.				

5. CONCLUSIONES Y RECOMENDACIONES

La **transformación digital** de nuestra sociedad se orienta en gran medida a mejorar la vida de la población. Sin embargo, el uso de la tecnología también entraña grandes peligros y retos, entre los cuales destaca la ciberseguridad. El establecimiento de determinadas **medidas de seguridad**, el **uso responsable** de los dispositivos o la **formación**, son algunos de los requerimientos mínimos que deben asumir los ciudadanos.

Entre ellos, **menores de edad, personas mayores, población en edad laboral o colectivos en riesgo de exclusión**, como discapacitados o inmigrantes, constituyen grupos que requieren una especial atención por su vulnerabilidad en cuanto al buen uso de la tecnología y la ciberseguridad.

Con independencia de las recomendaciones propuestas en cada uno de los ámbitos analizados en esta Brújula, existe un **denominador común a todos ellos que es la falta de conocimiento y concienciación de la ciudadanía** sobre los peligros inherentes a un mal uso de la tecnología. A esto hay que añadir la falta de una infraestructura y dispositivos seguros.

Para avanzar en la corresponsabilidad, los ciudadanos deben tener acceso a información y la Administración debe promover fórmulas, utilizando todos los recursos a su alcance, para explicar los riesgos a los que aquellos están sometidos, así como las recomendaciones sobre las medidas adecuadas para combatirlos. Si bien es cierto que existen muchas actuaciones en este sentido, los datos muestran que queda mucho por hacer, no tanto quizá en cuanto a número de iniciativas, sino más bien desde la **perspectiva de la unidad de acción y coordinación a través de una visión estratégica**.

En definitiva, sería necesario acometer el diseño e implantación de un **Plan estratégico de ciberseguridad ciudadana,** que contenga la descripción de las acciones a ejecutar sobre cada colectivo de riesgo y sus modalidades: formación a todos los niveles, concienciación mediante campañas dirigidas a cada público objetivo, mejora de la regulación de aquellos aspectos que facilitan la progresión de los riesgos, promoción de acuerdos con diseñadores y fabricantes de *software* y dispositivos para incorporar desde el diseño inicial medidas de seguridad adecuadas en los dispositivos, impulso y facilitación del acceso a los servicios de denuncia y ayuda ante incidentes, y todo cuanto contribuya a mejorar la

capacidad de respuesta frente a los riesgos por parte de la población. En este sentido, es particularmente importante poner el foco en los menores, mediante una **Estrategia de protección de menores online**[53] unitaria, y dotarse de los recursos necesarios para su implementación. Como viene señalando la Fiscalía General del Estado en su Memoria Anual[54] "la endémica carencia de medios personales y materiales en la lucha contra la ciberdelincuencia tiene en este ámbito unas consecuencias especialmente graves".

La consecución de un objetivo tan ambicioso exige realizar una detallada planificación de las acciones, un compromiso y una involucración de los niveles políticos y una sensibilización de los ciudadanos, para dotar a la sociedad en su conjunto de las herramientas necesarias para enfrentar los crecientes riesgos de ciberseguridad.

Para ello, el Plan definiría las áreas y los objetivos estratégicos, así como los indicadores para medir su consecución, entre los que se incluirían los siguientes:

- Educación y formación, con la implantación de la formación obligatoria en materia de ciberseguridad en el currículo escolar.

- Concienciación de ciberseguridad responsable que consiga un cambio de comportamiento de los usuarios.

- Seguridad por diseño de los dispositivos para facilitar su uso confiable.

En el pasado, hemos asistido a la puesta en marcha de planes de este tipo con notable éxito: campañas para promover la práctica del deporte o el ejercicio de hábitos saludables. En particular, **la Estrategia de Seguridad Vial 2011-2020 constituye un excelente modelo de referencia** a los fines que se pretenden por el paralelismo de las acciones a acometer.

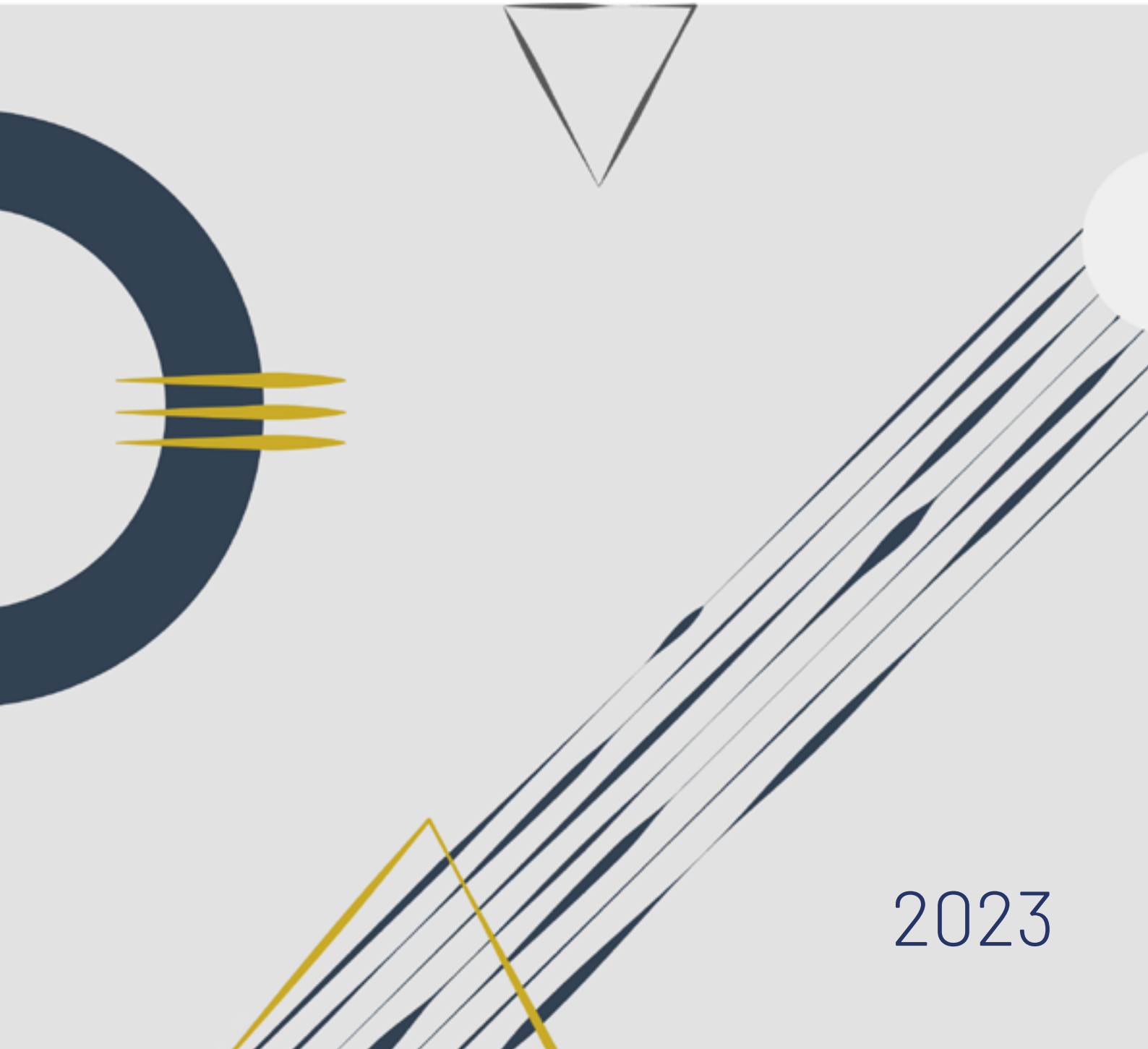
[53] España ocupa el cuarto puesto en el índice global de la ciberseguridad de la Unión Internacional de Telecomunicaciones. Para poder seguir avanzando en el compromiso con la ciberseguridad que mide el índice, sería necesario poder responder con una Estrategia unitaria a la pregunta incluida en su cuestionario: ¿Hay una estrategia nacional de Protección de la Infancia en Línea? https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCIv4_Spanish.pdf

[54] https://www.fiscal.es/memorias/memoria2021/FISCALIA_SITE/recursos/pdf/MEMFIS21.pdf

PLAN ESTRATÉGICO DE SEGURIDAD VIAL	PLAN ESTRATÉGICO DE CIBERSEGURIDAD
Educación Vial	Educación en Internet
Protección a los usuarios más vulnerables	Protección a los usuarios más vulnerables
Cumplimiento normas circulación	Elaboración y cumplimiento normas tráfico en la red
Mejora infraestructuras viarias	Internet segura
Vehículos más seguros	Dispositivos más seguros
Promoción del uso de las tecnologías modernas para aumentar la seguridad vial	Promoción del uso de las tecnologías para aumentar la ciberseguridad
Mejora de los servicios de emergencia y atención tras las lesiones	Mejora de los servicios de emergencia y atención tras los incidentes

FORO NACIONAL DE CIBERSEGURIDAD

CÓDIGO DE BUEN GOBIERNO DE LA CIBERSEGURIDAD



2023

CÓDIGO DE BUEN GOBIERNO DE LA CIBERSEGURIDAD

Los expertos participantes en los Grupos de Trabajo lo son a título personal y no a título institucional. Por lo tanto, sus opiniones y recomendaciones no representan ni comprometen a las instituciones a las que pertenecen.

El resultado de los trabajos es producto de un ejercicio de reflexión colectivo, si bien, no tiene por qué representar la opinión individual de todos los participantes, quienes no necesariamente comparten todas las conclusiones o propuestas.

AGRADECIMIENTOS

Coordinador sociedad civil:

Gianluca D'Antonio (Presidente de ISMS Forum)

Coordinador institucional:

Andrés J. Ruiz Vázquez (Departamento de Seguridad Nacional)

Autores y colaboradores:

Raúl Amigorena Eguiluz

Roberto Baratta Martínez

Mariano J. Benito Gómez

Juan Fco. Cornago Baratech

Ángel Domínguez Fernández-Burgos

Javier García Quintela

Daniel Largacha Lamela

Idoia Mateo Murillo

Francisco del Olmo Fons

Luis Paredes Hernández

Julia Perea Velasco

Olga Ramírez Sánchez

Antonio Ramos García

Jesús Sánchez López

Alejandro Viana Lara

María Elisa Vivancos Cerezo

ÍNDICE

1. INTRODUCCIÓN

En abril del año 2019, el Consejo de Seguridad Nacional aprobó la **Estrategia Nacional de Ciberseguridad** en cuyo texto se destaca la cooperación público-privada como un elemento clave en la consecución de los objetivos marcados en ciberseguridad. Así mismo la Estrategia prevé el Foro Nacional de Ciberseguridad, espacio encuadrado en el Sistema de Seguridad Nacional e integrado por representantes de la sociedad civil, expertos independientes, sector privado, instituciones académicas, asociaciones y organismos sin ánimo de lucro, entre otros, a fin de potenciar y crear sinergias público-privadas.

La ciberseguridad se ha convertido en el pilar estratégico sobre el que poder asentar la revolución digital que han experimentado todos los sectores de la sociedad, incluyendo Administraciones públicas, empresas y ciudadanía. Solo sobre la base de la ciberseguridad es posible continuar avanzando de forma segura en dicha transformación.

El marco regulatorio en materia de ciberseguridad ha evolucionado en los últimos años, tanto a nivel nacional como europeo, con el objetivo de mejorar la ciberseguridad de nuevos sectores cuyas obligaciones se han visto incrementadas. Gran parte de las novedades y cambios normativos en esta materia han venido propiciados por los cada vez más frecuentes y costosos efectos negativos soportados por las organizaciones, bien a causa de ciberataques, bien debido a la inadecuada gestión interna de los riesgos en ciberseguridad.

A nivel nacional, el nuevo **Esquema Nacional de Ciberseguridad**, recogido en el Real Decreto 311/2022[1], menciona explícitamente la necesidad de seguir una dinámica de mejora continua y adaptativa de la ciberseguridad, que es parte cada vez más relevante del modelo de **sostenibilidad del país**, debido al impacto que puede generar, no solamente en la propia organización, sino también en sus empleados, proveedores, clientes y grupos de interés que puedan verse afectados por las actividades de la organización. Así mismo, el **Real Decreto 43/2021**[2] exige el nombramiento de un **responsable de la seguridad de la información** en las organizaciones que reporte directamente a la alta dirección y

[1] Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

[2] Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

que mantenga la debida independencia respecto de los responsables de las redes y los sistemas de información.

A nivel europeo, la Directiva UE 2022/2555 conocida como **NIS 2**, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, incluye medidas específicas de gobernanza de la ciberseguridad. Entre ellas, establece que los órganos de dirección de las organizaciones **aprueben las medidas para la gestión de riesgos de ciberseguridad y supervisen su puesta en práctica**.

El **Foro Nacional de Ciberseguridad**, en reunión plenaria el 8 de octubre de 2021, procedió a la aprobación de las líneas de trabajo para el periodo 2021–2022 por cada uno de los grupos de trabajo que lo conforman. Concretamente, la **incorporación de la ciberseguridad al buen gobierno corporativo de las organizaciones** fue la línea de trabajo aprobada para desarrollar por parte del **Grupo de Trabajo número 1 de Cultura de Ciberseguridad**.

Desde los **órganos de administración se ejerce el liderazgo de las organizaciones** y se lleva a cabo el seguimiento de su correcto funcionamiento, incluyendo la supervisión de la gestión y control de los **riesgos corporativos**, entre los que cada vez con mayor frecuencia e intensidad se incluyen los de carácter cibernético.

En este sentido y siguiendo la línea aprobada en el Foro Nacional de Ciberseguridad, el Grupo de Trabajo 1 dio comienzo a la labor de desarrollar un trabajo de **recopilación de los principios fundamentales y recomendaciones asociadas a los mismos, que los órganos de gobierno de una organización**, con independencia de su tamaño o sector, pudieran seguir para realizar una adecuada gobernanza de su ciberseguridad.

El presente Código de buen gobierno es el fruto final del trabajo del grupo referido, compuesto por expertos en materia de ciberseguridad, así como del análisis de distintas normativas y estándares existentes, examinadas desde una perspectiva práctica y actual, para la mejora del buen gobierno corporativo en materia de ciberseguridad.

2. OBJETIVO

Los nuevos retos derivados de la materialización de amenazas en el ciberespacio, han generado un notable incremento de los ciberataques, tanto en volumen como en frecuencia y sofisticación. Hacer frente a los nuevos retos de ciberseguridad requiere de políticas de revisión y mejora continuada, así como de la optimización de los controles y medidas de ciberseguridad, aplicadas tanto a la protección del valor y funcionamiento de las organizaciones, como a la protección de los datos de los ciudadanos en poder de aquellas.

El presente Código de buen gobierno no es una definición de un nuevo estándar de controles ni un manual de implantación. Por el contrario, el objetivo del Código es proponer a las organizaciones las prácticas dirigidas a sustentar el **modelo de buen gobierno de la ciberseguridad** que facilite la gestión de la seguridad de las redes y los sistemas de información y contribuya a mejorar el proceso de toma de decisiones en este ámbito por parte de los órganos de gobierno de las organizaciones y, en especial, por el órgano de administración.

Teniendo en cuenta este objetivo general, a continuación, se establecen una serie de objetivos específicos:

- **Objetivo I. Integrar en un único código de buen gobierno los principios maestros para gobernar la ciberseguridad**.

  Agrupar, de forma concreta y sucinta, las principales actividades que una organización debe realizar para gobernar de forma adecuada y madura la ciberseguridad corporativa.

  Disponer de un enfoque común de los principios maestros, medidas de seguridad y procedimientos de auditoría, así como de elementos que permitan llevar a cabo el seguimiento del cumplimiento de estándares actuales o futuros del ámbito de la ciberseguridad que puedan ser implantados.

- **Objetivo II. Desarrollar un documento de ayuda para el órgano de administración de la organización y su equipo directivo**.

  Identificar las principales materias relacionadas con la gestión y los riesgos en materia de ciberseguridad que deben ser tratadas por una organización, así como, las sesiones en las que dichas cuestiones deban abordarse y su periodicidad.

- **Objetivo III. Formar y concienciar a los órganos de gobierno y a los equipos directivos de las organizaciones sobre su rol y responsabilidad en materia de ciberseguridad**.

  Servir como referencia para que los administradores de las organizaciones y sus órganos de gobierno puedan conocer sus responsabilidades y funciones en la correcta gestión de la ciberseguridad corporativa.

- **Objetivo IV. Proporcionar una visión integrada de las responsabilidades de supervisión y reporte de la ciberseguridad**.

  Definir de forma explícita las responsabilidades de supervisión y reporte en materia de ciberseguridad, así como proporcionar orientación sobre qué eventos o incidentes significativos deben reportarse a la dirección, a los órganos de gobierno o a los organismos supervisores.

3. ALCANCE

El presente Código de buen gobierno de la ciberseguridad **ofrece recomendaciones de alcance general**, organizadas en principios para que pueda ser utilizado por cualquier organización que persiga realizar una adecuada gobernanza de la ciberseguridad, con independencia de su tamaño, sector, actividad o incluso grado de madurez en la materia.

La efectiva incorporación de los principios y recomendaciones recogidos en el presente Código por parte de una organización podría interpretarse de hecho como una **señal de madurez en ciberseguridad** y contribuir tanto a una mejor gestión del riesgo como a la protección de sus objetivos y los de aquellos grupos de interés que puedan verse afectados por las actividades de la organización.

Asimismo, este Código **podría ser utilizado por parte de la organización como guía para el cumplimiento de las obligaciones** de información que pudieran requerirle los distintos organismos de supervisión.

4. ESTRUCTURA

El Código plantea un **enfoque de principios** definidos como el conjunto de valores, experiencias y normas que orientan y regulan el buen gobierno de la ciberseguridad.

Estos principios podrían considerarse **como el soporte de la visión, misión y objetivos estratégicos** de la gestión del riesgo asociado a la ciberseguridad. Su seguimiento tendría el objetivo de mejorar el proceso de toma de decisiones por parte de los órganos responsables de cualquier organización, con atención al principio de proporcionalidad y con independencia de su tamaño o actividad.

Los principios se desarrollan en recomendaciones que son fundamentales a la hora de implantarlos.

Se han organizado en tres grandes bloques:

- **Estrategia y organización**

  Detalla los principios más importantes sobre los que los órganos de gobierno deben construir la estrategia y organización de la ciberseguridad. Estos principios están relacionados, de manera directa, con la gestión de la ciberseguridad.

- **Gestión**

  Conjunto de actividades, controles y decisiones fundamentales que deben las organizaciones para garantizar que disponen de una madurez adecuada en ciberseguridad, incluyendo la prevención, detección, respuesta y recuperación ante incidentes. Estos principios deben ser aplicados por la dirección de la organización desde la unidad de ciberseguridad o seguridad de la información.

- **Supervisión**

  Detalla los elementos mínimos que deben validar los órganos de gobierno de la organización, así como los requerimientos básicos que debe cubrir la información requerida para poder realizar esta validación. Concreta cómo debería realizarse la supervisión de forma continua por parte de la dirección de las organizaciones y la unidad de ciberseguridad o seguridad de la información.

5. PRINCIPIOS Y RECOMENDACIONES

Principio 1: Proporcionalidad

Las recomendaciones contenidas en este Código se aplicarían a las organizaciones bajo el principio de proporcionalidad, teniendo en cuenta su propia complejidad, tamaño, riesgos a los que estén sometidas, recursos con los que cuenten y el resto de circunstancias aplicables.

5.1 Estrategia y organización

Principio 2: Alineamiento estratégico y visión de futuro

La ciberseguridad, como disciplina que ayuda a las organizaciones a alcanzar sus objetivos, **debe estar alineada con la misión y visión de la organización**.

Recomendación 1: El órgano de administración reconocerá formalmente, en un documento visible públicamente, los principios y compromisos de la ciberseguridad como elemento fundamental para proteger los activos del negocio, con el fin de lograr sus objetivos y cumplir con su misión.

Recomendación 2: Uno de los ámbitos explícitos de la política de control y gestión de riesgos de la organización será la ciberseguridad.

Recomendación 3: La organización, teniendo en cuenta las necesidades operativas del negocio y los riesgos que puedan afectar a la consecución de sus objetivos, definirá planes a corto, medio y largo plazo que aseguren la visión de futuro y mejora continua de la ciberseguridad, permitiendo reducir su exposición al riesgo dentro de los niveles de tolerancia definidos.

Recomendación 4: Se tomarán decisiones en materia de ciberseguridad en función del riesgo real de la materialización de las amenazas sobre la organización. Se implantará, de igual manera, un sistema de monitorización de la eficiencia y el cumplimiento de los objetivos de seguridad definidos.

Principio 3: Responsabilidad y organización

La ciberseguridad es una disciplina compleja y transversal que afecta a todas las actividades de una organización. Es por esto que requiere de un adecuado liderazgo y una estructura que, para ser implantada y gestionada adecuadamente, a su vez debe estar integrada por profesionales con formación y experiencia adecuados.

Recomendación 5: La organización aspirará a que, dentro del órgano de administración, haya, al menos, un miembro con experiencia en gestión de ciberseguridad que apoye y valide los objetivos con anterioridad a su aprobación por el equipo directivo.

Recomendación 6: La organización dispondrá de una unidad que asuma la función de definición, impulso y control de la ciberseguridad y que participe en la toma de decisiones y estrategias en este ámbito. Del mismo modo deberá asegurar el reporte adecuado, y a los niveles oportunos, de los riesgos relacionados con la ciberseguridad, así como de los mecanismos de mitigación y control de los mismos que sean necesarios.

Esta unidad contará con suficientes capacidades y recursos, materiales y humanos, para la consecución de sus objetivos, y dependerá funcionalmente del órgano de administración, de alguna de sus comisiones especializadas o de cualquier otro órgano o miembro de la alta dirección de la organización, siempre que se mantenga la debida independencia respecto de los responsables de sistemas de redes y de información.

Recomendación 7: El máximo responsable de esta unidad será el director de ciberseguridad, director de seguridad de la información o Chief Information Security Officer (en adelante CISO). Esta figura será una persona con el conocimiento, experiencia y competencias adecuadas para desarrollar la función y contará con la suficiente capacidad de decisión e influencia en la organización.

Recomendación 8: Existirá un comité de ciberseguridad, constituido formalmente, en el que estarán representado, además del CISO, un número adecuado de áreas de la organización para adoptar cualquier resolución, con relevancia en materia de seguridad de la información, que pueda afectar sustancialmente a la actividad de la organización.

Recomendación 9: Las organizaciones, en función de su complejidad y exposición al riesgo cibernético, deberán tener en cuenta la ciberseguridad al menos en uno de sus comités de crisis.

Recomendación 10: El órgano de administración asignará la supervisión ejecutiva de la gestión de la ciberseguridad a alguna de sus comisiones especializadas (por ejemplo, la comisión de riesgos, la comisión de auditoría ...).

Principio 4: Ética y cumplimiento

El gobierno de la ciberseguridad debe incluir no sólo el cumplimiento de la normativa aplicable, sino también las **buenas prácticas de seguridad y el uso ético de los recursos de la organización**.

Recomendación 11: El órgano de administración comprenderá las implicaciones de las buenas prácticas, entre otras, en la gestión de los riesgos en materia de ciberseguridad, tanto en su organización, como en cada uno de los mercados en los que opera y en su relación con los distintos grupos de interés.

5.2 Gestión

Principio 5: Modelo de gestión

La ciberseguridad es una materia transversal a toda la organización y a sus procesos de negocio. La gestión de la ciberseguridad debe estar guiada por las mejores prácticas y ser las adecuadas para cada organización.

Recomendación 12: La organización se apoyará en reconocidos estándares, nacionales, europeos o internacionales, adecuados a sus necesidades, para un mejor seguimiento de la evolución de su madurez.

Principio 6: Dotación de recursos

Las organizaciones deben tener en cuenta que la función de la **ciberseguridad requiere una constante y adecuada dotación de recursos** asignados a su mantenimiento y mejora.

> **Recomendación 13:** El órgano de administración se asegurará de que la unidad responsable de la gestión de la ciberseguridad, así como otras unidades con responsabilidad en la consecución de los objetivos establecidos, disponen de suficientes capacidades materiales y humanas para poder llevar a cabo las funciones asignadas de forma efectiva y eficiente.

Principio 7: Gestión de incidentes y resiliencia

Una de las finalidades perseguidas por la ciberseguridad es asegurar la continuidad de la capacidad operativa para los fines de la organización y la de los grupos de interés que puedan verse afectados por sus actividades. Esto se conoce como **resiliencia operativa** y por ello se deben desarrollar capacidades para contener o recuperarse de los ciberincidentes.

> **Recomendación 14:** Se definirá cuándo un incidente tiene la consideración de significativo en función del impacto, del tipo de organización, su sector y las regulaciones a las que pudiera estar sometida en los mercados en los que opere.
>
> **Recomendación 15:** Se identificarán los grupos operativos encargados de su gestión (tanto a nivel técnico y táctico, como estratégico) para minimizar el impacto en el negocio y para asegurar el cumplimiento regulatorio y la adecuada comunicación interna o externa.
>
> **Recomendación 16:** Se dispondrá de capacidades que permitan a la organización ser resiliente para asegurar la continuidad de las operaciones y la recuperación completa de los servicios en un plazo adecuado de tiempo que se determinará en el plan de continuidad de negocio.

Principio 8: Formación y concienciación

Todo **el personal de la organización necesita poseer suficientes conocimientos en materia de ciberseguridad** para enfrentarse y mitigar el riesgo al que esté expuesto[3].

> **Recomendación 17:** La dirección y el órgano de administración fomentarán la formación, concienciación y cultura de ciberseguridad en toda la organización con el objetivo de capacitar a su personal acerca de los hábitos y prácticas recomendables para prevenir y mitigar riesgos en el ámbito de la ciberseguridad.

Principio 9: Innovación y mejora continua

La ciberseguridad requiere adaptarse y mejorar en consonancia con los nuevos y constantes avances de la tecnología y de las ciberamenazas.

> **Recomendación 18:** La gestión de la ciberseguridad estará en constante mejora y evolución para garantizar una defensa adecuada ante las amenazas.

5.3 Supervisión

Principio 10: Ciberinteligencia

La anticipación es un elemento clave en la protección contra cualquier riesgo no sólo de la propia organización, sino también de los grupos de interés que puedan verse afectados por sus actividades, por lo que la organización necesita apoyarse en la ciberinteligencia como base de la preparación en la gestión de la ciberamenazas.

[3] Las personas son el principal activo que disponen las organizaciones para la adecuada protección en materia de ciberseguridad. A la vez, los principales riesgos en esta materia suelen provenir de incidentes que, de forma activa o pasiva, son generados por las personas.

Recomendación 19: El comité de ciberseguridad informará a la dirección y al órgano de administración de las ciberamenazas que podrían afectar a los objetivos de la organización. Para ello, se tendrán en cuenta, al menos, los principales actores y las principales y más recientes ciberamenazas, considerando su potencial impacto sobre las operaciones de la organización.

Principio 11: Informe periódico

Constituye una buena práctica de gobierno según las normas internacionales, y en algunos casos una obligación, **el reporte periódico de la situación de la ciberseguridad de la organización a los órganos de gobierno de la misma**.

Recomendación 20: El órgano de administración realizará un seguimiento regular de la ciberseguridad, incluyendo este tema en el orden del día de sus reuniones o en las de sus comisiones especializadas correspondientes donde aplique (auditoría, riesgos, sostenibilidad u otras comisiones específicas para el tratamiento del riesgo de ciberseguridad), para lo que requerirá informes periódicos de la gestión de ciberseguridad al responsable ejecutivo (director de seguridad de la información o CISO). Este reporte deberá realizarse periódicamente. Se considera una buena práctica su realización al menos dos veces al año.

Recomendación 21: El informe periódico debe contener al menos el estado de la ciberseguridad, la evolución del grado de madurez y del ciberriesgo, la evolución de las amenazas, la asignación de los recursos destinados a la seguridad de las redes y los sistemas de información, los incidentes significativos gestionados si los hubiera, el estado de la seguridad de las operaciones de la cadena de suministro que dependan de terceros, así como cualquier resolución con relevancia en materia de ciberseguridad adoptada por el equipo directivo que pueda afectar sustancialmente a la actividad de la organización. El director de seguridad de la información o CISO también deberá reportar, en su caso, cualquier obstáculo o impedimento que pudiera restringir el adecuado desempeño de su actividad.

Recomendación 22: Cuando en el orden del día de las reuniones del órgano de administración figure algún tema que pueda afectar a la ciberseguridad, se tendrán que tratar las repercusiones que tenga la ciberseguridad en el referido tema como, por ejemplo: grandes iniciativas de transformación digital, implementación de nuevas tecnologías y grandes inversiones en activos tecnológicos, fusiones y adquisiciones, expansión de instalaciones o grandes actualizaciones.

Principio 12: Continuidad

La ciberseguridad es parte de la estrategia de continuidad de la organización y su ensayo es esencial para una correcta preparación ante los ciberincidentes.

Recomendación 23: El órgano de administración requerirá el desarrollo de pruebas periódicas completas que pongan a prueba los mecanismos de resiliencia de la organización como parte de los planes de ciberseguridad.

En este contexto:

- Deben realizarse pruebas del plan de continuidad de negocio, así como simulaciones y ejercicios de preparación de los comités de gestión de crisis.
- En general, las compañías deben ejecutar de forma sistemática simulacros y pruebas efectivas de las distintas medidas de protección, respuesta y recuperación.
- Estos ejercicios han de implicar a toda la organización, con especial atención a los procesos críticos de la compañía, y deben involucrar también a la cadena de suministro.

Recomendación 24: El órgano de administración se asegurará de que la dirección apoye la creación, implementación, prueba y mejora continua de los mecanismos de ciberresiliencia.

Principio 13: Gestión del riesgo

La correcta gestión, evaluación y comunicación del riesgo de ciberseguridad es un **elemento clave en la gestión del riesgo corporativo para toda organización**.

Recomendación 25: Se deberán realizar evaluaciones independientes respecto a la unidad de ciberseguridad, al menos una vez al año, que permitan al órgano de administración obtener un punto de vista adicional y complementario del correcto estado del programa de gestión de los riesgos de ciberseguridad de los procesos críticos de la organización, incluyendo a la cadena de suministro.

6. GLOSARIO

A continuación, se incluye un glosario para facilitar la comprensión de los conceptos presentados en este Código:

Activo de información: es cualquier información o sistema relacionado con el tratamiento de esta que tenga valor para la organización. Pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, equipamiento auxiliar o instalaciones. Esta información es susceptible de ser atacada, deliberada o accidentalmente, con consecuencias para la organización.

Ciberamenaza: amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de este.

Ciberataque: intento deliberado de un ciberdelincuente de obtener acceso a un sistema informático sin autorización sirviéndose de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente daños al sistema.

Ciberinteligencia: es la disciplina que permite que la información procesada sobre la intención, la oportunidad y la capacidad que poseen los actores maliciosos sirva para anticipar la ciberseguridad más adecuada.

Ciberseguridad: la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos. Se materializa en la combinación de personas, políticas, procesos y tecnologías empleadas por una organización para proteger sus activos contra las ciberamenazas con el fin de lograr sus objetivos y cumplir con su misión.

Organización: en este término se engloba no solamente la propia sociedad, sino también a todas las entidades de su grupo.

Riesgo cibernético o ciberriesgo: circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas puede derivar en un incidente de seguridad.

FORO NACIONAL DE CIBERSEGURIDAD

IMPULSO A LA INDUSTRIA Y A LA I+D+i. RESUMEN DE PROPUESTAS Y TRABAJOS DE LA FASE 2

OBJETIVOS Y ALCANCE

2023

Autores

Coordinador sociedad civil:

Luis Álvarez Satorre (Cámara de Comercio de España)

Coordinadora institucional:

Lola Rebollo Revesado (INCIBE)

Autores y colaboradores:

Cristina Alcaraz Tello

Luis Fernando Álvarez-Gascón Pérez

Félix Arteaga Martín

Ana Ayerbe Fernández-Cuesta

Maite Boyero Egido

Juan Miguel Cuéllar del Río

Juan Díez González

Albert Estrada i Capilla

Juan González Martínez

Javier Jarauta Sánchez

Javier López Muñoz

Gregorio Martínez Pérez

César Maurín Castro

José Miguel Rosell Tejada

Francisco Sampalo Lainz

Salvador Trujillo González

Urko Zurutuza Ortega

ÍNDICE

1. INTRODUCCIÓN

El Foro Nacional de Ciberseguridad, como órgano de asistencia al Consejo Nacional de Ciberseguridad Nacional tiene la misión de articular y cohesionar un entorno de colaboración público-privada que, a través de diferentes líneas de acción, genere el máximo conocimiento sobre los desafíos a la Seguridad Nacional en el ciberespacio, ya sean oportunidades o amenazas, y siempre en colaboración con el Consejo Nacional de Ciberseguridad. El establecimiento de sinergias público-privadas permiten establecer un dialogo activo y ejecutable de acciones que permitan avanzar en la protección de la sociedad, y es clave en este marco poder articular acciones concretas para el fortalecimiento de la industria española y el crecimiento del ecosistema nacional de investigación.

El grupo de trabajo 2 (GT2), encargado de impulsar la industria e I+D+i nacionales, presentó sus primeros trabajos y conclusiones el pasado mes de marzo 2021 y decidió la continuidad de estos trabajos en las siguientes áreas:

- Definir una taxonomía nacional alineada con ECSO, JRC y posteriormente la del CCN, INCIBE y otras (SGT2).

- Continuar con los trabajos del barómetro incorporando a este grupo de trabajo a ObservaCiber, englobado dentro del Observatorio Nacional de Tecnología y Sociedad (ONTSI) (SGT2).

- Evaluar las acciones puestas en marcha por Gobierno de España para aumentar la digitalización y la protección frente a ciberataques de las PYMES españolas (SGT3).

- Comenzar la definición de una Agenda de Investigación e Innovación (A2I) de Ciberseguridad como elemento de aumento de competitividad para el ecosistema nacional.

- Trasladar los trabajos y conclusiones obtenidos de la primera fase en cuanto a la necesidad de talento identificado por la industria de ciberseguridad (SGT6) al Grupo de Trabajo 3 (GT3 – Formación, Capacitación y Talento) liderado por el CCN y la CRUE-Universidades.

- Trabajar en acciones de promoción exterior de la industria española de ciberseguridad (SGT1 y SGT8).

Los trabajos presentados en este informe se han realizado durante el 2022 en reuniones bimensuales entre todos los subgrupos de trabajo y reflejan la imperante necesidad de continuar con las actividades del GT2, más allá de las conclusiones y resultados presentados en este documento, lo que permitirá alcanzar el objetivo de impulsar y mejorar las capacidades de la industria y de la investigación nacional que convertirán a España en un país líder en el ámbito de la ciberseguridad.

2. CONTEXTO

La **ciberseguridad** es hoy uno de los **retos más importantes** a los que se enfrentan gobiernos, empresas y ciudadanos. En un contexto global, interconectado y dependiente de la tecnología como es el actual, **la ciberseguridad resulta imprescindible para alcanzar la necesaria confianza en el ámbito digital ligada a la imparable transformación digital de la sociedad y su tejido productivo**.

La importancia que adquiere en la actualidad el **diseño de políticas públicas para impulsar la ciberseguridad** es creciente. Un fenómeno que está alineado con la prioridad estratégica de la Unión Europea en digitalizar la economía, pues ello comportará una mayor autonomía estratégica de su industria y sectores críticos. Ya en la Comunicación oficial de la Comisión Europea "Configurar el futuro digital de Europa" (2020) [1] se prefiguraban iniciativas para promover las soluciones tecnológicas que permitirán a la UE liderar la transformación digital.

Por su parte, la **Estrategia Europea de Datos** [2], de febrero de 2020, establece cuatro pilares como requisitos previos esenciales para una sociedad empoderada por el uso de los datos, la **protección de datos**, los **derechos fundamentales**, la **seguridad** y la **ciberseguridad**.

En este marco de actuación, se lanzaba el nuevo **Programa Europa Digital** (2021-2027) [3] con una inversión total de 8.200 M€, de los cuales, 1.900 M€ se destinan al despliegue de capacidades para la ciberseguridad para administraciones públicas, empresas e individuos. Y, de forma complementaria, el **Plan de Recuperación Europeo** (*EU Recovery Plan*) [5] apuesta por una presencia tecnológica más fuerte en ámbitos como la IA, la infraestructura de datos, las redes 5G y 6G, el *blockchain* y la ciberseguridad y ciber-resiliencia.

En este contexto, la reciente Estrategia Europea de Ciberseguridad [5], presentada el 16 de diciembre de 2020 por la Comisión Europea y el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad, busca **impulsar la resiliencia colectiva en Europa contra las amenazas cibernéticas y ayudar a garantizar que todos los ciudadanos y empresas puedan beneficiarse plenamente de servicios fiables** (4.500 millones de euros de inversión combinada entre la UE, los Estados miembros y la industria). Así, el objetivo 3 de la Estrategia pretende reforzar las capacidades industriales y tecnológicas de la UE en materia de ciberseguridad, incluso mediante proyectos financiados conjuntamente por los presupuestos nacionales y de la UE. Esta estrategia es un componente clave de otros planes y estrategias como el *Shaping Europe's Digital Future*, la *New Industrial Strategy*, el *EU Recovery Plan* y la *EU Security Union Strategy* 2020-2025.

A nivel nacional existe un **alineamiento con la política industrial y digital europea** y, en concreto, con la Estrategia Europea de Ciberseguridad, a través de:

- La **Estrategia Nacional de Ciberseguridad** [6], dentro de su *Objetivo IV: Cultura y compromiso con la Ciberseguridad y potenciación de las capacidades humanas y tecnológicas*, desarrolla a través de una serie de medidas que incluyen "impulsar programas de apoyo de I+D+I en seguridad digital y ciberseguridad en empresas, universidades y centros de investigación".

- La **Agenda España Digital 2026** [7], que tiene como cuarta medida de acción: *"Reforzar la capacidad española en ciberseguridad, consolidando su posición como uno de los polos europeos de capacidad empresarial".* Además, como ejes de la Agenda, se presentaron en diciembre de 2020, el Plan para la Conectividad y las Infraestructuras Digitales y la Estrategia de Impulso a la Tecnología 5G, dotados con 4.320 millones de euros hasta 2025.

- El **Plan de Recuperación, Transformación y Resiliencia de España** [8] en el contexto global del plan europeo "*Next Generation EU*", constituye el *marco global estratégico del país al incorporar una importante agenda de inversiones y reformas estructurales*, que se interrelacionan y retroalimentan para lograr objetivos transversales tales como la transformación digital de la sociedad y su tejido productivo.

- Las Directrices Generales de la **Nueva Política Industrial 2030** [9], en concreto, en el eje 1. Digitalización, "*se hace hincapié en la promoción de la ciberseguridad como una de las acciones clave a llevar a cabo dentro de la actuación 1. Impulso a la transformación digital desde el Estado*".

- La **Estrategia Española de Ciencia, Tecnología e Innovación (2021-2027)** [10] incide en la *necesidad de impulsar instrumentos de apoyo público en I+D+I para promover la ciberseguridad en la industria y en tecnologías clave*, a través del Sector estratégico 4. Seguridad para la Sociedad (línea estratégica de ciberseguridad).

- Otras estrategias vinculadas: Estrategia de Seguridad Nacional (2021) [11] y **Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave (2019-2023)** [12].

Como **instrumento para impulsar la colaboración público-privado** en esta materia se creó, en julio de 2020 en España, el **Foro Nacional de Ciberseguridad** [13], para dar respuesta al objetivo 3 de la Estrategia Nacional de Ciberseguridad *"Protección del ecosistema empresarial y social y de los ciudadanos",* a través de la línea de acción 4 *"Impulsar la ciberseguridad de ciudadanos y empresas".* Liderado por el Consejo de Seguridad Nacional y en asistencia al Consejo Nacional de Ciberseguridad, integra a representantes de la sociedad civil, expertos independientes, centros de investigación, empresas, asociaciones, etc., para debatir y generar conocimiento sobre las oportunidades y amenazas para la seguridad en el ciberespacio.

La ambición de alcanzar una **posición de liderazgo internacional en materia de ciberseguridad** será más viable si se orientan los esfuerzos de entidades públicas y

privadas con una perspectiva de especialización, seleccionando nichos con alto potencial de desarrollo y comercialización no cubiertos en la actualidad, que además de contar con las capacidades actuales del sector, respondan a retos de la industria nacional y dispongan de alta capacidad de escalado e internacionalización.

3. BARÓMETRO Y TAXONOMÍA

Durante la primera fase de los trabajos del FNCS, en el Subgrupo de Trabajo 2, se identificaron como críticas tres acciones para el sector español de la ciberseguridad:

- **Identificar la cadena de valor** completa que incluya oferta y demanda, e identifique y cualifique los actores de dicha cadena.
- **Definir, diseñar e implantar un barómetro** que mida los principales indicadores del ecosistema de ciberseguridad español.
- **Acordar una taxonomía común entre la industria y la investigación** que establezca los productos y servicios de ciberseguridad a desarrollar e implantar.

Estas tres acciones, disminuirán el gap identificado en el ecosistema de ciberseguridad español y europeo entre la industria y la investigación.

Adicionalmente, consideramos que la base de la mejora se encuentra en una adecuada medición, orientada a precisar los siguientes puntos:

- QUIÉN: **cadena** de valor global de la ciberseguridad.
- QUÉ: **taxonomía** de las competencias en ciberseguridad.
- CÓMO y CUÁNTO: **barómetro** de ciberseguridad en la industria e investigación.
- DÓNDE: **observatorio** integral de la ciberseguridad.

En esta segunda fase de los trabajos se propone mantener y profundizar en el desarrollo e implantación de las tres acciones críticas identificadas, pero cambiando el orden de estas: taxonomía, cadena de valor y barómetro.

Así pues, se propone priorizar la taxonomía de las competencias de ciberseguridad, es decir, definiendo inicialmente el "qué" debemos hacer, para continuar con la cadena de valor que identifique el "quién" con los actores principales en el ecosistema, y terminar con el "cómo y cúanto" que se concretarán en el barómetro integral de la ciberseguridad.

Igualmente, esta nueva priorización ayudará a la interacción necesaria con otros grupos de trabajo que necesitan para su labor, disponer lo antes posible de una taxonomía común.

Por último, la aparición en los últimos meses del Observatorio de la Ciberseguridad (Observaciber) nos hace concluir que han de estar alineados los trabajos de este grupo de

trabajo sobre el barómetro, con los que se están realizando en Observaciber y, por tanto, agendar los trabajos de dicho barómetro, para la segunda parte del año 2023.

3.1. Situación actual de los modelos de taxonomía

En los trabajos de Foro en su fase inicial, se identificaron dos propuestas de taxonomías de referencia europeas publicadas por ECSO orientadas, hacia la industria, y por JRC orientada a la investigación y se elaboró una propuesta inicial de taxonomía híbrida, que permite relacionar ambas y cuya estructura será objeto de revisión y detalle en esta segunda fase.

Por otra parte, existen varios trabajos en diferentes organizaciones y proyectos europeos orientados a la revisión y actualización de las taxonomías existentes, que es necesario seguir y alinear con los trabajos en nuestro país.

De hecho, la importante representación española actualmente en organismos como ECSO, ENISA y otros, así como el gran impulso a la industria e investigación nacional promovido durante los últimos meses por el DSN, CCN e INCIBE, hace que consideremos que nuestro país se encuentra en condiciones idóneas para promover y liderar un modelo de taxonomía integrada de ciberseguridad.

3.2 Otras taxonomías para incluir en el modelo integrado

Durante el año 2022, se han venido desarrollando importantes iniciativas y proyectos por parte de las administraciones públicas, entre los que se pueden destacar los siguientes:

- En febrero, el Gobierno aprueba la creación del SOC-AGE [14].
- En marzo, el CCN actualiza Taxonomía de productos STIC-140 [15].
- En mayo, se publica el RD 311/2022 sobre el nuevo ENS [16].
- En octubre INCIBE publica la primera Compra Publica Precontractual (CPP1) [17].
- En octubre INCIBE publica la segunda Compra Publica Precontractual (CPP2) [18].
- En noviembre CCN anuncia un “Ciberescudo Único” y actualiza CPSTIC-105 [19].

Todas ellas, de un modo u otro, implican una actualización de los productos y servicios que se ofrecen y se demandan en nuestro sector, tanto por parte de organismos públicos como por parte de la industria y la investigación.

Estas iniciativas hacen que, durante el presente año, el sector de la ciberseguridad haya sido uno de los más dinámicos y con mayor impulso entre todos los sectores tecnológicos de la sociedad.

Al mismo tiempo, hacen que sea conveniente generar un modelo integrado de todas las taxonomías del sector, por lo que proponemos la creación y actualización constante de un **Modelo Integrado de una Taxonomía Española en Ciberseguridad** (en adelante **MITEC**) incluyendo los productos y servicios de ciberseguridad.

3.2.1. Taxonomía CCN-STIC-140. Productos de seguridad TIC

El CCN dispone de un modelo de taxonomía de referencia para productos de seguridad TIC, plasmado en el catálogo CCN-SITC-140 y cuya última actualización es de marzo del presente año.

El modelo está estructurado en tres grupos:

1. Productos cualificados para información sensible, según el ENS:
   - Formado por 9 categorías y 49 familias de productos
2. Productos aprobados para información clasificada:
   - Formado por 1 categoría y 3 familias de productos.
3. Productos y servicios de conformidad y gobernanza:
   - Formado por 6 familias de productos y servicios.

Dicha taxonomía de referencia se plasma en el catálogo de productos CCN-STIC-105 que según el nuevo ENS 2022 es necesario utilizar para la implantación del nivel ENS requerido.

Todo ello, hace necesario incorporar e integrar esta taxonomía en el Modelo Integrado de Taxonomía que se defina en los trabajos de este subgrupo.

3.2.2. Retos de la Compra Pública Innovadora de INCIBE

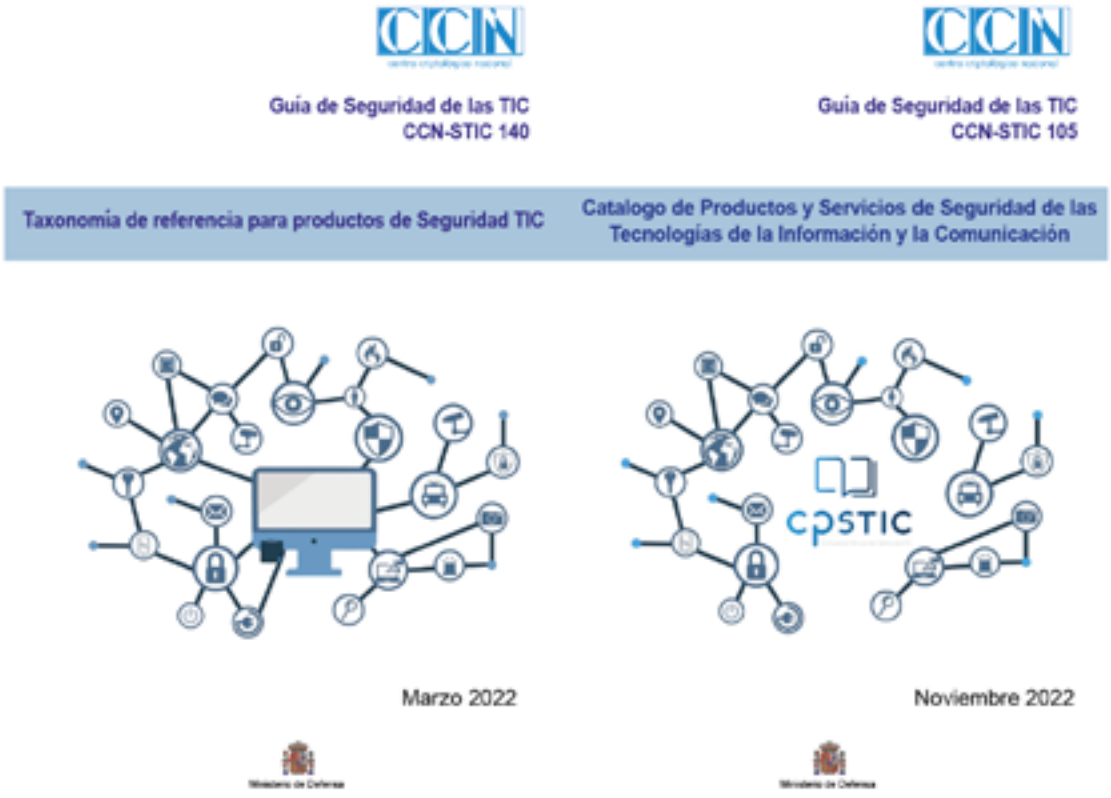
En julio de 2021, INCIBE puso en marcha una iniciativa estructurada en varias fases, que comenzó por un proceso de Consulta Preliminar al Mercado, que permitió definir un Mapa de Demanda Temprana, y seguidamente las dos iniciativas de Compra Pública Precomercial (CPP1 y CPP2) del presente año, que han supuesto un importante impulso al ecosistema de la ciberseguridad.

Desde la primera fase de dicha iniciativa, todo el sector de la ciberseguridad español, incluyendo industria e investigación, proporcionó la información necesaria para que INCIBE pudiera identificar, de forma realista y actualizada, los principales productos y servicios que se ofrecen y se requieren hoy en día en el ecosistema de ciberseguridad español.

La consecuencia práctica de dicha iniciativa, son las dos convocatorias para programas de I+D lanzados al mercado como Compra Pública Precomercial que se detallan seguidamente.

- Compra Pública Precomercial 1, donde se establecen 7 retos y necesidades públicas.
- Compra Pública Precomercial 2, donde se establecen 30 retos, incluyendo productos y centros de operaciones de ciberseguridad sectoriales.

Por tanto, el objetivo del Modelo Integrado de Taxonomía será incluir tanto los 7 retos de la primera convocatoria, como los 30 retos de la segunda, estableciendo una congruencia entre la taxonomía que se defina, con los retos que empezarán a funcionar durante 2023.



3.2.3. Servicios SOC para las Administraciones Públicas

España es el país que dispone del mayor número de CSIRT actualmente en el catálogo establecido por ENISA, contando con 84 CSIRTs públicos y privados. Esto nos posiciona igualmente como uno de los países europeos con mayor cantidad y calidad de servicios SOC.

El Gobierno español, con su iniciativa a comienzos de 2022 de crear un servicio SOC integrado para las organizaciones de la Administración General del Estado (SOC-AGE), se posiciona como pionero a nivel europeo en este tipo de iniciativas. De hecho, la Comisión Europea, dentro de su iniciativa DEP – *Digital Europe Program*, acaba de solicitar propuestas para un proyecto similar de SOCs europeos para 2023.

Como parte de esta iniciativa, en el SOC-AGE se ha definido un catálogo de más de **20 servicios** que actualmente es confidencial, pero que respetando dicha confidencialidad, en los trabajos del FNCS se verificará que los mismos estén incluidos en el modelo de taxonomía que se defina.


Spain
84 teams
OBSAE
Observatorio de Administración Electrónica
Relaciones entidades
Coordinación incidentes
CCN
SGAD
Implantación
Operación
Detección de incidentes
Coordinación
Seguimiento servicio
Entidades AGE
SOC (Servicio de Operaciones de Ciberseguridad
Infraestructura ciberseguridad
Inteligencia ciberseguridad

3.3. Planificación de las acciones

Hasta el momento, los trabajos de este subgrupo han estado orientados a la identificación y actualización de las diferentes fuentes de productos y servicios de ciberseguridad en los que se está trabajando en España y Europa, para posteriormente comenzar los trabajos de la definición del Modelo Integrado de Taxonomía, que se realizará durante el primer trimestre de 2023, con el objetivo de lanzar un piloto en el primer semestre del próximo año.

Posteriormente, se continuará con los trabajos de cadena de valor y de barómetro para completar los mismos en la segunda parte del año próximo, según la siguiente planificación:

DESCRIPCIÓN	Q1-23	Q2-23	Q3-23	Q4-23
1.0 Taxonomía Común de Ciberseguridad para la Industria & I+D+i				
1.1 Identificar estado actual en España y EU	■			
1.2 Propuesta de Taxonomía Común		■		
1.3 Prueba de concepto en algún Caso de Uso			■	
2.0 Cadena de valor de la Ciberseguridad				
3.1 Clasificación e identificación de actores		■		
3.2 Metodología para la identificación de actores y BBDD			■	
3.3 Presentación en Plataforma				■
3.0 Barómetro Integral de la Ciberseguridad				
1.1 Identificar estado actual en EU		■		
1.2 Definición de los KPI principales y metodología de obtención			■	
1.3 Presentación en ObservaCiber				■
1.4 Metodología de seguimiento y comunicación				■

4. RETOS DE CIBERSEGURIDAD EN LAS PYMES

Ante los desafíos planteados por la pandemia de la COVID-19 y la necesidad de construir la Europa de la nueva generación, se ha puesto en marcha el programa ***Kit Digital***, financiado por los fondos Next Generation de la Unión Europea, que se materializa a través del Mecanismo de Recuperación y Resiliencia (MRR) y React-UE. El programa *Kit Digital*, se encuadra bajo el Componente 13 Inversión 3, dedicado al impulso a las PYME, asimismo, contribuye a actuaciones del Componente 15 y Componente 19.

En un país dónde su tejido empresarial está formado por pymes en un 99,83%, y la mayoría son micropymes, bien sin asalariados, bien de hasta 9 empleados, **la digitalización acelerada está suponiendo un gran reto puesto que este tipo de empresas no tiene realmente concienciación ni preparación en ciberseguridad** y, además, su nivel de madurez digital en esta materia es bajo, por lo que se considera imprescindible y prioritario trabajar a corto plazo en las siguientes actividades: sensibilización, competencias en ciberseguridad y dotación de herramientas específicas.

Para la definición y ejecución de las actividades propuestas a continuación se considera necesaria la estrecha colaboración del INCIBE con la Cámara de España.

Por otro lado, con el fin de maximizar la llegada a las empresas de las medidas propuestas, se considera la **participación activa** de la Red de cámaras de comercio, dada su capilaridad y cercanía a las pymes. Asimismo, la coordinación de la Cámara de España asegura un tratamiento uniforme en el conjunto del territorio nacional y garantiza la prestación de servicios homogéneos a las empresas.

Asimismo, para la ejecución de las medidas se pone a disposición la **red de Oficinas Acelera Pyme de las Cámaras de comercio**, creadas en colaboración con la entidad pública empresarial Red.es, para el impulso de la transformación digital de las pequeñas y medianas empresas, autónomos y emprendedores, conforme a lo establecido en el Real Decreto-ley 8/2020, de 17 de marzo, de medidas urgentes extraordinarias para hacer frente al impacto económico y social del COVID-19, en el que se identifica como prioridad inmediata preparar y dotar de los recursos necesarios a las pymes para su desarrollo digital, así como **mejorar los servicios de asesoramiento personalizado a las PYMES y acompañamiento en su esfuerzo de digitalización**, señalando además la necesaria colaboración de las cámaras de comercio en el apoyo a la transformación digital de las pymes, a través del Plan Acelera PYME de Red.es.

Para todas las actividades que se indican a continuación se tendrá en cuenta:

- La información generada en el **Programa de Ciberseguridad de la Cámara de España** durante sus ejecuciones de 2020, 2021 y 2022.

- Asimismo, se realizará una categorización más detallada, a partir de 2023, de los asesoramientos que se realizan en las **Oficinas Acelera Pyme**, y que estén relacionados con la ciberseguridad.

- El nivel de contratación de soluciones de ciberseguridad en el ámbito del **Programa Kit Digital**, en el que la Cámara de España actúa como entidad colaboradora de Red.es.

Se adjunta en el Anexo 1 la actualización a diciembre de 2022, de los principales indicadores de los tres programas mencionados.

Por tanto, se explotará esta información para determinar los potenciales sectores prioritarios, las temáticas más urgentes, y las mayores necesidades de las pymes en materia de ciberseguridad (ya sea de concienciación o de herramientas o soluciones a implantar).

4.1. Sensibilización en ciberseguridad

Se propone la definición y realización de un ciclo de jornadas de sensibilización en las sedes de las cámaras de comercio y de las Oficinas Acelera Pyme. Para ello, se realizarán las siguientes tareas:

- Definición de temáticas.

- Identificación de cámaras y oficinas Acelera Pyme y establecimiento del calendario.

- Ejecución del ciclo de jornadas.

Asimismo, se propone la realización de una campaña de comunicación a nivel nacional. Para ello se definirá previamente un plan de comunicación adecuado.

4.2. Definición de una matriz de categorización de pymes

Con el fin de poder adaptar y personalizar las actuaciones, contenidos y herramientas de ciberseguridad a las características y circunstancias concretas de las pymes, se considera necesaria la definición de una matriz que permita su categorización. Para ello, con el apoyo del Servicio de Estudios de las Cámara de España:

- Se realizará una encuesta de ciberseguridad a pymes, a través del Observatorio de Competitividad.

- Se definirán los criterios de categorización de las pymes.

- Se identificarán y seleccionarán las fuentes de información adecuadas.

4.3. Competencias en ciberseguridad

4.3.1. Formación y capacitación a asesores

Se considera necesario disponer de personal cualificado que pueda asesorar y sensibilizar adecuadamente a las pymes, en una red que tenga la capilaridad suficiente para llegar a ellas. Por tanto, se propone realizar un programa de formación por parte del INCIBE a técnicos de cámaras de comercio localizada en la red de Oficinas Acelera Pyme, de manera que puedan prestar correctamente los servicios en materia de atención personalizada y de sensibilización a empresas.

4.3.2. Diagnóstico y asesoramiento personalizado

La Cámara de España, ejecuta, a través de la Red de cámaras de comercio, un programa de ayudas, que capacita a las pymes a prevenir los principales riesgos en ciberseguridad, asumibles por ellas mismas, para garantizar que los sistemas de información y telecomunicaciones que utilizan poseen un adecuado nivel de ciberseguridad.

La primera fase del programa para la pyme consiste en un análisis exhaustivo de sus sistemas de información y telecomunicaciones para identificar los principales riesgos referidos a la ciberseguridad.

Este diagnóstico continuará con su ejecución en 2023, a través de las cámaras de comercio, si bien se actualizará en función de la explotación de los datos de ejecución del propio programa y de la definición de la matriz de categorización de pymes.

Asimismo, se puede prestar asesoramiento personalizado y acompañamiento a pymes en materia de ciberseguridad, a través de la Red de Oficinas Acelera Pyme de las cámaras de comercio, establecidas en colaboración con Red.es.

4.3.3. Ayudas para la implantación de soluciones

En la segunda fase del programa mencionado en el apartado anterior, la empresa recibe una subvención para la implantación de herramientas de ciberseguridad. Se realiza un seguimiento del ritmo de ejecución y de la adecuación de los proyectos de implantación.

Las soluciones por implantar se corresponden con las recomendadas en la fase I, de asesoramiento. Por tanto, parte de los trabajos a corto-medio plazo sería revisar y actualizar, en su caso, el catálogo de soluciones subvencionables del programa. En cualquier caso, este no detendrá su ejecución.

4.3.4. Creación e implantación del sello de procesos de ciberseguridad INCIBE – CCE en empresas y entidades

INCIBE y la Cámara de España, a través de la Red de Cámaras, podrían convertirse en referencia y emisoras del "Sello de Confianza de Ciberseguridad" INCIBE - CCE, actuando como prescriptora y emisora de una homologación (sello o certificado) referido a temas de ciberseguridad. Esto es, actuar como institución que delimitara los términos y condiciones que una empresa española debería disponer para cumplir con unos determinados estándares en materia de ciberseguridad.

Las cámaras se encargarían de informar a las empresas sobre los requisitos precisos, así como de comprobar el cumplimiento de éstos.

Las tareas relativas a esta actividad serían:

- Definición de requisitos.
- Elaboración de un estándar.
- Formación y capacitación a cámaras.
- Despliegue del "Sello de Confianza de Ciberseguridad" INCIBE – CCE.

4.4. Cronograma de próximos pasos

DESCRIPCIÓN	Q1-23	Q2-23	Q3-23	Q4-23
1 Sensibilización en Ciberseguridad				
1.1 Jornadas de sensibilización y talleres de capacitación				
1.2 Campaña de Comunicación Nacional				
2 Definición matriz de categorización de pyme				
2.1 Observatorio Competitividad CCE-Encuesta Ciberseguridad a Pymes				
2.2 Selección y definición de criterios de categorización				
2.3 Identificación y selección de fuentes de información				
3 Competencias en Ciberseguridad				
3.1 Formación y capacitación a asesores				
3.2 Diagnóstico y asesoramiento pesonalizado				
3.3 Ayudas para implantación de soluciones				
3.4 Sello Ciberseguridad INCIBE - CCE				

5. AGENDA DE INVESTIGACIÓN E INNOVACIÓN EN CIBERSEGURIDAD (A2I)

En la documentación generada y publicada en 2021 [20] por el Grupo de Trabajo 2, "Impulso a la industria y a la I+D+i" se recomienda la definición de una **agenda de investigación e innovación** a nivel nacional, de forma que se prioricen los ámbitos de I+D+i en los que se debe apostar a nivel regional y nacional y en donde deben centrarse los esfuerzos investigadores de innovación y de financiación.

Para la elaboración de dicha agenda, tendrán un papel protagonista en el desarrollo de la agenda las **universidades, centros tecnológicos y empresas de ciberseguridad especializadas.** Por su parte, el valor de organizaciones como las infraestructuras críticas y esenciales, las empresas consumidoras y las asociaciones o clústeres de ciberseguridad residirá en su conocimiento de las necesidades actuales y de los retos futuros de la industria.

Para racionalizar los esfuerzos y sacar un mayor partido de los recursos que se asignen, conviene tener en cuenta que existen en Europa **diferentes iniciativas que pueden servir de modelo** para el desarrollo de la agenda de investigación e innovación (en adelante A2I). Es destacable el esfuerzo llevado a cabo por la *European Cyber Security Organisation* (ECSO) [21] en su grupo de trabajo WG6 y también los trabajos de cuatro pilotos europeos: SPARTA, ECHO, CONCORDIA y CyberSec4Europe [22] a través de sus respectivas hojas de ruta.

Es en este contexto donde se plantea la definición de una A2I nacional, y cuyos objetivos, alcance y metodología se describen en el resto de este documento.

5.1. Objetivos de la A2I

El objetivo principal de la A2I es analizar las necesidades en materia de I+D+i en ciberseguridad, conocer las capacidades actuales del ecosistema español, y con todo ello identificar las oportunidades que se pueden presentar como país en esta materia a medio y largo plazo. De esta manera, se pretende contribuir de forma activa a la coordinación de las actividades españolas de investigación e innovación en el marco de la Estrategia de Ciberseguridad Nacional.

La elaboración de la A2I persigue los siguientes objetivos concretos:

- **Detección de las capacidades y fortalezas** del ecosistema nacional de I+D+i en ciberseguridad, identificando ámbitos o temáticas y su desarrollo (productos, servicios, patentes, publicaciones).

- **Detección de las prioridades y necesidades** de ciberseguridad por parte de los usuarios finales (Administraciones Públicas, Ministerio de Defensa, Fuerzas y Cuerpos de Seguridad del Estado, Ministerio del Interior, empresas, ciudadanos, etc.) y en especial por parte de la demanda sofisticada (sectores estratégicos, SOCs, etc.).

- **Identificación de la capacidad de adquisición de soluciones o volumen de mercado** por parte de las administraciones y otros usuarios finales.

- **Análisis de los condicionantes sociales, tecnológicos, económicos o políticos**.

- **Análisis de los instrumentos** dedicados de manera específica a la ciberseguridad, como convocatorias de apoyo a la I+D+i de, entre otros, los países identificados en la sección 4.3.3, así como un análisis comparativo entre países de los resultados derivados de dichos instrumentos.

- **Contrastes y correlaciones** entre necesidades, capacidades e instrumentos existentes a nivel nacional y su comparación con el resto de los países identificados.

- **Detección de los nichos y oportunidades** existentes en el panorama nacional e internacional de soluciones y productos de ciberseguridad y, por consiguiente, oportunidad para la Industria de ciberseguridad nacional en combinación con los demás actores del ecosistema de I+D+i.

- **Propuesta de las líneas estratégicas** de I+D+i en ciberseguridad con alto potencial en España.

- **Armonización de los programas de financiación** en España (nacionales, regionales y locales) de la I+D+i en ciberseguridad acorde a objetivos estratégicos.

- **Identificar e involucrar al ecosistema inversor** nacional público y privado.

5.2. Modelo de gobernanza

Para la elaboración de los resultados previstos, se propone la creación de un modelo de gobernanza basado en la colaboración público-privada abierto a la colaboración y participación de los agentes y actores relevantes, con espíritu de transparencia, neutralidad, consenso en sus decisiones y coordinado con otras iniciativas relacionadas.

El objetivo es que todos los posibles participantes, puedan primeramente aportar su visión, participar en revisiones y, finalmente, aportar su refrendo o conformidad con el texto generado.

Los trabajos para la elaboración de la A2I estarán liderados por INCIBE, como responsable último de su gestión y seguimiento, y contarán con la participación activa de un **grupo decisor** (conformado preliminarmente con los integrantes del subgrupo 5, del grupo de trabajo 2 "Impulso a la industria y a la I+D+i" del Foro Nacional de Ciberseguridad con la posibilidad de unirse miembros de otros subgrupos de dicho grupo), en el que participará un grupo de agentes reducido, pero representativo del sector para la toma

ágil de decisiones y revisión de la documentación y entregables, así como del trabajo final, actuando igualmente como tractores dentro de lo colectivos a los que representan.

5.3. Alcance

La A2I será un documento que identifique las principales líneas de investigación e innovación en ciberseguridad y que tendrá como público objetivo principal el sector de la ciberseguridad nacional, integrado fundamentalmente tanto por la industria de ciberseguridad, los organismos de investigación, así como agentes normalizadores y reguladores y las autoridades competentes en esta materia. También es de interés para aquellas entidades con alta demanda de soluciones en ciberseguridad, en especial los SOCs y CSIRTS públicos y privados, Fuerzas y Cuerpos de Seguridad del Estado, así como operadores estratégicos de sectores críticos. Por último, es también de alto interés, tanto para inversores privados especializados en ciberseguridad como para las Administraciones públicas (locales, regionales, o nacionales) con programas de financiación a la I+D+i.

5.3.1. Partes interesadas

Las partes interesadas serán las entidades que, a través de sus representantes designados, participen en la elaboración y validación de la A2I para lo cual podrán proporcionar su aportación y opinión, y participar en la discusión y debates con el objetivo de que la versión final de la A2I sea debidamente consensuada y contrastada.

Los participantes de esta iniciativa serán seleccionados por ser expertos en alguna de las áreas de interés identificados en esta A2I de conformidad con los objetivos establecidos. El grupo de participantes debe ser suficiente en número y suficientemente representativo de todos los colectivos del sector para garantizar una perspectiva global desde todos los puntos de vista.

Se busca contar con representantes de los siguientes colectivos:

5.3.2. Autoridades competentes nacionales.

La creación de un documento de estas características requiere la colaboración y la aprobación por parte de todos los actores principales implicados en el marco de la Ciberseguridad nacional definido por la **Estrategia de Ciberseguridad Nacional** para contar con el consenso y respaldo de todos los intervinientes, entre los que se encuentran todos los actores implicados con competencias en ciberseguridad.

5.3.3. Usuarios finales

Los **usuarios finales** que demandan soluciones de ciberseguridad, entre los que se encuentran las Administraciones Públicas, el Ministerio de Defensa, el Ministerio de Interior, incluyendo las Fuerzas y Cuerpos de Seguridad del Estado, los representantes de pymes, de ciudadanos, así como la demanda sofisticada (sectores y operadores estratégicos) son también actores relevantes en la elaboración de esta A2I.

5.3.4. Organismos de investigación

De igual modo, el documento debe plasmar las capacidades de los **organismos de investigación** de carácter nacional**,** por lo que se requiere contar con su visión y activa participación. Según la Ley 14/2011 (reformada por la Ley 17/2022), un organismo de investigación es una entidad pública o privada que tiene como objetivo principal la realización de actividades de investigación científica y técnica. Estos organismos pueden ser universidades, centros de investigación, institutos y/o centros tecnológicos, unidades de I+D empresarial, fundaciones, etc.

5.3.5. Industria de ciberseguridad

La visión de la **industria de la ciberseguridad** como agente capaz de generar soluciones y productos de ciberseguridad a los usuarios finales, guiando y canalizando la actividad del ecosistema investigador, también es fundamental a la hora de redactar un documento de estas características. En esta categoría se engloban entidades de todos los tamaños desde startups de nicho, micropymes, pymes y grandes empresas, y tanto centradas en producto como en servicios.

5.3.6. Asociaciones y agrupaciones sectoriales

Representativas tanto de la industria, como de la investigación, así como de usuarios finales sectoriales.

Por ejemplo, la Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC) [23], compuesta por universidades y centros de investigación y tecnológicos, ha identificado la creación de esta A2I como una de las medidas prioritarias a realizar para la formulación, definición y aterrizaje de las estrategias tanto nacionales como europeas en materia de I+D+i en ciberseguridad.

5.3.7. Ecosistema inversor

Potenciar nuestra industria de ciberseguridad nacional actual y futura requerirá también identificar, involucrar y hacer partícipe a los agentes públicos y privados de inversión sensibles a la A2I y los propósitos que persigue.

5.3.8. Otros agentes

Se invita a otros agentes involucrados en la actividad investigadora, innovadora, financiadora, normativa o reguladora a que aporten su visión y colaboren de forma activa y participativa.

INCIBE y el resto de los miembros del grupo decisor podrán proporcionar contactos en las entidades enumeradas anteriormente, si fuera necesario, para la elaboración de la A2I.

5.4. Taxonomía

Para la elaboración de los resultados previstos, es preciso disponer de una taxonomía o taxonomías de referencia que permitan clasificar las fortalezas, las oportunidades, las soluciones, así como las líneas de investigación u otras características necesarias. Esto permitirá seguir esquemas de referencia aceptados por el sector de ciberseguridad español y que permitan la clasificación de elementos y facilitar su comparación.

La taxonomía por emplear será la elaborada por el SGT2 denominada MITEC y será utilizada a lo largo de los trabajos descritos en este documento. La taxonomía en sí misma no forma parte del alcance de la A2I, pero deberá ser utilizada a lo largo de los trabajos descritos en este documento.

Los anexos de este documento amplían más información en relación con la taxonomía a emplear.

5.5. Resultados previstos

El resultado principal a generar en este proyecto es la elaboración de la propia **A2I** como documento de referencia, que aglutina los objetivos planteados.

Adicionalmente, para poder completar esta información se prevé también como resultado previo la generación de determinados **informes preparatorios**. Estos informes deberán contener un diagnóstico riguroso sobre el estado actual de determinadas temáticas y tener entidad de documento independiente con posibilidad de poder publicarse por separado siendo autocontenidos y aportando información completa por sí mismos.

Se detallan a continuación los citados informes preparatorios:

5.5.1. Análisis comparativo de agendas estratégicas y otras iniciativas internacionales

En el contexto europeo, disponemos de distintos estudios en ámbito de la ciberseguridad y la seguridad. Más concretamente, la asociación europea ECSO (*European Cybersecurity Organisation*) elaboró a finales de 2016 una Agenda Estratégica de Investigación e Innovación (SRIA) [24] en el ámbito de la ciberseguridad, que fue posteriormente analizado por ENISA [25].

Del mismo modo se incluye el *roadmap* tecnológico elaborado por SPARTA [26] que es uno de los 4 pilotos de centros de competencia en ciberseguridad lanzados por la Comisión Europea.

La Comisión Europea ha elaborado también un “Cybersecurity Atlas” [27] donde se realiza un mapeado de todos los grupos de investigación europeos en el ámbito de la ciberseguridad.

Asimismo, en el contexto europeo, la Comisión Europea acaba de hacer públicos los resultados del estudio de caracterización del sector de la seguridad civil europeo [28].

Estos documentos deberán ser analizados y comparados previamente para la elaboración de la A2I en España, así como otros posibles documentos de referencia de consorcios de proyecto, asociaciones u organizaciones internacionales, u hojas de ruta para facilitar objetivos comunes, así como perfilar oportunidades diferenciales identificadas.

5.5.2. Mapa de capacidades de I+D en ciberseguridad

El objetivo es identificar las líneas de investigación del ecosistema nacional de I+D+i en ciberseguridad, identificando su grado de madurez y liderazgo en el contexto internacional, así como las más noveles, o inexistentes.

Incluyendo los siguientes grupos:

- Organismos de investigación.
- Unidades de I+D empresarial.

Para el informe de las capacidades de I+D nacionales de universidades y organismos de investigación se realizará de forma coordinada con la Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC).

5.5.3. Informe de capacidades de la Industria de ciberseguridad – Oferta

El objetivo de este informe será formalizar la industria de ciberseguridad nacional (productos/soluciones y servicios) y conocer sus capacidades, en particular, en comparación con un conjunto de países de referencia, entre los que podrían encontrarse los siguientes:

- Alemania
- Francia
- Reino Unido
- Estonia
- Israel
- Estados Unidos

El informe deberá segmentar los mercados en base a la taxonomía definida, poniendo especial atención en ámbitos de valor y crecimiento.

5.5.4. Informe del mercado de la ciberseguridad – demanda

El objetivo de este informe es detectar las necesidades del mercado, actuales y futuras, tanto de sectores usuarios de ciberseguridad (Administración Pública, finanzas, transporte, fabricación, servicios de suministro, etc.) como de la propia industria de ciberseguridad (empresas de productos y servicios de ciberseguridad), en particular a necesidades que no estén suficientemente cubiertas por productos nacionales o de estados miembros de la Unión Europea.

Se deberán identificar igualmente los principales retos de ciberseguridad a los que se enfrentan las organizaciones y para los que no existe una solución adecuada.

5.5.5. Mercado de la ciberseguridad

Se incluirá en el informe el nivel de madurez y capacidad de adquisición de tecnología de los usuarios finales nacionales de tecnologías de ciberseguridad. Esta parte del informe se deberá realizar por sectores cuya resiliencia haya que preservar como son sectores relevantes del ámbito económico, de infraestructuras y de servicios, o sectores estratégicos y/o críticos. Un listado posible, sin ser exhaustivo de sectores a cubrir es:

- Financiero
- Transporte y movilidad
- Fabricación
- Servicios de suministro (agua, energía, etc.)
- Comercio
- Salud
- Alimentación
- Logística
- Telecomunicaciones
- Gobierno electrónico
- Servicios profesionales (abogados, notarios, oficinas en general).

5.5.6. Retos

Realizar una prospección tecnológica, tomando como referencia las industrias que en España se consideren prioritarias, y analizar sus retos o necesidades en ciberseguridad no cubiertas actualmente por el mercado.

Se propone segmentar los retos tecnológicos en función del ámbito de aplicación, siguiendo los ámbitos tecnológicos de la taxonomía seleccionada.

5.5.7. Informe de la financiación de la I+D en ciberseguridad

Identificación de programas de financiación de la I+D+i en España (nacionales, regionales y locales) tanto específicos como aquellos con cabida para la ciberseguridad. Adicionalmente establecer una comparativa con dichos programas de iniciativas a nivel EU y otros países siguiendo las recomendaciones descritas en el “Apartado 5.5.3”.

Visualmente podría ilustrarse esta información a modo de mapa geográfico mostrando las zonas con mayor o menor cobertura de financiación de la I+D+i en ciberseguridad.

Adicionalmente se deberían analizar los procesos de inversión (públicos, privados y mixtos) y sus actores en los últimos años y conocer sus motivaciones.

5.6. Fases previstas

Se identifican inicialmente las siguientes fases:

5.6.1. Fase previa

Esta primera fase contempla la elaboración de la A2I incluyendo la generación de sus informes preparatorios. Para ello será preciso la preparación de la licitación, con sus pliegos de descripciones técnicas y cláusulas administrativas, el proceso de validación y aprobación jurídico-económico, así como la publicación en la Plataforma de Contratación del Sector Público. A continuación, el proceso de recepción de ofertas, su valoración, comprobación de solvencias, y por último la **firma del contrato** con la entidad que resulte adjudicataria de este proceso.

5.6.2. Fase preparatoria y documental

Incluye la **investigación de escritorio** en la que se identificará y analiza documentación existente relevante a nivel nacional e internacional relacionada con los objetivos de la A2I y los distintos apartados en los que se espera una contribución.

En esta fase se realiza un **diseño preliminar** de la A2I y se identifican los **informes preparatorios** necesarios para su elaboración, con hipótesis a contrastar con la contribución de las partes interesadas. También se identifican los posibles candidatos a participar en la redacción de este documento y sus estudios preparatorios. Con esta información se puede preparar la recogida de datos por parte de los participantes con la generación de cuestionarios y guiones de entrevista. En paralelo esta fase actualiza la planificación prevista con una visión más realista de entregables, hitos y plazos.

A continuación, se procede a la **presentación oficial** de la iniciativa, en la que se invita formalmente a la participación abierta y colaboración de los participantes.

5.6.3. Fase de recopilación de datos

Se procede a la **toma de datos** en la que se entrevista de una forma guiada a los participantes de forma individual o grupal para recoger de forma completa y sistemática su visión y aportación con respecto a las temáticas a contrastar. La toma de información puede basarse en entrevistas, cuestionarios o reuniones de trabajo siguiendo técnicas como *focus group* o *think tank* u otras relevantes.

5.6.4. Fase de análisis, redacción y consolidación

Su objetivo es realizar un **análisis metodológico completo** de la documentación preparatoria junto con la opinión recabada de los participantes para la redacción

progresiva del texto de los informes preparatorios y de la A2I incluyendo sus conclusiones y recomendaciones.

Esta fase contará con hitos intermedios de validación y revisión por parte del grupo decisor y debe permitir la colaboración y refinamiento por parte de los participantes.

En esta fase se deben contrastar las hipótesis de partida, a la vez que se pueden generar nuevas que requieran de posibles contrastes específicos y puntuales por parte de los participantes. El resultado final de esta fase es un texto objetivo consensuado por todos los participantes. El texto definitivo debe contar con el refrendo específico de los participantes el cual se recomienda se encuentre explicitado en el propio documento final.

5.6.5. Fase de divulgación y difusión

Consensuado y refrendado el texto final de los informes preparatorios y la A2I, se dará comienzo a las principales actividades de esta fase, para dar a conocer el texto final de estos entregables al público objetivo indicado en el "Apartado **5.3.1.**.1" de este documento y al público en general. Los informes preparatorios podrían difundirse a medida que se vayan finalizando por diversos canales, y en el caso de la A2I, se efectuará una **presentación oficial.** Para todos los entregables, se incluirán presentaciones en otros eventos relacionados, adaptando la difusión, en cada caso, al público objetivo. En esta fase, se generarán materiales de difusión que acompañarán a las presentaciones y harán más sencillo asimilar su contenido.

5.7. Metodología

Aunque la metodología concreta a utilizar se definirá en la fase previa, se contempla utilizar al menos las siguientes técnicas:

- **Análisis documental.** Se deberá realizar un análisis profundo de la documentación que le pueda proporcionar INCIBE como input, así como una recopilación y estudio de fuentes secundarias nacionales e internacionales a identificar que puedan contribuir a enriquecer el diagnóstico de los resultados a generar.

- **Entrevistas en profundidad a actores relevantes en el sector.** Se deberá contar con la visión y aportación de actores relevantes en el sector de la ciberseguridad a través de la realización de entrevistas individuales o grupales en profundidad. La relación de participantes a entrevistar, el plan de entrevistas, y en su caso, el guion para las entrevistas semiestructuradas, serán aprobados por INCIBE.

- **Técnicas cuantitativas: realización de encuestas basadas en cuestionario a participantes identificados.**

- **Análisis y consolidación de la información** de partida junto con la contribución de los participantes.

- **Contribución de los participantes en la elaboración de los resultados** para participar en el refinamiento de los resultados y en el refrendo de los textos definitivos.
- **Difusión de los resultados** generados a través de diversos canales.
- **Uso de las herramientas colaborativas y de comunicación** para la orquestación de todas las actividades.

5.8. Cronograma e hitos principales

Las fases e hitos principales se detallan a continuación:

1. **Fase previa**, para la preparación de licitación, publicación, gestión y firma de contrato.
2. **Fase preparatoria**, durante la cual se desarrollará:

   a. Metodología propuesta y recursos disponibles.

   b. Identificación y análisis de documentación existente de referencia.

   c. Definir el diseño y marco analítico para desarrollar la iniciativa.

   d. Mapeado de las entidades de interés (potenciales participantes en el estudio) y creación de un catálogo interactivo de participantes, basado en la lista presentada en el "Apartado 5.3.1".

   e. Estrategia de recogida de datos.

   f. Principio de segmentación del resultado objetivo de cada informe preparatorio y A2I.

   g. Desarrollar documentos, cuestionarios y guiones de entrevista para recabar los datos por parte de los participantes.

   h. Integrar el documento de taxonomía elaborado por el Foro nacional de ciberseguridad.

   i. Al final de esta fase, se presentará un informe de la fase preparatoria.

3. **Fase de recopilación de datos,** durante la cual:

   a. Se elaborará de forma detallada la segmentación del resultado objetivo de cada informe preparatorio y A2I.

   b. Se recogerá y recopilará datos e información relevante utilizando metodologías estándares (informes, estadísticas, opiniones, etc.).

c. Al final de esta fase, se presentarán 2 informes intermedios, como resultado de los trabajos realizados.

4. **Fase de análisis, redacción y consolidación** durante la cual:

   a. Se elaborará un análisis de los datos e información recopilada en la fase anterior, utilizando las herramientas adecuadas.

   b. Se tratará de abordar y responder a todos los objetivos descritos en el "Apartado 5.1".

   c. Se extraerá conclusiones y lecciones aprendidas, así como un análisis pormenorizado de los datos.

   d. Se contrastará con los participantes la redacción y conclusiones que se vayan consolidando.

   e. Una presentación de la A2I, incluyendo un apartado de conclusiones globales basadas en el análisis y las características del sector de la ciberseguridad en España.

   f. Se propondrán recomendaciones (de financiación, regulación, estandarización, comunicación, etc.) que permitan a INCIBE y el grupo decisor proponer futuras tareas y acciones que favorezcan al sector de la ciberseguridad en España.

   g. Durante esta fase, el contratista presentará dos informes finales, como resultado de los trabajos realizados.

5. **Fase de divulgación y difusión,** durante la cual se desarrollarán:

   a. Un plan de difusión contemplando públicos objetivos y las acciones de difusión relacionadas.

   b. Materiales de difusión y presentaciones particularizadas para los diferentes públicos objetivos.

Se muestra a continuación, de forma resumida, una propuesta de cronograma para la realización de los trabajos incluyendo las fases y los hitos principales previstos.

DESCRIPCIÓN	Q1-23	Q2-23	Q3-23	Q4-23
1 FASE PREVIA				
Preparación de licitación				
Contratación				
2 FASE PREPARATORIA Y DOCUMENTAL				
Identificación y análisis de documentación de referencia				
Mapa de entidades de interés y participantes				
Metodología, diseño y marco analítico				
Diseño de segmentación de resultados				
Preparación cuestionarios y entrevistas				
Consolidación de taxonomía de referencia				
Informe fase preparatoria				
3 FASE DE RECOPILACIÓN DE DATOS				
Segmentación de resultados				
Recopilación y consolidación de información				
Informe intermedio 1				
Informe intermedio 2				
4 FASE DE ANÁLISIS, REDACCIÓN Y CONSOLIDACIÓN				
Análisis de datos				
Extracción de conclusiones				
Contraste con los participantes				
Presentación y recomendaciones				
Informe final para revisión				
Informe final para validación				
5 FASE DE DIVULGACIÓN Y DIFUSIÓN				
Plan de difusión				
Materiales y presentaciones				

6. PROMOCIÓN EXTERIOR DE LA INDUSTRIA DE CIBERSEGURIDAD ESPAÑOLA

Tras los primeros trabajos realizados por el grupo de trabajo de impulso a industria de ciberseguridad y a la I+D+i española en esta materia, se propone realizar un **plan estratégico a nivel país** que recopile todas aquellas acciones que se deberían abordar **para una exitosa promoción exterior**, teniendo como ejemplos a países como EE. UU., Israel, Estonia y Corea del Sur. En esta primera iteración, se ha contado con la contribución de ICEX y AMETIC.

Se propone desarrollar los siguientes puntos dentro del Plan Estratégico de Comunicación para la promoción de la industria de ciberseguridad española:

- Creación de una **marca país específica** para la promoción de la ciberseguridad española.
- Realización de una **estrategia de promoción exterior**: objetivos, destinatarios, presupuestos, esquemas de coinversión con el sector privado, KPIs, etc.
- Establecer un **organismo público líder de la iniciativa**, que dirija y decida la ciberseguridad nacional a todos los niveles.
- Desarrollo de un **catálogo de empresas españolas**: clasificado al menos, por tamaño, por especialización tecnológica o de servicios, por localización y por sectores de actividad de sus clientes principales.
- **Colaboración** estrecha dentro de este plan **con organismos internacionales** colaboradores como puedan ser: embajadas, oficinas comerciales de España en el exterior, cámaras de comercio oficiales españolas en el Exterior, comunidades, lobbies, etc...
- **Designación para los tres mercados prioritarios de un interlocutor** específico en la Oficina Comercial de España (Ofecomes), un punto de contacto, que centralice y focalice todas las actividades de promoción y generación de oportunidades comerciales.
- **Coordinación de acciones con foco en ciberseguridad dentro del Plan Cameral de Internacionalización**, que se elabora y ejecuta de acuerdo con el Ministerio de Industria, Comercio y Turismo y consensuado con ICEX. Este Plan contiene actuaciones de interés general en materia de formación, información y promoción dirigidas a promover la internacionalización de las empresas, tales como misiones comerciales, visitas y participaciones en ferias, realizadas por las cámaras de comercio. Además, el Plan incluye misiones comerciales específicas

realizadas por la Cámara de Comercio de España. Asimismo, incluye programas específicos de asesoramiento individualizado a pymes para su salida a mercados exteriores, con especial atención a la innovación, digitalización y posicionamiento exterior como factores claves de la competitividad de las pymes.

- **Creación de un programa de becarios** específicos en ciberseguridad, en una selección de Ofecomes según intereses de mercado, con una II Fase en España, tanto en empresas como en Instituciones/Asociaciones.

- **Formación y cultura de la ciberseguridad en el personal de los organismos internacionales colaboradores** en el plan estratégico, conocedor del ecosistema de ciberseguridad de España.

- Definición de un **plan de atracción de inversiones** específico a través de ***Invest In Spain*.**

De cara a cumplir con los objetivos anteriormente descritos se pueden identificar como acciones concretas dentro del Plan estratégico de comunicación para el impulso de la industria de ciberseguridad fuera de España las siguientes:

- **Encuentros bilaterales**. Por ejemplo, en programas de innovación estatales, en rondas de financiación de Startups, en eventos organizados por organismos públicos.

- Campañas específicas en **grandes eventos internacionales.**

- **Campañas específicas países clave**: EE. UU., Israel, Estonia.

- **Campañas específicas zonas clave**: Europa, América latina y Asia

- Creación de un **programa específico de internacionalización** para empresas del sector de ciberseguridad con apoyo mínimo de 5 años, al estilo de ***ICEX NEXT***: apoyos individualizados en esfuerzos de promoción de marca individual; o bien ***XPande***: Plan de Expansión Internacional de las Pymes de la Cámara de Comercio de España.

- Lanzamiento de **concursos internacionales de ideas** de aplicación a la administración pública española.

Se propone un cronograma de alto nivel para el año 2023

DESCRIPCIÓN	Q1-23	Q2-23	Q3-23	Q4-23
1. Plan detallado de trabajo y acuerdos institucionales				
2. Implementación de acciones				

7. CONCLUSIONES

Los objetivos planteados al comienzo de los trabajos de esta segunda fase del GT2 han sido alcanzados en gran medida. Sin embargo, es obvio que persisten necesidades comunes dentro del ecosistema nacional para alcanzar la misión global del FNCS, especialmente relacionadas con:

- la generación de un marco común en cuanto a una **única taxonomía** que alinee a todos los actores del ecosistema de ciberseguridad nacional y europeos (**MITEC**)
- la protección del tejido productivo nacional, impulsando la adopción de medidas de mejora de la **ciberseguridad por parte de pymes, micropymes y autónomos**
- la generación de actuaciones de I+D+i mediante la **definición de la Agenda de Investigación e Innovación (A2I)** en ciberseguridad
- el **incremento de la oferta y demanda de productos y servicios de ciberseguridad** de la industria española, así como su internacionalización
- **y el incremento el peso de la industria española de ciberseguridad** en el mercado europeo y global.

Es clave **continuar midiendo las capacidades nacionales** de manera constante y continuada, lo que permitirá comprobar que las medidas adoptadas por el Gobierno central y autoridades con competencias en ciberseguridad son efectivas y, si no lo fueran, poder adaptarlas de manera ágil. Del mismo modo la **definición de la cadena de valor** en ciberseguridad y de un **modelo relacional entre la oferta y la demanda** es fundamental para la **generación de nuevas oportunidades** para la industria en base a las prioridades de país para la protección del ciberespacio y de toda la sociedad en global.

En relación con la **taxonomía (MITEC)** y con el principal objetivo de tener un **registro común entre todos los actores de la cadena de valor**, es prioritario finalizar estos trabajos durante el primer trimestre del 2023 para que puedan ser validados por todo el sector y ser utilizados para la definición de la Agenda de investigación e innovación en ciberseguridad (A2I).

Si queremos avanzar como país tenemos que seguir protegiendo al tejido productivo, que son principalmente pymes que, durante estos últimos dos años, han comenzado una digitalización acelerada y que, si bien les permitirá ser mucho más competitivas, también les expone mucho más a los ciberataques. Por eso **es clave la continuidad y la vigilancia de la efectividad de las acciones globales** que se han puesto en marcha durante este 2022 en el ámbito de la **protección, concienciación y formación de este colectivo de PYMES, micropymes y autónomos**.

INCIBE lanzará durante el 2023 un **programa de impulso y fomento a la acreditación de proveedores de las administraciones en el ENS y en la ISO 22.300**. Este programa no solo aumentará el número de proveedores de la administración con este tipo de acreditaciones, sino que también **fomentará y dinamizará la industria que se dedica a la implantación y certificación de estas normativas**. Este programa estará alineado con las acciones descritas en el Plan de Choque de Ciberseguridad aprobado en el Acuerdo de Ministros de mayo de 2021 [29].

El objetivo de crear una Agenda de Investigación e Innovación a nivel nacional es ambicioso, a la par que necesario, y se determina que para que tenga éxito debe contar con una **participación público-privada** suficiente en número de participantes, y representativa de todas las partes interesadas. Adicionalmente, debe prestar especial atención a los cambios en las políticas industriales afines a la ciberseguridad para asegurar la participación e influencia en las mismas. Debe contar con una **gobernanza** igual de participativa, con el liderazgo del INCIBE y la presencia de miembros del Foro con compromiso firme para guiar y dirigir la preparación de la Agenda. También cabe destacar que previo a la redacción de esta A2I, se ve necesario la generación de una colección de **informes preparatorios** que proporcionen información previa específica de diferentes ámbitos tales como capacidades de I+D+i, necesidades de los usuarios finales, capacidad de la industria, oportunidades de mercado y mecanismos de financiación. Con esta información, y con la colaboración de los todos, se podrá concluir con una Agenda debidamente contrastada y refrendada, que en un escenario 2023-2030 fije los objetivos y prioridades en esta materia a nivel nacional.

El **crecimiento** de la industria y su **promoción internacional** no puede ser exitoso sin un **plan global e institucional** en el que participen todos los organismos públicos y asociaciones sectoriales que apoyen la promoción de la industria en el exterior, así como la atracción de inversión extranjera. Acciones concretas a nivel de país deben ser una prioridad para los siguientes 12 meses.

En conclusión, este grupo de trabajo plantea continuar con las acciones descritas en este documento durante el 2023 y podrá incluir nuevas si alguno de los agentes lo considera o si bien recibe una petición expresa del Consejo Nacional de Ciberseguridad.

8. REFERENCIAS

[1] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future_es

[2] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_es

[3]https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/digital-europe-programme_es

[4] https://commission.europa.eu/strategy-and-policy/recovery-plan-europe_es

[5] https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

[6] https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019

[7] https://espanadigital.gob.es/

[8] https://planderecuperacion.gob.es/

[9]https://industria.gob.es/es-es/Documents/Directrices%20Generales%20de%20la%20Pol%C3%ADtica%20industrial%20espa%C3%B1ola%2025.02.19%20FINAL.pdf

[10] https://www.ciencia.gob.es/Estrategias-y-Planes/Estrategias/Estrategia-Espanola-de-Ciencia-Tecnologia-e-Innovacion-2021-2027.html;jsessionid=9462AFB00463E8B7EAE488B3FAA97A9F.2

[11] https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional-2017

[12] https://www.dsn.gob.es/es/documento/estrategia-nacional-contra-crimen-organizado-delincuencia-grave

[13] https://foronacionalciberseguridad.es/

[14] https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio-2019/Febrero/Noticia-2019-02-18-El-Gobierno-aprueba-creacion-Centro-de-Operaciones-de-Ciberseguridad-para-AGE.html

[15] https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2518-ccn-stic-140-taxonomia-de-referencia-para-productos-de-seguridad-tic/file.html

[16] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191

[17] https://www.incibe.es/industria-cpi/cpi-primera-convocatoria

[18] https://www.incibe.es/industria-cpi/cpi-segunda-convocatoria

[19] https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion/file.html

[20] https://foronacionalciberseguridad.es/index.php/publicaciones

[21] https://ecs-org.eu/

[22] https://cybercompetencenetwork.eu/

[23] https://www.renic.es/es

[24] https://web.archive.org/web/20220319210957/https:/www.ecs-org.eu/documents/publications/59e615c9dd8f1.pdf

[25] https://www.enisa.europa.eu/publications/priorities-for-eu-research/at_download/fullReport

[26] https://www.sparta.eu/assets/deliverables/SPARTA-D3.2-Updated-SPARTA-SRIA-roadmap-v1-PU-M12.pdf

[27] https://cybersecurity-atlas.ec.europa.eu/

[28] https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security/eu-security-market-study_en

[29] Plan de choque de Ciberseguridad https://portal.mineco.gob.es/es-es/comunicacion/Paginas/210525_np_ciberseguridad.aspx).".

[30] ECSO Market Radar Taxonomy. Recuperado de https://ecs-org.eu/documents/uploads/ecso-cybersecurity-market-radar-taxonomy-table.pdf

[31] A proposal for a European Cybersecurity Taxonomy. Joint Research Centre (2019). Recuperado de https://ec.europa.eu/jrc/en/publication/proposal-european-cybersecurity-taxonomy

ANEXO I – ACTUALIZACIÓN DE KPIs. PROGRAMAS DE DIGITALIZACIÓN DE LAS PYMES

Ciberseguridad en las Pymes
Situación diciembre 2022

Juan Miguel Cuéllar del Río
Subdirector de Competitividad
Cámara de Comercio de España

1. **Programa Ciberseguridad de la Cámara de Comercio de España**
2. **Oficinas Acelera Pyme - Cámaras de Comercio**
3. **Programa Kit Digital**

1. **Programa Ciberseguridad de la Cámara de Comercio de España**

1. Programa Ciberseguridad

El uso SEGURO Y FIABLE del ciberespacio, protegiendo los derechos y las libertades de los ciudadanos y promoviendo el progreso socio económico.

Objetivos **Estratégicos**

1 Que haya más **EMPLEADOS SENSIBILIZADOS** a través de sus empleadores mediante **planes de sensibilización**. Cuantas más empresas pongan en marcha planes de sensibilización, habrá más potenciales empleados sensibilizados en ciberseguridad que apliquen medidas de seguridad.

2 **MEJORAR LA SEGURIDAD DE LOS SERVICIOS DE LAS EMPRESAS EN EL CIBERESPACIO**
- Fomentar que las empresas dispongan de un **plan de seguridad** como una fuente para generar confianza: más empresas/clientes harán negocios con ellas (B2B y B2C), confiarán más en ellas.
- Fomentar que las empresas cuiden de la seguridad de su web, en particular si disponen de tienda online y utilizan formas de pago online.

3 Promover la implantación de **HERRAMIENTAS DE CIBERSEGURIDAD** en el día a día de las empresas y sus operaciones y gestiones más habituales.

4 Fomentar que las empresas tengan un plan de **CONTINGENCIA Y CONTINUIDAD.**

1. Programa Ciberseguridad

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

Objetivo III

Protección del ecosistema empresarial y social y de los ciudadanos.

Líneas de acción

- Impulsar la **ciberseguridad en las pymes**, micropymes y autónomos mediante la articulación de políticas públicas en ciberseguridad, y especialmente con actuaciones dirigidas al fomento de la resiliencia.
- Impulsar en el sector empresarial la **implantación de estándares** reconocidos de ciberseguridad.

Objetivo IV

Cultura y compromiso con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas.

Líneas de acción

- Incrementar las **campañas de concienciación** a ciudadanos y empresas, y poner a su disposición información útil adaptada a cada perfil, especialmente en el ámbito de los autónomos, pequeñas y medianas empresas.
- Promover la **difusión de la cultura de la ciberseguridad** como una buena práctica empresarial.
- **Concienciar a directivos de organizaciones**, a los efectos de que habiliten los recursos necesarios y promuevan los proyectos de ciberseguridad que sus entidades puedan necesitar.

1. Programa Ciberseguridad

Ciberseguridad

Programa de ayudas *que capacite a las pymes a prevenir los principales* **riesgos en Ciberseguridad**, *asumibles por ellas mismas, para garantizar que los Sistemas de Información y Telecomunicaciones que utilizan, poseen un adecuado nivel de Ciberseguridad.*

Fase I Plan Director

- Situación de partida y recomendaciones genéricas
- Estrategia de la organización
- Proyectos recomendados

Fase II Implantación

- Implantación de herramientas de seguridad
- Seguimiento de la implantación
- Ayuda a la Inversión

Acciones de sensibilización Ciberseguridad

Fase I

Análisis exhaustivo de los Sistemas de Información y Telecomunicaciones de la empresa para identificar los principales **riesgos referidos a la ciberseguridad**.

- Sin coste para la empresa.
- Realizado por los técnicos de las Cámaras.
- Cofinanciado por FEDER y **otro cofinanciador público.**

Fase II

La empresa recibe una **subvención** para la implantación de herramientas de ciberseguridad. Se realizará un seguimiento del ritmo de ejecución y de la adecuación de los proyectos de implantación.

- Gasto máximo cofinanciable: 4.000 €.
- Ayuda de entre un 40% y un 85%, según la CCAA.
- Cofinanciado por FEDER y la empresa.

1. Programa Ciberseguridad

Fase I: Asesoramiento

Diagnóstico individualizado para establecer recomendaciones y priorizar acciones y proyectos a implantar, en materia de ciberseguridad.

1. Programa Ciberseguridad

Fase de Ayudas

Catálogo de herramientas y soluciones tipo específicas de ciberseguridad

Herramientas de Seguridad - Ejemplos gastos elegibles:

- Gestión de la identidad y contraseñas
- Protección en el puesto de trabajo
- Detección y eliminación de malware
- Seguridad en aplicaciones y datos
- Gestión de parches y vulnerabilidades
- Seguridad en las redes
- Redes Privadas Virtuales
- Antivirus, cortafuegos, ransomware
- Adaptación a la RGPD

1. Programa Ciberseguridad

Empresas Participantes

	2020	2021	2022	Total
Beneficiarias Directas	212	279	483 (compromiso)	974
Soluciones Implantadas	349	516	662 (diciembre 2022)	1.527
Jornadas Sensibilización	39	15	10 (diciembre 2022)	64
Empresas Sensibilizadas	1.402	717	560 (estimado 2022)	2.679

1. Programa Ciberseguridad

Tamaño de las Empresas

	2020	2021	2022	Total
0 – 2 Empleados	26,42 %	31,18 %	34,62 %	31,64 %
3 – 9 Empleados	35,38 %	27,60 %	34,62 %	32,64 %
>= 10 Empleados	38,21 %	41,22 %	30,77 %	35,72 %

1. Programa Ciberseguridad

Nivel de Madurez en Ciberseguridad

		0 a 2	3 a 9	10 o más	Total
Nivel 1 (Incipiente)	La ciberseguridad de la empresa depende de los conocimientos de los empleados, no existiendo protocolos internos que establezcan la forma de actuar	88,15 %	84,07 %	69,75 %	80,15 %
Nivel 2 (Emergente)	La empresa ha establecido una serie de medidas informales con el objetivo de salvaguardar la estructura informática, no existe un plan para la formación de los trabajadores en materia de ciberseguridad	10,45 %	14,92 %	27,78 %	18,08 %
Nivel 3 (Avanzado)	La empresa ha documentado un procedimiento de actuación en materia de ciberseguridad, además de ofrecer formación a los trabajadores en esta materia	1,39 %	1,02 %	2,47 %	1,76 %

1. Programa Ciberseguridad

Nivel de Madurez en Ciberseguridad

	Incipiente	Emergente	Avanzado
Seguridad de los Equipos y Recursos Humanos	81,26 %	16,76 %	1,98 %
Medidas de Protección	73,32 %	24,48 %	2,21 %
Seguridad de las Operaciones y Comunicaciones	80,04 %	17,86 %	2,09 %
Adopción de Aspectos Normativos y Regulatorios	43,33 %	37,38 %	19,29 %

1. Programa Ciberseguridad

Proyectos Implantados

1.527 Proyectos de Ciberseguridad implantados.

Proyectos	Total	%
Copias de Seguridad	190	12,44 %
Adaptación a la RGPD	172	11,26 %
Auditoría Técnica de Seguridad.	167	10,94 %
Antimalware	155	10,15 %
Firewall (hardware)	149	9,76 %
Auditoría Página Web y Cumplimiento LSSI-CE	137	8,97 %
Sistema de Alimentación Ininterrumpida (SAI)	109	7,14 %
Red VPN (Accesos remotos seguros)	97	6,35 %
Análisis de Vulnerabilidades	95	6,22 %
Seguridad de Correo Electrónico	63	4,13 %

1. Programa Ciberseguridad

Proyectos Implantados

1.527 Proyectos de Ciberseguridad implantados.

Proyectos	Total	%
Obtención Certificación ISO 27001.	47	3,08 %
Autenticación Multifactor	30	1,96 %
Gestión centralizada de dispositivos	23	1,51 %
Plan de Contingencia y Continuidad	23	1,51 %
Encriptación de datos	19	1,24 %
Sistema de Control de Acceso	14	0,92 %
Sistema de Centralización de Certificados	11	0,72 %
Plataforma de Monitorización de Redes	10	0,65 %
Sistema SIEM (Información de seguridad y gestión de eventos)	8	0,52 %
Control de Aplicaciones (Whitelisting)	8	0,52 %

1. Programa Ciberseguridad

Próximos Pasos

- Actualización del diagnóstico personalizado, en función de la explotación de los datos de ejecución del propio programa y de la definición de la matriz de categorización de pymes.
- Actualización y ampliación de los proyectos subvencionables.
- Continuar y potenciar la sensibilización a las empresas en materia de ciberseguridad.

2. Oficinas Acelera Pyme - Cámaras de Comercio

2. Oficinas Acelera Pyme – Cámaras de Comercio

Ayudar a las **EMPRESAS** a ser más **COMPETITIVAS** en sus procesos de negocio/producción, productos o servicios utilizando **TECNOLOGÍAS DIGITALES**

Objetivos **Estratégicos**

1. **DAR CUMPLIMIENTO** a las prioridades nacionales y regionales en materia de transformación digital.
2. **APOYAR A LAS PYMES EN SU PROCESO DE DIGITALIZACIÓN.**
3. **FOMENTAR LA INNOVACIÓN, LA CREACIÓN DE EMPLEO y el EMPRENDIMIENTO DIGITAL** fortaleciendo así la competitividad.
4. **DIFUNDIR Y SENSIBILIZAR** en el uso de las tecnologías.
5. **BRINDAR INFORMACIÓN SOBRE APOYO FINANCIERO** a las pymes en la demanda para dominar la transformación digital.
6. **FOMENTAR LAS RELACIONES ENTRE LOS DISTINTOS AGENTES DEL ECOSISTEMA,** facilitando un punto de encuentro y compartiendo mejores prácticas.

2. Oficinas Acelera Pyme – Cámaras de Comercio

Actividades

Asesoramiento y Atención personalizada

- Resolución de dudas respecto a procesos de transformación digital de la pyme.
- Ilustración de las oportunidades que la digitalización puede crear para las pymes y cómo éstas pueden implementarse con éxito en la práctica.
- Apoyo específico en el diseño y la implementación de una estrategia de digitalización.
- Acceso a instalaciones y servicios para experimentación en el desarrollo de productos o soluciones.
- Información sobre ayudas de las distintas Administraciones Públicas o privadas para promover o hacer uso de tecnologías digitales innovadoras.
- Fomento de las relaciones entre los distintos agentes del ecosistema, facilitando un punto de encuentro, así como la conexión entre oferta y demanda y compartiendo mejores prácticas.

2. Oficinas Acelera Pyme – Cámaras de Comercio

Actividades

Acciones de Sensibilización

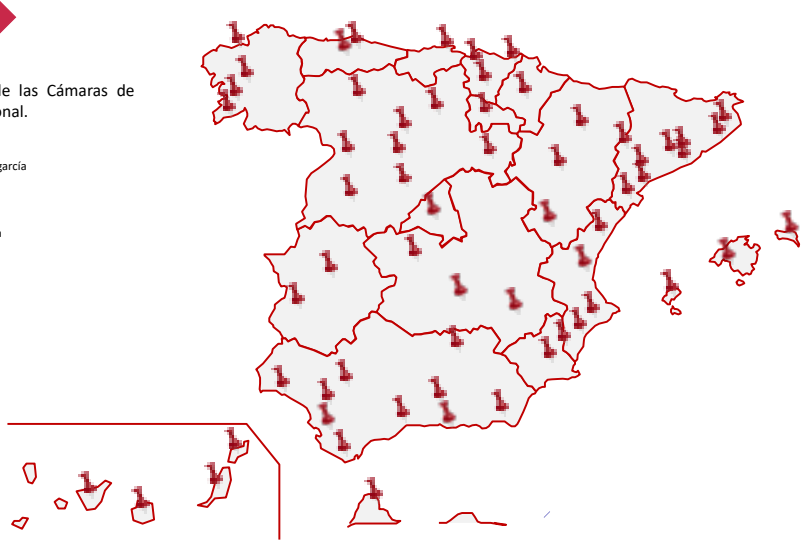
- Labores de difusión y sensibilización, incluyendo la generación, difusión y puesta en valor de contenidos, sobre las ventajas de la incorporación de las Tecnologías de la Información y las Comunicaciones (TIC) en los procesos de negocio, para optimizar su funcionamiento, de modo que se favorezca la demanda de tecnologías innovadoras que contribuyan a la mejora de su productividad.
- Establecimiento de Centros Demostradores de Tecnología para la incorporación de las nuevas tecnologías en las empresas.
- Capacitación sobre tecnologías digitales.
- Otras actividades de promoción del uso de las TIC para la mejora competitiva de las empresas.

2. Oficinas Acelera Pyme – Cámaras de Comercio

Distribución de las Oficinas Acelera Pyme

Hay un total de 62 Oficinas Acelera Pyme de las Cámaras de Comercio, repartidas por todo el territorio nacional.

A Coruña	Gran Canaria	Pontevedra, Vigo y Vilagarcía
Álava	Granada	Sabadell
Albacete	Huelva	Salamanca
Alcoy	Huesca	Sant Feliu de Gíxols
Alicante	Ibiza y Formentera	Santiago de Compostela
Almería	Jerez de la Frontera	Segovia
Badajoz	La Rioja	Sevilla
Barcelona	Lanzarote	Soria
Bilbao	León	Tarragona
Burgos	Linares	Tenerife
Cáceres	Lleida	Terrasa
Cádiz	Madrid	Teruel
Campo de Gibraltar	Málaga	Toledo
Cantabria	Mallorca	Tortosa
Castellón	Menorca	Tui
Ceuta	Motril	Valencia
Ciudad Real	Murcia	Valladolid
Fuerteventura	Navarra	Valls
Gijón	Orihuela	Zamora
Gipuzkoa	Oviedo	Zaragoza
Girona	Palencia	



2. Oficinas Acelera Pyme – Cámaras de Comercio

Actividad en Ciberseguridad

	2021	2022	Total
N.º Oficinas Cámaras	39	(39) + 23	62
Asesoramientos Personalizados	3.523	12.482	16.025
Asesoramientos en Ciberseguridad	71 (2%)	87 (0,70%)	158 (0,59%)
Jornadas Realizadas	444	1.217	1.661
Jornadas sobre Ciberseguridad	31 (6,98%)	76 (6,24%)	107 (6,44%)
Empresas sensibilizadas	12.155	22.614	34.769
Empresas sensibilizadas en Ciberseguridad	551 (4,53%)	1.947 (8,61%)	2.498 (7,18%)

2. Oficinas Acelera Pyme – Cámaras de Comercio

Próximos Pasos

- Formación específica en ciberseguridad para los técnicos de las Oficinas Acelera Pyme de las Cámaras de Comercio.
- Aprovechar el potencial de las Oficinas Acelera Pyme de las Cámaras de Comercio para:
  - Continuar y potenciar la sensibilización a las empresas en materia de ciberseguridad.
  - Plan de Comunicación para realizar sensibilización en ciberseguridad y fomentar el asesoramiento en ciberseguridad por parte de las Oficinas Acelera Pyme.

3. Programa Kit Digital

3. Programa Kit Digital

Marco del Programa

El programa Kit Digital **está financiado por los fondos Next Generation de la Unión Europea,** creados para hacer frente a los desafíos planteados por la pandemia de la COVID-19 y construir la Europa de la nueva generación. En concreto, se materializa a través del **Mecanismo de Recuperación y Resiliencia (MRR) y React-UE.**

El **Plan de Recuperación, Transformación y Resiliencia** se construye sobre la base de 4 ejes transversales, 10 políticas palanca y 30 Componentes divididos en una gran variedad de Reformas e Inversiones.

El **programa Kit Digital**, en concreto, se encuadra bajo el **Componente 13 Inversión 3,** dedicado al impulso a las PYME. Así mismo, contribuye a actuaciones del **Componente 15 y Componente 19.**

3. Programa Kit Digital

Objetivo

El **programa Kit Digital**, **nace para apoyar la transformación digital de pequeñas empresas, microempresas y personas en situación de autoempleo**, con el **objetivo de subvencionar la adopción de soluciones de digitalización disponibles en el mercado,** lo que facilitará un progreso significativo en sus niveles de madurez digital**.**

Estas soluciones permitirán a las empresas **avanzar en la digitalización de áreas clave** como *presencia en internet, venta electrónica, gestión de clientes y proveedores, oficina digital, gestión y automatización de procesos* y *ciberseguridad.*

OBJETIVO

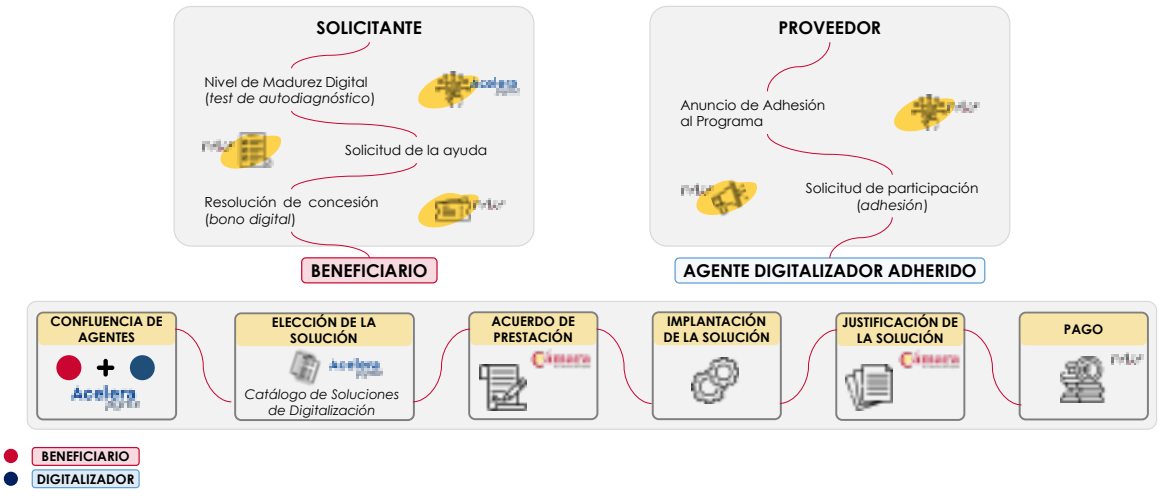
Dar cobertura a **1.000.000 de PYME y/o personas en situación de autoempleo.**

AYUDAS

Por valor de **3.067 millones de euros**, en el periodo 2021-2024.

3. Programa Kit Digital

Esquema general del Programa



3. Programa Kit Digital

Beneficiarios

Pequeñas empresas, microempresas y personas en situación de autoempleo.

Cuyo domicilio fiscal esté ubicado en territorio español.

Independientemente de su sector o tipología de negocio.

		IMPORTE POR BONO
SEGMENTO I	Pequeñas empresas de entre 10 y menos de 50 empleados	12.000 €
SEGMENTO II	Pequeñas empresas o Microempresas de entre 3 y menos de 10 empleados	6.000 €
SEGMENTO III	Pequeñas empresas o Microempresas de entre 0 y menos de 3 empleados	2.000 €

3. Programa Kit Digital

Categorías de Soluciones de Digitalización

El **bono digital** se podrá consumir en la **adquisición e implantación de soluciones de digitalización de las diferentes Categorías** disponibles en la plataforma Acelera Pyme y ofertadas por los Agentes Digitalizadores Adheridos. Estas Categorías de Soluciones de Digitalización, que **son extensibles a todos los sectores de actividades**, son las siguientes:

1. **SITIO WEB Y PRESENCIA EN INTERNET**
   Expansión de la presencia en internet por la creación de una web
2. **COMERCIO ELECTRÓNICO**
   Creación de una tienda online de compraventa con medios digitales
3. **GESTIÓN DE REDES SOCIALES**
   Promoción del beneficiario en redes sociales
4. **GESTIÓN DE CLIENTES**
   Digitalización y optimización de la gestión de relaciones comerciales
5. **BI Y ANALÍTICA**
   Explotación de datos para mejorar la toma de decisiones
6. **GESTIÓN DE PROCESOS**
   Automatización de procesos de negocio del beneficiario
7. **FACTURA ELECTRÓNICA**
   Digitalización de la emisión de facturas entre beneficiario y clientes
8. **SERVICIOS DE OFICINA VIRTUAL**
   Implantación de soluciones que permitan una colaboración eficiente
9. **COMUNICACIONES SEGURAS**
   Provisión de conexiones seguras entre los dispositivos del beneficiario
10. **CIBERSEGURIDAD**
    Seguridad básica y avanzada para los dispositivos del beneficiario

3. Programa Kit Digital

Funcionalidades y Servicios

Comunicaciones Seguras

- **SSL:** la solución deberá utilizar un protocolo de capa de sockets seguros, para crear una conexión segura y cifrada**.**
- **Cifrado extremo a extremo:** la solución deberá mantener las comunicaciones cifradas en todo su recorrido, con el objetivo de prevenir ataques.
- **Logs de conexión:** la solución deberá mantener un registro de los dispositivos que se han conectado a la red privada de la pyme.
- **Control de acceso:** la solución deberá permitir la conexión a la red privada de la pyme única y exclusivamente a los dispositivos autorizados por la empresa.
- **Dispositivos móviles:** la solución deberá estar disponible para su uso desde dispositivos móviles.
- **Configuración inicial y actualizaciones de seguridad:** se debe realizar una configuración inicial para su correcto uso, con las respectivas actualizaciones de firmas de *malware* y otros datos para detección de amenazas además de las actualizaciones de software de seguridad periódicas requeridas.

3. Programa Kit Digital

Funcionalidades y Servicios

Ciberseguridad

- ***Antimalware*:** la solución deberá proporcionar una herramienta que analice el dispositivo, su memoria interna y los dispositivos de almacenamiento externos**.**
- ***Antispyware*:** la solución deberá proporcionar una herramienta que detecte y evite el malware espía.
- **Correo seguro:** la solución deberá proporcionar herramientas de análisis del correo electrónico con las siguientes características: *Antispam*, con detección y filtro de correo no deseado; *Antiphishing*, con detección de correos con enlaces o malware que se sospecha sirvan para robar credenciales.
- **Navegación segura:** control de contenidos; *Antiadware* para evitar anuncios maliciosos.
- **Análisis y detección de amenazas:** la solución deberá permitir conocer el comportamiento de las amenazas conocidas y nuevas.
- **Monitorización de la red:** la solución deberá proporcionar herramientas que analicen el tráfico de red y alerten de amenazas.
- **Configuración inicial y actualizaciones de seguridad:** se debe realizar una configuración inicial para su correcto uso, con las respectivas actualizaciones de firmas de *malware* y otros datos para detección de amenazas además de las actualizaciones de software de seguridad periódicas requeridas.
- **Requisitos especiales de formación:** la formación impartida al beneficiario deberá incluir una tutorización para la configuración del software de seguridad, así como incluir un kit de concienciación en ciberseguridad para complementar la solución con habilidades de *firewall* humano.

3. Programa Kit Digital

Implantación de Soluciones de Ciberseguridad

Penetración de las categorías de soluciones de ciberseguridad en el programa. Porcentaje y número de Acuerdos de Prestación de Soluciones de Digitalización, correspondientes a las categorías de ciberseguridad, frente al total de Acuerdos (datos a 11.12.2022):

Número de empleados	Segmento I (10 – 49)	Segmento II (3 – 9)	Segmento III (0 – 2)	Total
Comunicaciones Seguras	4,13 % (2.114)	1,65 % (117)	0,50 % (1)	3,82 % (2.232)
Ciberseguridad	8,84 % (4.518)	4,98 % (353)	0,50 % (1)	8,34 % (4.872)

3. Programa Kit Digital

Próximos Pasos

- Plan de Comunicación para realizar sensibilización en ciberseguridad y fomentar la implantación de las categorías de solución de ciberseguridad y comunicaciones seguras.

ANEXO II- TAXONOMÍA DE COMPETENCIAS EN LA INDUSTRIA (ECSO)

En este Anexo I se detalla la taxonomía de capacidades definida por ECSO [30] que se utiliza principalmente por los actores de la Industria. Está constituida por 5 funciones, 21 categorías y 60 subcategorías.

Seguidamente se proporciona la lista de las 60 subcategorías agrupadas por las cinco funciones principales de la seguridad definidas en el marco de ciberseguridad NIST [30]: *Identify, Protect, Detect, Respond & Recover*.

INDUSTRIA - TAXONOMIA ECSO - QUÉ			
ID	FUNCIÓN	CATEGORÍA	SUBCATEGORÍA
1	IDENTIFY	Asset Management	Software & Security Lifecycle Management
2	IDENTIFY	Asset Management	IT Service Management
3	IDENTIFY	Business Environment	Business Impact Analysis
4	IDENTIFY	Governance & Risk Management	Security Certification
5	IDENTIFY	Governance & Risk Management	Governance, Risk & Compliance (GRC)
6	IDENTIFY	Risk Assessment	Risk Management solutions & services
7	IDENTIFY	Rissk Management Strategy	Risk Management Strategy Development & Consulting
8	IDENTIFY	Supply Chain Risk Management	Supply chain risk monitoring solutions & services

INDUSTRIA - TAXONOMIA ECSO - QUÉ			
ID	FUNCIÓN	CATEGORÍA	SUBCATEGORÍA
9	PROTECT	Identity Management & Access Control	Access Management
10	PROTECT	Identity Management & Access Control	Authentication
11	PROTECT	Identity Management & Access Control	Authorisation
12	PROTECT	Identity Management & Access Control	Identity Management
13	PROTECT	Awareness and Training	Awareness Trainings
14	PROTECT	Awareness and Training	Cyber Ranges
15	PROTECT	Data Security	PKI / Digital Certificates
16	PROTECT	Data Security	Data Leakage Prevention
17	PROTECT	Data Security	Encryption
18	PROTECT	Data Security	Cloud Access Security Brokers
19	PROTECT	Data Security	Hardware Security Modules (HSM)
20	PROTECT	Data Security	Digital Signature
21	PROTECT	Information Protection Processes and Procedures	Application Security
22	PROTECT	Information Protection Processes and Procedures	Static Application Security Testing (SAST)
23	PROTECT	Maintenance	Patch Management
24	PROTECT	Maintenance	Vulnerability Management
25	PROTECT	Maintenance	Penetration Testing / Red Teaming
26	PROTECT	Protective Technology	Wireless Security
27	PROTECT	Protective Technology	Remote Access / VPN
28	PROTECT	Protective Technology	IoT Security
29	PROTECT	Protective Technology	PC/Mobile/End Point Security
30	PROTECT	Protective Technology	Mobile Security /Device management
31	PROTECT	Protective Technology	Sandboxing
32	PROTECT	Protective Technology	Content Filtering & Monitoring
33	PROTECT	Protective Technology	Firewalls / NextGen Firewalls
34	PROTECT	Protective Technology	Unified Threat Management (UTM)
35	PROTECT	Protective Technology	Anti Spam
36	PROTECT	Protective Technology	Anti Virus/Worm/Malware
37	PROTECT	Protective Technology	Backup / Storage Security

INDUSTRIA - TAXONOMIA ECSO - QUÉ			
ID	FUNCIÓN	CATEGORÍA	SUBCATEGORÍA
38	DETECT	Anomalies and Events	Fraud Management
39	DETECT	Anomalies and Events	Intrusion Detection
40	DETECT	Security Continuous Monitoring	SIEM / Event Correlation Solutions
41	DETECT	Security Continuous Monitoring	Cyber Threat Intelligence
42	DETECT	Security Continuous Monitoring	Security Operations Center (SOC)
43	DETECT	Detection Processes	Underground/Darkweb investigation
44	DETECT	Detection Processes	Honeypots / Cybertraps
45	DETECT	Detection Processes	Social Media & Brand Monitoring

INDUSTRIA - TAXONOMIA ECSO - QUÉ			
ID	FUNCIÓN	CATEGORÍA	SUBCATEGORÍA
46	RESPOND	Planing Response	Incident Management
47	RESPOND	Planing Response	Crisis Management
48	RESPOND	Communication	Crisis Communication
49	RESPOND	Analysis	Fraud Investigation
50	RESPOND	Analysis	Forensics
51	RESPOND	Mitigation	Cyber Security Insurance
52	RESPOND	Mitigation	DDoS protection
53	RESPOND	Mitigation	Data Recovery
54	RESPOND	Mitigation	Incident Response Services (CSRIT aaS)
55	RESPOND	Mitigation	Takedown Services
56	RESPOND	Improvements	Containment support

INDUSTRIA - TAXONOMIA ECSO - QUÉ			
ID	FUNCIÓN	CATEGORÍA	SUBCATEGORÍA
57	RECOVER	Recover y Planning	System Recovery
58	RECOVER	Recover y Planning	Business Continuity/ Recovery Planning
59	RECOVER	Improvements	Post Incident reviews & consulting
60	RECOVER	Communication	Communications coaching & consulting

ANEXO III - TAXONOMÍA DE COMPETENCIAS EN LA INVESTIGACIÓN (JRC)

En este Anexo II se detalla la taxonomía de capacidades definida por la Comisión Europea, *Joint Research Comitee* (JRC) [31], que se utiliza principalmente por los actores de la Investigación. Es una taxonomía basada en tres dimensiones:

- Dominios de Investigación, constituida por 15 categorías y 149 subcategorías.
- Tecnologías y Casos de Uso, constituida por 23 casos de uso.
- Sectores, constituida por 15 sectores.

Seguidamente, se proporciona una lista de las 149 subcategorías agrupadas en las 15 categorías.

Esta taxonomía está actualmente en revisión.

INVESTIGACIÓN - TAXONOMIA JRC - DOMINIOS - QUÉ		
ID	**CATEGORIA**	**SUBCATEGORIA**
1	Assurance Audit and Certification	Assurance;
2		Audit;
3		Assessment;
4		Certification;
5	Cryptology (Cryptography & Cryptoanalisys)	Asymmetric cryptography;
6		Symmetric cryptography;
7		Cryptanalysis methodologies, techniques and tools;
8		Functional encryption;
9		Mathematical foundations of cryptography;
10		Crypto material management (e.g. key management, PKI);
11		Secure multi-party computation;
12		Random number generation;
13		Digital signatures;
14		Hash functions;
15		Message authentication;
16		Quantum cryptography;
17		Post-quantum cryptography;
18		Homomorphic encryption
19		Privacy requirements for data management systems;

INVESTIGACIÓN - TAXONOMIA JRC - DOMINIOS - QUÉ		
ID	CATEGORIA	SUBCATEGORIA
20	Data Security and Privacy	Design, implementation, and operation of data management systems that include security and privacy functions;
21		Anonymity, pseudonymity, unlinkability, undetectability, or unobservability30;
22		Data integrity;
23		Privacy Enhancing Technologies (PET);
24		Digital Rights Management (DRM);
25		Risk analysis and attacks with respect to de-anonymization or data re-identification (e.g. inference attack);
26		Eavesdropping techniques (e.g. via electromagnetic radiation, visual observation of blinking LEDs, acoustic via keyboard typing noise);
27		Data usage control.
28	Educational and Training	Higher Education;
29		Professional training;
30		Cybersecurity-aware culture (e.g. including children education);
31		Cyber ranges, Capture the Flag, exercises, simulation platforms, educational/training tools, cybersecurity awareness;
32		Education methodology;
33		Vocational training.
34	Human Aspects	Accessibility;
35		Usability;
36		Human-related risks/threats (social engineering, insider misuse, etc.)
37		Socio-technical security;
38		Enhancing risk perception;
39		Psychological models and cognitive processes; Forensic cyberpsychology;
40		User acceptance of security policies and technologies;
41		Automating security functionality;
42		Non-intrusive security;
43		Privacy concerns, behaviours, and practices;
44		Computer ethics and security;
45		Transparent security;
46		Cybersecurity profiling;
47		Cyberpsychology;
48		Security visualization;
49		Gamification;
50		Human aspects of trust;
51		Human perception of cybersecurity;
52		History of cybersecurity.

INVESTIGACIÓN - TAXONOMIA JRC - DOMINIOS - QUÉ		
ID	CATEGORIA	SUBCATEGORIA
53	Identity Management	Identity and attribute management models, frameworks, applications, technologies, and tools (e.g. PKI, RFID, SSO, attribute-based credentials, federated IdM etc.);
54		Protocols and frameworks for authentication, authorization, and rights management;
55		Privacy and identity management (e.g. privacy-preserving authentication);
56		Identity management quality assurance;
57		Optical and electronic document security;
58		Legal aspects of identity management;
59		Biometric methods, technologies and tools.
60	Incident Handling and Digital Forensics	Incident analysis, communication, documentation, forecasting (intelligence based), response, and reporting;
61		Theories, techniques and tools for the identification, collection, attribution, acquisition, analysis and preservation of digital evidence (e.g. code authorship and attacker identification, provenance assurance, digital evidence correlation, digital evidence triage);
62		Vulnerability analysis and response;
63		Digital forensic processes and workflow models;
64		Digital forensic case studies;
65		Policy issues related to digital forensics;
66		Resilience aspects;
67		Anti-forensics and malware analytics;
68		Citizen cooperation and reporting;
69		Coordination and information sharing in the context of cross-border/organizational incidents.
70	Legal Aspects	Cybercrime prosecution and law enforcement;
71		Intellectual property rights;
72		Cybersecurity regulation analysis and design;
73		Investigations of computer crime (cybercrime) and security violations;
74		Legal and societal issues in information security (e.g. identity management, digital forensics, cybersecurity litigation).

INVESTIGACIÓN - TAXONOMIA JRC - DOMINIOS - QUÉ		
ID	CATEGORIA	SUBCATEGORIA
75	Network and Distributed Systems	Network security (principles, methods, protocols, algorithms and technologies);
76		Distributed systems security;
77		Managerial, procedural and technical aspects of network security;
78		Requirements for network security;
79		Protocols and frameworks for secure distributed computing;
80		Network layer attacks and mitigation techniques;
81		Network attack propagation analysis;
82		Distributed systems security analysis and simulation;
83		Distributed consensus techniques;
84		Fault tolerant models;
85		Secure distributed computations;
86		Network interoperability;
87		Secure system interconnection;
88		Privacy-friendly communication architectures and services (e.g. Mix-networks, broadcast protocols, and anonymous communication);
89		Network steganography.
90	Security Management and Governance	Risk management, including modelling, assessment, analysis and mitigations;
91		Modelling of cross-sectoral interdependencies and cascading effects
92		Threats and vulnerabilities modelling
93		Attack modelling, techniques, and countermeasures (e.g. adversary machine learning)
94		Managerial aspects concerning information security
95		ssment of information security effectiveness and degrees of control
96		Identification of the impact of hardware and software changes on the management of Information Security
97		Standards for Information Security;
98		Governance aspects of incident management, disaster recovery, business continuity
99		Techniques to ensure business continuity/disaster recovery
100		Compliance with information security and privacy policies, procedures, and regulations
101		Economic aspects of the cybersecurity ecosystem
102		Privacy impact assessment and risk management
103		Processes and procedures to ensure device end-of-life security and privacy (e.g. IT waste management and recycling);
104		Capability maturity models (e.g. assessment of capacities and capabilities).
105	Security Measurements	Security analytics and visualization;
106		Security metrics, key performance indicators, and benchmarks;
107		Validation and comparison frameworks for security metrics;
108		Measurement and assessment of security levels

INVESTIGACIÓN - TAXONOMIA JRC - DOMINIOS - QUÉ		
ID	CATEGORIA	SUBCATEGORIA
109	Software and Hardware Security Engineering	Security requirements engineering with emphasis on identity, privacy, accountability, and trust;
110		Security and risk analysis of components compositions;
111		Secure software architectures and design (security by design);
112		Security design patterns;
113		Secure programming principles and best practices;
114		Security support in programming environments;
115		Security documentation;
116		Refinement and verification of security management policy models;
117		Runtime security verification and enforcement;
118		Security testing and validation;
119		Vulnerability discovery and penetration testing;
120		Quantitative security for assurance;
121		Intrusion detection and honeypots;
122		Malware analysis including adversarial learning of malware;
123		Model-driven security and domain-specific modelling languages;
124		Self-* including self-healing, self-protecting, self-configuration systems;
125		Attack techniques (e.g. side channel attacks, power attacks, stealth attacks, advanced persistent attacks, rowhammer attacks);
126		Fault injection testing and analysis;
127		Cybersecurity and cyber-safety co-engineering;
128		Privacy by design.
129	Steganography, Steganalysus and Watermarking	Steganography;
130		Steganalysis;
131		Digital watermarking

INVESTIGACIÓN - TAXONOMIA JRC - DOMINIOS - QUÉ		
ID	**CATEGORIA**	**SUBCATEGORIA**
132	Theoretical Foundations	Formal specification of various aspects of security (e.g properties, threat models, etc.);
133		Formal specification, analysis, and verification of software and hardware;
134		Information flow modelling and its application to confidentiality policies, composition of systems, and covert channel analysis;
135		New theoretically-based techniques for the formal analysis and design of cryptographic protocols and their applications;
136		Formal verification of security assurance;
137		Cybersecurity uncertainty models;
138		Cybersecurity concepts, definitions, ontologies, taxonomies, foundational aspects
139	Trust Management and Accountability	Semantics and models for security, accountability, privacy, and trust;
140		Trust management architectures, mechanisms and policies;
141		Trust and privacy;
142		Identity and trust management;
143		Trust in securing digital as well as physical assets;
144		Trust in decision making algorithms;
145		Trust and reputation of social and mainstream media;
146		Social aspects of trust;
147		Reputation models;
148		Trusted computing;
149		Algorithmic auditability and accountability (e.g. explainable AI).

Como se ha comentado, en la segunda dimensión de la taxonomía JRC se detallan las 23 tecnologías y casos de uso aplicables para la clasificación de las capacidades.

USER CASES - JRC	
ID	**SUBCATEGORÍA**
1	Artificial Intelligence & Big Data Analytics
2	Big Data
3	Blockchain and Distributed Ledger Technology (DLT)
4	Cloud, Edge and Virtualization
5	Critical Infrastructures Protection (CIP)
6	Protection of public spaces
7	Disaster resilience and crisis management
8	Fight against crime and terrorism
9	Border and external security
10	Local/wide area observation and surveillance
11	Hardware technology (RFID, Networking, etc.)
12	High-Performance Computing (HPC)
13	Human Machine Interface (HMI)
14	Industrial IoT and Control Systems (e.g. SCADA & CPS)
15	Information Systems
16	Internet of Things, Embedded Systems, Pervasive Systems
17	Mobile Devices
18	Operating Systems
19	Quantum Technologies (e.g. Computing & communication)
20	Robotics
21	Satellite systems and applications
22	Vehicular Systems (e.g. autonomous vehicles)
23	UAV (unmanned aerial vehicles)

ANEXO IV – EJEMPLO DE TAXONOMÍA INTEGRADA GENERADA EN EL SGT2

Actualmente, se cuenta con una propuesta de taxonomía generada en el grupo de trabajo SGT2 del FNCS, que integra las taxonomías de ECSO [30] y del JRC [31], generando una taxonomía hibrida que partiendo de la taxonomía de ECSO permite mapear cada categoría de ECSO (60) con varias de las del JRC (149).

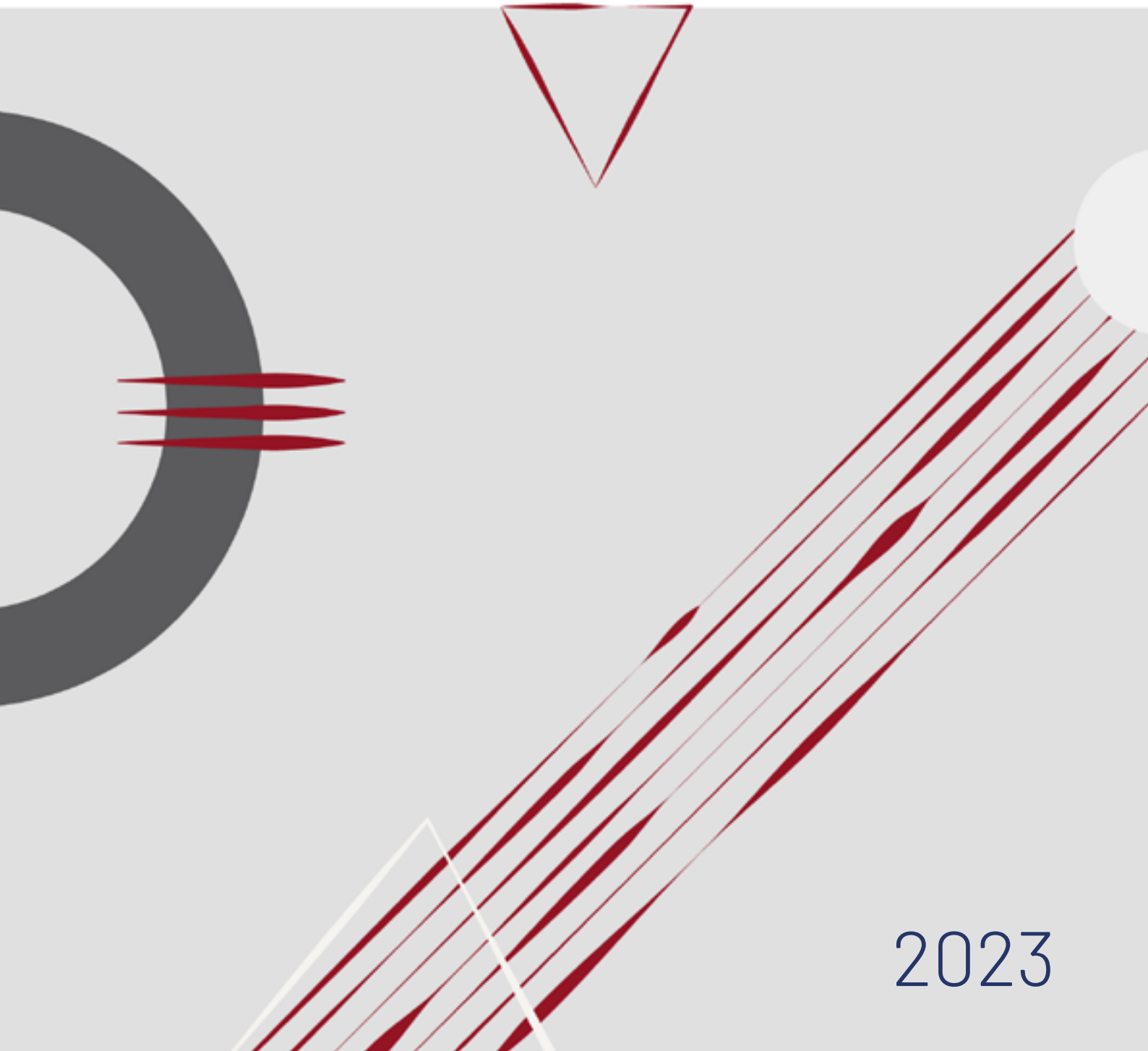
Se proporciona a modo de ejemplo una parte de la taxonomía integrada.

Esta taxonomía está siendo actualmente revisada en el marco del SGT2.

TAXONOMIA ECSO				TAXONOMIA JRC			
ID	FUNCIÓN	CATEGORÍA	SUBCATEGORÍA	JRC - 1	TAXONOMIA JRC - PRIMARIO	JRC-2	TAXONOMÍA JRC - SECUNDARIO
1	IDENTIFY	Asset Management	Software & Security Lifecycle Management	103, 109, 111, 112, 113, 114, 123, 124, 127, 128	Processes and procedures to ensure device end-of-life security and privacy (e.g. IT waste management and recycling);Security requirements engineering with emphasis on identity, privacy, accountability, and trust; Secure software architectures and design (security by design); Security design patterns; Secure programming principles and best practices; Security support in programming environments; Model-driven security and domain-specific modelling languages; Self-* including self-healing, self-protecting, self-configuration systems; Cybersecurity and cyber-safety co-engineering; Privacy by design.	115, 116, 117, 133	Security documentation; Refinement and verification of security management policy models; Security testing and validation; Formal specification, analysis, and verification of software and hardware;
2	IDENTIFY	Asset Management	IT Service Management	94, 134	Managerial aspects concerning information security; Information flow modelling and its application to confidentiality policies, composition of systems, and covert channel analysis;		
3	IDENTIFY	Business Environment	Business Impact Analysis	72, 74, 101, 102, 137	Cybersecurity regulation analysis and design; Legal and societal issues in information security (e.g. identity management, digital forensics, cybersecurity litigation); Economic aspects of the cybersecurity ecosystem; Privacy impact assessment and risk management; Cybersecurity uncertainty models;		
4	IDENTIFY	Governance & Risk Management	Governance, Risk & Compliance (GRC)	1, 24, 40, 43, 44, 97, 106, 107, 108, 115, 116, 120, 138, 139, 140, 146	Assurance; Digital Rights Management (DRM); User acceptance of security policies and technologies; Privacy concerns, behaviours, and practices; Computer ethics and security; Standards for Information Security; Security metrics, key performance indicators, and benchmarks; Validation and comparison frameworks for security metrics; Measurement and assessment of security levels; Security documentation; Refinement and verification of security management policy models; Cybersecurity concepts, definitions, ontologies, taxonomies, foundational aspects; Quantitative security for assurance; Semantics and models for security, accountability, privacy, and trust; Semantics and models for security, accountability, privacy, and trust; Trust management architectures, mechanisms and policies; Social aspects of trust;		Techniques to ensure business continuity/disaster recovery, 99; Compliance with information security and privacy policies, procedures, and regulations, 100;
5	IDENTIFY	Governance & Risk Management	Security Certification	2, 3, 4, 65, 100, 132, 136	Audit; Assesment; Certification; Policy issues related to digital forensics; Compliance with information security and privacy policies, procedures, and regulations; Formal specification of various aspects of security (e.g properties, threat models, etc.); Formal verification of security assurance;		
6	IDENTIFY	N/A	Supply Chain Risk Assessment				
7	IDENTIFY	N/A	Risk Management Strategy	38, 90, 91, 92, 93, 96	Enhancing risk perception; Risk management, including modelling, assessment, analysis and mitigations; Modelling of cross-sectoral interdependencies and cascading effects; Threats and vulnerabilities modelling; Attack modelling, techniques, and countermeasures (e.g. adversary machine learning); Identification of the impact of hardware and software changes on the management of Information Security	102	Privacy impact assessment and risk management;
8	IDENTIFY	N/A	Risk Assessment	25, 26, 95, 104, 110	Risk analysis and attacks with respect to de-anonymization or data re-identification (e.g. inference attack); Eavesdropping techniques (e.g. via electromagnetic radiation, visual observation of blinking LEDs, acoustic via keyboard typing noise); Assment of information security effectiveness and degrees of control; Capability maturity models (e.g. assessment of capacities and capabilities); Security and risk analysis of components compositions;	90, 91, 92, 93, 96	Risk management, including modelling, assessment, analysis and mitigations; Modelling of cross-sectoral interdependencies and cascading effects; Threats and vulnerabilities modelling; Attack modelling, techniques, and countermeasures (e.g. adversary machine learning); Identification of the impact of hardware and software changes on the management of Information Security

FORO NACIONAL DE CIBERSEGURIDAD

MARCO DE COMPETENCIAS PARA PROGRAMAS SUPERIORES DE FORMACIÓN ESPECIALIZADA EN CIBERSEGURIDAD



2023

Coordinadores sociedad civil:

Víctor A. Villagrá (CRUE Universidades Españolas)

Marta Beltrán Pardo (CRUE Universidades Españolas)

Coordinador institucional:

Pablo López (Centro Criptológico Nacional)

Autores y colaboradores:

Cristina Alcaraz Tello

Eduardo Fernández-Medina Patón

Ana Fernández-Vilas

Lorena González Manzano

Jesús Lizárraga

Gabriel Maciá Fernández

Iván Marsá Maestre

José Javier Martínez Herráiz

Elena Matilla Rodríguez

Helena Rifà Pous

Ricardo Rodríguez Fernández

Francisco J. Sampalo Lainz

Antonio Skármeta

Índice

Acrónimos y terminología

00

/// **ACM**	Association for Computing Machinery
/// **AIS**	Association for Information Systems
/// **CC**	Computing Curriculum
/// **CE**	Computer Engineering
/// **CS**	Computer Society
/// **CS**	Computer Science
/// **CSEC**	CiberSecurity
/// **DS**	Data Science
/// **EDSIG /ISCAP**	Education Special Interest Group of Information Systems and Computing Academic Professionals
/// **GSOC**	Global Security Operations Centers
/// **IaaS**	Identity as a Service
/// **IDS**	Intrusion Detection Systems
/// **IEEE**	Institute of Electrical and Electronics Engineers
/// **IETF**	Internet Engineering Task Force
/// **IPS**	Intrusion Prevention Systems
/// **IS**	Information Systems
/// **IT**	Information Technology
/// **SE**	Software Engineering
/// **SIGCHI**	Special Interest Group for Computer Human Interaction
/// **TIC**	Tecnologías de la información y la comunicación
/// **UE**	Unión Europea
/// **VPN**	Virtual Private Networks

Objeto

01

Este documento tiene como objeto definir un marco de competencias que sirva como referencia para el diseño de programas superiores de formación especializada en ciberseguridad en España. Estas competencias podrán ser de dos tipos:

· **Competencias específicas**, relacionadas con el área de la ciberseguridad, que deben ser tratadas en programas de formación específicos.

· **Competencias básicas/generales**, que no son específicas del área de la ciberseguridad (pueden ser comunes con títulos de otras disciplinas), pero que se consideran especialmente importantes dentro de esta área.

También se identificarán conocimientos que se pueden considerar como pre-requisitos de acceso para adentrarnos en programas superiores específicos en ciberseguridad (por ejemplo, post-grados) o que permitan definir competencias específicas relacionadas con el área de la ciberseguridad, pero en un nivel básico o fundamental (por ejemplo, en los primeros cursos de títulos de grado).

Por ello, este documento se estructura de la siguiente forma:

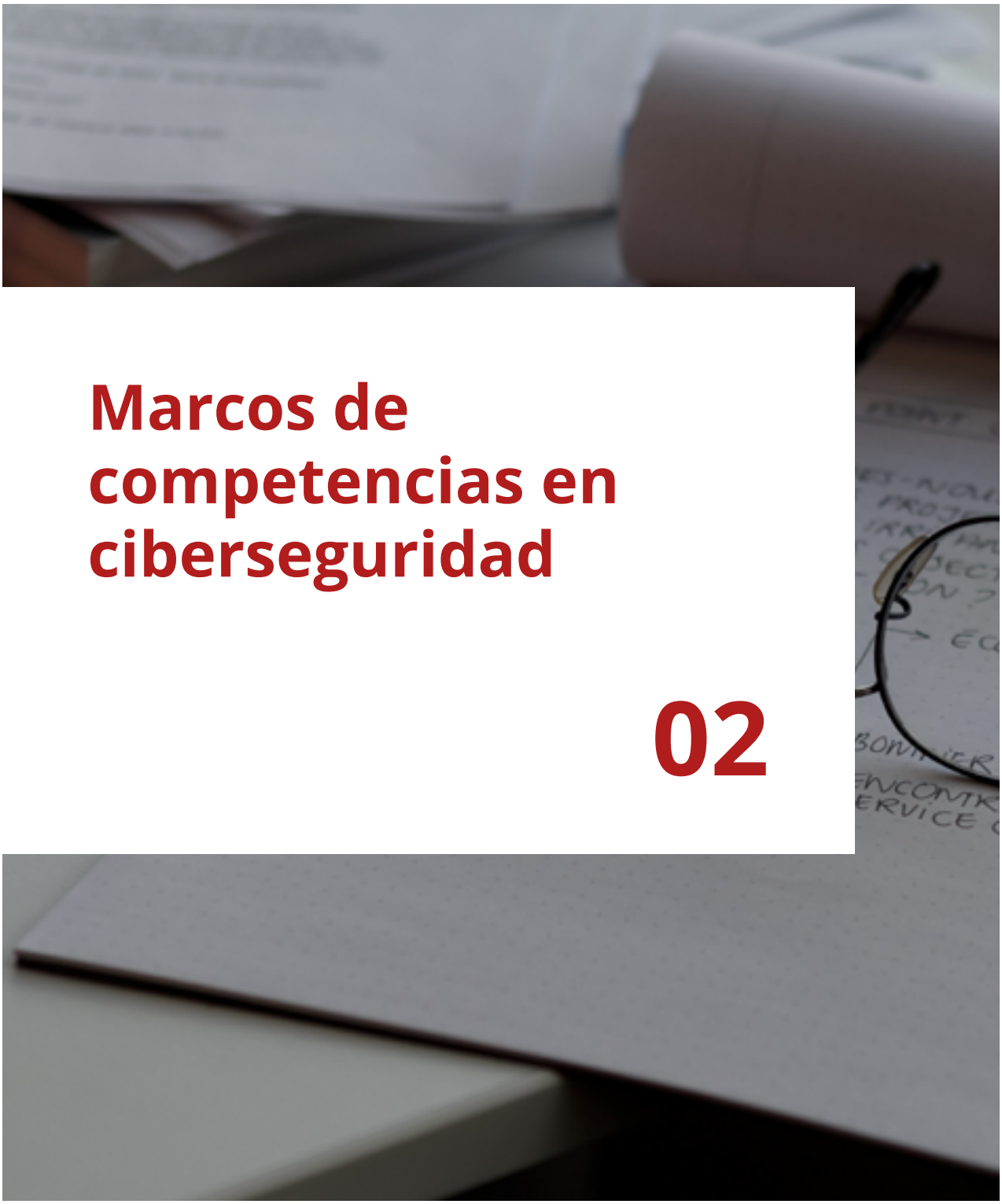
· La sección 2 identifica y analiza los marcos de competencias en ciberseguridad existentes en la actualidad en el ámbito internacional, que pueden ser tomados como base para la identificación de competencias que se pretende realizar.

· La sección 3 expone en detalle el marco curricular ACM/IEEE en ciberseguridad, que ha sido identificado como el más apropiado para realizar un análisis de los programas superiores actuales.

· La sección 4 estudia el soporte del marco curricular ACM/IEEE en ciberseguridad por parte de una muestra significativa de los programas de formación superior en España, que permita obtener un punto de partida para la definición de competencias específicas necesarias. Este punto de partida no es más que un análisis de la oferta actual de títulos universitarios.

· La sección 5 propone el marco de competencias objeto del presente documento distinguiendo entre competencias específicas, básicas o generales y pre-requisitos.

· Por último, la sección 6 discute cómo emplear el marco de competencias propuesto durante el diseño de nuevos planes de estudios universitarios.



Marcos de competencias en ciberseguridad

02

La necesidad de estructurar, organizar y secuenciar las competencias de un "experto en ciberseguridad" lleva ocupando a profesionales de la ciberseguridad y de la docencia desde hace décadas [H2008]. A lo largo de todos estos años, diferentes organismos académicos y profesionales han propuesto marcos referenciales con los que estructurar el conocimiento en ciberseguridad (lo que en inglés se conoce como cybersecurity frameworks). Estas iniciativas permiten informar sobre el diseño de actividades y programas formativos en ciberseguridad, así como evaluar los existentes (como ejemplo de una evaluación sobre la formación en diseño seguro en Europa, puede consultarse [DLMS2021]). En esta sección, ofrecemos una breve panorámica de iniciativas existentes en esta línea, para después centrarnos en el marco que hemos seleccionado como base para nuestro estudio.

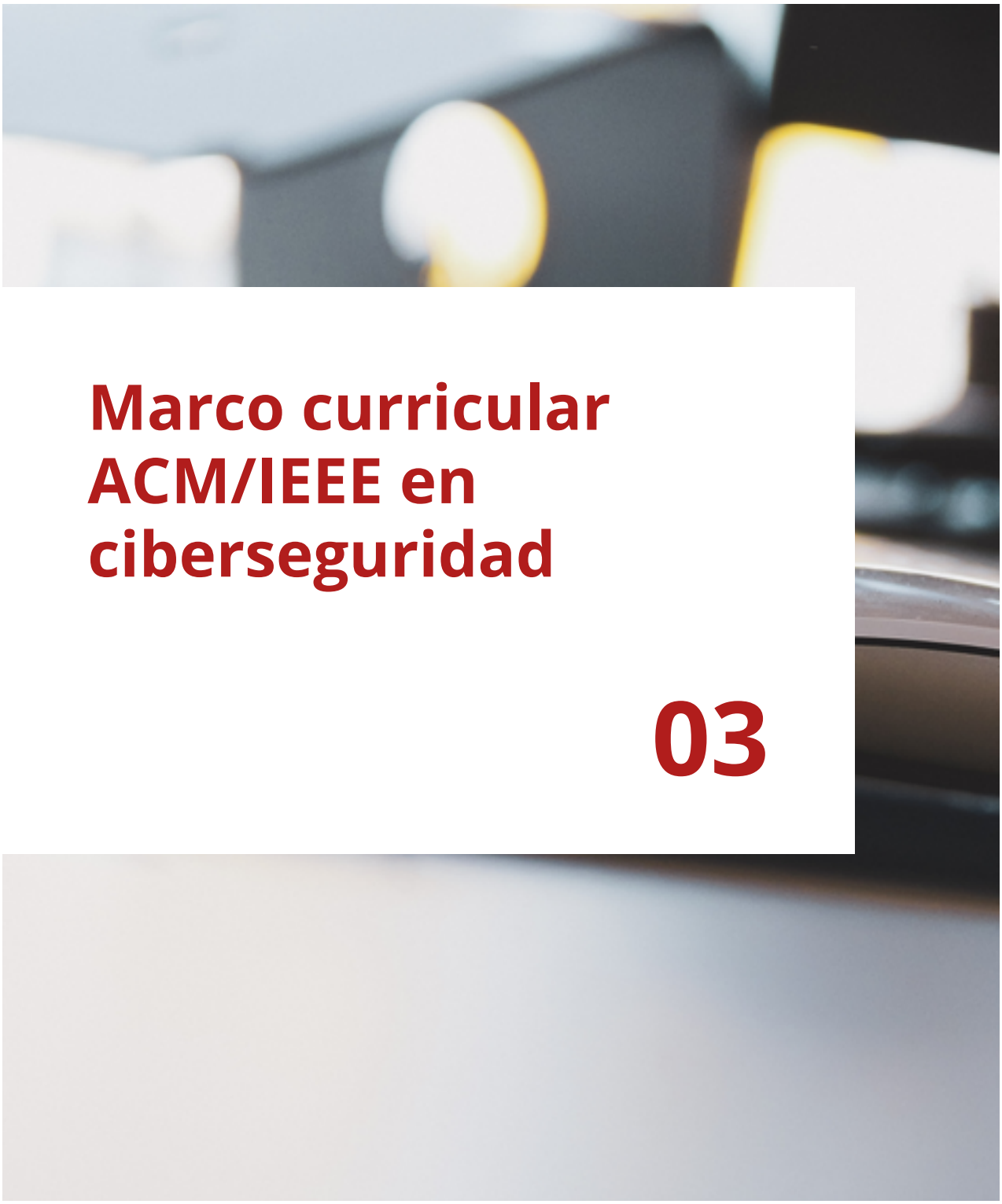
Uno de los marcos referenciales más utilizados es el de NICE (National Initiative for Cybersecurity Education). NICE es un esfuerzo conjunto del gobierno estadounidense junto con instituciones académicas y del sector privado para fortalecer las capacidades formativas en ciberseguridad de los Estados Unidos. Dentro de esa iniciativa se crea el marco referencial CWF (Cybersecurity Workforce Framework), que pretende servir de ayuda a las organizaciones para identificar, reclutar, desarrollar y retener el talento en ciberseguridad [NICE2017]. Su enfoque es mayoritariamente funcional, agrupando las funciones de ciberseguridad en 7 categorías y 32 áreas de especialización. Dentro de este marco define un total de 52 puestos de trabajo (work roles), para cada uno de los cuales especifica un conjunto de tareas (tasks), conocimientos (knowledge), habilidades (skills) y capacidades (abilities). Se trata de un mapeo sumamente exhaustivo que permite definir la especificidad de un puesto de trabajo de forma altamente granular.

También en los Estados Unidos, aunque con un enfoque diferente surge CyBOK (Cyber Security Body of Knowledge) [CYBOK2018]. CyBOK es una iniciativa del NCSC (National Cyber Security Centre) con el objetivo de categorizar y clasificar el conocimiento científico existente en la disciplina. Para ello, define cinco categorías de amplio espectro en torno a las cuales agrupa 19 áreas de conocimiento (Knowledge Áreas, KAs). Dentro de esas áreas define hasta 244 temas (topics). Aquí no vemos roles de trabajo, habilidades o capacidades, puesto que el enfoque es más científico que profesional.

En Europa, también desde un enfoque científico, surge la taxonomía de ciberseguridad del JRC (Joint Research Centre) [JRC2019], con el objetivo de proporcionar un conjunto de categorías de alto nivel que sirvan de referencia para las actividades en ciberseguridad y para la catalogación de entidades de investigación en ciberseguridad de Europa. La taxonomía propone 15 dimensiones sectoriales, 15 dominios de ciberseguridad (con un total de 150 subdominios) y 23 dimensiones tecnológicas y casos de uso.

Dentro del proyecto europeo SPARTA (Strategic Programs for Advanced Research and Technology in Europe) se desarrolla también un marco referencial de habilidades en ciberseguridad, SPARTA CSF (Cybersecurity Skill Framework) [SPARTA2020], que se apoya en los esfuerzos previos de NICE y del JRE. El CSF de SPARTA mantiene las mismas categorías y áreas de especialización de NICE, así como la gran mayoría de las definiciones de puestos de trabajo (work roles), si bien introduce como roles nuevos el Responsable de Protección de Datos (Data Protection Officer) y el Responsable de Ciberseguridad (Cyber Security Officer), que capturan las particularidades de la legislación europea y de la de algunos estados miembro.

Finalmente, la Association for Computing Machinery (ACM), en colaboración con la IEEE Computer Society (IEEE-CS) y otros organismos, creó a finales de 2017 el Cybersecurity Curricula [CC2020], especialmente orientado al diseño de planes educativos en ciberseguridad. Por su enfoque claramente alineado con los intereses de este estudio, la taxonomía de ACM ha sido la que finalmente hemos adaptado, por lo que la describimos en mayor detalle a continuación.



Marco curricular ACM/IEEE en ciberseguridad

03

El Marco curricular de Association for Computing Machinery (ACM)/ Institute of Electrical and Electronics Engineers (IEEE) en materia de ciberseguridad se encuentra enmarcado dentro del proyecto Computing Curriculum 2020 (CC2020) [CC2020], el cual corresponde a una iniciativa lanzada recientemente por ACM e IEEE Computer Society (IEEE-CS) junto con otras sociedades, como, por ejemplo: Association for Information Systems (AIS) y el Education Special Interest Group of Information Systems and Computing Academic Professionals (EDSIG/ISCAP), y el ACM Special Interest Group for Computer Human Interaction (SIGCHI). El proyecto CC2020 se centra en mostrar el estado actual de las directrices curriculares de los programas académicos en informática y el futuro de las enseñanzas curriculares de informática en los próximos años.

Dentro del CC2020, se identifican hasta siete disciplinas distintas dentro del campo de la informática cuyos modelos curriculares son:

1. Computer Engineering (CE)
2. Computer Science (CS)
3. Information Systems (IS)
4. Information Technology (IT)
5. Software Engineering (SE)
6. CiberSecurity (CSEC)
7. Data Science (DS)
8. Otras disciplinas emergentes

Figura 1. Relación de disciplinas por área de aplicación y tecnología [CC2020]

De este conjunto hay que destacar el modelo curricular de CSEC definido por ACM/IEEE en 2017 [CS2017], que según el CC2020 guarda una especial vinculación con el resto de disciplinas tal como se muestra en la Figura 1. Esta figura caracteriza las relaciones entre disciplinas de acuerdo a las tecnologías implicadas y las áreas/dominios de aplicación (ej. seguridad, transformación digital e inteligencia, o plataforma TIC -Tecnologías de la Información- y la Comunicación) e infraestructura.

3.1. Modelo CSEC 2017

El modelo CSEC aborda los contenidos de la disciplina de ciberseguridad de acuerdo a tres dimensiones específicas:

1. Área de conocimiento, conocido como Knowledge Areas (KAs), la cual establece la estructura básica de organización para el contenido de ciberseguridad. En concreto, cada KA define un conjunto de unidades de conocimiento, donde cada unidad específica temas, y cada tema establece resultados de aprendizaje esperados.

En CSEC 2017 se identifican hasta 8 áreas de conocimiento:
· **KA-1**: seguridad de los datos (Data Security),
· **KA-2**: seguridad del software (Software Security),
· **KA-3**: seguridad de los componentes (Component Security),
· **KA-4**: seguridad de las conexiones (Connection Security),
· **KA-5**: seguridad del sistema (System Security),
· **KA-6**: seguridad del ser humano (Human Security),
· **KA-7**: seguridad de la organización (Organizational Security), y
· **KA-8**: seguridad de la sociedad (Societal Security).

Las cinco primeras (dato, software, componente, conexión y sistema), representan generalmente los contenidos más técnicos, mientras que el resto describen las dimensiones humanas, organizativas y sociales.

Dentro de una KA se puede identificar los contenidos esenciales, los cuales abordan las "competencias básicas de ciberseguridad" que todo estudiante debe superar. Los conceptos esenciales deben introducirse desde el inicio y reforzarse a lo largo de todo el programa de ciberseguridad hasta alcanzar los resultados de aprendizaje esperados.

2. Conceptos transversales (CT), que establecen las conexiones y las relaciones entre las KAs, y hay seis conceptos transversales:
· **CT-1**: confidencialidad,
· **CT-2**: integridad,
· **CT-3**: disponibilidad,
· **CT-4**: riesgo,
· **CT-5**: pensamiento adversarial, y
· **CT-6**: pensamiento sistémico/defensivo.

3. Lente disciplinaria, la cual representa la disciplina informática esencial/base a partir de la cual se asientan o se desarrollan los contenidos de ciberseguridad.

3.2. Áreas de Conocimiento en Ciberseguridad

Teniendo en cuenta el modelo de CSEC descrito en la sección anterior y las ocho áreas de conocimiento, esta sección detalla los contenidos curriculares específicos recomendados por el ACM/IEEE.

KA-1: Seguridad del dato	
Se centra en la protección de los datos (almacenados, procesados o en tránsito), y requiere como conocimiento previo la aplicación de algoritmos matemáticos y analíticos para su completa implementación.	Contenidos esenciales: • Conceptos básicos de criptografía • Forense digital • Comunicaciones seguras de extremo a extremo • Integridad y autenticación de los datos • Seguridad del almacenamiento de la información

Unidades de conocimiento	Temas
Criptografía	- Conceptos básicos de criptografía - Conceptos avanzados - Antecedentes matemáticos - Cifras históricas - Cifras simétricas (de clave privada) - Cifrados asimétricos (de clave pública)
Análisis forense digital	- Introducción de la definición y los límites y tipos de herramientas - Cuestiones legales - Herramientas forenses digitales - Proceso de investigación - Adquisición y conservación de pruebas - Análisis de las pruebas - Presentación de resultados - Autenticación de las pruebas - Presentación de informes, respuesta y gestión de incidentes - Análisis forense móvil
Integridad y autenticación de datos	- Fuerza de autenticación - Técnicas de ataque a las contraseñas - Técnicas de almacenamiento de contraseñas - Integridad de los datos
Control de acceso	- Seguridad física de los datos - Control de acceso a los datos lógicos - Diseño de arquitecturas seguras - Técnicas de prevención de fugas de datos

Protocolos de comunicación seguros	- Protocolos de la capa de aplicación y transporte - Ataques a TLS - Capa de Internet/Red - Protocolos de preservación de la privacidad - Capa de enlace de datos
Criptoanálisis	- Ataques clásicos - Ataques de canal lateral - Ataques contra cifrados de clave privada - Ataques contra cifradores de clave pública - Algoritmos para resolver el problema del logaritmo discreto - Ataques a RSA
Privacidad de datos	- Panorama general (definiciones, aspectos legales, recopilación de datos, agregación de datos, difusión de datos, invasión de la privacidad, ingeniería social y redes sociales)
Seguridad del almacenamiento de la información	- Encriptación de discos y archivos - Borrado de datos - Enmascaramiento de datos - Seguridad de las bases de datos - Ley de seguridad de los datos

KA-2: Seguridad del software	
Se centra en el desarrollo y la utilización de programas informáticos que preserven de forma fiable las propiedades de seguridad de la información y los sistemas que éstos aplican.	Contenidos esenciales: • Principios fundamentales de diseño, incluyendo el mínimo privilegio, el diseño abierto y la abstracción • Requisitos de seguridad y su rol en el diseño • Cuestiones de implementación • Pruebas/testing estáticas y dinámicas • Configuración y aplicación de parches • Ética, especialmente en el desarrollo, las pruebas y la divulgación de vulnerabilidades
Unidades de conocimiento	**Temas**
Principios fundamentales	- Mínimo privilegio - Fallo seguro (por defecto) - Mediación completa - Separación de privilegios - Minimizar la superficie de confianza - Economía de mecanismo - Minimización de la implementación (mecanismo menos común) - Mínima sorpresa (aceptación psicológica) - Diseño abierto - Diseño por capas (defensa en profundidad) - Abstracción - Modularidad - Vinculación completa - Diseño para la iteración
Diseño	- Derivación de los requisitos de seguridad - Especificación de los requisitos de seguridad - Ciclo de vida del desarrollo del software / ciclo de vida del desarrollo de la seguridad - Lenguajes de programación y de tipo seguro
Implementación	- Validación de la entrada y comprobación de su representación - Utilización correcta de las API - Uso de las funciones de seguridad - Comprobación de las relaciones de tiempo y estado - Manejar adecuadamente las excepciones y los errores - Programación robusta - Encapsular estructuras y módulos - Tener en cuenta el entorno
Análisis y pruebas	- Análisis estático y dinámico - Pruebas unitarias - Pruebas de integración - Pruebas de software

Despliegue y mantenimiento	- Configuración - Parcheado y ciclo de vida de la vulnerabilidad - Comprobación del entorno - DevOps - Desmantelamiento/retirada
Documentación	- Documentos de instalación - Guías y manuales de usuario - Documentación de aseguramiento/garantía - Documentación sobre seguridad
Ética	- Cuestiones éticas en el desarrollo de software - Aspectos sociales del desarrollo de software - Aspectos legales del desarrollo de software - Revelación de vulnerabilidades - Qué, cuándo y por qué probar

KA-3: Seguridad de los componentes	
Se centra en el ciclo de vida de los componentes, desde el diseño, la adquisición, las pruebas, el análisis hasta el mantenimiento de componentes integrados en sistemas.	Contenidos esenciales: • Vulnerabilidades de los componentes del sistema • Ciclo de vida de los componentes • Principios de diseño de componentes seguros • Seguridad en la gestión de la cadena de suministro • Pruebas de seguridad • Ingeniería inversa
Unidades de conocimiento	**Temas**
Diseño de componentes	- Seguridad en el diseño de componentes - Principios de diseño seguro de componentes - Identificación de componentes - Técnicas de ingeniería inversa - Mitigación de ataques de canal lateral - Tecnologías antimanipulación
Adquisición de componentes	- Riesgos de la cadena de suministro - Seguridad de la cadena de suministro - Investigación de proveedores
Pruebas de componentes	- Principios de las pruebas unitarias - Pruebas de seguridad
Ingeniería inversa de componentes	- Ingeniería inversa del diseño - Ingeniería inversa del hardware - Ingeniería inversa del software

KA-4: Seguridad de las conexiones	
Se centra en la seguridad de las conexiones establecidas entre componentes, incluyendo las conexiones físicas y lógicas.	Contenidos esenciales: • Sistemas, arquitectura, modelos y normas • Interfaces de componentes físicos • Interfaces de componentes de software • Ataques de conexión • Ataques de transmisión
Unidades de conocimiento	**Temas**
Medios físicos	- Transmisión en un medio - Medios compartidos y punto a punto - Modelos de compartición - Tecnologías comunes
Interfaces físicas y conectores	- Características y materiales del hardware - Estándares - Conectores comunes
Arquitectura de hardware	- Arquitecturas estándar - Estándares de interfaz de hardware - Arquitecturas comunes
Arquitectura de sistemas distribuidos	- Conceptos generales - Web global - Internet, protocolos y estratificación - Computación de alto rendimiento (superordenadores) - Hipervisores e implementaciones de computación en la nube - Vulnerabilidades y ejemplos de explotaciones
Arquitectura de red	- Conceptos generales - Arquitecturas comunes - Reenvío / enrutamiento - Conmutación/recuperación - Tendencias emergentes - Virtualización y arquitectura de hipervisor virtual
Implementación de redes	- Redes IEEE 802/ISO - Redes IETF y TCP/IP - Integración práctica y protocolos de cola - Vulnerabilidades y ejemplos de explotaciones.
Servicios de red	- Concepto de servicio - Modelos de servicio (cliente-servidor, peer-to-peer) - Conceptos de protocolo de servicio (IPC, API, IDL) - Arquitecturas comunes de comunicación de servicios - Virtualización de servicios - Vulnerabilidades y ejemplos de explotaciones

Defensa de la red	- Endurecimiento de la red - Implantación de IDS/IPS - Implantación de cortafuegos y redes privadas virtuales (VPN) - Defensa en profundidad - Honeypots y honeynets - Monitorización de la red - Análisis del tráfico de la red - Minimización de la exposición (superficie de ataque y vectores) - Control de acceso a la red (interno y externo) - Redes perimetrales (zonas desmilitarizadas o DMZ) / servidores proxy - Desarrollo y aplicación de políticas de red - Procedimientos de ataque (por ejemplo, secuestro de sesión, hombre en el medio) - Búsqueda de amenazas y aprendizaje automático

KA-5: Seguridad de sistemas	
Se centra en la seguridad de sistemas compuesta de conexiones, componentes y software.	Contenidos esenciales: • Enfoque holístico • Política de seguridad • Autenticación • Control de acceso • Supervisión • Recuperación • Pruebas • Documentación
Unidades de conocimiento	**Temas**
Pensamiento sistémico	- Definición de sistemas - Aproximaciones globales al diseño de sistemas - Seguridad de Sistemas de Propósito General - Seguridad de Sistemas de Propósito Específico - Modelos de Amenazas - Análisis de Requisitos - Principios Fundamentales de Seguridad de Sistemas - Desarrollo de pruebas
Gestión de sistemas	- Modelos de política - Composición de políticas - Uso de la automatización - Parcheo y ciclo de vida de la vulnerabilidad - Operación - Puesta en marcha y desmantelamiento - Amenaza interna - Documentación . Sistemas y procedimientos

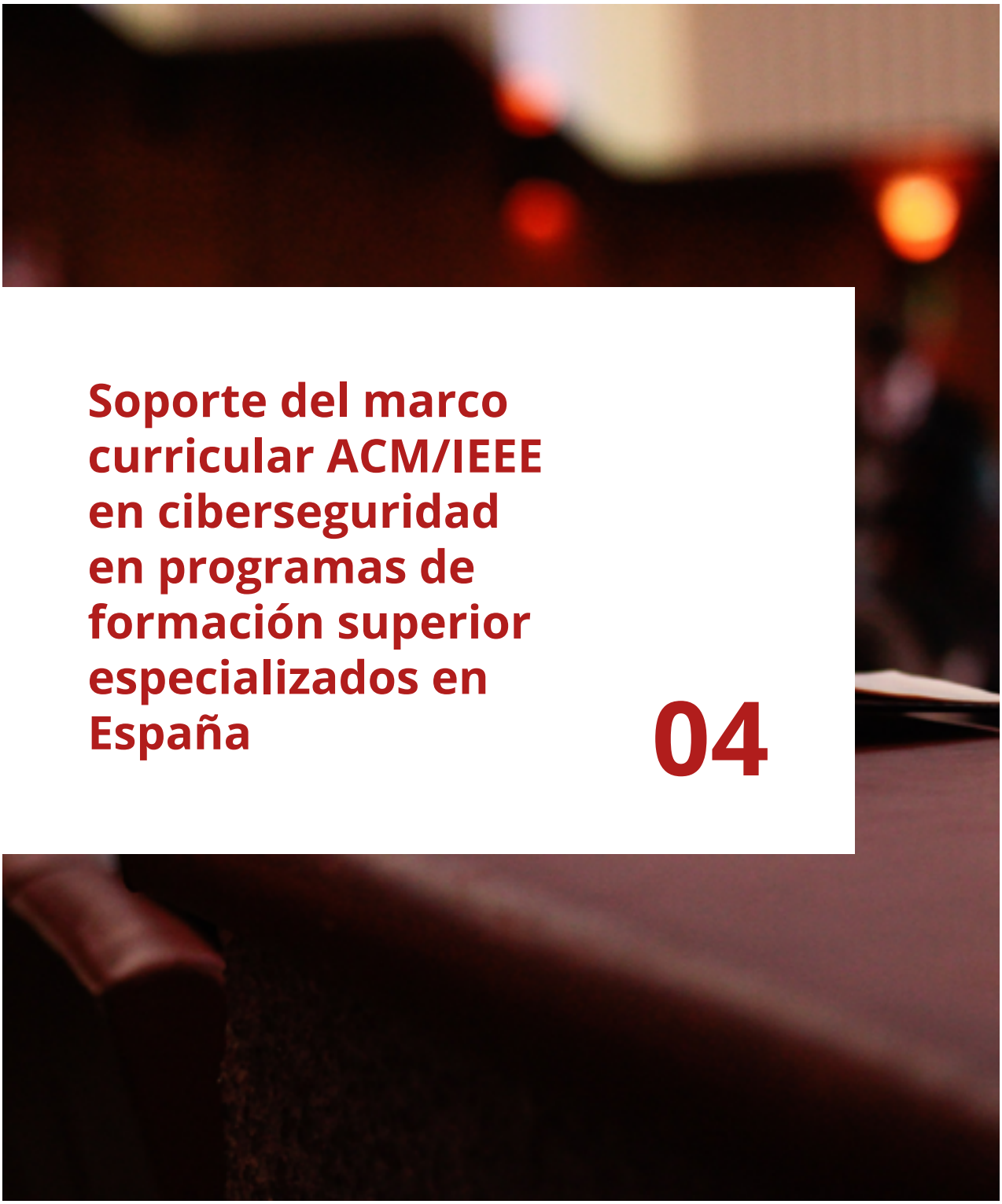
Acceso al sistema	- Métodos de autenticación - Identidad
Control del sistema	- Control de acceso - Modelos de autorización - Detección de intrusos - Ataques - Defensas - Auditoría - Malware - Modelos de vulnerabilidad - Pruebas de penetración - Análisis forense - Recuperación, resiliencia
Retirada del sistema	- Desmantelamiento - Eliminación
Prueba del sistema	- Validación de los requisitos - Validación de la composición de los componentes - Pruebas unitarias frente a pruebas del sistema - Verificación formal de sistemas
Ejemplos de arquitecturas de sistemas	- Máquinas virtuales - Sistemas de control industrial - Internet de las cosas - Sistemas embebidos - Sistemas móviles - Sistemas autónomos - Sistemas de propósito general

KA-6: Seguridad del ser humano	
Se centra en garantizar la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos pertenecientes a una persona (dispositivos personales) o a una organización.	Contenidos esenciales: • Gestión de la identidad • Ingeniería social • Conciencia y comprensión • Privacidad y seguridad del comportamiento social • Privacidad y seguridad de los datos personales
Unidades de conocimiento	**Temas**
Gestión de la identidad	- Identificación y autenticación de personas y dispositivos - Control de activos físicos y lógicos - Identidad como servicio (Identity as a Service, IaaS) - Servicios de identidad de terceros - Ataques al control de acceso y medidas de mitigación
Ingeniería social	- Tipos de ataques de ingeniería social - Psicología de los ataques de ingeniería social - Engañar a los usuarios - Detección y mitigación de los ataques de ingeniería social
Cumplimiento de las reglas/políticas/ normas éticas de ciberseguridad	- Mal uso del sistema y mal comportamiento de los usuarios - Aplicación y normas de comportamiento - Comportamiento adecuado en condiciones de incertidumbre
Conciencia y comprensión	- Percepción del riesgo y comunicación - Ciberhigiene - Educación de los usuarios en materia de ciberseguridad - Conocimiento de las cibervulnerabilidades y amenazas
Privacidad social y de comportamiento	- Teorías sociales de la privacidad - Privacidad y seguridad en las redes sociales
Privacidad y seguridad de los datos personales	- Datos personales sensibles - Seguimiento personal y huella digital
Seguridad y privacidad aplicables	- Usabilidad y experiencia del usuario - Factores de seguridad humana - Conocimiento y comprensión de la política - Política de privacidad - Orientación e implicaciones del diseño

KA-7: Seguridad de la organización	
Se centra en proteger la información de las organizaciones y conlleva a temas relativos a la gestión de riesgo.	Contenidos esenciales: • Gestión de riesgos • Gobernanza y política • Leyes, ética y cumplimiento • Estrategia y planificación
Unidades de conocimiento	**Temas**
Gestión de riesgos	- Identificación de riesgos - Evaluación y análisis de riesgos - Amenazas internas - Modelos y metodologías de medición y evaluación de riesgos - Control de riesgos
Gobernanza y política de seguridad	- Contexto organizativo - Privacidad - Leyes, ética y cumplimiento - Gobernanza de la seguridad - Comunicación a nivel ejecutivo y del consejo de administración - Política de gestión
Herramientas analíticas	- Medidas de rendimiento (métricas) - Análisis de datos - Inteligencia de seguridad
Administración de sistemas	- Administración de sistemas operativos - Administración de sistemas de bases de datos - Administración de redes - Administración de la nube - Administración de sistemas ciberfísicos - Bastionado del sistema - Disponibilidad
Planificación de la ciberseguridad	- Planificación estratégica - Gestión operativa y táctica
Continuidad de negocio, recuperación de desastres y gestión de incidentes	- Continuidad del negocio, recuperación de desastres y gestión de incidentes
Gestión de programas de seguridad	- Gestión de proyectos - Gestión de recursos - Métricas de seguridad - Garantía y control de calidad

Seguridad del personal	- Concienciación, formación y educación en materia de seguridad - Prácticas de contratación de seguridad - Prácticas de despido por motivos de seguridad - Seguridad de terceros - Seguridad en los procesos de revisión - Cuestión especial en la privacidad de la información personal de los empleados
Operaciones de seguridad	- Convergencia de la seguridad - Centros de operaciones de seguridad global (Global Security Operations Centers, GSOC).

KA-8: Seguridad en la sociedad	
Se centra en aspectos de la ciberseguridad que repercuten de manera positiva o negativa al conjunto de la sociedad.	Contenidos esenciales: • Ciberdelincuencia (Cibercrimen) • Ciberderecho (cyber law) • Ciberética • Ciberpolítica • Privacidad
Unidades de conocimiento	**Temas**
Ciberdelincuencia	- Comportamiento cibercriminal - Ciberterrorismo - Investigaciones cibercriminales - Economía de la ciberdelincuencia
Ciberderecho	- Fundamentos constitucionales del ciberderecho - Propiedad intelectual relacionada con la ciberseguridad - Leyes de privacidad - Derecho de la seguridad de los datos - Leyes de piratería informática - Pruebas digitales - Contratos digitales - Convenios multinacionales (acuerdos) - Leyes transfronterizas de privacidad y seguridad de datos
Ciberética	- Definición de la ética - Ética profesional y códigos de conducta - Ética y equidad/diversidad - Ética y derecho - Autonomía/ética de los robots - Ética y conflicto - Hacking ético - Marcos éticos y teorías normativas
Ciberpolítica	- Ciberpolítica internacional - Ciberpolítica de la UE - Impacto global - Política de ciberseguridad y seguridad nacional - Implicaciones económicas nacionales de la ciberseguridad - Nuevas adyacencias a la diplomacia
Privacidad	- Definición de la privacidad - Derecho a la intimidad - Protección de la intimidad - Normas y actitudes en materia de privacidad - Violación de la intimidad - La privacidad en las sociedades



Soporte del marco curricular ACM/IEEE en ciberseguridad en programas de formación superior especializados en España

04

En los últimos años se han desarrollado a lo largo de España múltiples ofertas de programas de formación superior con especialización en el área de Ciberseguridad. De acuerdo con la última actualización (febrero 2021) del catálogo de formación de ciberseguridad en España [INCIBE2021a], se han identificado un total de 72 programas de Máster y 3 Grados, así como un total de 129 centros dónde se puede realizar algún estudio en ciberseguridad, en modalidad máster o en otro formato [INCIBE2021b].

En estos catálogos se incluyen programas formativos de másteres y grados de diversos tipos: estudios oficiales, que han sido verificados por un organismo de verificación de estudios superiores oficial (ANECA u organismos autonómicos) y estudios propios, que son propuestos por cada institución sin verificación oficial externa. Igualmente, existen másteres propuestos por universidades públicas, universidades privadas y otras instituciones.

Por todo ello, el rango de contenidos de los mismos es muy variado y con distintos enfoques. Con el objetivo de analizar los contenidos de los mismos y cuáles son las áreas más cubiertas y menos cubiertas de los mismos, en el Grupo de Trabajo de Formación, Capacitación y Talento (GT3) establecido en el marco de acciones del Foro Nacional de Ciberseguridad impulsado por el Departamento de Seguridad Nacional, los participantes de CRUE (Conferencia de Rectores de las Universidades Españolas) de este grupo de trabajo han realizado un estudio sobre el soporte que tiene el Marco Curricular ACM/IEEE en Ciberseguridad, en estos programas.

En base a las distintas universidades participantes en este grupo de trabajo, a través de CRUE y RENIC (Red de Excelencia Nacional de Investigación en Ciberseguridad), se realizó una consulta a todas ellas para evaluar el soporte en sus programas formativos superiores en ciberseguridad del Marco Curricular ACM/IEEE en Ciberseguridad. Para ello, el cuestionario marcaba:

• Inclusión de cada uno de los temas (clasificados por áreas y unidades de conocimiento) en el programa formativo de dicha universidad, con una indicación de inclusión significativa, inclusión parcial o no soportado

• Identificación de temas que son considerados en los programas formativos de las universidades como conocimientos previos necesarios para afrontar el programa formativo

• Identificación de temas incluidos en los programas formativos que no están incluidos en el marco curricular ACM/IEEE en Ciberseguridad.

De esta consulta, se recibieron informes provenientes de:

• 10 másteres especializados en ciberseguridad, de distintos puntos de España, oficiales y propios, y con distinta antigüedad.

• 2 grados especializados en ciberseguridad (por completo o parcialmente), oficiales.

Estos informes se consideraron suficientes para la realización de este análisis, proporcionado una muestra significativa de la oferta formativa en formación superior especializada en ciberseguridad existente en España.

En las siguientes secciones se detalla el análisis agregado sobre el nivel de soporte de todas estas ofertas formativas respecto a los distintos componentes del marco curricular ACM/IEEE en Ciberseguridad. Para cada unidad de conocimiento se incluye un gráfico con el soporte encontrado en cada uno de sus temas.

4.1. Área de conocimiento KA-1: Seguridad del dato

Se centra en la protección de los datos (almacenados, procesados o en tránsito), y requiere como conocimiento previo la aplicación de algoritmos matemáticos y analíticos para su completa implementación.

Esta área cubre como contenidos esenciales conceptos básicos de criptografía, forense digital, comunicaciones seguras de extremo a extremo, integridad y autenticación de los datos y seguridad del almacenamiento de la información. Por ello, se divide en 8 unidades de conocimiento distintas:

- Criptografía
- Análisis forense digital
- Integridad y autenticación de datos
- Control de acceso
- Protocolos de comunicación seguros
- Criptoanálisis
- Privacidad de datos
- Seguridad del almacenamiento de la información

4.1.1. Criptografía

La unidad de conocimiento de criptografía cubre conceptos básicos y avanzados de criptografía, aspectos matemáticos de los algoritmos, así como el estudio de los distintos algoritmos, de criptografía clásica y moderna, y simétricos y asimétricos. Se observa un soporte **alto** de todos los temas, excepto de los aspectos matemáticos que no son cubiertos en los programas.

El detalle de soporte de cada tema se muestra en la figura siguiente.

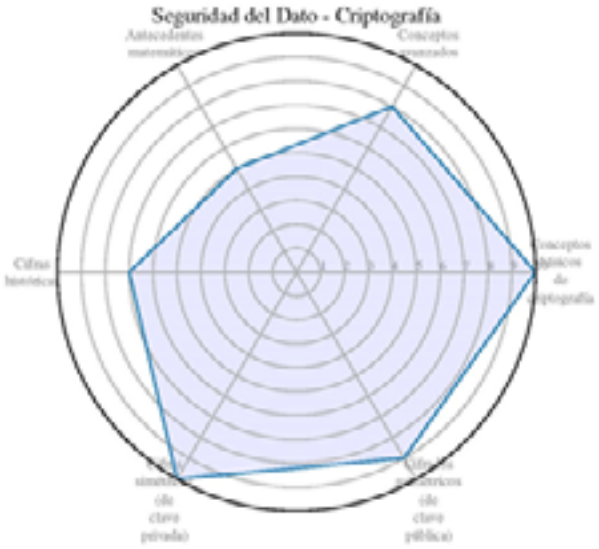


Figura 2: Soporte de temas de Criptografía

4.1.2. Análisis forense digital

La unidad de conocimiento de análisis forense digital cubre la introducción de la definición y los límites y tipos de herramientas, cuestiones legales, herramientas forenses digitales, proceso de investigación, adquisición y conservación de pruebas, análisis de las pruebas, presentación de resultados, autenticación de las pruebas, presentación de informes, respuesta y gestión de incidentes y análisis forense móvil.

El estudio refleja un soporte **medio** de todos los temas, con menor énfasis en aquellos más relacionados con aspectos legales y con los aspectos de análisis forense en móviles. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 3: Soporte de temas de Análisis Forense Digital

4.1.3. Integridad y autenticación de datos

La unidad de conocimiento de Integridad y autenticación de datos incluye los aspectos de fuerza de autenticación, técnicas de ataque a las contraseñas, técnicas de almacenamiento de contraseñas e integridad de los datos.

El estudio refleja un soporte **alto** de todos los temas, con un menor soporte en los aspectos de almacenamiento de contraseñas. El detalle de soporte de cada tema se muestra en la figura siguiente.

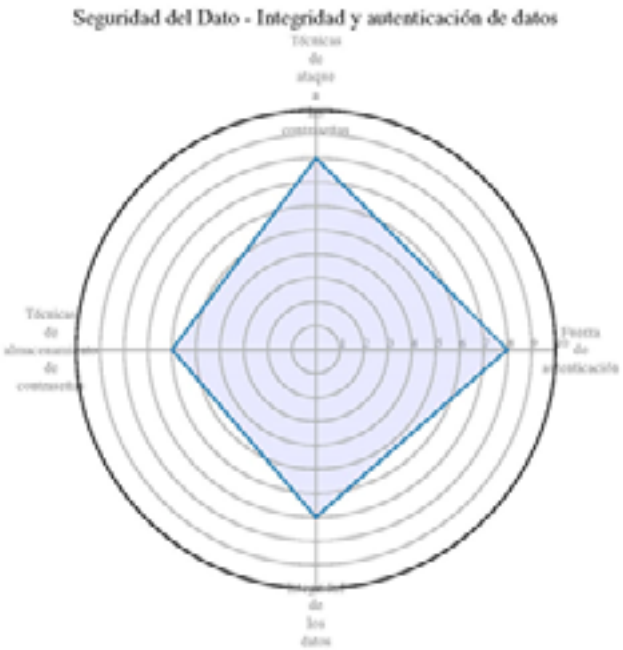


Figura 4: Soporte de temas de Integridad y autenticación de datos

4.1.4. Control de acceso

La unidad de conocimiento de control de acceso incluye los aspectos de seguridad física de los datos, control de acceso a los datos lógicos, diseño de arquitecturas seguras y técnicas de prevención de fugas de datos.

El estudio refleja un soporte **alto** de los temas de Diseño de arquitecturas seguras, y un soporte **medio** de los temas de control de acceso a los datos lógicos, seguridad física de los datos y técnicas de prevención de fugas de datos. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 5: Soporte de temas de Control de Acceso

4.1.5. Protocolos de comunicación seguros

La unidad de conocimiento de protocolos de comunicación seguros incluye los aspectos de protocolos de la capa de aplicación y transporte, ataques a TLS, capa de Internet/Red, protocolos de preservación de la privacidad y capa de enlace de datos.

El estudio refleja un soporte **alto** de todos los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

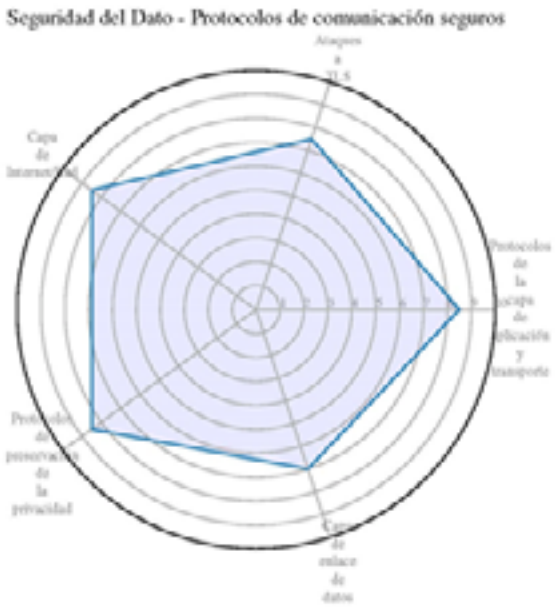


Figura 6: Soporte de temas de Protocolos de comunicación seguros

4.1.6. Criptoanálisis

La unidad de conocimiento de criptoanálisis incluye los aspectos de ataques clásicos, ataques de canal lateral, ataques contra cifrados de clave privada, ataques contra cifradores de clave pública, algoritmos para resolver el problema del registro discreto y ataques a RSA.

El estudio refleja un gran soporte **bajo** de todos los temas de esta unidad, excepto los ataques clásicos. El detalle de soporte de cada tema se muestra en la figura siguiente.

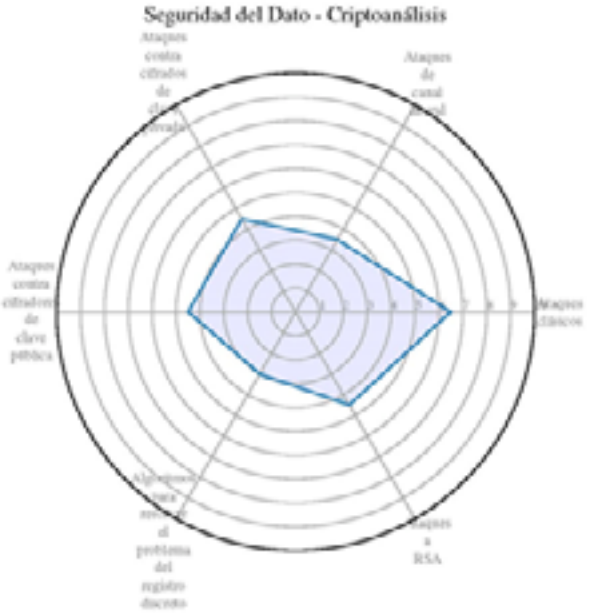


Figura 7: Soporte de temas de Criptoanálisis

4.1.7. Privacidad de datos

La unidad de conocimiento de privacidad de datos incluye un único tema relacionado con el panorama general (definiciones, aspectos legales, recopilación de datos, agregación de datos, difusión de datos, invasión de la privacidad, ingeniería social y redes sociales).

El estudio refleja un gran soporte **alto** de este tema (cubierto en el 80% de los programas analizados).

4.1.8. Seguridad del almacenamiento de la información

La unidad de conocimiento de seguridad del almacenamiento de la información incluye los aspectos de cifrado de discos y archivos, borrado de datos, enmascaramiento de datos, seguridad de las bases de datos y ley de seguridad de los datos.

El estudio refleja un soporte **medio/alto** de los temas de esta unidad de conocimiento, exceptuando el enmascaramiento de datos, que tiene un soporte **bajo**. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 8: Soporte de temas de seguridad del almacenamiento de la información

4.2. Área de Conocimiento KA-2: Seguridad del software

Se centra en el desarrollo y la utilización de programas informáticos que preserven de forma fiable las propiedades de seguridad de la información y los sistemas que éstos aplican.

Esta área cubre como contenidos esenciales principios fundamentales de diseño, incluyendo el mínimo privilegio, el diseño abierto y la abstracción, requisitos de seguridad y su rol en el diseño, cuestiones de implementación, pruebas / testing estáticas y dinámicas, configuración y aplicación de parches y ética, especialmente en el desarrollo, las pruebas y la divulgación de vulnerabilidades. Por ello, se divide en las siguientes unidades de conocimiento:

- Principios fundamentales
- Diseño
- Implementación
- Análisis y pruebas
- Despliegue y mantenimiento
- Documentación
- Ética

4.2.1. Principios fundamentales

La unidad de conocimiento de principios fundamentales incluye los aspectos de mínimo privilegio, fallo seguro (por defecto), mediación completa, separación de privilegios, minimizar la superficie de confianza, economía de mecanismo, minimización de la implementación (mecanismo menos común), mínima sorpresa (aceptación psicológica), diseño abierto, diseño por capas (defensa en profundidad), abstracción, modularidad, vinculación completa y diseño para la iteración.

El estudio refleja un soporte **medio/alto** en la mayor parte de los temas de esta unidad de conocimiento, exceptuando algunos de ellos que tienen un soporte **medio/bajo**. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 9: Soporte de temas de principios fundamentales

4.2.2. Diseño

La unidad de conocimiento de diseño incluye los aspectos de derivación de los requisitos de seguridad, especificación de los requisitos de seguridad, ciclo de vida del desarrollo del software ciclo de vida del desarrollo de la seguridad y lenguajes de programación y lenguajes de tipo seguro.

El estudio refleja un soporte **alto** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

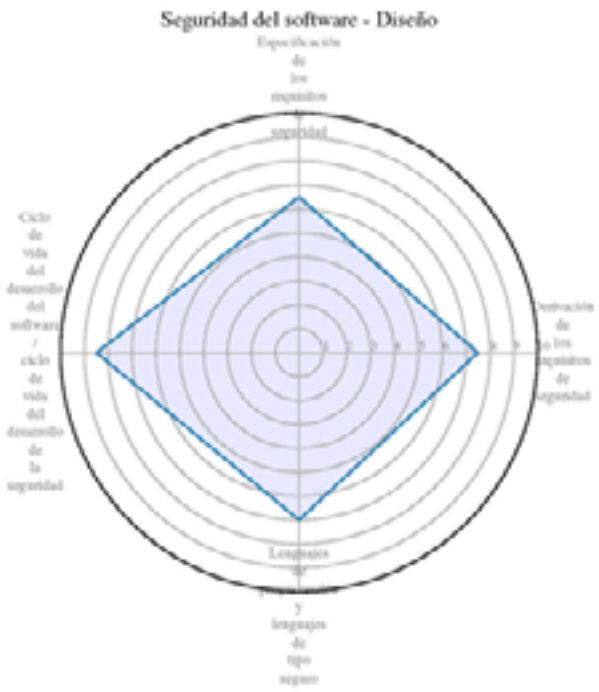


Figura 10 Soporte de temas de diseño

4.2.3. Implementación

La unidad de conocimiento de implementación incluye los aspectos de validación de la entrada y comprobación de su representación, utilización correcta de las API, uso de las funciones de seguridad, comprobación de las relaciones de tiempo y estado, manejar adecuadamente las excepciones y los errores, programación robusta, encapsular estructuras y módulos así como tener en cuenta el entorno.

El estudio refleja un soporte **alto** en la mayor parte de los temas de esta unidad de conocimiento, exceptuando algunos de ellos que tienen un soporte medio. El detalle de soporte de cada tema se muestra en la figura siguiente.

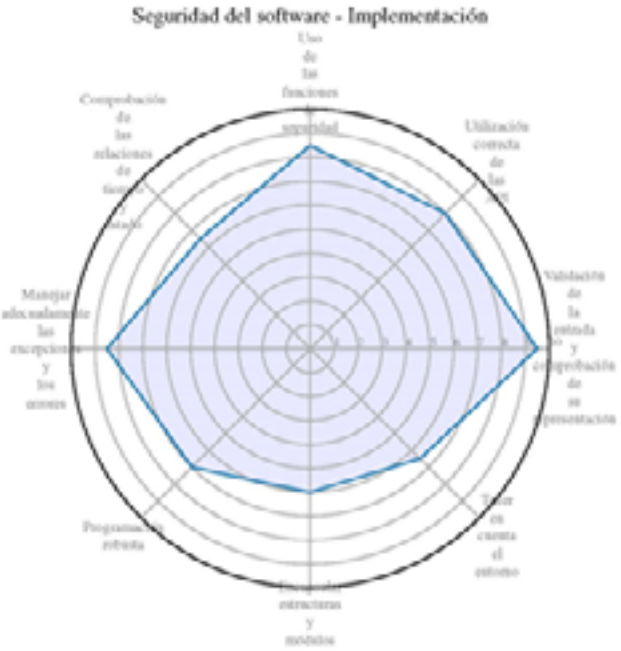


Figura 11 Soporte de temas de implementación

4.2.4. Análisis y pruebas

La unidad de conocimiento de análisis y pruebas incluye los aspectos de análisis estático y dinámico, pruebas unitarias, pruebas de integración y pruebas de software.

El estudio refleja un soporte **medio** en los temas de esta unidad de conocimiento, excepto el tema de análisis estático y dinámico, que tiene un soporte **alto**. El detalle de soporte de cada tema se muestra en la figura siguiente.

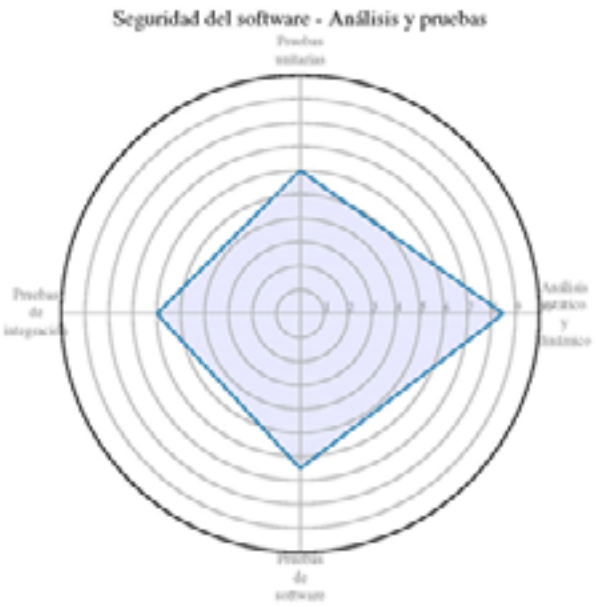


Figura 12 Soporte de temas de análisis y pruebas

4.2.5. Despliegue y mantenimiento

La unidad de conocimiento de despliegue y mantenimiento incluye los aspectos de configuración, parcheado y ciclo de vida de la vulnerabilidad, comprobación del entorno, DevOps y desmantelamiento/retirada.

El estudio refleja un soporte **bajo** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 13 Soporte de temas de despliegue y mantenimiento

4.2.6. Documentación

La unidad de conocimiento de documentación incluye los aspectos de documentos de instalación, guías y manuales de usuario, documentación de aseguramiento/garantía y documentación sobre seguridad.

El estudio refleja un soporte **bajo** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 14 Soporte de temas de documentación

4.2.7. Ética

La unidad de conocimiento de ética incluye los aspectos de cuestiones éticas en el desarrollo de software, aspectos sociales del desarrollo de software, aspectos legales del desarrollo de software, revelación de vulnerabilidades y qué, cuándo y por qué probar.

El estudio refleja un soporte **bajo** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

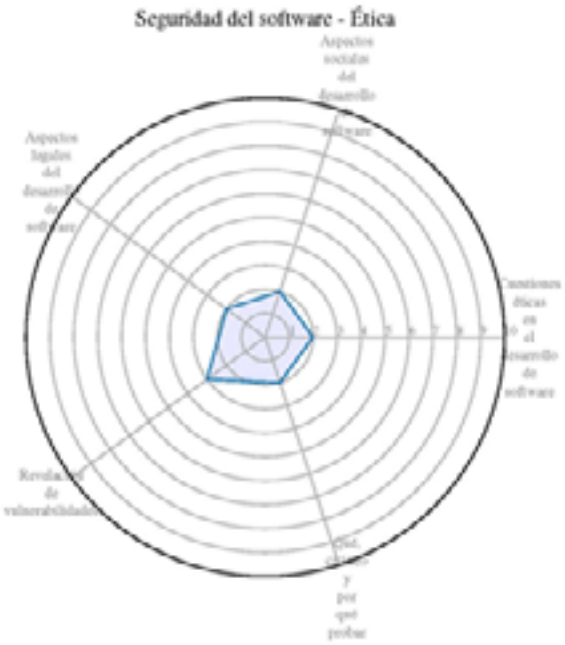


Figura 15 Soporte de temas de ética

4.3. Área de Conocimiento KA-3: Seguridad de los componentes

Se centra en el ciclo de vida de los componentes, desde el diseño, la adquisición, las pruebas, y el análisis hasta el mantenimiento de componentes integrados en sistemas.

Esta área cubre como contenidos esenciales las vulnerabilidades de los componentes del sistema, ciclo de vida de los componentes, principios de diseño de componentes seguros, seguridad en la gestión de la cadena de suministro, pruebas de seguridad e ingeniería inversa. Por ello, se divide en las siguientes unidades de conocimiento:

- Diseño de componentes
- Adquisición de componentes
- Pruebas de componentes
- Ingeniería inversa de componentes

4.3.1. Diseño de componentes

La unidad de diseño de componentes incluye los aspectos de seguridad en el diseño de componentes, principios de diseño seguro de componentes, Identificación de componentes, técnicas de ingeniería inversa, mitigación de ataques de canal lateral y tecnologías antimanipulación.

El estudio refleja un soporte **bajo** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 9: Soporte de temas de principios fundamentales

4.3.2. Adquisición de componentes

La unidad de adquisición de componentes incluye los aspectos de riesgos de la cadena de suministro, seguridad de la cadena de suministro e investigación de proveedores.

El estudio refleja un soporte **muy bajo** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 17 Soporte de temas de adquisición de componentes

4.3.3. Pruebas de componentes

La unidad de pruebas de componentes incluye los aspectos de principios de las pruebas unitaria y pruebas de seguridad.

El estudio refleja un soporte **medio** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 18 Soporte de temas de pruebas de componentes

4.3.4. Ingeniería inversa de componentes

La unidad de Ingeniería inversa de componentes incluye los aspectos de ingeniería inversa del diseño, ingeniería inversa del hardware e ingeniería inversa del software.

El estudio refleja un soporte **bajo** en los temas de esta unidad de conocimiento, exceptuando el tema de ingeniería inversa del software que cuenta con un soporte **medio**. El detalle de soporte de cada tema se muestra en la figura siguiente.

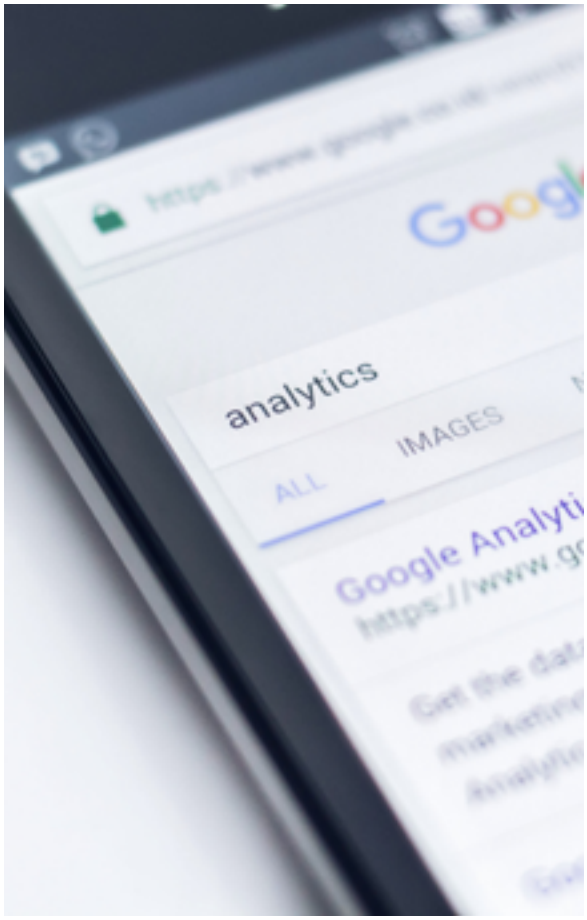
Figura 19 Soporte de temas de ingeniería inversa de componentes

4.4. Área de Conocimiento KA-4: Seguridad de las conexiones

Se centra en la seguridad de las conexiones establecidas entre componentes, incluyendo las conexiones físicas y lógicas.

Esta área cubre como contenidos esenciales los sistemas, arquitectura, modelos y normas, interfaces de componentes físicos, interfaces de componentes de software, ataques de conexión y ataques de transmisión. Por ello, se divide en las siguientes unidades de conocimiento:

- Medios físicos
- Interfaces físicas y conectores
- Arquitectura de hardware
- Arquitectura de sistemas distribuidos
- Arquitectura de red
- Implementación de redes
- Servicios de red
- Defensa de la red



4.4.1. Medios físicos

La unidad de medios físicos incluye los aspectos de transmisión en un medio, medios compartidos y punto a punto, modelos de compartición y tecnologías comunes.

El estudio refleja un soporte **nulo** en los temas de esta unidad de conocimiento como se ve en el detalle de soporte de cada tema mostrado en la figura siguiente. Estos temas son asumidos como conocimientos previos para estos estudios superiores especializados.

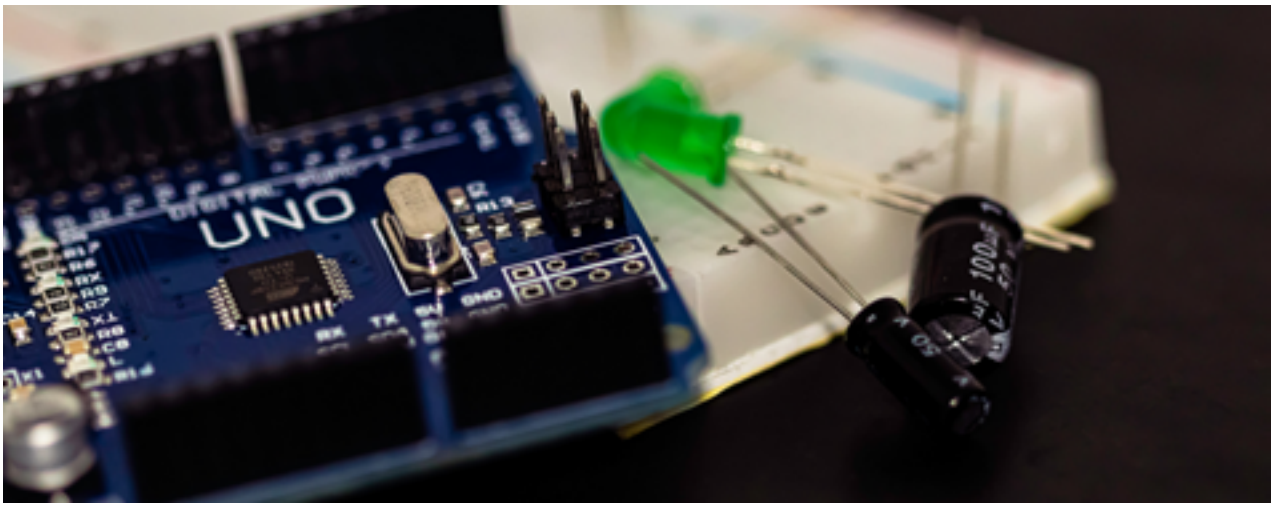
Figura 20 Soporte de temas de medios físicos

4.4.2. Interfaces físicas y conectores

La unidad de interfaces físicas y conectores incluye los aspectos de características y materiales del hardware, estándares y conectores comunes.

El estudio refleja un soporte **nulo** en los temas de esta unidad de conocimiento como se ve en el detalle de soporte de cada tema mostrado en la figura siguiente. Estos temas son asumidos como conocimientos previos para estos estudios superiores especializados.

Figura 21 Soporte de temas de Interfaces físicas y conectores



4.4.3. Arquitectura de hardware

La unidad de arquitectura de hardware incluye los aspectos de arquitecturas estándar, estándares de interfaz de hardware y arquitecturas comunes.

El estudio refleja un soporte **nulo** en los temas de esta unidad de conocimiento, como se ve en el detalle de soporte de cada tema mostrado en la figura siguiente. Estos temas son asumidos como conocimientos previos para estos estudios superiores especializados.

Figura 22 Soporte de temas de arquitectura de hardware

4.4.4. Arquitectura de sistemas distribuidos

La unidad de arquitectura de sistemas distribuidos incluye los aspectos de conceptos generales, web global, internet; protocolos y estratificación, computación de alto rendimiento (superordenadores), hipervisores e implementaciones de computación en la nube y vulnerabilidades y ejemplos de explotaciones.

El estudio refleja un soporte desigual en los temas de esta unidad de conocimiento como se ve en el detalle de soporte de cada tema mostrado en la figura siguiente. El tema de vulnerabilidades tiene un soporte **completo**, mientras que los temas de conceptos generales e Internet tienen un soporte **medio/alto** y el resto un soporte **bajo**. La mayor parte de estos temas son asumidos como conocimientos previos para estos estudios superiores especializados.

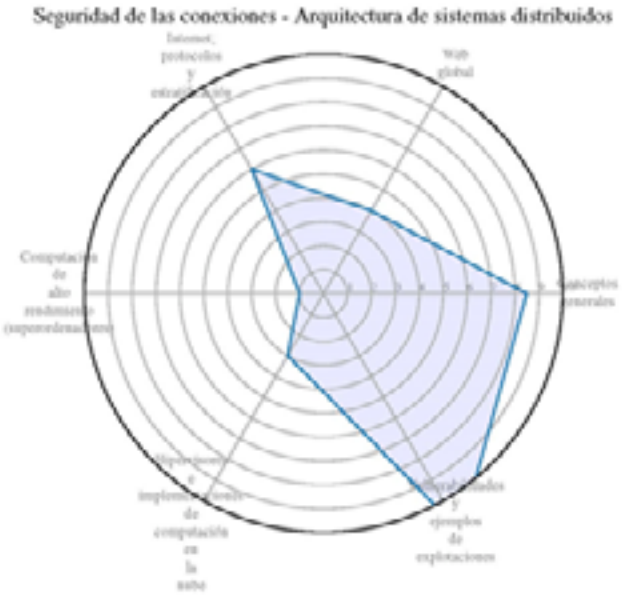


Figura 23 Soporte de temas de arquitectura de sistemas distribuidos

4.4.5. Arquitectura de red

La unidad de arquitectura de red incluye los aspectos de conceptos generales, arquitecturas comunes, reenvío / enrutamiento, conmutación/recuperación, tendencias emergentes y virtualización y arquitectura de hipervisor virtual.

El estudio refleja un soporte **medio/bajo** en los temas de esta unidad de conocimiento como se ve en el detalle de soporte de cada tema mostrado en la figura siguiente. La mayor parte de estos temas son asumidos como conocimientos previos para estos estudios superiores especializados.

Figura 24 Soporte de temas de arquitectura de red

4.4.6. Implementación de redes

La unidad de implementación de redes incluye los aspectos de redes IEEE 802/ISO, redes IETF y TCP/IP, integración práctica y protocolos de cola y vulnerabilidades y ejemplos de explotaciones.

El estudio refleja un soporte desigual en los temas de esta unidad de conocimiento como se ve en el detalle de soporte de cada tema mostrado en la figura siguiente. El tema de vulnerabilidades tiene un soporte **alto**, mientras que el resto de temas tienen un soporte **medio/bajo**. La mayor parte de estos temas son asumidos como conocimientos previos para estos estudios superiores especializados.

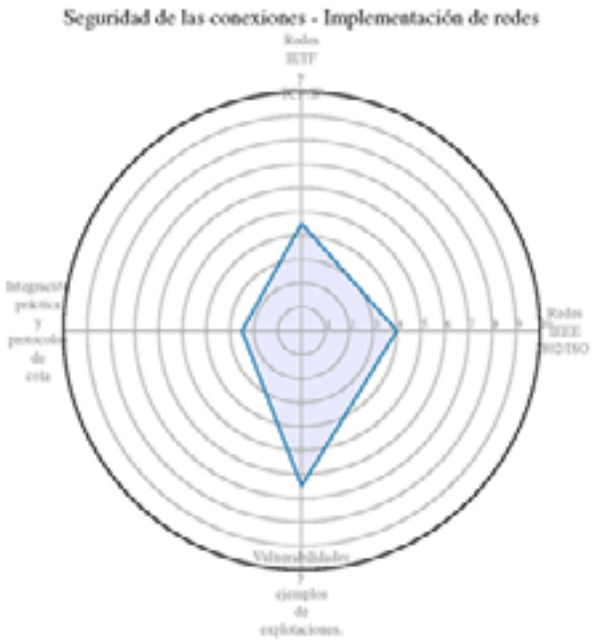


Figura 25 Soporte de temas de implementación de redes

4.4.7. Servicios de red

La unidad de servicios de red incluye los aspectos de concepto de servicio, modelos de servicio (cliente-servidor, peer-to-peer), conceptos de protocolo de servicio (IPC, API, IDL), arquitecturas comunes de comunicación de servicios, virtualización de servicios y vulnerabilidades y ejemplos de explotaciones.

El estudio refleja un soporte desigual en los temas de esta unidad de conocimiento como se ve en el detalle de soporte de cada tema mostrado en la figura siguiente. El tema de vulnerabilidades tiene un soporte **completo**, mientras que el resto de temas tienen un soporte **medio/bajo**. La mayor parte de estos temas son asumidos como conocimientos previos para estos estudios superiores especializados.

Figura 26 Soporte de temas de servicios de red

4.4.8. Defensa de la red

La unidad de defensa de red incluye los aspectos de endurecimiento de la red, Implantación de IDS/IPS, implantación de cortafuegos y redes privadas virtuales (VPN), defensa en profundidad, Honeypots y honeynets, monitorización de la red, análisis del tráfico de la red, minimización de la exposición (superficie de ataque y vectores), control de acceso a la red (interno y externo), redes perimetrales (zonas desmilitarizadas o DMZ)/servidores proxy, desarrollo y aplicación de políticas de red, procedimientos de ataque (por ejemplo, secuestro de sesión, hombre en el medio) y búsqueda de amenazas y aprendizaje automático.

El estudio refleja un soporte **completo o muy alto** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

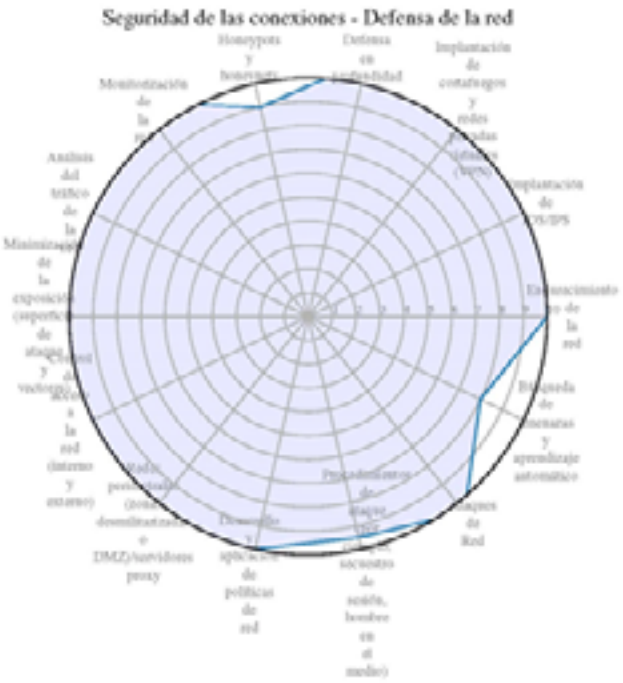


Figura 27 Soporte de temas de defensa de la red

4.5. Área de Conocimiento KA-5: Seguridad de sistemas

Se centra en la seguridad de sistemas compuesto de conexiones, componentes y software.

Esta área cubre como contenidos esenciales un enfoque holístico, política de seguridad, autenticación, control de acceso, supervisión, recuperación, pruebas y documentación. Por ello, se divide en las siguientes unidades de conocimiento:

- Pensamiento sistémico
- Gestión de sistemas
- Acceso al sistema
- Control del sistema
- Retirada del sistema
- Prueba del sistema
- Ejemplos de arquitecturas de sistemas

4.5.1. Pensamiento sistémico

La unidad de pensamiento sistémico incluye los aspectos de definición de sistemas: aproximaciones globales al diseño de sistemas, seguridad de sistemas de propósito general, seguridad de Sistemas de propósito específico, modelos de amenazas, análisis de requisitos, principios fundamentales de seguridad de sistemas, y desarrollo de pruebas.

El estudio refleja un soporte **bajo** en los temas de esta unidad de conocimiento. La mayor parte de estos temas son asumidos como conocimientos previos para estos estudios superiores especializados El detalle de soporte de cada tema se muestra en la figura siguiente.

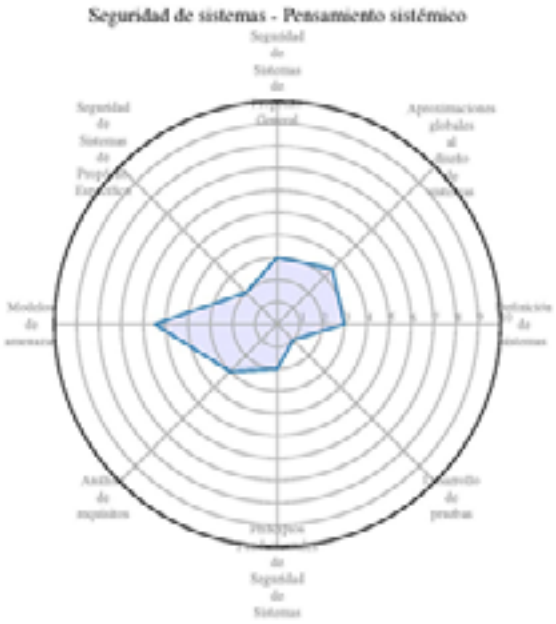


Figura 28 Soporte de temas de pensamiento sistémico

4.5.2. Gestión de sistemas

La unidad de gestión de sistemas incluye los aspectos de modelos de política, composición de políticas, uso de la automatización, parcheo y ciclo de vida de la vulnerabilidad, operación, puesta en marcha y desmantelamiento, amenaza interna, documentación y sistemas y procedimientos.

El estudio refleja un soporte **medio** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 29 Soporte de temas de gestión de sistemas

4.5.3. Acceso al sistema

La unidad de acceso al sistema incluye los aspectos de métodos de autenticación e identidad.

El estudio refleja un soporte **muy alto** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 30 Soporte de temas de acceso al sistema

4.5.4. Control del sistema

La unidad de control del sistema incluye los aspectos de control de acceso, modelos de autorización, detección de intrusos, ataques, defensas, auditoría, malware, modelos de vulnerabilidad, pruebas de penetración, análisis forense y recuperación, resiliencia.

El estudio refleja un soporte **muy alto** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

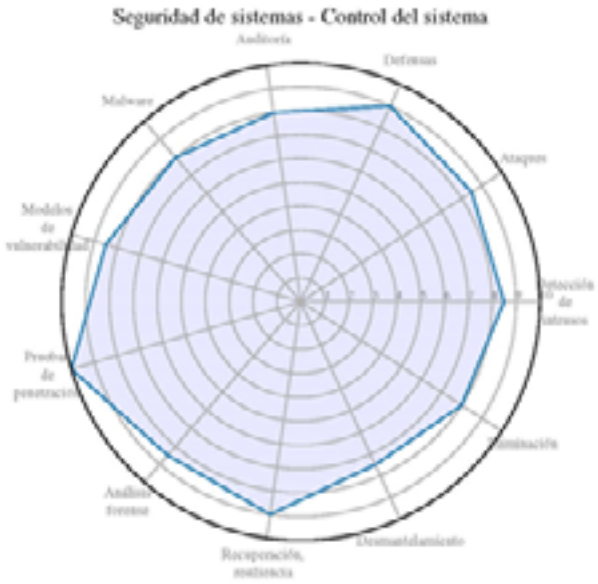


Figura 31 Soporte de temas de control del sistema

4.5.5. Retirada del sistema

La unidad de retirada del sistema incluye los aspectos de desmantelamiento y eliminación.

El estudio refleja un soporte nulo en los temas de esta unidad de conocimiento.

4.5.6. Prueba del sistema

La unidad de prueba del sistema incluye los aspectos de validación de los requisitos, validación de la composición de los componentes, pruebas unitarias frente a pruebas del sistema y verificación formal de sistemas.

El estudio refleja un soporte **muy bajo** en los temas de esta unidad de conocimiento. La mayor parte de estos temas son asumidos como conocimientos previos para estos estudios superiores especializados. El detalle de soporte de cada tema se muestra en la figura siguiente.

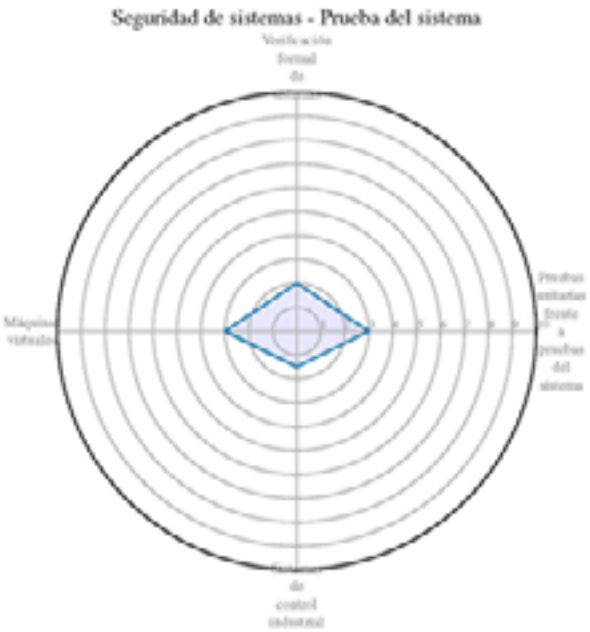


Figura 32 Soporte de temas de prueba del sistema

4.5.7. Ejemplos de arquitecturas de sistemas

La unidad de ejemplos de arquitecturas de sistemas incluye los aspectos de máquinas virtuales, sistemas de control industrial, internet de las cosas, sistemas embebidos, sistemas móviles, sistemas autónomos y sistemas de propósito general.

El estudio refleja un soporte **medio/bajo** en los temas de esta unidad de conocimiento. La mayor parte de estos temas son asumidos como conocimientos previos para estos estudios superiores especializados. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 33 Soporte de temas de ejemplos de arquitecturas de sistemas

4.6. Área de Conocimiento KA-6: Seguridad del ser humano

Se centra en garantizar la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos pertenecientes a una persona (dispositivos personales) o a una organización.

Esta área cubre como contenidos esenciales la gestión de la identidad, ingeniería social, conciencia y comprensión. privacidad y seguridad del comportamiento social y privacidad y seguridad de los datos personales. Por ello, se divide en las siguientes unidades de conocimiento:

- Gestión de la identidad
- Ingeniería social
- Cumplimiento de las reglas/políticas/normas éticas de ciberseguridad
- Conciencia y comprensión
- Privacidad social y de comportamiento
- Privacidad y seguridad de los datos personales
- Seguridad y privacidad aplicables

4.6.1. Gestión de la identidad

La unidad de Gestión de la identidad incluye los aspectos de identificación y autenticación de personas y dispositivos, control de activos físicos y lógicos, identidad como servicio (Identity as a Service, IaaS), servicios de identidad de terceros y ataques al control de acceso y medidas de mitigación.

El estudio refleja un soporte desigual en los temas de esta unidad de conocimiento con soporte **alto** de identificación y autenticación de personas y dispositivos y ataques al control de acceso y medidas de mitigación y un soporte **medio/bajo** en el resto. El detalle de soporte de cada tema se muestra en la figura siguiente.

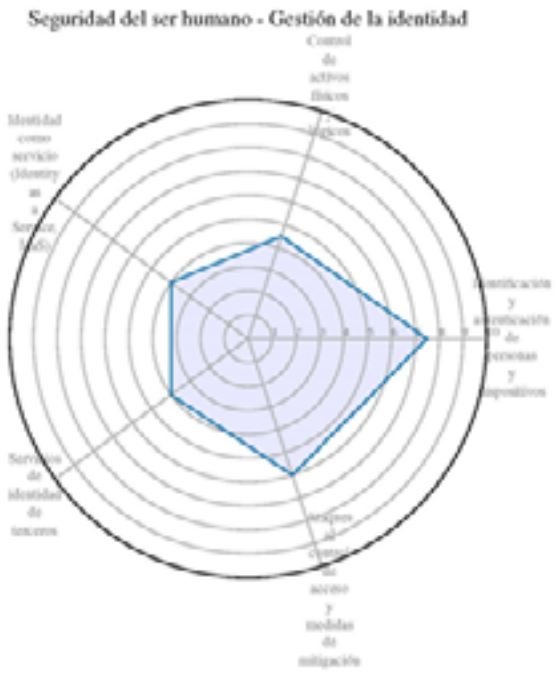


Figura 34 Soporte de temas de gestión de la identidad

4.6.2. Ingeniería social

La unidad de ingeniería social incluye los aspectos de tipos de ataques de ingeniería social, psicología de los ataques de ingeniería social, engañar a los usuarios y detección y mitigación de los ataques de ingeniería social.

El estudio refleja un soporte **medio/alto** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 35 Soporte de temas de Ingeniería social

4.6.3. Cumplimiento de las reglas/políticas/normas éticas de ciberseguridad

La unidad de cumplimiento de las reglas/políticas/normas éticas de ciberseguridad incluye los aspectos de mal uso del sistema y mal comportamiento de los usuarios, aplicación y normas de comportamiento y comportamiento adecuado en condiciones de incertidumbre.

El estudio refleja un soporte **muy bajo** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 36 Soporte de temas de cumplimiento de las reglas/políticas/normas éticas de ciberseguridad

4.6.4. Conciencia y comprensión

La unidad de conciencia y comprensión incluye los aspectos de percepción del riesgo y comunicación, ciberhigiene, educación de los usuarios en materia de ciberseguridad y conocimiento de las cibervulnerabilidades y amenazas.

El estudio refleja un soporte **bajo** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 37 Soporte de temas de conciencia y comprensión

4.6.5. Privacidad social y de comportamiento

La unidad de privacidad social y de comportamiento incluye los aspectos de teorías sociales de la privacidad y seguridad en las redes sociales.

El estudio refleja un soporte **muy bajo** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 38 Soporte de temas de privacidad social y de comportamiento

4.6.6. Privacidad y seguridad de los datos personales

La unidad de privacidad y seguridad de los datos personales incluye los aspectos de datos personales sensibles y seguimiento personal y huella digital.

El estudio refleja un soporte desigual en los temas de esta unidad de conocimiento, siendo **alto** para datos personales sensibles y **bajo** para seguimiento personal y huella digital. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 39 Soporte de temas de privacidad y seguridad de los datos personales.

4.6.7. Seguridad y privacidad aplicables

La unidad de seguridad y privacidad aplicables incluye los aspectos de usabilidad y experiencia del usuario, factores de seguridad humana, conocimiento y comprensión de la política, política de privacidad y orientación e implicaciones del diseño.

El estudio refleja un soporte **medio/bajo** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

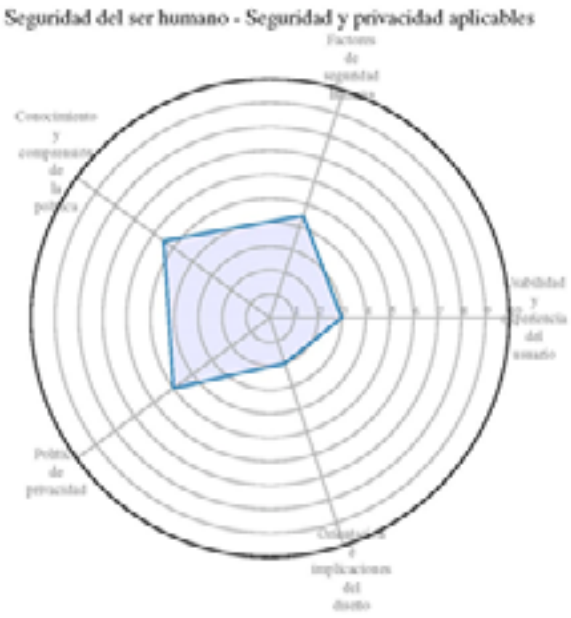
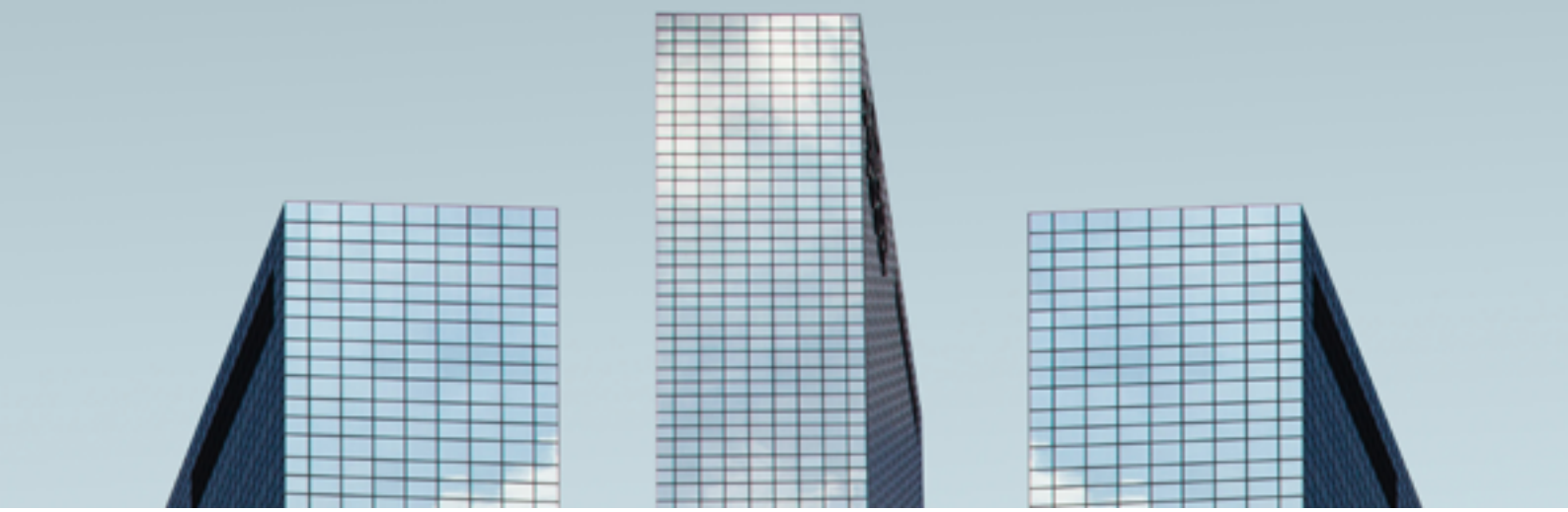


Figura 40 Soporte de temas de seguridad y privacidad aplicables



4.7. Área de Conocimiento KA-7: Seguridad de la organización

Se centra en proteger la información de las organizaciones y conlleva temas relativos a la gestión de riesgo.

Esta área cubre como contenidos la gestión de riesgos, la gobernanza y política, leyes, ética y cumplimiento y estrategia y planificación. Por ello, se divide en las siguientes unidades de conocimiento:

- Gestión de riesgos
- Gobernanza y política de seguridad
- Herramientas analíticas
- Administración de sistemas
- Planificación de la ciberseguridad
- Continuidad de negocio, recuperación de desastres y gestión de incidentes
- Gestión de programas de seguridad
- Seguridad del personal
- Operaciones de seguridad

4.7.1. Gestión de riesgos

La unidad de gestión de riesgos incluye los aspectos de identificación de riesgos, evaluación y análisis de riesgos, amenazas internas, modelos y metodologías de medición y evaluación de riesgos y control de riesgos.

El estudio refleja un soporte **alto** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

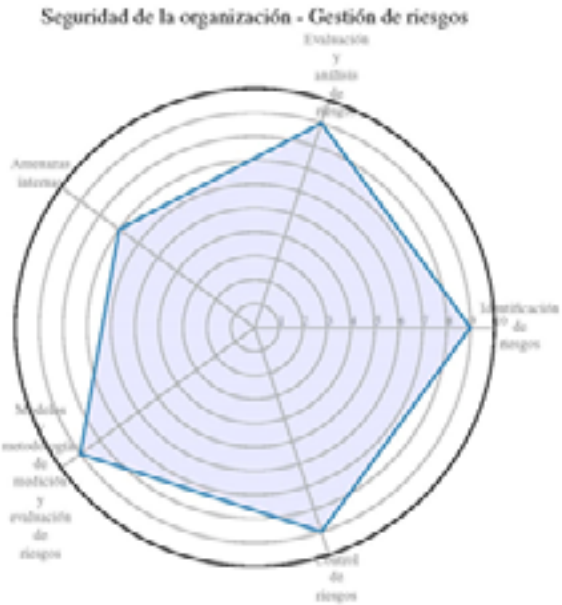


Figura 41 Soporte de temas de gestión de riesgos

4.7.2. Gobernanza y política de seguridad

La unidad de gobernanza y política de seguridad incluye los aspectos de contexto organizativo, privacidad, leyes, ética y cumplimiento, gobernanza de la seguridad, comunicación a nivel ejecutivo y del consejo de administración y política de gestión.

El estudio refleja un soporte **alto** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 42 Soporte de temas de gobernanza y política de seguridad

4.7.3. Herramientas analíticas

La unidad de herramientas analíticas incluye los aspectos de medidas de rendimiento (métricas), análisis de datos e inteligencia de seguridad.

El estudio refleja un soporte **medio** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 43 Soporte de temas de herramientas analíticas

4.7.4. Administración de sistemas

La unidad de administración de sistemas incluye los aspectos de administración de sistemas operativos, administración de sistemas de bases de datos, administración de redes, administración de la nube, administración de sistemas ciberfísicos, bastionado del sistema y disponibilidad.

El estudio refleja un soporte desigual en los temas de esta unidad de conocimiento, siendo **alto** para bastionado del sistema y **medio/bajo** para el resto. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 44 Soporte de temas de administración de sistemas

4.7.5. Planificación de la ciberseguridad

La unidad de planificación de la ciberseguridad incluye los aspectos de planificación estratégica y gestión operativa y táctica.

El estudio refleja un soporte **medio** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 45 Soporte de temas de planificación de la ciberseguridad

4.7.6. Continuidad de negocio, recuperación de desastres y gestión de incidentes

La unidad de continuidad de negocio, recuperación de desastres y gestión de incidentes incluye solo un tema sobre ese aspecto, y el estudio refleja un soporte **alto** de dicho tema.

4.7.7. Gestión de programas de seguridad

La unidad de gestión de programas de seguridad incluye los aspectos de gestión de proyectos, gestión de recursos, métricas de seguridad y garantía y control de calidad.

El estudio refleja un soporte **bajo** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

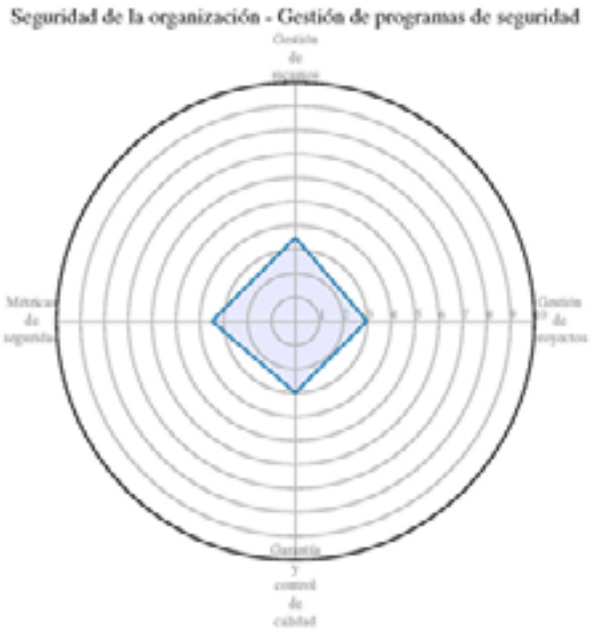


Figura 46 Soporte de temas de gestión de programas de seguridad

4.7.8. Seguridad del personal

La unidad de seguridad del personal incluye los aspectos de concienciación, formación y educación en materia de seguridad, prácticas de contratación de seguridad, prácticas de despido por motivos de seguridad, seguridad de terceros, seguridad en los procesos de revisión y cuestión especial en la privacidad de la información personal de los empleados.

El estudio refleja un soporte **bajo** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

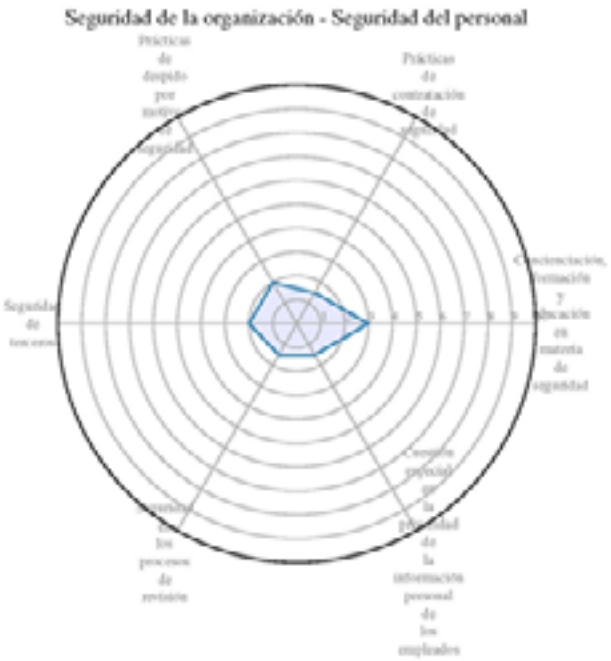


Figura 47 Soporte de temas de seguridad del personal

4.7.9. Operaciones de seguridad

La unidad de operaciones de seguridad incluye los aspectos de convergencia de la seguridad y centros de operaciones de seguridad global (Global Security Operations Centers, GSOC).

El estudio refleja un soporte **medio** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 48 Soporte de temas de operaciones de seguridad

4.8. Área de Conocimiento KA-8: Seguridad en la sociedad

Se centra en aspectos de la ciberseguridad que repercuten de manera positiva o negativa al conjunto de la sociedad.

Esta área cubre como contenidos la ciberdelincuencia (Cibercrimen), ciberderecho (cyber law), ciberética, ciberpolítica y privacidad. Por ello, se divide en las siguientes unidades de conocimiento:

- Ciberdelincuencia
- Ciberderecho
- Ciberética
- Ciberpolítica
- Privacidad

4.8.1. Ciberdelincuencia

La unidad de ciberdelincuencia incluye los aspectos de comportamiento cibercriminal, ciberterrorismo, Investigaciones cibercriminales y economía de la ciberdelincuencia.

El estudio refleja un soporte **medio** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 49 Soporte de temas de ciberdelincuencia

4.8.2. Ciberderecho

La unidad de ciberderecho incluye los aspectos de fundamentos constitucionales del ciberderecho, propiedad intelectual relacionada con la ciberseguridad, leyes de privacidad, derecho de la seguridad de los datos, leyes de piratería informática, pruebas digitales, contratos digitales, convenios multinacionales (acuerdos) y leyes transfronterizas de privacidad y seguridad de datos.

El estudio refleja un soporte desigual en los temas de esta unidad de conocimiento, siendo **altos** para los temas de leyes de privacidad, seguridad de datos y piratería informática y pruebas digitales y **bajos** para el resto de temas. El detalle de soporte de cada tema se muestra en la figura siguiente.

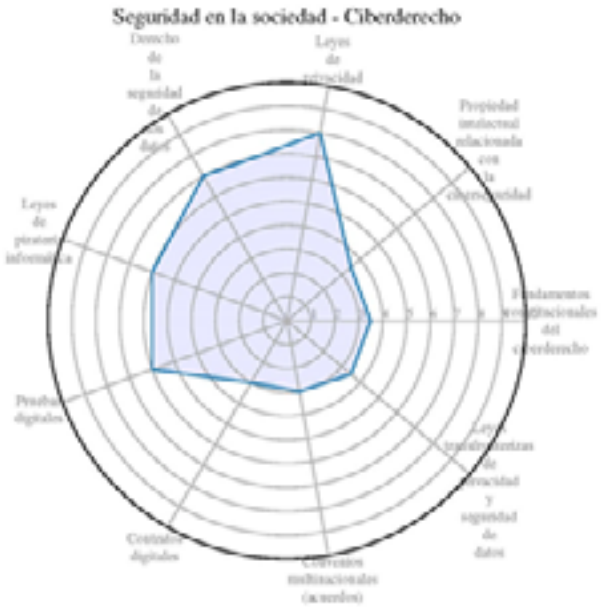


Figura 50 Soporte de temas de ciberderecho

4.8.3. Ciberética

La unidad de ciberética incluye los aspectos de definición de la ética, ética profesional y códigos de conducta, ética y equidad/diversidad, ética y derecho, autonomía/ética de los robots, ética y conflicto, hacking ético y marcos éticos y teorías normativas

El estudio refleja un soporte **bajo** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

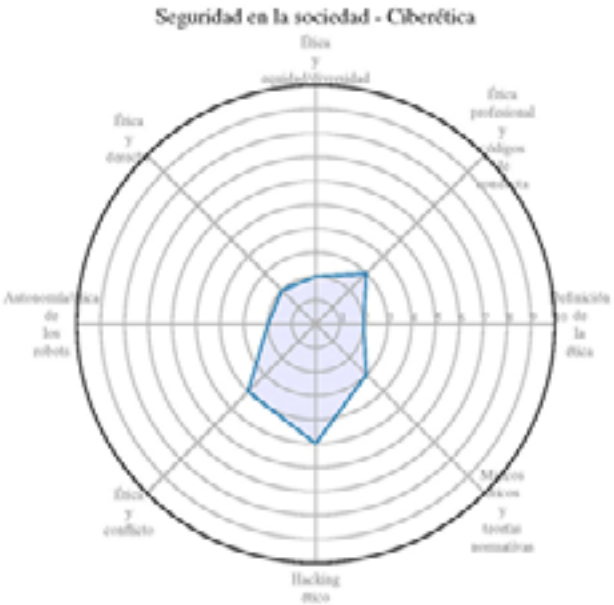


Figura 51 Soporte de temas de ciberética

4.8.4. Ciberpolítica

La unidad de ciberpolítica incluye los aspectos de ciberpolítica internacional, ciberpolítica de la UE, impacto global, política de ciberseguridad y seguridad nacional, implicaciones económicas nacionales de la ciberseguridad y nuevas adyacencias a la diplomacia.

El estudio refleja un soporte **bajo** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 52 Soporte de temas de ciberpolítca

4.8.5. Privacidad

La unidad de privacidad incluye los aspectos de definición de la privacidad, derecho a la intimidad, protección de la intimidad, normas y actitudes en materia de privacidad, violación de la intimidad y la privacidad en las sociedades.

El estudio refleja un soporte **medio** en los temas de esta unidad de conocimiento. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 53 Soporte de temas de privacidad

4.9. Conclusiones y resumen del soporte del marco curricular ACM/IEEE

En las secciones anteriores se han proporcionado los datos más relevantes sobre el soporte que tiene el Marco Curricular ACM/IEEE en Ciberseguridad en los programas de formación superior con especialización en el área de ciberseguridad en España. Este soporte se ha basado en una consulta a una muestra significativa de universidades públicas y privadas participantes en este grupo de trabajo del Foro Nacional de Ciberseguridad, a través de CRUE y RENIC (Red de Excelencia Nacional de Investigación en Ciberseguridad). La consulta incluía:

• Inclusión de cada uno de los temas (clasificados por áreas de conocimiento y unidades de conocimiento) en el programa formativo de dicha universidad, con una indicación de "inclusión significativa", "inclusión parcial" o "no soportado".

• Identificación de temas que son considerados en los programas formativos de las universidades como conocimientos previos necesarios para afrontar el programa formativo.

• Identificación de temas incluidos en los programas formativos que no están incluidos en el marco curricular ACM/IEEE en Ciberseguridad.

De esta consulta, se recibieron informes provenientes de:

• 10 Másteres especializados en ciberseguridad, de distintos puntos de España, oficiales y propios, y con distinta antigüedad.

• 2 grados especializados por completo o parcialmente en ciberseguridad, oficiales.

Estos informes se consideraron suficientes para la realización de este análisis, proporcionando una muestra significativa de la oferta formativa en formación superior especializada en ciberseguridad existente en España.

Las principales conclusiones de este estudio pueden resumirse de la siguiente forma:

• **Área de Seguridad del Dato**, con sus unidades de conocimiento de criptografía, análisis forense digital, integridad y autenticación de datos, control de acceso, protocolos de comunicación seguros, criptoanálisis, privacidad de datos, seguridad del almacenamiento de la información.

En general, todas las unidades de conocimiento tienen un soporte **alto o medio** por parte de los programas de formación superior. Solo temas concretos no son cubiertos, sobre todo aquellos relacionados con los modelos matemáticos, como los aspectos matemáticos relacionados con la criptografía, y aspectos de criptoanálisis.

• **Área de Seguridad del Software**, con sus unidades de conocimiento de principios fundamentales, diseño, implementación, análisis y pruebas, despliegue y mantenimiento, documentación y ética.

En general, las unidades de conocimiento principales tienen un soporte **alto o medio/alto** por parte de los programas de formación superior. Solo los temas relacionados con el despliegue y mantenimiento, documentación y ética tienen un soporte **bajo**.

• **Área de Seguridad de los Componentes**, con sus unidades de conocimiento de diseño de componentes, adquisición de componentes, pruebas de componentes e ingeniería inversa de componentes.

En general, las unidades de conocimiento tienen un soporte **bajo** por parte de los programas de formación superior, exceptuando el tema de ingeniería inversa software que es soportado con un nivel **medio**.

• **Área de Seguridad de las Conexiones**, con sus unidades de conocimiento de medios físicos, interfaces físicas y conectores, arquitectura de hardware, arquitectura de sistemas distribuidos, arquitectura de red, implementación de redes, servicios de red y defensa de la red.

Las unidades de conocimiento relacionadas con medios físicos, interfaces físicas y conectores y arquitectura de hardware tienen un soporte **nulo** por parte de los programas de formación superior ya que son considerados como conocimientos previos requeridos. Los temas de arquitectura de sistemas distribuidos, arquitectura de red, implementación de redes y servicios de red tienen un soporte **medio**, ya que se imparten, pero siguen siendo considerados como conocimientos previos. Sin embargo, los temas relacionados con las vulnerabilidades y la unidad de conocimiento de defensa de la red tienen un soporte **completo** en estos programas superiores de formación.

• **Área de Seguridad de Sistemas**, con sus unidades de conocimiento de pensamiento sistémico, gestión de sistemas, acceso al sistema, control del sistema, retirada del sistema, prueba del sistema y ejemplos de arquitecturas de sistemas.

El soporte de estas unidades de conocimiento es dispar. Por un lado, existen unidades de conocimientos con un soporte **nulo o muy bajo** ya que son consideradas como conocimientos previos, tales como pensamiento sistémico, pruebas del sistema y ejemplos de arquitecturas de sistemas. Por otro, se aprecia un soporte **medio** de la unidad de conocimiento de gestión de sistemas y un soporte **alto o muy alto** de las unidades de conocimiento de acceso al sistema y control del sistema. La unidad de conocimiento de retirada del sistema tiene un soporte **nulo**, no es tratada por ninguno de los programas consultados.

• **Área de Seguridad del Ser Humano**, con sus unidades de conocimiento de gestión de la identidad, ingeniería social, cumplimiento de las reglas / políticas / normas éticas de ciberseguridad, conciencia y comprensión, privacidad social y de comportamiento, privacidad y seguridad de los datos personales y seguridad y privacidad aplicables.

El soporte de estas unidades de conocimiento es dispar: Por un lado, existen unidades de conocimientos con un soporte **alto o medio**, como la gestión de la identidad, ingeniería social y privacidad y seguridad de los datos personales, y un soporte **bajo o medio/bajo** en el resto de unidades de conocimiento: cumplimiento de las reglas/políticas/normas éticas de ciberseguridad, conciencia y comprensión, privacidad social y de comportamiento y seguridad y privacidad aplicables.

• **Área de Seguridad de la Organización**, con sus unidades de conocimiento de gestión de riesgos, gobernanza y política de seguridad, herramientas analíticas, administración de sistemas, planificación de la ciberseguridad, continuidad de negocio, recuperación de desastres y gestión de incidentes, gestión de programas de seguridad, seguridad del personal y operaciones de seguridad.

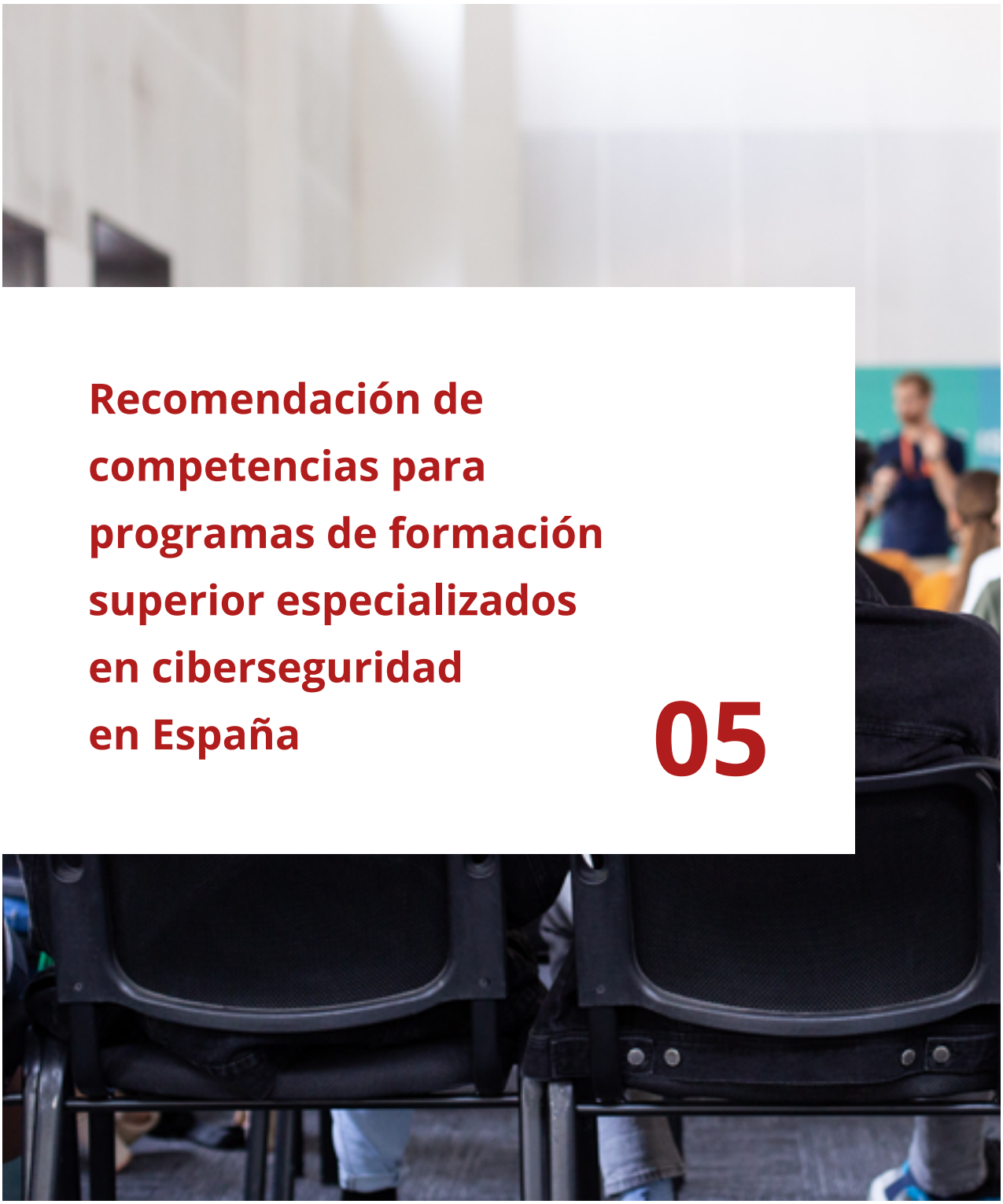
En general, las unidades de conocimiento principales tienen un soporte **alto o medio/alto** por parte de los programas de formación superior, con la salvedad de las unidades de conocimiento de administración de sistemas, cuyos temas son considerados como conocimientos previos (excepto el bastionado), la gestión de programas de seguridad y la seguridad del personal, que tienen un soporte **bajo**.

• **Área de Seguridad en la Sociedad**, con sus unidades de conocimiento de ciberdelincuencia, ciberderecho, ciberética, ciberpolítica y privacidad.

En general, las unidades de conocimiento tienen un soporte **medio** por parte de los programas de formación superior, aunque las unidades de conocimiento de ciberética y ciberpolítica tienen un soporte **bajo**.

Por último, destacar que las consultas a estos programas de formación superior incluyen el soporte a la formación en algunas áreas que no están incluidas expresamente en el marco curricular ACM/IEEE en Ciberseguridad, y que son las siguientes:

- Seguridad Ofensiva:
  - Análisis de Vulnerabilidades
  - Técnicas de Explotación
  - Análisis de Amenazas
- Auditoría:
  - Papel de la auditoría
  - Ámbito y objetivos de la auditoría
  - Tipos de auditoría, marcos, técnicas y herramientas
  - Acuerdos y documentación
- Otros:
  - Protección de los perímetros
  - Vigilancia e Inteligencia
  - Detección de Intrusiones
  - Esteganografía



Recomendación de competencias para programas de formación superior especializados en ciberseguridad en España

05

Las secciones anteriores de este documento han servido para analizar el soporte que tiene el Marco Curricular ACM/IEEE en Ciberseguridad en los programas de formación superior con especialización en el área de ciberseguridad que se imparten actualmente en España. Este análisis permite comprender que la cobertura de ciertos temas (clasificados por áreas de conocimiento y unidades de conocimiento) es alta o media, mientras que la de otros es baja o nula ya que se identifican como conocimientos previos. Incluso se han identificado algunos temas que suelen incluirse en los programas formativos, a pesar de que no estén incluidos en el marco curricular ACM/IEEE.

La elección de los temas que se incluyen en los programas formativos analizados se fundamenta en las competencias que se pretende que tengan los egresados de dichos programas. Pero no existe un marco de competencias específicas del que se pueda partir para diseñar los planes de estudios especializados en ciberseguridad. Es por este motivo que las competencias de los programas analizados varían considerablemente, tanto en su redacción como en su contenido. El objetivo del resto del presente documento es justo éste: proponer un marco de competencias que facilite el diseño de planes de estudios especializados.

Este marco de referencia permitirá a los centros de formación superior escoger aquellas competencias que consideren más oportunas para el perfil de egresado que desean formar y a partir de ellas, por ejemplo, utilizando el marco curricular ACM/IEEE, proponer los temas y unidades de conocimiento que deben incluirse en los planes de estudios. Es decir, se pretende proporcionar una herramienta que reduzca la dificultad de los procesos de diseño de planes de estudios especializados, permitiendo a las instituciones responsables de este proceso seleccionar las competencias de entre un conjunto compartido o común, completo y actualizado, validado por expertos en la materia y ajustado a las necesidades del mercado laboral a medio plazo.

Se persigue además un objetivo adicional, que el marco de competencias propuesto permita mejorar la colaboración entre la academia y la industria. Mientras que en el primer ámbito las competencias son el punto de partida para el diseño de los planes de estudios, en el segundo son el punto de partida para la definición de perfiles y roles dentro de las organizaciones. El marco de competencias propuesto permitirá, gracias a la estandarización proporcionada, aproximar el lenguaje que se utiliza en ambos contextos, permitiendo a las universidades que los estudiantes egresados de sus títulos respondan mejor a las necesidades del mercado laboral y a las organizaciones tener expectativas realistas respecto a las actividades y tareas que estos egresados puedan llevar a cabo con garantías cuando finalizan sus estudios.

5.1. Metodología

Para proponer el marco de competencias se ha partido de una consulta a los futuros empleadores de los egresados de programas formativos especializados en ciberseguridad, tanto en el sector público como en el privado.

Esta consulta se ha realizado mediante un formulario de recogida de información (anexo I de este documento) que debían responder personas con perfiles concretos dentro de estos potenciales empleadores (personas con responsabilidad técnica en departamentos de IT, seguridad o similares). Contestar el cuestionario requería de un tiempo aproximado entre los 30 y 40 minutos.

El objetivo era recoger información sobre las actividades y tareas que necesitarán realizar los profesionales de la ciberseguridad en el medio o largo plazo. El objetivo no era analizar el mercado laboral ni el organigrama actual de las organizaciones, sino investigar acerca de las competencias más adecuadas para los futuros planes de estudios especializados en función de los perfiles que los empleadores van a necesitar.

En este formulario se mostraban diez funciones/áreas diferentes de la ciberseguridad (tabla 5.1). Para cada una de ellas se identificaban una serie de tareas o actividades inspiradas en el marco propuesto por el NICE [NICE2017]. La persona que respondía el formulario debía usar la escala de Likert (1- nunca, 2 -casi nunca, 3 -ocasionalmente, 4 - a menudo, 5 - constantemente) para indicar si esa tarea o actividad se desarrolla en su organización, independientemente de la denominación que tenga el puesto o rol de la persona que la desempeñe o de si se centra en activos IT, OT, en la nube, etc. Se pedía que la respuesta no tuviera en cuenta sólo lo que ocurre actualmente, sino también la tendencia a medio o largo plazo. Es decir, lo que se espera que ocurra en los próximos años.

Arquitectura
Desarrollo y producto
Ingeniería y administración
Análisis
Detección y respuesta
Investigación
Responsabilidad y dirección
Ingeniería de la confiabilidad
Auditoría
Formación, concienciación y sensibilización

Tabla 5.1. Funciones/áreas consideradas para la definición del marco de competencias

Aunque la mayor parte de estas funciones o áreas son auto-explicativas dada su denominación, cabe aclarar que la función o área de Ingeniería de la confiabilidad incluye todos los aspectos relativos a privacy, reliability, resilience y safety.

En una última sección se pedía que, una vez comprendidas las tareas y actividades que se asocian a cada función/área, se priorizaran las diez que habían identificado teniendo en cuenta la importancia para la organización.

Para que la muestra fuera representativa, el formulario se hizo llegar en el mes de septiembre del 2021 a representantes de los sectores de actividad mostrados en la tabla 5.2. El tamaño de la muestra fue de 95 personas, durante el mes de octubre se analizaron y procesaron las 46 respuestas completas recibidas en ese momento.

En paralelo a este proceso, se trabajó en identificar un conjunto plano de competencias específicas asociadas a las tareas y actividades listadas dentro de cada función/área. Es decir, se analizaron las competencias esenciales para que un profesional lleve a cabo cada una de estas tareas o actividades. Una vez recibidas las respuestas de los formularios, se priorizaron unas competencias frente a otras (teniendo en cuenta las necesidades de los potenciales empleadores) de manera que se listaran entre 10 y 20 competencias por función/área, aquellas necesarias para poder realizar las tareas y actividades más importantes para las organizaciones que habían respondido al formulario de recogida de información.

Sector privado	Sector público
Big Four (consultoras de mayor tamaño)	Administración central
Consultoras especializadas	Administración autonómica
Ingenierías	Administración local
Fabricantes de software y empresas de desarrollo	Justicia
Fabricantes/proveedores del sector de la ciberseguridad	Sanidad
Banca	Educación y universidades
Seguros, mutuas y sanidad privada	Fuerzas Armadas
Operadores de telecomunicaciones	Fuerzas y cuerpos de seguridad del Estado y policías autonómicas
Otros proveedores tecnológicos	Centros de investigación y tecnológicos
Centros de investigación y tecnológicos	
Defensa	
Logística	
Energía	
Transporte	
Aeroespacial	
Aguas	
Industria y manufactura	
Marketing y medios de comunicación	

Tabla 5.2. Sectores de actividad consultados para la definición del marco de competencias

5.2. Listado de competencias específicas

Una vez realizado el proceso explicado en la sección anterior, se propone el siguiente marco de competencias específicas para programas formativos en seguridad, categorizando las competencias según la función/área con la que están más relacionadas.

Cabe exponer algunas aclaraciones sobre este marco de competencias. La primera, se ha tenido en cuenta la definición de competencias de la Organización para la Cooperación y Desarrollo Económico que se ha trasladado al Espacio Europeo de Educación Superior. Esto implica que las competencias son habilidades y capacidades adquiridas a través de un esfuerzo deliberado y sistemático por realizar actividades complejas. De esta forma, no se limitan a comportamiento observables, sino que combinan conocimientos, habilidades, actitudes y motivaciones. Una competencia no se centra sólo en los elementos cognitivos (teorías, conceptos o conocimientos), sino que abarca tanto habilidades técnicas como atributos interpersonales [OECD2001].

En resumen, las competencias que se proponen a continuación permiten al egresado de un título universitario realizar con garantías de éxito las tareas y actividades por las que se preguntó en el formulario disponible en el anexo I para cada área o función.

La segunda, se han empleado para la redacción de las competencias verbos que reflejen esta consideración y que se ajusten a los niveles 3 y 4 de la taxonomía de Bloom en su mayoría, Aplicación y Análisis respectivamente [P2018]. En algunos casos excepcionales, se ha recurrido a verbos en los niveles 5 y 6 (Síntesis y Evaluación) o en los niveles 1 y 2 (Conocimiento y Comprensión). Pero dado que el objetivo es definir competencias para programas universitarios, estos dos niveles, el 3 y el 4 se han considerado los más adecuados, por norma general, para títulos tanto de grado como de post-grado.

5.2.1. Competencias asociadas con el área de ARQUITECTURA

CE1	Recolectar y definir las capacidades y requisitos de seguridad de los sistemas.
CE2	Realizar procesos de análisis del riesgo y seleccionar las estrategias más adecuadas para gestionar los riesgos identificados en función de la tolerancia de la organización.
CE3	Aplicar y analizar la aplicación de los principios básicos de la ciberseguridad y la privacidad durante el desarrollo, despliegue, instalación, integración, mantenimiento y optimización de sistemas.
CE4	Conocer y aplicar métodos y técnicas específicas de depuración, prueba, validación y evaluación de la seguridad de los sistemas, y documentar adecuadamente el diseño, implementación, mantenimiento y operación de la seguridad de dichos sistemas.
CE5	Supervisar la integración de las metas y los objetivos de la organización en la arquitectura de seguridad y en su configuración.
CE6	Comprender las tendencias y los conceptos arquitectónicos de las tecnologías de la información para el diseño de la arquitectura de seguridad.
CE7	Determinar cómo debe funcionar un sistema de seguridad (incluidas sus capacidades de resiliencia y confiabilidad) y cómo los cambios en las condiciones, las operaciones o el entorno afectarán a este funcionamiento.
CE8	Comprender y categorizar los impactos operativos específicos de las debilidades y vulnerabilidades de los activos.
CE9	Conocer y aplicar mecanismos de cifrado de datos y de gestión de claves.
CE10	Diseñar y aplicar adecuadamente los distintos métodos de autenticación, autorización y control de acceso.
CE11	Conocer y analizar los métodos y mejores prácticas para realizar gestión segura de configuraciones.
CE12	Diseñar la arquitectura de la red, en relación con los objetivos de seguridad y los objetivos operativos.
CE13	Apoyar en la adquisición y contratación de mecanismos y servicios de seguridad, garantizando una gestión adecuada de la cadena de suministro.
CE14	Conocer la naturaleza y la función de la Estructura de Información pertinente (por ejemplo, Computer Emegency Response Team de referencia).
CE15	Conocer y aplicar conceptos de mejora de procesos organizativos y modelos de madurez de procesos.

CE16	Interpretar y aplicar las leyes, las regulaciones, las políticas y principios éticos en relación con la ciberseguridad y la confiabilidad.
CE17	Diferenciar los modelos de seguridad y su relación con los estándares del sector de la ciberseguridad.

5.2.2. Competencias asociadas con el área de DESARROLLO Y PRODUCTO

CE1	Recolectar y definir las capacidades y requisitos de seguridad de los sistemas.
CE18	Conocer y entender los requisitos de funcionalidad, calidad y seguridad, y la manera en que estos se aplican a elementos específicos del suministro.
CE2	Realizar procesos de análisis del riesgo y seleccionar las estrategias más adecuadas para gestionar los riesgos identificados en función de la tolerancia de la organización.
CE3	Aplicar y analizar la aplicación de los principios básicos de la ciberseguridad y la privacidad durante el desarrollo, despliegue, instalación, integración, mantenimiento y optimización de sistemas.
CE4	Conocer y aplicar métodos y técnicas específicas de depuración, prueba, validación y evaluación de la seguridad de los sistemas, y documentar adecuadamente el diseño, implementación, mantenimiento y operación de la seguridad de dichos sistemas.
CE6	Comprender las tendencias y los conceptos arquitectónicos de las tecnologías de la información para el diseño de la arquitectura de seguridad.
CE19	Conocer las vulnerabilidades más frecuentes de las aplicaciones, y los métodos y técnicas para descubrirlas y solventarlas.
CE20	Analizar la superficie de exposición de un software y producir modelos de amenazas dentro de procesos de desarrollo de software.
CE21	Utilizar los principios y métodos de seguridad y confiabilidad en procesos de ingeniería del software para producir software seguro desde el diseño.
CE22	Producir software siguiendo ciclos de vida, metodologías y prácticas de desarrollo seguros.
CE23	Conocer y saber aplicar las mejores prácticas en codificación segura para los lenguajes de programación y plataformas más extendidos.
CE24	Seleccionar, desplegar, configurar y mantener capacidades de protección de aplicaciones como diferentes tipos de filtros, firewalls de aplicación, etc.

CE25	Comprender las implicaciones que la configuración del software, o de su relación con otros componentes de los sistemas, pueden tener para la seguridad.
CE26	Investigar los vectores de ataque y amenazas actuales y emergentes que pueden afectar a una organización, apoyándose en diferentes fuentes de información privadas o públicas (boletines, alertas, etc.).
CE16	Interpretar y aplicar las leyes, las regulaciones, las políticas y principios éticos en relación con la ciberseguridad y la confiabilidad.
CE27	Conocer las principales categorías de incidentes de seguridad y seleccionar las metodologías más adecuadas para responder ante ellos y gestionarlos según el contexto y la responsabilidad.

5.2.3. Competencias asociadas con el área de INGENIERÍA Y ADMINISTRACIÓN

CE2	Realizar procesos de análisis del riesgo y seleccionar las estrategias más adecuadas para gestionar los riesgos identificados en función de la tolerancia de la organización.
CE28	Aplicar los principios básicos de la ciberseguridad y la privacidad para gestionar los riesgos relacionados con el uso, el procesamiento, el almacenamiento y la transmisión de información o datos.
CE4	Conocer y aplicar métodos y técnicas específicas de depuración, prueba, validación y evaluación de la seguridad de los sistemas, y documentar adecuadamente el diseño, implementación, mantenimiento y operación de la seguridad de dichos sistemas.
CE29	Seleccionar e interpretar indicadores de rendimiento y disponibilidad de sistemas.
CE30	Implementar, mantener y supervisar mecanismos de control de acceso a la red o los activos (por ejemplo, listas de control de acceso, capacidades).
CE31	Realizar copias de seguridad y recuperación de datos.
CE32	Realizar procesos de parcheo y actualización de sistemas y aplicaciones y analizar la conveniencia de dichos procesos en diferentes escenarios.
CE11	Conocer y analizar los métodos y mejores prácticas para realizar gestión segura de configuraciones.
CE33	Escoger, configurar y utilizar capacidades y herramientas de prevención y detección de intrusiones en hosts y redes.
CE34	Proteger y fortificar sistemas operativos, aplicaciones y redes aplicando métodos de defensa en profundidad.
CE27	Conocer las principales categorías de incidentes de seguridad y seleccionar las metodologías más adecuadas para responder ante ellos y gestionarlos según el contexto y la responsabilidad.

CE35	Comprender la seguridad de la cadena de suministro de las tecnologías de la información y conocer políticas, requisitos y procedimientos para gestionar los riesgos asociados a la misma.
CE36	Diseñar, desplegar, supervisar y seleccionar políticas, procesos y actividades de formación, concienciación y sensibilización.
CE37	Entender y participar en las operaciones y procesos que gestionan eventos e incidentes.

5.2.4 Competencias asociadas con el área de ANÁLISIS

CE3	Aplicar y analizar la aplicación de los principios básicos de la ciberseguridad y la privacidad durante el desarrollo, despliegue, instalación, integración, mantenimiento y optimización de sistemas.
CE2	Realizar procesos de análisis del riesgo y seleccionar las estrategias más adecuadas para gestionar los riesgos identificados en función de la tolerancia de la organización.
CE4	Conocer y aplicar métodos y técnicas específicas de depuración, prueba, validación y evaluación de la seguridad de los sistemas, y documentar adecuadamente el diseño, implementación, mantenimiento y operación de la seguridad de dichos sistemas.
CE38	Investigar y evaluar la fiabilidad de un servicio o producto y de su proveedor.
CE39	Utilizar herramientas de análisis de tráfico de red para identificar vulnerabilidades y anomalías.
CE19	Conocer las vulnerabilidades más frecuentes de las aplicaciones, y los métodos y técnicas para descubrirlas y solventarlas.
CE40	Llevar a cabo tests de penetración aplicando y utilizando los principios, técnicas y herramientas más adecuadas y conociendo las principales tácticas, técnicas y procedimientos (TTP) utilizadas por los adversarios.
CE41	Analizar y distinguir las diferentes clases de ataques y sus fases o etapas.
CE42	Aplicar principios y técnicas para realizar procesos de hacking ético.
CE43	Simular las tácticas, técnicas y procedimientos (TTP) utilizadas por los adversarios para poder emularlas o anticiparse a sus posibles impactos.
CE26	Investigar los vectores de ataque y amenazas actuales y emergentes que pueden afectar a una organización, apoyándose en diferentes fuentes de información privadas o públicas (boletines, alertas, etc.).
CE44	Investigar los vectores de ataque y amenazas actuales y emergentes que pueden afectar a una organización, apoyándose en diferentes fuentes de información privadas o públicas (boletines, alertas, etc.).

CE20	Aplicar técnicas de ingeniería inversa en activos hardware y software y analizar archivos binarios.
CE45	Entender las técnicas de análisis forense existentes, aplicarlas según proceda y proporcionar recomendaciones tras el análisis realizado.
CE46	Conocer las tácticas, técnicas y procedimientos que pueden ser utilizadas para que un análisis forense no revele la realidad (anti-forense).
CE47	Comprender el malware y generar firmas que resuman su comportamiento.
CE48	Utilizar herramientas de análisis de malware y conocer los conceptos y metodologías asociados a este análisis.

5.2.5. Competencias asociadas con el área de DETECCIÓN Y RESPUESTA

CE41	Analizar y distinguir las diferentes clases de ataques y sus fases o etapas.
CE49	Aplicar los principios de extracción, transformación y almacenamiento de datos y saber automatizarlos.
CE50	Conocer y aplicar métodos estándar para recoger y diseminar información relativa a la evaluación, monitorización, vigilancia y recuperación de la seguridad.
CE4	Conocer y aplicar métodos y técnicas específicas de depuración, prueba, validación y evaluación de la seguridad de los sistemas, y documentar adecuadamente el diseño, implementación, mantenimiento y operación de la seguridad de dichos sistemas.
CE29	Seleccionar e interpretar indicadores de rendimiento y disponibilidad de sistemas.
CE51	Localizar y analizar archivos de sistema con información relevante para la seguridad (archivos de registro de actividad, archivos de configuración, etc.).
CE39	Utilizar herramientas de análisis de tráfico de red para identificar vulnerabilidades y anomalías.
CE52	Seleccionar, preparar o implementar herramientas de correlación de eventos de seguridad.
CE33	Escoger, configurar y utilizar capacidades y herramientas de prevención y detección de intrusiones en hosts y redes.
CE27	Conocer las principales categorías de incidentes de seguridad y seleccionar las metodologías más adecuadas para responder ante ellos y gestionarlos según el contexto y la responsabilidad.
CE26	Investigar los vectores de ataque y amenazas actuales y emergentes que pueden afectar a una organización, apoyándose en diferentes fuentes de información privadas o públicas (boletines, alertas, etc.).
CE31	Realizar copias de seguridad y recuperación de datos.

CE53	Recoger, custodiar y presentar pruebas y evidencias válidos en procedimientos judiciales.
CE45	Entender las técnicas de análisis forense existentes, aplicarlas según proceda y proporcionar recomendaciones tras el análisis realizado.
CE36	Diseñar, desplegar, supervisar y seleccionar políticas, procesos y actividades de formación, concienciación y sensibilización.
CE16	Interpretar y aplicar las leyes, las regulaciones, las políticas y principios éticos en relación con la ciberseguridad y la confiabilidad.

5.2.6. Competencias asociadas con el área de INVESTIGACIÓN

CE54	Identificar problemas y retos de ciberseguridad en las tecnologías de la información actuales y emergentes.
CE55	Conocer el estado del mercado y la industria nacional e internacional de ciberseguridad, así como distinguir las tareas, conocimientos, destrezas y habilidades de los diferentes roles de trabajo asociados.
CE3	Aplicar y analizar la aplicación de los principios básicos de la ciberseguridad y la privacidad durante el desarrollo, despliegue, instalación, integración, mantenimiento y optimización de sistemas.
CE56	Entender cómo aprovechar los centros de investigación y desarrollo, los grupos de reflexión, la investigación académica y los sistemas de protección de propiedad intelectual o industrial, para llevar a cabo proyectos de investigación, innovación y transferencia.
CE57	Usar entornos de trabajo colaborativos empleando herramientas y plataformas de colaboración, y aprovechando y aportando experiencia analítica y técnica en grupos con otros analistas y expertos, tanto internos como externos a la organización.
CE50	Conocer y aplicar métodos estándar para recoger y diseminar información relativa a la evaluación, monitorización, vigilancia y recuperación de la seguridad.
CE58	Definir y liderar los procedimientos pertinentes de publicación y difusión de resultados de investigación teniendo en cuenta la protección la propiedad intelectual e industrial.
CE16	Interpretar y aplicar las leyes, las regulaciones, las políticas y principios éticos en relación con la ciberseguridad y la confiabilidad.

5.2.7. Competencias asociadas con el área de RESPONSABILIDAD Y DIRECCIÓN

CE28	Aplicar los principios básicos de la ciberseguridad y la privacidad para gestionar los riesgos relacionados con el uso, el procesamiento, el almacenamiento y la transmisión de información o datos.
CE27	Conocer las principales categorías de incidentes de seguridad y seleccionar las metodologías más adecuadas para responder ante ellos y gestionarlos según el contexto y la responsabilidad.
CE59	Diseñar, desplegar, supervisar, medir y mejorar planes de continuidad de operaciones, de continuidad de negocio, de contingencia y de recuperación ante desastres, así como programas a diferentes niveles.
CE50	Conocer y aplicar métodos estándar para recoger y diseminar información relativa a la evaluación, monitorización, vigilancia y recuperación de la seguridad.
CE35	Comprender la seguridad de la cadena de suministro de las tecnologías de la información y conocer políticas, requisitos y procedimientos para gestionar los riesgos asociados a la misma.
CE36	Diseñar, desplegar, supervisar y seleccionar políticas, procesos y actividades de formación, concienciación y sensibilización.
CE60	Conocer las leyes, políticas, procedimientos, marcos normativos y reglamentos que de forma explícita describan obligaciones y requerimientos relacionados con la gestión de la ciberseguridad en los diversos entornos en que son de aplicación (incluidas las infraestructuras críticas).
CE61	Conocer y saber aplicar mejores prácticas, guías y recomendaciones para la gobernanza de la seguridad.
CE62	Utilizar normas, marcos y metodologías que permitan categorizar y clasificar las fuentes de información y el uso y características de los datos utilizados en una organización, según su sensibilidad y otros factores de riesgo.
CE63	Planificar el proceso organizativo relacionado con la dotación de recursos y personal dedicado a la ciberseguridad.
CE64	Establecer los requisitos de adquisición y compras de tecnologías de la información.

5.2.8. Competencias asociadas con el área de INGENIERÍA DE LA CONFIABILIDAD

CE16	Interpretar y aplicar las leyes, las regulaciones, las políticas y principios éticos en relación con la ciberseguridad y la confiabilidad.
CE65	Realizar evaluaciones de impacto para la privacidad.
CE28	Aplicar los principios básicos de la ciberseguridad y la privacidad para gestionar los riesgos relacionados con el uso, el procesamiento, el almacenamiento y la transmisión de información o datos.
CE62	Utilizar normas, marcos y metodologías que permitan categorizar y clasificar las fuentes de información y el uso y características de los datos utilizados en una organización, según su sensibilidad y otros factores de riesgo.
CE66	Diseñar y ejecutar los programas y procedimientos de clasificación de la información de una organización, así como los procedimientos en caso de incidentes.
CE9	Conocer y aplicar mecanismos de cifrado de datos y de gestión de claves.
CE67	Conocer y aplicar mecanismos de gestión de identidades y accesos.
CE68	Utilizar los principios y métodos de ciberseguridad y confiabilidad en procesos de ingeniería del software para producir software seguro desde el diseño.
CE60	Conocer las leyes, políticas, procedimientos, marcos normativos y reglamentos que de forma explícita describan obligaciones y requerimientos relacionados con la gestión de la ciberseguridad en los diversos entornos en que son de aplicación (incluidas las infraestructuras críticas).
CE69	Comprender estándares y normas relacionados con la gestión de datos PII (Personally Identifiable Information).
CE7	Determinar cómo debe funcionar un sistema de seguridad (incluidas sus capacidades de resiliencia y confiabilidad) y cómo los cambios en las condiciones, las operaciones o el entorno afectarán a este funcionamiento.
CE70	Analizar los niveles de redundancia y resiliencia de los sistemas asociados a infraestructuras críticas.
CE71	Diseñar, desplegar, mantener y operar la que soporta las tecnologías de la información desplegadas en una organización de manera que se garantice la confiabilidad.
CE72	Conocer y saber aplicar estándares y normas relacionados con la gestión de datos PCI (Payment Card Industry), PHI (Personal Heath Information) o de otros dominios especialmente sensibles.
CE37	Entender y participar en las operaciones y procesos que gestionan eventos e incidentes.
CE53	Recoger, custodiar y presentar pruebas y evidencias válidas en procedimientos judiciales.

5.2.9. Competencias asociadas con el área de AUDITORÍA

CE16	Interpretar y aplicar las leyes, las regulaciones, las políticas y principios éticos en relación con la ciberseguridad y la confiabilidad.
CE73	Habilitar y documentar el proceso de evaluación y autorización de la seguridad.
CE74	Conocer y auditar principios como los de mínimo privilegio o segregación de funciones.
CE28	Aplicar los principios básicos de la ciberseguridad y la privacidad para gestionar los riesgos relacionados con el uso, el procesamiento, el almacenamiento y la transmisión de información o datos.
CE62	Utilizar normas, marcos y metodologías que permitan categorizar y clasificar las fuentes de información y el uso y características de los datos utilizados en una organización, según su sensibilidad y otros factores de riesgo.
CE15	Conocer y aplicar conceptos de mejora de procesos organizativos y modelos de madurez de procesos.
CE75	Conocer y entender los requisitos de funcionalidad, calidad y seguridad, y la manera en que estos se aplican a elementos específicos del suministro.
CE17	Diferenciar los modelos de seguridad y su relación con los estándares del sector de la ciberseguridad.
CE50	Conocer y aplicar métodos estándar para recoger y diseminar información relativa a la evaluación, monitorización, vigilancia y recuperación de la seguridad.
CE60	Conocer las leyes, políticas, procedimientos, marcos normativos y reglamentos que de forma explícita describan obligaciones y requerimientos relacionados con la gestión de la ciberseguridad en los diversos entornos en que son de aplicación (incluidas las infraestructuras críticas).
CE4	Conocer y aplicar métodos y técnicas específicas de depuración, prueba, validación y evaluación de la seguridad de los sistemas, y documentar adecuadamente el diseño, implementación, mantenimiento y operación de la seguridad de dichos sistemas.
CE7	Determinar cómo debe funcionar un sistema de seguridad (incluidas sus capacidades de resiliencia y confiabilidad) y cómo los cambios en las condiciones, las operaciones o el entorno afectarán a este funcionamiento.
CE11	Conocer y analizar los métodos y mejores prácticas para realizar gestión segura de configuraciones.
CE35	Comprender la seguridad de la cadena de suministro de las tecnologías de la información y conocer políticas, requisitos y procedimientos para gestionar los riesgos asociados a la misma.
CE76	Identificar los problemas de ciberseguridad y privacidad que surgen de las conexiones con clientes y socios internos o externos.

5.2.10. Competencias asociadas con el área de FORMACIÓN, CONCIENCIACIÓN Y SENSIBILIZACIÓN

CE8	Comprender y categorizar los impactos operativos específicos de las debilidades y vulnerabilidades de los activos.
CE77	Analizar políticas, procesos y procedimientos de formación, concienciación y sensibilización de la organización, contribuyendo a evaluar sus necesidades presentes y futuras.
CE36	Diseñar, desplegar, supervisar y seleccionar políticas, procesos y actividades de formación, concienciación y sensibilización.
CE78	Seleccionar los principios y métodos de enseñanza-aprendizaje más adecuados para diferentes personas y grupos, e interpretar los impactos producidos.
CE79	Aplicar niveles (es decir, la taxonomía de aprendizaje de Bloom), modos y estilos de aprendizaje.
CE80	Aplicar técnicas y métodos de producción, comunicación y difusión de los medios de comunicación, incluidas maneras alternativas de informar a través de medios escritos, orales y visuales.
CE81	Diseñar y aplicar técnicas de prueba y evaluación del aprendizaje (rúbricas, planes de evaluación, exámenes, pruebas cortas).
CE82	Incorporar el uso del ordenador en la formación, incluyendo servicios de aprendizaje en línea, técnicas de virtualización, etc.
CE83	Realizar o supervisar competiciones de ciberseguridad como una forma para desarrollar habilidades por medio de experiencias prácticas en situaciones simuladas del mundo real.

5.3. Listado de pre-requisitos

El marco de competencias propuesto en la sección anterior recoge competencias específicas relacionadas con las diez áreas que se han tenido en cuenta en la fase de recogida de información inicial realizada mediante el envío del formulario (anexo I). Durante el diseño de un plan de estudios será necesario traducir estas competencias a materias, asignaturas y contenidos o unidades temáticas.

En este proceso, se identificarán pre-requisitos o conocimientos previos necesarios, es decir, condiciones que los estudiantes deben cumplir para poder cursar estas materias o asignaturas y ser evaluados. Dependiendo del tipo de plan de estudios que se esté diseñando, grado o post-grado, estos pre-requisitos llevarán a la definición de nuevas competencias específicas (asociadas a asignaturas de los primeros cursos de un grado, por ejemplo) o permitirán identificar los requisitos de acceso a la titulación (materias que habrá sido necesario cursar antes de ser admitido en un post-grado, por ejemplo).

Se proporciona a continuación un listado de conocimientos específicos que pueden traducirse en el proceso de diseño de un plan de estudios en ciberseguridad a nuevas competencias específicas (grado) o a requisitos de acceso (post-grado). Se expresan de momento con el concepto genérico de "conocimiento" para que en cada plan de estudios se redacten de la manera más adecuada en función de su papel, competencia específica o requisito que determina perfil de acceso.

PR1	Conocimiento de matemática.
PR2	Conocimiento de estadística.
PR3	Conocimiento de teoría, técnicas y algoritmos de machine learning.
PR4	Conocimiento de estrategias de investigación y gestión del conocimiento.
PR5	Conocimiento de los objetivos y las principales misiones empresariales.
PR6	Conocimiento de los roles, de las responsabilidades y de la organización.
PR7	Conocimiento de las tecnologías de la información empresariales.
PR8	Conocimiento de herramientas y entornos de colaboración.
PR9	Conocimiento del funcionamiento básico de los ordenadores.
PR10	Conocimiento de sistemas cliente y servidor.
PR11	Conocimiento de procesado de datos.
PR12	Conocimiento de implementación, gestión y tipos de sistemas de archivos.
PR13	Conocimiento de sistemas operativos.
PR14	Conocimiento de arquitectura de ordenadores.
PR15	Conocimiento de sistemas embebidos.
PR16	Conocimiento de métodos para la evaluación y la prueba de sistemas.
PR17	Conocimiento de tipos, administración y funciones de los sitios web y los gestores de contenidos.
PR18	Conocimiento de las capacidades y la funcionalidad asociadas con las tecnologías de creación de contenido.

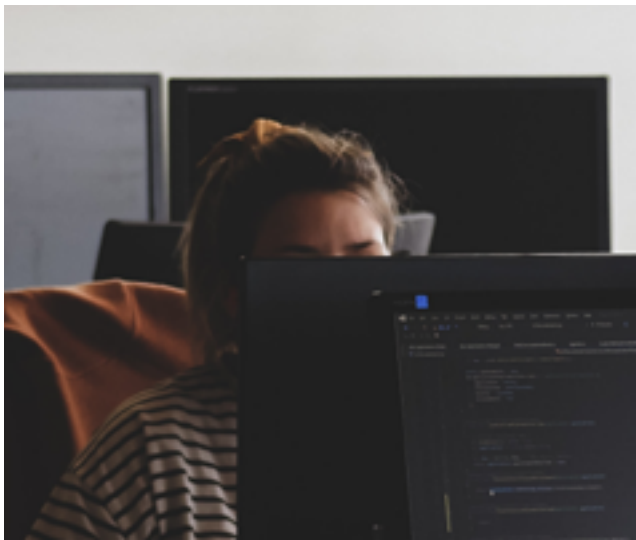
PR19	Conocimiento de los principales métodos, procedimientos y técnicas para la recogida de información y la producción, reporte o compartición de la misma.
PR20	Conocimiento de principios de interacción persona-ordenador.
PR21	Conocimiento de tecnologías de acceso remoto.
PR22	Conocimiento de sistemas de bases de datos, incluyendo su gestión, administración y mantenimiento.
PR23	Conocimiento de tecnologías de virtualización.
PR24	Conocimiento de modelos, administración, gestión y mantenimiento de sistemas y servicios en la nube.
PR25	Conocimiento de conceptos y marcos arquitectónicos de tecnología de la información.
PR26	Conocimiento de administración y mantenimiento de sistemas.
PR27	Conocimiento de técnicas y herramientas de depuración, diagnosis e identificación de fallos de sistemas.
PR28	Conocimiento de metodologías de tolerancia a fallos del sistema.
PR29	Conocimiento de procedimientos de auditoría y registro.
PR30	Conocimiento de principios y conceptos de programación como son lenguajes, depuradores o compiladores.
PR31	Conocimiento de programación en lenguajes de alto y bajo nivel.
PR32	Conocimiento de lenguajes de programación de bases de datos.
PR33	Conocimientos de programación en lenguajes de scripting.
PR34	Conocimiento de las implicaciones de seguridad en el diseño y la configuración de software.
PR35	Conocimiento de los principios de la ingeniería del software.
PR36	Conocimiento de procesos de control de calidad del software.
PR37	Conocimiento de los métodos para diseñar y analizar algoritmos.
PR38	Conocimiento de la estructura, arquitectura y diseño de sistemas de comunicación.
PR39	Conocimiento de sistemas de comunicación móvil.
PR40	Conocimiento de tipos de comunicación y protocolos de red.
PR41	Conocimiento de topologías de redes.
PR42	Conocimiento de mecanismos de control de acceso a nivel de host y red.
PR43	Conocimiento de administración de redes.
PR44	Conocimiento de dispositivos de red y sus configuraciones.
PR45	Conocimiento de aplicación de cortafuegos y sus funciones.
PR46	Conocimiento de métodos y herramientas de análisis de red.
PR47	Conocimiento básico de seguridad de red.
PR48	Conocimiento de funciones de seguridad actuales y emergentes del cifrado de datos en tránsito por redes de comunicaciones.

PR49	Conocimiento de registros de transmisión y técnicas de interferencia que permiten la transmisión de información no deseada o impiden que los sistemas instalados funcionen correctamente.
PR50	Conocimiento de algoritmos de cifrado y descifrado.
PR51	Conocimiento de gestión del ciclo de vida de las claves y secretos criptográficos.
PR52	Conocimiento de técnicas y conceptos de infraestructuras de clave pública y sistemas de certificados.
PR53	Conocimiento de funciones de seguridad actuales y emergentes del cifrado de datos en bases de datos.
PR54	Conocimiento de conceptos de cifrado en la nube.
PR55	Conocimiento de ciberamenazas y vulnerabilidades.
PR56	Conocimiento de técnicas y métodos de ciberataque.
PR57	Conocimiento de los modelos y las tecnologías de ciberseguridad.
PR58	Conocimiento de los principios y requisitos de confidencialidad, integridad y disponibilidad.
PR59	Conocimiento de técnicas básicas de fortificación ("hardening") de sistemas, redes y sistemas operativos.
PR60	Conocimiento de controles de seguridad y privacidad.
PR61	Conocimiento de gestión de la ciberseguridad.
PR62	Conocimiento del concepto de riesgo.
PR63	Conocimiento de regulaciones, políticas y leyes relevantes.
PR64	Conocimiento de los modelos de seguridad estándar industriales.

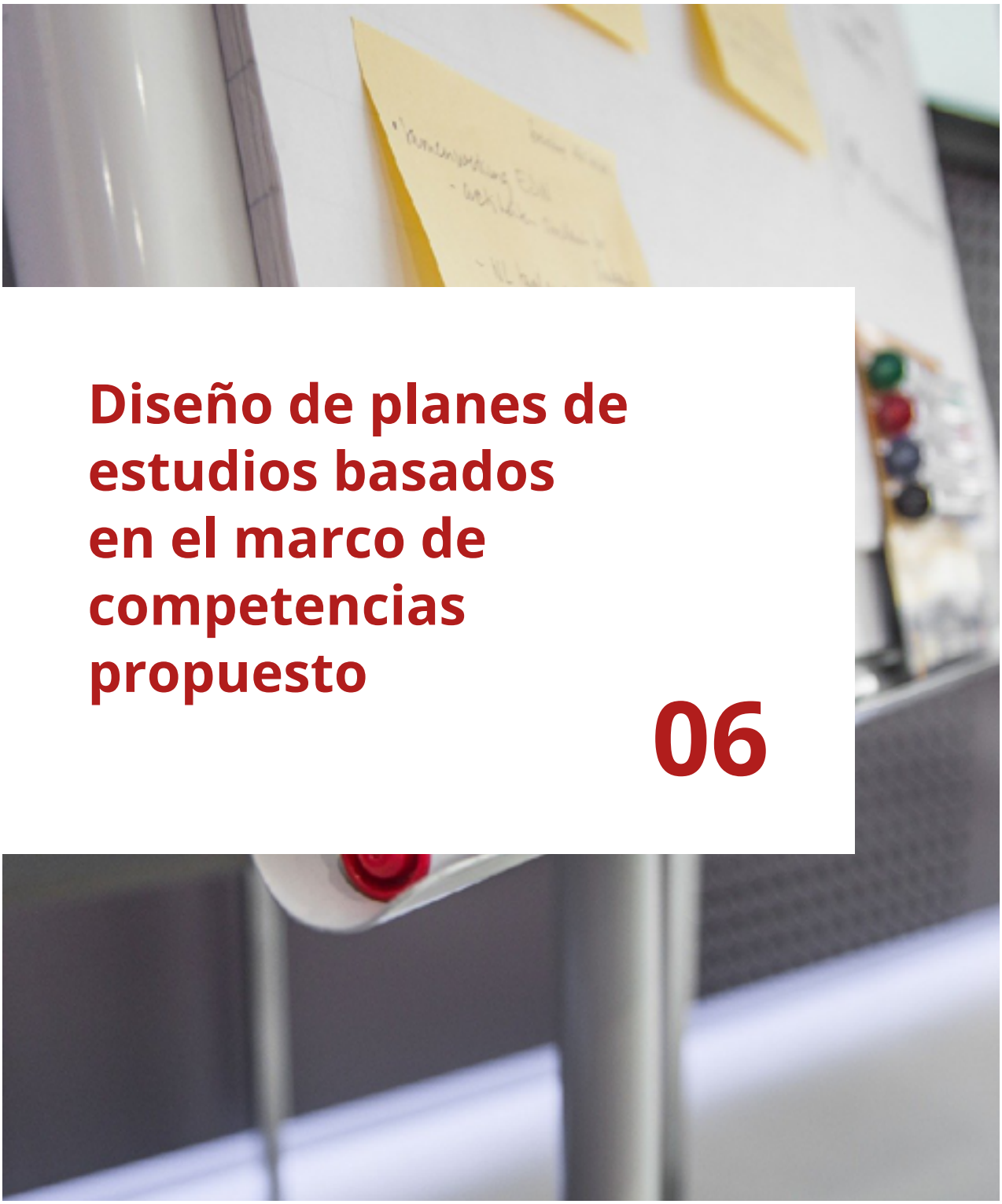
5.4. Listado de competencias básicas

Por último, para completar la propuesta de marco de competencias realizada en este documento, es necesario identificar conocimientos, destrezas y actitudes que todos los egresados de las titulaciones necesitan para su realización y desarrollo profesional, y su inclusión en el mercado laboral.

Estas competencias, también esenciales, relacionadas con lo que se suele denominar soft skills o competencias blandas, son necesarias en la mayoría de los puestos sin importar el sector o industria. Se enumeran a continuación las identificadas como esenciales en el sector de la ciberseguridad gracias al proceso de recogida de información realizado, ya que es necesario incluirlas en el diseño de cualquier plan de estudios.



CB1	Capacidad de comunicación oral y escrita.
CB2	Capacidad de comunicación en otros idiomas.
CB3	Capacidad de argumentación.
CB4	Capacidad de investigación.
CB5	Capacidad de razonamiento lógico.
CB6	Capacidad para demostrar y poner ejemplos.
CB7	Capacidad para identificar, plantear y resolver problemas con diferentes enfoques.
CB8	Capacidad para usar las tecnologías de la información y de la comunicación.
CB9	Capacidad para para buscar, procesar y analizar información procedente de fuentes diversas.
CB10	Capacidad para trabajar en forma autónoma.
CB11	Capacidad de abstracción, análisis y síntesis.
CB12	Capacidad de aprender y actualizarse permanentemente mediante diferentes formas y en diferentes foros de aprendizaje.
CB13	Capacidad de aplicar los conocimientos en la práctica.
CB14	Capacidad crítica y autocrítica.
CB15	Capacidad para organizar y planificar el tiempo.
CB16	Capacidad para adaptarse a situaciones de cambio constante.
CB17	Capacidad creativa.
CB18	Capacidad para formular, acometer y gestionar proyectos.
CB19	Capacidad para tomar decisiones y saber justificarlas, así como para establecer prioridades.
CB20	Capacidad para trabajar en equipo asumiendo diferentes roles.
CB21	Capacidad de motivar y conducir hacia metas comunes.
CB22	Capacidad de adquirir un compromiso con la calidad.
CB23	Capacidad de adquirir un compromiso con la preservación del medio ambiente.
CB24	Capacidad de asumir responsabilidad social y ética.
CB25	Capacidad para valorar y respetar la diversidad y la multiculturalidad.



Diseño de planes de estudios basados en el marco de competencias propuesto

06

El proceso de diseño de un plan de estudios en el marco de educación superior actual se podría resumir en las siguientes fases o etapas:

1. Decidir el perfil de los egresados de la titulación.

2. Identificar las competencias básicas/generales necesarias para el perfil.

3. Identificar las competencias específicas que permiten desarrollar este perfil.

4. Agrupar las competencias relacionadas en materias.

5. Definir asignaturas dentro de estas materias que permitan adquirir subconjuntos de estas competencias que estén relacionados.

6. Desarrollar los contenidos de estas asignaturas.

7. Establecer los pre-requisitos de estas asignaturas y comprobar si es necesario añadir competencias específicas nuevas (algunos se adquirirán en titulaciones previas, otros tendrán que abordarse en el propio plan de estudios).

8. Comprobar que todas las asignaturas se justifican en las competencias identificadas y que todas las competencias se cubren en, al menos, una asignatura.

9. Analizar las dependencias entre asignaturas y establecer una secuencia lógica para cursarlas.

El presente documento puede dar soporte a estas fases o etapas de las siguientes maneras:

- La primera fase o etapa suele depender de la estrategia de títulos de cada centro, de los recursos disponibles (humanos y en cuanto a infraestructuras) y también de la información disponible acerca de la necesidad de un título en la sociedad o en el mercado laboral. En este sentido, esta primera fase podría apoyarse, en mayor o menor medida, en los resultados obtenidos con la consulta realizada a los potenciales empleadores.

Aunque los resultados de dicha consulta se completarán y analizarán con mayor profundidad en el futuro, de momento han permitido seleccionar las competencias más representativas para cada función/área (sabiendo las actividades y tareas que es más probable que los egresados tengan que acometer en su labor profesional). Además, las prioridades de las funciones/áreas por las que se ha preguntado se muestran en la tabla 6.1. Estas valoraciones pueden tenerse en cuenta a la hora de decidir los perfiles más interesantes para los egresados, aunque de momento hay que recordar que provienen de una muestra pequeña. Hay que señalar que las áreas que han obtenido más puntuación son las transversales, la que se consideran con importancia media o alta en la mayor parte de organizaciones. Mientras que las que han obtenido menos puntuación, pueden resultar de importancia alta para algún tipo de organización, pero no para todas. Lo que puede hacer interesante, por ejemplo, un post-grado específico en ciertos contextos.

En el anexo I de este documento se proporciona el cuestionario que se ha empleado para la recogida de información, de manera que se pueda ampliar la recogida en el futuro para tener en cuenta una muestra mayor, actualizarla (ya que las necesidades del mercado evolucionan con el tiempo) o realizar iniciativas de recogida de información

propias basadas en ese cuestionario o en otro similar que lo utilice como punto de partida. Por ejemplo, una universidad podría realizar una consulta antes de diseñar un plan de estudios incidiendo en los empleadores de un sector o de una zona geográfica concretas.

1	Responsabilidad y dirección (331 puntos)
2	Detección y respuesta (300 puntos)
3	Formación, concienciación y sensibilización (273 puntos)
4	Arquitectura (267 puntos)
5	Auditoría (254 puntos)
6	Análisis (238 puntos)
7	Ingeniería y administración (237 puntos)
8	Desarrollo y producto (203 puntos)
9	Ingeniería de la confiabilidad (173 puntos)
10	Investigación (144 puntos)

Tabla 6.1. Funciones/áreas consideradas para la definición del marco de competencias ordenadas por prioridad según las respuestas obtenidas para el formulario

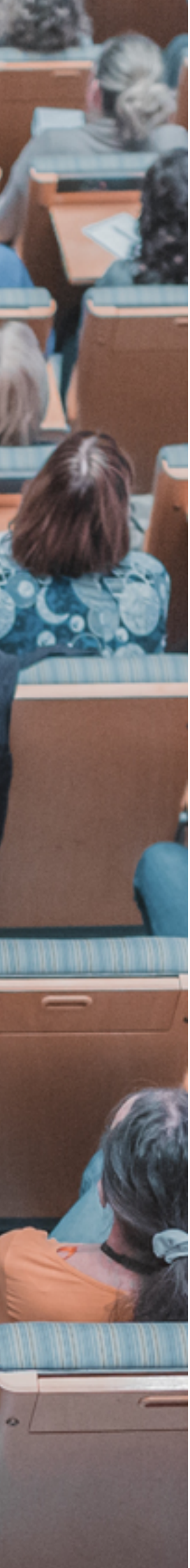
- La segunda fase o etapa, puede apoyarse en la discusión realizada en la sección 5.4 (listado de competencias básicas).

- La tercera fase o etapa puede apoyarse en el marco de competencias específicas proporcionado en la sección 5.2 (listado de competencias específicas).

- Las fases o etapas cuarta, quinta y sexta pueden usar como referencia el marco curricular ACM/IEEE en ciberseguridad y la sección 4 de este documento en la que se han analizado planes de estudios implantados en la actualidad que pueden servir como ejemplo.

- La séptima fase puede apoyarse en los pre-requisitos listados en la sección 5.3.

Se proporcionan a continuación algunos ejemplos ilustrativos acerca de cómo utilizar este documento en el proceso de diseño de planes de estudios. Estos ejemplos no son más que eso, muestras de cómo el presente marco puede ser útil a lo largo de las diferentes etapas identificadas para el diseño de un plan de estudios. No pretenden ser, en ningún caso, una recomendación acerca de títulos concretos que deberían implantarse en el futuro.



Ejemplo de uso 1: Diseño de títulos de grado en ciberseguridad

Si, por ejemplo, una universidad decide diseñar un plan de estudios de ciclo largo, un grado, con perfil de ingeniería que abarque las competencias técnicas de las áreas consideradas más importantes por los futuros empleadores consultados de momento, podría centrarse en las competencias específicas de las áreas Detección y respuesta, Arquitectura, Análisis e Ingeniería y administración. Con esto ya se tendría decidido el perfil de los egresados de la titulación.

A continuación, se deberían identificar las competencias básicas/generales necesarias para el perfil, escogiendo para ello el subconjunto más adecuado de las listadas en la sección 5.4 de este documento. Tras esta etapa, se deberían identificar las competencias específicas que permiten desarrollar este perfil. Para ello se debería escoger un subconjunto concreto de competencias de entre las listadas para las áreas de interés (Detección y respuesta, Arquitectura, Análisis e Ingeniería y administración) en la sección 5.2 de este documento. Y se agruparían las competencias relacionadas entre sí en materias. Para ello se podría emplear como punto de partida el Marco Curricular ACM/IEEE en Ciberseguridad, que ayudaría a definir asignaturas dentro de estas materias y a desarrollar sus programas y contenidos.

Ya que el acceso a este título de grado se realizaría desde bachillerato, ciclos formativos y formación profesional o acceso para mayores de 25 años, los pre-requisitos que se identifiquen como esenciales para poder cursar estas asignaturas y materias no pueden serlo directamente. Sino que tendrían que ser competencias específicas de asignaturas de los primeros años del grado que se cursen con la secuenciación adecuada respecto a las asignaturas más específicas del área de la ciberseguridad.

Por ello, para finalizar el diseño de las competencias de este plan de estudios sería necesario proponer un subconjunto de nuevas competencias específicas que garanticen que los conocimientos necesarios de la sección 5.3 se adquieren por parte de los estudiantes antes de cursar las asignaturas que provienen del primer grupo de competencias específicas seleccionadas. Por ejemplo, si una asignatura de Seguridad ofensiva de tercer curso del grado cubre la competencia CE40: “Llevar a cabo tests de penetración aplicando y utilizando los principios, técnicas y herramientas más adecuadas y conociendo las principales tácticas, técnicas y procedimientos (TTP) utilizadas por los adversarios.”, debería haber como mínimo una asignatura de primer o segundo curso del grado que cubriera cada una de las competencias asociadas a los siguientes pre-requisitos PR55, PR56 y PR33 “Conocimiento de ciberamenazas y vulnerabilidades”, “Conocimiento de técnicas y métodos de ciberataque.” y “Conocimientos de programación en lenguajes de scripting.”. Para redactar estos pre-requisitos en forma de competencias específicas en el plan de estudios se recomienda utilizar verbos en los primeros niveles de la taxonomía de Bloom como definir, describir, identificar, reconocer, seleccionar, explicar, incorporar, proporcionar, etc. [P2018].

El mismo proceso se seguiría para diseñar, por ejemplo, un plan de estudios que abarcara las áreas más relacionadas con tareas de responsabilidad, dirección, gestión y control. Para ello se podrían seleccionar competencias específicas de las áreas de Responsabilidad y dirección, Formación, concienciación y sensibilización y Auditoría, por ejemplo. Y se utilizaría este documento de la misma forma que en el ejemplo anterior.

Ejemplo de uso 2: Diseño de títulos de post-grado en ciberseguridad

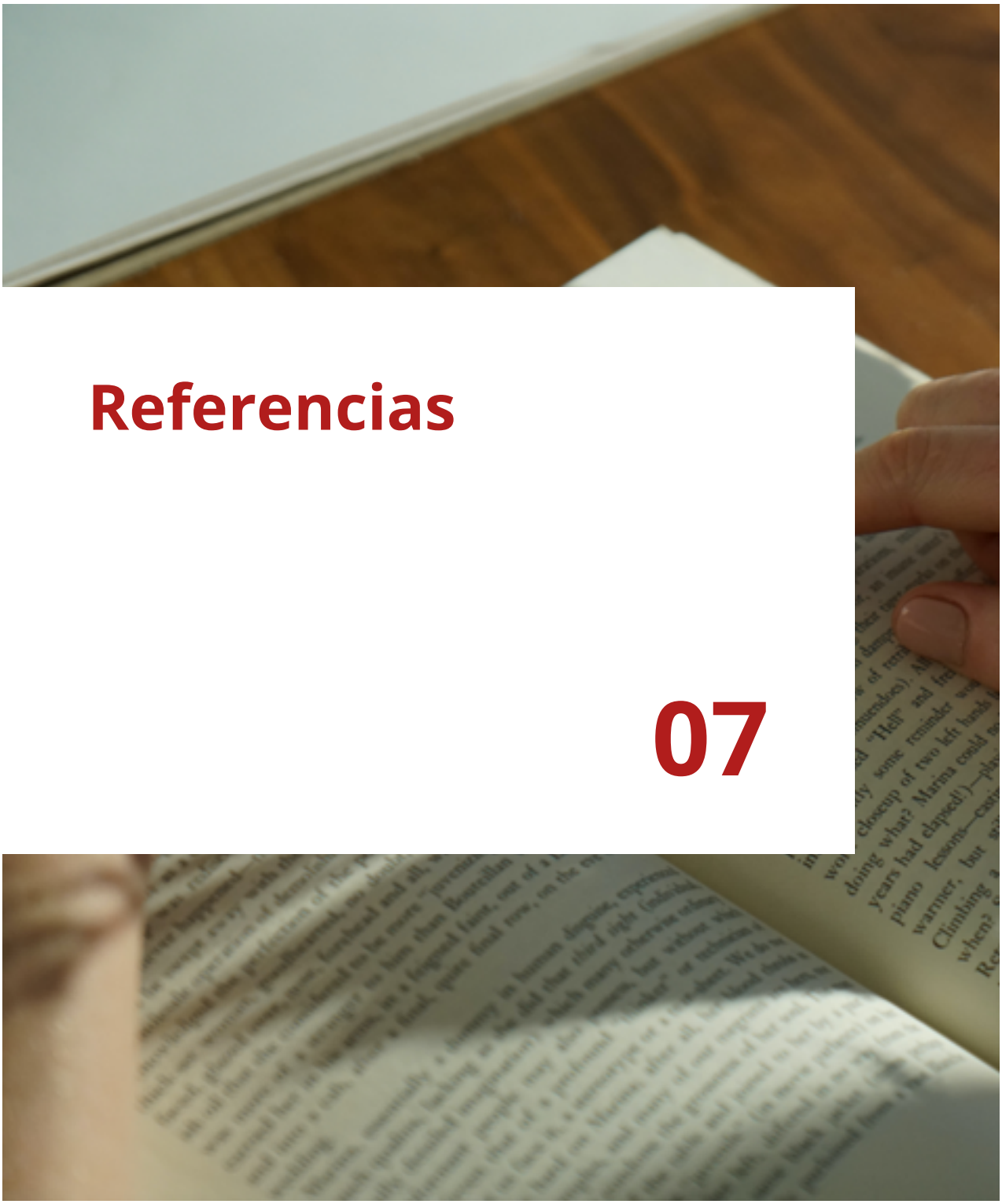
Otro ejemplo sería el de una universidad que desea diseñar un plan de estudios de post-grado (máster) centrado exclusivamente en el área de Responsabilidad y dirección, que parece ser transversal. Por ejemplo, pensando en proporcionar formación para profesionales que deseen certificarse en el futuro como responsables de ciberseguridad según el esquema nacional de certificación de responsables de ciberseguridad [ENCRC2021]. El proceso sería el mismo, pero en este caso sólo se escogerían competencias específicas del área de Responsabilidad y dirección.

Y sí se podrían establecer los conocimientos necesarios del listado proporcionado en la sección 5.3 como pre-requisitos, es decir, como conocimientos que los estudiantes admitidos en el máster deberían haber adquirido en las titulaciones que han cursado con anterioridad. Estos pre-requisitos ayudarían, por tanto, a establecer el perfil de acceso al título de máster. O a diseñar algún tipo de curso cero o curso puente que habilitara el acceso al máster a personas interesadas pero cuyos estudios anteriores no cubran los pre-requisitos identificados.

Lo mismo ocurriría si se deseara diseñar post-grados específicos en cualquiera de las otras áreas para las que se han propuesto competencias específicas en la sección 5.2: Detección y respuesta, Arquitectura, Análisis, etc. El proceso sería similar.

Ejemplo de uso 3: Diseño de títulos de post-grado mixtos o híbridos

También se podría emplear este marco de competencias para diseñar planes de estudios mixtos o híbridos, por ejemplo, un máster en Desarrollo seguro o DevSecOps, un máster en Ciberseguridad industrial y safety (incluida en el área de Ingeniería de la confiabilidad en el presente marco) o un máster en Aspectos legales de la ciberseguridad y privacidad (incluida también en el área de Ingeniería de la confiabilidad en el presente marco). Simplemente habría que buscar la combinación y equilibrio adecuados entre las competencias específicas de las disciplinas o áreas que se pretendiera combinar (desarrollo + ciberseguridad- Desarrollo y producto, industria/OT + ciberseguridad – Ingeniería de la confiabilidad, derecho + ciberseguridad – Ingeniería de la confiabilidad). Y habría que prestar especial cuidado a la identificación de los pre-requisitos para garantizar que los estudiantes pueden aprovechar el programa en su totalidad ya que poseen los conocimientos necesarios cuando acceden a él.



Referencias

07

/// **[CC2020]** ACM/IEEE, Computing Curricula 2020, CC2020, Paradigms for Global Computing Education, 31 de diciembre de 2020. URL: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2020.pdf

/// **[CS2017]** ACM/IEEE, Cybersecurity Curricula 2017, Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity, Computing Curricula Series Joint Task Force on Cybersecurity Education, 31 de diciembre de 2017. URL: https://cybered.hosting.acm.org/wp/wp-content/uploads/2018/02/csec2017_web.pdf

/// **[CYBOK2018]** Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M., & Peersman, C. (2018). Scoping the cyber security body of knowledge. IEEE Security & Privacy, 16(3), 96-102.

/// **[DLMS2021]** Dragoni, N., Lluch Lafuente, A., Massacci, F., & Schlichtkrull, A. (2021). Are We Preparing Students to Build Security In? A Survey of European Cybersecurity in Higher Education Programs [Education]. IEEE Security & Privacy, 19(1), 81-88.

/// **[ENCRC2021]** Propuesta de Esquema Nacional de Certificación de Responsables de Ciberseguridad, desarrollada por el Grupo de Trabajo de Formación, Capacitación y Talento, del Foro Nacional de Ciberseguridad, creado por mandato de la Estrategia Nacional de Cibserseguridad de 2019.

/// **[H2008]** Howard, M. (2008). Becoming a security expert. IEEE Security & Privacy, 6(1), 71-73.

/// **[INCIBE2021a]** INCIBE. Másteres y Grados en Ciberseguridad en España. Febrero 2021. https://www.incibe.es/sites/default/files/paginas/talento/catalogos-formacion/catalogo-masteres.pdf

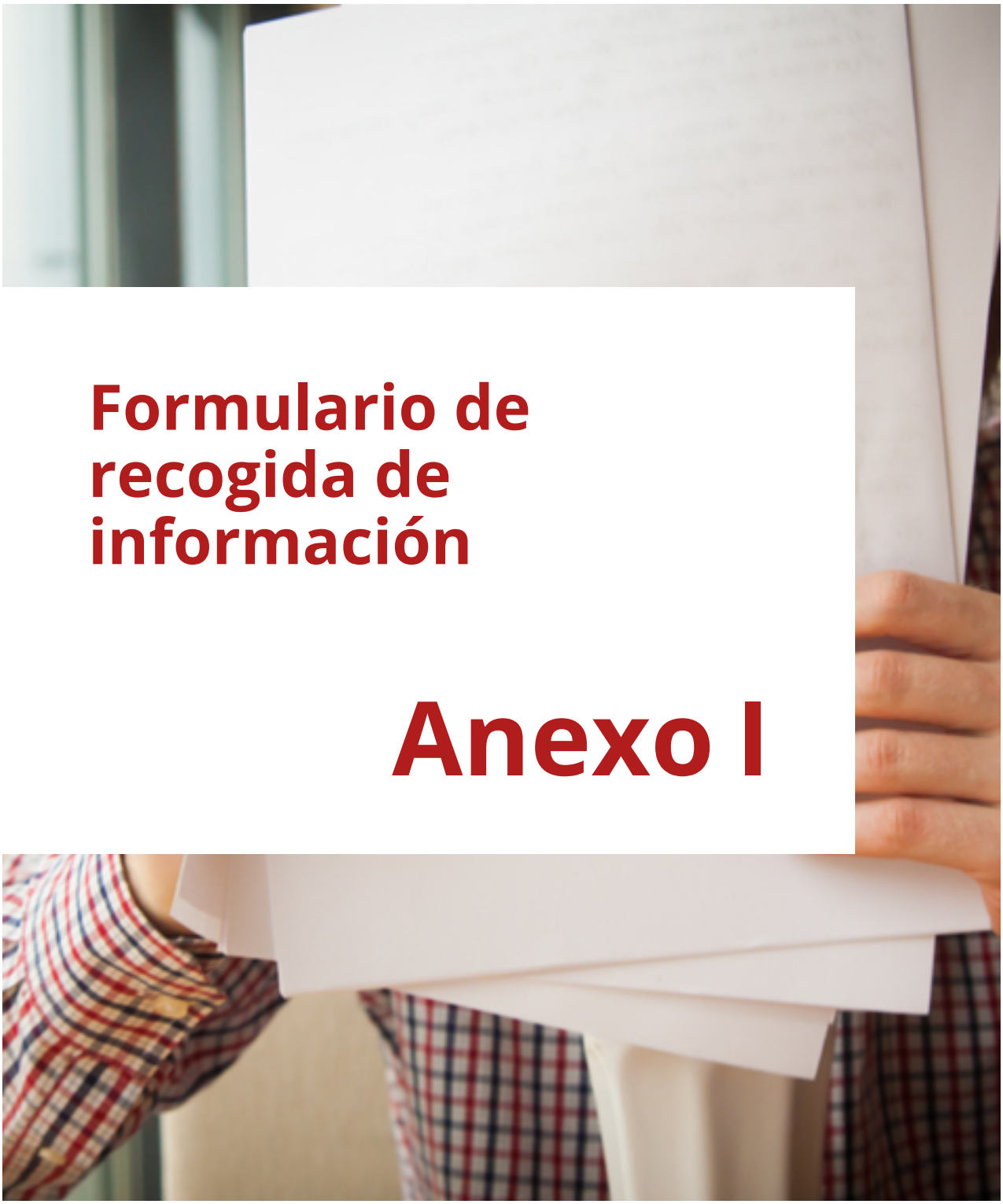
/// **[INCIBE2021b]** INCIBE. Instituciones que imparten formación en ciberseguridad en España. Febrero 2021. https://www.incibe.es/sites/default/files/paginas/talento/catalogos-formacion/catalogo-instituciones.pdf

/// **[JRC2019]** Fovino, I. N., Neisse, R., Hernandez Ramos, J. L., Polemi, N., Ruzzante, G. L., Figwer, M., & Lazari, A. (2019). A proposal for a European cybersecurity taxonomy. Luxembourg: Publications Office of the European Union.

/// **[OECD2001]** Rychen, D.S.,& Salganik, L.H. (2001). Defining and selecting key competencies. DeSeCo Project (Definition and Selection of Competencies: Theoretical and Conceptual Foundations), OECD. https://www.deseco.ch/bfs/deseco/en/index/02.html

/// **[P2018]** Parrish, A., Impagliazzo, J., Raj, R.K., Santos, H., Asghar, M.R., Jøsang, A., Pereira, T., & Stavrou, E., (2018). Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. In Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE 2018 Companion). Association for Computing Machinery, New York, NY, USA, 36–54. https://doi.org/10.1145/3293881.3295778

/// **[SPARTA2020]** D9.1 Cybersecurity skills framework. Deliverable. Available at https://www.sparta.eu/assets/deliverables/SPARTA-D9.1-Cybersecurity-skills-framework-PU-M12.pdf. Accessed April 2021



Formulario de recogida de información

Anexo I

Marco de competencias para programas superiores (universitarios) de formación en ciberseguridad

Instrucciones para responder el formulario

El siguiente formulario forma parte de la iniciativa para la definición de competencias para programas superiores (universitarios) de formación especializada en ciberseguridad del grupo de trabajo en Formación, Capacitación y Talento del Foro Nacional de Ciberseguridad. **Gracias** por colaborar con esta iniciativa.

Rellenar el formulario le llevará entre **30 y 40 minutos**.

Estamos intentando **recoger información sobre las actividades y tareas que necesitarán realizar los profesionales de la ciberseguridad en el medio plazo** para definir el conjunto de competencias más adecuado para los títulos universitarios que se oferten en esta área. Nuestro objetivo no es analizar el mercado laboral ni el organigrama de las organizaciones, sino **definir planes de estudios para títulos universitarios** con las competencias apropiadas.
En las primeras secciones se muestran 10 funciones/áreas de la ciberseguridad. Para cada una de ellas se identifican una serie de tareas o actividades asociadas a la función/área. Por favor, **usando la escala de Likert (1- nunca, 2 -casi nunca, 3 -ocasionalmente, 4 - a menudo, 5 - constantemente), indique si esa tarea o actividad se desarrolla en su organización**, independientemente de la denominación que tiene el puesto o rol de la persona que la desempeña en su organización en concreto. También independientemente del dominio (IT, OT, cloud, etc.). Al indicar su respuesta, no tenga en cuenta sólo lo que ocurre actualmente, sino también la tendencia a medio o largo plazo. Es decir, lo que se espera que ocurra en los próximos años.

Dispone de una caja de **texto libre** por si quiere indicarnos alguna tarea o actividad que cree importante y no ha encontrado.

En la última sección se le pide que, una vez comprendidas las tareas y actividades que se asocian a cada una, **ordene las 10 funciones/áreas por las que se le acaba de preguntar en relación con la importancia que tiene para su organización** contar con ella dentro de su equipo. Siendo el puesto 1 el que corresponde a la primera, la más importante, la que seguro que es necesaria. Y el puesto 10 el que corresponde a la menos importante. Se trata de una puntuación relativa, comparando unas funciones con otras.

Información básica sobre Protección de Datos

• Datos y procedencia: Se tratarán los siguientes datos proporcionados por los interesados: nombre completo, organización, cargo y dirección de correo electrónico.

• Responsable: Foro Nacional de Ciberseguridad, Grupo de Trabajo 3 – Formación, Capacitación y Talento.

• Finalidad: Recogida de información para el Grupo de Trabajo 3 del Foro Nacional de Ciberseguridad, como parte de la iniciativa cuyo objetivo es proponer un marco de competencias para programas superiores (universitarios) de formación en ciberseguridad.

• Legitimación: Consentimiento del interesado.

• Destinatarios: No se cederán datos a terceros, salvo obligación legal.

• Derechos: Los interesados tienen derecho a solicitar el acceso a sus datos personales, a solicitar su rectificación o supresión, a solicitar la limitación de su tratamiento, a oponerse al tratamiento y a la portabilidad de sus datos. Para ello deben dirigirse por email al responsable antes citado.

• Información adicional: Puede consultar la información adicional y detallada sobre Protección de Datos dirigiéndose al responsable antes citado.

1. Nombre completo

2. Organización

3. Cargo

Arquitectura

Tarea o actividad
Identificar las necesidades de seguridad de la organización para diseñar su arquitectura de seguridad en consecuencia.
Determinar los niveles adecuados de confidencialidad, integridad y disponibilidad para los activos críticos que permiten la continuidad de las operaciones de la organización y dar soporte a dicha continuidad.
Determinar las necesidades en seguridad física en relación con la protección de personas, bienes, instalaciones o medio.
Evaluar arquitecturas posibles y tomar decisiones respecto al diseño y localización de las capacidades de seguridad.
Traducir las capacidades de seguridad de alto nivel a especificaciones criptográficas y técnicas relacionadas con mecanismos y servicios de seguridad concretos.
Asegurar que los mecanismos y servicios seleccionados son consistentes con las necesidades de seguridad de la organización y cumplen los requisitos establecidos.
Documentar requisitos de seguridad, especificaciones funcionales, patrones de diseño, etc.
Definir configuraciones base seguras para diferentes tipos de activos tanto físicos como lógicos.
Señalar los gaps entre las arquitecturas diseñadas y las realmente desplegadas y ayudar a gestionar los riesgos.
Comprender cómo los cambios en la infraestructura pueden afectar a los niveles de seguridad disfrutados.
Asesorar durante la realización de los proyectos en aspectos de diseño, patrones, costes y riesgos.
Apoyar en la adquisición y contratación de mecanismos y servicios de seguridad, garantizando una gestión adecuada de la cadena de suministro.
Por favor, en la celda inferior indique si ha echado en falta alguna tarea o actividad que en su organización tendría una puntuación de 5.

Desarrollo y producto

Tarea o actividad
Trasladar requisitos de seguridad a aspectos de diseño del software.
Aplicar metodologías de desarrollo seguro para minimizar el número de vulnerabilidades con las que se libera el código desarrollado.
Identificar la superficie de exposición del software desarrollado.
Realizar modelado de amenazas/análisis de riesgos del software desarrollado en diferentes momentos de su ciclo de vida.
Llevar a cabo análisis de código tanto estático como dinámico de código.
Planificar y llevar a cabo las tareas de testing y validación de seguridad.
Identificar las dependencias del software y las implicaciones que tienen para su seguridad.
Gestionar adecuadamente las implicaciones que tiene para la seguridad la interacción del software con el sistema operativo, el hipervisor, el hardware, etc.
Automatizar las tareas repetitivas que tienen que ver con la seguridad del software.
Documentar los aspectos de seguridad del software para otros desarrolladores, usuarios y demás agentes involucrados en el ciclo de vida del software.
Generar parches y actualizaciones que resuelvan las vulnerabilidades encontradas en el software tras ser liberado.
Definir planes de respuesta ante incidentes de productos software y dar soporte a esta respuesta.
Implementar mecanismos, controles y mitigaciones de seguridad mediante software.
Apoyar a otras funciones del área de la ciberseguridad en el desarrollo de herramientas, scripts, etc. que les ayuden a desarrollar sus tareas o actividades.
Por favor, en la celda inferior indique si ha echado en falta alguna tarea o actividad que en su organización tendría una puntuación de 5.

Ingeniería y administración

Tarea o actividad
Instalar, configurar, desplegar, integrar, mantener, actualizar los activos de la organización cumpliendo las especificaciones y políticas de seguridad.
Realizar test y diagnósticos de capacidad, conectividad o rendimiento y optimizar las prestaciones de los activos sin incumplir estas especificaciones y políticas.
Colaborar con la definición de especificaciones y políticas de seguridad en los que se refiere a los procedimientos técnicos.
Gestionar cuentas, permisos, privilegios, etc. en el acceso a los activos según el modelo de control de accesos definido para la organización.

Realizar inventarios de activos y mapas de red a diferentes niveles.
Planificar los cambios en la infraestructura/activos para minimizar los riesgos que producen los proyectos que los implementan.
Realizar la gestión de la configuración de los activos.
Realizar backup y copias de seguridad de diferentes tipos de datos e información.
Automatizar las tareas repetitivas que tienen que ver con la administración segura de los activos de la organización.
Proporcionar recomendaciones de uso seguro a los usuarios finales de los activos.
Proporcionar los medios para que los usuarios finales puedan cumplir las políticas de seguridad (o no puedan incumplirlas).
Monitorizar los activos bajo su responsabilidad y analizar tendencias para ayudar en la detección de anomalías, intrusiones, etc.
Dar soporte a los equipos de respuesta a incidentes.
Recuperar los activos tras incidentes de seguridad, contingencias y catástrofes.
Por favor, en la celda inferior indique si ha echado en falta alguna tarea o actividad que en su organización tendría una puntuación de 5.

Análisis

Tarea o actividad
Asegurar que la configuración, despliegue, integración, etc. de los activos cumplen con las especificaciones y políticas de seguridad.
Asegurar que los controles de seguridad y los productos/servicios de seguridad que se incorporan reducen el riesgo como se esperaba.
Realizar distintos tipos de verificaciones de seguridad, revisiones y test a diferentes tipos de activos para analizar los niveles de seguridad a los que llegan.
Asegurar que las especificaciones y políticas de seguridad se llevan a la práctica de la manera establecida y permiten que se cumplan los requisitos de seguridad.
Analizar los parches y actualizaciones de seguridad antes de que sean aplicados en los activos de la organización.
Realizar diferentes tipos de análisis y escaneo de vulnerabilidades en la infraestructura de la organización.
Realizar test de penetración y ejercicios de simulación de adversarios.
Crear, desplegar y mantener conjuntos de herramientas actualizados de seguridad ofensiva para realizar análisis periódicos de vulnerabilidades, continuos, etc.
Analizar las tendencias de los agentes de amenaza y del mercado para apoyar a otras áreas en su labor (arquitectura, ingeniería y administración, investigación, etc.).
Realizar procesos de ingeniería inversa para comprender cómo funcionan diferentes artefactos y objetos estáticos y dinámicos empleados por los agentes de amenaza.

Colaborar con las funciones de desarrollo y producto para ayudarles a reducir la superficie de exposición y a desarrollar los artefactos de software necesarios.
Asesorar en la toma de decisiones en base a los resultados de los análisis realizados.
Dar soporte a los equipos de respuesta a incidentes, por ejemplo, con capacidades de análisis forense.
Por favor, en la celda inferior indique si ha echado en falta alguna tarea o actividad que en su organización tendría una puntuación de 5.

Detección y respuesta

Tarea o actividad
Definir mecanismos de monitorización necesarios para detectar incidentes de seguridad.
Definir los requisitos de las fuentes de datos y herramientas necesarias para realizar detección.
Desarrollar estándares, especificaciones y políticas en relación con estos datos y herramientas.
Gestionar la captura de datos y su ciclo de vida de manera que sean útiles para la detección de incidentes.
Valorar la validez y valor de los datos y de sus fuentes en relación con la detección.
Plantear hipótesis a partir de grandes volúmenes de datos y validarlas mediante distintos tipos de modelos matemáticos o estadísticos.
Caracterizar las situaciones consideradas normales y detectar las anomalías.
Conocer las TTPs empleadas por los adversarios para proponer métricas, indicadores, etc. que permitan detectarlas en tiempos razonables para el contexto y levantar alertas.
Compartir inteligencia de amenazas e información similar con terceros según los objetivos de la organización con los formatos y mecanismos adecuados.
Automatizar las tareas repetitivas mediante lenguajes de scripting o específicos para manejo de grandes volúmenes de datos.
Realizar triaje y priorizar eventos de seguridad y alertas.
Coordinar personas y equipos internos y externos con diferentes perfiles e intereses durante y después del incidente (comunicación, reporting, denuncia, etc.).
Investigar el incidente y sus causas, realizar atribución y comprender los patrones de ataque empleados.
Realizar análisis forense incluyendo la recogida y custodia de evidencias digitales.
Analizar artefactos y objetos estáticos y dinámicos para extraer de ellos información relevante en cuanto a detección y respuesta.
Contener el incidente con soluciones temporales.
Asesorar a otras funciones para contener el incidente con soluciones permanentes y evitar que se produzca en el futuro.
Documentar los incidentes.
Extraer lecciones aprendidas de los incidentes.

Apoyar a otras funciones en la recuperación de activos tras los incidentes.
Por favor, en la celda inferior indique si ha echado en falta alguna tarea o actividad que en su organización tendría una puntuación de 5.

Investigación

Tarea o actividad
Llevar a cabo revisiones de la literatura y del estado del arte.
Identificar aspectos en los que se puede avanzar el estado del arte, así como tendencias del mercado o de los agentes de amenaza.
Descubrir nuevas vulnerabilidades, malware o amenazas; proponer nuevos mecanismos y capacidades defensivas; romper criptosistemas con técnicas novedosas, etc.
Coordinarse con otras funciones para determinar los objetivos de I+D+i de la organización.
Formular proyectos, coordinarlos y gestionar los recursos y presupuesto asignado.
Desarrollar metodologías, técnicas o herramientas propias apropiadas para conseguir los objetivos planteados.
Apoyar a otras funciones para que incorporen las innovaciones producidas a sus tareas y actividades.
Captar financiación para llevar a cabo los proyectos de I+D+i.
Establecer alianzas estratégicas con posibles socios que contribuyan en actividades de I+D+i.
Proteger la propiedad intelectual producida mediante patentes y licencias adecuadas.
Participar en consorcios, foros, redes, etc. que puedan enriquecer la función de investigación y permitan compartir el conocimiento generado según los objetivos de la organización.
Por favor, en la celda inferior indique si ha echado en falta alguna tarea o actividad que en su organización tendría una puntuación de 5.

Responsabilidad y dirección

Tarea o actividad
Contribuir al desarrollo de la Política de Seguridad de la organización y a definir su tolerancia al ciberriesgo.
Definir la estrategia de seguridad de la organización y coordinar la creación de normas, políticas, etc.
Informar y reportar a la dirección general y al comité de dirección acerca del estado de la organización en cuanto a la ciberseguridad, KPIs, ROI, etc.
Coordinar los procesos de evaluación. y análisis de riesgos así como las auditorías de seguridad.
Proponer estrategias de mitigación y transferencia del riesgo y alinearlas con los objetivos de negocio.
Planificar el despliegue de las mitigaciones y controles.

Predecir la evolución de los paradigmas tecnológicos y de los agentes de amenaza para intentar anticiparse de manera proactiva.
Definir y coordinar Programas y Planes para garantizar una correcta gobernanza de la seguridad.
Definir y coordinar planes de continuidad de negocio, contingencia, respuesta a incidentes, etc.
Definir KPIs e indicadores de éxito que permitan evaluar el éxito o eficiencia de estos Programas y Planes, también desde el punto de vista de negocio (ROI, etc.), actualizarlos y realizar mejora continua.
Fomentar la cultura de seguridad mediante la definición y comunicación de políticas de seguridad y otros documentos.
Analizar el grado de cumplimiento de estas políticas y garantizar que se cumplen en un grado adecuado.
Identificar las obligaciones de cumplimiento regulatorio.
Analizar qué certificaciones, evaluaciones, etc. es necesario o conveniente obtener (individuales y organizativas).
Identificar las necesidades de recursos humanos y materiales para conseguir los niveles de seguridad adecuados en la organización.
Gestionar las nuevas contrataciones, evaluar sus riesgos y hacer seguimiento durante la relación.
Gestionar presupuesto, adquisiciones, subcontrataciones, cadena de suministro, etc.
Validar que las contrataciones y adquisiciones responden a los objetivos y requisitos establecidos previamente.
Apoyar a la comunicación interna, vertical y horizontal, para transmitir el valor de la seguridad para la organización y coordinar a todas las funciones relacionadas con la seguridad.
Apoyar a la comunicación externa con terceras partes, socios, proveedores, clientes, etc.
Mantener el contacto con autoridades y grupos de interés.
Coordinar la respuesta a incidentes y la recuperación cuando sea necesario ejecutar los planes correspondientes.
Por favor, en la celda inferior indique si ha echado en falta alguna tarea o actividad que en su organización tendría una puntuación de 5.

Ingeniería de confiabilidad

Tarea o actividad
Ayudar a otras funciones a definir la Política de Privacidad de la organización y su tolerancia al riesgo para la protección de datos.
Coordinar los procesos de evaluación de impacto para la protección de datos y la evaluación de riesgos para la privacidad.
Identificar categorías de datos, realizar inventarios y etiquetarlos.
Ayudar a otras funciones a proponer estrategias de mitigación y transferencia del riesgo para la privacidad y la protección de datos y alinearlas con los objetivos de negocio.

Evaluar y probar mecanismos de privacidad desde el diseño.
Incorporar estos mecanismos a los activos, proyectos, etc. en los que sea necesario.
Mantener una actitud proactiva que permita identificar oportunidades para incorporar en la organización nuevas herramientas, prácticas, etc. que mejoren los niveles de privacidad.
Definir y coordinar el Plan de Cumplimiento relacionado con la privacidad y otros programas y planes relacionados.
Ayudar a otras funciones a definir la Política de Safety de la organización y su tolerancia al riesgo para la salud de las personas, para el medio ambiente, etc.
Ayudar a otras funciones a proponer estrategias de mitigación y transferencia del riesgo para la safety y alinearlas con los objetivos de negocio.
Evaluar y probar mecanismos de safety desde el diseño.
Incorporar estos mecanismos a los activos, proyectos, etc. en los que sea necesario.
Mantener una actitud proactiva que permita identificar oportunidades para incorporar en la organización nuevas herramientas, prácticas, etc. que mejoren los niveles de safety.
Definir y coordinar el Plan de Cumplimiento relacionado con la safety y otros programas y planes relacionados.
Identificar las obligaciones de cumplimiento regulatorio en relación con la confiabilidad (privacidad, safety, resiliencia, etc.).
Analizar qué certificaciones, evaluaciones, etc. en relación con la confiabilidad (privacidad, safety, resiliencia, etc.) es necesario o conveniente obtener (individuales y organizativas).
Apoyar a la comunicación interna, vertical y horizontal, para transmitir el valor de la confiabilidad para la organización y coordinar a todas las funciones.
Realizar comunicación externa con terceras partes, socios, proveedores, clientes, etc.
Mantener el contacto con autoridades y grupos de interés.
Coordinar la respuesta a incidentes de privacidad o safety y la recuperación.
Gestionar las acciones legales relacionadas con los incidentes de privacidad o safety.
Por favor, en la celda inferior indique si ha echado en falta alguna tarea o actividad que en su organización tendría una puntuación de 5.

Auditoría

Tarea o actividad
Conocer los procesos de negocio que soportan la organización y sus objetivos y requisitos de seguridad.
Planificar y realizar auditorías de seguridad de activos, proyectos, procesos, programas, etc.
Seleccionar o proponer los estándares y las metodologías más adecuados para realizar estas auditorías en cada caso.
Proponer y validar mecanismos para monitorizar y medir riesgo, nivel de cumplimiento, nivel de seguridad.

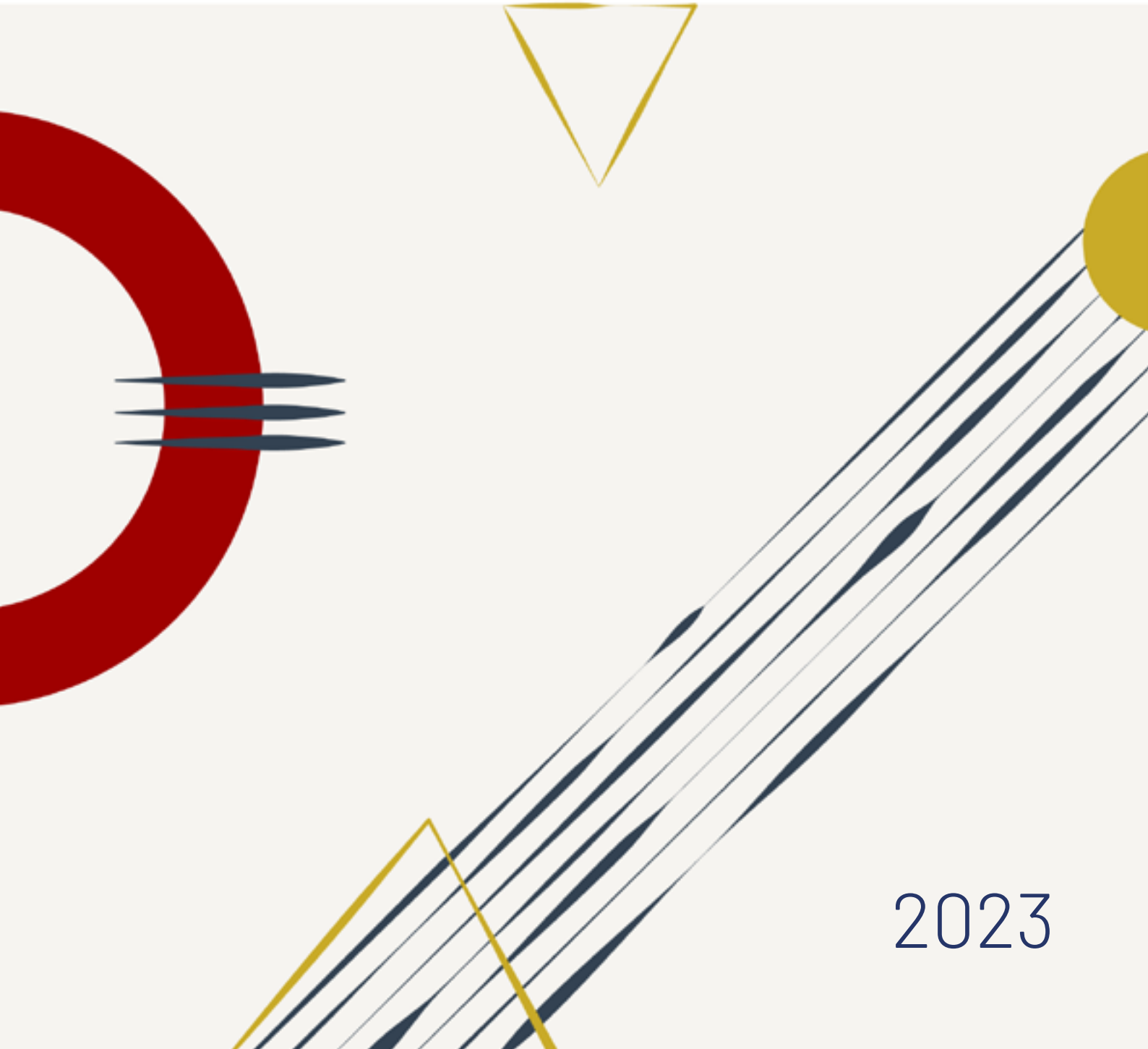
Proponer y validar métricas para cuantificar riesgo, nivel de cumplimiento, nivel de seguridad.
Proporcionar recomendaciones para realizar acciones correctoras y mejora continua en la seguridad de la organización tras los resultados de los diferentes procesos de auditoría.
Comunicar los resultados de los procesos de auditoría y documentarlos adecuadamente.
Evaluar el grado de cumplimiento de otras funciones respecto de los objetivos y requisitos fijados en la organización.
Evaluar el grado de segregación de funciones.
Revisar el grado de cumplimiento que proveedores y otras terceras partes hacen de sus obligaciones.
Ayudar a otras funciones a incluir en contratos, consentimientos, etc. la expresión de estas obligaciones en un lenguaje claro y adecuado.
Por favor, en la celda inferior indique si ha echado en falta alguna tarea o actividad que en su organización tendría una puntuación de 5.

Formación, concienciación y sensibilización

Tarea o actividad
Ayudar a otras funciones (gestión y dirección, etc.) a definir las necesidades de formación, concienciación y sensibilización de diferentes funciones dentro de la organización y a preparar programas y planes.
Diseñar iniciativas que permitan cubrir estas necesidades.
Llevar a cabo actividades internas de formación, concienciación y sensibilización.
Definir KPIs e indicadores de éxito que permitan evaluar el éxito o eficiencia de estas actividades, también desde el punto de vista de negocio (ROI, etc.) y realizar mejora continua.
Preparar materiales adecuados para las iniciativas internas de formación, concienciación y sensibilización.
Identificar a agentes adecuados para llevar a cabo actividades de formación, concienciación y sensibilización externas y coordinar su trabajo.
Establecer alianzas estratégicas con posibles socios que contribuyan en actividades de formación, concienciación y sensibilización.
Evaluar la adquisición de competencias por parte de todos los agentes involucrados en las iniciativas de formación, concienciación y sensibilización.
Cuantificar el nivel de madurez de la organización en relación con la formación, concienciación y sensibilización en seguridad de sus recursos humanos.
Sensibilizar a la dirección acerca de la importancia de la ciberseguridad para la consecución de los objetivos de negocio, cumplimiento normativo, etc.
Analizar, desplegar, escoger, configurar, etc. plataformas de entrenamiento, simulación, gemelos digitales o similares para dar soporte a las actividades que se realicen.
Por favor, en la celda inferior indique si ha echado en falta alguna tarea o actividad que en su organización tendría una puntuación de 5.

FORO NACIONAL DE CIBERSEGURIDAD

Informe sobre las necesidades, capacidades y retos para la colaboración público-privada en materia de Ciberdefensa en las empresas del Sector de la Defensa y la Seguridad



2023

Autores

Coordinador sociedad civil:

Ricardo Martí Fluxá (TEDAE)

Coordinadores institucionales:

GD Rafael García Hernandez (Mando Conjunto del Ciberespacio. Ministerio de Defensa)

Alberto Sotillo Miguel (Dirección General de Armamento y Material. Ministerio de Defensa)

Autores y colaboradores:

Javier Aguado
Ana I. Ayerbe
Juan Carlos Batanero
Fernando Borredá
Miriam del Campo
Juan Jesús Carretero
Diego Fernández
Luis Gimeno
Héctor Naranjo
Mamen Ocaña
Arsenio Pérez
César Ramos
Luis Vicente Sánchez – Crespo
Clara Tébar
Miguel Ángel Thomas
CA Francisco Javier Roca Rivero
CA Manuel Alvargonzález Méndez
CN Enrique Cubeiro Cabello
TCOL Juan Adolfo Montero Garcia
TCOL Mónica Mateos Calle
TCOL Roberto Alcalá Sánchez
TCOL Rubén Vega Bustelo

ÍNDICE

RESUMEN EJECUTIVO

El Foro Nacional de Ciberseguridad, en el marco de la **Estrategia Nacional de Ciberseguridad de 2019** (ENCS), creó en el año 2020 el Grupo de Trabajo Nº4 (GT4) de Análisis e Impulso a la Industria de Ciberdefensa, cuyo objetivo se centró en la identificación de necesidades, capacidades y retos para la colaboración público-privada para el fomento de la industria española en el sector de la defensa y la seguridad. Este GT4 está compuesto por TEDAE, el MCCE y la DGAM.

El presente documento es el resultado final de los trabajos realizados para el *Informe sobre las necesidades, capacidades y retos para la colaboración público-privada en materia de Ciberdefensa en las empresas del Sector de la Defensa y la Seguridad* y los trabajos realizados por el GT4 para el *Informe* [...] *y la seguridad*. En él se han estudiado las capacidades tecnológicas aún en desarrollo así como los servicios y productos en el mercado demandados por el sector de la defensa y la seguridad. También se han identificado áreas de mejora en el ámbito de la ciberdefensa y ciberseguridad.

La **metodología** utilizada para la realización de este trabajo se ha basado en la realización de un cuestionario. El público objetivo considerado es el ecosistema nacional de la ciberseguridad y la ciberdefensa. Para ello, se invitó a participar en él a empresas, universidades y centros de investigación y tecnológicos relacionados con los organismos participantes en este grupo. De las 120 entidades identificadas, 88 mostraron interés y se obtuvieron 30 respuestas al formulario que se han tomado como muestra del estudio. Las respuestas proceden principalmente de empresas especializadas en ciberdefensa asociadas a TEDAE y las inscritas en el registro de la DGAM.

A continuación, se indican los aspectos más relevantes del estudio, empezando por las principales **conclusiones** obtenidas:

Las entidades participantes han mostrado un gran nivel de colaboración público-privada con el sector público y declaran un alto conocimiento de las estructuras y procesos del Ministerio de Defensa y de las Fuerzas Armadas.

En lo relativo a la gestión de la seguridad de la información, la mayoría de las entidades demuestra un alto nivel de madurez, sería recomendable mejorar algunos aspectos como los referentes a la posesión de certificados de seguridad reconocidos, la mayor concienciación en ciberseguridad y ciberdefensa o el conocimiento y empleo de las guías del CCN-STIC, tan necesarias en defensa. También sería aconsejable la obtención de las habilitaciones de seguridad (HSEM/HPS) requeridas para licitar en ciertos proyectos del sector público.

Sobre las capacidades operativas necesarias para defensa, las entidades muestran un nivel medio o alto para su desarrollo que se pone de manifiesto en las múltiples participaciones en proyectos internacionales (OTAN, UE) por parte de un gran número de estas, aunque con una cantidad limitada de productos concretos a corto plazo. En el aspecto positivo, destacan los sistemas de coordinación y control, de defensa y de apoyo técnico a las operaciones, siendo mejorable la oferta en los sistemas de Respuesta y Explotación. En todos ellos existen subcapacidades en las que las entidades demuestran una gran solvencia y otras en las que hay margen de mejora, también limitadas por el modelo de contratación propio del sector de la defensa.

Respecto a los ámbitos tecnológicos, las entidades han sido consultadas sobre un conjunto de tecnologías relacionadas con la ciberdefensa y ciberseguridad, en las que han demostrado una capacidad de desarrollo media o alta y variedad de productos propios. Entre ellos, destacan la seguridad en las redes, la inteligencia artificial, la criptografía, la seguridad de los dispositivos móviles o el procesamiento de lenguaje natural, aunque todavía con un limitado nivel de implantación en ciberdefensa. De la misma forma, se han identificado ciertas tecnologías en las que sería recomendable invertir y realizar labores de I+D+i como el *data mining*, criptografía y *blockchain*.

El presente informe también ha permitido detectar ciertas tecnologías, con funcionalidades muy potentes y que en un futuro serán imprescindibles, que las entidades no están desarrollando a corto plazo o que se están aplicando para tareas básicas, cuando podría aprovecharse mucho más dicho potencial. Entre ellas destacan el *data mining*, analítica avanzada o la inteligencia artificial.

Sobre las necesidades identificadas por la mejora o falta de desarrollos y herramientas en ciertas áreas que el Ministerio de Defensa ha estimado necesario tener cubiertas con capacidades nacionales podemos destacar los siguientes **retos**:

- Impulsar la presencia de las entidades en las licitaciones y, por tanto, incrementar el número de entidades registradas en la Plataforma de Contratación del Sector Público.
- Promover y facilitar la internacionalización de las entidades españolas del sector, fomentando su participación en proyectos de cooperación internacionales del ámbito de la OTAN y de la UE, como forma de adquisición y fortalecimiento de las capacidades propias.
- Conseguir que la totalidad de las entidades cuenten con un Sistema de Gestión de Seguridad de la Información (SGSI) implantado y una certificación de la serie ISO 27K o similar. Del mismo modo conseguir que estas entidades implanten planes de concienciación en ciberseguridad para todos los empleados; así como conseguir que conozcan y apliquen las guías CCN-STIC requeridas en las licitaciones de defensa.
- Mejorar y simplificar el procedimiento de obtención de las habilitaciones de seguridad (HSEM/HPS). Un proceso más sencillo y rápido facilitaría la incorporación de más entidades a proyectos de defensa, lo que a su vez, permitiría aumentar la masa crítica de personal cualificado para trabajar en el sector de la defensa.

- Potenciar la industria nacional con las capacidades necesarias para hacer realidad los desarrollos de los sistemas de planificación, mando, coordinación y control de operaciones en el ciberespacio, defensa, explotación, respuesta y apoyo técnico a estas operaciones en las subcapacidades en que se ha detectado una falta de desarrollos.
- Dar mayor difusión a las posibilidades y funcionalidades que ofrecen las distintas tecnologías tratadas en el presente informe que puedan aplicarse en el ámbito de la Ciberdefensa y las entidades desconozcan. Relacionado con ello, también se debe promover la formación para adquirir los conocimientos específicos que permitan el desarrollo de las capacidades relativas a este ámbito. Además, se debe potenciar el desarrollo nacional de dichas capacidades, de forma coordinada entre los diferentes actores, buscando su interoperabilidad y evitando una dependencia tecnológica de terceros.
- Establecer la necesidad de desarrollos de aplicaciones para su uso en el ámbito de la Defensa. Del mismo modo, incorporar las diferentes tecnologías analizadas, y potenciar e incentivar la inversión en I+D+i para estas tecnologías. Por último, establecer líneas estratégicas priorizadas según su importancia.
- Colaborar conjuntamente en el desarrollo de estándares de las distintas tecnologías que adolecen de estos para facilitar su implantación.

Estos y otros nuevos retos deberán ser abordados en próximos trabajos del GT4 dentro del marco del Foro Nacional de Ciberseguridad y otras iniciativas de colaboración.

1. INTRODUCCIÓN

La Estrategia Nacional de Ciberseguridad (ENCS) de 2019 establece en su objetivo III "la protección del ecosistema empresarial y social y de los ciudadanos", por el que todas las personas y organizaciones tienen derecho a hacer un uso seguro del ciberespacio. Para ello, indica que el Estado es responsable de promover e impulsar las medidas para alcanzar y mantener un nivel suficiente de ciberseguridad, que proteja especialmente a los más vulnerables y que permita el adecuado desarrollo socioeconómico de España.

La ENCS reseña que la ciberseguridad es una responsabilidad compartida con los actores privados que puedan afectarla, por acción u omisión; y que no es posible conseguirla sin su participación. Por tanto, deben promoverse medidas que fomenten la cooperación entre agentes con el objetivo de alcanzar una seguridad común. En este marco se constituyó en el año 2020 el Foro Nacional de Ciberseguridad con el objetivo de fomentar la cultura de ciberseguridad, ofrecer apoyo a la Industria e I+D+i y promover la formación y el talento en un entorno de colaboración público-privada y en conformidad con las directrices del Consejo de Seguridad Nacional.

A su vez, el Foro Nacional de Ciberseguridad creó varios grupos de trabajo, entre los que se encuentra el Grupo de Trabajo Nº4 (GT4) de Análisis e Impulso a la industria de Ciberdefensa. Este GT4 se centra en la tarea de identificar necesidades y retos para la colaboración público-privada que fomente la industria española de ciberdefensa en el sector de defensa y seguridad.

El presente informe es el resultado final de los trabajos realizados por el GT4 para completar esta tarea, está compuesto por la Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio (TEDAE), el Mando Conjunto del Ciberespacio (MCCE) y la Dirección General de Armamento y Material (DGAM. Los objetivos de estos trabajos son:

- Conocer y analizar las capacidades actuales en el ámbito nacional (fundamentalmente dentro de la industria y las academias) en el marco de las áreas genéricas de necesidades de ciberdefensa.
- Identificar posibles retos o áreas de desarrollo I+D+i en el ámbito de la ciberdefensa.

Para conocer el estado de madurez tecnológica en la que se encuentra el desarrollo de las tecnologías y capacidades requeridas en el sector de la defensa y la seguridad, se han estudiado desde capacidades de I+D+i hasta servicios o productos ya en el mercado, pasando por capacidades en materia de consultoría. Con respecto a las áreas de especialidad en ciberseguridad y ciberdefensa examinadas, destacan **tecnologías** como rea-

lidad virtual y realidad aumentada*, fog y cloud computing,* procesamiento del lenguaje natural, RPA y automatización, dispositivos móviles, seguridad en redes, *Blockchain y* DLT *(Distributed Ledger Technology),* criptografía*, Data Mining,* y analítica avanzada*,* internet de las cosas (IoT)*,* inteligencia artificial y biometría. También se han estudiado **capacidades** relevantes para el Ministerio de Defensa (MINISDEF), en otras áreas más singulares, como consciencia situacional del ciberespacio, defensa activa, intercambio de información de ciberseguridad, *cyberrange o combat cloud*. El conjunto completo de estas tecnologías y capacidades se detalla en los apartados siguientes.

Para completar el estudio, se identificaron 120 entidades del sector de la defensa y la deguridad con capacidades en materia de ciberseguridad y ciberdefensa, del ámbito empresarial, centros de investigación[1] y universidades. De estas, hubo 88 entidades que mostraron interés en participar y fueron consultadas acerca de los campos de conocimiento y capacidades tecnológicas, dentro de la ciberseguridad y ciberdefensa, que dominan y desarrollan. La mayoría de estas entidades, independientemente de su tamaño o actividad principal, apuestan por la I+D+i en ciberseguridad y ciberdefensa para ser más competitivas en sus sectores y han realizado proyectos de este tipo en los últimos años, algunas incluso obteniendo financiación externa para su ejecución.

Finalmente, tras los análisis realizados de las treinta entidades que respondieron al cuestionario, se han identificado diferentes oportunidades de mercado o retos en cuanto a la realización de proyectos I+D+i relacionados con la ciberseguridad y la ciberdefensa, no cubiertos actualmente por las tecnologías y capacidades estudiadas que se considera que tienen mayores expectativas en los próximos años.

[1] Bajo el término centros de investigación están también incluidos los centros tecnológicos.

2. CONTEXTO

El reconocimiento del ciberespacio como un ámbito operativo militar impone la necesidad de contar tanto con unidades especializadas como con sistemas específicos para operar en él y para lograr una superioridad en el enfrentamiento contra ciberataques de potenciales adversarios que, derivada de la transversalidad del ciberespacio, tendrá importante incidencia en el resto de ámbitos operativos (terrestre, naval, aéreo y espacial).

Por otra parte, la evolución hacia las operaciones multidominio, la hiperconectividad creciente entre los elementos en zona de operaciones y la transversalidad del ciberespacio incrementan enormemente el frente de ataque, exponiendo mayor cantidad de sistemas a posibles adversarios. Por tal motivo, la ciberdefensa no puede enfocarse solamente a las redes y a los sistemas de información, sino que debe también abarcar los sistemas de armas y plataformas, sensores, sistemas no tripulados, sistemas autónomos y otros sistemas que basen su funcionamiento en el uso del ciberespacio.

Es por ello que nuestras Fuerzas Armadas deben contar con medios que les permitan:

- Una visión común y completa de la situación en el ciberespacio de interés militar.
- El intercambio rápido y completo de información con el fin de apoyar convenientemente la toma de decisiones.
- La ejecución coherente y coordinada de todas las operaciones (de infraestructura, defensa, explotación y ataque) que se desarrollen en el ciberespacio.
- La formación, instrucción y adiestramiento correspondientes.

Entendemos el término **Ciberseguridad**[2] como "la actividad, proceso, capacidad o estado por el cual las redes y sistemas de información y telecomunicaciones, así como la información que contienen, procesan y transmiten, están protegidos o defendidos frente al daño, uso no autorizado, modificación o explotación, preservando la confidencialidad, integridad y disponibilidad de la información en el ciberespacio. Comprende las tecnologías, políticas, procesos y prácticas diseñados para proteger las redes, ordenadores, programas, datos e información frente a ataques, daños o cambios, accesos no intencionados o no autorizados, abarcando todo el espectro de reducción de amenazas y de vulnerabilidades, la disuasión, la respuesta a incidentes, la resiliencia y las políticas y actividades de recuperación, incluyendo *computer network operations*, seguridad de la información *(information assurance),* la aplicación de medidas legales,

[2] Definición obtenida del documento PDC-3.20 "Doctrina de operaciones en el ámbito ciberespacial" (adaptación nacional del AJP 3.20 de la OTAN) sancionada por el JEMAD en abril de 2021.

los compromisos internacionales, las acciones diplomáticas, militares y operaciones de inteligencia".

Por su parte, la **Ciberdefensa**[3] se entiende como "el conjunto de capacidades de coordinación y control, defensa, explotación y ataque que permiten llevar a cabo operaciones en el ciberespacio con la finalidad de preservar o ganar la libertad de acción en el ciberespacio de interés militar, impedir o dificultar su uso por parte del adversario, y contribuir a alcanzar la superioridad en el enfrentamiento en el resto de ámbitos físicos y cognitivo".

En síntesis, se puede decir que la Ciberseguridad y la Ciberdefensa se complementan, con la diferencia de que la primera trata de las soluciones que protegen frente a amenazas genéricas del ciberespacio, mientras que la segunda se refiere además a capacidades orientadas a realizar operaciones militares en el ciberespacio para defender activamente de los ciberataques, obtener información de las ciberamenazas y generar efectos sobre las redes y sistemas del adversario. Por tanto, los desarrollos y productos de ciberseguridad son de gran interés para reforzar las capacidades de ciberdefensa que requiere la Defensa Nacional.

---

[3] Definición obtenida del documento Concepto de ciberdefensa, aprobado por el JEMAD, de 28 de septiembre de 2018.

3. METODOLOGÍA DEL ESTUDIO

A continuación, se detallan las fases de la metodología seguida para la realización del estudio:

Figura 1: Metodología del estudio

3.1. Definición de datos que se desean obtener y elaboración de cuestionario

En primer lugar, fue necesario establecer y definir un conjunto de datos generales de las entidades y áreas de conocimiento dentro de la Ciberseguridad y Ciberdefensa, acorde a las últimas tendencias y necesidades específicas del MINISDEF, para poder tratar y explotar esta información posteriormente.

Las áreas de conocimiento identificadas fueron las cuatro siguientes:

1. Datos de la organización y punto de contacto: información que permite segmentar los resultados del estudio sobre la base del tipo de organización que responde al cuestionario. Dentro de esta sección se han identificado los siguientes datos que se desea obtener:
    - Detalle de la empresa, tipo de organización, pertenencia a mercado bursátil/tipo, sector, grado de implantación y número de sedes.
2. Cuestiones generales: información general de la entidad referente a contratación, habilitaciones de seguridad, seguridad de la información, etc. Dentro de esta sección se ha identificado la siguiente información datos que se desea obtener:
    - Relaciones previas con el sector público, conocimiento de la estructura y procesos del Ministerio de Defensa y las Fuerzas Armadas, experiencia en proyectos OTAN/EDA, Plan de Gestión de la Seguridad de la Información, conocimiento de las guías CCN-STIC y disposición de habilitaciones de seguridad (HSEM y HPS).
3. Desarrollos aplicables a las capacidades operativas: información sobre desarrollos (o capacidad de la organización para llevarlos a cabo a corto plazo) relacionados con las capacidades operativas genéricas de ciberdefensa y su vinculación con tecnologías. Dentro de esta sección se han identificado las siguientes capacidades, cada una a su vez con un conjunto de subcapacidades de más bajo nivel que se definen en detalle a lo largo del informe:
    - Coordinación y control en operaciones en el ciberespacio, defensa, explotación, respuesta y apoyo técnico a las operaciones.
4. Ámbitos tecnológicos: información segmentada en doce ámbitos tecnológicos, enfocada a su aplicación en las necesidades en ciberdefensa. La información obtenida en esta sección complementa la de la sección anterior para determinar las capacidades reales y potenciales de la Industria nacional. Dentro de esta sección se han identificado los siguientes ámbitos de interés:
    - Cuestiones generales, realidad virtual y realidad aumentada, *cloud* y *fog computing*, procesamiento de lenguaje natural, RPA y automatización, dispositivos móviles, seguridad de redes, *blockchain* y DLT, criptografía, *data mining*, analítica avanzada, IoT, inteligencia artificial y biometría.

La definición y explicación de los ámbitos tecnológicos tratados en el cuestionario se describen exhaustivamente en el ANEXO I: Descripción de los ámbitos tecnológicos.

A continuación, se elaboró un cuestionario, compuesto de 83 preguntas relativas a estas cuatro áreas definidas. Se facilitó un conjunto de respuestas adaptadas para facilitar su cumplimentación y posterior análisis. El formato permitía a los participantes añadir información adicional que pudiera ser de interés.

3.2. Selección de entidades y puntos de contacto

Se determinó el público objetivo del cuestionario dentro del ecosistema nacional de la ciberseguridad y la ciberdefensa. Para ello, se invitó a participar en él a empresas, universidades y centros de investigación relacionados con los organismos participantes en el GT4: TEDAE, MCCE, DGAM y RENIC (Red de Excelencia Nacional de Investigación en Ciberseguridad).

Se identificaron 120 entidades del sector de la defensa y la seguridad con capacidades aplicables a la ciberseguridad y ciberdefensa, tanto del ámbito empresarial como centros de investigación y universidades, para las que se estableció un punto de contacto.

3.3 Envío de cuestionarios

Se remitió el cuestionario por correo electrónico a las 88 entidades que mostraron interés en participar para su distribución y cumplimentación en el ámbito de su entidad.

Se estableció un plazo inicial de dos meses, que posteriormente fue ampliado debido a la complejidad del cuestionario para completarlo y devolverlo para su estudio.

3.4. Recepción y extracción de la información

Dado que la información recogida en el cuestionario podía ser de carácter sensible para las organizaciones, se solicitó que fuera devuelta en formato cifrado. Para garantizar su confidencialidad, se facilitó el uso de un *software* de cifrado (EP880) aprobado por el Centro Criptológico Nacional (CCN) a los participantes.

Finalmente, treinta entidades respondieron con el cuestionario cumplimentado. Estos cuestionarios han sido empleados para generar la muestra de datos del estudio.

A continuación, se realizó la extracción segura de los datos recibidos y su homogeneización debido a las diferencias encontradas en las distintas respuestas. Éstas fueron categorizadas y formateadas para facilitar su posterior tratamiento. Además, estos datos fueron anonimizados evitando relacionar las distintas respuestas obtenidas con las entidades participantes.

3.5. Análisis de los resultados

Al estar dirigido el cuestionario a un conjunto de organizaciones muy heterogéneo, las respuestas recibidas han sido dispares. Esta circunstancia ha obligado a desarrollar un cuidadoso proceso de análisis mediante el cual se pudieran obtener resultados de valor.

A partir de la información generada, un grupo de expertos en ciberseguridad y ciberdefensa realizó su tratamiento estadístico y análisis, obteniendo una serie de conclusiones y reflexiones. Además, se generaron los gráficos y estadísticas necesarios para apoyar estos resultados.

3.6. Elaboración del informe

La estructura adoptada para este documento buscó la representación de los resultados obtenidos de forma clara y útil.

A continuación, se elaboró el presente informe que comprendía el análisis realizado, las conclusiones obtenidas y los retos identificados, junto con otros apartados generales de ayuda y anexos.

3.7. Publicación del informe

Finalmente, el informe se ha publicado en la página del Foro Nacional de Ciberseguridad[4] para permitir su libre consulta.

Además, se pretende compartir el estudio realizado en diferentes jornadas relacionadas con la ciberseguridad y la ciberdefensa.

[4] https://foronacionalciberseguridad.es/

4. COMPARATIVAS SOBRE DATOS DE LA ORGANIZACIÓN Y PUNTO DE CONTACTO

A continuación, se muestran las comparativas realizadas sobre el apartado Datos de la organización y punto de contacto del cuestionario. Dentro de cada subapartado se recoge la pregunta realizada, las respuestas obtenidas y las primeras conclusiones alcanzadas.

Hay que aclarar que algunas entidades han declarado que varias opciones (respuestas múltiples) son de aplicación en algunas cuestiones, por lo que estas no son excluyentes entre sí y se han tenido en cuenta todas. Por esta razón, en algunas gráficas se puede encontrar que la suma de los porcentajes de las opciones es superior al 100% al estar referido al número de entidades que ha respondido a cada opción.

4.1. Tipo de organización

Los datos recogidos en la pregunta *1. Indique a qué tipo de organización pertenece* se muestran en la siguiente figura:

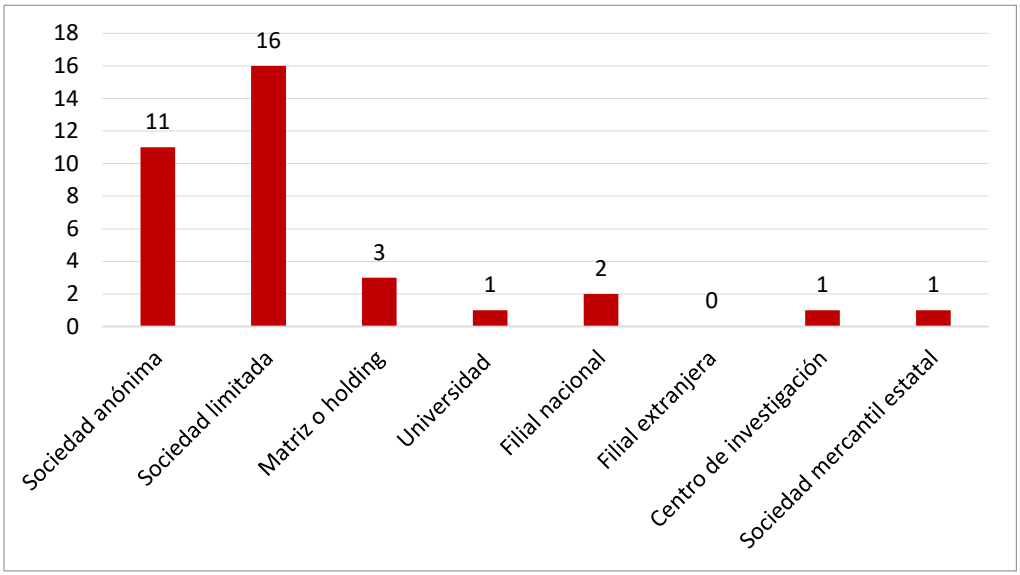


Figura 2. P1: Datos Tipo de organización

La representación gráfica de estos datos se muestra en la siguiente figura:

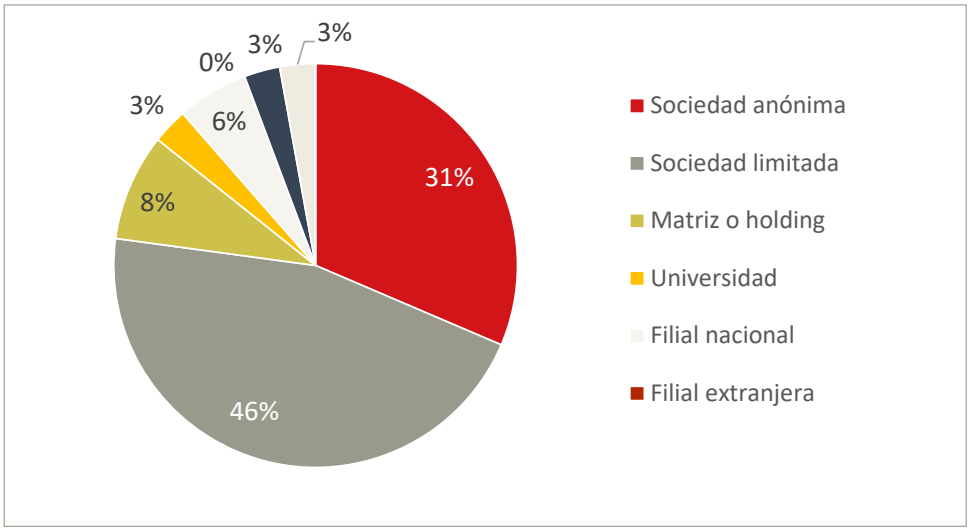


Figura 3. P1: Gráfico. Tipo de organización

Se puede observar que la mayoría de las entidades encuestadas son sociedades limitadas y sociedades anónimas. Un grupo menor ha detallado aún más su tipo de organización indicando también que son matriz o *holding* o filial nacional de algún grupo de empresas.

En cuanto a la participación de universidades, centros de investigación y de sociedades mercantiles estatales en el estudio tan solo se ha contado con un 3% de cada tipo y ha sido nula en el caso de filiales extranjeras de empresas.

4.2 Pertenencia a mercado bursátil

Los datos recogidos en la pregunta *2. ¿Pertenece al mercado bursátil?* se muestran en la siguiente figura:

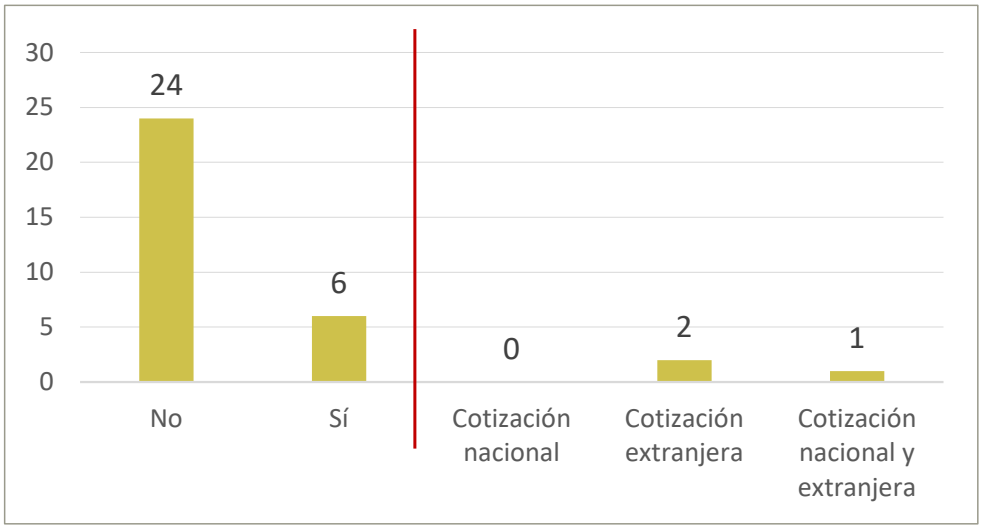


Figura 4. P2: Datos Pertenencia mercado bursátil

Se puede observar que la mayoría de las entidades encuestadas no cotiza en ningún tipo de mercado bursátil. Para la minoría que sí lo hace (6), la representación gráfica de los datos del tipo de cotización se muestra en la siguiente figura:

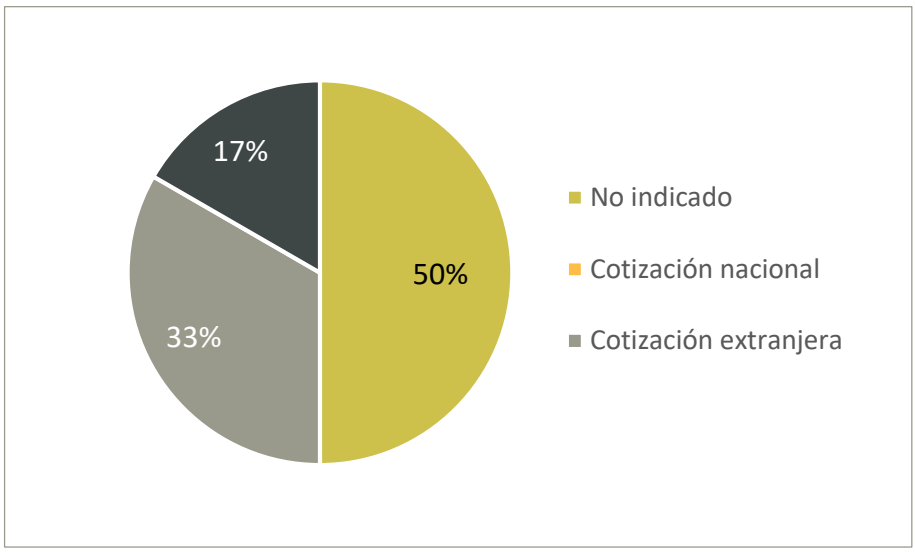


Figura 5. P2: Gráfico. Tipo mercado bursátil

De las entidades que cotizan en algún mercado bursátil, la mitad no ha indicado el tipo y las otras indican que prefieren la bolsa extranjera a la nacional.

4.3 Sectores según su actividad principal

Los datos recogidos en la pregunta *3. ¿En qué sector se ubica su empresa según su actividad principal?* se muestran en la siguiente figura:

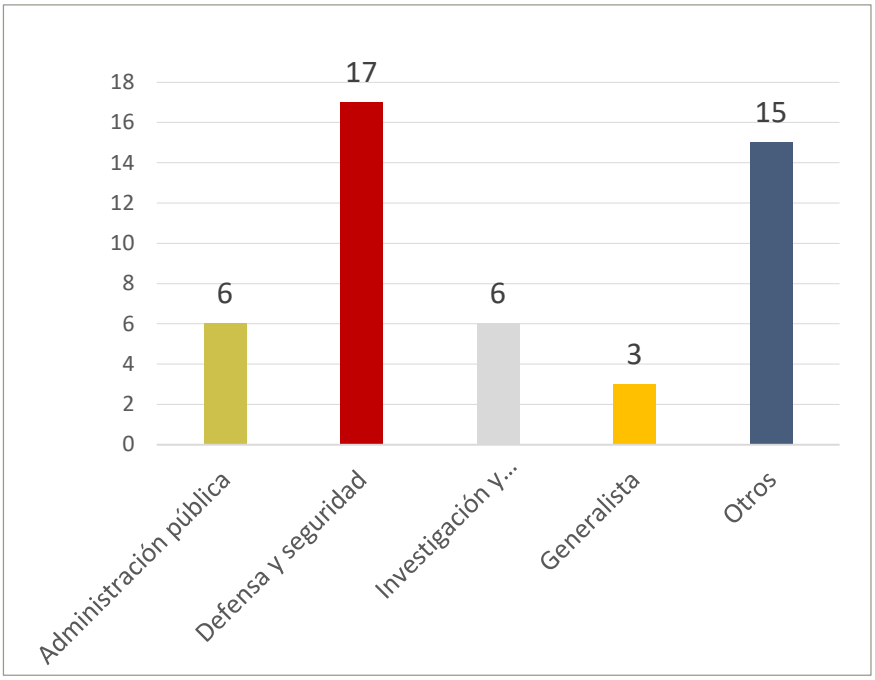


Figura 6. P3: Datos Actividad principal

La representación gráfica de los datos se muestra en la siguiente figura:

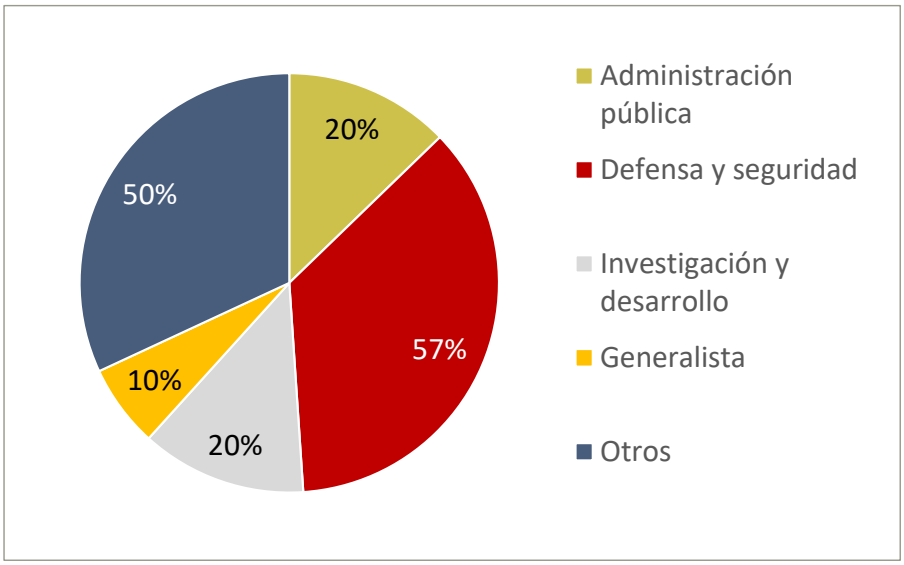


Figura 7. P3: Gráfico. Actividad principal

Como era de esperar, más de la mitad de las entidades relacionadas con la ciberseguridad y la ciberdefensa se encuentra en el sector de la defensa y seguridad, y otra mitad ha respondido pertenecer a otros sectores no indicados. Los siguientes sectores que más interés han mostrado en estos ámbitos son la Administración Pública y la investigación y desarrollo, ambos con un 20%.

Dentro de los sectores genéricos definidos en el estudio, algunas entidades han detallado en sus comentarios la pertenencia a diferentes entornos específicos como consultoría, telecomunicaciones, laboratorio, ciberseguridad, Inteligencia en o a través del ciberespacio, aeroespacial o aeronáutico.

No se ha podido atraer a un mayor número de empresas, centros de investigación y universidades para la elaboración de este estudio por, tal vez, razones de sensibilidad de la información. Para futuros estudios sería recomendable invitar a otro tipo de entidades para lograr mayor diversidad de respuestas, soluciones y proyectos.

4.4 Grado de implantación de las entidades

Los datos recogidos en la pregunta *4. ¿Qué grado de implantación tiene su organización?* se muestran en la siguiente figura:

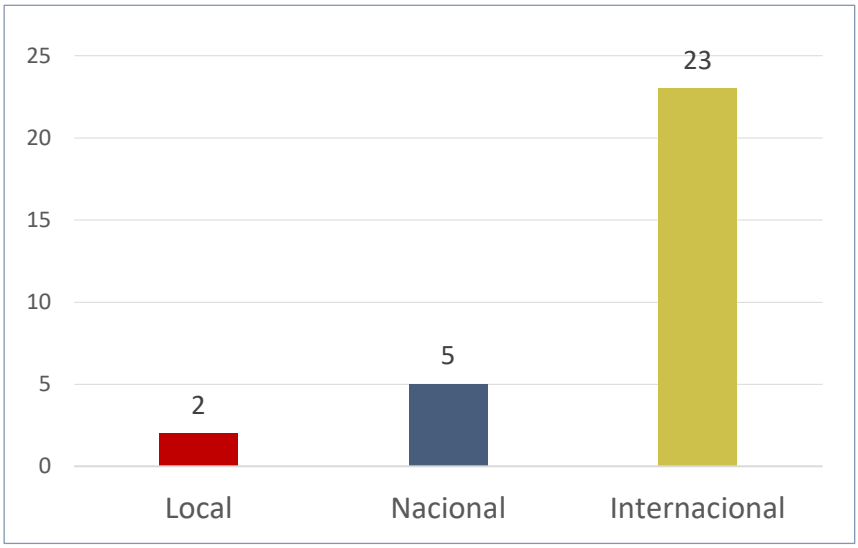


Figura 8. P4: Datos Grado de implantación de entidades

La representación gráfica de los datos se muestra en la siguiente figura:

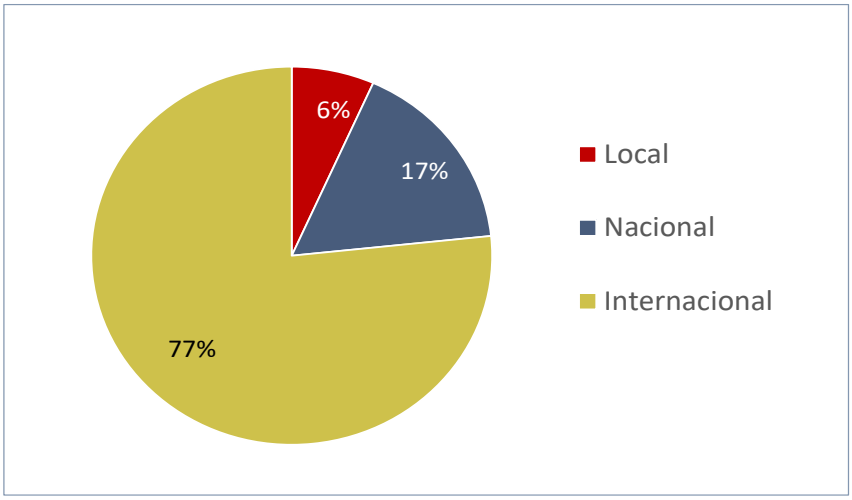


Figura 9. P4: Gráfico. Grado de implantación de las entidades

Destaca la implantación internacional de la mayoría de las entidades participantes. Se considera que este dato tiene su explicación en que los sectores de la ciberseguridad y ciberdefensa requieren una fuerte cooperación internacional por las altas inversiones necesarias y el gran número de tecnologías implicadas. Esto ofrece grandes beneficios al participar en proyectos multinacionales; además de la ampliación de negocio a los mercados internacionales. Este dato es coherente con la información posterior relacionada con la participación en proyectos internacionales.

4.5 Número de sedes de las entidades

Los datos recogidos en la pregunta *5. Indique el número de sedes que tiene su organización* se muestran en la siguiente figura:

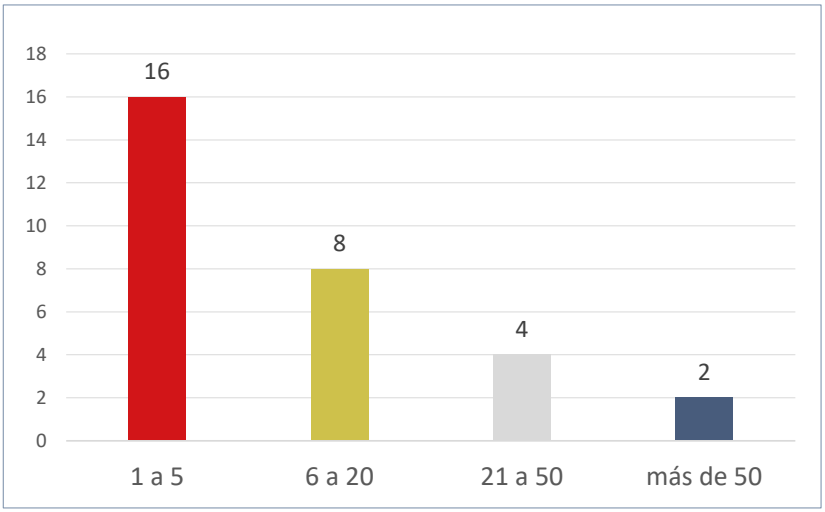


Figura 10. P5: Datos Número de sedes

La representación gráfica de los datos se muestra en la siguiente figura:

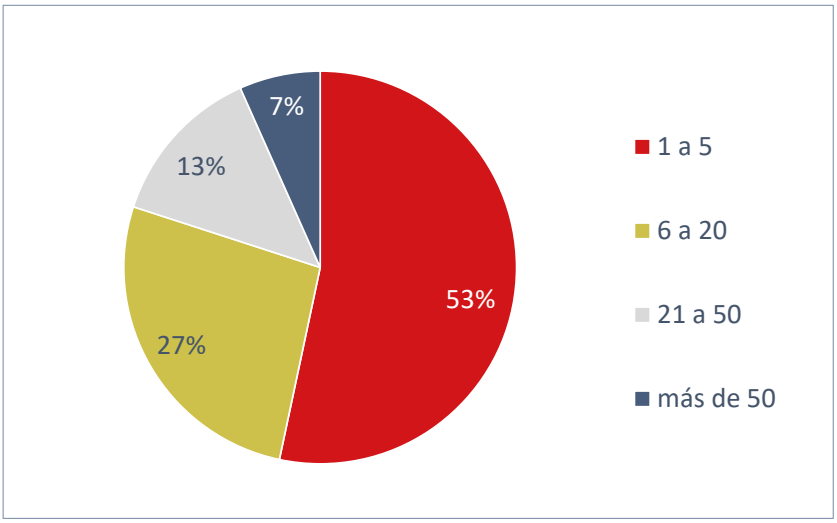


Figura 11. P5: Gráfico. Número de sedes

Se observa que la mitad de las entidades participantes tienen cinco sedes o menos. Y dentro de éstas, la mitad tienen solo una sede, siendo el dato más repetido. Destaca la participación en el estudio de grandes entidades con más de veinte sedes, incluso al menos una declara tener más de doscientas cincuenta.

Los datos obtenidos son coherentes con los tipos de organización (matriz/*holding*) y de implantación indicados en preguntas anteriores al contar con un gran número de entidades con más de una sede y con un 80% de los participantes.

5. COMPARATIVAS SOBRE CUESTIONES GENERALES

A continuación, se muestran las comparativas realizadas sobre el apartado Cuestiones generales del cuestionario. Dentro de cada subapartado se recoge la pregunta realizada, las respuestas obtenidas y las primeras conclusiones alcanzadas.

5.1 Familiarización con la Ley de Contratos del Sector Público

Los datos recogidos en la pregunta *6. ¿Su organización está familiarizada con la Ley de Contratos del Sector Público?* se muestran en la siguiente figura:

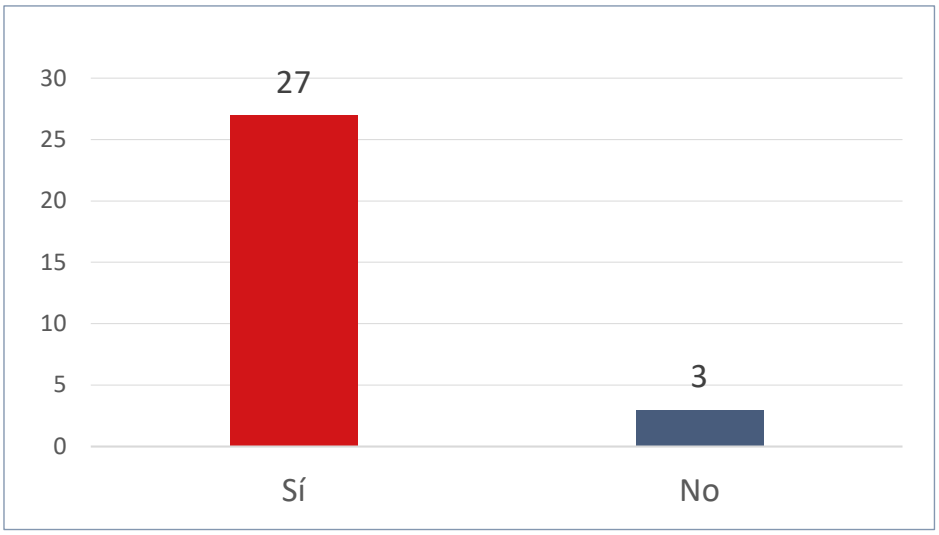


Figura 12. P6: Datos Familiarización con la Ley de Contratos del Sector Público

La representación gráfica de los datos se muestra en la siguiente figura:

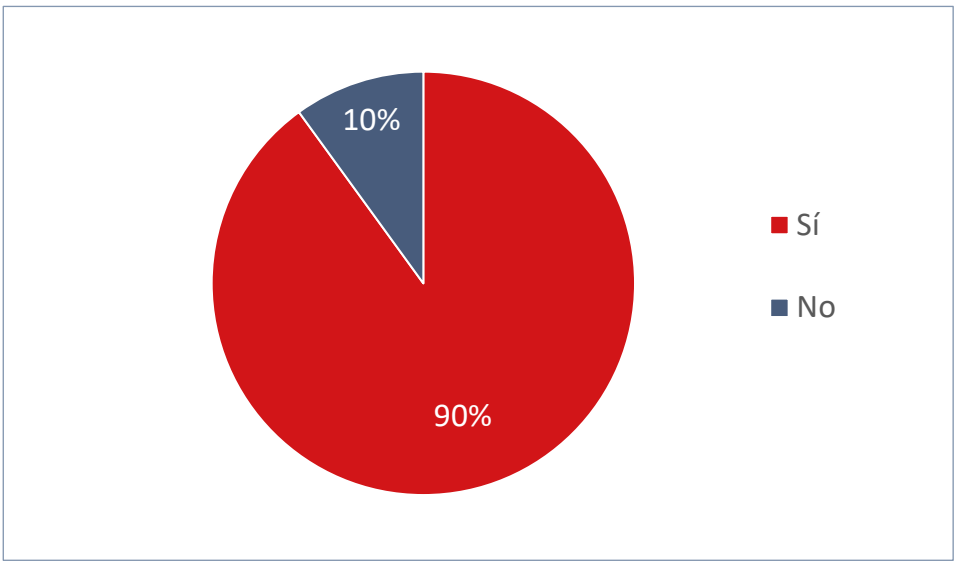


Figura 13. P6: Gráfico. Familiarización con la Ley de Contratos del Sector Público

El gráfico anterior refleja la importante relación público-privada existente en el sector de la ciberseguridad y ciberdefensa. Se deduce que la mayor parte de las entidades ha tenido relación directa con el sector público y pone de manifiesto el buen nivel de colaboración de la Industria nacional con este sector.

5.2 Alta en Plataforma de Contratación del Sector Público

Los datos recogidos en la pregunta 7. *¿Su organización está dada de alta en Plataforma de Contratación del Sector Público?* se muestran en la siguiente figura:

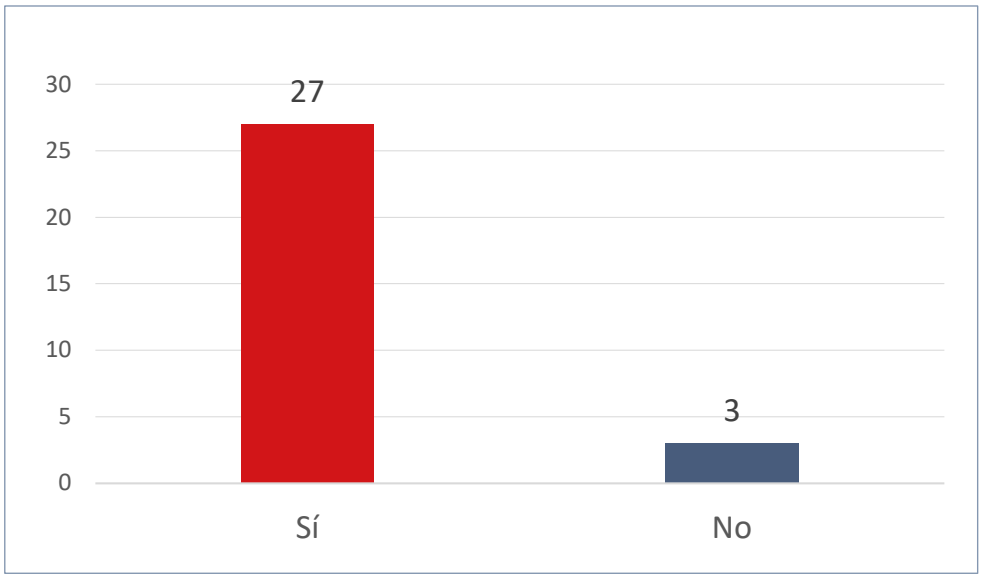


Figura 14. P7: Datos Alta en Plataforma de Contratación del Sector Público

La representación gráfica de los datos se muestra en la siguiente figura:

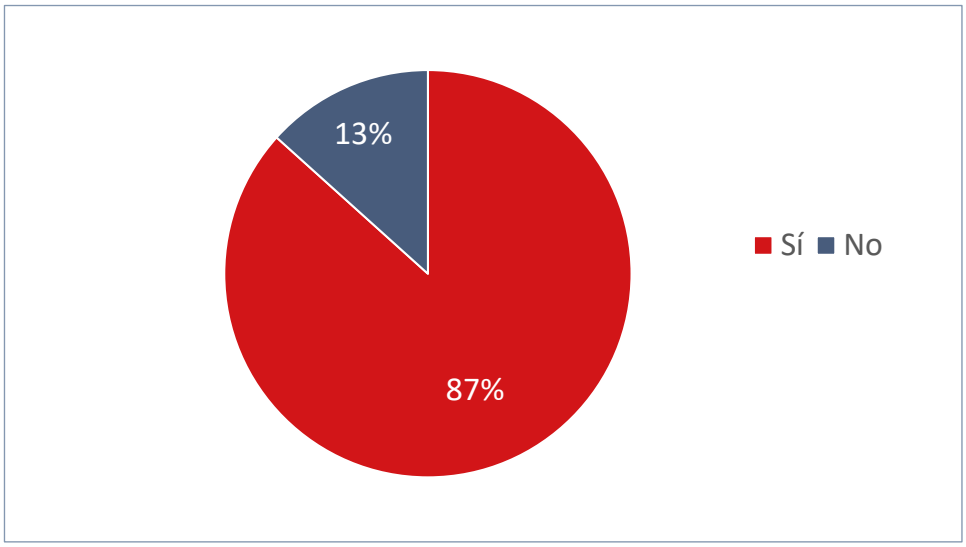


Figura 15. P7: Gráfico. Alta en Plataforma de Contratación del Sector Público

Los resultados son coherentes con los obtenidos en la pregunta anterior. Como resultado la mayoría de las entidades se encuentran dadas de alta en la Plataforma de Contratación del Sector Público. Se deduce que la mayor parte de las entidades ha participado en alguna licitación del sector público.

5.3 Disposición de expertos con conocimientos de la estructura y procesos del Ministerio de Defensa

Los datos recogidos en la pregunta *8. ¿Disponen de expertos que conozcan la estructura y procesos del Ministerio de Defensa?* se muestran en la siguiente figura:

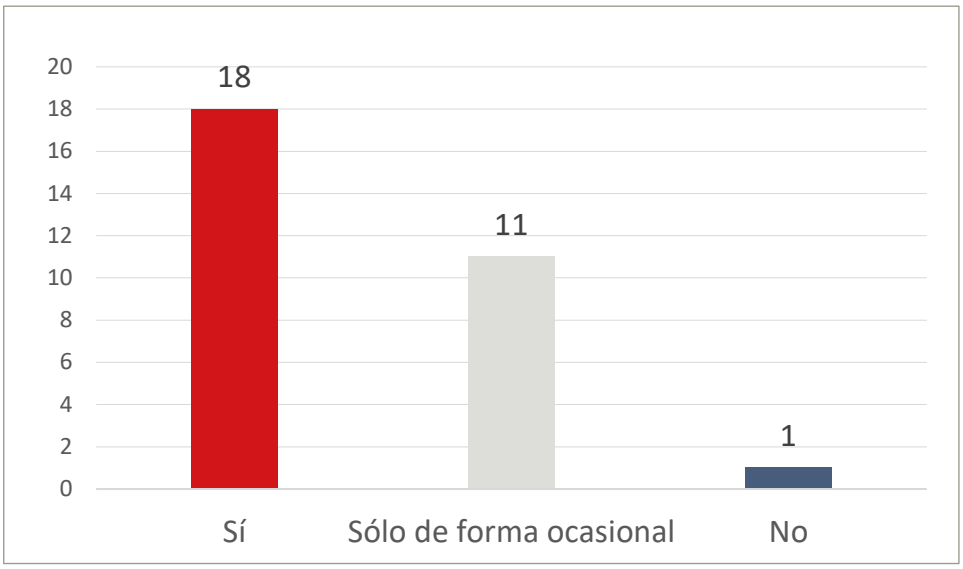


Figura 16. P8: Datos Expertos con conocimiento de la estructura y procesos del Ministerio de Defensa

La representación gráfica de los datos se muestra en la siguiente figura:

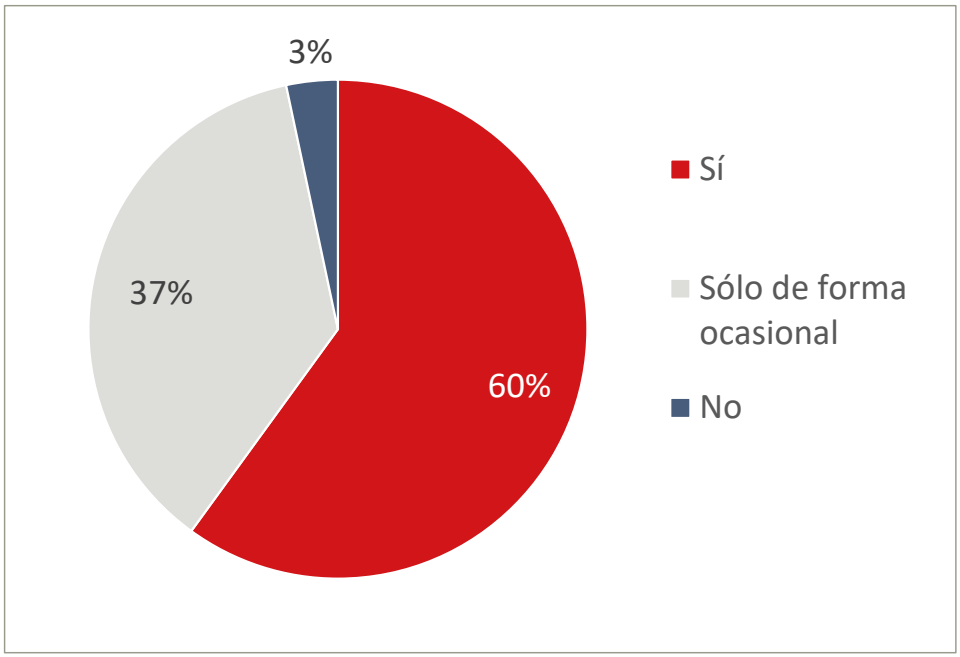


Figura 17. P8: Gráfico. Expertos con conocimiento de la estructura y procesos del Ministerio de Defensa

De forma muy relacionada con las dos cuestiones anteriores, la mayoría de las entidades declara que cuenta entre su personal con expertos que conocen la estructura y procesos del MINISDEF, lo que constituye un requisito imprescindible para participar exitosamente en cualquier licitación lanzada por este ente. Otro tercio indica que ha contado con dicho personal ocasionalmente, de lo que se deduce que la entidad obtuvo asesoramiento. Y cabe recalcar que sólo una entidad indica que no dispone de este tipo de conocimiento en su organización.

5.4 Disposición de expertos con conocimientos de la estructura y procesos de las Fuerzas Armadas

Los datos recogidos en la pregunta *9. ¿Disponen de expertos que conozcan la estructura y procesos de las Fuerzas Armadas?* se muestran en la siguiente figura:

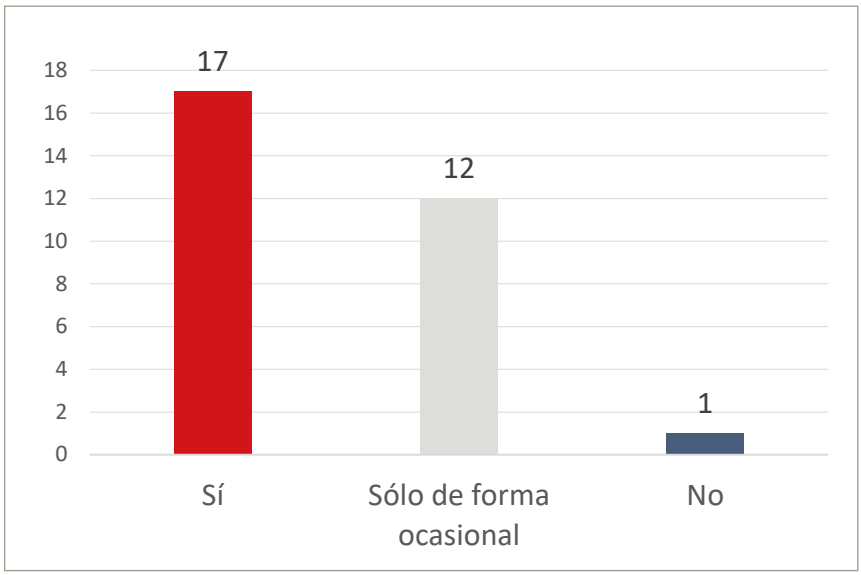


Figura 18. P9: Datos Expertos con conocimientos de la estructura y procesos de Ministerio de las Fuerzas Armadas

La representación gráfica de los datos se muestra en la siguiente figura:

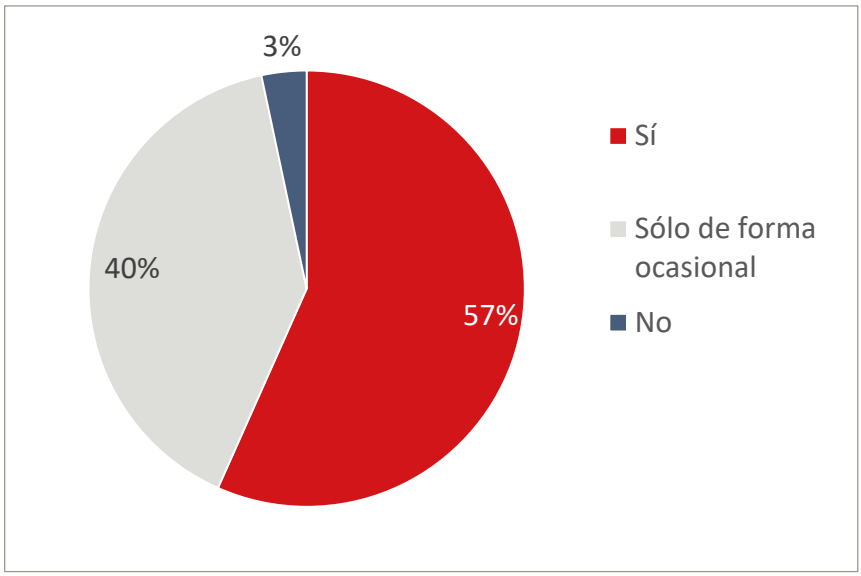


Figura 19. P9: Gráfico. Expertos con conocimientos de la estructura y procesos de Ministerio de las Fuerzas Armadas

Los resultados obtenidos en esta cuestión son coherentes con los de la pregunta anterior sobre el conocimiento de la estructura y procesos del MINISDEF, dada la relación entre

ellas. Más de la mitad de las entidades declara que cuenta entre su personal con expertos que conocen la estructura y procesos de las Fuerzas Armadas, mientras que algo menos de la mitad indica haber contado con este tipo de personal ocasionalmente.

5.5 Experiencia en proyectos de la OTAN o de la Agencia Europea de Defensa (EDA)

Los datos recogidos en la pregunta *10. ¿Tiene su organización experiencia en proyectos de la OTAN o de la Agencia Europea de Defensa (PESCO, EDF, EDIPD, etc.)?* se muestran en la siguiente figura:

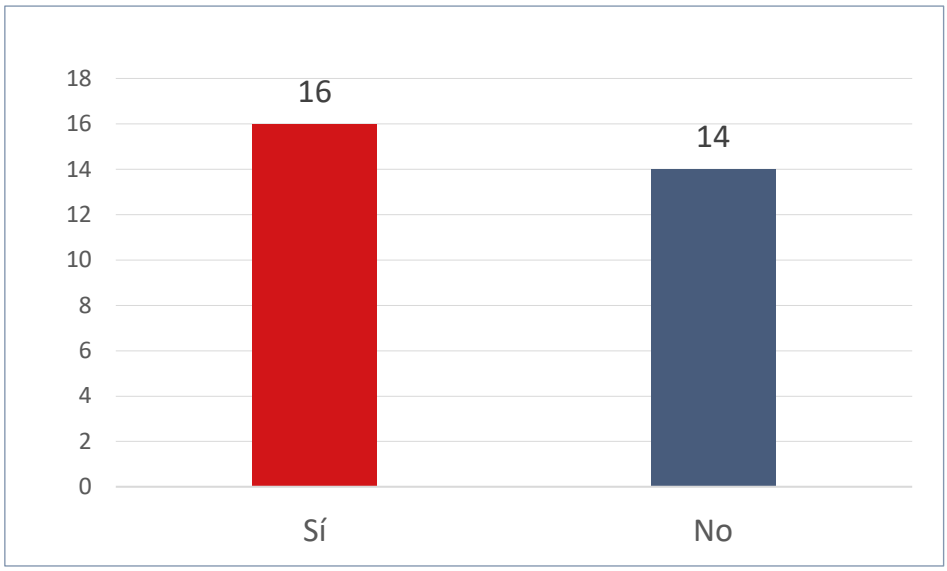


Figura 20. P10: Datos Experiencia en proyectos OTAN/EDA

La representación gráfica de los datos se muestra en la siguiente figura:

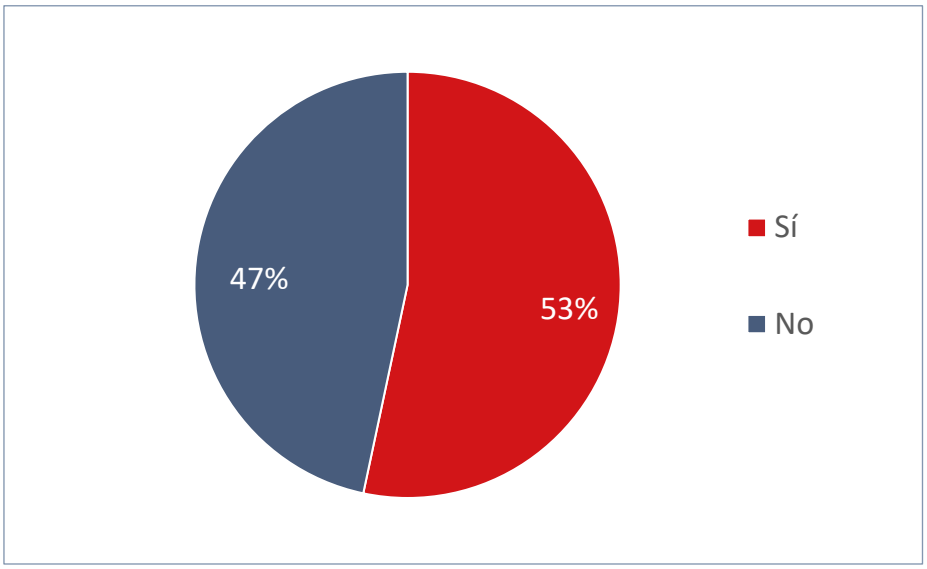


Figura 21. P10: Gráfico. Experiencia en proyectos OTAN/EDA

En los últimos años se ha apreciado un notable incremento en el número de proyectos internacionales en el ámbito de la ciberseguridad y ciberdefensa, fundamentalmente enmarcados en PESCO, EDIPD y EDF de la Agencia Europea de Defensa. El hecho de que más de la mitad de las entidades haya participado en algún proyecto de este tipo es una señal de la calidad de los desarrollos y la buena imagen internacional de la Industria española de ciberseguridad y ciberdefensa.

En relación con esto, es importante recordar que una de las funciones del **Foro Nacional de Ciberseguridad** es "apoyar la proyección y participación de España a nivel internacional y europeo en materia de ciberseguridad y ciberdefensa". Para ello, se creó el **Grupo de Trabajo 4 (GT4)** de Análisis e impulso a la industria de ciberdefensa) que tiene como objetivo, entre otros, "fomentar la oferta de productos y capacidades de ciberdefensa de la industria española para satisfacer las necesidades de la defensa". Dentro de este GT4, participa entre otros la **DGAM**, la cual tiene como una de las misiones fundamentales "apoyar el desarrollo de la base industrial y tecnológica nacional de defensa", y **TEDAE** que tiene entre sus fines la "promoción de sus asociados tanto a nivel nacional como internacional". Todos ellos, de forma coordinada, buscan apoyar la participación de la Industria española en proyectos de cooperación internacionales del ámbito de la OTAN y la EDA.

Con lo indicado en las preguntas 2, 4 y 10, podemos decir que las entidades participantes en el cuestionario tienen un nivel de internacionalización alto. La mayoría declara que tiene implantación internacional, incluso en algunos casos cotizan fuera de España. Además, la mitad de las entidades indica que ha participado en proyectos de la OTAN o de la EDA, lo que confirma la calidad de los desarrollos y la la buena imagen internacional de la Industria española de Ciberseguridad y Ciberdefensa. Esta participación de la Industria en proyectos internacionales nos permite augurar una mayor actividad a corto plazo en el ámbito internacional de ciberdefensa.

5.6 Implantación del Plan de Gestión de Seguridad de la Información

Los datos recogidos en la pregunta *11. ¿Cuenta la organización con un Plan de Gestión de Seguridad de la Información?* se muestran en la siguiente figura:

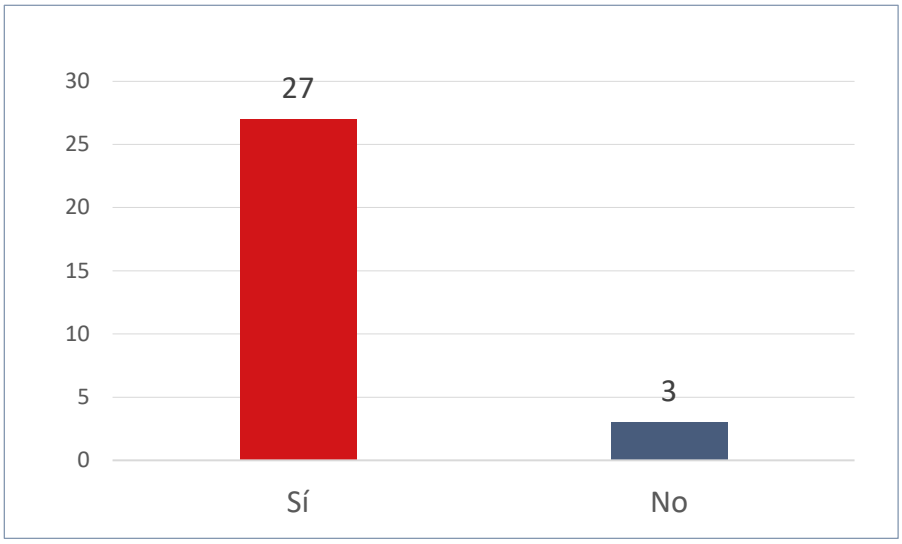


Figura 22. P11: Datos Plan de Gestión de Seguridad de la Información

La representación gráfica de los datos se muestra en la siguiente figura:

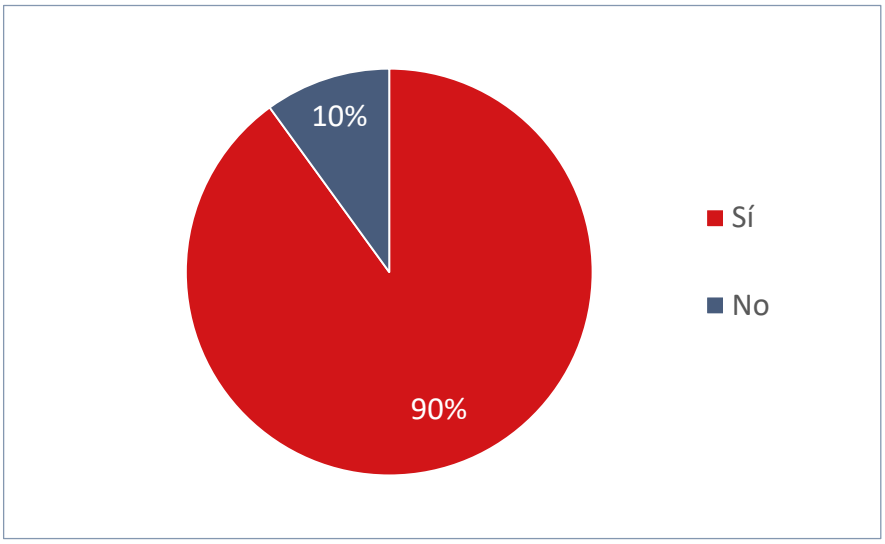


Figura 23. P11: Gráfico. Plan de Gestión de Seguridad de la Información

En esta pregunta, era de esperar que el 100% de las entidades relacionadas con el sector de la ciberseguridad y ciberdefensa hubieran implementado un Plan de Gestión de Seguridad de la Información en sus propias organizaciones, pero la cifra se ha quedado en un 90%. Esto demuestra que la mayoría de las entidades están concienciadas adecuadamente en ciberseguridad, aunque no todas.

La concienciación en ciberseguridad de todo el personal de las entidades, especialmente los involucrados en el desarrollo de los sistemas, los prestadores de servicios y la alta dirección es un objetivo muy importante para preservar la ciberseguridad de la entidad. Debe perseguirse una madurez en la cultura de ciberseguridad empresarial o académica que fomente la concienciación entre sus empleados para poder aplicarla posteriormente a los servicios prestados o a los productos desarrollados.

Además, la mayoría de las licitaciones en el sector público incluye como requisito obligatorio el cumplimiento del ENS (Esquema Nacional de Seguridad) para poder participar. Este está siendo un factor diferenciador entre los licitadores, lo que en la práctica funciona como una criba automática entre los que realizan una adecuada y evaluada Gestión de Seguridad de la Información en sus entidades y los que no.

5.7 Certificaciones de la serie ISO 27K o similar

Los datos recogidos en la pregunta *12. ¿Cuenta la organización con alguna certificación de la serie ISO 27K o similar?* se muestran en la siguiente figura:

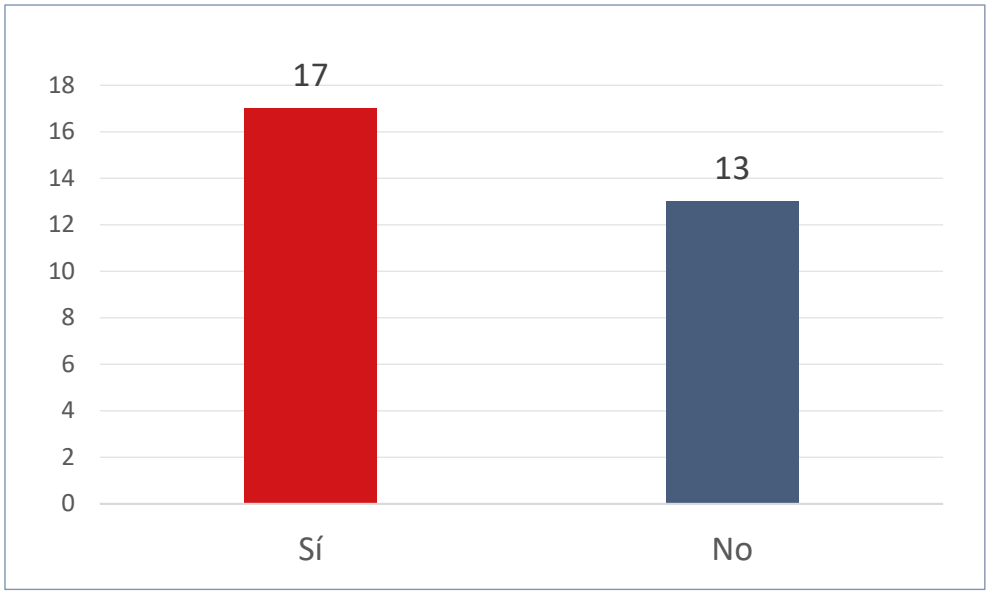


Figura 24. P12: Datos Certificación ISO 27K o similar

La representación gráfica de los datos se muestra en la siguiente figura:

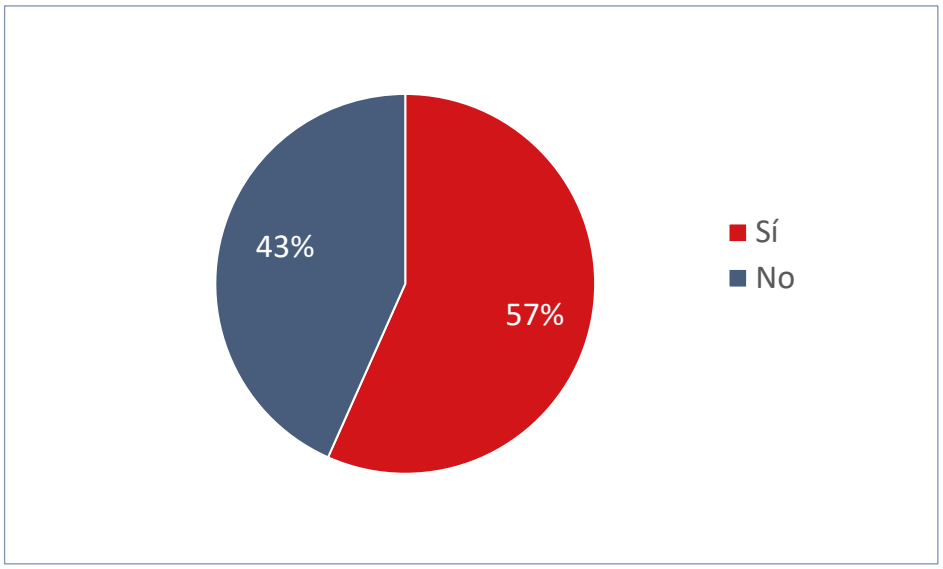


Figura 25. P12: Gráfico. Certificación ISO 27K o similar

Al igual que en la pregunta anterior, se esperaba un porcentaje muy alto de respuestas positivas y, sin embargo, la diferencia ha sido aún mayor, ya que poco más de la mitad de las entidades disponen de alguna certificación de seguridad. Al haber indicado anteriormente que se dispone de un Plan de Gestión de Seguridad de la Información, seguramente apoyado por un Sistema de Gestión de Seguridad de la Información (SGSI), sería relativamente sencillo completar las acciones necesarias para obtener la certificación relacionada.

Estas respuestas pueden poner en duda la adecuada concienciación en ciberseguridad de las entidades y su personal. No disponer de al menos una certificación de este tipo puede llevar a pensar que la gestión de la ciberseguridad en las entidades no se esté realizando de la mejor forma posible o de una forma reconocida o evaluada.

La posesión de este tipo de certificado puede resultar muy positiva para las entidades ya que, por un lado, van a ver incrementada su madurez en ciberseguridad y, por otro, estas entidades tomarán ventaja frente a aquellas que no cuenten con él en las licitaciones que lo exijan, tanto a nivel nacional como internacional.

Habría que fomentar que la Administración Pública solicitara este requisito en las licitaciones del Estado dado que actualmente se exige el cumplimiento del ENS, de las obligaciones de seguridad en las redes y sistemas de información indicado en el *Real Decreto-ley 12/2018 de transposición de la Directiva NIS de la UE* que lo desarrolla, que podría ser acreditado mediante la certificación en un esquema de seguridad reconocido por una autoridad competente, como el ISO 27K, y requisitos de ciberseguridad relacionada con el riesgo tecnológico y la cadena de suministros.

5.8 Familiarización con las Guías de seguridad de la serie CCN-STIC

Los datos recogidos en la pregunta *13. ¿Está la organización familiarizada con las Guías de seguridad de la serie CCN-STIC?* se muestran en la siguiente figura:

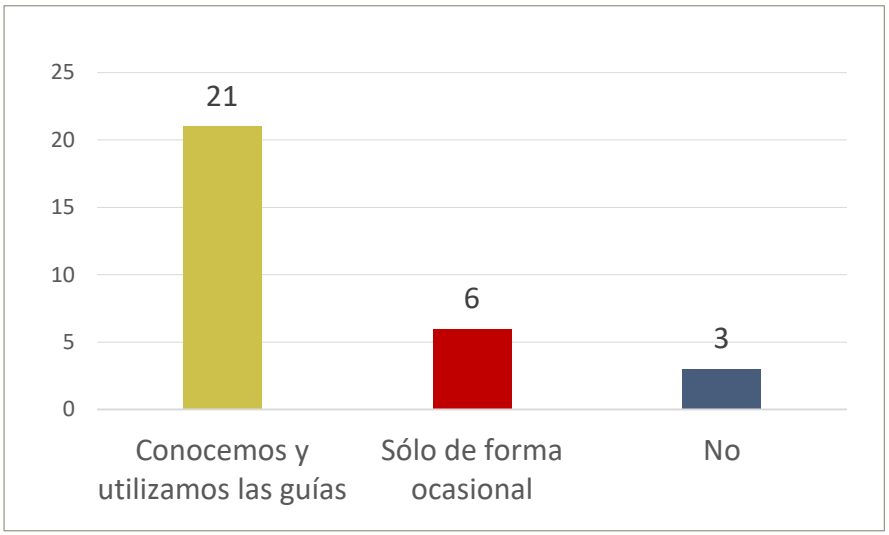


Figura 26. P13: Datos Familiarización con guías de seguridad de la serie CCN-STIC

La representación gráfica de los datos se muestra en la siguiente figura:

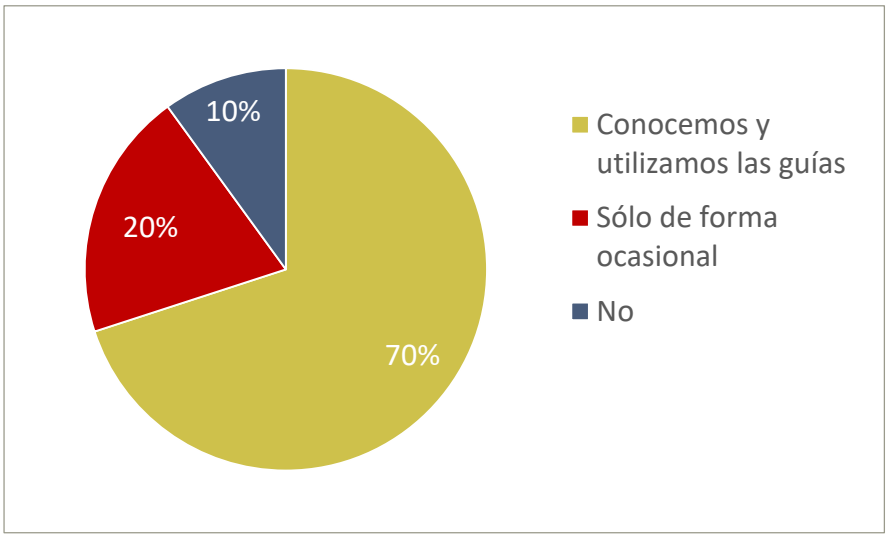


Figura 27. P13: Gráfico. Familiarización con guías de seguridad de la serie CCN-STIC

De nuevo, aunque se ha obtenido una amplia respuesta positiva a esta cuestión se considera que podría haber sido superior tratándose de entidades dedicadas a la ciberseguridad y a la ciberdefensa en el ámbito del MINISDEF. El empleo de estas guías para proteger los sistemas empleados en las propias entidades, los desarrollos realizados y los servicios prestados a sus clientes debería ser un elemento principal y obligatorio en su metodología de trabajo habitual cuando el cliente final es el MINISDEF u otro ente de la Administración Pública. Y, aunque sigue siendo válido y recomendable para el ámbito civil, no puede considerarse como un requisito obligatorio.

Además, en muchas licitaciones de la Administración Pública se exige que algunos sistemas "más sensibles" sean acreditables a la entrega y para ello es necesario que se aplique correctamente un conjunto importante de estas guías de seguridad en función de su composición. Por ello, es importante no sólo conocerlas, sino tener mucha experiencia trabajando con ellas, ya que ofrecen unos grandes beneficios de ciberseguridad, aunque su aplicación también pueda generar conflictos que se deben saber resolver.

5.9 Disposición de HSEM

Los datos recogidos en la pregunta *14. ¿Dispone su organización de HSEM?* se muestran en la siguiente figura:

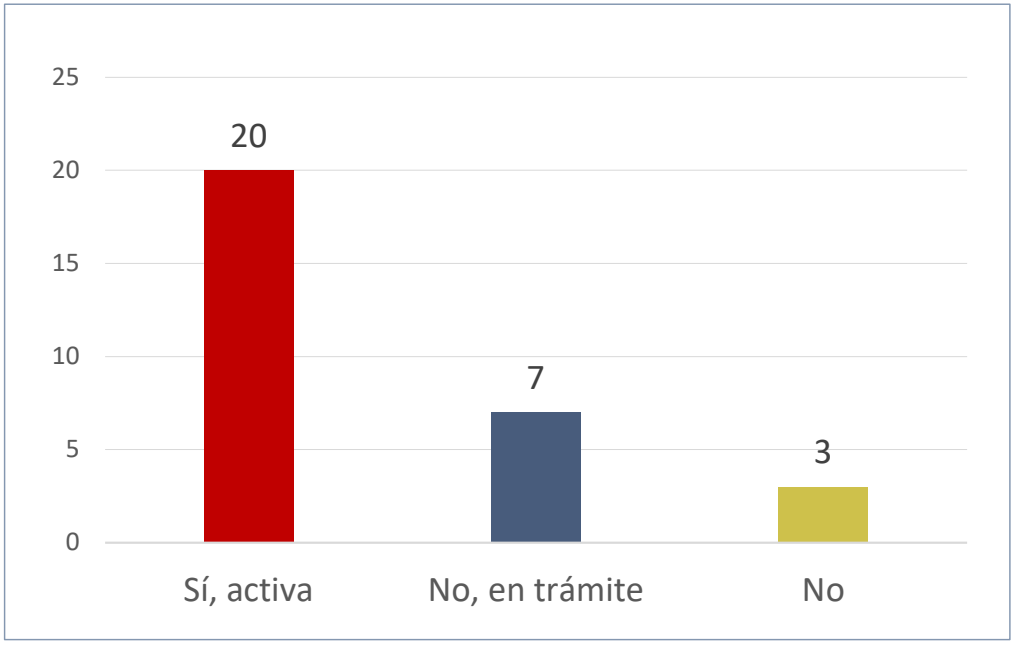


Figura 28. P14: Datos Disposición de HSEM

La representación gráfica de los datos se muestra en la siguiente figura:

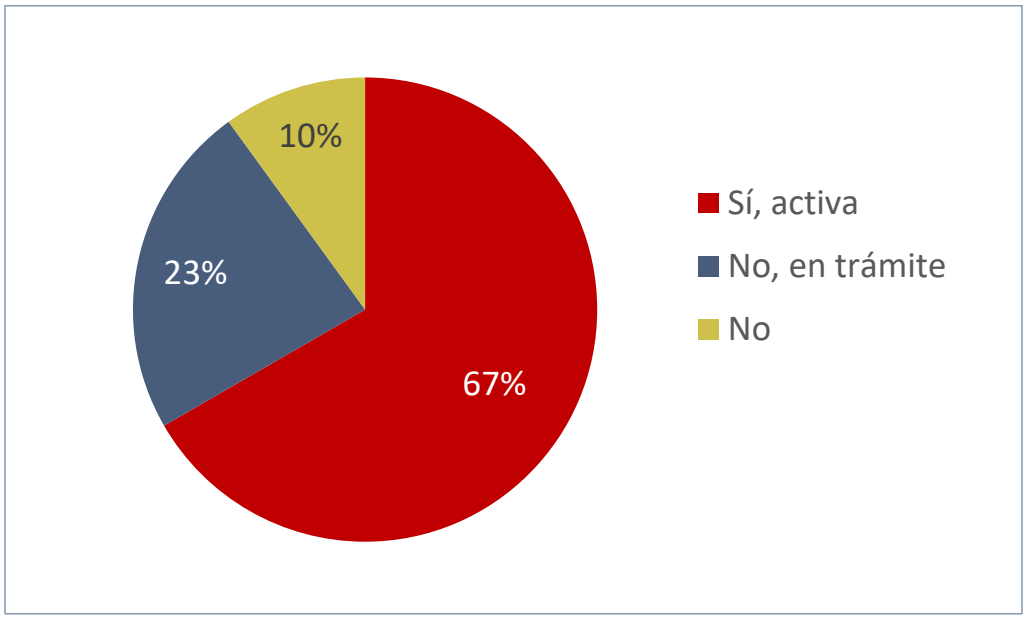


Figura 29. P14: Gráfico. Disposición de HSEM

Primero, recordar que la Habilitación de Seguridad de Empresa (HSEM) es[5] "la determinación positiva por la que la Autoridad Nacional reconoce formalmente la capacidad y fiabilidad de un contratista para generar y acceder a *Información Clasificada* hasta un determinado grado, sin que pueda manejarla o almacenarla en sus propias *instalaciones*.". Que la entidad disponga de ella implica que es apta para contratar con el sector público, cumple con las condiciones de seguridad establecidas por la Autoridad Nacional para la Protección de la Información Clasificada (ANPIC), tiene constituidos y aprobados el servicio de protección de información clasificada así como los órganos de control necesarios, y las personas responsables disponen de la HPS requerida.

Su disposición es un requisito exigido y excluyente para la participación en programas, proyectos o contratos clasificados (de nivel "confidencial" o superior) del MINISDEF o para ser seleccionada como Entidad Auditora de Seguridad en la certificación de sistemas del ámbito de aplicación del Esquema Nacional de Seguridad (ENS).

Los resultados obtenidos en esta pregunta indican que la mayoría de las entidades consultadas ha requerido acceder a información clasificada o sensible para la participación en este tipo de proyectos y que una cuarta parte está en proceso de obtener dicha

[5] Definición obtenida de la guía guía CCN-STIC-101 de Acreditación de Sistemas TIC que manejan información clasificada.

habilitación para poder hacerlo. Este dato es alto, aun tratándose de entidades muy relacionadas con el MINISDEF, a las que se presupone que antes o después han tenido relación con este tipo de proyectos y que actualmente están en condiciones de seguir participando en los mismos. Este aspecto es muy importante para el MINISDEF ya que necesita disponer de un conjunto de entidades capaces de proveerle de ciertos servicios con las garantías de seguridad necesarias.

Como se indicaba en la definición de la habilitación, sólo es obligatoria tenerla para ciertos proyectos, pero un aspecto positivo que cabe destacar es que su disposición (o tramitación) implica una mayor confianza en la aplicación de medidas de seguridad en la entidad al haber sido inspeccionada por una Entidad de Seguridad reconocida (ANPIC). De cara a una posible licitación fuera del ámbito de la defensa, su disposición reconoce que la entidad cumple con unas condiciones de seguridad mínimas, lo que le podría suponer una mejor valoración respecto a otras que no dispongan de ella.

5.10 Disposición de personal con HPS

Los datos recogidos en la pregunta *15. ¿Dispone la organización de personal con HPS?* se muestran en la siguiente figura:

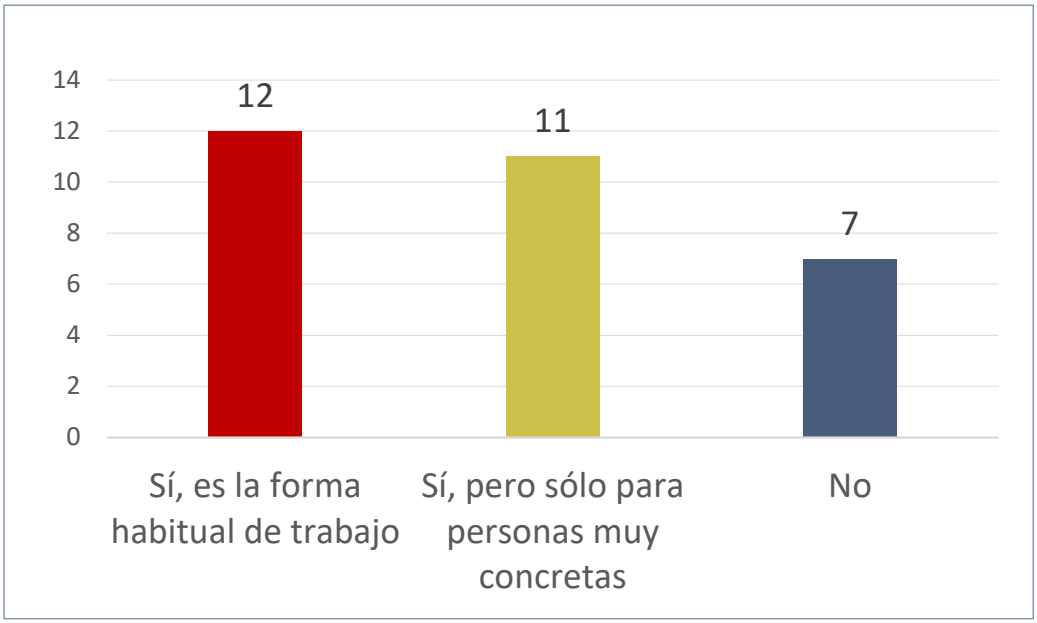


Figura 30. P15: Datos Disposición de personal HPS

La representación gráfica de los datos se muestra en la siguiente figura:

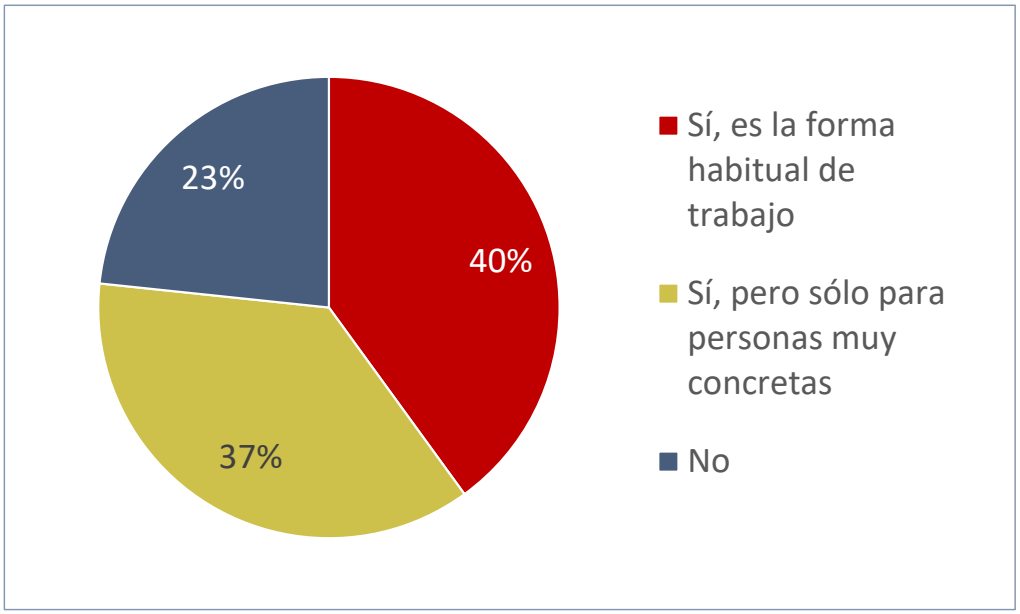


Figura 31. P15: Gráfico. Disposición de personal HPS

Como se explicó anteriormente la Habilitación Personal de Seguridad (HPS) es el documento que acredita que una persona determinada cumple los criterios necesarios para acceder a Información Clasificada. Que la persona disponga de ella implica que: se reconoce formalmente su capacidad, idoneidad y fiabilidad para tener acceso a información clasificada (en el ámbito y grado máximo autorizado), que ha superado el proceso de acreditación de seguridad y que ha sido adecuadamente concienciado en el compromiso de reserva que adquiere y en sus responsabilidades.

Su disposición es un requisito exigido y excluyente para la participación de la persona en programas, proyectos o contratos clasificados (de nivel "confidencial" o superior) del MINISDEF o en la certificación de sistemas del ámbito de aplicación del ENS. Para ello, la entidad solicitará únicamente la HPS de aquellos empleados que participen activamente en el desarrollo de una actividad o contrato clasificado que requiera acceder a información clasificada.

Los resultados obtenidos en esta pregunta indican que casi un tercio de las entidades consultadas cuenta entre su personal habitual con personas habilitadas para acceder a información clasificada que le permite participar en este tipo de proyectos. Casi otro tercio indica que sólo cierto personal dispone de esta habilitación y, finalmente, una minoría indica que no dispone de este tipo de personal, por lo que se limita su participación en estos proyectos.

Estos datos se corresponden con los de la pregunta anterior ya que es lógico pensar que la entidad que disponga de la HSEM contará con personal habilitado; pero también se puede dar el caso contrario, en el que una entidad cuente con personal habilitado aun sin tener la HSEM al no ser un requisito para que el personal pueda obtenerla. Por ejemplo, las entidades de tipo consultoría pueden contar con este tipo de personal con HPS para desplazarlo a los clientes que desarrollan estos proyectos clasificados, sin tener la HSEM, con la limitación de no poder manejar la información en la propia empresa y deber hacerlo siempre en las instalaciones del cliente.

Como aspecto positivo que cabe destacar, las entidades que disponen de este tipo de personal habilitado en su plantilla están mejor posicionadas respecto a otras al poder participar en proyectos clasificados, al ser un requisito excluyente, y gracias a la mejor valoración de su personal en el ámbito de la Ciberseguridad. Además, este aspecto vuelve a ser muy importante ya que el MINISDEF necesita disponer de personas capaces de participar en estos proyectos con las garantías de seguridad necesarias.

A pesar de que la mayoría de las entidades disponen de las habilitaciones de seguridad de empresa y las del personal para poder participar en proyectos clasificados del MINISDEF, sería recomendable que más entidades siguieran su ejemplo para asegurarse de que todas sus necesidades quedan cubiertas.

6. COMPARATIVAS SOBRE DESARROLLOS APLICABLES A CAPACIDADES OPERATIVAS

A continuación, se muestran las comparativas realizadas sobre el apartado Desarrollos aplicables a capacidades operativas del cuestionario. Dentro de cada subapartado se recoge la pregunta realizada, las respuestas obtenidas y las primeras conclusiones alcanzadas.

Hay que aclarar que algunas entidades han declarado que varias opciones (respuestas múltiples) son de aplicación en algunas cuestiones, por lo que estas no son excluyentes entre sí y se han tenido en cuenta todas. Por esta razón, en algunas gráficas se puede encontrar que la suma de los porcentajes de las opciones es superior al 100% al estar referido al número de entidades.

Indicar que en los gráficos de datos se muestra una línea roja para separar visualmente las respuestas positivas (izquierda) de las negativas (derecha).

6.1. Capacidad de coordinación y control en operaciones en el ciberespacio

Esta capacidad permite el ejercicio de la autoridad en los niveles estratégico, operacional y táctico, y la conducción y seguimiento por el mando operativo sobre las fuerzas asignadas para el cumplimiento de la misión, así como a la observación de la actividad del adversario, propiciando un conocimiento fiable de la situación que permita la oportuna toma de decisiones.

Esta capacidad se desglosa en **tres subcapacidades** que se detallan a continuación:

Control de conducción y ejecución de ciberoperaciones

Esta subcapacidad facilita la conducción y el seguimiento de las fuerzas. Su objetivo es proporcionar información de la ejecución para valorar la situación, tomar decisiones y dirigir las acciones.

Los datos recogidos en la pregunta *16. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?* correspondientes a la subcapacidad de **Control de conducción y ejecución de ciberoperaciones**, se muestran en la siguiente figura:

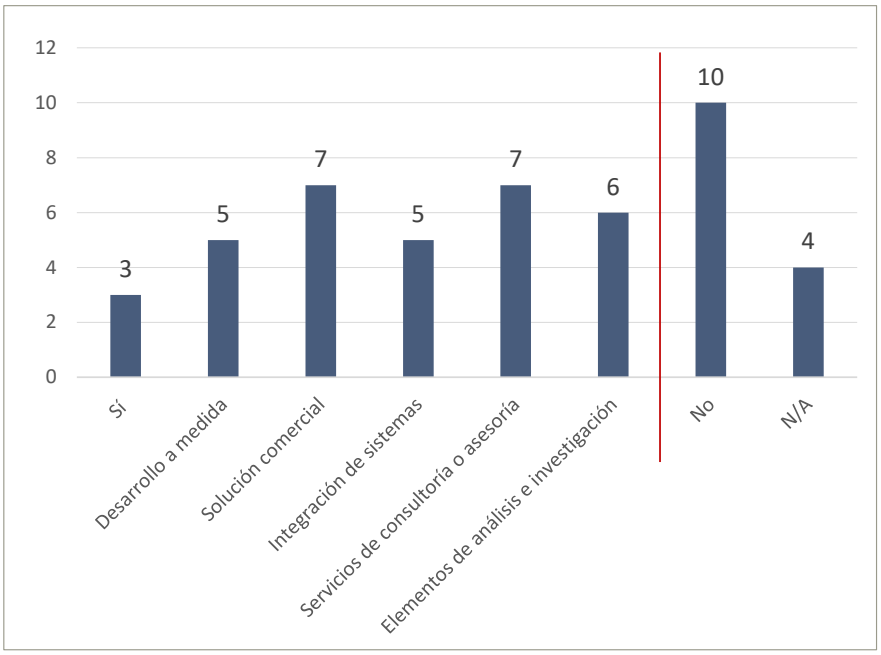


Figura 32. P16: Datos Control de la conducción y ejecución de ciberoperaciones

La representación gráfica de los datos positivos se muestra en la siguiente figura:

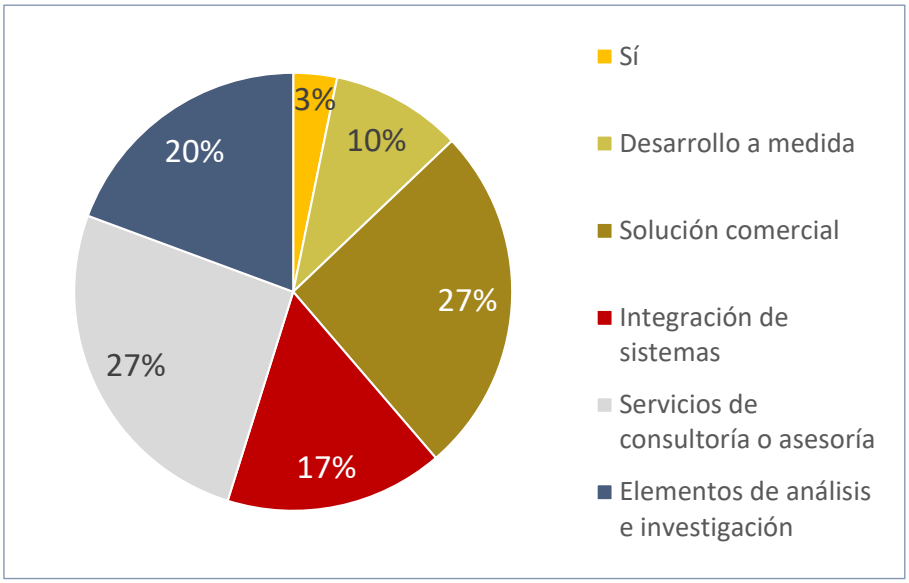


Figura 33. P16: Gráfico. Control de la conducción y ejecución de ciberoperaciones

Casi la mitad de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con el control de la conducción y ejecución de ciberoperaciones.

De las entidades que sí lo hacen, la cuarta parte indica que dispone de una solución comercial de este tipo o que realiza servicios de consultoría o asesoría relacionados con

esta subcapacidad. Una quinta parte indica que se están realizando trabajos de análisis e investigación o de integración de sistemas de este tipo de capacidades.

Entre la información adicional aportada en los comentarios de esta pregunta, destaca que algunas entidades están realizando desarrollos de capacidades a medida de apoyo a la decisión en el ciberespacio y para la conducción de operaciones de Ciberdefensa para el MINISDEF. Otras tienen sistemas propios para la explotación y respuesta de la ciberdefensa implantados en distintos clientes, y que otras están trabajando en desarrollos de sistemas de Mando y Control para el MINISDEF y agencias internacionales con proyectos con la OTAN y la EDA, destacando las funciones de planificación, conducción y seguimiento.

Consciencia situacional en ciberdefensa

Esta subcapacidad proporciona proporciona un conocimiento de la situación en el Ciberespacio, basado en el análisis de la información obtenida de diversas fuentes, a partir del cual se puede observar, comprender y evaluar el riesgo de acciones adversarias, de forma que permita desarrollar las acciones oportunas para contrarrestarlas. Comprende el conocimiento de los activos en las redes y sistemas propios, amenazas y análisis-gestión dinámicos de riesgos y evaluación del impacto en la misión, gestión del CIBER-ORBAT (orden de batalla en el Ciberespacio y conocimiento de las redes del adversario) y presentación visual de la información.

Los datos recogidos en la pregunta *17.¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Consciencia situacional en ciberdefensa**, se muestran en la siguiente figura:

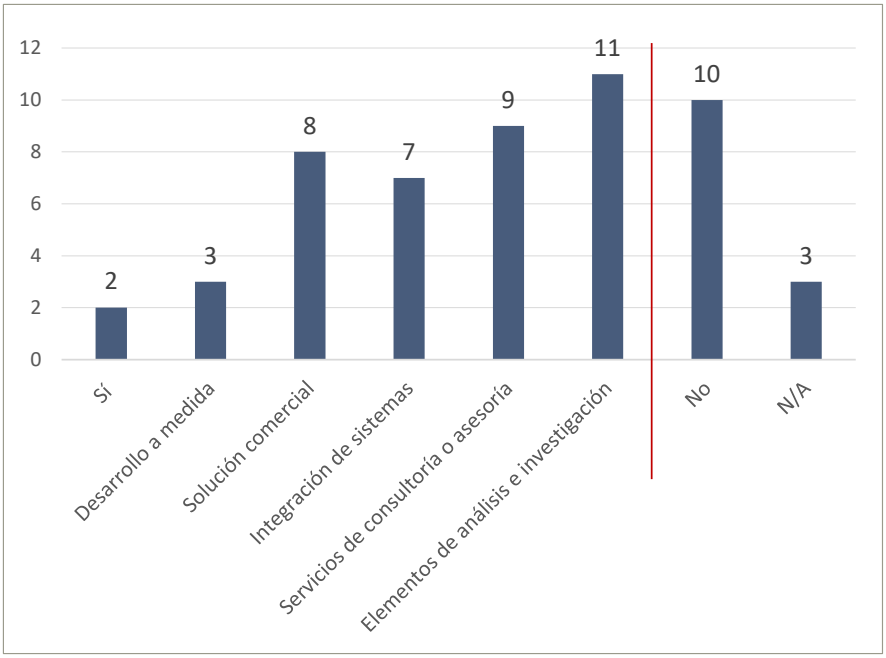


Figura 34- P17: Datos Consciencia situacional en ciberdefensa

La representación gráfica de los datos positivos se muestra en la siguiente figura:

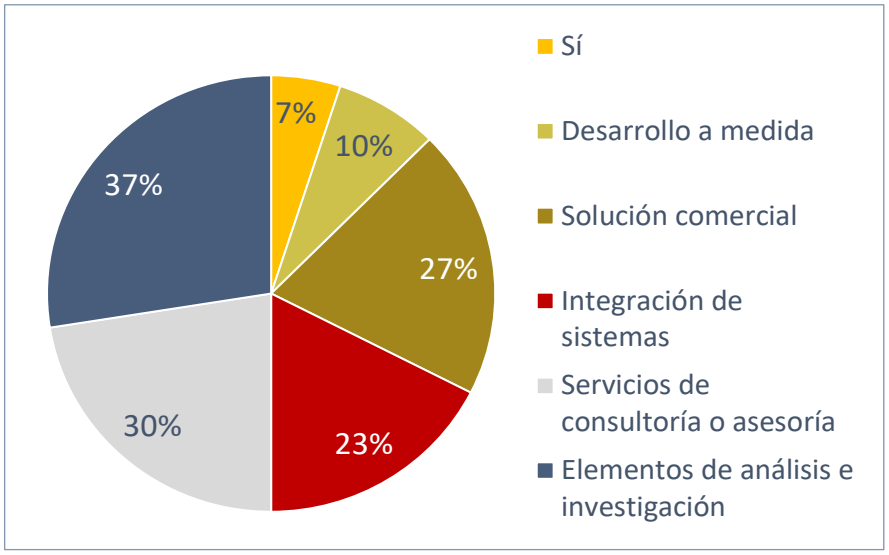


Figura 35- P17: Gráfico. Consciencia situacional ciber en ciberdefensa

Casi la mitad de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la consciencia situacional en ciberdefensa.

De las entidades que ofrecen estos servicios, destaca que más de un tercio indica que realiza trabajos de análisis e investigación sobre este tipo de capacidades y casi otro tercio indica que realiza servicios de consultoría o asesoría relacionados por lo que resulta un área de gran interés para ellas. Una cuarta parte indica que dispone de una solución comercial de este tipo de capacidades y declara que está capacitada para la integración de estos sistemas. Finalmente, una minoría indica realizar desarrollos a medida de sistemas relacionados con este tipo de capacidad.

En la información adicional aportada por las entidades en los comentarios de esta pregunta se indica que algunas de ellas lideran grandes proyectos europeos para el desarrollo de una plataforma de adquisición en tiempo real de ciberconsciencia situacional en operaciones militares (ECYSAP – Plataforma Europea para la Ciberconsciencia Situacional en Ciberdefensa), en ella se implementarán capacidades de visualización, detección y respuesta a ciberamenazas y ofrecerá soporte a la toma de decisiones. Así como la plataforma de conciencia situacional de fuentes heterogéneas para escenarios de guerra híbrida CLAUDIA (*Cloud Intelligence for Decision Making Support and Analysis*) de la EDA que cuenta con módulos vanzados de visualización y análisis. Otras entidades indican que disponen de desarrollos propios con consolas de mando y control que dan comprensión a la situación operacional, en relación con las capacidades de explotación y respuesta, siendo integrables con otras fuentes de información. Otras, que no desarrollan productos propios, recurren a servicios prestados por terceros para estas tareas.

Centro de operaciones del ciberespacio

Es elemento que alberga los sistemas que permiten desarrollar la función de coordinación y control de las operaciones militares en el Ciberespacio.

Los datos recogidos en la pregunta *18. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Centro de operaciones del ciberespacio**, se muestran en la siguiente figura:

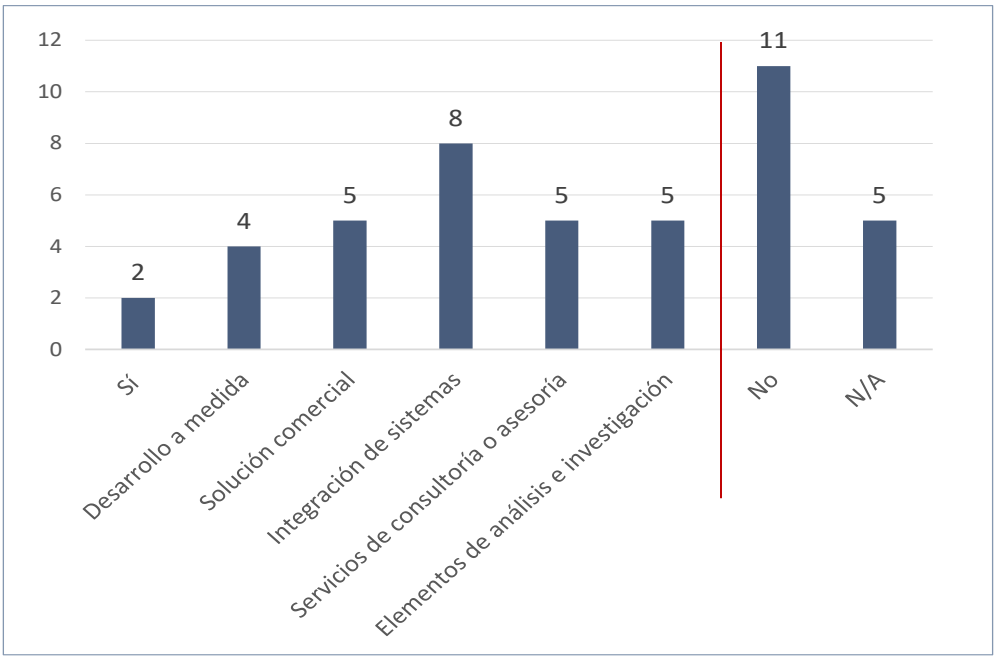


Figura 36. P18: Datos Centro de operaciones del ciberespacio

La representación gráfica de los datos positivos se muestra en la siguiente figura:

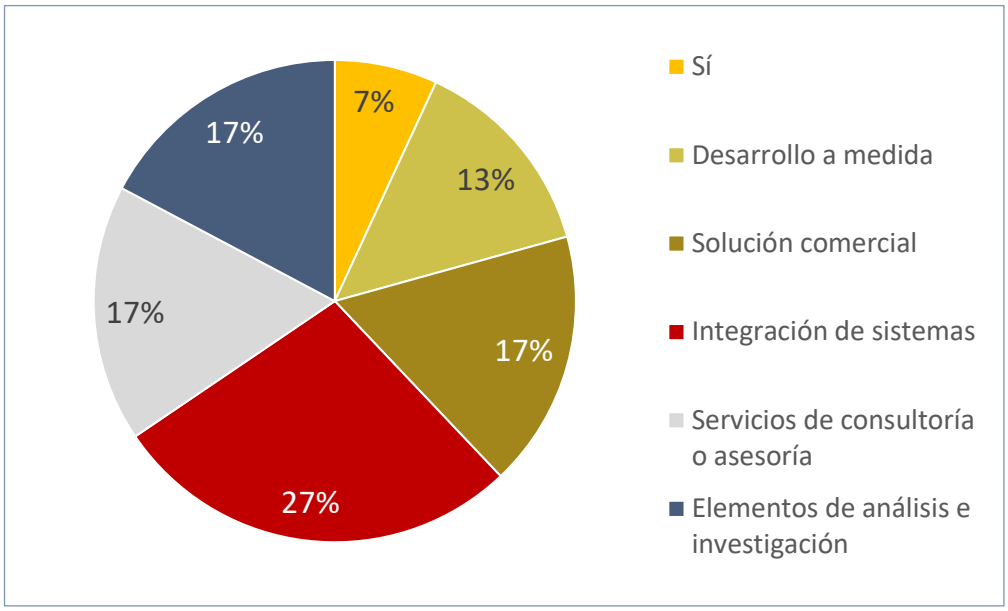


Figura 37. P18: Gráfico. Centro de operaciones del ciberespacio

La mitad de las entidades ha contestado que realiza desarrollos o trabajos relacionados con la subcapacidad de Centro de operaciones del ciberespacio, pero analizando la información adicional aportada en sus respuestas, se hace imprescindible aclarar el concepto sobre el que se refiere la pregunta. La mayoría de ellas ha identificado un centro de operaciones del ciberespacio con un Centro de Operaciones de Seguridad (SOC), cuando no tienen mucho que ver y sobre el que se pregunta más adelante. El SOC se dedica, entre otros, a la monitorización continua y análisis proactivo de amenazas, gestión de incidentes de seguridad o investigación y análisis forense, lo que mejora la capacidad de respuesta ante ataques. Por su parte, el centro de operaciones del ciberespacio es el lugar desde donde se planean y conducen las operaciones militares en el Ciberespacio. Del tercio de las entidades que ha contestado positivamente a la pregunta y que no han detallado más sobre esta capacidad, no se puede decir si realmente desarrollan o no lo que se entiende por Centro de Operaciones del Ciberespacio.

El ejemplo más claro de este tipo de elemento es el Centro de Operaciones del Ciberespacio de la OTAN (*CyOC: Cyberspace Operations Centre)*) en Mons (Bélgica). Es un centro de operaciones que apoya a la estructura de la Alianza en el ámbito del ciberespacio a nivel operacional, coordinando los esfuerzos de los centros de operaciones de los países aliados. Su función principal es apoyar a los mandos militares, proporcionando el conocimiento de la situación del ciberespacio, permitiendo la preparación, planificación, conducción y coordinación o ejecución de operaciones de la OTAN y garantizando la libertad de acción en el Ciberespacio de modo que sean más resilientes a las ciberamenazas.

Además, este CyOC tiene la misión de optimizar el empleo de los efectos en el ciberespacio o a través de él. Proporcionar conocimientos especializados sobre el Ciberespacio y proveer un asesoramiento oportuno y eficaz sobre la planificación y realización de las operaciones en el Ciberespacio.

A la vista de las respuestas afirmativas, una de una de las entidades ha entendido el concepto global de la pregunta y ha indicado que realiza trabajos relacionados. En este caso dentro de la iniciativa PESCO donde se están cerrando acuerdos para aportar personal y capacidades de Ciberdefensa al *Cyber and Information Domain Coordination Centre* (CIDCC). El objetivo de este proyecto es desarrollar, establecer y operar un Centro de Coordinación del Dominio Cibernético y de la Información como elemento militar multinacional permanente. En él los estados miembros participantes contribuyen continuamente con personal, medios o información para luchar contra las ciberamenazas y ciberincidentes, y apoyar en las operaciones en el ciberespacio.

En el caso del resto de entidades, algunas trabajan en la creación de Centro de Operaciones de Seguridad para distintos entes públicos como Administración General del Estado (AGE). Otras ya disponen de un SOC propio (integrado en la red NCIA-OTAN) para prestar servicios horizontales de ciberseguridad, como vigilancia y detección de amenazas o respuesta ante ataques Por último, otras entidades simplemente emplean los SOC de terceros.

Finalmente, hay que comentar que una de las entidades indica estar desarrollando una herramienta a medida para la conducción de operaciones de ciberdefensa. Esta herramienta dispone de varios módulos para la coordinación y control de las operaciones y

de varios cuadros de mando. Por su finalidad, es probable que esta herramienta termine integrada en un centro de operaciones del ciberespacio.

Si bien la mayor parte de las soluciones existentes están orientadas a las necesidades de los centros de operaciones de seguridad, estas herramientas suponen una base importante para el desarrollo de soluciones que cubran las necesidades y características más avanzadas y específicas requeridas para la coordinación y control de las Operaciones en el Ciberespacio. La solvencia técnica y experiencia de las entidades españolas en el desarrollo de este tipo de herramientas para el resto de los ámbitos de las operaciones (tierra, mar, aire y espacio) hace que este sea también un buen punto de partida.

6.2. Capacidad de defensa

Esta capacidad permite detectar, entorpecer o anular las acciones ofensivas de un adversario contra los sistemas propios para preservar la libertad de acción. Permite ejecutar medidas defensivas para contrarrestar ciberataques y mitigar sus efectos y, así, preservar y restaurar la seguridad de los sistemas de comunicación, de información u otros sistemas electrónicos. Responde en tiempo real u oportuno frente a una amenaza concreta con la finalidad de mitigar riesgos detectados y defenderse contra adversarios que están ejecutando, o a punto de hacerlo, acciones ofensivas.

Esta capacidad se desglosa en **nueve subcapacidades** que se detallan a continuación:

Defensa activa

Este tipo de defensa empleamedidas y acciones dirigidas a neutralizar todo tipo de ataques del adversario por medio de acciones de respuesta en el Ciberespacio del adversario para evitar que consiga sus propósitos. Permite aprender de los ataques del adversario para prepararse ante nuevos ataques en el futuro. Dentro de este tipo de subcapacidades podemos encontrar: **recolección** (*collection*) de información de las herramientas y tácticas del adversario, **detección** (*detection*) de los artefactos y sistemas de engaño del adversario, **detención** (*prevention*) total o parcialmente la capacidad del adversario, **disuasión** (*direction*) al adversario de llevar a cabo su operación, **reducción** (*disruption*) de la capacidad de un adversario para llevar a cabo su operación, añadir **autenticidad** (*reassurance*) a los artefactos de engaño para convencer a un adversario de que el entorno es real o **motivación** (*motivation*) al adversario para llevar a cabo una parte o la totalidad de su misión. Consultar *MITRE ENGAGE*[6] para más información."

[6] https://engage.mitre.org/matrix/

Los datos recogidos en la pregunta *19. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Defensa activa**, se muestran en la siguiente figura:

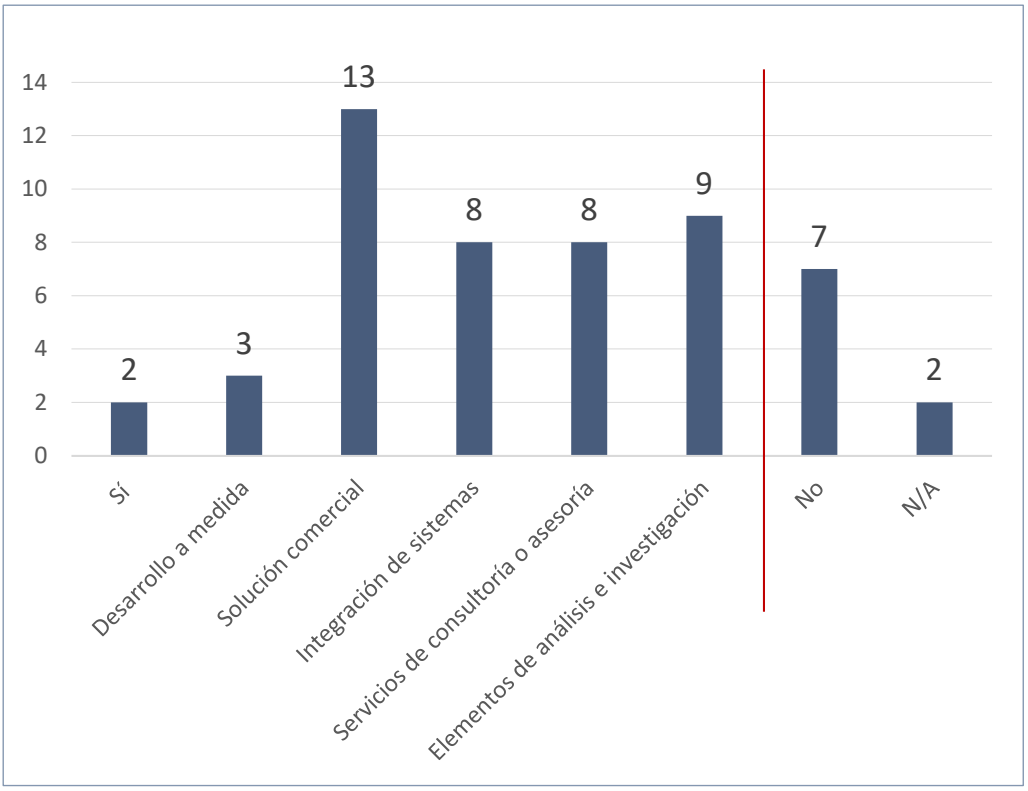


Figura 38. P19: Datos Defensa activa

La representación gráfica de los datos positivos se muestra en la siguiente figura:

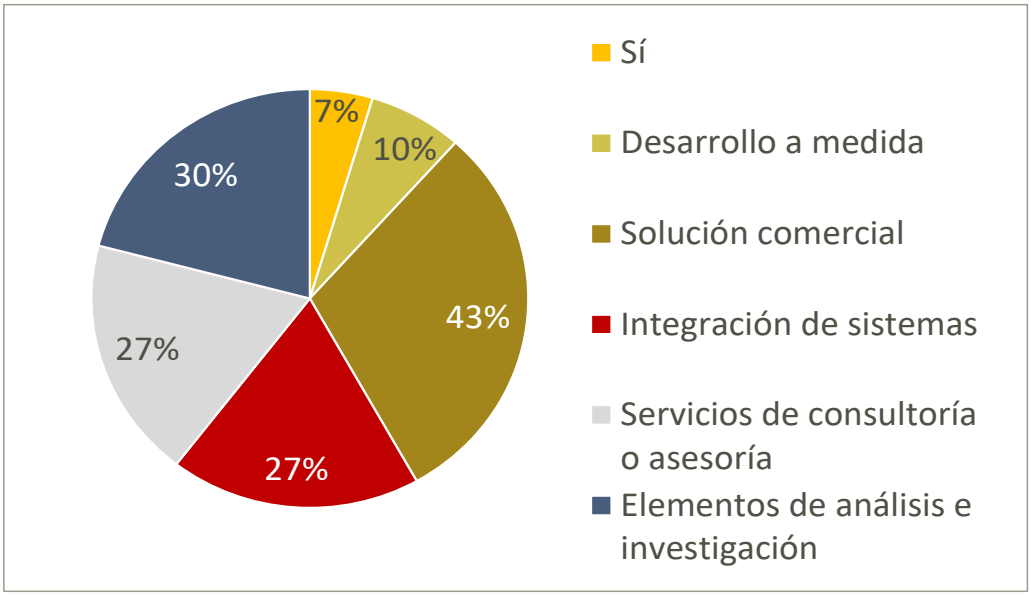


Figura 39. P19: Gráfico. Defensa activa

Casi un tercio de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la defensa activa. Del resto de entidades que sí lo hacen, destaca que casi la mitad indica que dispone de una solución comercial. Un tercio de las entidades realiza trabajos de análisis e investigación en este tipo de capacidades y otra cuarta parte realiza servicios de consultoría o asesoría e Integración de sistemas relacionados. Finalmente, una minoría indica que realiza desarrollos a medida de esos sistemas.

Tras analizar la información adicional aportada por las entidades en los comentarios de esta pregunta, encontramos que no todas las entidades han entendido correctamente la capacidad sobre la que se trata. Algunas entidades han identificado este tipo de sistemas con los de defensa pasiva clásica, sin que sean equivalentes. Entre las entidades que han diferenciado correctamente estos dos tipos de capacidad, la mayoría integra soluciones comerciales y son las menos las que desarrollan productos propios relacionados.

Algunas entidades declaran estar realizando desarrollos de soluciones orientadas a la defensa activa desde la perspectiva MILDEC (*Military Deception*), centradas en la disuasión (*direction*) o la interrupción (*disruption*) de las acciones enemigas. Otras trabajan en desarrollos propios orientados al aspecto de recolección de información del adversario, identificando y analizando los patrones, las tácticas, técnicas y procedimientos (TTP) o los vectores de ataque utilizados. También existen desarrollos sobre el aspecto de engaño (*deception*) o autenticidad (*reassurance*), con el diseño de señuelos para la detección de ataques o recolección de información en una etapa temprana. Por último, otras entidades declaran disponer de soluciones para realizar la disrupción controlada y dirigida de la comunicación de un dispositivo wifi dentro una red (*jammering* selectivo) o enmarcadas en la Ciberseguridad centrada en los datos para proteger el acceso a la información y prevenir su exfiltración.

Sobre las entidades que no desarrollan soluciones propias e implantan herramientas comerciales[7], entre las más empleadas están las relacionadas con el aspecto de recolección (*collection*) dedicadas a la monitorización de red e infraestructuras y la recolección y correlación de eventos. Para los aspectos de detección (*detection*), las relacionadas con la detección y gestión de vulnerabilidades; para los aspectos de detención (*prevention*), las relacionadas con la capacidad de aislamiento (*isolation*) o para reducción (*disruption*) que proporcionan seguridad perimetral lógica y web. Por último, sobre el aspecto sobre el aspecto de disuasión (*direction*), las dedicadas a la protección de correo y la gestión de dispositivos.

Como curiosidad, al menos una entidad indica que no tiene soluciones de este tipo habitualmente implantadas y que sólo las emplea en respuesta ante incidentes para realizar el análisis de la situación y proporcionar las medidas necesarias para la toma de control, expulsión de adversario y limitación de impacto.

Finalmente, otras entidades que no desarrollan productos propios ni implantan estas herramientas se apoyan en servicios prestados por terceros para estas tareas.

[7] Sin resultar un listado exhaustivo y a título de ejemplo, se reseñan algunas de estas herramientas comerciales indicadas en las respuestas: NAGIOS, Fortinet, Splunk, Tenable.IO, Crowdstrike, Cisco Umbrella, Netskope, Imperva, Proofpoint TAP, Intune/SCCM & Airwatch.

Defensa pasiva

Este tipo de defensa, desplegada en las redes propias, protege contra amenazas provenientes del Ciberespacio mediante la vigilancia permanente y detección, interceptación, identificación y neutralización de ciberataques inminentes o en curso y la aplicación de medidas de seguridad para la protección de los sistemas de comunicación, de información y otros sistemas electrónicos en la infraestructura propia.

Los datos recogidos en la pregunta *20. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Defensa pasiva**, se muestran en la siguiente figura:

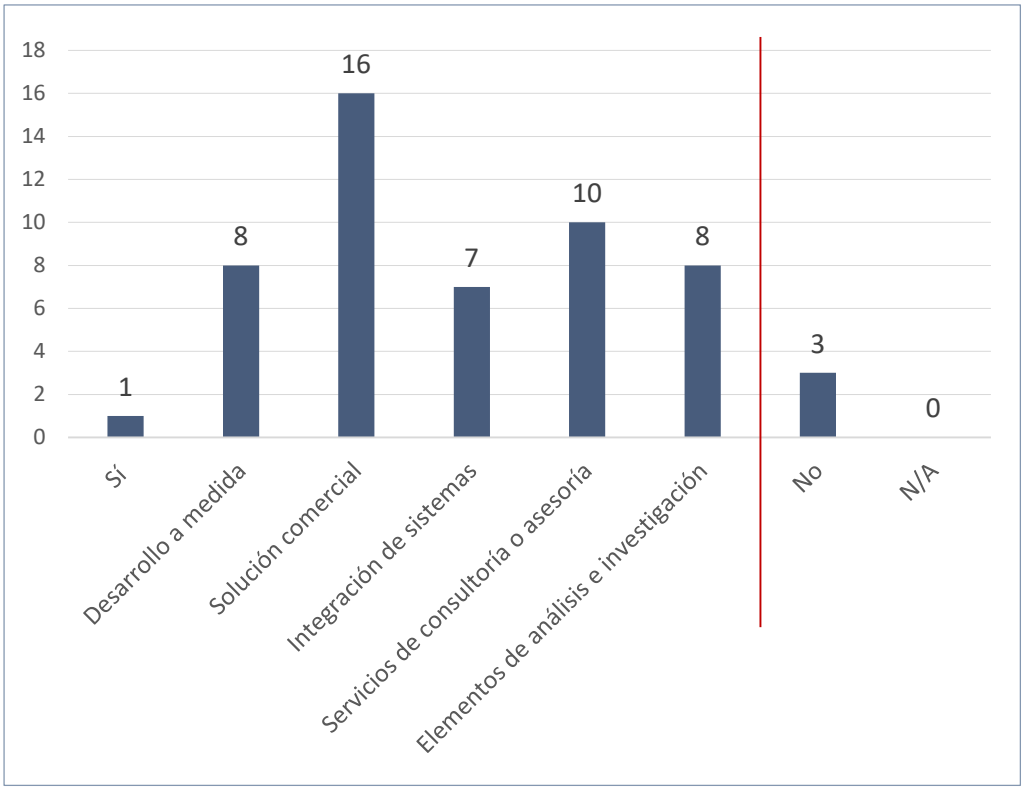


Figura 40. P20: Datos Defensa pasiva

La representación gráfica de los datos positivos se muestra en la siguiente figura:

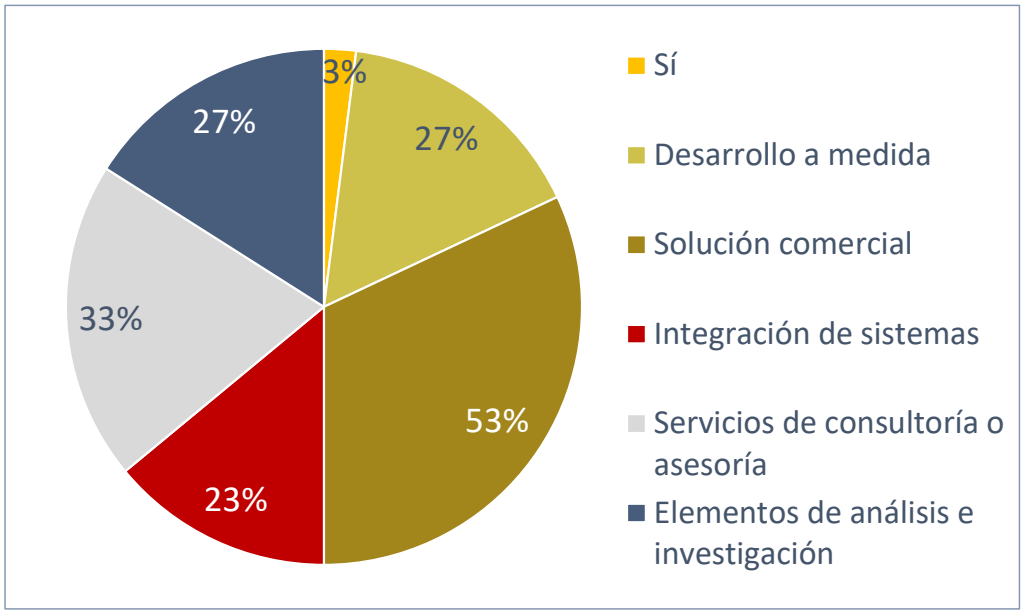


Figura 41. P20: Gráfico. Defensa pasiva

Una minoría de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la defensa pasiva. Del resto de entidades que sí lo hacen, la mayoría indica que disponen de una solución comercial y un tercio realiza servicios de consultoría o asesoría relacionados. Una cuarta parte de las entidades realiza desarrollos a medida, trabajos de análisis e investigación o integración de sistemas relacionados.

Algunas entidades indican que que disponen bien de soluciones y capacidades propias[8] para centros de operaciones de seguridad (SOC) militares, bien de herramientas basadas en IA para detectar incidentes en entornos de la Industria IoT o bien de una *suite* de productos para Segmentos Terrenos de Misiones Espaciales para el control de autenticación, autorización y registro de acceso y credenciales de usuario en la red y en la nube. Destaca la participación de entidades en VACCINE, proyecto de la Comisión Europea para la detección de ciberanomalías en tiempo real, con el uso de inteligencia artificial en plataformas aeronáuticas usando inteligencia artificial. También destaca la participación en una plataforma del Programa Europeo de Desarrollo Industrial de la Defensa (EDIDP) de Ciberdefensa para la búsqueda de amenazas en tiempo real, respuesta a incidentes y el intercambio de información (PANDORA) para plataformas tipo corbeta o fragata. Otras de las soluciones propias nombradas realizan detección y cancelación de interferencias en comunicaciones inalámbricas por satélite o protección de ataques a través de dispositivos de almacenamiento USB.

[8] Sin resultar un listado exhaustivo, las respuestas han nombrado ejemplos de estas herramientas propias como CYBERDEEP, GS4EO o SAFEDOOR.

Muchas entidades ofrecen servicios de monitorización de diversas fuentes o de disponibilidad de servicios e infraestructura de seguridad para la detección de actividad maliciosa y respuesta a incidentes de seguridad para identificar información que permita detectar la fuga de información, suplantación de identidad, ataques organizados, actividades fraudulentas, espionaje industrial, APT (*Advanced Persistent Threat*), *phishing*, *pharming*, *spam*, información obtenida a través de ataques contra la organización, credenciales de usuarios en los diferentes servicios de la organización, etc.

Otras entidades indican participar en desarrollos para la Agencia Europea de Defensa (EDA) y para la Agencia Europea de la Guardia de Fronteras y Costas (FRONTEX), integrando en sus redes y sistemas herramientas comerciales y procesos para la monitorización y prevención de incidentes.

Algunas entidades indican que no desarrollan soluciones propias e implantan herramientas comerciales[9] gestionadas desde sus propios SOC o desde las redes de los clientes. Además, muchas entidades ofrecen, entre otros, servicios de gestión de amenazas, de inteligencia, de detección y respuesta a través de su red de centros de ciberdefensa o servicios de *threat hunting*, integrados en las redes de los clientes para analizar la telemetría y detectar y bloquear ataques.

[9] Algunos ejemplos de herramientas nombradas son Windows Defender, Azure Sentinel o Advanced Threats Analytics.

Seguridad perimetral

Esta capacidad proporciona distintos tipos de información (accesos no autorizados, ataques, anomalías, comportamientos sospechosos, eventos, alertas...) sobre las amenazas para los sistemas propios.

Los datos recogidos en la pregunta *21. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Seguridad perimetral**, se muestran en la siguiente figura:

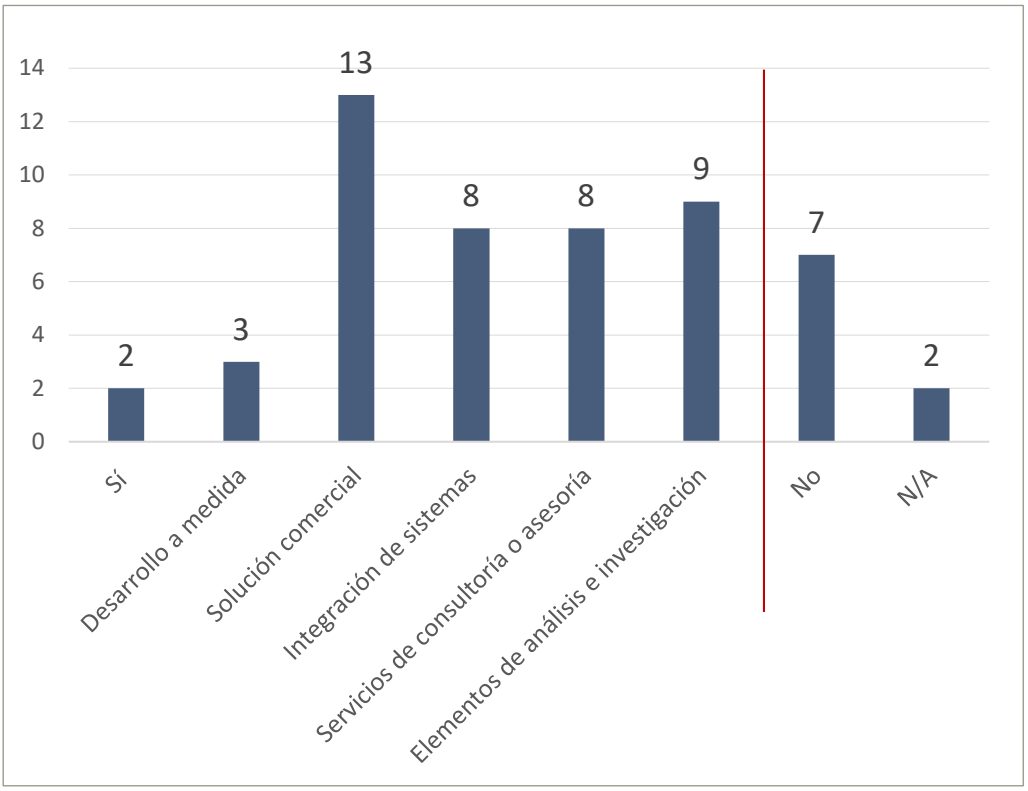


Figura 42. P21: Datos Seguridad perimetral

La representación gráfica de los datos positivos se muestra en la siguiente figura:

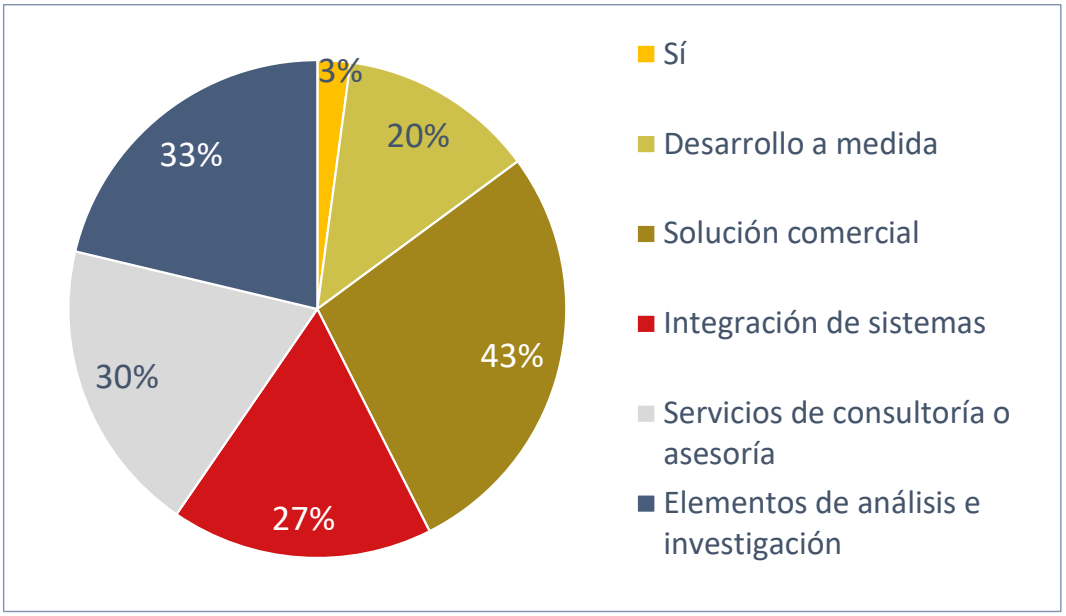


Figura 43. P21: Gráfico. Seguridad perimetral

Un tercio de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la Seguridad perimetral. Del resto de entidades destaca que casi la mitad indica que dispone de una solución comercial. Un tercio indica que realiza trabajos de análisis e investigación y servicios de consultoría o asesoría. Las siguientes actividades más declaradas por las entidades son la Integración de sistemas y los desarrollos a medida de estos sistemas.

Algunas entidades indican que disponen de tecnologías y capacidades propias de detección y respuesta gestionadas (*MDR: Managed Detection and Response*) como *endpoint* MDR, *managed* SIEM, *threat intelligence*, *fraud operation* con las que ofrecen servicios de CSIRT, *red team services*, *vulnerability management*, DEVSecOps, CIS *technical controls*, etc.

Algunas entidades han desarrollado productos para monitorización de la infraestructura y los sistemas desplegados (monitor4EO) que detecta anomalías, eventos y alertas en el comportamiento de los elementos, empleados también en despliegues en la nube, que se espera evolucionar para mejorar su capacidad de detección de accesos no autorizados y ataques externos. Por ultimo, hay entidades que han desplegado sistemas acreditados para aplicaciones de defensa y OTAN (Programa ESPRESS, Programa SIGLO/SANTIAGO, proyecto PST-BGX para OTAN) o la red EUROSUR (FRONTEX) donde se han diseñado y puesto en marcha las soluciones de seguridad perimetral.

Sobre las entidades que no desarrollan soluciones propias, la mayoría indica que cuentan con la capacidad de integrar o adaptar soluciones comerciales[10] a medida de los clientes. A través de los *datacenter* o los CERT corporativos desplegados en diferentes sedes críticas, prestan un conjunto de servicios gestionados con las actividades básicas proporcionadas por un equipo de respuesta de incidentes de seguridad, entre ellos operación de infraestructuras de seguridad (cortafuegos, WAF, IDS/IPS, UEBA, EDR, etc.) o el soporte y mantenimiento de las infraestructuras de seguridad.

Monitorización y detección de amenazas

Esta subcapacidad analiza la actividad en las redes, servidores, puntos finales, bases de datos, aplicaciones, sitios web y otros sistemas, buscando actividades anómalas que puedan ser indicativas de un incidente o compromiso de seguridad.

Los datos recogidos en la pregunta *22. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Monitorización y detección de amenazas**, se muestran en la siguiente figura:

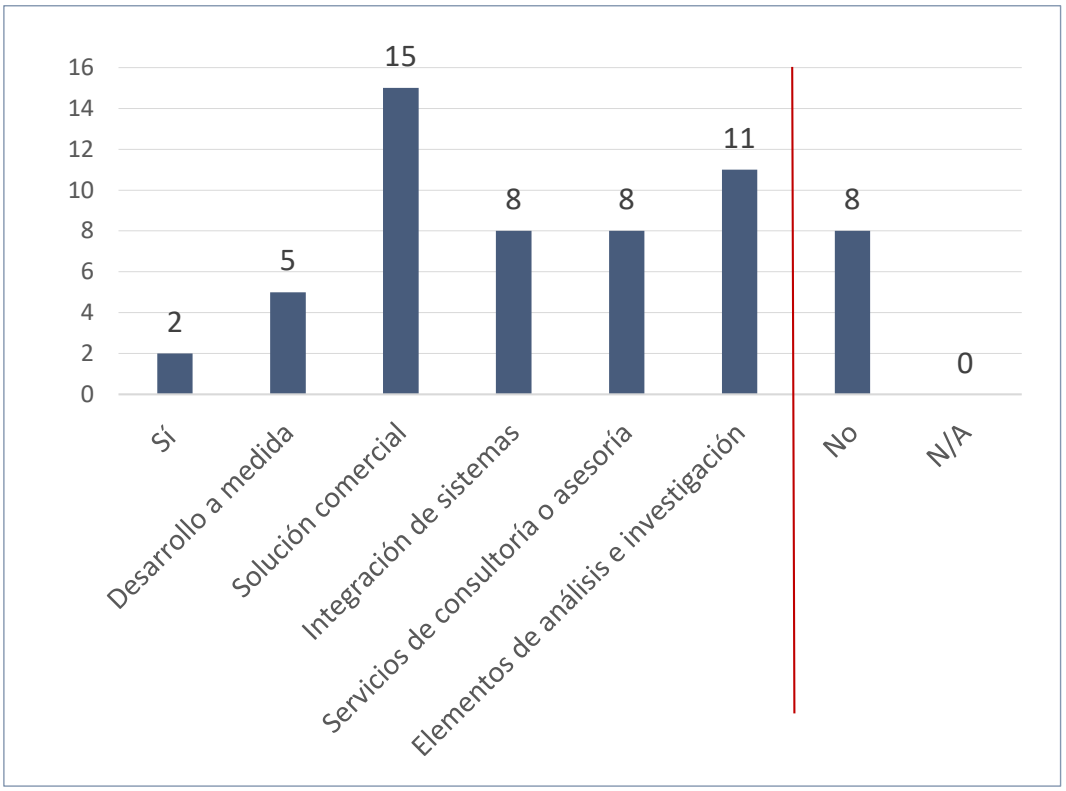


Figura 44. P22: Datos Monitorización y detección de amenazas

[10] Algunos ejemplos de herramientas nombradas son los firewalls Fortigate, Citrix ADC, 2FA Office 365 o Office 365 Alerts.

La representación gráfica de los datos positivos se muestra en la siguiente figura:

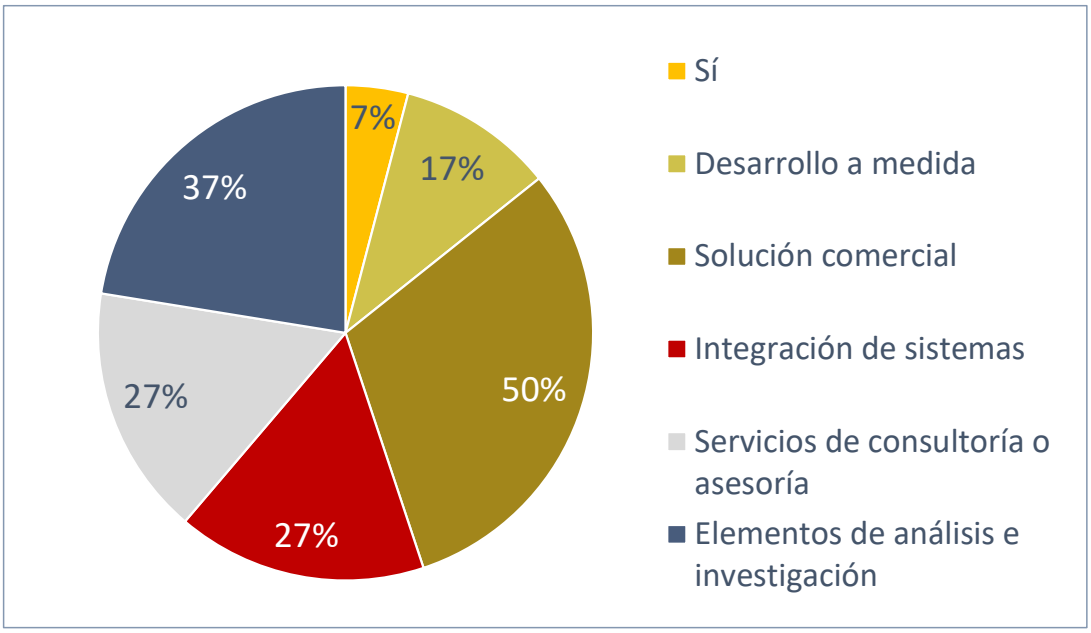


Figura 45. P22: Gráfico. Monitorización y detección de amenazas

Una cuarta parte de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la monitorización y detección de amenazas. De las entidades que ofrecen estos servicios, destaca que la mitad indica que dispone de una solución comercial y que un tercio realiza trabajos de análisis e investigación en este tipo de capacidades. Un cuarto de las entidades se dedican a los **servicios de consultoría o asesoría** o a la **integración de sistemas** relacionados. Finalmente, una minoría indica que realiza desarrollos a medida de estos sistemas.

De nuevo, relacionado con esta capacidad, algunas entidades declaran utilizar soluciones propias basadas en la inteligencia artificial para detectar incidentes en entornos de la industria IoT. Bien trabajos que realizan en proyectos internacionales para la detección de ciberanomalías en tiempo real (VACCINE) en una plataforma aeronáutica. O bien para la recopilación e intercambio en tiempo real de datos con el fin de detección de ciberanomalías (EDIDP PANDORA) en una plataforma naval.

Varias entidades declaran disponer de SOC o CERT corporativo y su pertenencia a Equipos de Ciberseguridad y Gestión de Incidentes Españoles (CSIRT), desde los que ofrecen este tipo de servicios de monitorización y detección de amenazas.

Otras entidades ofrecen servicios de información de Inteligencia de seguridad o detección y respuesta a las amenazas contra la imagen y el negocio de la Empresa en internet o el análisis del comportamiento de los usuarios en el uso de información confidencial. Otros servicios prestados son *threat hunting* y análisis de compromiso, operando la telemetría generada en los *endpoint* (EDR/XDR) para la identificación de nuevas amenazas, protección de *firmware* y detección de *malware*, basado en soluciones propias de inmutabilidad de objetos digitales con tecnologías similares a *blockchain*.

Recolección de información

Esta subcapacidad recopila información de diferentes sensores y elementos para su posterior tratamiento. Ejemplos de ellos son los sensores de presencia física, wifi, *bluetooth*, telefonía móvil, GPS o de radiofrecuencia.

Los datos recogidos en la pregunta *23. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Recolección de información**, se muestran en la siguiente figura:

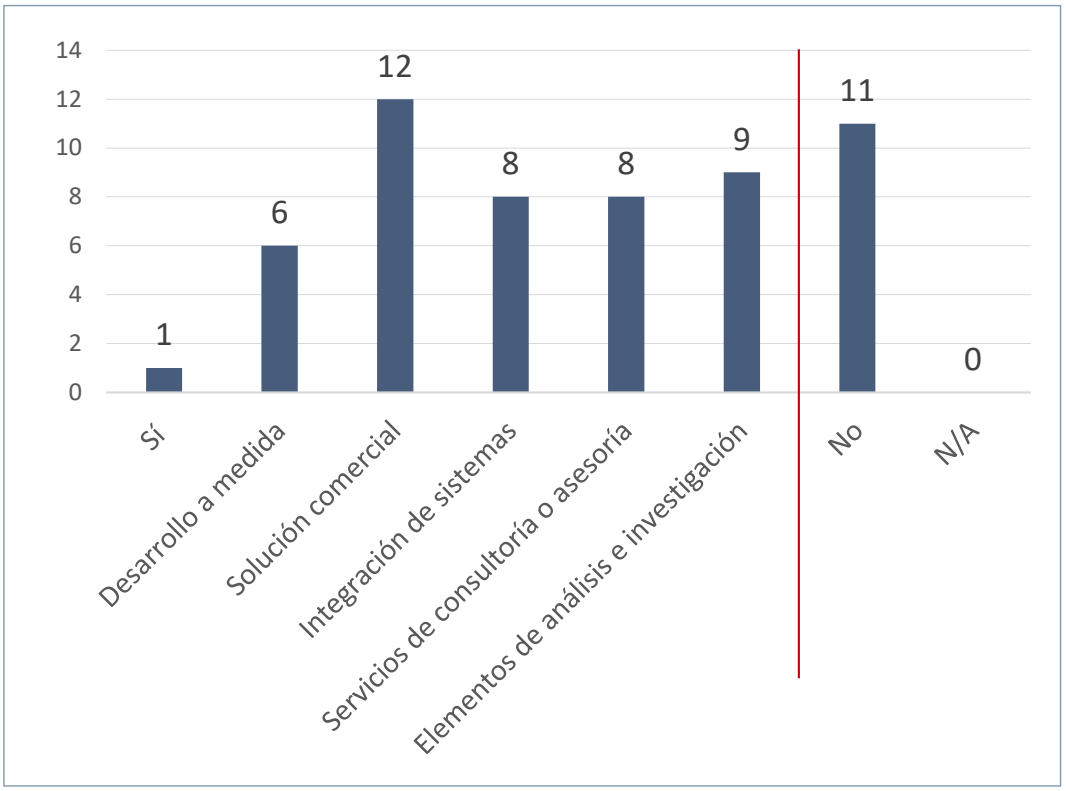


Figura 46. P23: Datos Recolección de información

La representación gráfica de los datos positivos se muestra en la siguiente figura:

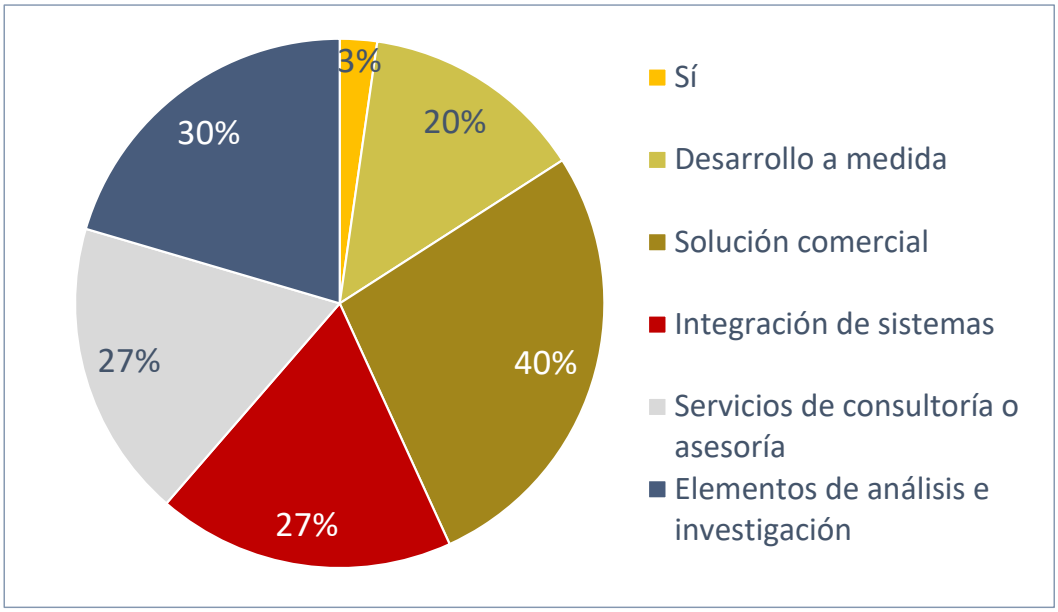


Figura 47. P23: Gráfico. Recolección de información

Un tercio de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la Recolección de información. De las entidades que ofrecen estos servicios, destaca que casi la mitad indica que dispone de una solución comercial y que un tercio realiza trabajos de análisis e investigación en este tipo de capacidades. Las siguientes actividades a las que se dedican un cuarto de las entidades son los Servicios de consultoría o asesoría e Integración de sistemas relacionados. Finalmente, una quinta parte indica que realiza Desarrollos a medida de estos sistemas.

En relación con la capacidad de Recolección de información, una entidad ha desplegado una red de estaciones de registro de datos GNSS (*Global Navigation Satellite System*) con cobertura mundial para monitorizar las prestaciones de navegación de los sistemas GNSS (GPS/GALILEO/GLONAS) y generar datos de corrección para sistemas de navegación GNSS con elevados requisitos de precisión (como la conducción autónoma de vehículos). Además, ha desarrollado para la Comisión Europea el sistema TGVF (*Time and Geodesy Validation Facility*), que recopila datos de una red de 13 estaciones de tierra repartida por los 5 continentes que monitoriza la señal GALILEO y sistemas de monitorización y registro de señales RF en la banda GNSS (GPS/GALILEO) para la detección de *jamming* y *spoofing* (para ENAIRE), así como análisis forense de la señal en caso de incidentes. También, desarrolla sistemas de control de acceso que incluyen monitorización de sensores de presencia física implantados en grandes corporaciones o en la sede de Varsovia-Polonia de FRONTEX.

Es destacable que otra entidad participa en el desarrollo de soluciones[11] para proteger infraestructuras críticas de telecomunicaciones frente a ataques digitales y físicos, permitiendo la detección de intrusos o terminales wifi/*bluetooth* y estaciones terrestres sospechosas.

Otra de las entidades declara disponer de una solución especializada en la recolección de información relacionada con los datos confidenciales de los accesos. Otras cuentan con desarrollos I+D que conectan sensores de presencia física, wifi, *bluetooth* y GPS a los sistemas de seguridad integral o pulseras para trabajadores en entornos industriales para temas de seguridad (*safety*).

Otra entidad desarrolla soluciones[12] de análisis y localización de comunicaciones wifi, *bluetooth*, *zigbee* y otros protocolos utilizados por dispositivos IoT, e implementa ataques de un *purple team* contra este tipo de dispositivos a través de estos protocolos y buscar vulnerabilidades.

Finalmente, varias entidades ofrecen servicios de monitorización de seguridad implementados sobre las arquitecturas y redes de los clientes, basadas en sus capacidades propias de *threat intelligence*, KMS para centralización segura de gestión de claves criptográficas o gestión de la ciberseguridad en entornos IoT.

[11] Como RESISTO, dentro del programa Horizonte H2020.

[12] Como Acrylic WIFI.

Análisis y gestión de riesgos de ciberdefensa

Esta subcapacidad analiza y gestiona los ciberriesgos mediante la identificación de escenarios (conjuntos de activos) y la selección de patrones, generando mapas de ciberriesgos y planes de recomendaciones para mitigarlos. Supone la evolución de los sistemas clásicos de análisis de riesgos.

Los datos recogidos en la pregunta *24. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Análisis y gestión de riesgos de ciberdefensa**, se muestran en la siguiente figura:

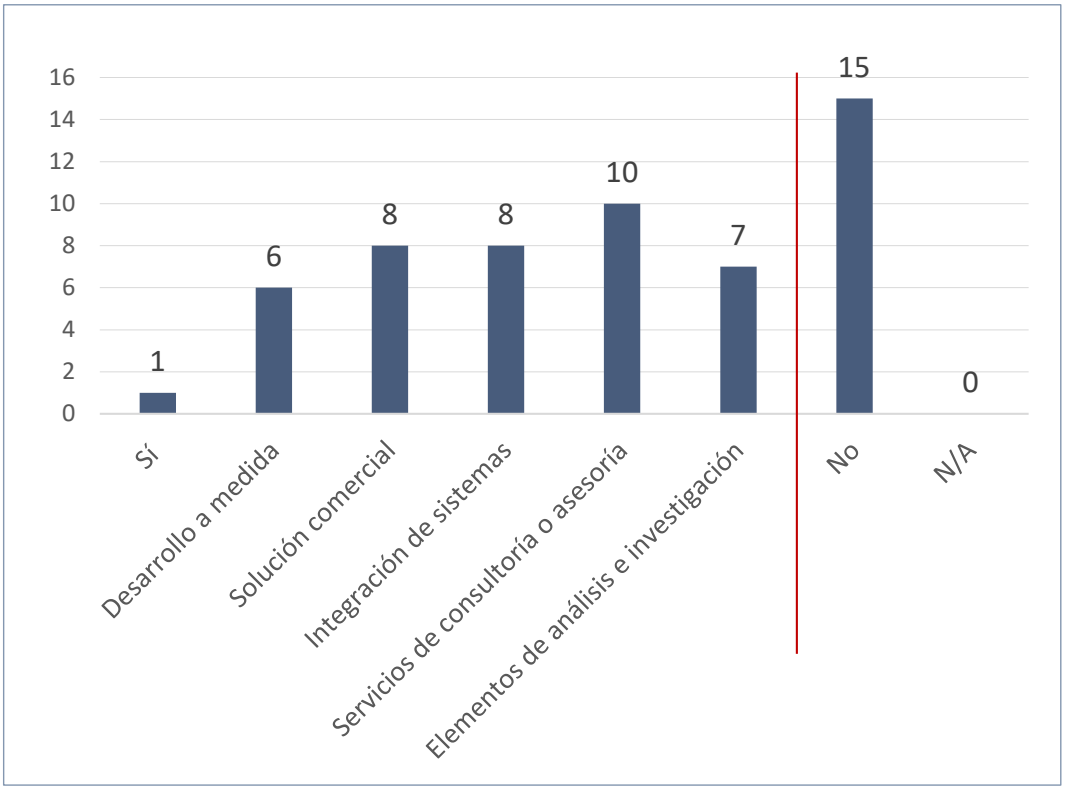


Figura 48. P24: Datos análisis y gestión de riesgos de ciberdefensa

La representación gráfica de los datos positivos se muestra en la siguiente figura:

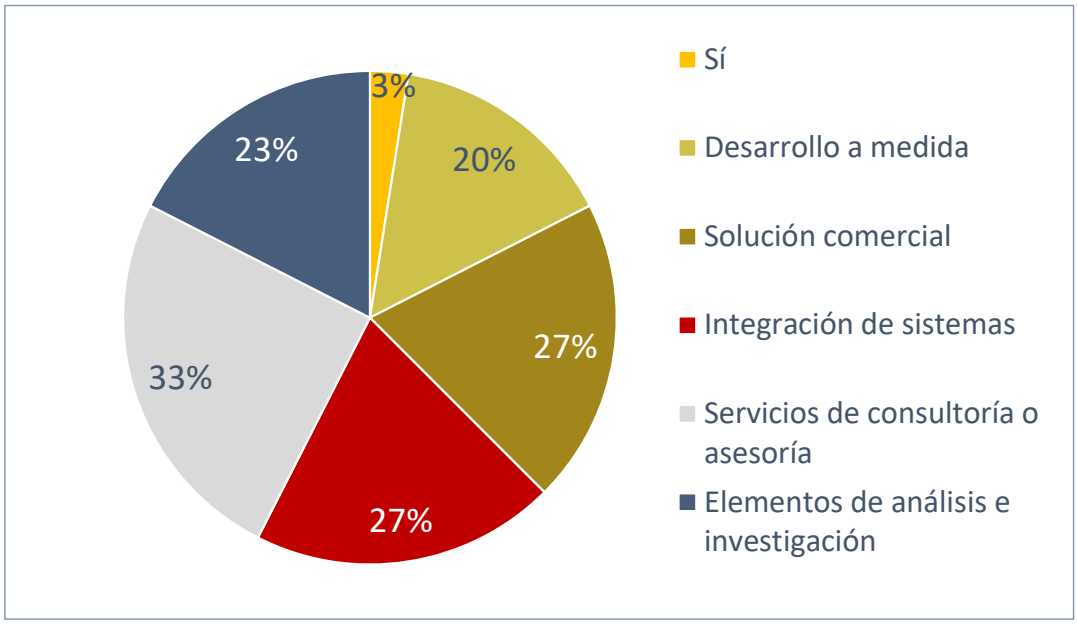


Figura 49. P24: Gráfico. Datos análisis y gestión de riesgos de ciberdefensa

La mitad de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con el análisis y gestión de riesgos de ciberdefensa. De las entidades que ofrecen estos servicios, destaca que un tercio indica que realizan servicios de consultoría o asesoría. Las siguientes actividades a la que se dedica un cuarto de las entidades que ofrecen estos servicios, son la Integración de sistemas relacionados, la disposición de una solución comercial propia y los trabajos de análisis e investigación en este tipo de capacidades. Finalmente, una minoría indica que realiza desarrollos a medida de estos sistemas.

En relación con esta capacidad, una entidad declara haber liderado el desarrollo del componente de gestión de riesgos a nivel de misión construido en el marco *Cyber Situation Awareness Package* (CySAP) de la EDA, además de encontrarse desarrollando y mejorando capacidades de gestión de riesgos, dinámica enfocada en las necesidades nativas (contexto operacional, misión, objetivos, criticidad del ciberespacio que constituye, etc.).

Algunas entidades indican que están realizando trabajos de análisis y gestión de riesgos de ciberdefensa en clientes militares de Europa o del **ámbito OTAN**. Estas entidades emplean las herramientas y metodologías utilizadas por la OTAN, las Instituciones Europeas y la Agencias Nacionales de Seguridad de Sistemas de Información (como MAGERIT/PILAR o ANSSI/EBIOS RM). Otro grupo de entidades indica que realiza los despliegues en los clientes. Este grupo desarrolla un análisis de riesgos en el ámbito del acceso a la información confidencial, mediante software comercial[13] y servicios de consultoría especializada, o de predicción de impacto y propagación de riesgos con IA en infraestructuras críticas.

[13] Como por ejemplo SEALPATH o DYNABIC.

También encontramos entidades que realizan análisis de riesgos en el sector financiero. Este grupo prioriza las matrices de decisión para definir planes de actuación y empleaestándares como TIBER-EU del Banco Central Europeo. Además, estas entidades diseñan escenarios de ataque (servicio de *red team*) basado en los resultados obtenidos para realizar intrusiones en los sistemas informáticos de los clientes.

Entidades del ámbito de defensa y seguridad despliegan redes y sistemas que requieren ser acreditados para el manejo de información clasificada (nacional, EU y OTAN), Debido a esto, es básico que las actividades de análisis de riesgos sigan las metodologías reconocidas, como MAGERIT, son básicas, además de prestar estos servicios en su CERT/CSIRT. Desde los distintos SOC se ofrecen servicios de identificación formal de ciberriesgos y su posterior tratamiento.

Finalmente, otras entidades realizan análisis de riesgos formales con base en MAGERIT teniendo en cuenta las amenazas contra la seguridad de la información (activos, indicadores de riesgo, vulnerabilidades y recomendaciones para mitigarlos) aunque sin centrarse en amenazas concretas del ciberespacio (cibercrimen, grupos esponsorizados por estados...), para lo que emplean la herramienta CCN-ANA integrada con CCN-CLARA y otras herramientas de análisis de vulnerabilidades[14].

[14] Como Nessus.

Reacción y recuperación ante ataques

Esta subcapacidad reacciona ante los ataques, recogiendo información para su tratamiento y clasificación. Entre otras acciones, realizan parcheos de emergencia, reconfiguraciones del sistema, despliegue de herramientas de ciberseguridad o captura de evidencias.

Los datos recogidos en la pregunta *25. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Reacción y recuperación ante ataques**, se muestran en la siguiente figura:

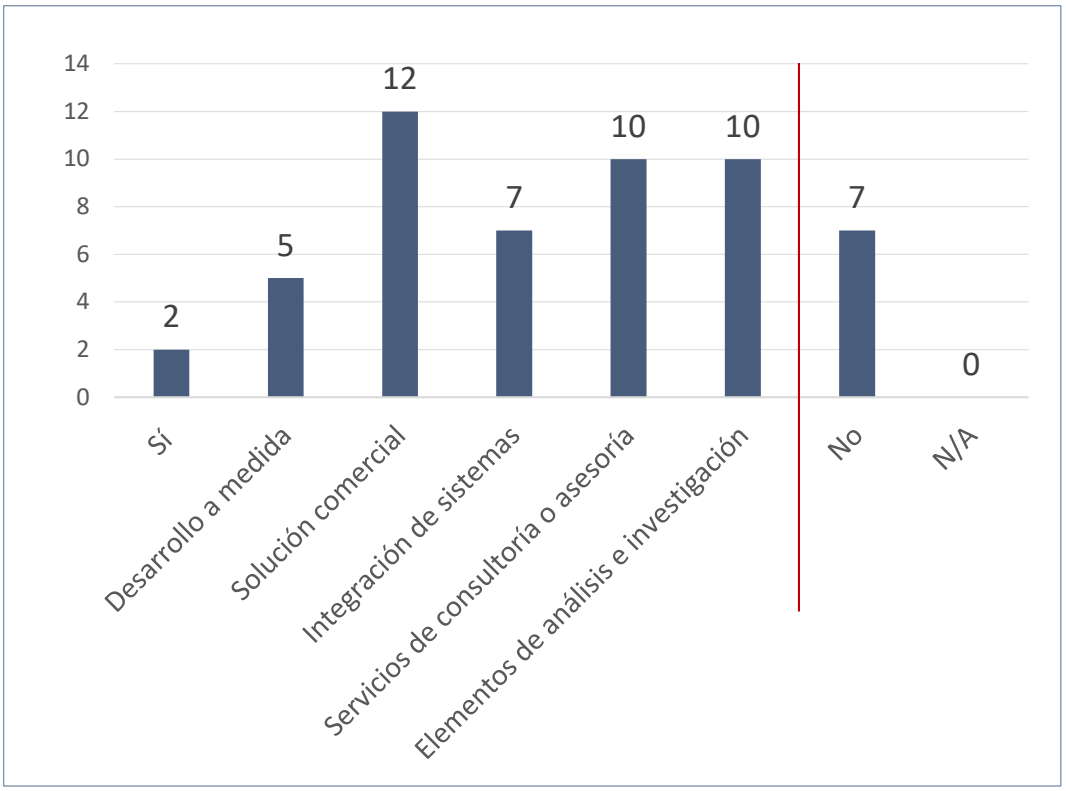


Figura 50. P25: Datos reacción y recuperación ante ataques

La representación gráfica de los datos positivos se muestra en la siguiente figura:

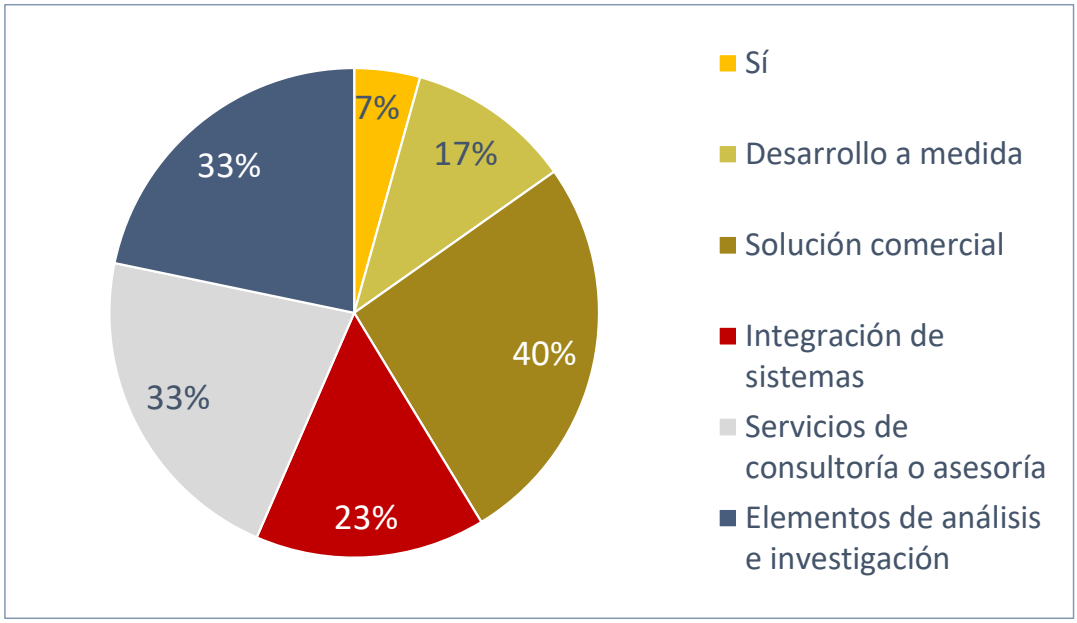


Figura 51. P25: Gráfico. Reacción y recuperación ante ataques

Un cuarto de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la reacción y recuperación ante ataques. De las entidades que ofrecen estos servicios, destaca que casi la mitad indica que dispone de una solución comercial. Las siguientes actividades a la que se dedica un tercio de las entidades son los trabajos de análisis e investigación y los servicios de consultoría o asesoría. Finalmente, una cuarta parte de las entidades se dedica a la Integración de sistemas relacionados y una quinta parte indica que realiza desarrollos a medida de estos sistemas.

Relacionado con esta capacidad, varias entidades indican que disponen de un SOC o CSIRT propio, integrado con la red NCIA-OTAN y miembro del CSRIT.es, con hasta un nivel 3 para la respuesta a incidentes de seguridad y con capacidad de respuesta remota en un máximo de dos horas y capacidad de desplegarse en cualquier parte de Europa en un máximo de 48 horas.

Otras entidades ofrecen servicios de reacción y recuperación ante ataques mediante la preparación para incidentes (DFIR: *Digital Forensic & Incident Response*), realización de ciberejercicios, evaluación del compromiso y recuperación de la infraestructura después de los incidentes. Otras prestan servicios de *compromise assessment* para intervenir en entornos potencialmente comprometidos, detectar el alcance de la intrusión y ayudar a contener la intrusión.

Otro grupo de entidades ofrece soluciones propias para la recuperación de imágenes autenticadas de *firmware* en dispositivos IoT. Estas soluciones están basadas en *blockchain* y en sistemas de *backup and restore*, de alta disponibilidad, de gestión centralizado

de parcheos o de despliegue de agentes de seguridad del *endpoint.* Su priorización se realizará según la información proporcionada por herramientas comerciales, las CMDB de los clientes y las herramientas de SCCM en función de la disponibilidad, sensibilidad y confidencialidad de la información asociada.

Otras de las herramientas más empleadas son de tipo SOAR (*Security Orchestration, Automation and Response*) apoyadas con inteligencia artificial y RL (*Reinforcement Learning*)[15] o integración con herramientas SIEM (Administración de eventos e información de seguridad) para generar procesos de modificación de políticas de protección o revocación de accesos a la información.

Intercambio de información de ciberseguridad

Esta subcapacidad permite agilizar la labor de análisis de ciberincidentes y compartir información de ciberamenazas, contextualizada y correlacionada con las principales fuentes de información, mediante un lenguaje común de peligrosidad y clasificación del incidente. Se basa en gran medida en la tecnología MISP (*Malware Information Sharing Platform*).

Los datos recogidos en la pregunta *26. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Intercambio de información de ciberseguridad**, se muestran en la siguiente figura:

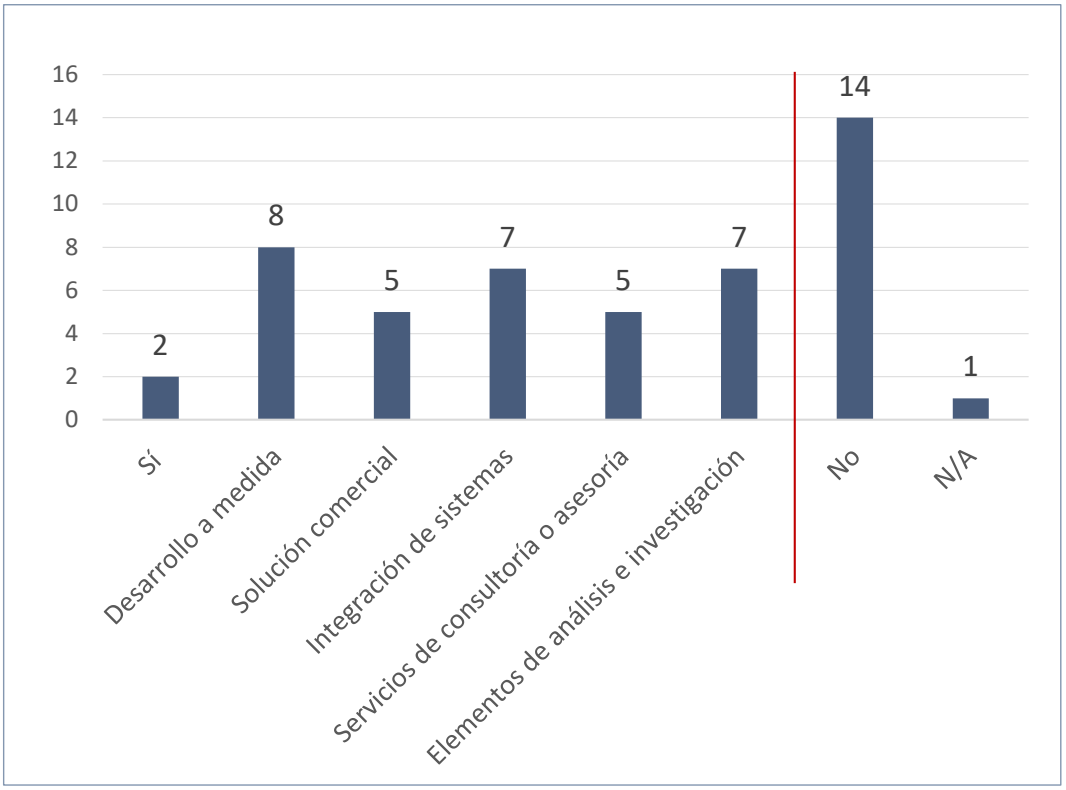


Figura 52. P26: Datos intercambio de información de ciberseguridad

[15] Como AI4CYBER.

La representación gráfica de los datos positivos se muestra en la siguiente figura:

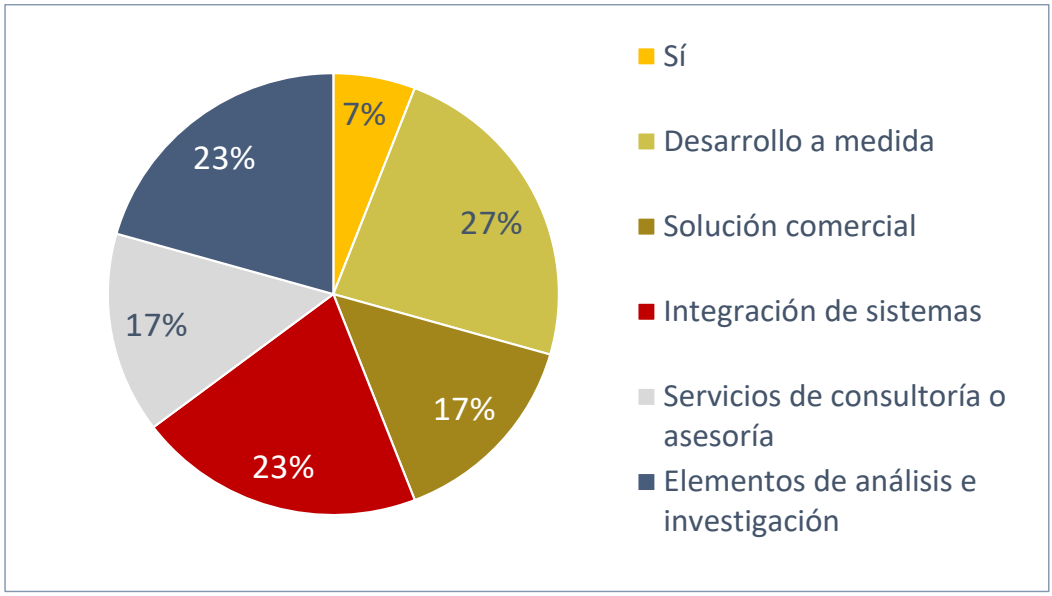


Figura 53. P26: Gráfico.Intercambio de información de ciberseguridad

La mitad de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con el Intercambio de información de ciberseguridad. De las entidades que ofrecen estos servicios, destaca que una cuarta parte realiza desarrollos a medida de este tipo de capacidades, integración de sistemas relacionados y trabajos de análisis e investigación. Finalmente, una minoría indica que dispone de una solución comercial y que realiza servicios de consultoría o asesoría de estos sistemas.

Varias entidades disponen de sistemas MISP para la comunicación de incidentes de ciberseguridad basados en la NIS2 (*Network and Information Security*) o integrados en redes como la del CSIRT.es o de la NCIA. Sus equipos de ciberseguridad y gestión de incidentes intercambian información para poder actuar de forma rápida y coordinada ante cualquier ciberincidente y ciberamenaza que pueda afectar simultáneamente a distintas entidades.

Algunas de ellas indican que trabajan en su propia base de datos de conocimiento integrando tecnologías[16] para el intercambio de información de *threat actors* e incidentes, con el objetivo de poder ofrecer estos *feeds* de información.

Como se ha indicado anteriormente, varias entidades disponen de SOC propio desde el que comparten información sobre ciberamenazas con otros SOC autorizados.

Otra entidad declara disponer de una solución, integrable con sistemas SIEM, para la notificación en tiempo real de los ataques detectados y neutralizados por el sistema, identificando patrones y ataques dirigidos.

[16] Como MISP + CORTEX + THE HIVE.

Finalmente, aunque no directamente relacionado con la información de ciberseguridad, en el cuestionario han participado entidades expertas en el intercambio automático o selectivo de información sensible. Esta información se refiere a datos JISR (J*oint Intelligence, Surveillance and Reconnaissance*) en coaliciones de la OTAN o a datos en vigilancia de fronteras y vigilancia marítima en las redes europeas EUROSUR y CISE mediante mecanismos software de distribución de datos no centralizados.

Despliegue de centros de operaciones de seguridad (COS-D)

Esta subcapacidad permite desplegar un COS desplegable en las redes e infraestructuras IT y OT, transportable, para realizar funciones de monitorización continua y análisis proactivo de amenazas, gestión de incidentes de seguridad o investigación y análisis forense, entre otras funciones,con el objetivo de mejorar la capacidad de respuesta ante ataques para sistemas IT y OT.

Los datos recogidos en la pregunta *27. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Despliegue de centros de operaciones de seguridad**, se muestran en la siguiente figura:

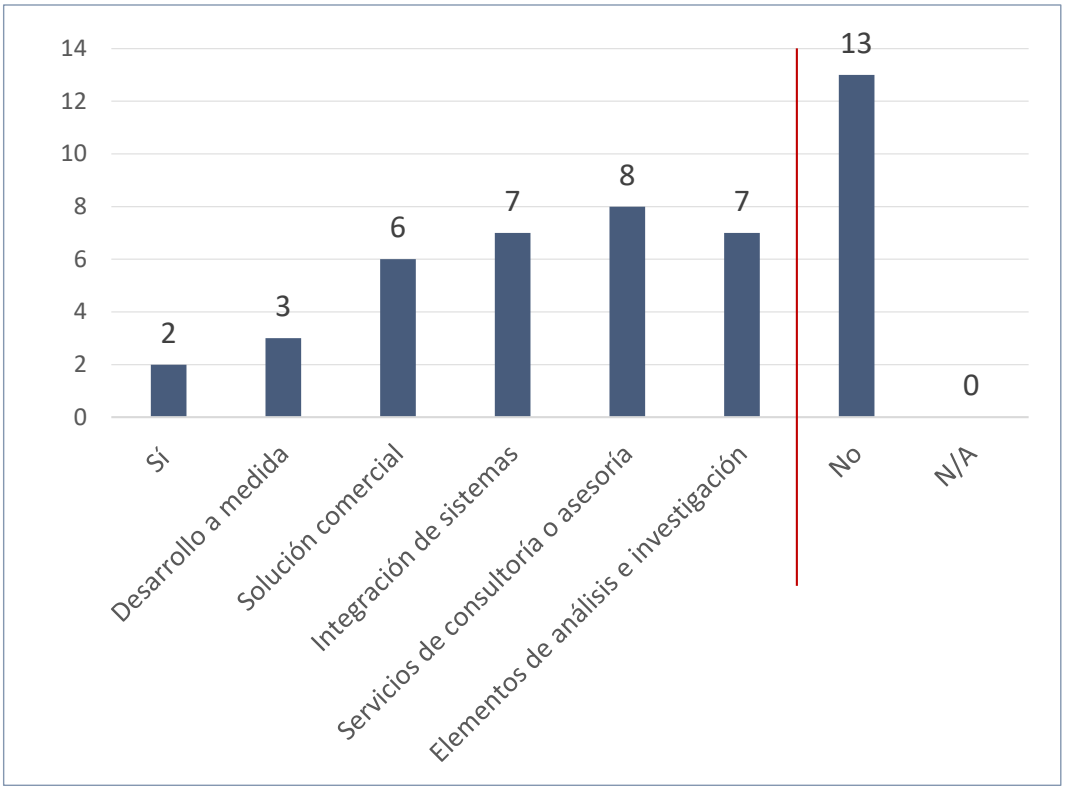


Figura 54. P27: Datos Despliegue de Centro de operaciones de seguridad

La representación gráfica de los datos positivos se muestra en la siguiente figura:

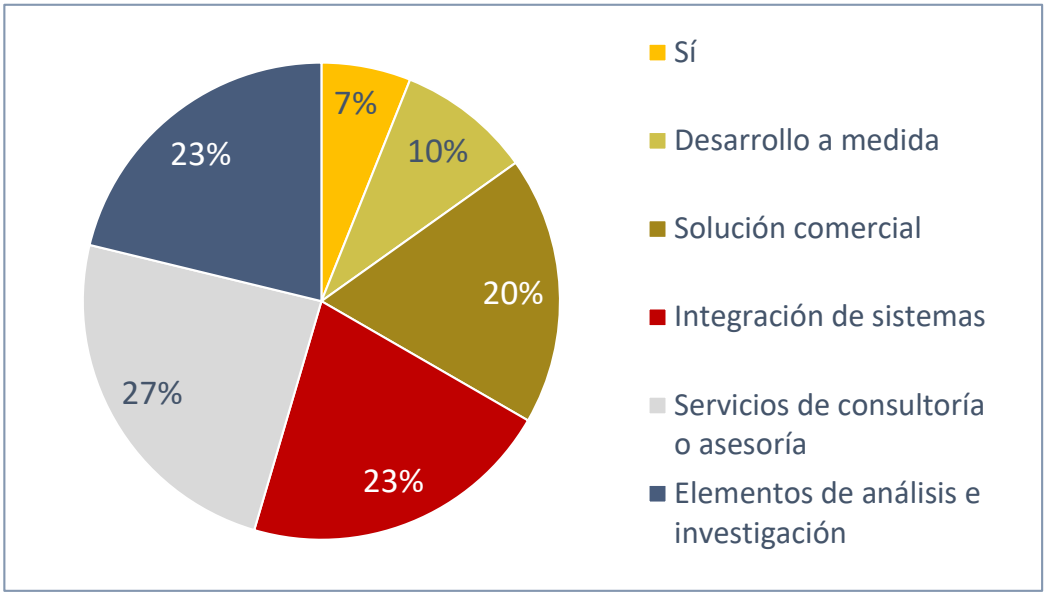


Figura 55, P27: Gráfico. Despliegue de centro de operaciones de seguridad

Casi la mitad de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con el despliegue de centros de operaciones de seguridad. De las entidades que ofrecen estos servicios, destaca que una cuarta parte indica que realiza servicios de consultoría o asesoría, trabajos de análisis e investigación y de Integración de sistemas. Finalmente, una quinta parte de las entidades dispone de una solución comercial y una minoría indica que realiza desarrollos a medida de estos sistemas.

Relacionado con esta capacidad, sólo una de las entidades indica disponer de soluciones desplegables y transportables para COS militares, poniendo de ejemplo un SOC táctico.

Otras entidades indican haber realizado desarrollos a medida de redes y sistemas (para la EDA o FRONTEX entre otros) donde han diseñado y desplegado COS que integran diferentes herramientas comerciales y servicios típicos o proyectos como el *Deployable Cyber Evidence Collection and Evaluation Capability* (DCEC2) para la EDA en el que han desarrollado un demostrador de tecnología forense desplegable para operaciones militares aplicando soluciones tecnológicas como las medidas antiforenses.

Del resto de entidades, algunas indican que disponen de SOC propio no desplegable o que se pueden desplegar en un COS para realizar la monitorización de eventos de red, *endpoint* y otro tipo de amenazas de forma conjunta.

Por tratarse del área más extendida, existe una gran cantidad de entidades enfocadas en este campo, aunque cabe destacar el amplio uso de herramientas de terceros frente a desarrollos propios. Es recomendable lograr un mayor aprovechamiento de las fortalezas y experiencias adquiridas en este ámbito para aumentar las soluciones nacionales en cada una de las subáreas, aunque se aprecia en todas ellas un incipiente interés en el desarrollo de soluciones propietarias. Además, sería de interés conseguir la interoperabilidad entre estas soluciones para contribuir a una capacidad nacional global.

6.3. Capacidad de explotación

Esta capacidad es un conjunto de herramientas, propias o de terceros, destinadas a extraer datos e inteligencia de las redes y sistemas del adversario.

Esta capacidad se desglosa en **nueve subcapacidades** que se detallan a continuación:

Recolección de inteligencia de fuentes abiertas

Esta subcapacidad permite recopilar datos públicos sobre organizaciones, sitios web e identidades, para conocer la presencia social y tecnológica en Internet. Permite un análisis profundo de las interrelaciones en línea y amplía la capacidad de conocimiento de las identidades digitales.

Los datos recogidos en la pregunta *28. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Recolección de inteligencia de fuentes abiertas**, se muestran en la siguiente figura:

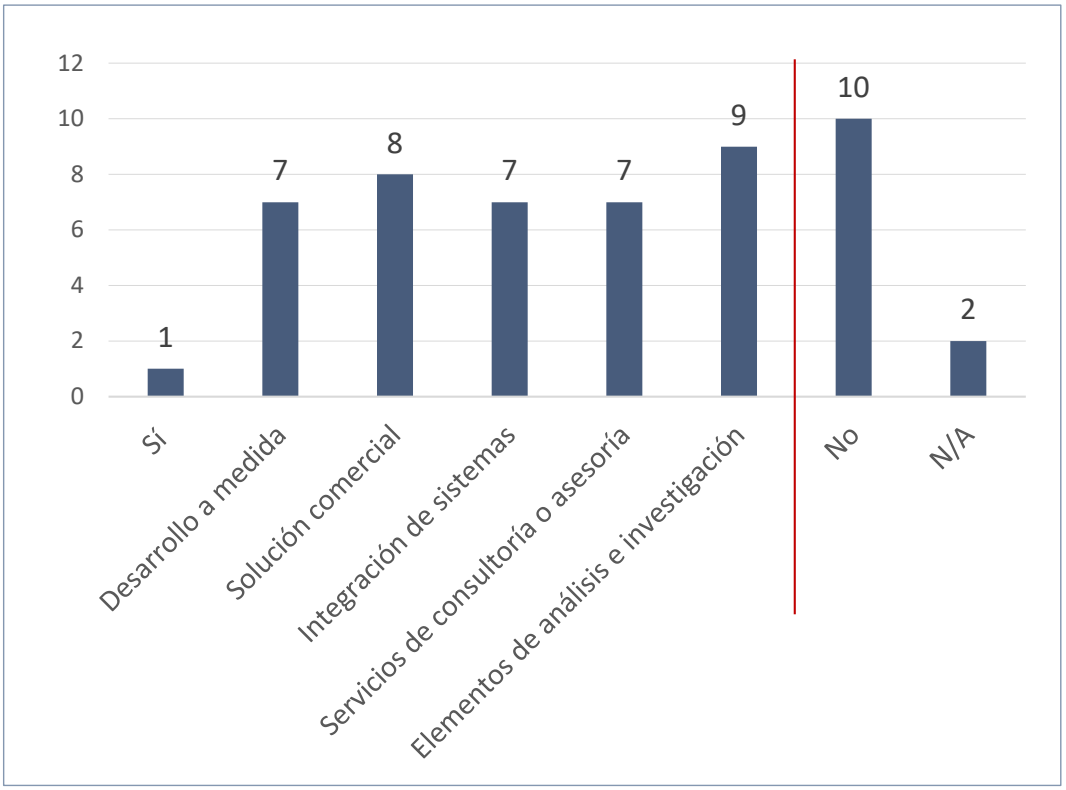


Figura 56. P28: Datos recolección de inteligencia de fuentes abiertas

La representación gráfica de los datos positivos se muestra en la siguiente figura:

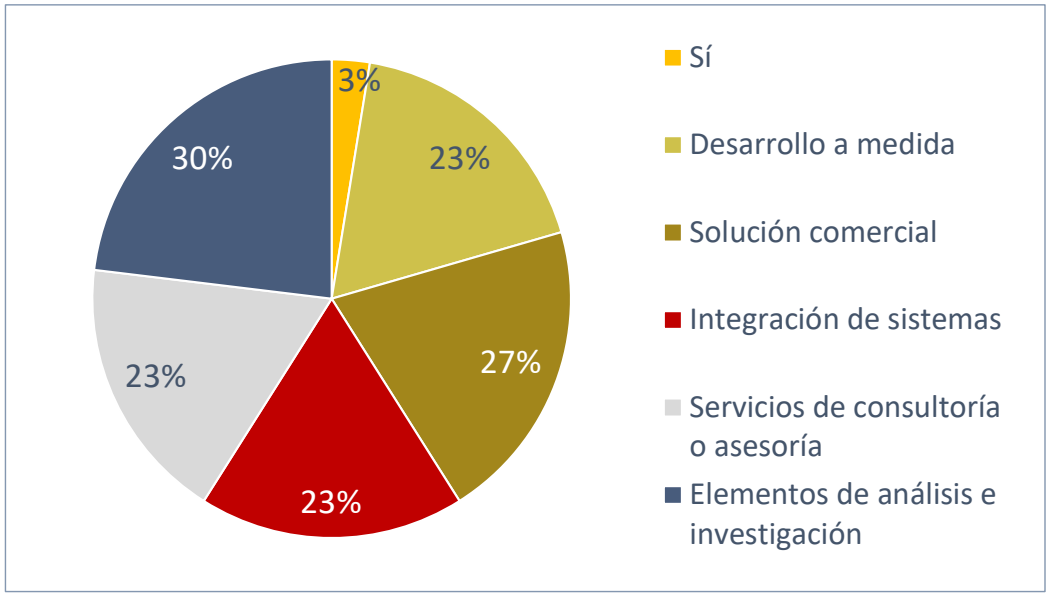


Figura 57. P28: Gráfico. Recolección de inteligencia de fuentes abiertas

Casi un tercio de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de recolección de inteligencia de fuentes abiertas. De las entidades que ofrecen estos servicios, destaca que casi un tercio indica que realiza trabajos de análisis e investigación. Del resto, una cuarta parte indica que dispone de una solución comercial, que realiza servicios de consultoría o asesoría, de Integración de sistemas y desarrollos a medida de estos sistemas.

Relacionado con esta capacidad, al menos indica que utiliza soluciones comerciales conocidas que ofrecen capacidades relacionadas con esta área. Además estas entidades dispondrían de una célula de inteligencia formada por analistas con formación especializada en esta área y capaces de realizar labores de *background check*[17], *social listening*, vigilancia digital, *screening* digitales de personas físicas y jurídicas, análisis de eventos de desinformación digital masiva, etc. Otras entidades expresan que disponen de personal técnico que realiza este tipo de operaciones de recolección de inteligencia de fuentes abiertas para explotación interna y al menos otra que proporciona servicios para la recopilación en fuentes abiertas utilizando[18] productos comerciales o servicios de terceros.

En las respuestas, también se indica la participación de una entidad en el proyecto PASTOR (Plataforma de Análisis de Servicios en TOR), financiado por el Instituto de Competitividad Empresarial (ICE) de la Junta de Castilla y León, a través de los Fondos FEDER de la Unión Europea, y coordinado técnicamente por INCIBE.

[17] *Background check*: verificación de los antecedentes de una persona. *Social Listening*: análisis de opinión social de la propia marca.

[18] Como 4IQ o Blueliv.

Reconocimiento

Esta subcapacidad permite el descubrimiento de redes, vulnerabilidades y capacidades defensivas de los sistemas adversarios con fines de inteligencia, identificación de direcciones IP de una red (estáticas, dinámicas, reservadas y abandonadas) y puertos en uso o abiertos en cada dispositivo, así como información sobre los hosts del adversario (*hardware*, *software*, *firmware* o configuraciones de los clientes) o detalles sobre su topología (DNS, nombres de dominio, etc.).

Los datos recogidos en la pregunta *29. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Reconocimiento**, se muestran en la siguiente figura:

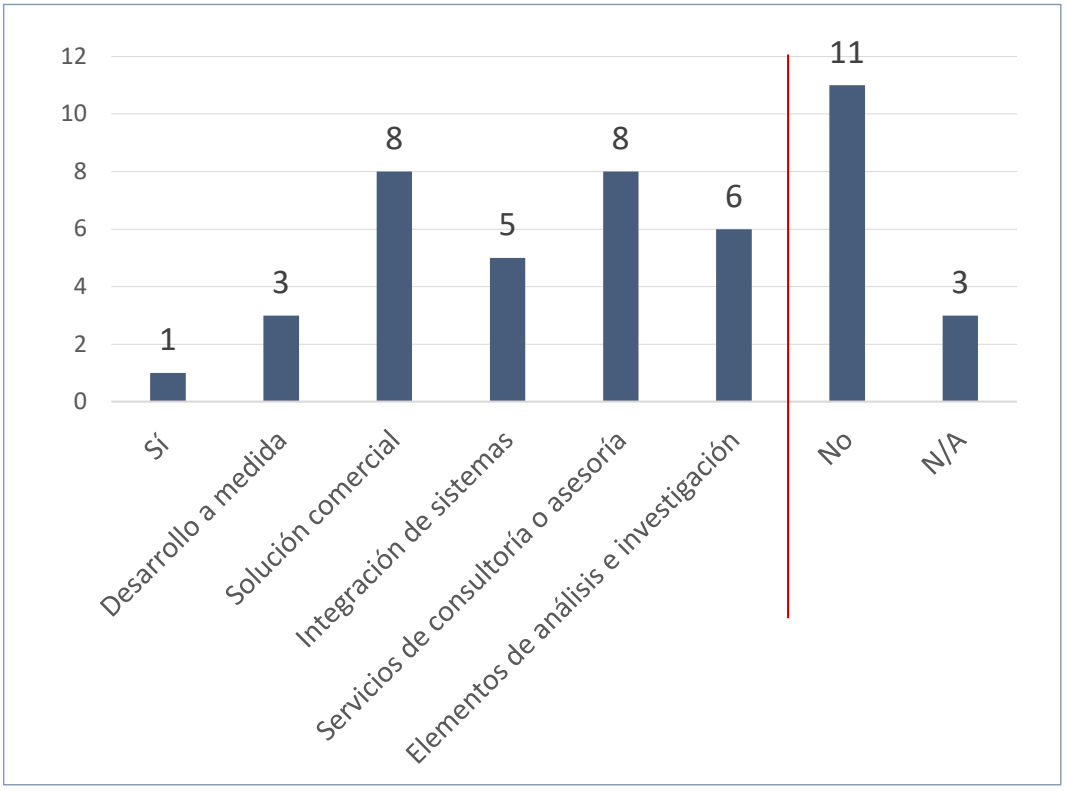


Figura 58. P29: Datos Reconocimiento

La representación gráfica de los datos positivos se muestra en la siguiente figura:

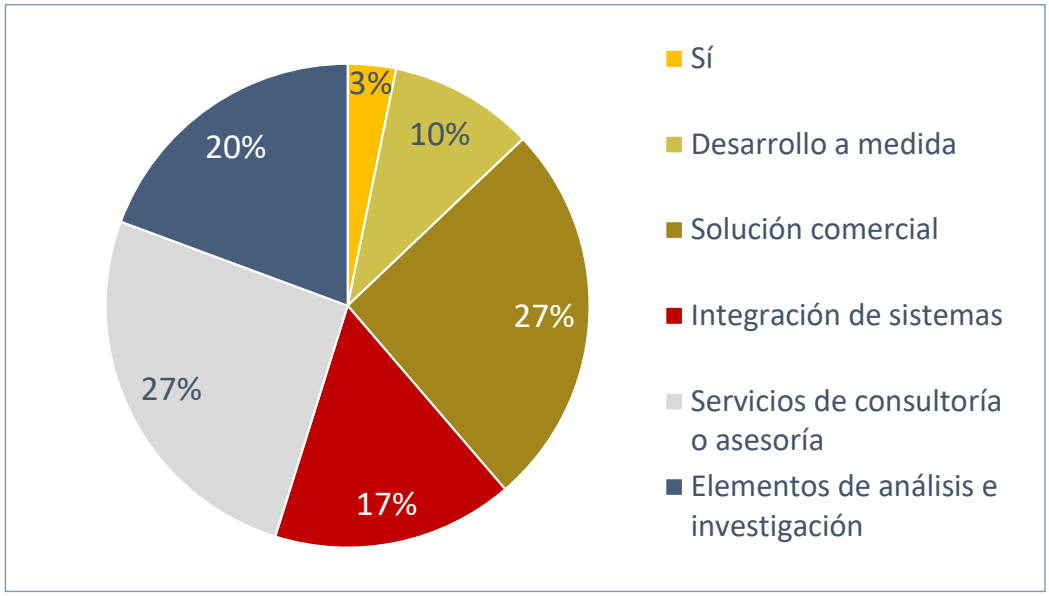


Figura 59. P29: Gráfico.Reconocimiento

Casi la mitad de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de reconocimiento. De las entidades que ofrecen estos servicios, destaca que la cuarta parte indica que dispone de una solución comercial y que realiza servicios de consultoría o asesoría. El resto de actividades con mayor dedicación son las tareas de análisis e investigación e Integración de sistemas. Finalmente, una minoría indica que realiza desarrollos a medida de este tipo de capacidad.

Aunque algunas entidades indican que emplea soluciones para reconocimientos de su superficie de ataque y al menos otra que indica que proporciona servicios de reconocimientos de superficie expuesta, en estos casos parece que hacen referencia al uso de productos comerciales y no a desarrollos propios. Parece a priori que existe una falta de capacidad de desarrollo de sistemas de reconocimientos propios que incluya la alta capacidad de discreción necesaria para operaciones de reconocimientos de carácter militar y en apoyo a operaciones ofensivas.

Transformación, integración y enumeración de la información

Esta subcapacidad, gracias al empleo de técnicas de tratamiento masivo de datos, transforma y relaciona los datos obtenidos con el objetivo de adquirir información útil para los analistas.

Los datos recogidos en la pregunta *30. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Transformación, integración y enumeración de la información**, se muestran en la siguiente figura:

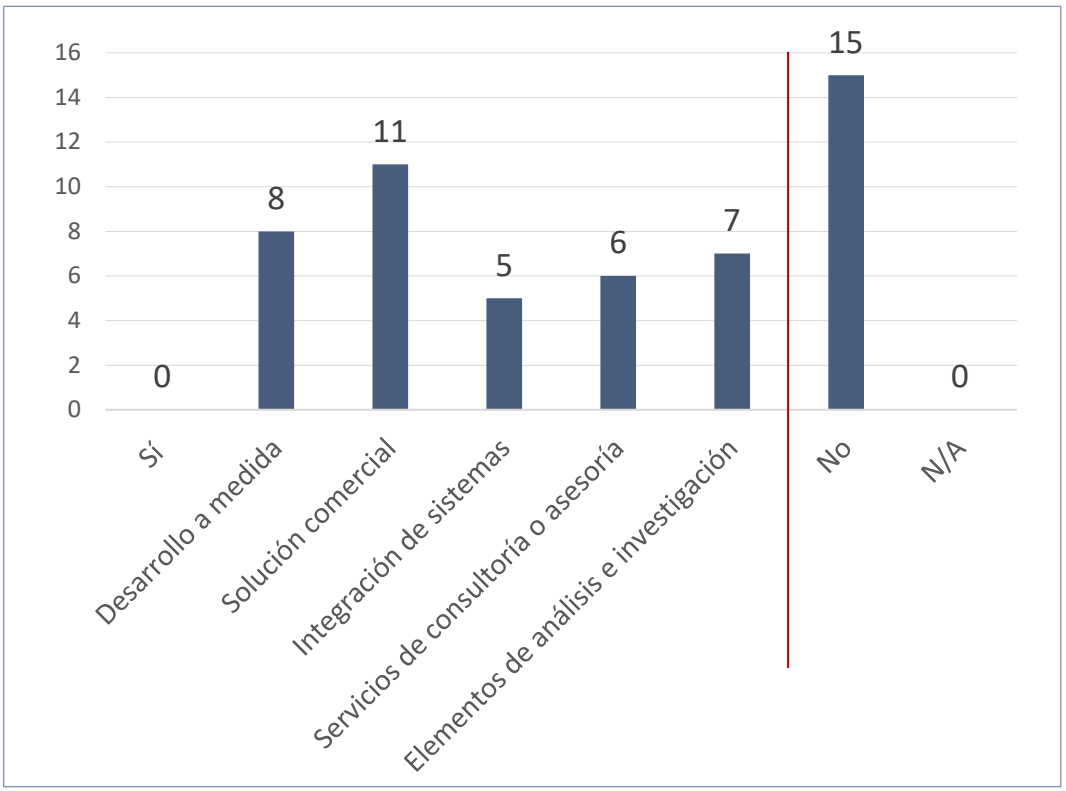


Figura 60. P30: Datos Transformación, integración y ennumeración de la información

La representación gráfica de los datos positivos se muestra en la siguiente figura:

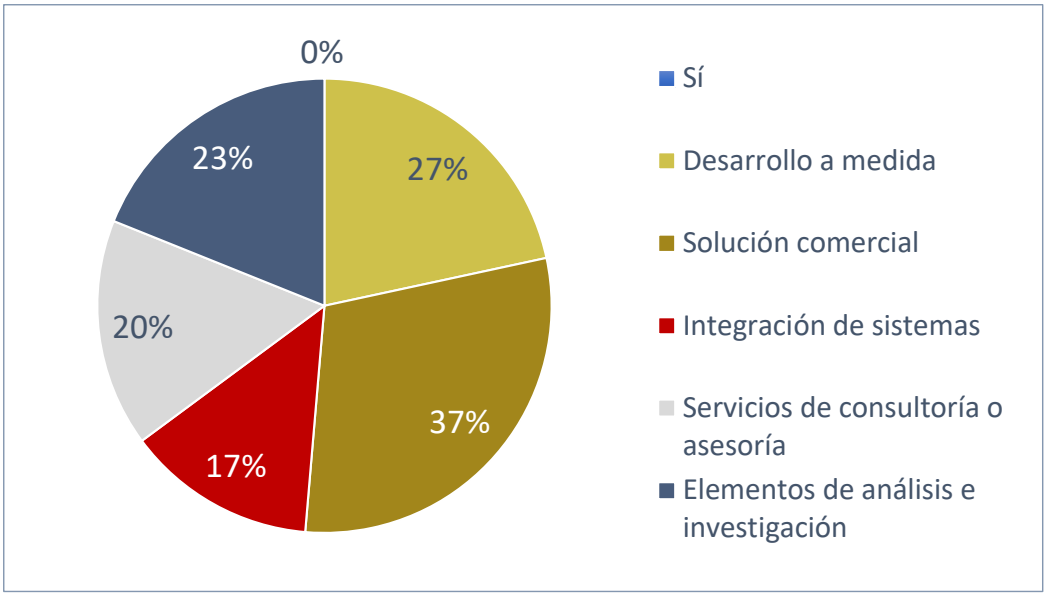


Figura 61. P30: Gráfico. Transformación, integración y ennumeración de la información

La mitad de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de transformación, integración y enumeración de la información. De las entidades que ofrecen estos servicios, destaca que un tercio indica que dispone de una solución comercial. Las siguientes actividades a la que se dedica un cuarto de las entidades relacionadas con esta capacidad son los desarrollos a medida de este tipo de sistemas y los trabajos de análisis e investigación. Finalmente, las actividades menos citadas son los servicios de consultoría o asesoría e Integración de sistemas de este tipo.

En relación con esta capacidad alguna entidad ha indicado que desarrollan aplicaciones de análisis de datos con avanzadas técnicas de fusión y correlación y una incorporación creciente de técnicas de inteligencia artificial para defensa y seguridad. Destacan como referencias[19] el programa SIGLO/SANTIAGO y la *suite* de *Business Intelligence* para análisis desarrollada para FRONTEX (BI *Analytical tools*) junto con proyectos de I+D como ABIDE (*Artificial Intelligence and Big Data for Decision Making in* C4ISR) para la EDA y el proyecto AI4DEF (*Artificial Intelligence for Defence*) enfocado al uso de inteligencia artificial en defensa dentro del EDIDP.

Otras entidades indican que ofrece servicios comerciales y de investigación en el ámbito de la ciberdefensa basados en técnicas de *machine learning,* inteligencia artificial sobre volúmenes masivos de datos y *deep learning*.

[19] Algunos ejemplos propios son SAPIIEM JISR o la *suite* Sócrates para agencias de vigilancia marítima.

Representación de la información

Esta subcapacidad presenta la información en distintos formatos de forma visual o simbólica y muestra las distintas relaciones existentes entre la información presentada.

Los datos recogidos en la pregunta *31. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Representación de la información**, se muestran en la siguiente figura:

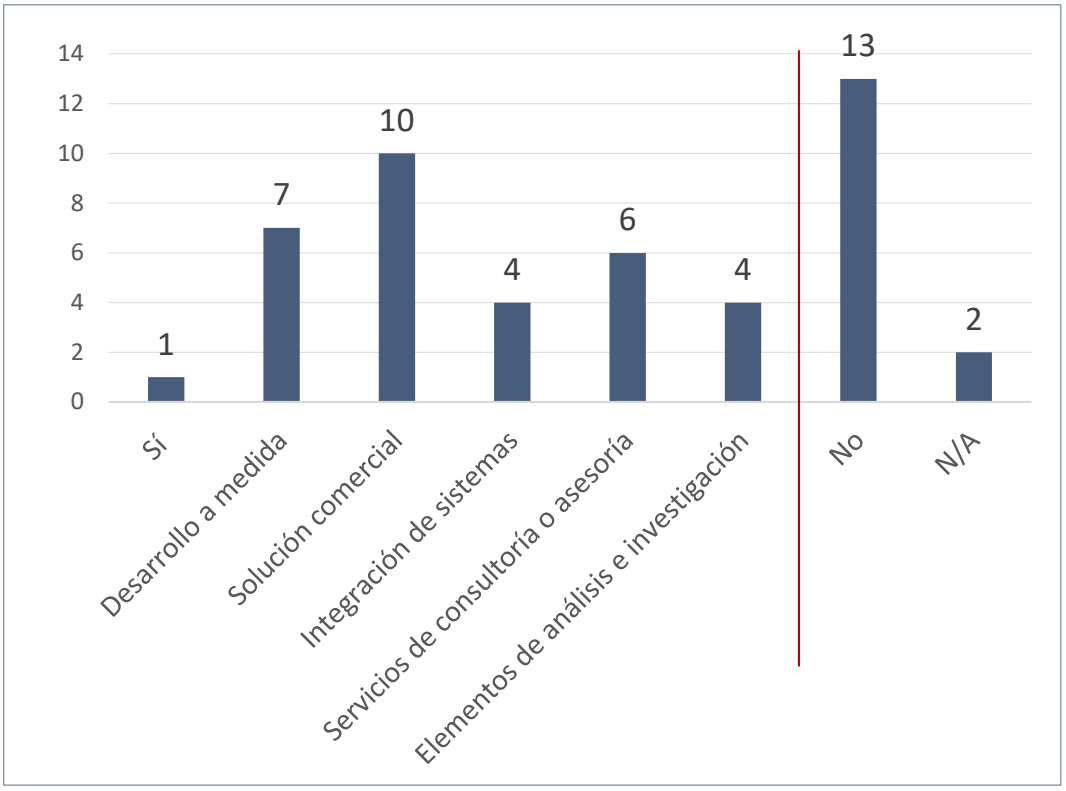


Figura 62. P31: Datos Representación de la información

La representación gráfica de los datos positivos se muestra en la siguiente figura:

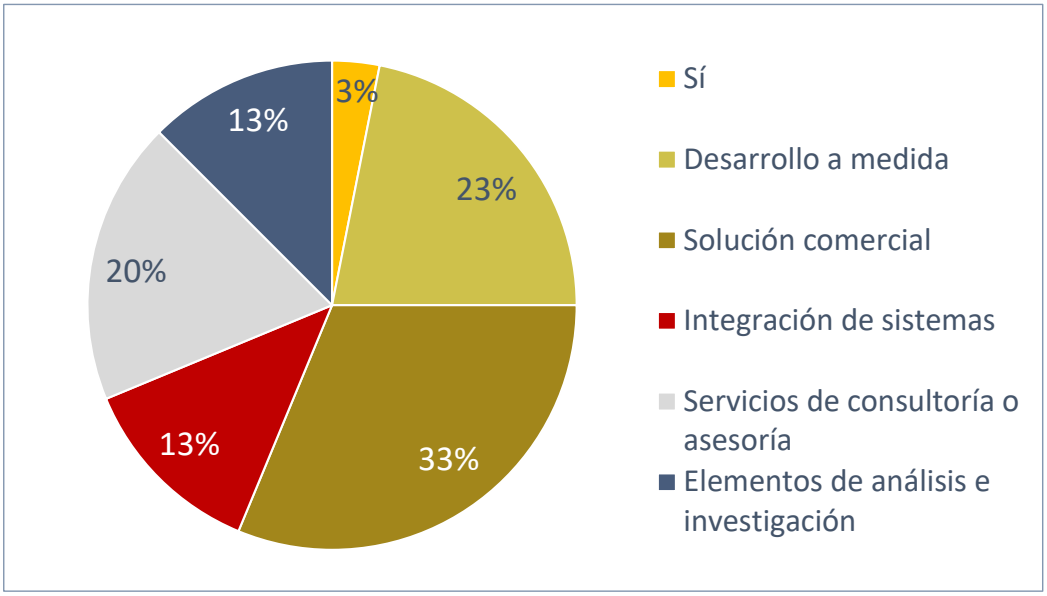


Figura 63. P31: Gráfico. Representación de la información

La mitad de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de representación de la información. De las entidades que ofrecen estos servicios, destaca que un tercio indica que dispone de una solución comercial. Del resto, un cuarto indica que realiza desarrollos a medida y una quinta parte que realiza servicios de consultoría o asesoría. Finalmente, una minoría indica dedicarse a tareas de análisis e investigación e Integración de sistemas de este tipo.

En relación con esta capacidad algunas entidades indican que disponen de potentes herramientas de visualización de datos ya sea con soluciones propias o bien con herramientas de terceros. Esto permiten a los analistas identificar patrones y correlaciones entre eventos y otros tipos de información y realizar análisis de manera visual e interactiva a fin de facilitar su comprensión y toma de decisiones. Otras entidades indican que disponen de capacidad de análisis y elaboración de inteligencia en el ciberespacio.

Una entidad indica que ofrece soluciones con diferentes formatos de visualización de la información en sus productos, sobre todo orientados a la representación geográfica de los datos recogidos. También disponen de numerosas herramientas con cuadros de mando. En concreto, esta entidad está desarrollando, dentro de un proyecto, una herramienta para la conducción de operaciones de ciberdefensa que maneja datos complejos y relacionados entre ellos, así como un módulo específico que muestra una arquitectura de red compleja y con distintos niveles de abstracción.

Gestor de mapeo de identidades y vínculos de red en internet

Esta subcapacidad recopila datos públicos sobre organizaciones, sitios web e identidades, para conocer su presencia social y tecnológica en internet. Permite la exploración de correos electrónicos, números de teléfono, sitios web, organizaciones o dominios recopilados automáticamente de fuentes públicas, mostrándolos en forma de árboles de relaciones.

Los datos recogidos en la pregunta *32. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Gestor de mapeo de identidades y vínculos de red en internet**, se muestran en la siguiente figura:

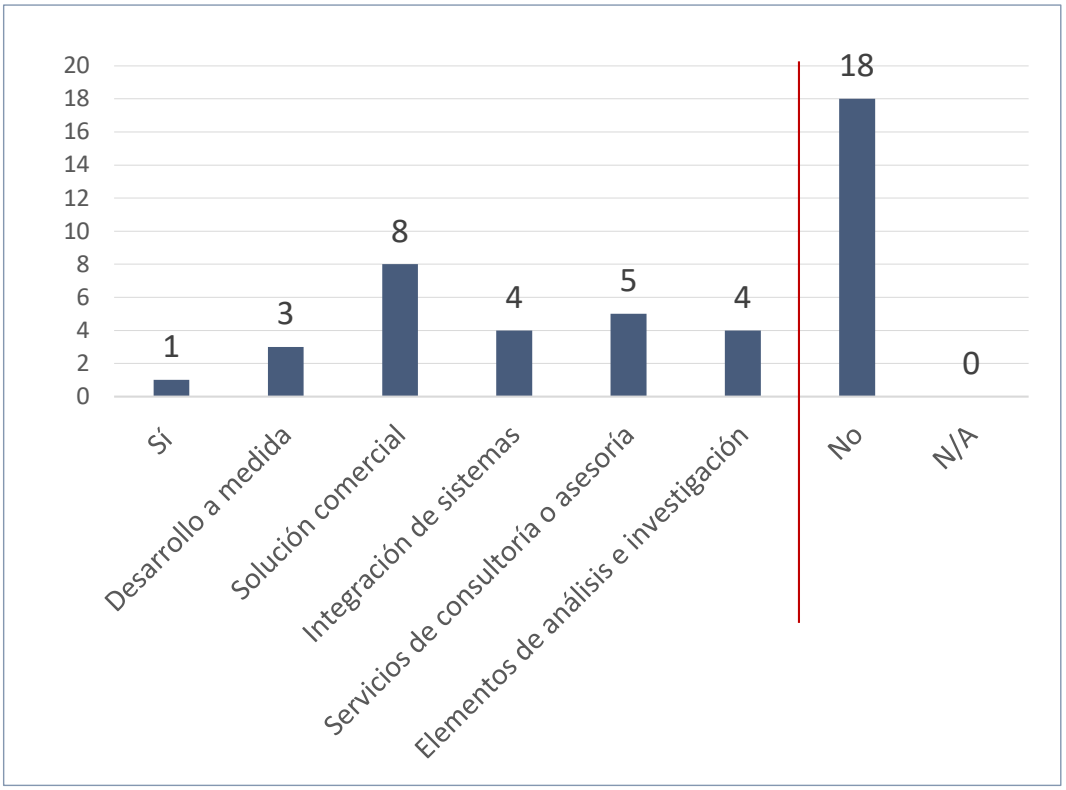


Figura 64. P32: Datos Gestor de mapeo de identidades y vínculos de red en internet

La representación gráfica de los datos positivos se muestra en la siguiente figura:

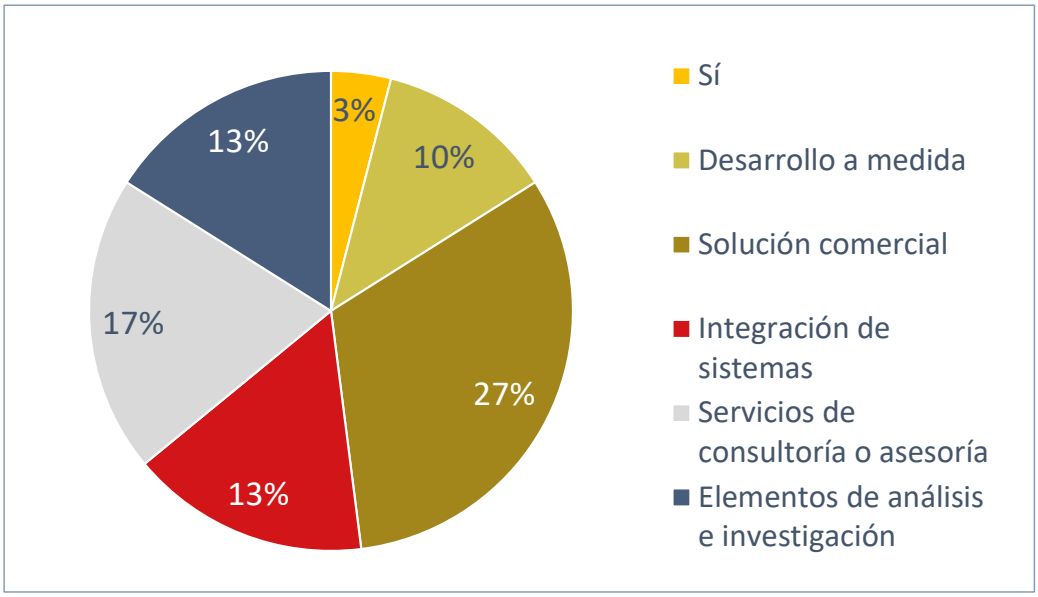


Figura 65. P32: Gráfico. Gestor de mapeo de identidades y vínculos de red en internet

La mayoría de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de gestión de mapeo de identidades y vínculos de red en internet. De las entidades que ofrecen estos servicios, destaca que una cuarta parte indica que dispone de una solución comercial. Del resto, las siguientes actividades relacionadas con esta capacidad a la que más se dedican las entidades son servicios de consultoría o asesoría, Integración de sistemas y trabajos de análisis e investigación. Finalmente, una minoría indica dedicarse a los desarrollos a medida de este tipo de sistemas.

Aunque en el cuestionario se referencian ocho entidades como desarrolladoras de productos en esta área, ninguna hace referencia a productos desarrollados y tan solo una entidad hace referencia a la integración de productos de terceros. Así pues, probablemente se trata de entidades con potencial para desarrollar estas capacidades pero que aún no han desarrollado productos específicos.

Análisis de redes sociales

Esta subcapacidad facilita la comprensión de una comunidad mediante el mapeo de las relaciones que las conectan como una red para luego tratar de extraer individuos clave, grupos dentro de la red (componentes) o asociaciones entre los individuos (personas, contenido, tecnologías).

Los datos recogidos en la pregunta *33. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Análisis de redes sociales**, se muestran en la siguiente figura:

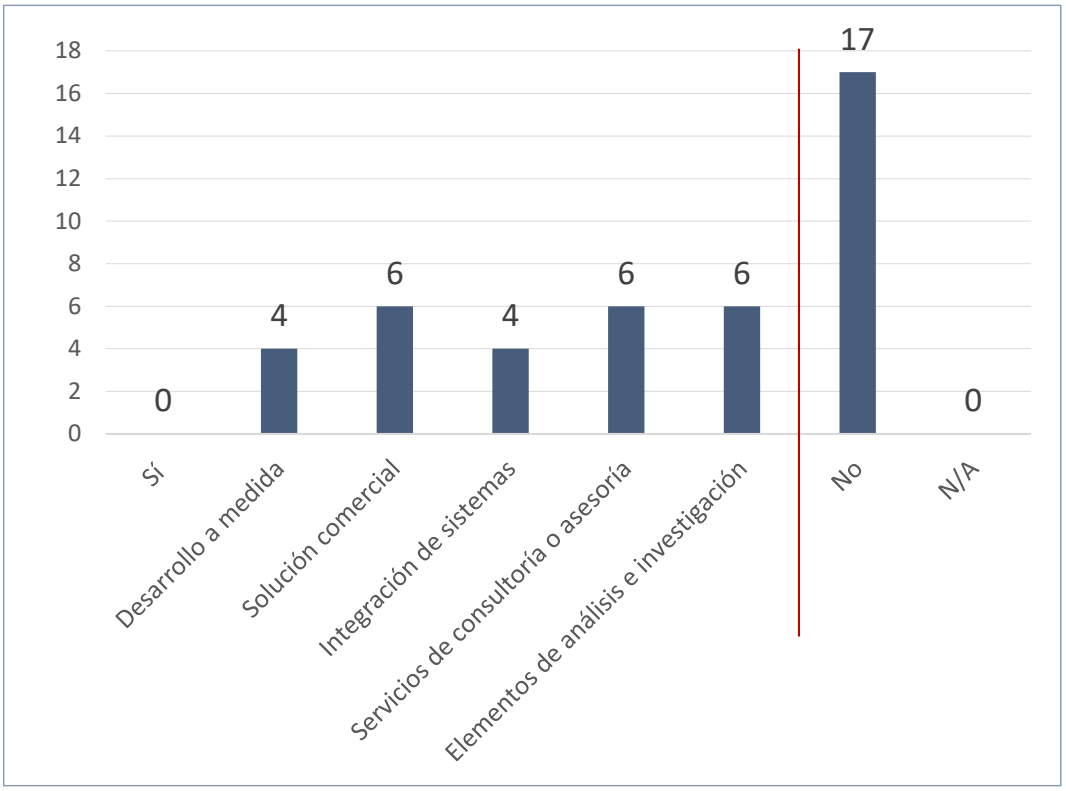


Figura 66. P33: Datos Análisis de redes sociales

La representación gráfica de los datos positivos se muestra en la siguiente figura:

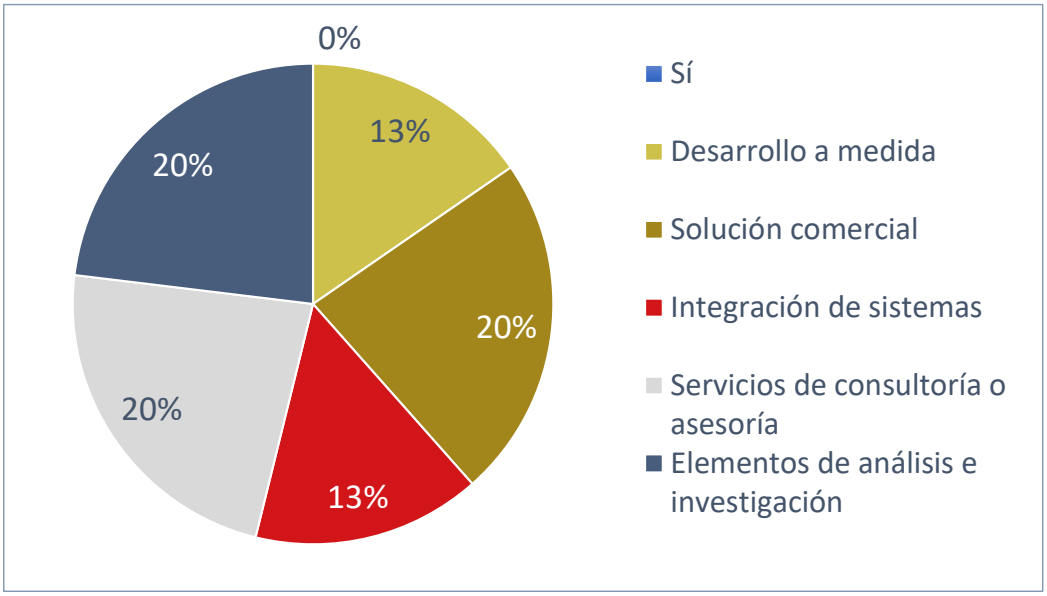


Figura 67. P33: Gráfico. Análisis de redes sociales

La mayoría de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de análisis de redes sociales. De las entidades que ofrecen estos servicios, destaca que la quinta parte indica que dispone de una solución comercial, realiza servicios de consultoría o asesoría o trabajos de análisis e investigación. Finalmente, las actividades a las que se dedica una minoría de las entidades son los desarrollos a medida de este tipo de sistemas y la Integración de sistemas relacionados con esta capacidad.

Respecto a esta capacidad hay algunas entidades que indican que tienen capacidad para realizar este tipo de actividades para consumo interno y otras que la proporcionan como servicio a sus clientes.

Al menos una alguna entidad especializada en esta parte de la inteligencia de fuentes abiertas (OSINT) con productos propios[20].

[20] Como FS ENTIDADES.

Gestor de *feeds* de inteligencia de pago y proveedores de datos

Esta subcapacidad proporciona una lista de indicadores de compromiso (IoC) que incluye URL maliciosas, *hashes* de *malware* y direcciones de correo electrónico e IP maliciosas relacionadas con ataques conocidos y validados. La obtención de esta información actualizada sobre ciberamenazas mejora la capacidad de identificación temprana y respuesta a amenazas sofisticadas.

Los datos recogidos en la pregunta *34. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Gestor de** feeds **de inteligencia de pago y proveedores de datos**, se muestran en la siguiente figura:

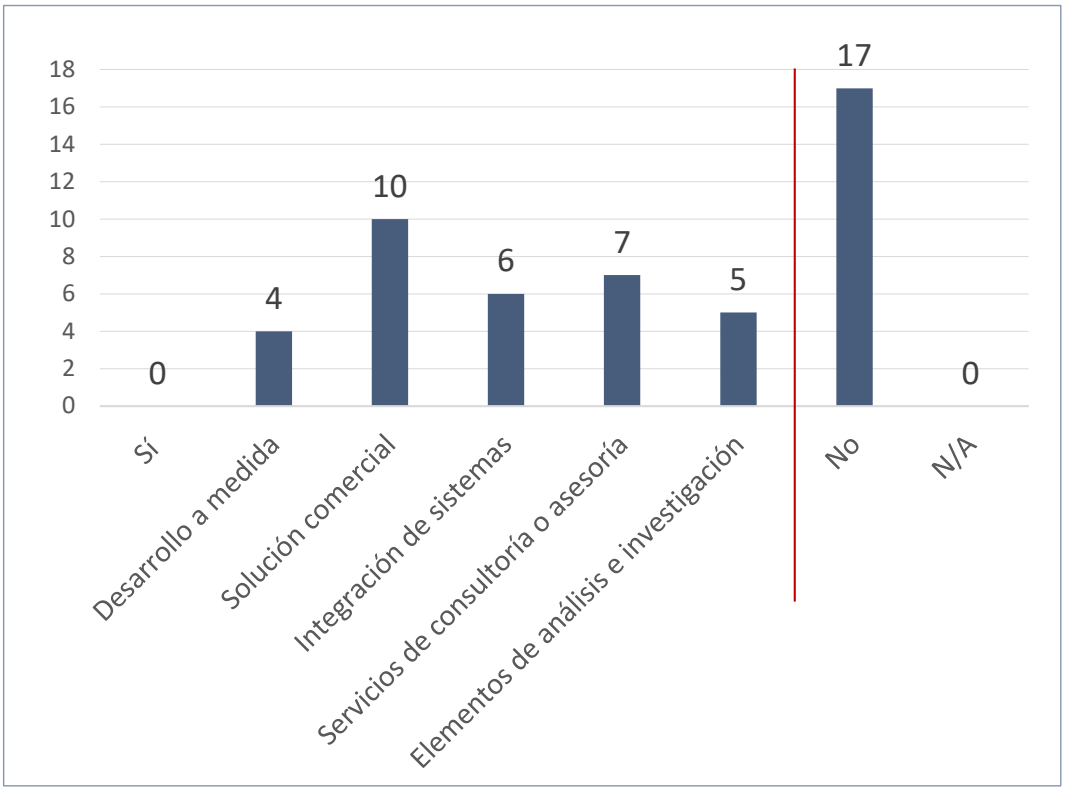


Figura 68. P34: Datos Gestor de feeds de inteligencia de pago y proveedores de datos

La representación gráfica de los datos positivos se muestra en la siguiente figura:

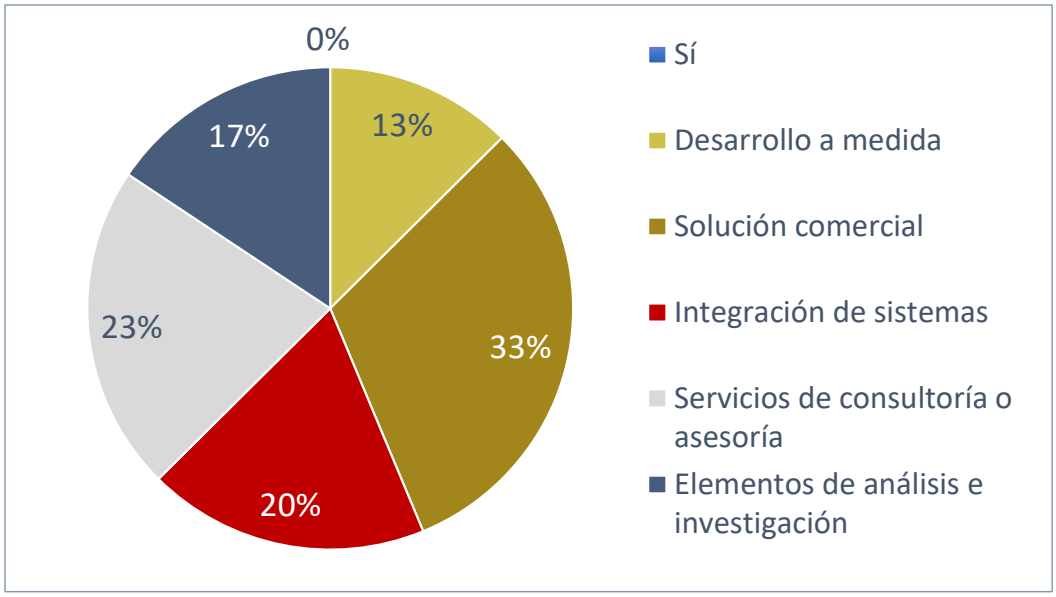


Figura 69. P34: Gráfico. Gestor de feeds de inteligencia de pago y proveedores de datos

Más de la mitad de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de gestión de *feeds* de inteligencia de pago y proveedores de datos. De las entidades que ofrecen estos servicios, destaca que un tercio indica que dispone de una solución comercial. La siguiente actividad relacionada con esta capacidad a la que se dedica un cuarto de las entidades son los servicios de consultoría o asesoría, seguida por una quinta parte de la Integración de sistemas. Finalmente, las actividades menos citadas son los trabajos de análisis e investigación y los desarrollos a medida de este tipo de sistemas.

Con respecto a esta capacidad, algunas entidades hacen mención únicamente a la integración o consumo de *feeds* de inteligencia de pago y proveedores de datos en sus herramientas o desarrollos.

Anonimización

Esta subcapacidad permite la navegación web anónima a través de servidores proxy, redes privadas virtuales y otros programas de anonimato para evitar dejar rastros en la red, ocultando el origen y el destino de la información.

Los datos recogidos en la pregunta *35. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Anonimización**, se muestran en la siguiente figura:

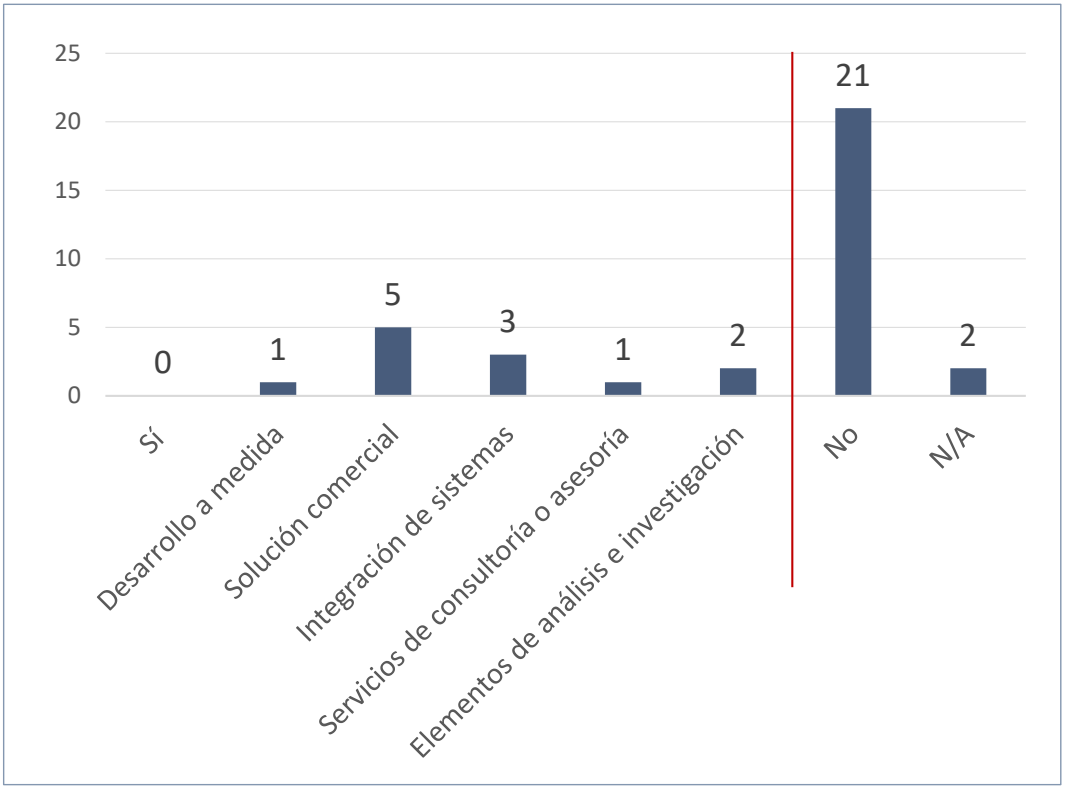


Figura 70. P35: Datos Anonimización

La representación gráfica de los datos positivos se muestra en la siguiente figura:

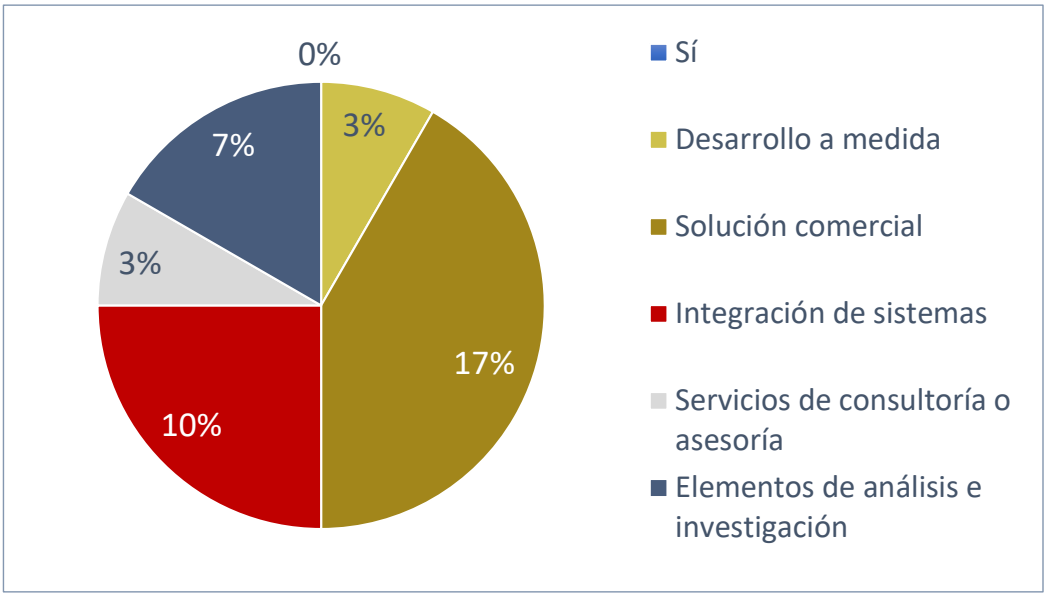


Figura 71. P35: Gráfico. Anonimización

La mayoría de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de anonimización. De las entidades que ofrecen estos servicios, destaca que, como máximo valor, un quinto indica que dispone de una aolución comercial, seguida por las actividades de Integración de sistemas y la realización de trabajos de análisis e investigación. Finalmente, una pequeña parte indica dedicarse a los servicios de consultoría o asesoría y los desarrollos a medida de este tipo de sistemas.

Respecto a esta capacidad, hay una entidad que indica que en sus desarrollos incorpora una capa de anonimización para garantizar la confidencialidad de las operaciones. Esta capacidad, quizás por ser una necesidad operativa más específica en el ámbito de las FF.AA., es menos común en el ámbito civil y, por lo tanto, pendiente de desarrollar.

Generación de avatares e identidades digitales

Esta subcapacidad permite la creación de avatares (identidad virtual de un usuario que lo representa en el ciberespacio) e identidades digitales, de forma autónoma, con perfiles adaptados a los ámbitos o sectores de interés de los analistas.

Los datos recogidos en la pregunta *36. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Generación de avatares e identidades digitales**, se muestran en la siguiente figura:

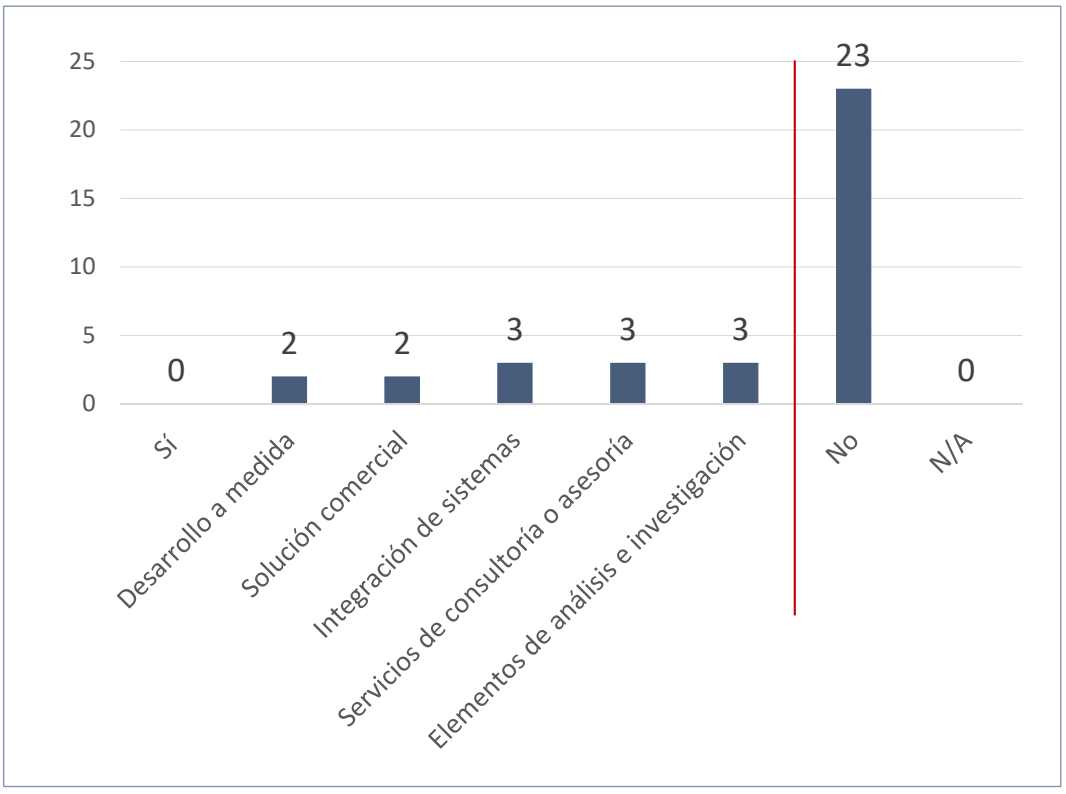


Figura 72. P36: Datos Generación de avatares e identidades digitales

La representación gráfica de los datos positivos se muestra en la siguiente figura:

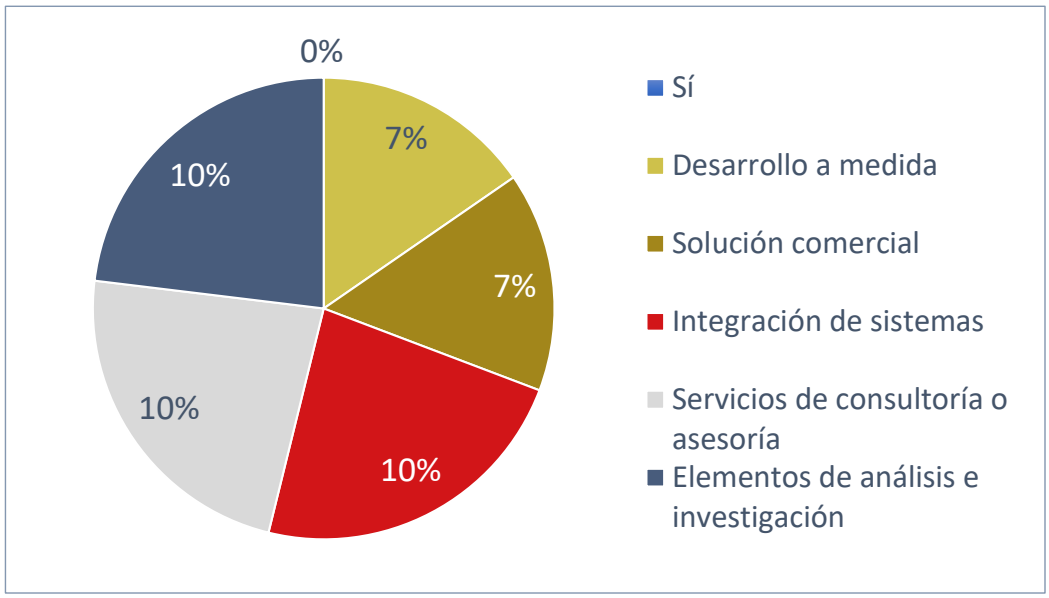


Figura 73. P36: Gráfico. Generación de avatares e identidades digitales

La mayoría de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de generación de avatares e identidades digitales. De las entidades que ofrecen estos servicios, destaca que la décima parte indica que realiza trabajos de Integración de sistemas, de servicios de consultoría o asesoría y de análisis e investigación. Finalmente, las actividades menos citadas son los desarrollos a medida y la disposición de una solución comercial de este tipo de sistemas.

Respecto a esta capacidad, no han existido comentarios por parte de las entidades encuestadas, quizás por tratarse de una capacidad que es muy específica de las FF.AA. y no tan empleada en el ámbito civil. Por tanto, es probable que sea un área en el que se requiera una potenciación del desarrollo específico nacional.

6.4 Capacidad de respuesta

La finalidad de esta capacidad es lograr es lograr un efecto sobre los activos del adversario en el ciberespacio o a través de él, por medio de la intrusión, manipulación, denegación, interrupción, degradación o destrucción de dispositivos, sistemas o la información que estos almacenan o manejan.

Esta capacidad puede desglosarse siguiendo las tácticas, técnicas y procedimientos de MITRE ATT@CK[21] en **quince subcapacidades**:

Gestión de recursos para operaciones de respuesta

Esta capacidad permite crear, adquirir o comprometer recursos, como infraestructura (dominios, DNS, VPS, servidores, *botnet*...), cuentas, certificados o *malware* (*payloads*, *exploits*...) que puedan ser utilizados para apoyar los objetivos.

Los datos recogidos en la pregunta *37. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Gestión de recursos para operaciones de respuesta**, se muestran en la siguiente figura:

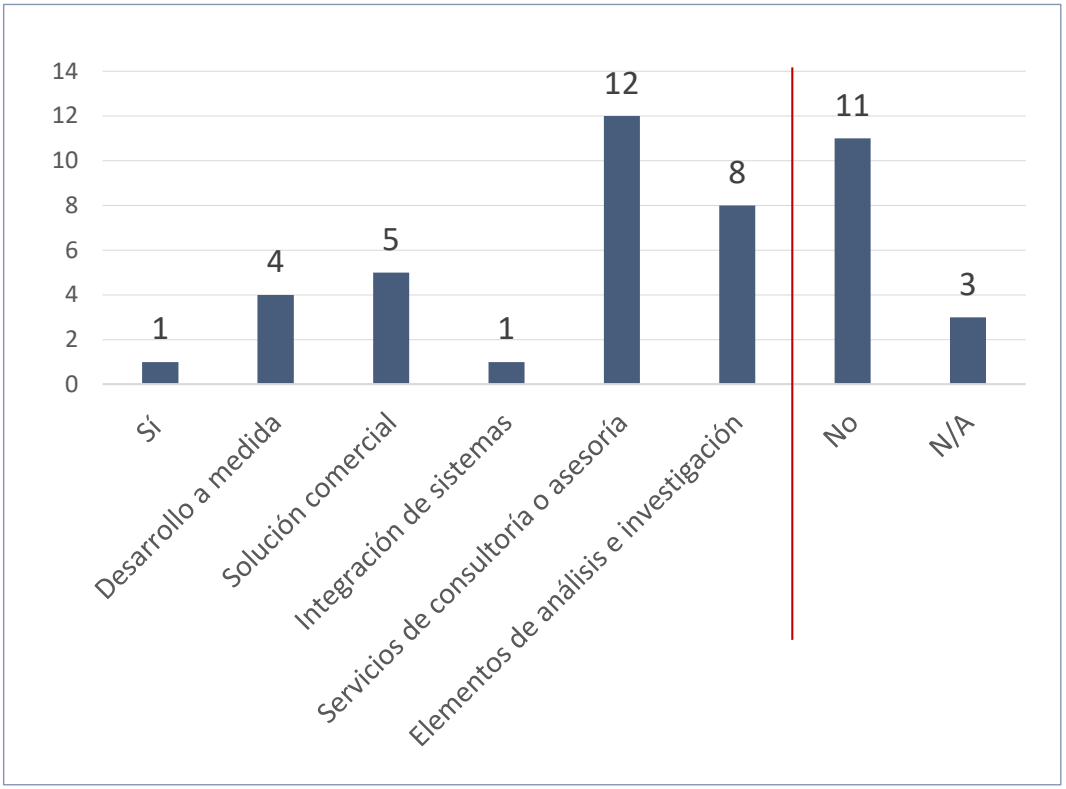


Figura 74. P37: Datos gestión de recursos para operaciones de respuesta

[21] https://attack.mitre.org/

La representación gráfica de los datos positivos se muestra en la siguiente figura:

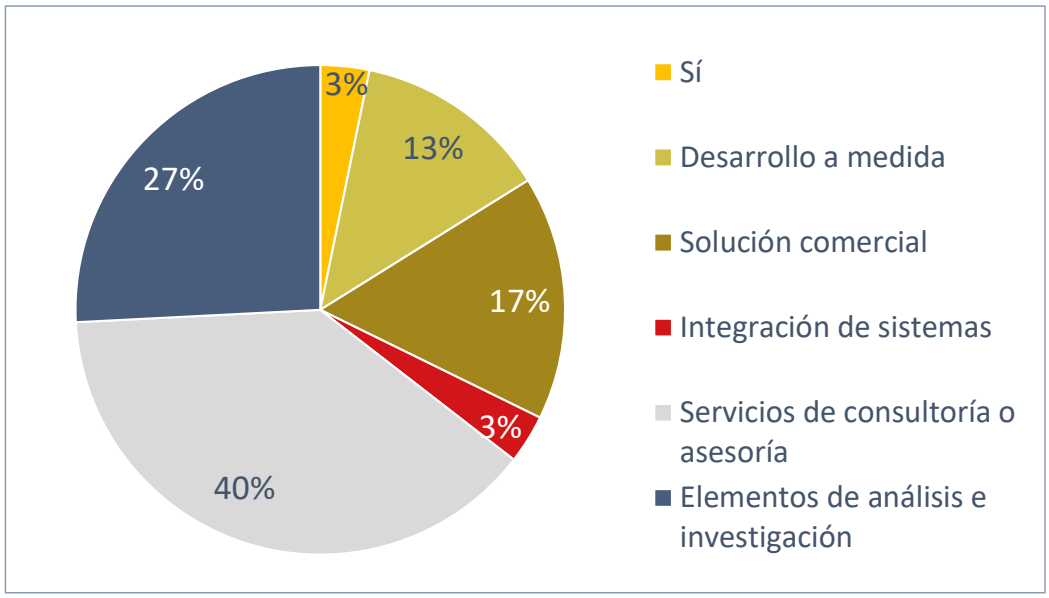


Figura 75. P37: Gráfico. Gestión de recursos para operaciones de respuesta

Casi la mitad de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de gestión de recursos para operaciones de respuesta. De las entidades que ofrecen estos servicios, destaca que casi la mitad indica que realiza servicios de consultoría o asesoría. Las siguientes actividades relacionadas con esta capacidad a las que se dedica una cuarta parte de las entidades son los trabajos de análisis e investigación y minoritariamente a la disposición de una solución comercial, los desarrollos a medida y los trabajos de Integración de sistemas.

Hay diversas entidades que indican que disponen de equipos de *hacking* ético o de *red team* para consumo interno o como servicio proporcionado. Pero solo algunas indican que desarrollan capacidades en esta área. Quizás esta área de capacidades tenga una de las menores posibilidades de desarrollo en el futuro ya que es muy específica de las FF.AA., y aunque pueda tener cierto empleo para equipos de *red team* no es un nicho muy amplio en el ámbito civil.

Acceso inicial

Esta subcapacidad permite emplear distintos vectores de entrada para obtener el acceso inicial a una red. Dentro de este apartado, podemos encontrar diferentes tipos según su funcionalidad: compromiso por navegación, explotación de aplicaciones públicas, gestor de servicios remotos externos, gestor de hardware añadido, soporte a la ingeniería social o gestor del compromiso de la cadena de suministro.

Los datos recogidos en la pregunta *38. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Acceso inicial**, se muestran en la siguiente figura:

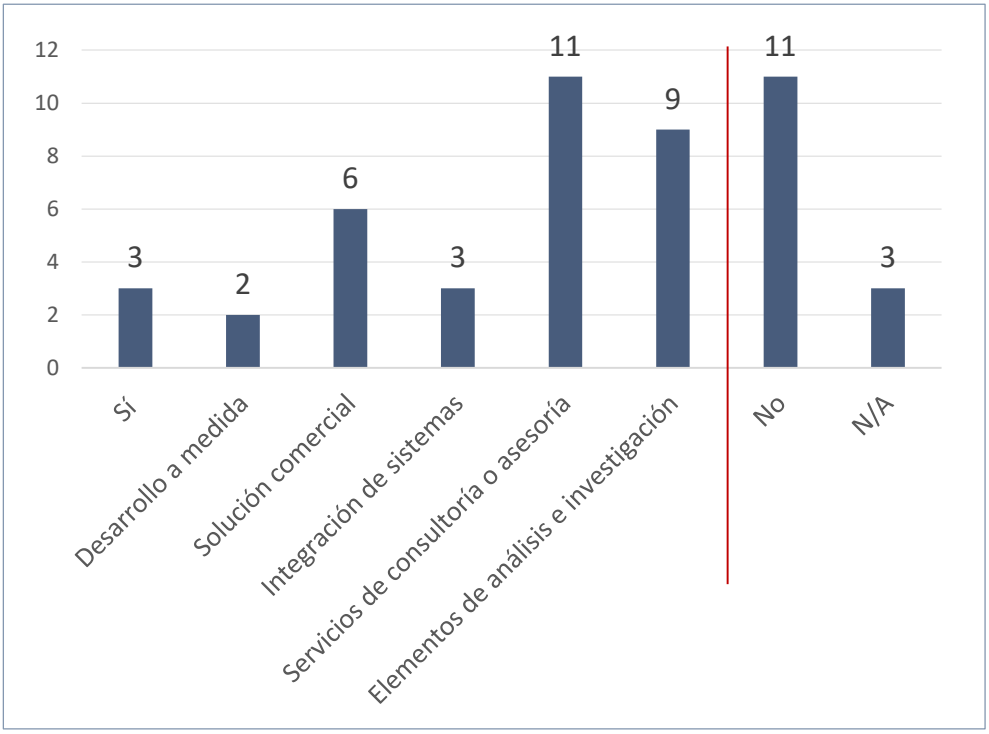


Figura 76. P38: Datos Acceso inicial

La representación gráfica de los datos positivos se muestra en la siguiente figura:

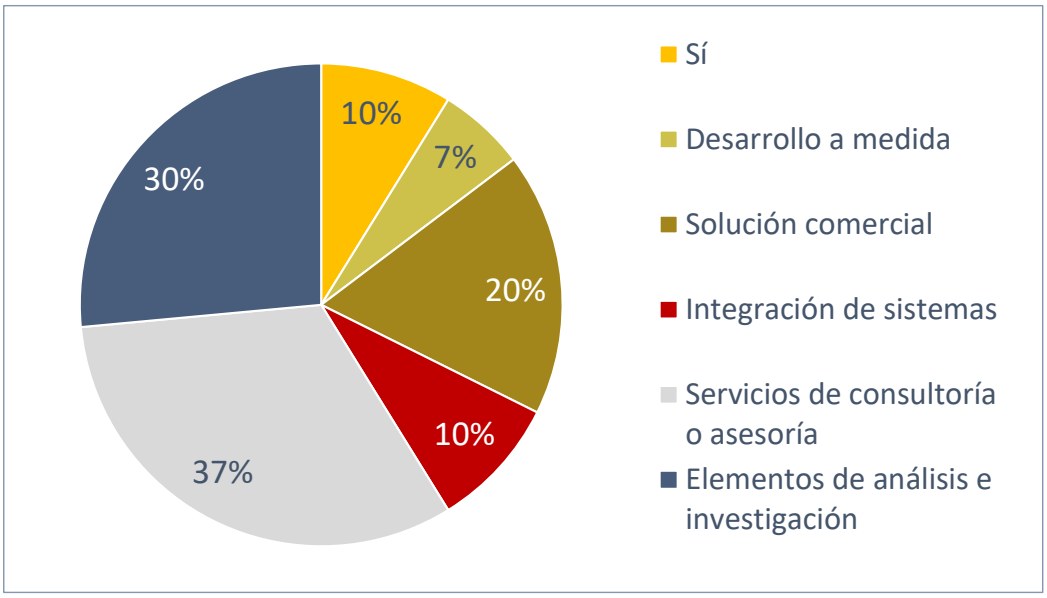


Figura 77. P38: Gráfico. Acceso inicial

Casi la mitad de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de acceso inicial. De las entidades que ofrecen estos servicios, destaca que más de un tercio indica que realiza servicios de consultoría o asesoría. Las siguientes actividades relacionadas con esta capacidad a las que se dedica casi un tercio de las entidades son los trabajos de análisis e investigación y la disposición de una solución comercial. Finalmente, las actividades menos citadas son los trabajos de integración de sistemas y los desarrollos a medida.

La mayoría de las respuestas indican que disponen de capacidades de *red team* o de auditorías, capaces de realizar acciones de intrusión aprovechando vulnerabilidades de sistemas, pero solo una entidad hace referencia a llevar a cabo desarrollos, elaboración de *software* o herramientas específicos en esta área, innovando y desarrollando nuevos vectores de intrusión.

Ejecución

Esta subcapacidad realiza el ataque mediante técnicas que permitan la ejecución ejecución de código en un sistema local o remoto. Dentro de este apartado, podemos encontrar diferentes tipos según su funcionalidad: intérprete de comandos y *scripts*, gestor de administración de contenedores, explotación para la ejecución de clientes, gestor de tareas o trabajos programados, gestor de módulos compartidos y herramientas de despliegue de software o gestor de servicios del sistema.

Los datos recogidos en la pregunta *39. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Ejecución**, se muestran en la siguiente figura:

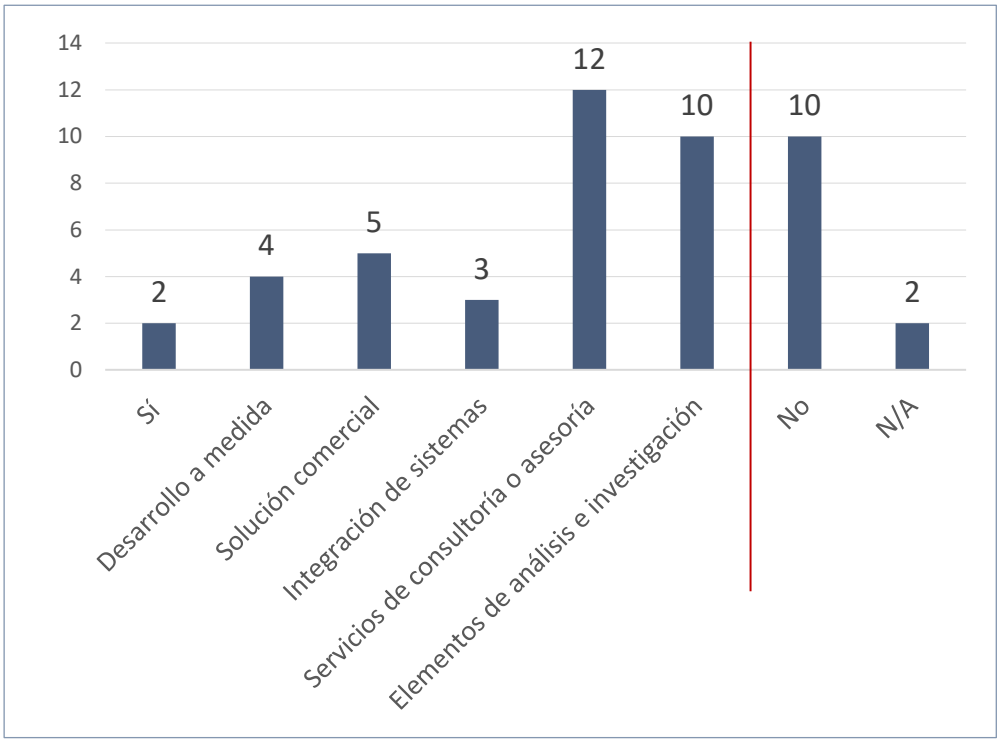


Figura 78. P39: Datos Ejecución

La representación gráfica de los datos positivos se muestra en la siguiente figura:

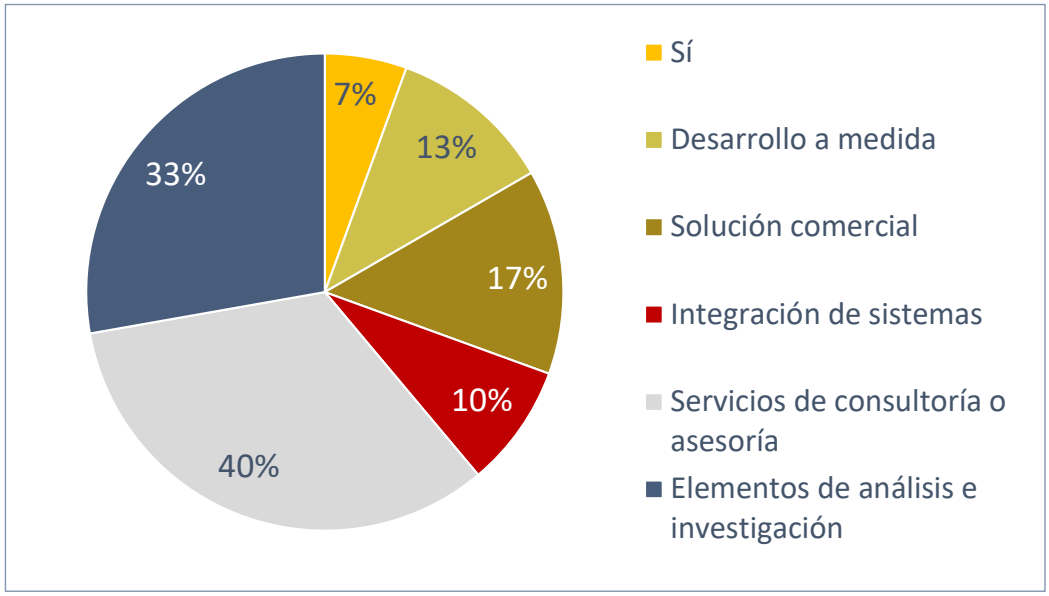


Figura 79. P39: Gráfico. Ejecución

Casi la mitad de las entidades declaran que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de ejecución. De las entidades que ofrecen estos servicios, casi la mitad indica que realiza servicios de consultoría o asesoría. Las siguientes actividades relacionadas con esta capacidad a las que se dedica un tercio de las entidades son los trabajos de análisis e investigación. Finalmente, las actividades menos citadas son son la disposición de una solución comercial, los desarrollos a medida y los trabajos de Integración de sistemas.

Existen tres entidades que indican que disponen de algún desarrollo a medida muy específico en esta área. Estos desarrollos permiten la posibilidad de ejecutar código remoto en entornos *cloud*, tomar el control remoto de dispositivos interceptados o extraer información de forma invisible para evitar los sistemas defensivos. Otra posibilidad que aportan estos desarrollos es el despliegue de sistemas de ejecución remota de comandos sobre entornos comprometidos con herramientas propias. El uso de tecnología de tunelización minimiza la posibilidad de ser detectados así como conservar la dirección desde un sistema C&C (mando y control) permite la ejecución de comandos sobre la infraestructura comprometida.

Persistencia

Esta subcapacidad permite mantener el acceso a los sistemas comprometidos, a pesar de los reinicios, cambios de credenciales y otras interrupciones que podrían cortar su acceso. Dentro de este apartado podemos encontrar diferentes tipos según su funcionalidad: creación y manipulación de cuentas, ejecución de arranque o inicio de sesión automático, gestor de las extensiones del navegador, ejecución activada por eventos, secuestro del flujo de ejecución, modificación del proceso de autenticación, gestor del prearranque del sistema operativo.

Los datos recogidos en la pregunta de la encuesta 40. *¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondiente a la subcapacidad de **Persistencia**, se muestran en la siguiente figura:

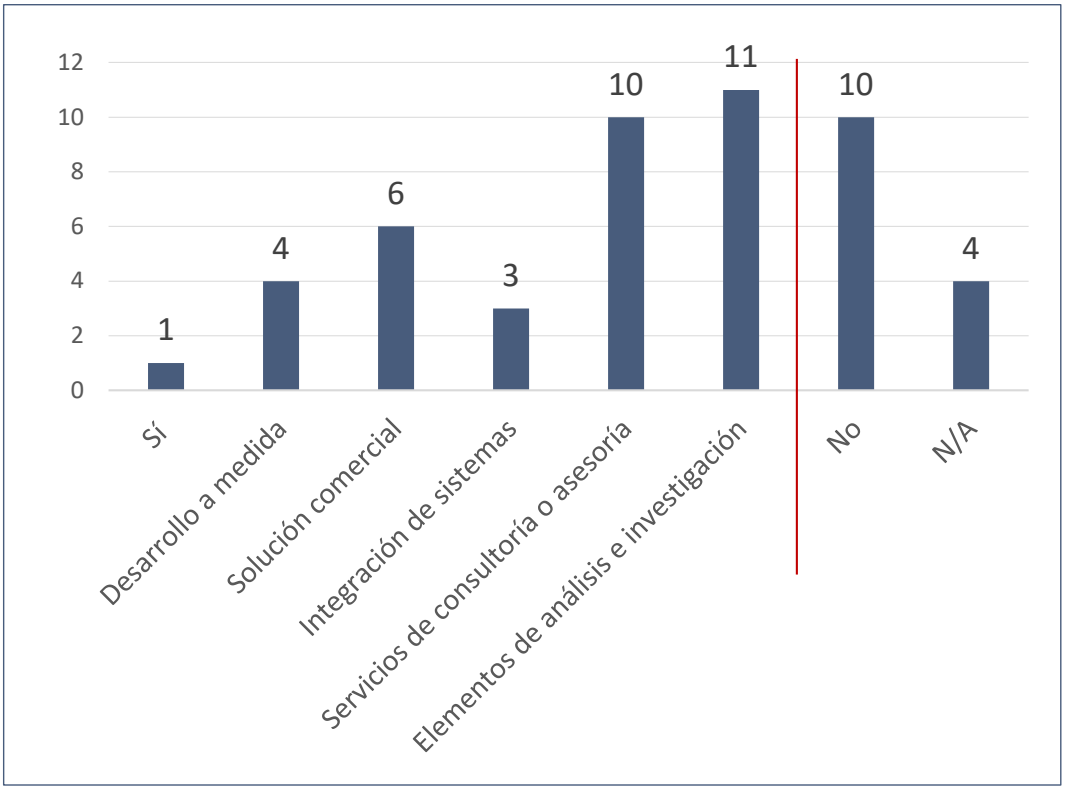


Figura 80. P40: Datos Persistencia

La representación gráfica de los datos positivos se muestra en la siguiente figura:

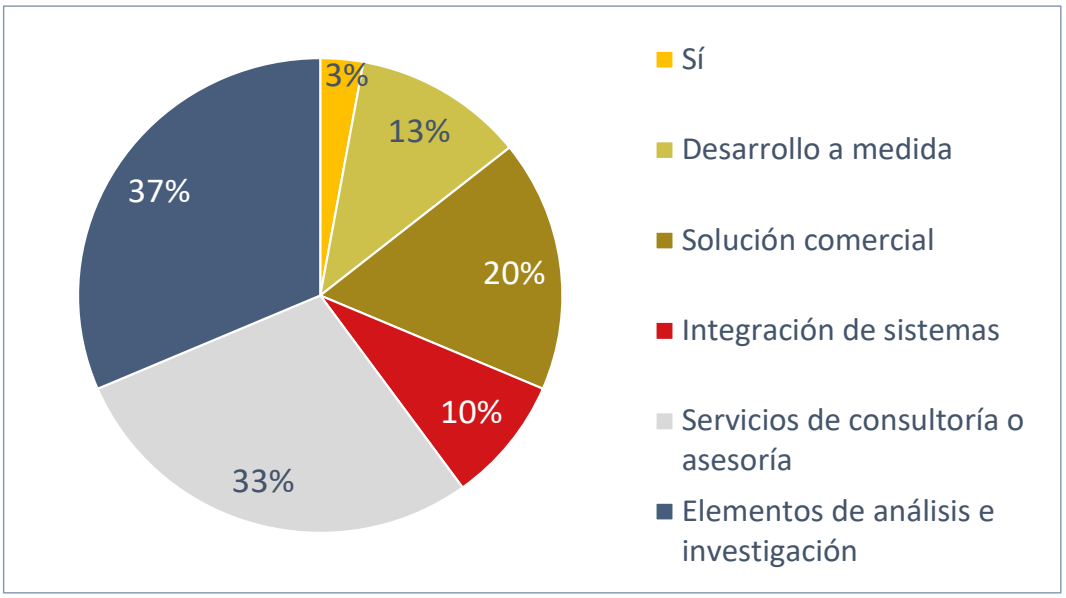


Figura 81. P40. Gráfico. Persistencia

Casi la mitad de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de persistencia. De las entidades que ofrecen estos servicios, destaca que más de un tercio indica que realiza trabajos de análisis e investigación y servicios de consultoría o asesoría. La siguiente actividad relacionada con esta capacidad a las que más se dedican las entidades es la disposición de una solución comercial. Finalmente, las actividades menos citadas son los desarrollos a medida y los trabajos de Integración de sistemas.

Existen dos entidades que indican que llevan a cabo algún desarrollo a medida sobre tecnología y técnicas de persistencia de sesión en entornos *cloud* y de *endpoint*. Existe una tercera entidad que indica que dispone de técnicas de persistencia, tanto a nivel de red como a nivel de usuario, con un desarrollo propio que permite actuar como una APT minimizando la posibilidad de ser detectado y dispone también de un *framework* propio diseñado para la realización de implantes en ficheros o memoria.

Escalada de privilegios

Esta subcapacidad se utiliza para incrementar los privilegios de administración sobre la red objetivo. Dentro de este apartado podemos encontrar diferentes tipos según su funcionalidad: control de elevación de permisos, manipulación de *tokens* de acceso, modificación de la política de dominio, secuestro del flujo de ejecución o inyección de procesos.

Los datos recogidos en la pregunta 41. *¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Escalada de privilegios**, se muestran en la siguiente figura:

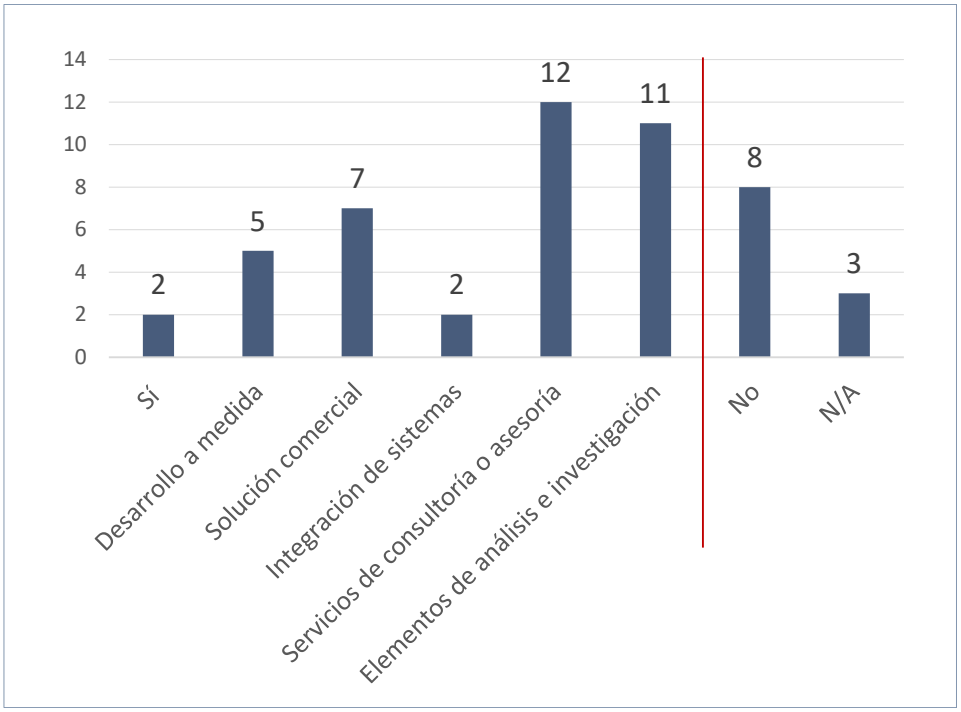


Figura 82. P41: Escalada de privilegios

La representación gráfica de los datos positivos se muestra en la siguiente figura:

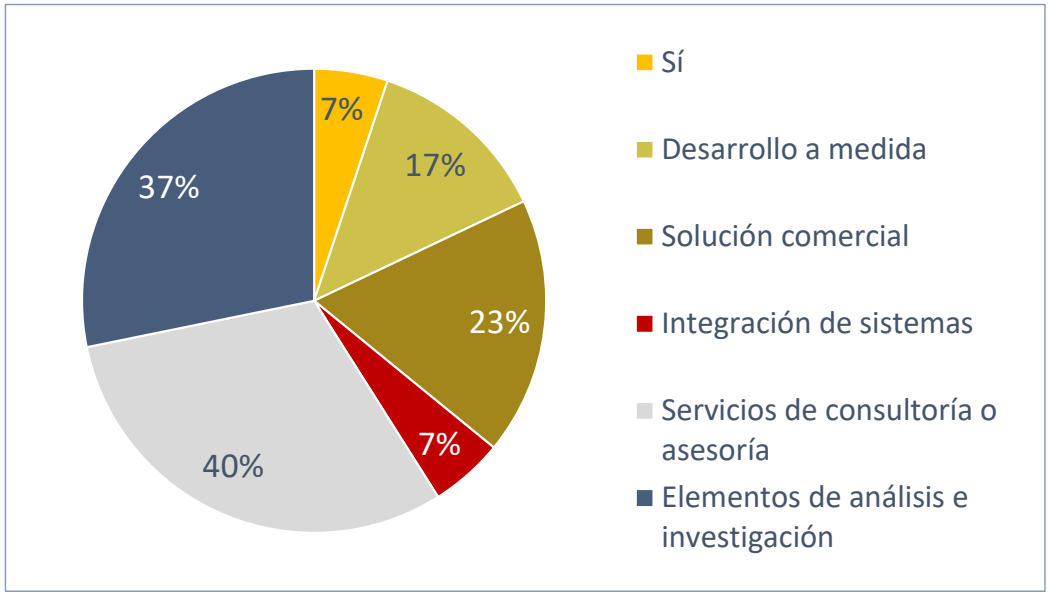


Figura 83. P41: Gráfico. Escalada de privilegios

Casi un tercio de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de escalada de privilegios. De las entidades que ofrecen estos servicios, destaca que casi la mitad indica que realiza servicios de consultoría o asesoría. Las siguientes actividades relacionadas con esta capacidad a las que se dedica un tercio de las entidades son los trabajos de análisis e investigación y la disposición de una solución comercial. Finalmente, las actividades menos citadas son los desarrollos a medida y los trabajos de integración de sistemas.

Existen dos entidades que expresan la capacidad de innovación y desarrollo a medida de técnicas y *payloads* que buscan la posibilidad de escalar privilegios dentro de infraestructuras *cloud*, desarrollar troyanos con *payloads* para realizar ataques laterales y técnicas de escalado de privilegios. Además, permiten el desarrollo de *exploits* para la explotación de debilidades de tipo *zero-day* y la búsqueda de nuevas formas de elevación de privilegios para las cuales no existe información previa.

Evasión de defensas

La finalidad de esta subcapacidad es evitar es evitar la detección a lo largo de la acción ofensiva. Dentro de este apartado, podemos encontrar diferentes tipos según su funcionalidad: ofuscación de artefactos, archivos e información, acceso directo al volumen, explotación para evasión de defensas, modificación de permisos de archivos y directorios, deterioro de las defensas, eliminación de indicadores de intrusión en el host, enmascaramiento de capacidades ofensivas o debilitado del cifrado.

Los datos recogidos en la pregunta 42. *¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Evasión de defensas**, se muestran en la siguiente figura:

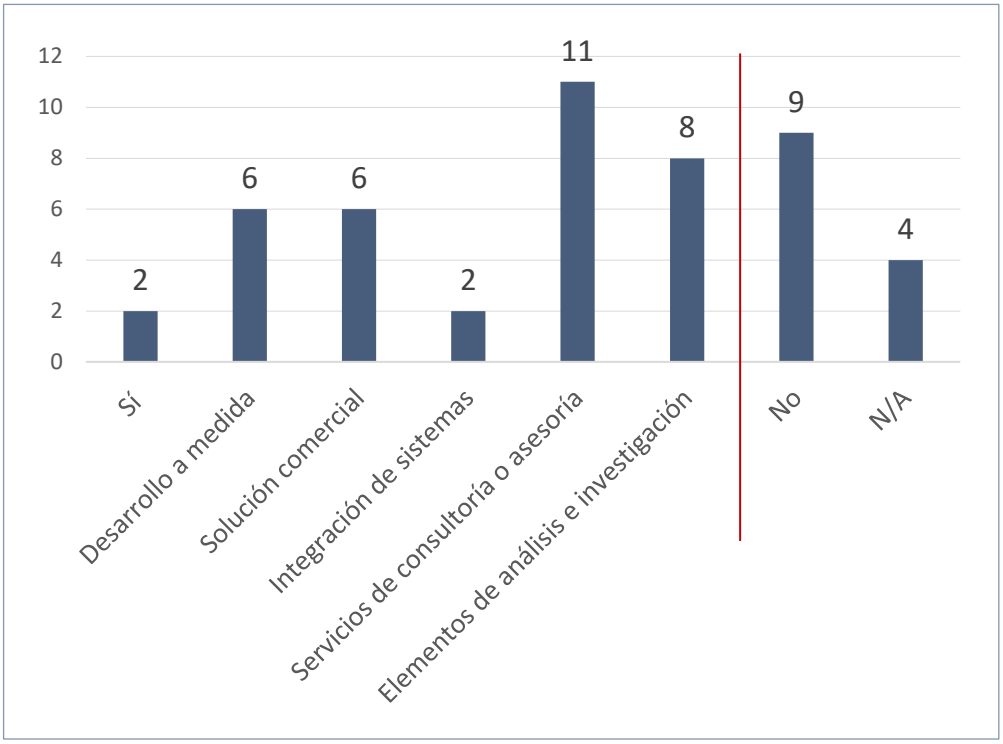


Figura 82. P42: Datos Evasión de defensas

La representación gráfica de los datos positivos se muestra en la siguiente figura:

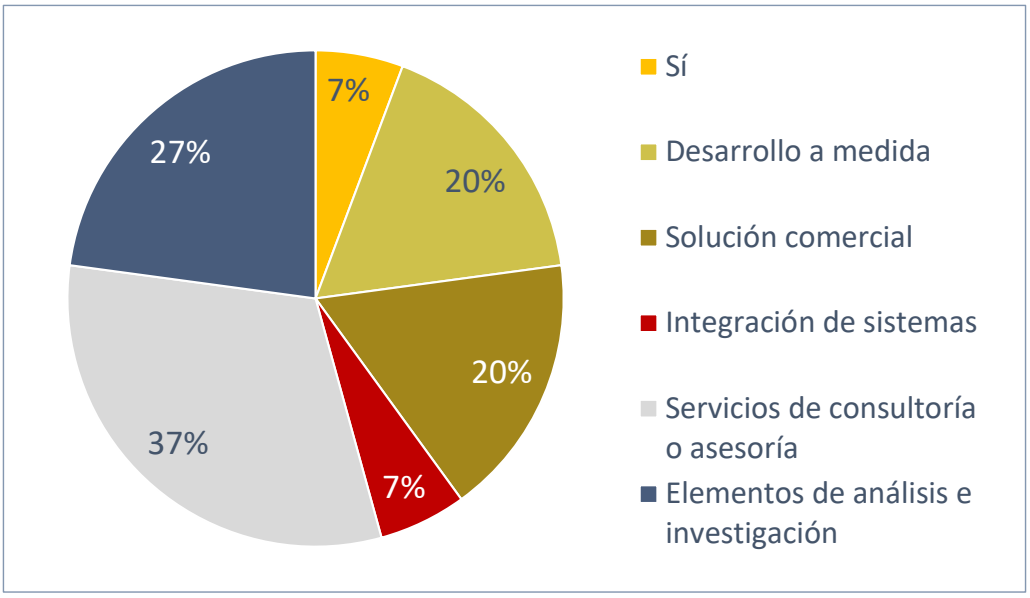


Figura 82. P42: Gráfico. Evasión de defensas

Casi la mitad de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de evasión de defensas. De las entidades que ofrecen estos servicios, destaca que más de un tercio indica que realiza servicios de consultoría o asesoría y más de un cuarto trabajos de análisis e investigación. Las siguientes actividades relacionadas con esta capacidad a las que más se dedican las entidades son la disposición de una solución comercial y los desarrollos a medida. Finalmente, la actividad menos citada son los trabajos de integración de sistemas.

Existen tres entidades que manifiestan la capacidad de llevar a cabo desarrollos a medida para la evasión de sistemas de defensa, el uso de técnicas de infección y de exfiltración de información así como el desarrollo de *TTP* específicas que pasen desapercibidas a las principales tecnologías defensivas y de *threat hunting*.

Acceso a credenciales

La finalidad de esta subcapacidad es obtener credenciales de acceso a los sistemas objetivo. Las técnicas utilizadas para obtener credenciales incluyen el *keylogging* o el *dumping* de credenciales. Dentro de este apartado podemos encontrar diferentes tipos, según su funcionalidad: fuerza bruta y criptoanálisis, gestión de las credenciales de los almacenes de contraseñas, falsificación de credenciales web, captura de entradas, escaneo de red y ataque *man-in-the-middle* o robo de *tokens* de acceso.

Los datos recogidos en la pregunta 43. *¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Acceso a credenciales**, se muestran en la siguiente figura:

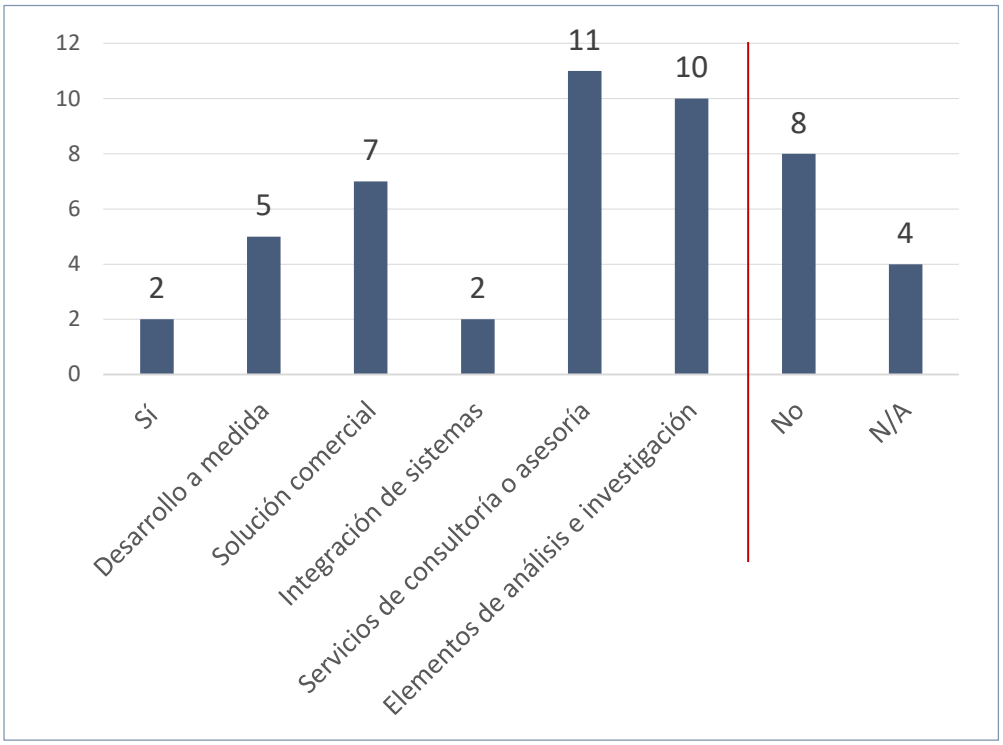


Figura 86. P43: Datos Acceso a credenciales

La representación gráfica de los datos positivos se muestra en la siguiente figura:

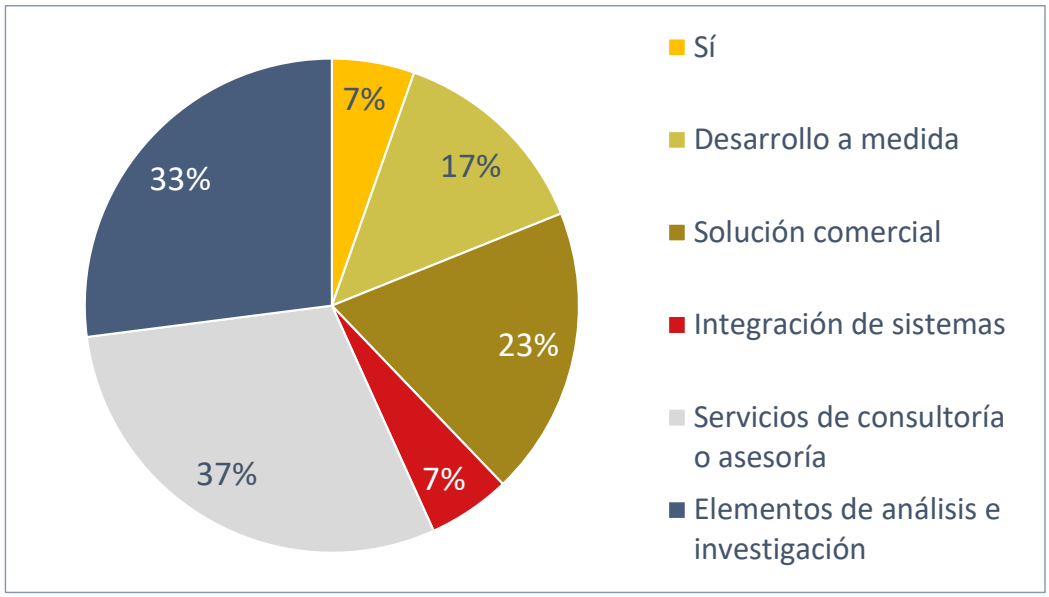


Figura 87. P43: Gráfico. Acceso a credenciales

Más de un tercio de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de acceso a credenciales. De las entidades que ofrecen estos servicios, destaca que más de un tercio indica que realiza servicios de consultoría o asesoría o trabajos de análisis e investigación. Las siguientes actividades relacionadas con esta capacidad a las que más se dedican las entidades son la disposición de una solución comercial y los desarrollos a medida. Finalmente, la actividad menos citada son los trabajos de integración de sistemas.

Existen tres entidades que indican que disponen de capacidad para llevar a cabo desarrollos a medida de acceso y captura de credenciales, desarrollo de *keyloggers* avanzados para ordenadores y teléfonos móviles, y técnicas de postexplotación y obtención de credenciales.

Descubrimiento

La finalidad de esta subcapacidad es apoyar el ataque con la obtención de información sobre los sistemas y la red interna del adversario, apoyando el ataque. Dentro de este tipo podemos encontrar diferentes grupos según su funcionalidad: descubrimiento de cuentas, descubrimiento de dominios de confianza, descubrimiento de archivos y directorios, escaneo de servicios y recursos compartidos de red, detección de dispositivos periféricos, descubrimiento de *software*, detección de la configuración de red o descubrimiento de la infraestructura y servicios de la nube.

Los datos recogidos en la pregunta 44*. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Descubrimiento**, se muestran en la siguiente figura:

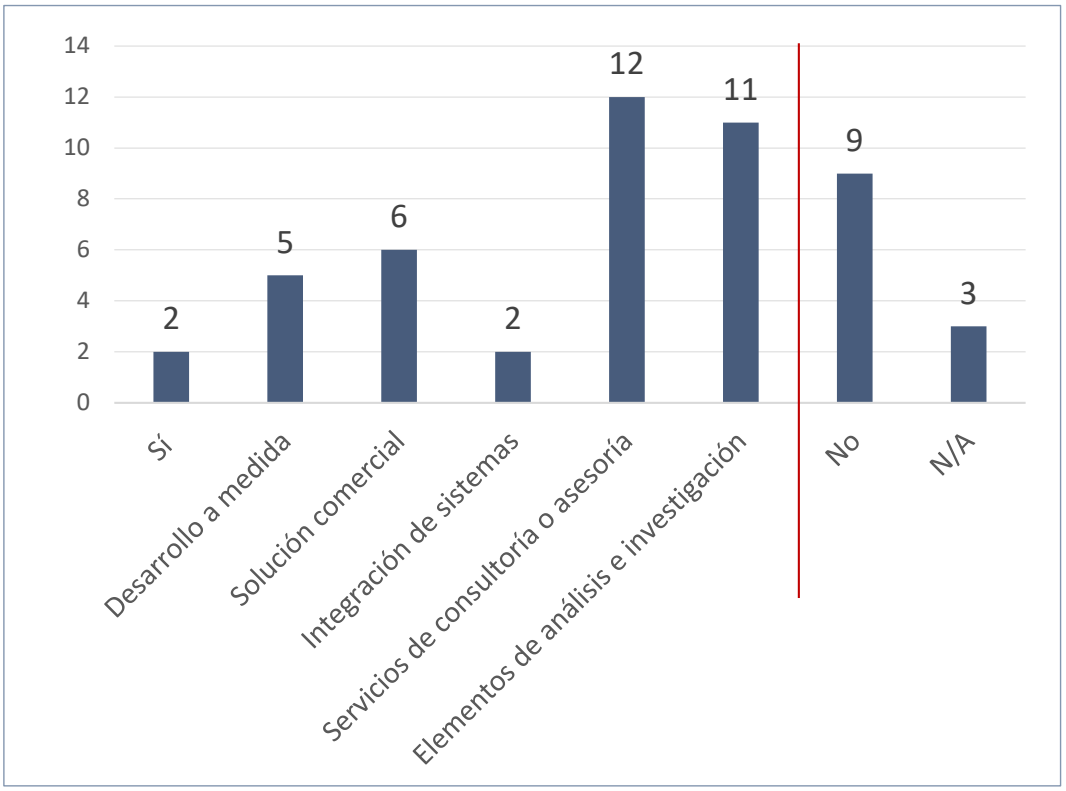


Figura 88. P44: Datos Descubrimiento

La representación gráfica de los datos positivos se muestra en la siguiente figura:

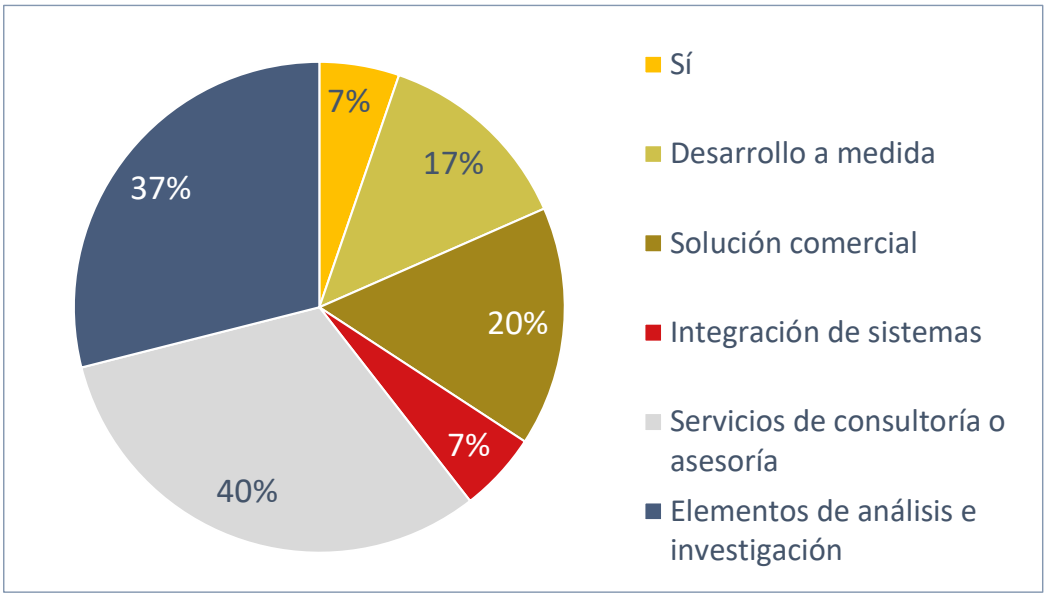


Figura 89. P44: Gráfico. Descubrimiento

Más de un tercio de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de descubrimiento. De las entidades que ofrecen estos servicios, destaca que casi la mitad indica que realiza servicios de consultoría o asesoría. Las siguientes actividades relacionadas con esta capacidad a las que más se dedican las entidades son los trabajos de análisis e investigación y la disposición de una solución comercial. Finalmente, las actividades menos citadas son los desarrollos a medida y los trabajos de integración de sistemas.

Existen dos entidades que indican que disponen de algunas funcionalidades en desarrollos a medida que persiguen el descubrimiento de activos dentro de una infraestructura, pero no llegan a indicar si se lleva a cabo de forma discreta y con medidas OPSEC (*Operations security*) .

Movimiento lateral

La finalidad de esta subcapacidad es pivotar a través de múltiples sistemas, dispositivos o cuentas para ganar acceso a un sistema adversario empleando herramientas propias de acceso remoto o utilizando credenciales legítimas junto con herramientas nativas de la red y del sistema operativo. Dentro de este tipo podemos encontrar diferentes grupos según su funcionalidad: transferencia lateral, secuestro de protocolos de gestión y acceso remoto o replicación a través de medios extraíbles.

Los datos recogidos en la pregunta 45. *¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Movimiento lateral**, se muestran en la siguiente figura:

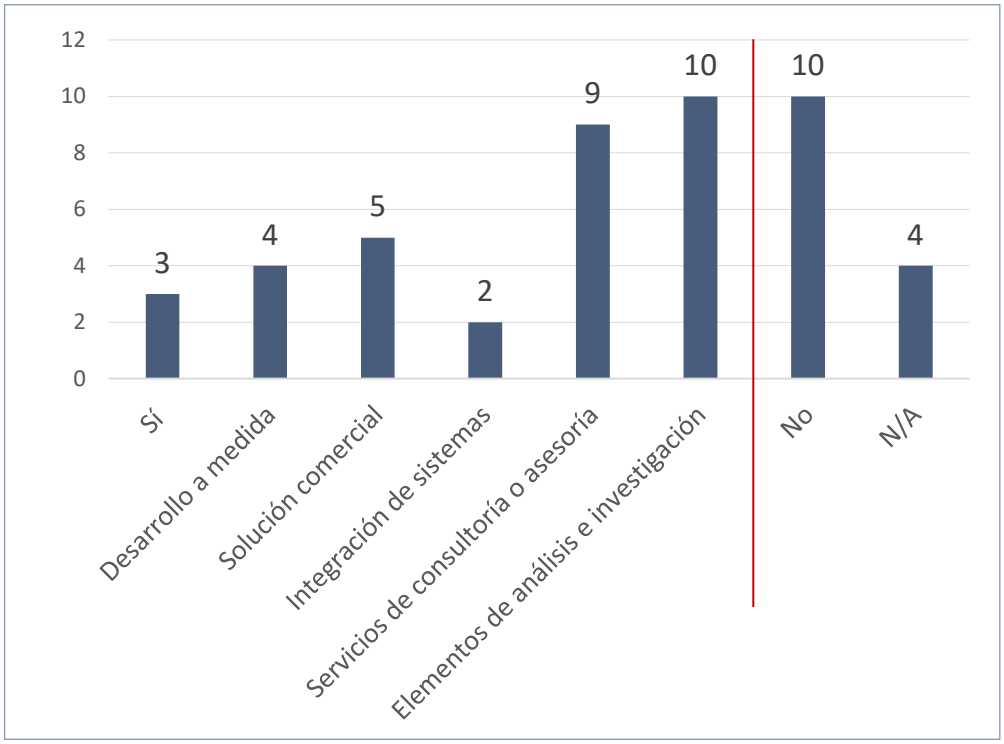


Figura 90. P45: Datos Movimiento lateral

La representación gráfica de los datos positivos se muestra en la siguiente figura:

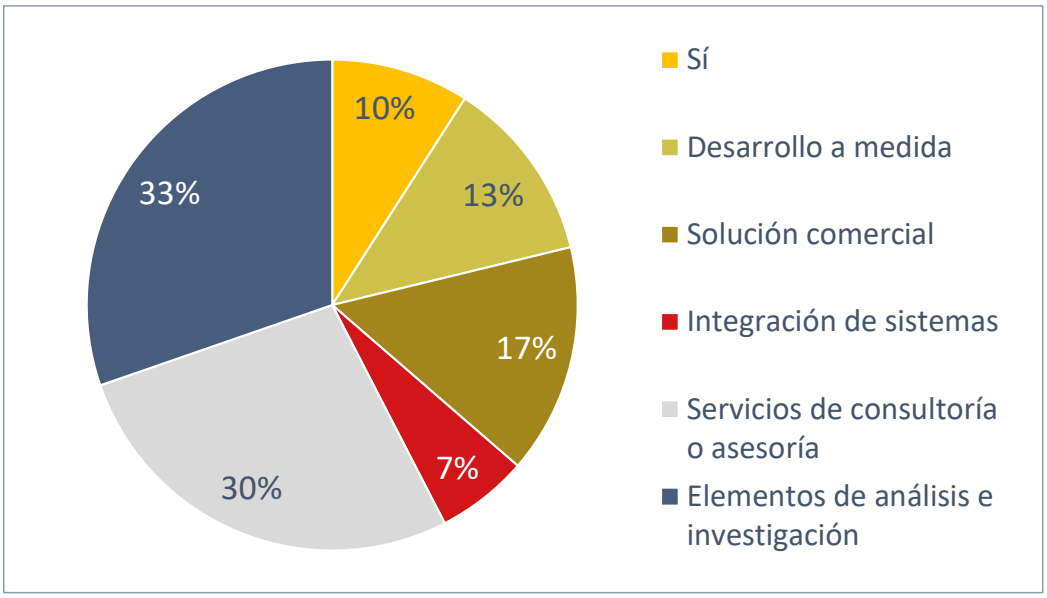


Figura 91. P45: Gráfico. Movimiento lateral

La mitad de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de movimiento lateral. De las entidades que ofrecen estos servicios, destaca que un tercio indica que realiza trabajos de análisis e investigación o servicios de consultoría o asesoría. Las siguientes actividades relacionadas con esta capacidad a las que más se dedican las entidades son la disposición de una solución comercial y los desarrollos a medida. Finalmente, la actividad menos citada son los trabajos de integración de sistemas.

Muchos entidades indican que dispone de equipos de *hacking* ético, capaces de realizar las diferentes fases de la *cyber killchain*, pero no de sus propios desarrollos específicos de por sí. En este caso solo una entidad indica explícitamente la capacidad de llevar a cabo desarrollos para movimiento lateral utilizando un *payload* específico.

Recogida

La finalidad de esta subcapacidad es la recolección es la recolección de información de interés (credenciales de acceso, documentos...) dentro de una red adversaria mediante búsquedas especializadas, captura de pantallas o la lectura de datos del teclado, entre otras. Dentro de este tipo podemos encontrar diferentes grupos según su funcionalidad: archivado de los datos recogidos, búsqueda de datos en repositorios de información, recogida de correo electrónico, captura de pantalla y vídeo, gestor de las credenciales de los almacenes de contraseñas, falsificación de credenciales web o captura de entradas.

Los datos recogidos en la pregunta 46. *¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Recogida**, se muestran en la siguiente figura:

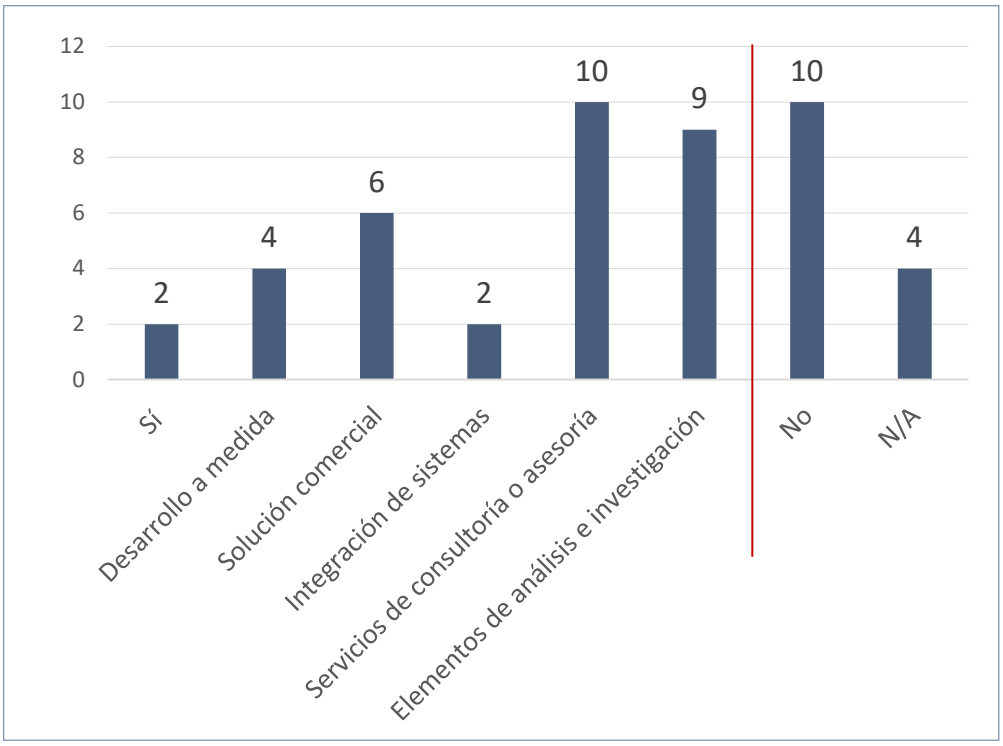


Figura 92. P46: Datos Recogida

La representación gráfica de los datos positivos se muestra en la siguiente figura:

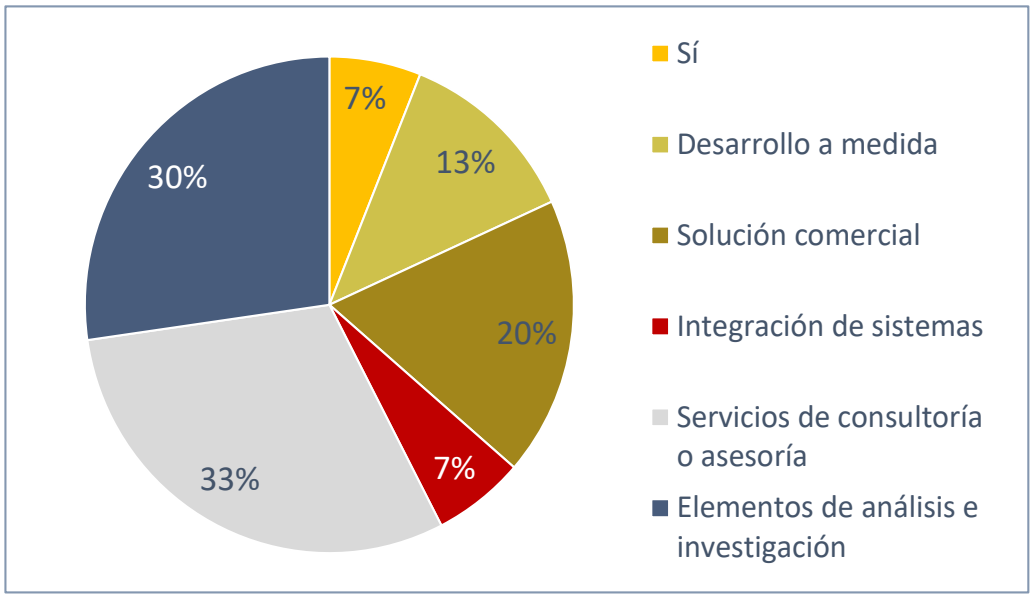


Figura 93. P46: Gráfico. Recogida

La mitad de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de recogida. De las entidades que ofrecen estos servicios, destaca que un tercio indica que realiza servicios de consultoría o asesoría o trabajos de análisis e investigación. Las siguientes actividades relacionadas con esta capacidad a las que más se dedican las entidades son la disposición de una solución comercial y los desarrollos a medida. Finalmente, la actividad menos citada son los trabajos de integración de sistemas.

Algunas entidades indican que sus equipos de *red team* llevan a cabo técnicas de postexplotación habituales de búsqueda de información sensible para avanzar hacia nuevos compromisos o en apoyo a servicios de inteligencia, pero ninguna indica explícitamente la capacidad de llevar a cabo desarrollos tecnológicos específicos.

Mando y control

La finalidad de esta subcapacidad es ejecutar el mando y control del ataque, enmascarado entre el tráfico legítimo para evitar la detección. Dentro de este apartado, podemos encontrar diferentes tipos según su funcionalidad: gestión de protocolo de la capa de aplicación, codificación de datos, resolución dinámica, cifrado del canal, transferencia de herramientas de entrada, gestión de protocolo de tunelización o herramientas de *proxy*.

Los datos recogidos en la pregunta 47. *¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Mando y control**, se muestran en la siguiente figura:

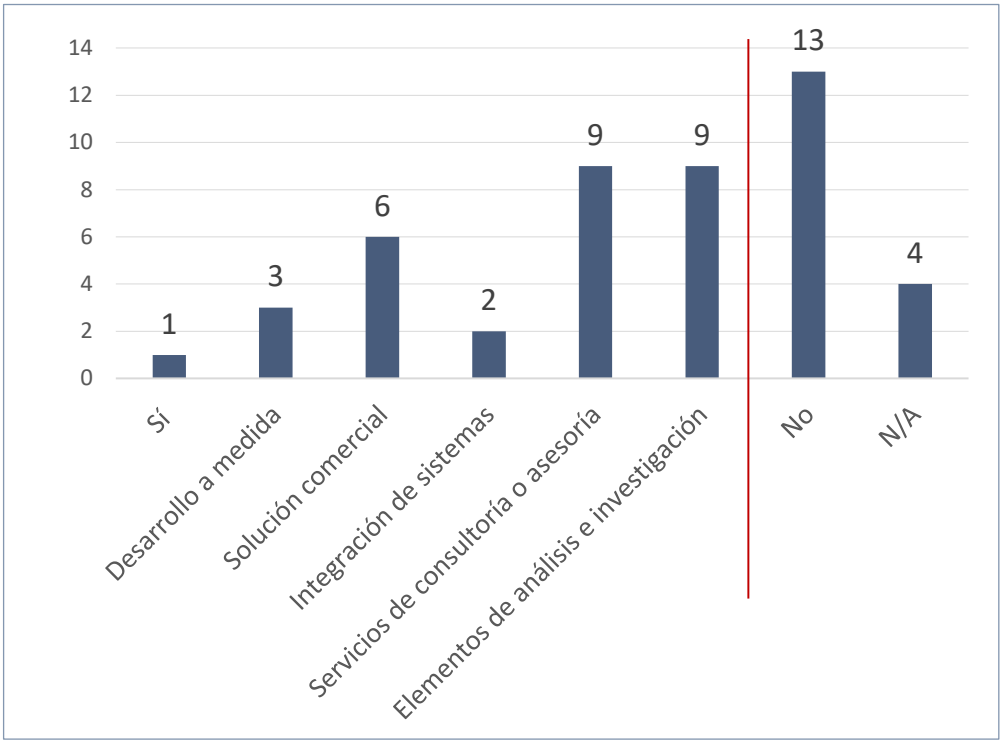


Figura 94. P47: Datos Mando y control

La representación gráfica de los datos positivos se muestra en la siguiente figura:

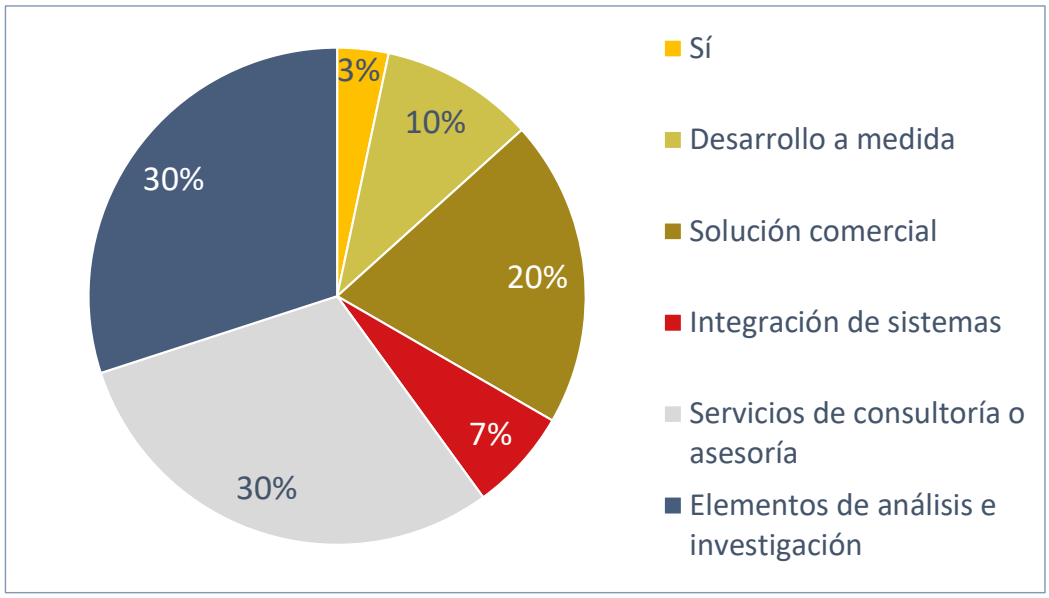


Figura 95. P47: Gráfico. Mando y control

Más de la mitad de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de mando y control (del ataque). De las entidades que ofrecen estos servicios, destaca que un tercio indica que realiza servicios de consultoría o asesoría y trabajos de análisis e investigación. Las siguientes actividades relacionadas con esta capacidad a las que más se dedican las entidades son la disposición de una solución comercial o los desarrollos a medida. Finalmente, la actividad menos citada son los trabajos de integración de sistemas.

Solo dos entidades expresan explícitamente que disponen de tecnología de mando y control anónimo e intrazable entre el objetivo infectado y la consola de mando y control. Esta tecnología propia no es conocida por las capas de seguridad del objetivo, lo que facilita la realización de las operaciones sin ser detectados.

Exfiltración

La finalidad de la subcapacidad de exfiltración es la extracción no detectada de datos a un objetivo.. Dentro de este apartado, podemos encontrar diferentes tipos según su funcionalidad: exfiltración a través de un protocolo alternativo, a través de otro medio de red o físico, o a través de un servicio web.

Los datos recogidos en la pregunta 48. *¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Exfiltración**, se muestran en la siguiente figura:

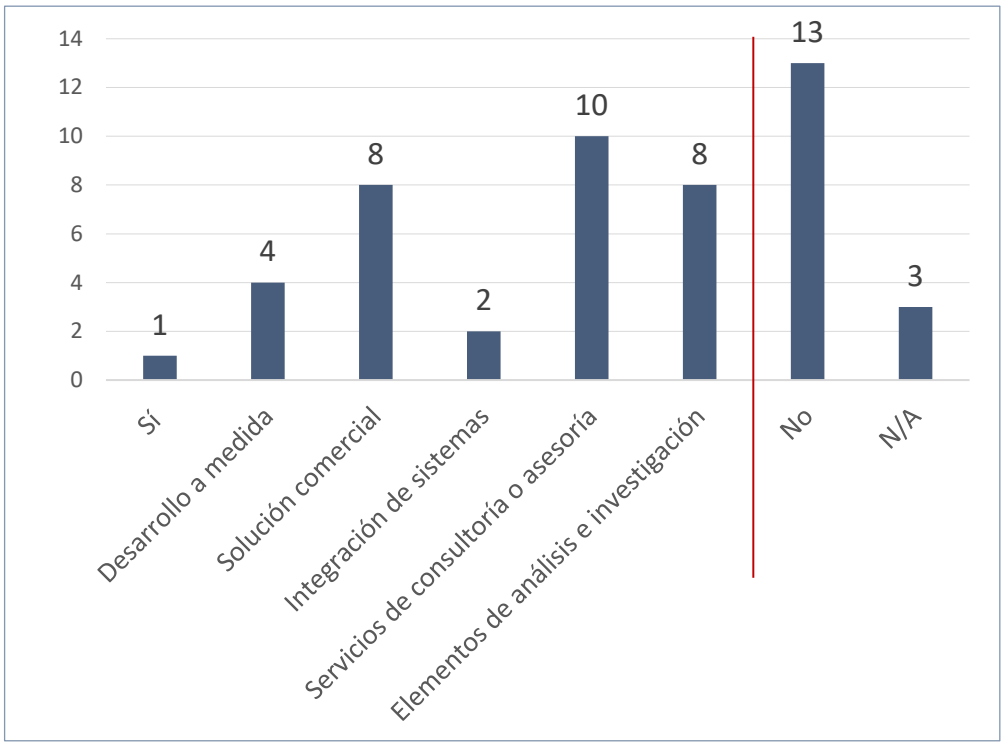


Figura 96. P48: Datos Exfiltración

La representación gráfica de los datos positivos se muestra en la siguiente figura:

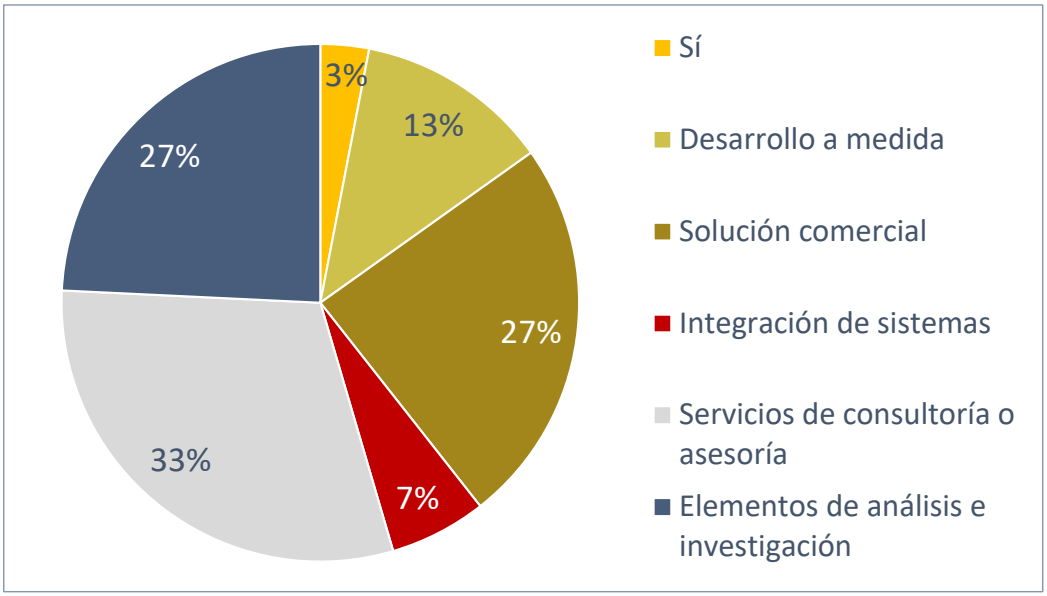


Figura 98. P48: Gráfico. Exfiltración

Más de la mitad de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de exfiltración. De las entidades que

ofrecen estos servicios, destaca que un tercio indica que realiza servicios de consultoría o asesoría. Las siguientes actividades relacionadas con esta capacidad a las que se dedica más de un cuarto de las entidades son los trabajos de análisis e investigación y la disposición de una solución comercial. Finalmente, llas actividades menos citadas son los desarrollos a medida y los trabajos de Integración de sistemas.

Existe al menos una entidad que indica que dispone de equipos de *red team* habituados a exfiltrar información a través de múltiples técnicas y plataformas, mediante servicios altamente confiables, *side channels*, cifrado o inclusos esteganografía, pero sin indicar si son mediante soluciones propias o comerciales y públicas. Solo existe una entidad que indica explícitamente que dispone de una técnica de desarrollo propio de exfiltración de datos.

Impacto

La finalidad de esta subcapacidad es interrumpir la disponibilidad o comprometer la integridad de los sistemas del adversario mediante el compromiso de los sistemas o servicios o la manipulación de los datos Dentro de este apartado, podemos encontrar diferentes tipos según su funcionalidad: explotación y ataque de vulnerabilidades específicas del sistema objetivo, eliminación del acceso a la cuenta, destrucción de datos, impacto por cifrado de datos, manipulación de datos, desfiguración, denegación de servicio, corrupción del *firmware*, inhibición de la recuperación del sistema, parada del servicio o apagado o reinicio del sistema.

Los datos recogidos en la pregunta 49*. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Impacto**, se muestran en la siguiente figura:

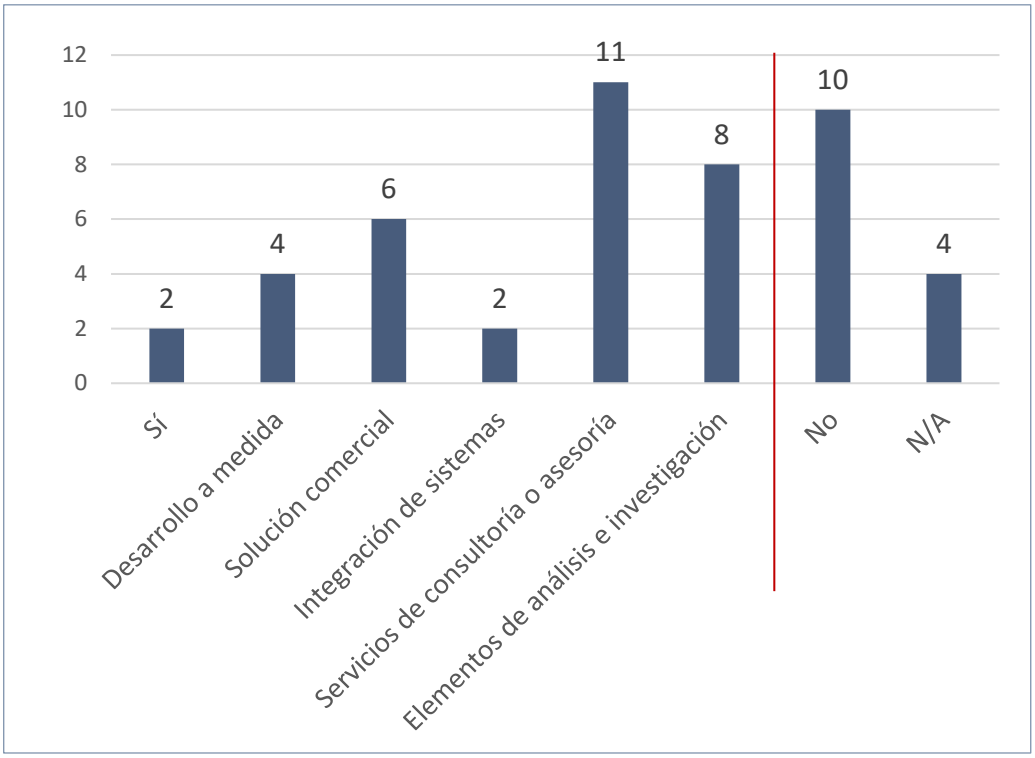


Figura 97. P49: Datos Impaqcto

La representación gráfica de los datos positivos se muestra en la siguiente figura:

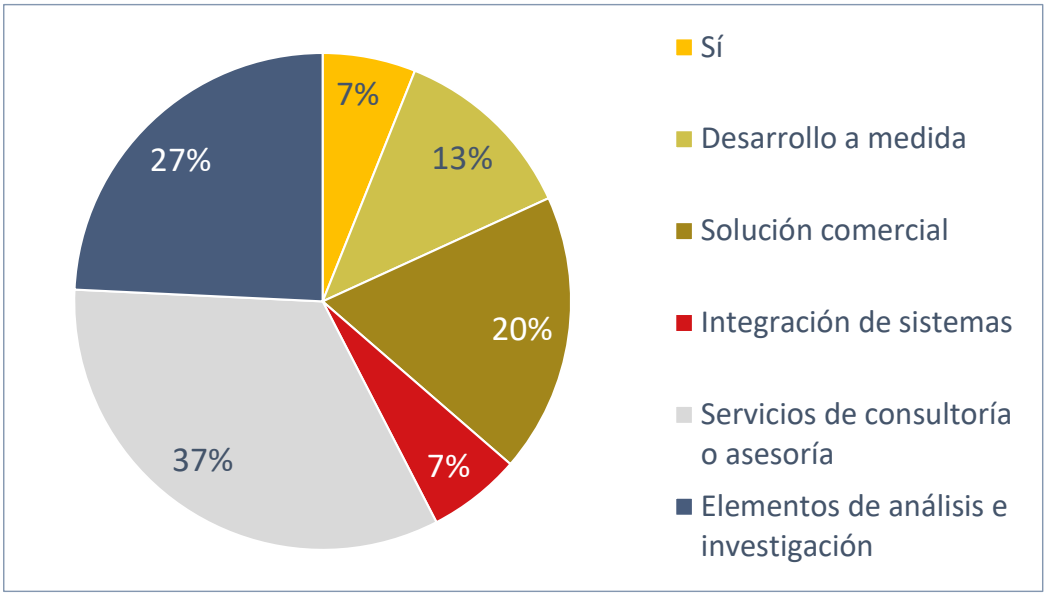


Figura 98. P49: Gráfico. Impacto

La mitad de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de Impacto. De las entidades que ofrecen estos servicios, destaca que más de un tercio indica que realiza servicios de consultoría o asesoría. Las siguientes actividades relacionadas con esta capacidad a las que más se dedican las entidades son los trabajos de análisis e investigación y la disposición de una solución comercial. Finalmente, las actividades menos citadas son los desarrollos a medida y los trabajos de integración de sistemas.

Existen algunas entidades que indican que disponen de equipos de *red team* que pueden llevar a cabo cualquier tipo de impacto contra la disponibilidad, integridad o confidencialidad de la información comprometida, pero sin indicar si lo llevan a cabo mediante desarrollos y técnicas propias o mediante productos y herramientas públicas. Sólo una entidad indica que cuenta con desarrollos de secuestro, control o compromiso de datos, instancias y sistemas operativos.

Efectos en la red (móviles)

La finalidad de esta subcapacidad es provocar efectos en la red móvil del adversario, manipulando el tráfico de red sin necesidad de acceder al propio dispositivo móvil. Dentro de este apartado, podemos encontrar diferentes tipos según su funcionalidad: disminución de versión a protocolos inseguros, explotación de protocolos de señalización, bloqueo o denegación de servicio o estaciones base de telefonía móvil y puntos de acceso wifi no autorizados.

Los datos recogidos en la pregunta 50. *¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Efectos en la red (móviles)**, se muestran en la siguiente figura:

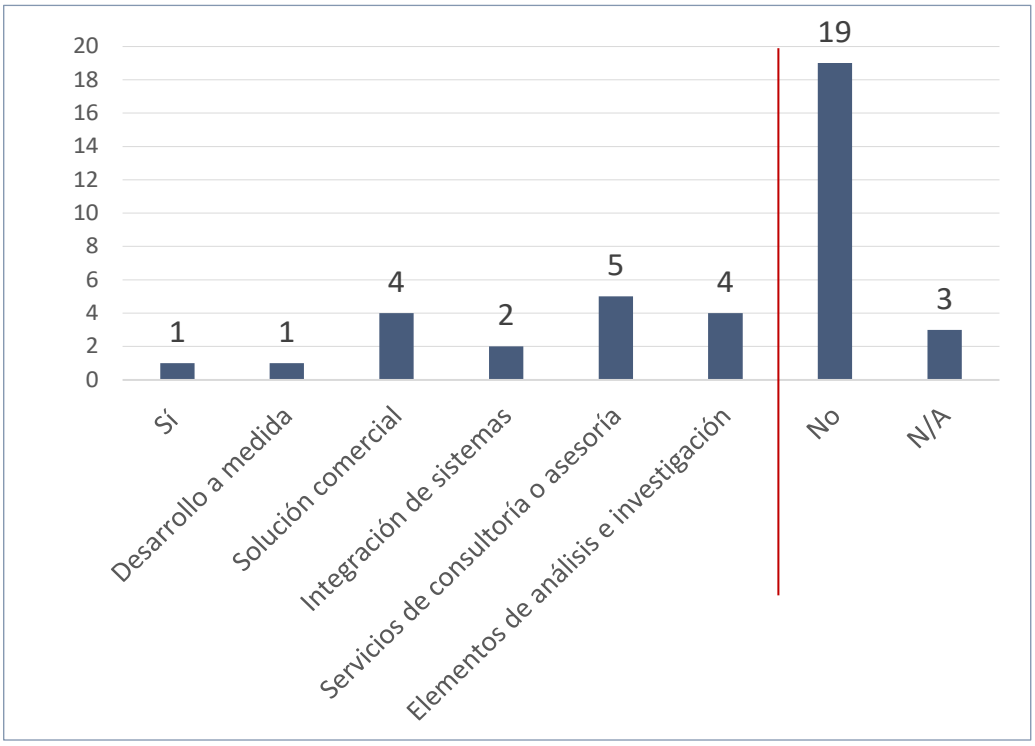


Figura 99. P50: Datos Efectos en la red (móviles)

La representación gráfica de los datos positivos se muestra en la siguiente figura:

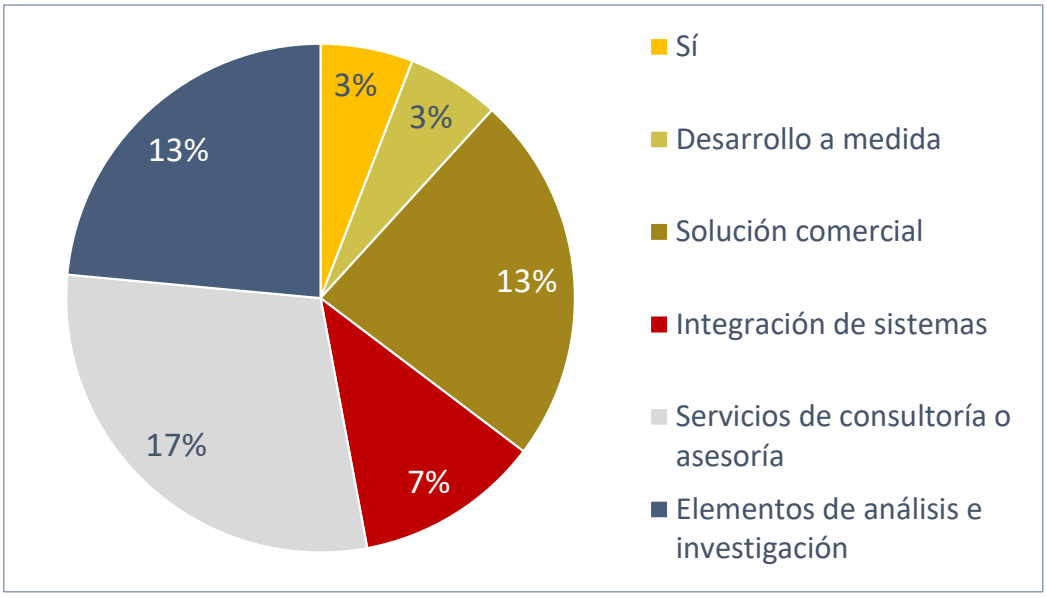


Figura 100. P50: Gráfico. Efectos en la red (móviles)

La mayoría de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de efectos en la red (móviles). De las entidades que ofrecen estos servicios, destaca que casi la quinta parte indica que realiza servicios de consultoría o asesoría. Las siguientes actividades relacionadas con esta capacidad a las que se dedican minoritariamente las entidades son los trabajos de análisis e investigación y la disposición de una solución comercial. Finalmente, las actividades menos citadas son los trabajos de integración de sistemas y los desarrollos a medida.

Efectos en los servicios remotos (móviles)

La finalidad de esta subcapacidad es provocar efectos en los servicios remotos, como los servicios en la nube o los servicios de gestión de la movilidad empresarial (EMM) y gestión de dispositivos móviles (MDM), sin acceder al propio dispositivo móvil. Dentro de este tipo se pueden encontrar diferentes grupos según su funcionalidad: obtención de copias de seguridad en la nube del dispositivo, rastreo remoto del dispositivo sin autorización, borrado de datos de forma remota sin autorización.

Los datos recogidos en la pregunta 51. *¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Efectos en los servicios remotos (móviles)**, se muestran en la siguiente figura:

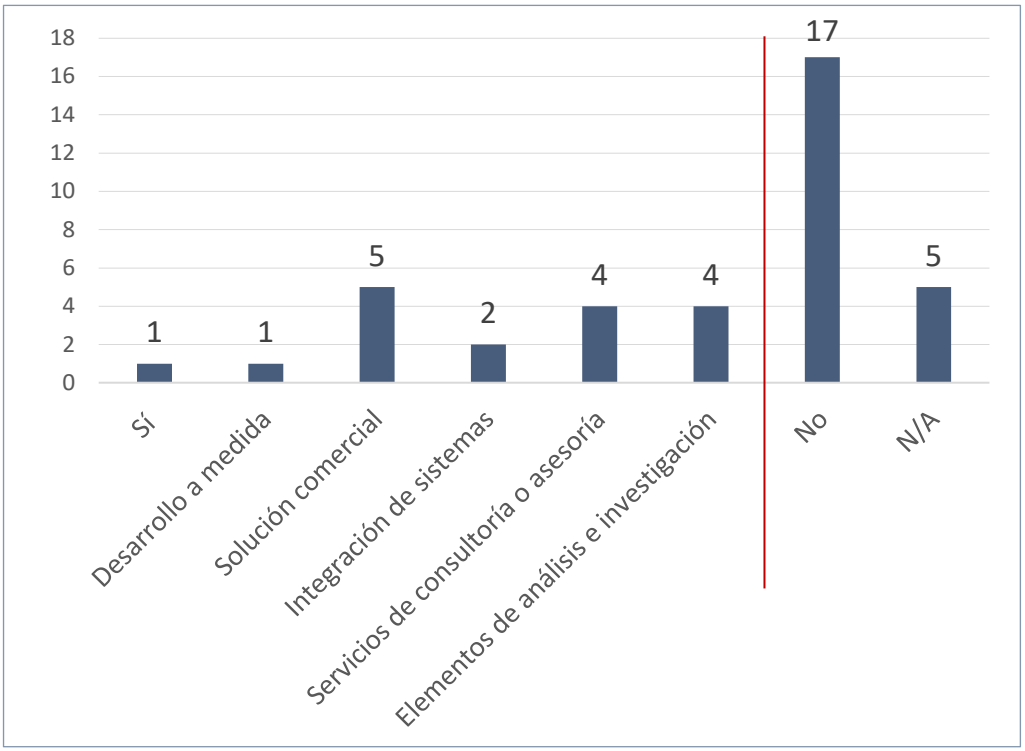


Figura 101. P51: Datos Efectos en los servicios remotos (móviles)

La representación gráfica de los datos positivos se muestra en la siguiente figura:

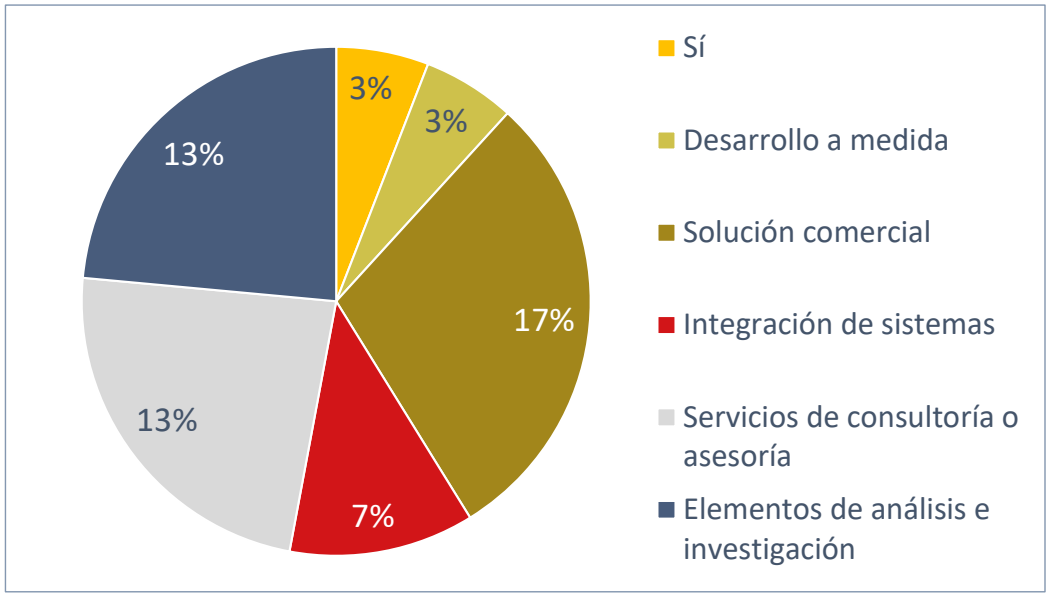


Figura 102. P51: Gráfico. Efectos en los servicios remotos (móviles)

La mayoría de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de efectos en los servicios remotos (móviles). De las entidades que ofrecen estos servicios, destaca que una quinta parte indica que dispone de una solución comercial. Las siguientes actividades relacionadas con esta capacidad a las que se dedican minoritariamente las entidades son los trabajos de servicios de consultoría o asesoría y de análisis e investigación. Finalmente, las actividades menos citadas son los trabajos de integración de sistemas y los desarrollos a medida.

Existe una respuesta que ha indicado explícitamente la capacidad de establecer un módulo *man-in-the-middle* entre dispositivos Android y la nube de Google, sin penetrar en el dispositivo.

Por lo general, el número de entidades que declara poseer capacidades de desarrollo en las distintas subáreas relacionadas con esta capacidad (como persistencia, escalada de privilegios o exfiltración) es bastante más reducido que en el resto. Esto era lo previsible, dado que se trata de un ámbito de actuación muy restringido y de menor demanda. Asimismo, debe de entenderse que la orientación de estos desarrollos está dirigida al ámbito civil y, más concretamente, al de las auditorías de sistemas (*hacking* ético, *pentesting*, *red team*, ...). No obstante, estas capacidades tienen una naturaleza dual y podrían ser aprovechables en el ámbito de las operaciones militares en el ciberespacio.

6.5 Capacidad de apoyo técnico a las operaciones

Esta capacidad da soporte al resto de capacidades principales (coordinación y control, defensa, explotación y respuesta).

Esta capacidad se desglosa en **cinco subcapacidades** que se detallan a continuación:

El cyberrange es una plataforma virtual que simula entornos operativos reales (estáticos o desplegables, clasificados o no) para la formación y el adiestramiento del personal, así como la experimentación, el testeo y la validación de nuevos conceptos, tecnologías, técnicas y tácticas de ciberseguridad y ciberdefensa, permitiendo reproducir diferentes ataques de forma segura para estudiar cómo defenderlos o reproducirlos. Dentro de este tipo podemos encontrar capacidades para la simulación de sistemas de control industrial (ICS), la simulación de comportamiento humano, la simulación de tráfico de red legítimo y malicioso, así como el uso de realidad virtual (RV), realidad aumentada (RA) y realidad mixta (RM), y la gestión de escenarios de pruebas de ciberseguridad y de despliegue de ciberejercicios.

Los datos recogidos en la pregunta *52. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Cyberrange**, se muestran en la siguiente figura:

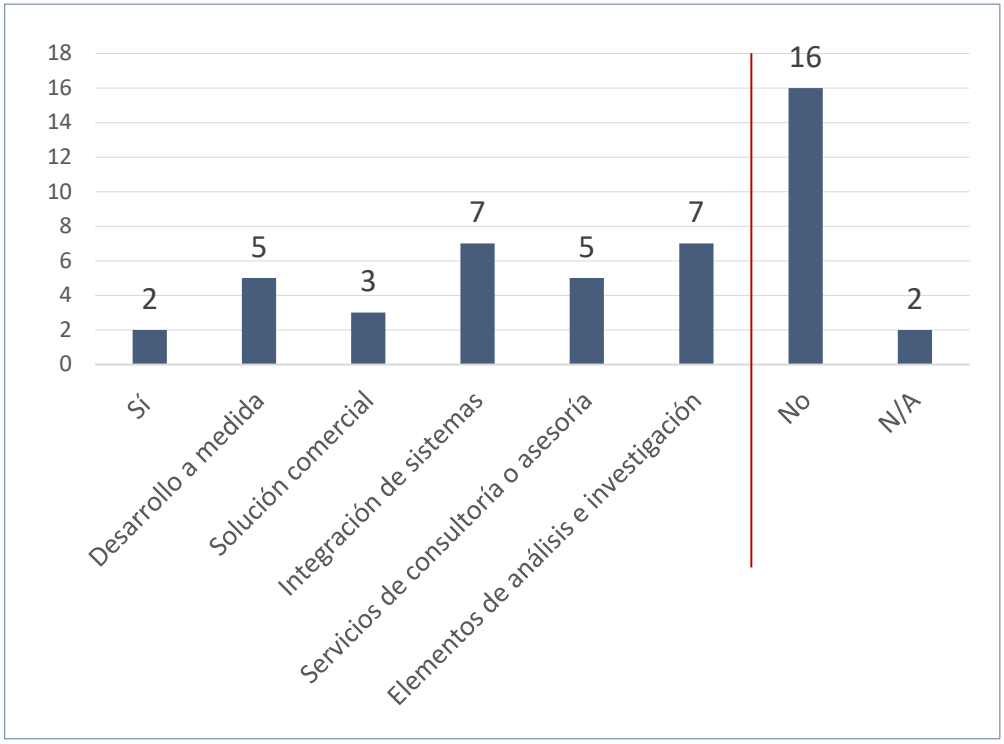


Figura 103. P52: Datos Cyberrange

La representación gráfica de los datos positivos se muestra en la siguiente figura:

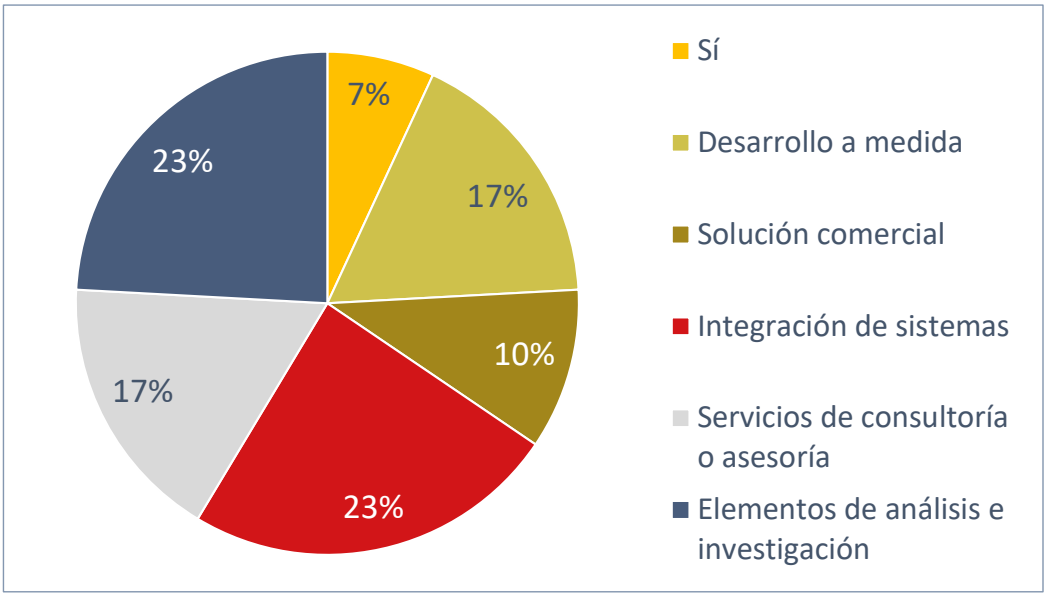


Figura 104. P52: Gráfico. Cyberrange

La mayoría de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de *cyberrange*. De las entidades que ofrecen estos servicios, destaca que una cuarta parte indica que realiza trabajos de análisis e investigación o de integración de sistemas relacionados. La siguiente actividad relacionada con esta capacidad a la que más se dedican las entidades son los servicios de consultoría o asesoría y otro tanto indican que disponen de una solución comercial. Finalmente, una pequeña parte de las entidades indica que realiza desarrollos a medida de estos sistemas.

Una de las entidades es la principal contratista de una plataforma de formación y ejercicios de ciberdefensa, coordinación y apoyo (CDTEXP: *Cyber Defence Training & Exercise, Coordination And Support Platform*) de la EDA para la puesta en marcha de servicios de entrenamiento y experimentación en el ámbito de la ciberdefensa. Permite la realización de entrenamientos y ejercicios de ciberdefensa en base a amenazas reales y actuales, facilitando la selección de escenarios en un entorno de trabajo real. Además, permite realizar distintos cursos que forman parte de una carrera especializada en ciberdefensa. También permite disponer de varios nodos del sistema, de forma federada, integrando distintas escuelas europeas de ciberdefensa, lo que permite ejercicios combinados (más complejos) y el intercambio de conocimientos y experiencia sobre el desarrollo y empleo de los *cyberranges*. Asimismo, dentro de otro contrato con la EDA, esta entidad está desarrollando un proyecto para el uso de inteligencia artificial en *cyberranges* (AI-CYBER), con el objetivo de utilizar el aprendizaje automático y profundo de la IA para realizar análisis predictivos y mejorarlos.

Otras entidades disponen de soluciones propias de *cyberrange,* para el entrenamiento y formación de los comandos del ciberespacio y profesionales del campo de la

ciberseguridad y ciberdefensa en un entorno a medida. Estas soluciones disponen de versiones escalables y están disponibles tanto en versión *stand-alone* como servicio en la nube, así como algunas se basan en el marco NICE (*National Initiative for Cybersecurity Education*) del Instituto NIST. En ellas se emplean técnicas y tecnologías novedosas para la capacitación de los usuarios en diferentes áreas de especialización.

Otro grupo dispone de soluciones específicas[22] para la realización de simulacros de ataques de *phishing* sobre el correo electrónico de los usuarios, desarrollan ejercicios de *cyberrange* a medida (*capture the flag*, *blue team, ...*) en el ámbito industrial o desarrollan plataformas de adiestramiento básico de acceso a entidades a partir de *software* de código abierto.

Laboratorio de análisis forense digital

Esta subcapacidad permite realizar labores de detección, adquisición, investigación y análisis de evidencias digitales con equipos y *software* especializado, extrayendo y analizando los datos contenidos en pruebas electrónicas. Dentro de este tipo podemos encontrar capacidades para: recolección y recuperación de evidencias digitales de dispositivos, copia segura de las pruebas y evidencias originales o análisis de memoria, archivos y extracción de metadatos.

Los datos recogidos en la pregunta *53. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Laboratorio de análisis forense digital**, se muestran en la siguiente figura:

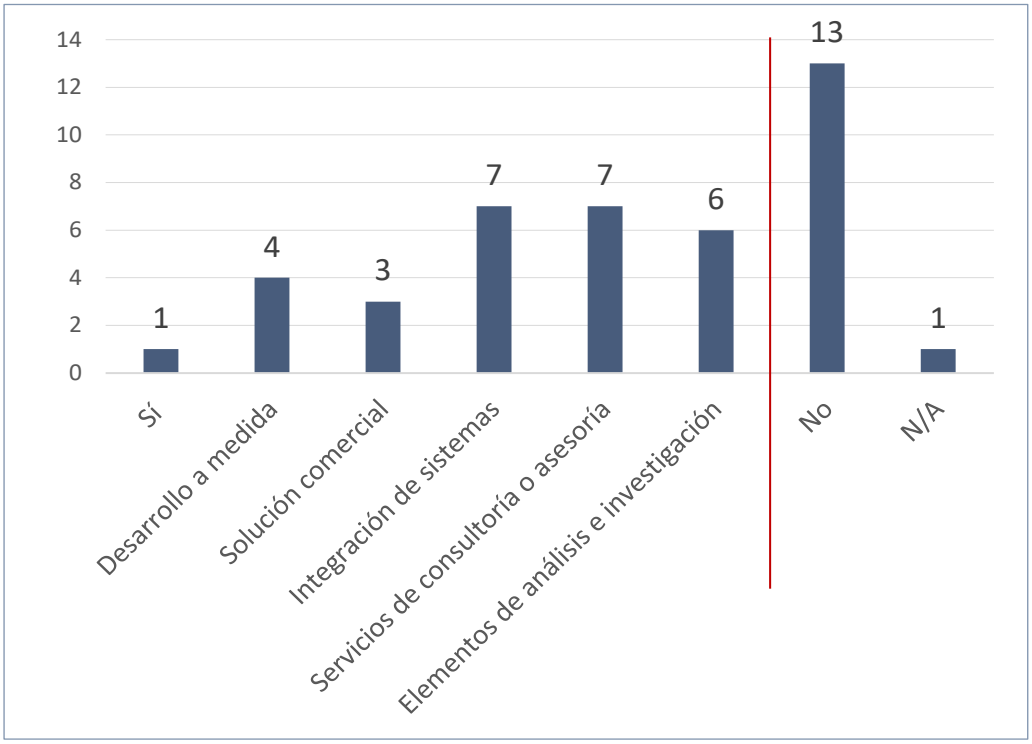


Figura 105. P53: Datos Laboratorio de análisis digital

[22] Como por ejemplo Proofpoint Awareness con Mellivora

La representación gráfica de los datos positivos se muestra en la siguiente figura:

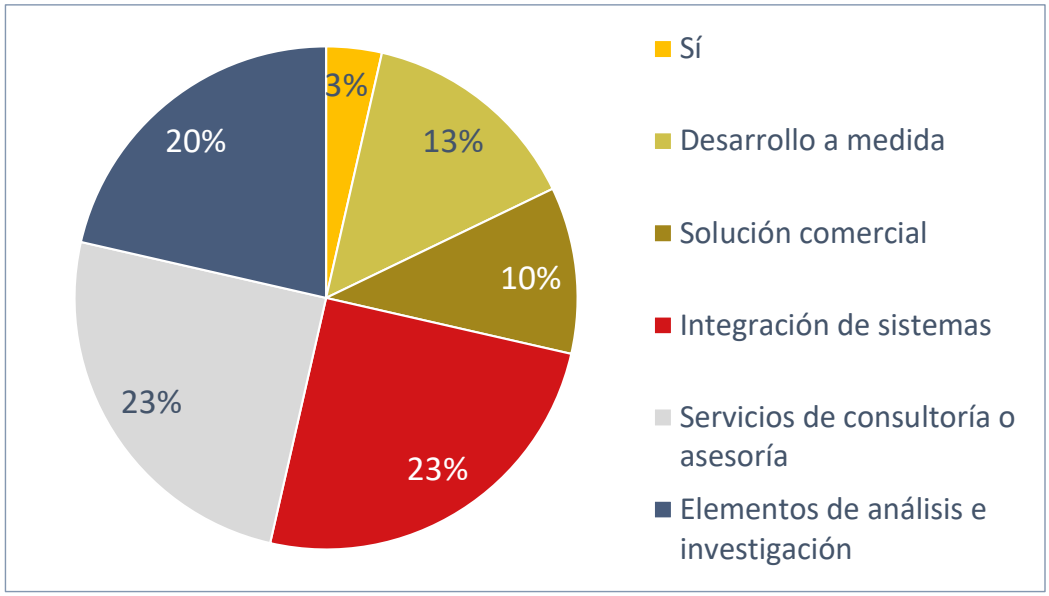


Figura 106. P53: Gráfico. Laboratorio de análisis digital

La mitad de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de laboratorio de análisis forense digital. De las entidades que ofrecen estos servicios, destaca que una cuarta parte indica que realiza trabajos de servicios de consultoría o asesoría o de integración de sistemas relacionados. Las siguientes actividades relacionadas con esta capacidad a las que se dedican menos las entidades son los trabajos de análisis e investigación y los desarrollos a medida. Finalmente, la actividad minoritaria es la disposición de una solución comercial de estos sistemas.

Algunas entidades declaran disponer de capacidades de forense propias con las que realizan investigación, análisis y extracción de datos contenidos en diferentes dispositivos u ofrecen estos servicios, desde el SOC, para la extracción y análisis de evidencias digitales.

Otras, dentro de los desarrollos a medida para la EDA o FRONTEX, integran en sus redes y sistemas herramientas comerciales y procesos para la adquisición y análisis de evidencias digitales que faciliten su posterior análisis forense.

Por último, encontramos entidades que no desarrollan, pero son usuarias de este tipo de servicios de forma externa.

Despliegue automático de sistemas seguros

Esta subcapacidad permite el despliegue automático de Infraestructura como código (IAC *Infrastructure As Code*) que, a su vez, posibilita el despliegue de servicios de forma automatizada y bastionada con guías CCN-STIC sobre una plataforma *hardware* limpia.

Los datos recogidos en la pregunta *54. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Despliegue automático de sistemas seguros**, se muestran en la siguiente figura:

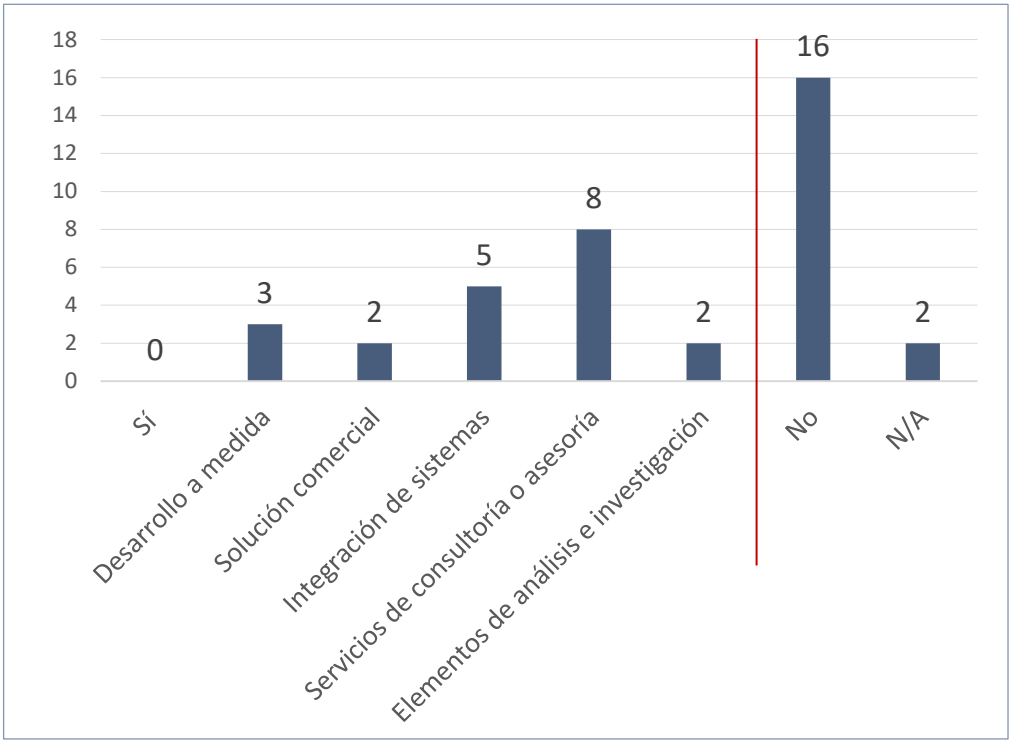


Figura 107. P54: Datos Despliegue automático de sistemas seguros

La representación gráfica de los datos positivos se muestra en la siguiente figura:

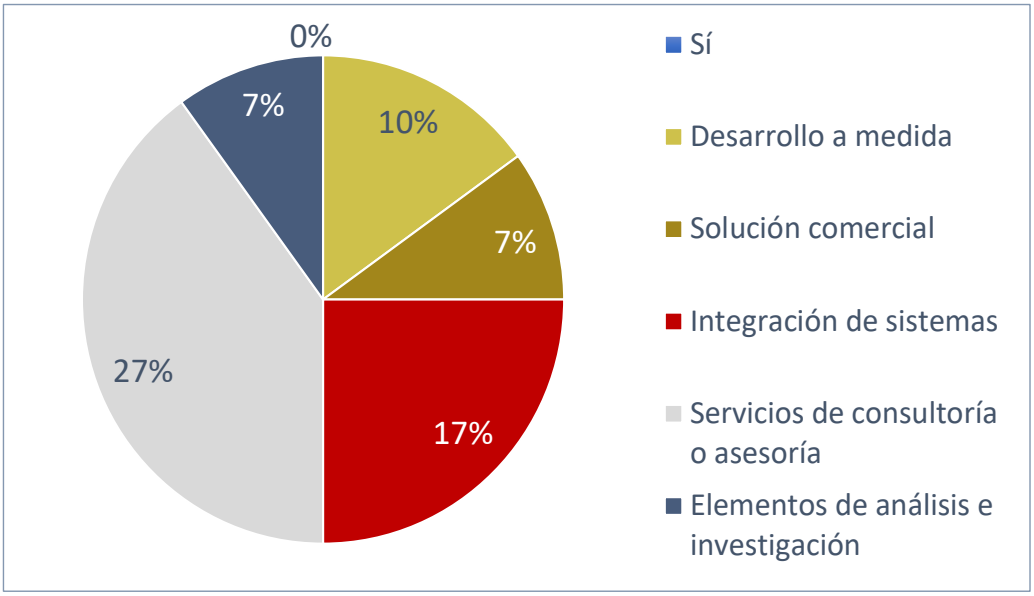


Figura 108. P54: Gráfico. Despliegue automático de sistemas seguros

La mitad de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de despliegue automático de sistemas seguros. De las entidades que ofrecen estos servicios, destaca que casi la cuarta parte indica que realiza trabajos de servicios de consultoría o asesoría. Las siguientes actividades relacionadas con esta capacidad a las que se dedican las entidades son integración de sistemas relacionados, los trabajos de análisis e investigación y los desarrollos a medida. Finalmente, solo un grupo pequeño de entidades indica que dispone de una solución comercial para esta capacidad.

Varias de las entidades han contestado que trabajan en desarrollos relacionados con la subcapacidad de despliegue automático de sistemas seguros pero, analizando la información adicional aportada en sus respuestas, la mayoría de ellas la ha identificado con algún hipervisor, lo que no está relacionado con esta subcapacidad..

Es importante aclarar que la **capacidad de despliegue automático de sistemas seguros** está relacionada con el concepto de IAC (*Infrastructure As Code*) por el cual se emplea la tecnología de Microsoft Azure para instalar, desplegar y configurar servicios y aplicaciones de Microsoft a través de un Powershell y el lenguaje CLR (*Common Language Runtime*) de la plataforma .NET de Microsoft.. En este proceso se recogen las variables y configuraciones a desplegar y se envían al orquestador que automatiza configuraciones que se vayan a desplegar, controladores de dominio DC (con GPO) y otros elementos del sistema. Mediante la funcionalidad DSC (*Desired State Configuration*), los administradores convierten *scripts* de configuración de sistemas en sistemas desplegados y funcionales. Además, estos lenguajes y funcionalidades permiten aplicar plantillas de instalación

con los *scripts* de las guías CCN-STIC y mejores prácticas de seguridad necesarias para obtener, a partir de un conjunto de *hardware*, un sistema compuesto por varias máquinas configuradas de forma segura (y sin conflictos), bastionadas y con un dominio común listo para usarse. Actualmente, existe un proyecto de I+D+i del MINISDEF para generar un nodo de misión a partir del *hardware* y los *scripts* necesarios en unas horas, listo para ser desplegado en zona de operaciones e integrado en la red de la misión.

Atendiendo a la información aportada, algunas entidades están realizando despliegues automáticos y *dockerizando*[23] sistemas para ser desplegados en infraestructuras limpias y orquestadas[24], pero no sobre máquinas bastionadas de forma segura con guías CCN-STIC. Sin embargo, otras sí realizan los bastionados de sistemas limpios siguiendo las guías CCN-STIC.

Otras entidades indican que despliegan máquinas virtuales, aplicando configuraciones bastionadas previamente con guías aprobadas, aplicando SCCM (*System Center Configuration Manager*) o INTUNE (administración de dispositivos y aplicaciones móviles).

Finalmente, encontramos entidades que participan en el desarrollo de guías CCN-STIC y desarrollan despliegues desatendidos de entornos seguros y bastionados.

---

[23] Empaquetar una aplicación, para luego distribuirla y ejecutarla a través de los contenedores de software.

[24] Como KUBERNETES o VmWare

Combat cloud

Esta subcapacidad constituye una red de información descentralizada, resiliente y colaborativa que conecta los nodos de todas las fuerzas en zona de operaciones, posibilitando la obtención de inteligencia y los intercambios de información en tiempo real.

Los datos recogidos en la pregunta *55. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Combat cloud**, se muestran en la siguiente figura:

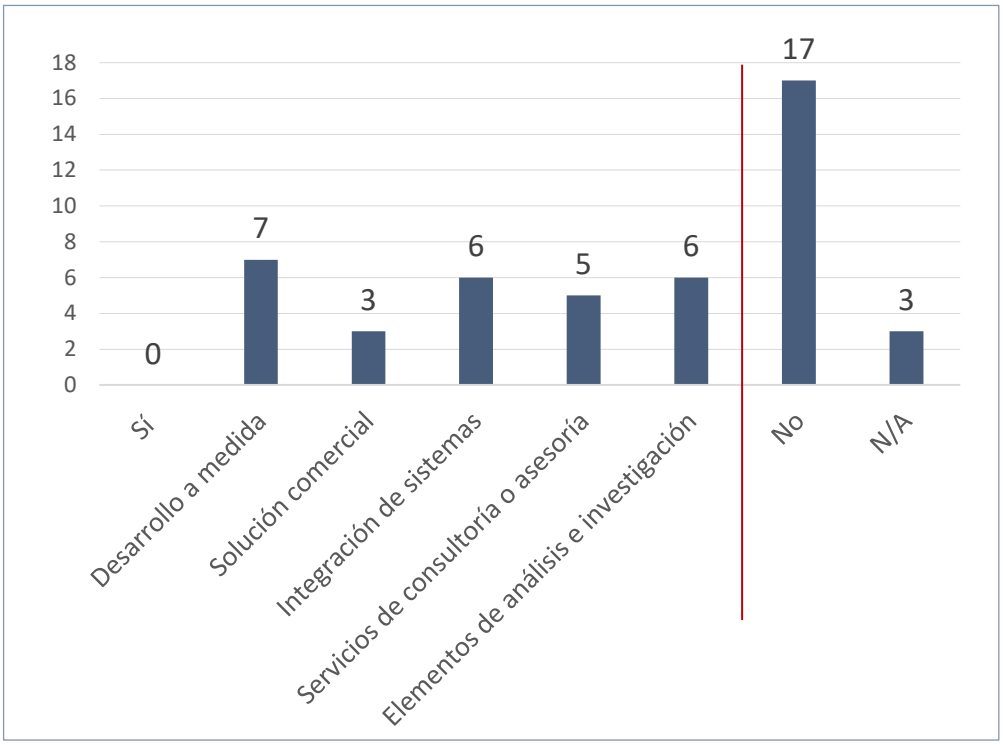


Figura 109. P55: Datos Combat cloud

La representación gráfica de los datos positivos se muestra en la siguiente figura:

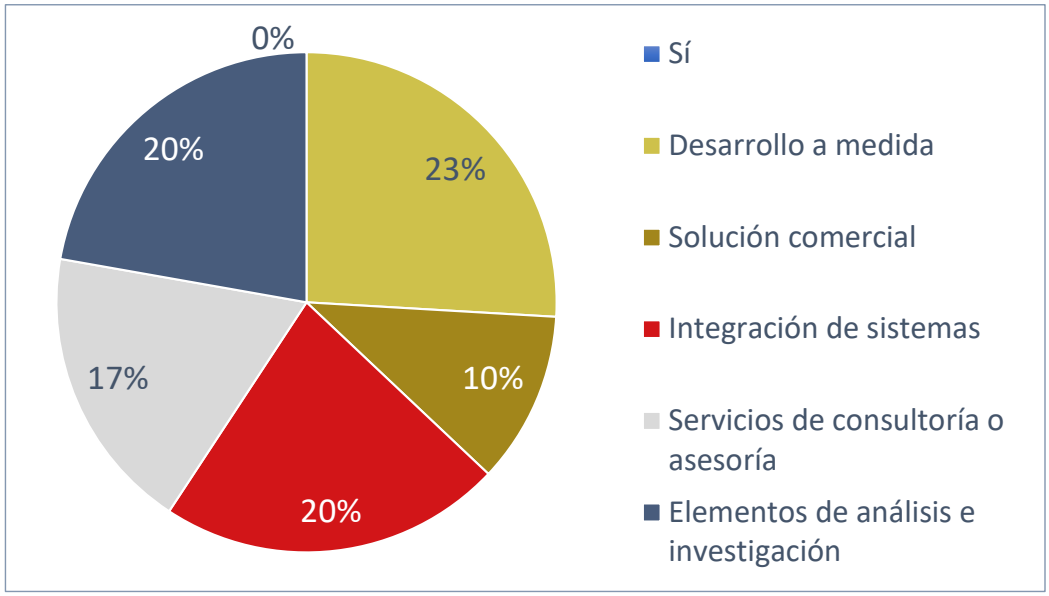


Figura 110. P55: Gráfico. Combat cloud

La mayoría de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de *combat cloud*. De las entidades que ofrecen estos servicios, destaca que una cuarta parte indica que realiza desarrollos a medida. Las siguientes actividades relacionadas con esta capacidad a las que se dedican las entidades son los trabajos de Integración de sistemas y de análisis e investigación. Finalmente, una pequeña parte indica que realiza servicios de consultoría o asesoría y que dispone de una solución comercial para esta capacidad.

Algunas entidades indican que son coordinadores del programa de desarrollo del sistema de combate aéreo (NGWS/FCAS) para el MINISDEF donde un avión tripulado volará integrado con otras aeronaves no tripuladas que realizan detecciones de amenazas a través de su visión artificial y que notifican automáticamente al piloto y a las unidades en tierra. De esta forma, opera como un único sistema, dentro de una nube de combate conectada mediante radios tácticas, que da soporte a soldados a pie en el campo de batalla. Además de este, trabajan en múltiples proyectos internacionales tanto en el desarrollo de soluciones *combat cloud* a medida como en el desarrollo de soluciones comerciales descalables en diferentes tecnologías como *cloud* federadas, *fog y cloud computing* o certificación de *clouds*. Esta nube está basada en soluciones comerciales con un ordenador miniaturizado que habilita el uso de inteligencia artificial y se integra la plataforma de conciencia situacional (EDA-CLAUDIA) e intercambio de información de nivel estratégico u operacional.

También se han realizado análisis de riesgos de la tecnología *cloud* para su utilización con información clasificada para la solución de intercambio de información (RESTRICTED) del programa de la EDA EUCI-CIS (*Communication and Information systems for the processing of EU unclassified and classified information*), dentro de un grupo de trabajo de OTAN.

Otras entidades cuentan con un servicio de SOC integrado en redes de intercambio de información global (*CyberAlliance*, etc.) donde comparten datos anónimos de amenazas de red y correo con fabricantes[25].

Producción de *malware* específico

Esta subcapacidad permite desarrollar *software* con la finalidad de penetrar en sistemas objetivo con fines destructivos o de inteligencia.

Los datos recogidos en la pregunta *56. ¿Está su organización trabajando en desarrollos que puedan ser aplicables a esta área o cuenta con capacidad para hacerlo a corto plazo?*, correspondientes a la subcapacidad de **Producción de malware específico**, se muestran en la siguiente figura:

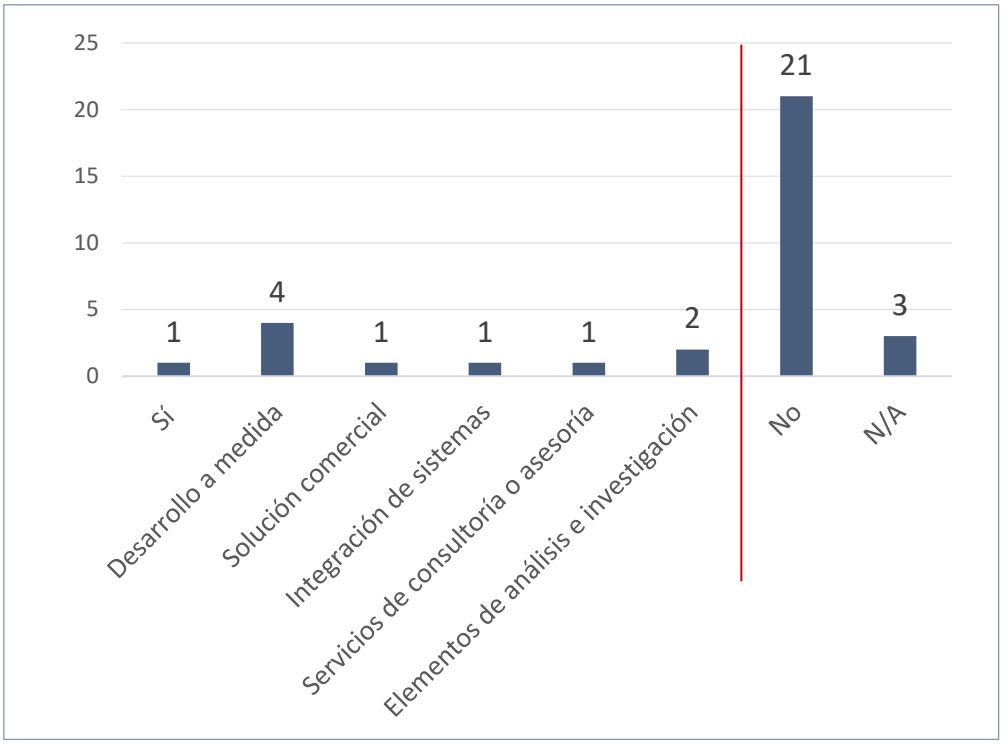


Figura 111. P56: Datos Producción de malware específico

[25] Como Fortinet, Proofpoint o Netskope.

La representación gráfica de los datos positivos se muestra en la siguiente figura:

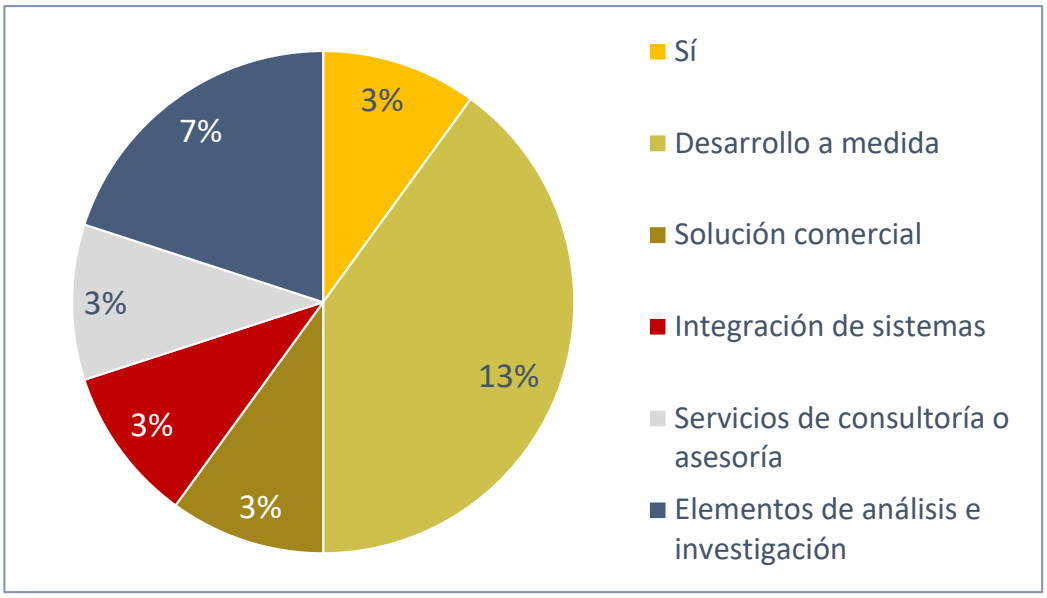


Figura 112. P56: Gráfico. Producción de malware específico

La mayoría de las entidades declara que en su organización no se desarrollan sistemas ni se ofrecen servicios relacionados con la capacidad de Producción de *malware* específico. De las entidades que ofrecen estos servicios, las actividades más dedicadas son los desarrollos a medida y los trabajos de análisis e investigación. Al resto de actividades sólo se dedica una minoría.

Algunas entidades indican que están especializadas en el desarrollo de *malware* y troyanos, y, de la misma forma, disponen de una red de provisión de *exploits* en caso de requerirse.

Otras, destacan que a través del conocimiento adquirido en diferentes sistemas se plantean una línea de evolución de su equipo *offensive* para el desarrollo de artefactos que permitan la explotación de vulnerabilidades en entornos móviles.

Al menos una entidad declara disponer de capacidades de forense y *reversing engineering*, pero no realizan *malware.*

Finalmente, alguna entidad indica que desarrolla este tipo de elementos, pero solo en entornos simulados o virtuales.

En esta área es necesario destacar un desarrollo muy desigual marcado por las subáreas. Si bien todos los desarrollos relativos a la generación y uso de *cyberranges* son punteros y muy extendidos, no ocurre lo mismo con las áreas relativas al desarrollo específico de *malware* o al despliegue automático de sistemas.

Del resto de las tecnologías que se han analizado y que se recogen en el presente informe, existe potencial para poder seguir mejorando en el desarrollo de estas áreas y en el conocimiento profundo de estas tecnologías.

7. COMPARATIVAS SOBRE ÁMBITOS TECNOLÓGICOS

A continuación, se muestra tanto la información recogida de las entidades participantes sobre desarrollos de tecnologías como su aplicabilidad en el sector de la ciberdefensa y los inconvenientes que han surgido en el proceso. Dentro de cada subapartado se recoge la pregunta realizada, las respuestas obtenidas y las primeras conclusiones alcanzadas.

Como hemos mencionado anteriormente, la definición y explicación de los ámbitos tecnológicos de este apartado se describen exhaustivamente en el ANEXO I: Descripción de los ámbitos tecnológicos.

Hay que aclarar que algunas entidades han declarado que varias opciones (respuestas múltiples) son de aplicación en algunas cuestiones, por lo que estas no son excluyentes entre sí y se han tenido en cuenta todas. Por esta razón, en algunas gráficas se puede encontrar que la suma de los porcentajes de las opciones es superior a un 100% al estar referido al número de entidades que ha respondido a cada opción.

7.1. Cuestiones Generales

El análisis de las respuestas de este aspecto se desglosa en **cuatro áreas** (trabajos y desarrollos, aplicación del sector de defensa, I+D+i y barreras tecnológicas) que se detallan a continuación:

Trabajos y desarrollos

Conocer la hoja de ruta temporal que establecen las entidades a la hora de incorporar o no las diferentes tecnologías en sus soluciones o productos, permite obtener una foto de qué tecnologías identifican como prioritarias y sobre las que generarán o mejorarán las capacidades de sus productos y servicios. A continuación, se recoge por ámbitos tecnológicos el mapa temporal que identifica cada entidad para el desarrollo de actividades con las diferentes tecnologías.

Los datos recogidos en la pregunta 57. *¿Está su organización trabajando y/o desarrollando las siguientes tecnologías?,* en el marco temporal "No, nunca, no a corto plazo, sí a corto plazo y sí, a largo plazo", se muestran en la siguiente figura:

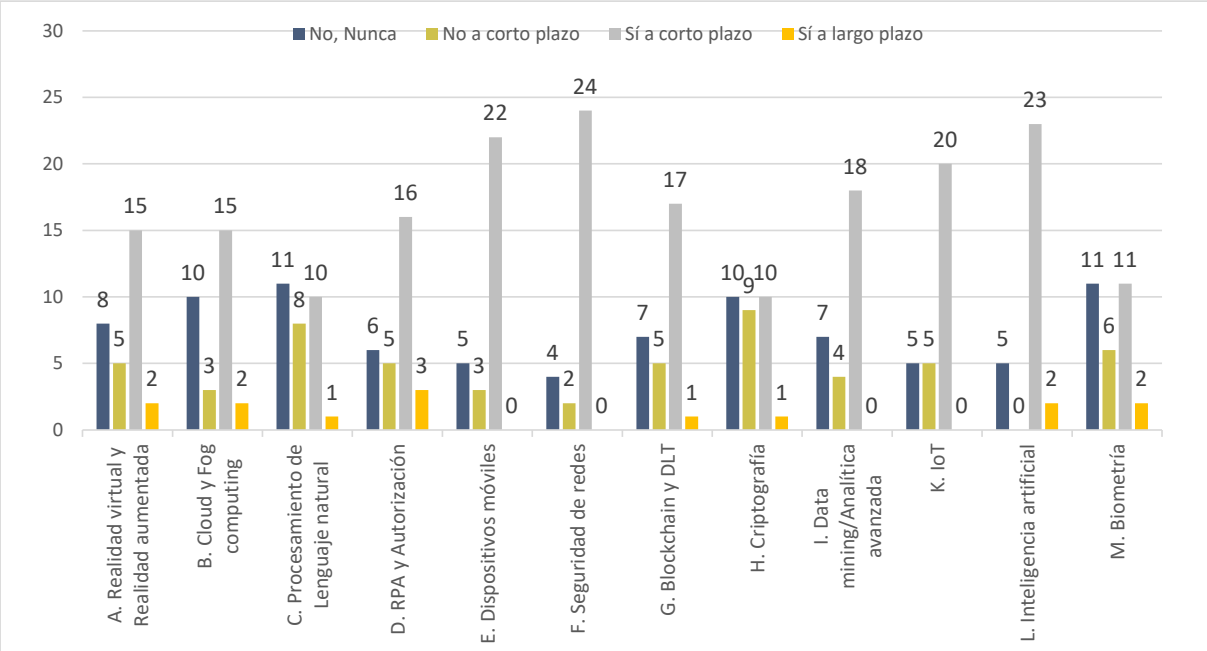


Figura 113. P57: Datos tecnologías: Trabajos y desarrollos por la organización

La representación gráfica que recoge el porcentaje de las entidades con intención de trabajar o desarrollar, a corto o a largo plazo, para cada una de estas tecnologías, se muestra en la siguiente figura:

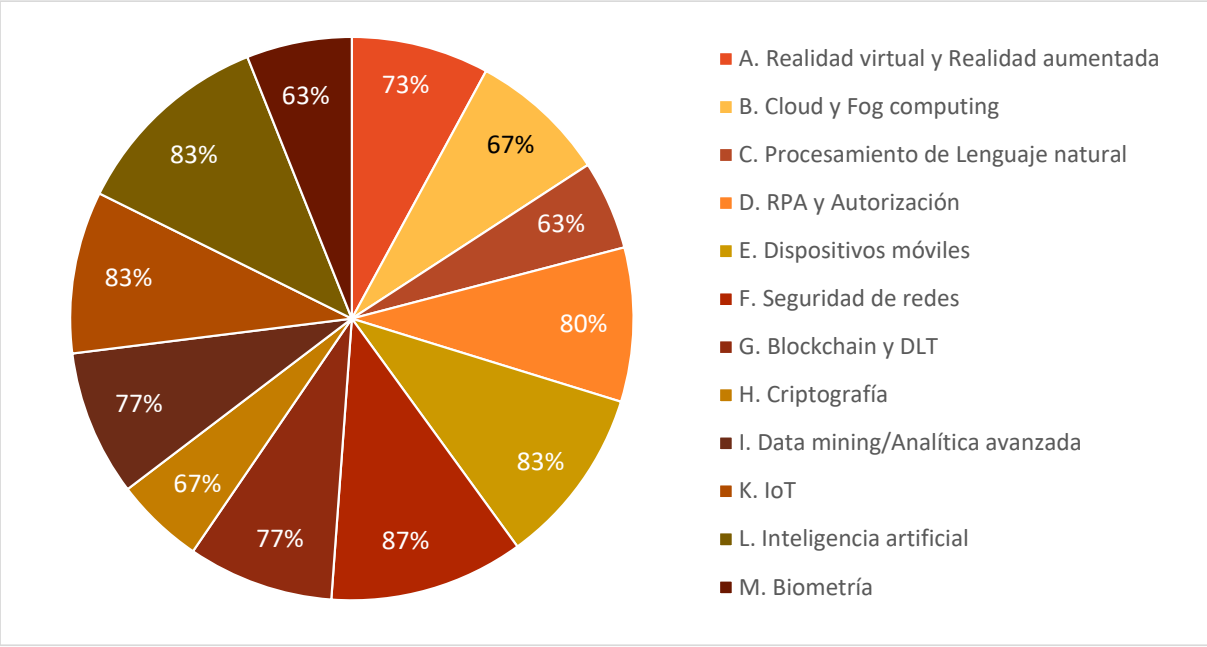


Figura 114. P57: Gráfico. Tecnologías: Trabajos y desarrollos por la organización

Como se puede observar en las gráficas anteriores, entre un 63% y un 87% de las entidades encuestadas indica que trabajarán o desarrollarán a corto o largo plazo las tecnologías propuestas. Principalmente destacan s**eguridad en redes, dispositivos móviles, LOT, inteligencia artificial, RPA y automatización** para la mayoría de las entidades consultadas.

Mientras que aproximadamente un cuarto de las entidades no las ha identificado dentro de su hoja de ruta, principalmente destacando cloud **y** fog computing**, procesamiento del lenguaje natural, criptografía y la biometría** como tecnologías con menos interés.

A continuación, se analizan las respuestas recibidas para cada tecnología en esta área.

Tal y como indican los datos, se puede observar que la mitad de las entidades que ha mostrado interés en la **realidad virtual y realidad aumentada** trabajará a corto plazo con ella y casi tres cuartas partes se espera hacerlo a largo plazo. A raíz de los datos parece relevante la intención de las entidades en desarrollar e integrar esta tecnología en sus productos.

En el caso de la tecnología de cloud **y** fog computing, la mitad de las entidades consultadas está o va a estar trabajando a corto plazo y alrededor de dos tercios indica que trabajará con ella a corto plazo. Se observa que esta tecnología también es relevante para la mayoría de las entidades, aunque existe un número significativo de entidades, un tercio, que no la identifican en su *roadmap* a futuro.

Para la tecnología de **procesamiento de lenguaje natura**l, se observa que sólo un tercio de las entidades consultadas está o va a estar trabajando a corto plazo en ella y un poco más de la mitad espera hacerlo a largo plazo. El desarrollo e integración de esta tecnología en sus productos muestra un interés moderado por parte de las entidades, existiendo un número significativo de entidades, un tercio, que no la considera en sus inversiones futuras.

En relación con la tecnología de **RPA y automatización**, la mitad de las entidades consultadas está o va a estar trabajando en el corto plazo y alrededor del 80% se espera hacerlo a largo plazo.. Estos datos demuestran un elevado interés de las entidades por esta tecnología.

Tal y como indican los datos, se puede observar que la mayoría de las entidades consultadas está o va a estar trabajando en **dispositivos móviles** a corto o a largo plazo. Esto evidencia el interés de las entidades en desarrollar e integrar estas tecnologías en sus productos.

En el caso de la tecnología de **seguridad de redes**, la mayoría de las entidades consultadas está o va a estar trabajando a corto o largo plazo en ella. Los datos muestran que se trata de la tecnología más señalada por las entidades en cuanto a interés en su desarrollo e integración en sus productos.

Para la tecnología de blockchain **y DLT**, la mitad de las entidades consultadas está o va a estar trabajando en el corto plazo y alrededor del 77% se espera hacerlo a largo plazo. Los datos señalan esta tecnología como una de las más interesantes para las entidades.

En relación con la **tecnología de criptografía**, sólo un tercio de las entidades consultadas está o va a estar trabajando en ella a corto plazo, mientras que alrededor del 66% se espera que lo haga a largo plazo. A raíz de los datos, se aprecia una intención moderada de desarrollo a corto plazo, siendo más amplia a largo plazo, aunque un tercio de las entidades no la consideran en sus planes de futuro

Tal y como indican los datos, se puede observar que más de la mitad de las entidades está o va a estar trabajando en data mining **y analítica avanzada** a corto plazo y alrededor del 77% a largo plazo. Existe un interés relevante por parte de las entidades en desarrollar e integrar estas tecnologías en sus productos.

En el caso de la tecnología de **IOT**, más de la mitad de las entidades consultadas está o va a estar trabajando en ella a corto plazo y alrededor del 84% espera hacerlo a largo plazo. De modo que esta tecnología resulta una de las más destacadas por parte de la mayoría de las entidades.

Para la tecnología de **inteligencia artificial**, se observa que la mayoría de las entidades consultadas está o va a estar trabajando en ella a corto o largo plazo, lo que demuestra un interés relevante de las entidades en desarrollar e integrar estas tecnologías en sus productos.

En relación con la tecnología de **biometría**, un tercio de las entidades consultadas está o va a estar trabajando en el corto plazo y alrededor del 64% espera hacerlo a largo plazo. Aun siendo una tecnología de interés para las entidades, un tercio de estas no la contempla en su hoja de ruta.

Como conclusión de este apartado de **trabajos y desarrollos** se puede extraer que, en el corto plazo, la Seguridad en las redes, la inteligencia artificial, la criptografía, el procesamiento de lenguaje natural y los dispositivos móviles son las tecnologías en las que más se están enfocando las entidades consultadas.

Aplicación del sector de la ciberdefensa

La aplicación a la ciberdefensa de las diferentes soluciones tecnológicas en desarrollo va estrechamente ligada a la situación del mercado y la necesidad establecida para el despliegue de las mismas. A continuación, se recogen por ámbitos tecnológicos la apuesta por el desarrollo de aplicaciones para la Ciberdefensa de las entidades encuestadas.

Los datos recogidos en la pregunta 58. *¿Está su organización trabajando concretamente en la aplicación de las mismas en el sector de la Ciberdefensa?*en el marco temporal "No, nunca, no a corto plazo, sí a corto plazo y sí, a largo plazo",y que completan la pregunta 57, se muestran en la siguiente figura:

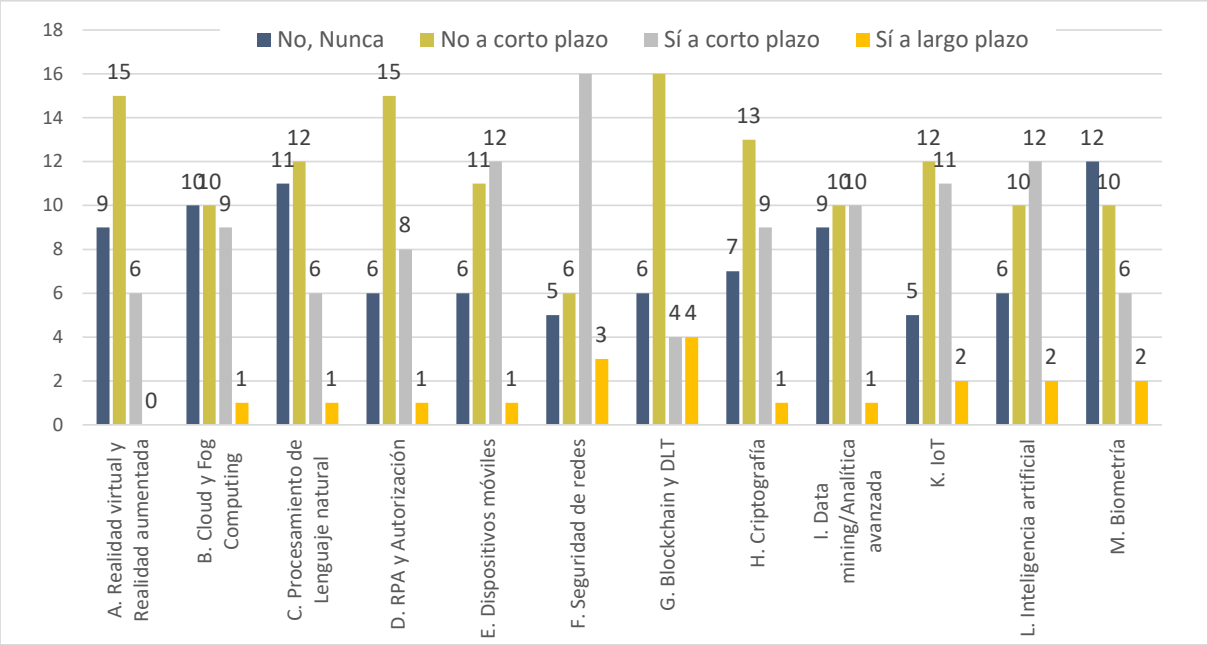


Figura 115. P58: Datos Tecnologías: Aplicación de las tecnologías a la ciberdefensa

La representación gráfica de los datos de las entidades con intención de aplicar dichas tecnologías a la Ciberdefensa, a corto o largo plazo, se muestra en la siguiente figura:

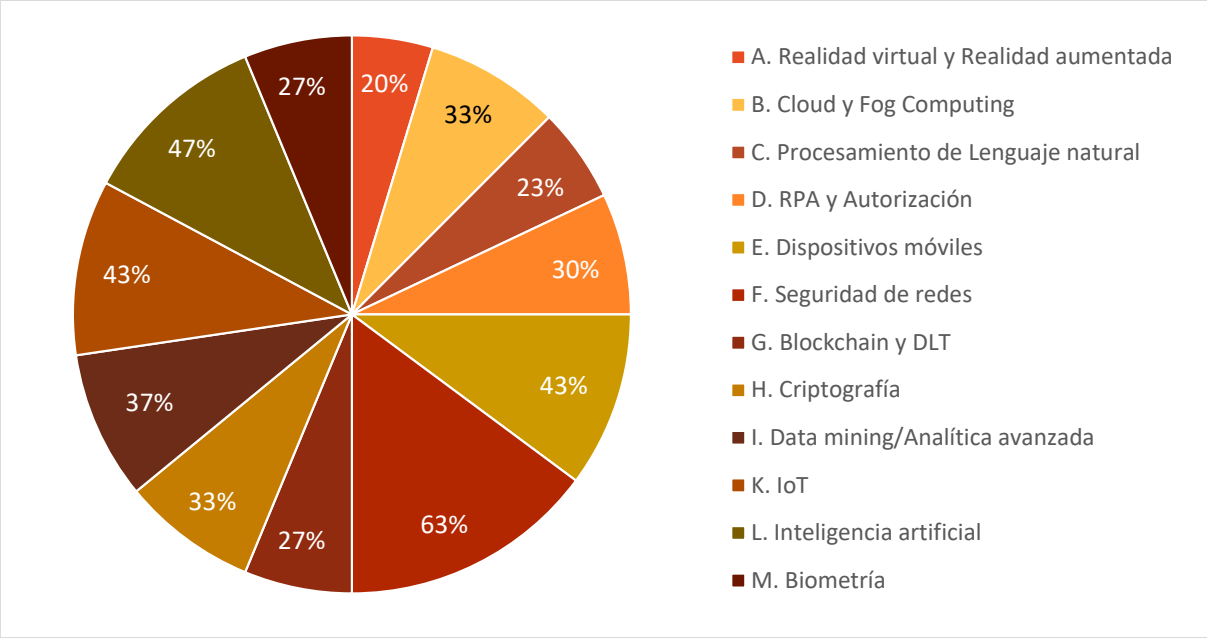


Figura 116. P58: Datos Tecnologías: Aplicación de las tecnologías a la ciberdefensa (corto o largo plazo)

Como se puede observar en las gráficas anteriores, entre el 20% y el 63% de entidades encuestadas indican que trabajarán a corto o largo plazo en la aplicación de estas tecnologías en el campo de la Ciberdefensa, principalmente en las tecnologías de **seguridad en redes, IOT, RPA y Automatización, dispositivos móviles,** blockchain **y DLT** e i**nteligencia artificial**. Destaca la preferencia de inversión de las entidades a corto plazo frente al largo plazo.

Por otro lado más de la mitad de las entidades no han identificado estas tecnologías dentro de su hoja de ruta por los motivos que se indican en los apartados siguientes; principalmente la **biometría**, el **procesamiento de lenguaje natural** y el cloud y fog computing.

A continuación, se analizan las respuestas recibidas para cada tecnología en esta área.

Tal y como indican los datos, se puede observar que solo la quinta parte de las entidades trabaja en aplicaciones de la tecnología de **realidad virtual y realidad aumentada** para la ciberdefensa a corto plazo y ninguna espera trabajar en ella a largo plazo. A raíz de los presentes datos y analizándolos junto con los de la pregunta 57, vemos que efectivamente parece haber interés de las entidades en desarrollar e integrar estas tecnologías en sus productos, aunque su aplicación a la ciberdefensa se centra en el corto plazo.

En el caso de la tecnología de cloud y fog computing, sólo un tercio de las entidades trabaja en su aplicación para la ciberdefensa a corto plazo y sólo una entidad espera trabajar en ella a largo plazo. Del análisis de estos datos y los de la pregunta 57, se aprecia el interés de las entidades en desarrollar e integrar esta tecnología en sus productos, aunque su aplicación a la ciberdefensa se centra en el corto plazo.

Para la tecnología de **procesamiento del lenguaje natural**, se observa que sólo la quinta parte de las entidades consultadas trabaja en su aplicación para la ciberdefensa a corto plazo y sólo una entidad espera trabajar en ella a largo plazo. Analizando estos datos y los de la pregunta 57, existe interés por parte de las entidades en desarrollar e integrar esta tecnología en sus productos, aunque su aplicación a la ciberdefensa se focaliza principalmente en el corto plazo.

En relación con la tecnología de **RPA y automatización**, la cuarta parte de las entidades consultadas trabaja en aplicaciones de la tecnología para la ciberdefensa a corto plazo y sólo una entidad espera trabajar en ella a largo plazo. Del análisis de estos datos y en conjunto con la pregunta 57, se aprecia interés de las entidades en desarrollar e integrar estas tecnologías en sus productos, pero su aplicación a la ciberdefensa se centra en el corto plazo.

Tal y como indican los datos, se puede observar que más de un tercio de las entidades trabaja en aplicaciones de la tecnología de **dispositivos móviles** para la ciberdefensa a corto plazo y sólo una entidad espera trabajar en ella a largo plazo. A raíz de estos datos y analizándolos con respecto a la pregunta 57, vemos que efectivamente existe un importante interés de las entidades en desarrollar e integrar esta tecnología en sus productos, aunque su aplicación a la ciberdefensa se centra en el corto plazo.

En el caso de la tecnología de **Seguridad de redes**, se observa que la mitad de las entidades consultadas trabaja en su aplicación para la ciberdefensa a corto plazo y otras tres entidades esperan hacerlo a largo plazo. Del análisis de estos datos y los de la pregunta

57, se deduce que hay un importante interés de las entidades en desarrollar e integrar esta tecnología en sus productos y su aplicación a la Ciberdefensa se estima en el corto plazo principalmente.

Para la tecnología de blockchain **y DLT**, sólo una minoría de las entidades consultadas trabaja en su aplicación para la ciberdefensa a corto plazo y otras cuatro entidades esperan hacerlo a largo plazo. Analizando estos datos y los de la pregunta 57, se observa que existe interés por parte de las entidades en desarrollar e integrar esta tecnología en sus productos. Aunque su aplicación a la ciberdefensa es baja en el corto plazo, resulta la tecnología con más proyección a largo plazo de las estudiadas.

En relación con la tecnología de **criptografía**, sólo un tercio de las entidades consultadas indica que trabajar en su aplicación para la ciberdefensa a corto plazo y sólo una entidad espera hacerlo a largo plazo. A raíz de los datos y analizándolos en conjunto con la pregunta 57, vemos que efectivamente hay interés de las entidades en desarrollar e integrar esta tecnología en sus productos, aunque su aplicación a la ciberdefensa se centra principalmente en el corto plazo.

Tal y como indican los datos, se puede observar que un tercio de las entidades consultadas trabaja en aplicaciones de la tecnología de data mining **y analítica avanzada** para la ciberdefensa a corto plazo y sólo una entidad espera estar trabajando a largo plazo. A raíz de los datos y analizándolos junto con la pregunta 57, vemos que existe interés de las entidades en desarrollar e integrar esta tecnología en sus productos, aunque su aplicación a la ciberdefensa se centra en el corto plazo.

En el caso de la tecnología de **IOT**, se observa que un tercio de las entidades consultadas trabaja en su aplicación para la ciberdefensa a corto plazo y sólo dos entidades esperan hacerlo a largo plazo. Analizando estos datos y los de la pregunta 57, se observa que existe interés por parte de las entidades en desarrollar e integrar esta tecnología en sus productos, aunque su aplicación a la ciberdefensa se centra en el corto plazo.

Para la tecnología de **inteligencia artificial**, casi la mitad de las entidades consultadas trabaja en aplicaciones para la ciberdefensa a corto plazo y solo dos entidades esperan hacerlo a largo plazo. Analizando estos datos y los de la pregunta 57, se observa interés de las entidades en desarrollar e integrar esta tecnología en sus productos, aunque su aplicación a la ciberdefensa se centra en el corto plazo.

En relación con la tecnología de **biometría**, sólo la quinta parte de las entidades consultadas trabaja en su aplicación para la ciberdefensa a corto plazo y solo dos entidades esperan hacerlo a largo plazo. A raíz de los datos y analizándolos con respecto a la pregunta 57, vemos que hay un relativo interés de las entidades en desarrollar e integrar esta tecnología en sus productos, y que su aplicación a la ciberdefensa se centra en el corto plazo. Cabe destacar que más de la mitad de las entidades encuestadas no contempla está tecnología en su mapa de ruta ni su aplicación en ciberdefensa.

Como conclusión del apartado **aplicación del sector de la ciberdefensa**, se puede extraer que, en el corto plazo, la Seguridad en las redes, la Inteligencia Artificial y los Dispositivos móviles son las tecnologías en las que más se están enfocando las entidades consultadas.

En el largo plazo, pocas entidades han mostrado interés en el desarrollo de estas tecnologías, aunque destacan sobre el resto *blockchain* y seguridad en redes.

Inversión I+D+i

La apuesta por la inversión en I+D+i dentro de las entidades en los diferentes ámbitos tecnológicos, puede indicar qué evolución de mercado de cara al futuro están contemplando las entidades encuestadas. A continuación, se recogen los datos de inversión en I+D+i de las distintas entidades que han participado en este análisis.

Los datos recogidos en la pregunta 59. *¿Cuál es el presupuesto anual de su empresa para proyectos de I+D+i en este tipo de tecnologías que pudieran ser aplicables en el ámbito de la Ciberdefensa?, en el siguiente marco económico:* "No dispongo de presupuesto, menos de 100.000€, de 100.001€ a 500.000€, más de 500.000€", se muestran en la siguiente figura:

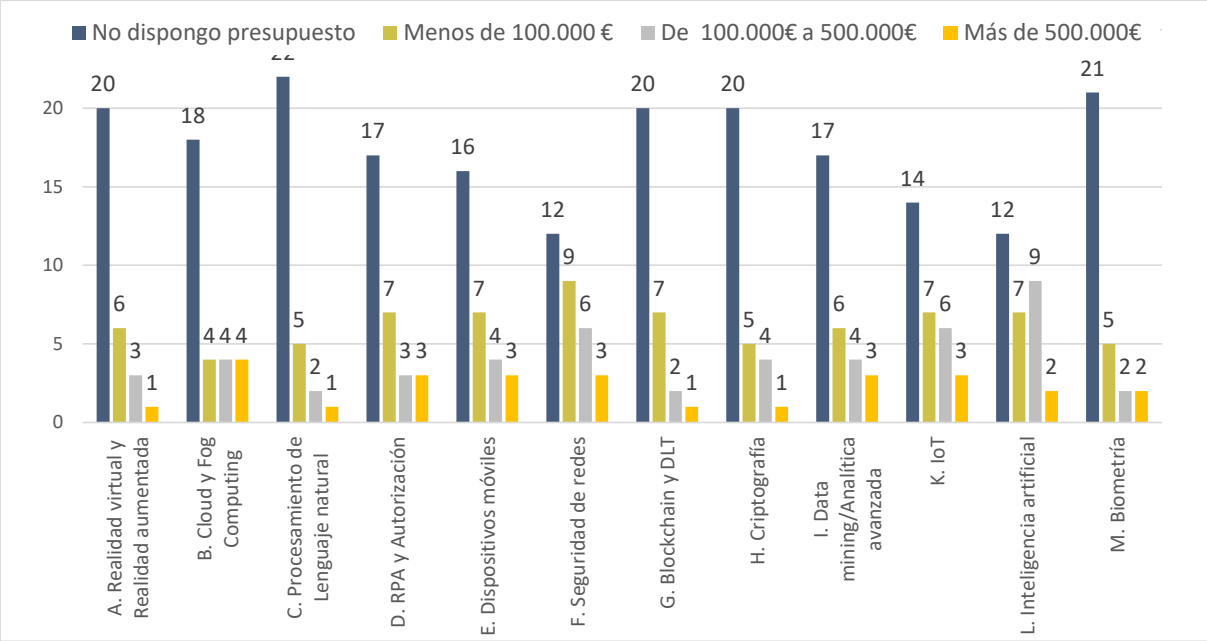


Figura 117. P59: Datos I+D+I: Inversiones en I+D+i en las diferentes tecnologías

La representación gráfica de los datos de las entidades con algún tipo de inversión en I+D+i para el desarrollo de estas tecnologías se muestra en la siguiente figura:

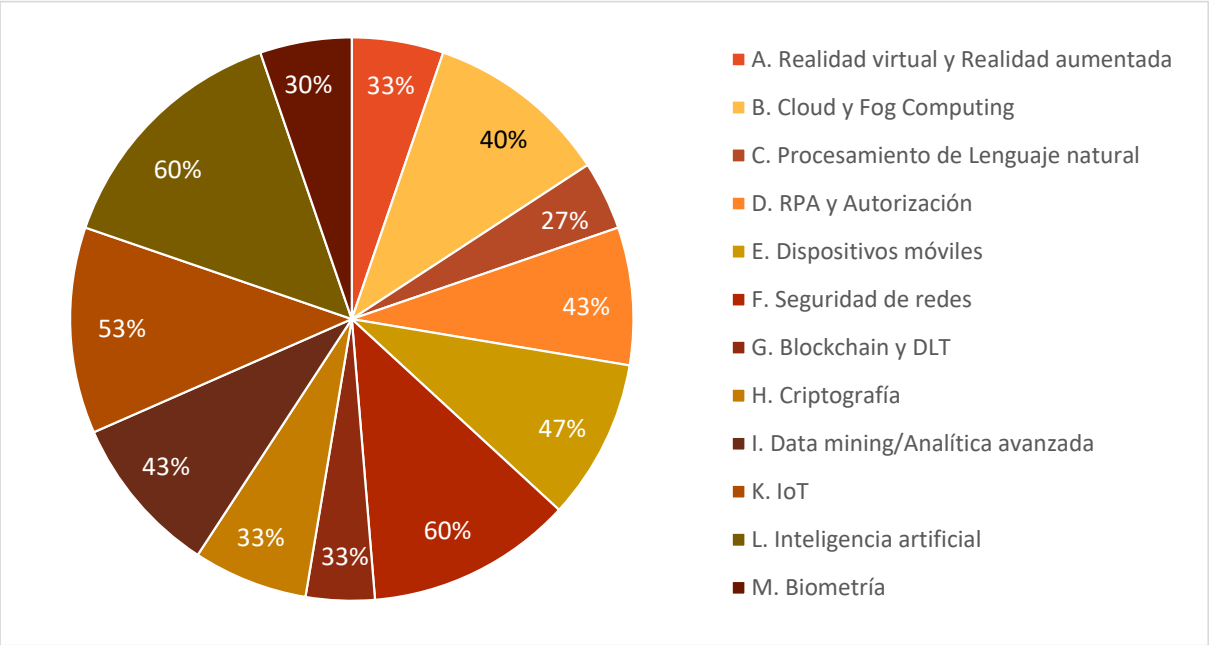


Figura 118. P59: Gráfico. I+D+I: Inversiones en I+D+i en las diferentes tecnologías (Disponen de inversión)

Como se puede observar en las gráficas anteriores, entre el 27% y el 60% de las entidades encuestadas indica que dispone de algún tipo de inversión para desarrollos I+D+i en estas tecnologías, entre las que destacan **seguridad en redes e inteligencia artificial** con interés de más de la mitad de las entidades.

Las tecnologías con menos inversiones en I+D+i son **procesamiento de lenguaje natural, biometría, realidad virtual y realidad aumentada,** blockchain **y DLT,** data mining **y criptografía.**

A continuación, se analizan las respuestas recibidas para cada tecnología en esta área.

Tal y como indican los datos, se puede observar que más de la mitad de las entidades consultadas no dispone de presupuesto para trabajar en aplicaciones de la tecnología de **realidad virtual y realidad aumentada** para la ciberdefensa. De hecho, sólo una entidad indica que dispone más de 500.000€ para inversiones y la quinta parte entre 100.000€ y 500.000€. Atendiendo a estos datos y las respuestas a las preguntas 57 y 58, se extrae que estos valores se modificarán e incrementarán a largo plazo. Parece interesante destacar que, siendo una tecnología de interés para las entidades, el volumen de inversión propia parece escaso.

En el caso de la tecnología de cloud y fog computing, se observa que más de la mitad de las entidades consultadas no dispone de presupuesto para trabajar en aplicaciones de esta tecnología en la ciberdefensa; cuatro entidades indican que disponen más de 500.000€ y sólo una minoría dispone entre 100.000€ y 500.000€. De estos datos, junto con los obtenidos en las preguntas 57 y 58, se deduce que estos valores se modificarán e

incrementarán a largo plazo. Aun siendo una tecnología de interés para las entidades, el volumen de inversión se estima escaso.

Para la tecnología de **procesamiento de lenguaje natural**, tres cuartas partes de las entidades consultadas no disponen de más presupuesto para su desarrollo en ciberdefensa. Solo una entidad indica que dispone de más de 500.000€ y una minoría indica que cuenta con un presupuesto de entre 100.000€ y 500.000€. Analizando estos datos junto con los de las preguntas 57 y 58, se deduce que estos valores se podrán modificar e incrementar moderadamente a largo plazo.

En relación con la tecnología de **RPA y automatización** aplicada a ciberdefensa, más de la mitad de las entidades consultadas no dispone de presupuesto para trabajar en ella. Sólo tres entidades indican que disponen más de 500.000€, mientras que una minoría indica que cuenta con un presupuesto entre 100.000€ y 500.000€. De estos datos, junto con los obtenidos en las preguntas 57 y 58, se obtiene que estos valores se modificarán e incrementarán a largo plazo. Aunque sea para la aplicación a la ciberdefensa a largo plazo, la mitad de las encuestadas indica disponer de cierto volumen de inversión propia, quizás pensando en la dualidad de esta tecnología.

Tal y como indican los datos, se puede observar que la mitad de las entidades consultadas no dispone de presupuesto para trabajar en aplicaciones de la tecnología de **dispositivos móviles** para la ciberdefensa. Sólo tres entidades indican disponer de más de 500.000€, una minoría entre 100.000€ y 500.000€, y el resto por debajo de los 100.000€. Atendiendo a los datos obtenidos en esta pregunta y las respuestas a las preguntas 57 y 58, se extrae que estos valores se incrementarán a largo plazo. Es interesante destacar que, siendo una tecnología claramente de interés para las entidades, el volumen de inversión propia parece escaso.

En el caso de la tecnología de **seguridad de redes**, se observa que casi la mitad de las entidades consultadas no dispone de presupuesto para ella. Sólo tres entidades indican que disponen más de 500.000€, mientras que una minoría de entre 100.000€ y 500.000€, y un tercio por debajo de los 100.000€. De estos datos, junto con los obtenidos en las preguntas 57 y 58, se deduce que estos valores se incrementarán a largo plazo. Pero, aun siendo una tecnología de gran interés para las entidades, su volumen de inversión parece escaso.

Para la tecnología de blockchain **y DLT**, la mayoría de las entidades consultadas no dispone de presupuesto para trabajar en su aplicación a la ciberdefensa. Sólo una entidad indica que dispone más de 500.000€, mientras que una pequeña parte indica que cuenta con un presupuesto entre 100.000€ y 500.000€ y la cuarta parte de menos de 100.000€. Analizando estos datos junto con los de las preguntas 57 y 58, se observa que estos valores se incrementarán a largo plazo.

En relación con la tecnología de **criptografía**, se observa que la mayoría de las entidades consultadas no dispone de presupuesto para ella. Sólo una entidad indica que dispone de más de 500.000€ y la minoría entre 100.000€ y 500.000€ o menos. De estos datos, junto con los obtenidos en las preguntas 57 y 58, se obtiene que estos valores se modificarán e incrementarán a largo plazo. Aunque sea para la aplicación a la ciberdefensa a largo plazo, su volumen de inversión se considera escaso.

Tal y como indican los datos, se puede observar que más de la mitad de las entidades consultadas no dispone de presupuesto para trabajar en aplicaciones de la tecnología data mining **y analítica avanzada** a la ciberdefensa. Sólo tres entidades indican disponer de más de 500.000€, mientras una pequeña parte cuenta con un presupuesto entre 100.000€ y 500.000€ y una quinta parte por debajo de 100.000€. Atendiendo a los datos obtenidos en esta pregunta y las respuestas a las preguntas 57 y 58, se extrae que estos valores se incrementarán a largo plazo. Es interesante destacar que, siendo una tecnología, como se indica en las respuestas anteriores, claramente de interés para las entidades, el volumen de inversión propia parece escaso.

En el caso de la tecnología de **inteligencia artificial,** casi la mitad de las entidades no dispone de presupuesto para trabajar en su aplicación a la ciberdefensa. Sólo dos entidades indican que disponen de más de 500.000€, un tercio entre 100.000€ y 500.000€ y una cuarta parte por debajo de 100.000€. De estos datos, junto con los obtenidos en las preguntas 57 y 58, se deduce que estos valores se incrementarán a largo plazo. Aun siendo una tecnología de interés, el volumen de inversión propia parece moderado.

Para la tecnología de **biometría**, se observa que casi tres cuartas partes de las entidades consultadas no disponen de presupuesto para ella. Sólo dos entidades indican disponer de más de 500.000€, mientras que una minoría cuenta con un presupuesto entre 100.000€ y 500.000€ y el resto por debajo de 100.000€. Analizando estos datos junto con los de las preguntas 57 y 58, se cree que estos valores no se incrementarán a largo plazo por su escaso interés en el desarrollo de soluciones de ciberdefensa.

Como conclusión del apartado **inversión I+D+i,** es interesante reseñar que, de aquellas entidades con inversión en I+D+i para estas tecnologías, alrededor de la mitad de ellas ofrece valores de menos de 100.000€ y no llegan a la cuarta parte las que aportan más de 500.000€. La Seguridad en las redes y la Inteligencia Artificial parecen ser las apuestas en I+D+i por parte de las entidades.

Barreras tecnológicas

Los desarrollos e implementaciones en los diferentes ámbitos tecnológicos se pueden ver afectados por distintas barreras tecnológicas. A continuación, se recogen los datos sobre las barreras propuestas que han podido afectar en la implementación o el desarrollo de las distintas tecnologías por parte de las entidades participantes.

Los datos recogidos en la pregunta 60. *¿Qué principales barreras se están encontrando a la hora de implementar o desarrollar este tipo de tecnologías?* se muestran en la siguiente figura:

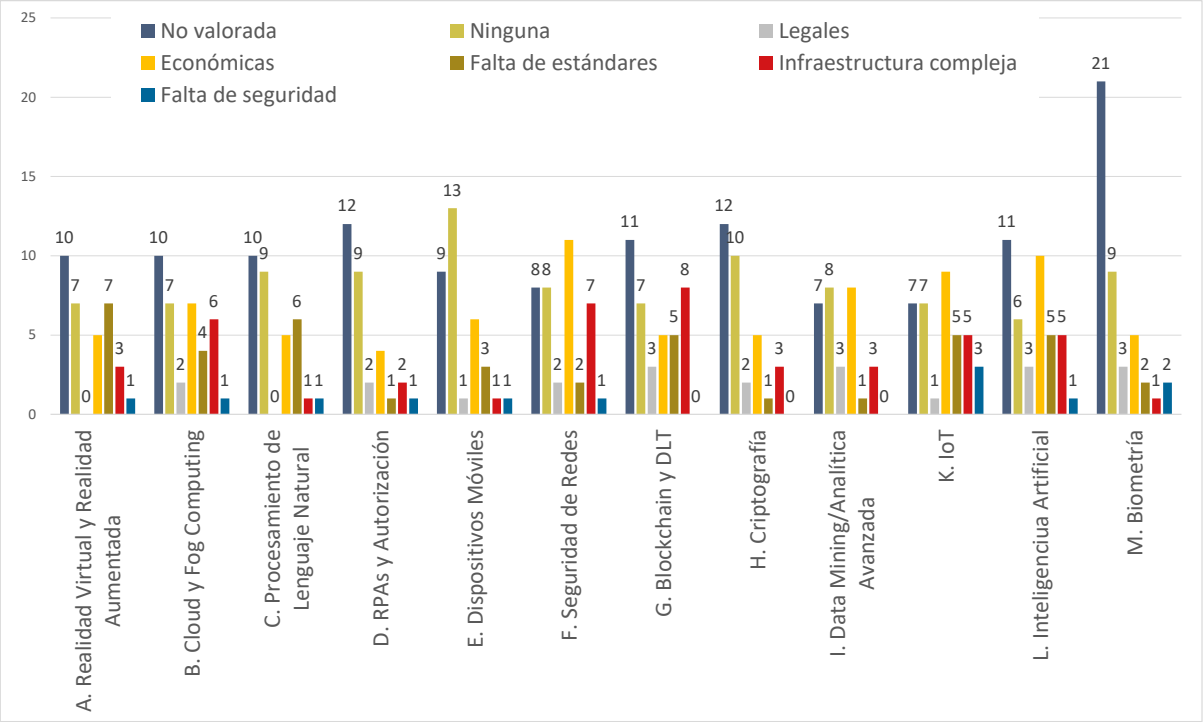


Figura 119. P60: Datos barreras tecnológicas

La representación gráfica de los datos de las barreras tecnológicas encontradas en el conjunto de tecnologías tratadas se muestra en la siguiente figura:

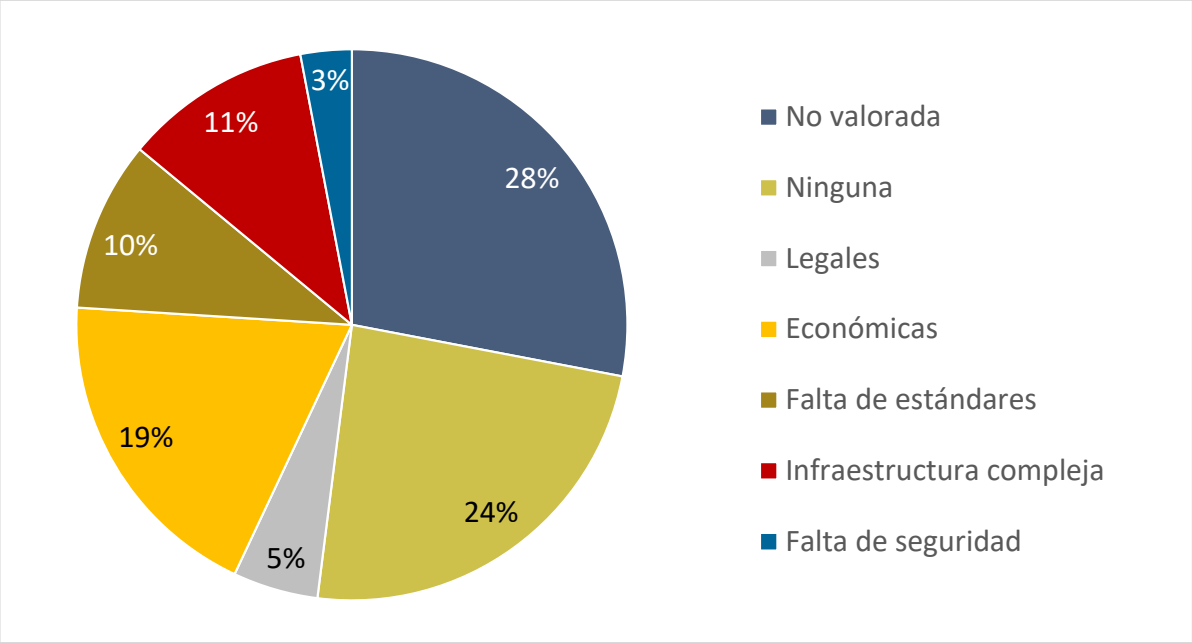


Figura 120. P60: Gráfico. Barreras tecnológicas

Un cuarto de las respuestas no han entrado a valorar las barreras que han encontrado. Esto se debe a que no todas las entidades desarrollan todas las tecnologías.

Según los datos obtenidos para las tecnologías de **realidad virtual y aumentada** y cloud **y** fog computing, cabe destacar que casi un tercio de las entidades no se ha encontrado barreras tecnológicas. De las entidades que sí lo hicieron, casi un tercio de las barreras se deben a la falta de estándares o a temas económicos.

En el caso de la tecnología de **procesamiento de lenguaje natural**, las principales barreras que se encuentra la cuarta parte de las entidades son la falta de estándares y otra quinta parte indica que son de tipo económicas. Destaca que un tercio de las entidades no ha encontrado barreras al afrontar esta tecnología.

Para las tecnologías **RPA y automatización** y **dispositivos móviles**, las principales barreras que se encuentran la cuarta parte de las entidades son las Económicas y, en menor medida, la falta de estándares. Cabe destacar que casi la mitad de las entidades no ha encontrado barreras al afrontar esta tecnología.

En relación con la tecnología de **seguridad de redes**, las principales barreras que se encuentran las entidades son mayoritariamente las Económicas. Destaca que la cuarta parte de las entidades no encuentra barreras al afrontar esta tecnología.

En el caso de la tecnología de Blockchain **y DLP**, la principal barrera que se encuentran las entidades es la Infraestructura compleja que requiere. Otras barreras señaladas son las económicas y la falta de estándares. Cabe destacar que una cuarta parte de las entidades no encuentran barreras al afrontar esta tecnología.

Para la tecnología de **criptografía**, las principales barreras que se encuentran aquellas entidades son laseconómicas o la infraestructura requerida. Destaca que casi la mitad de las entidades no encuentran barreras al afrontar esta tecnología.

En relación con la tecnología de data mining y **analítica avanzada**, la principal barrera que se encuentran las entidades son económicas. En este caso reseñan también las Legales y la Infraestructura necesaria. Cabe destacar que un tercio de las entidades no encuentran barreras al afrontar esta tecnología.

En el caso de las tecnologías de **IOT** y la **inteligencia artificial**, las principales barreras que se encuentran las entidades son las económicas. Se reseñan también la falta de estandares y la Infraestructura requerida. Destaca que un cuarto de las entidades no encuentra barreras al afrontar esta tecnología.

Para la tecnología de **biometría**, las principales barreras que se encuentran las entidades son las económicas y las legales. Es reseñable que casi la mitad de las entidades no encuentran barreras al afrontar esta tecnología.

Como conclusión del apartado de **barreras tecnológicas**, del volumen de respuestas obtenido cabe destacar el alto número de entidades, una cuarta parte, que no encuentra ningún tipo de barrera en el desarrollo e implementación de estas tecnologías. Sin embargo, para aquellas que sí las han encontrado, los principales escollos han sido el **aspecto económico**, la **falta de estándares** relacionados y la **compleja infraestructura requerida**. Como dato adicional, casi una cuarta parte de las entidades no ha valorado alguna de las doce tecnologías tratadas al no desarrollarlas en su organización.

7.2. Realidad virtual y realidad aumentada

El análisis de las respuestas sobre esta tecnología se desglosa en **dos áreas** que se detallan a continuación:

Actividades más relevantes para su organización

Los datos recogidos en la pregunta 61. *En su opinión, ¿Cuál de las siguientes actividades relacionadas con la ciberdefensa relacionadas con la realidad virtual o la realidad aumentada considera más relevante para su organización?* se muestran en la siguiente figura:

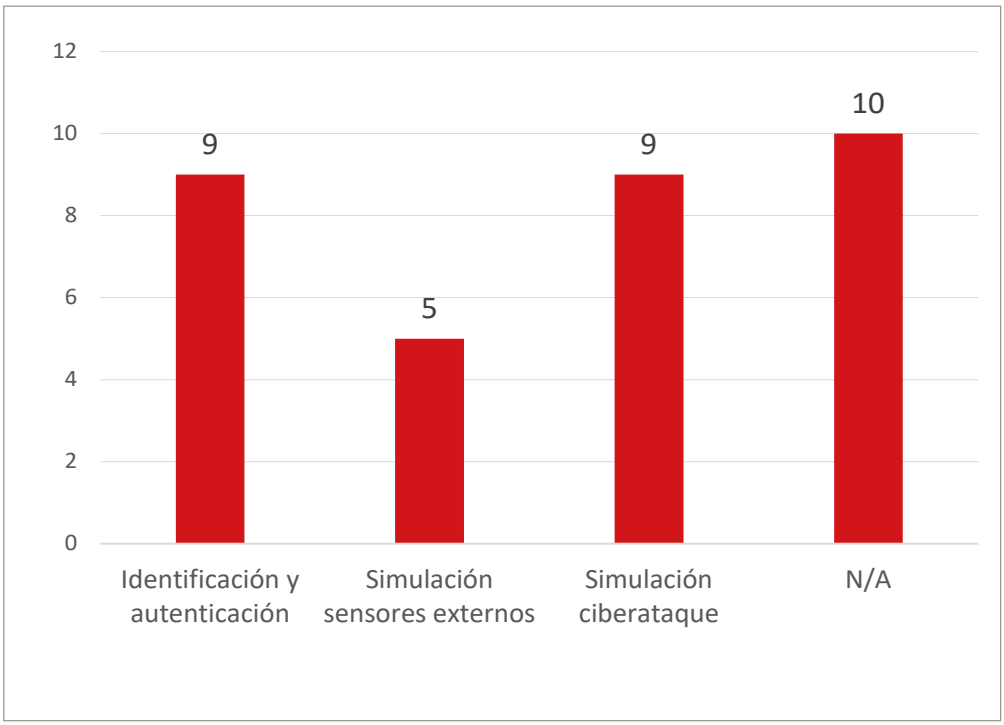


Figura 121. P61: Datos Actividades de la realidad virtual o la realidad aumentada más relevantes para su organización

La representación gráfica de estos datos se muestra en la siguiente figura:

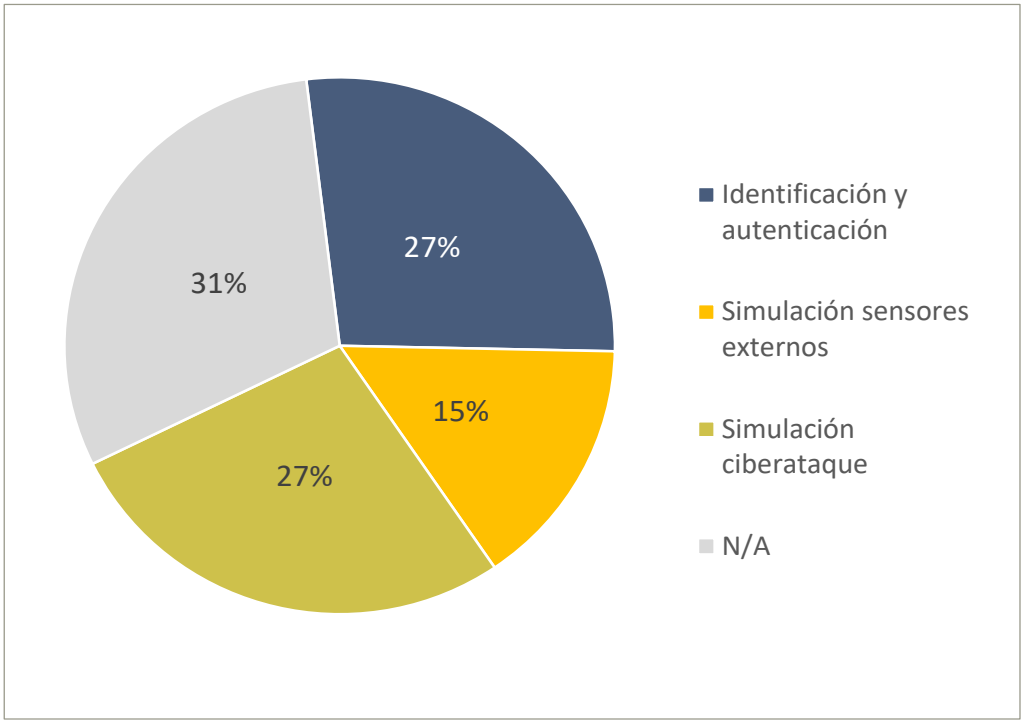


Figura 122. P61: Gráfico. Actividades de la realidad virtual o la realidad aumentada más relevantes para su organización

Hay que aclarar que no existía límite de respuestas por entidad, por lo que los tipos definidos no son excluyentes entre sí.

Se puede observar que los aspectos más importantes para las organizaciones en relación son la aplicación de la realidad virtual o la realidad aumentada, son la **identificación y autentificación y la simulación de ciberataques**, ambas con un 27%. La mayoría de las organizaciones no están implementando esta tecnología ni muestran interés en implementarla en un futuro próximo, en concreto, el 31% de ellas no la valoran. Por todo esto, se puede determinar que esta tecnología no está muy asentada, pues las organizaciones que las están implementando, mayoritariamente lo están haciendo en las fases más iniciales (identificación y autenticación y simulación de ciberataque), siendo una minoría las que se encuentran implementando las opciones más avanzadas (**simulación de sensores externos**).

Actividades más relevantes para ciberdefensa

Los datos recogidos en la pregunta 62. *En su opinión, ¿Cuál de las siguientes actividades relacionadas con la ciberdefensa relacionadas con la realidad virtual o la realidad aumentada considera más relevante para su organización?* se muestran en la siguiente figura:

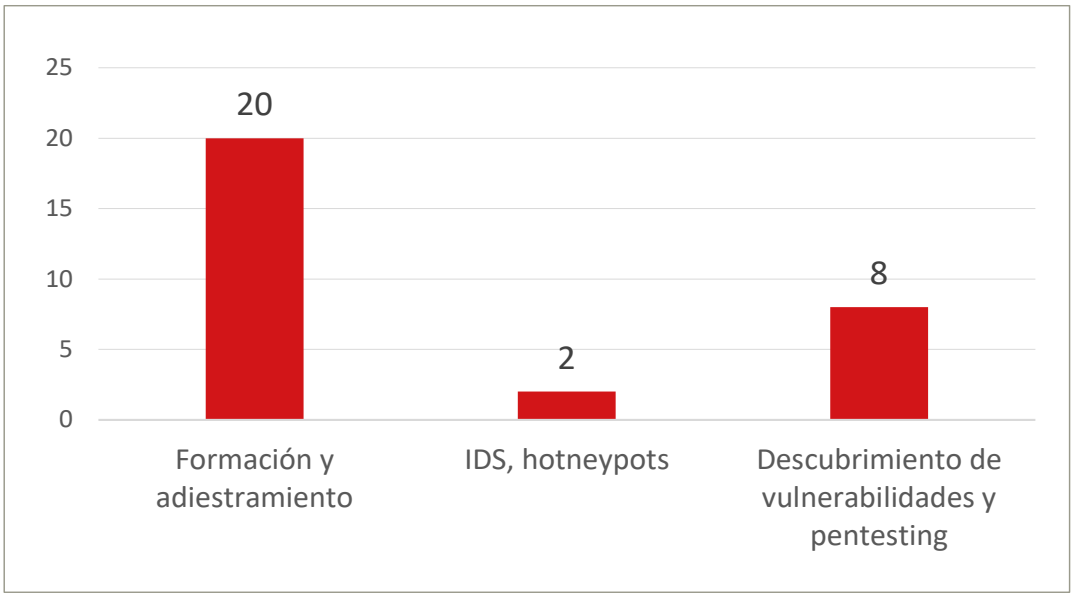


Figura 123. P62: Datos actividades de la realidad virtual o la realidad aumentada más relevantes para ciberdefensa

La representación gráfica de estos datos se muestra en la siguiente figura:

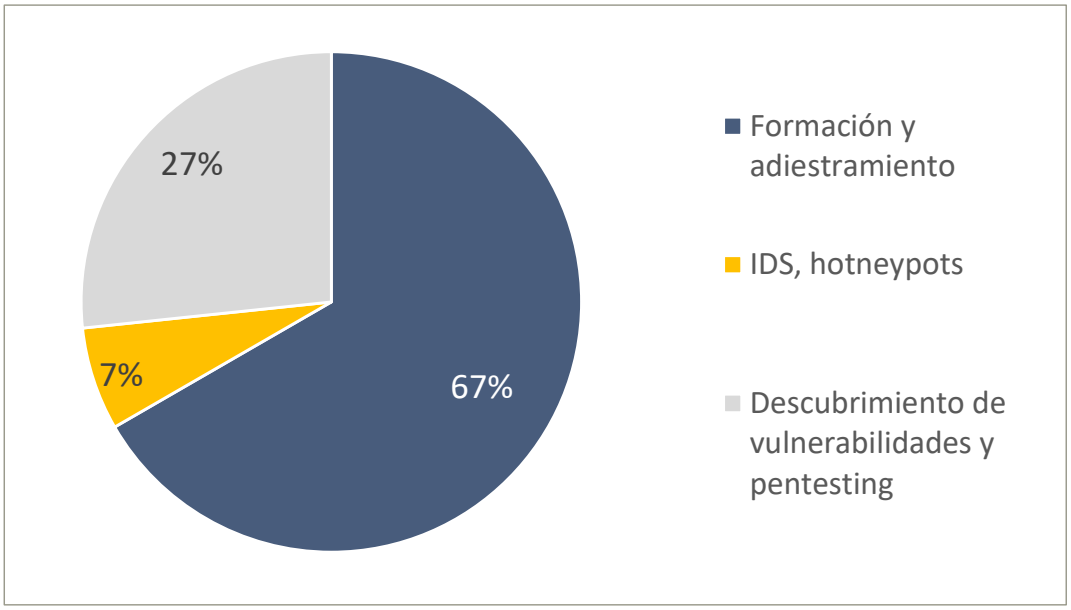


Figura 124. P62: Gráfico. Actividades de la realidad virtual o la realidad aumentada más relevantes para ciberdefensa

Hay que aclarar que no existía límite de respuestas por entidad, por lo que los tipos definidos no son excluyentes entre sí.

Ante las respuestas obtenidas, queda totalmente claro que esta tecnología se identifica actualmente para ser aplicada en la Ciberdefensa, como un medio para realizar **formación y adiestramiento** con un 67% y no con objetivos operativos. En menor medida, con un 27%, también se identifica para ser utilizada como ayuda para el **descubrimiento de vulnerabilidades y realización de** pentesting. Solo en unos pocos casos se identifica como medio para implementar ayudas para la monitorización y detección (como pueden ser los **IDS o los** honeypots**)**, por lo que, de momento, parece ser que esta opción está enfocada a la implementación en algún caso muy específico.

También es interesante resaltar que, aunque esta tecnología no se encuentra en una fase madura dentro de las propias organizaciones, es bastante relevante dado que el 80% de las entidades ha respondido a esta pregunta

A diferencia de otras tecnologías, la realidad virtual y la realidad aumentada no son vistas por las entidades como un ámbito de desarrollo de interés y únicamente la están empleando para tareas muy básicas, para lo que han externalizado su adquisición en proveedores externos.

7.3. *Cloud y fog computing*

El análisis de las respuestas esta tecnología se desglosa en **dos áreas** que se detallan a continuación:

Actividades más relevantes para ciberdefensa

Los datos recogidos en la pregunta *63. En su opinión, ¿Cuál de las siguientes actividades relacionadas con cloud y fog computing considera más relevante para aplicarlas en el sector de la ciberdefensa? (Marque dos únicamente)* se muestran en la siguiente figura:

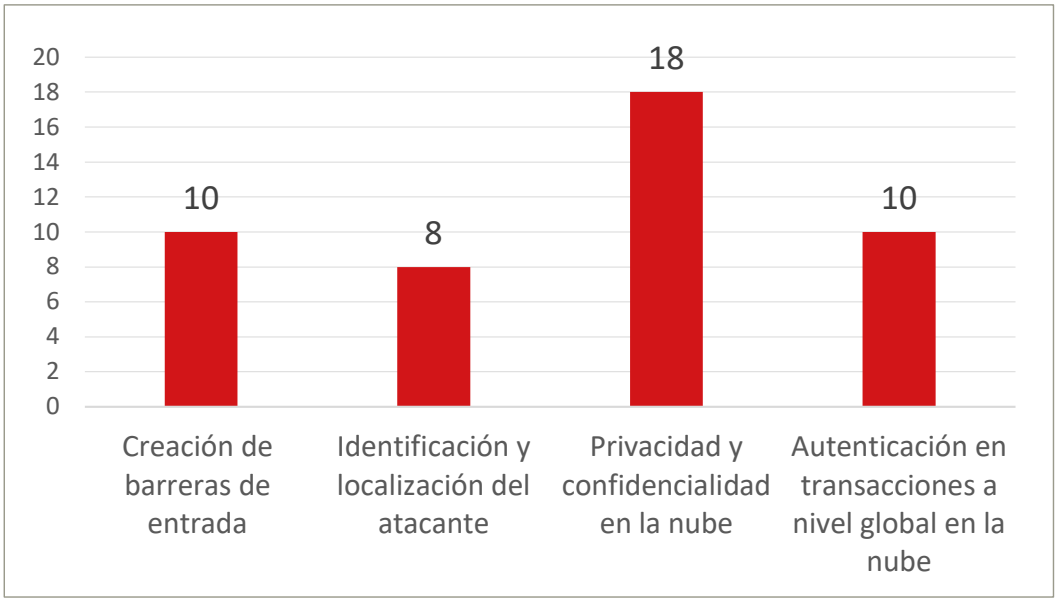


Figura 125. P63: Datos actividades de cloud y fog computing más relevantes para ciberdefensa

La representación gráfica de estos datos se muestra en la siguiente figura:

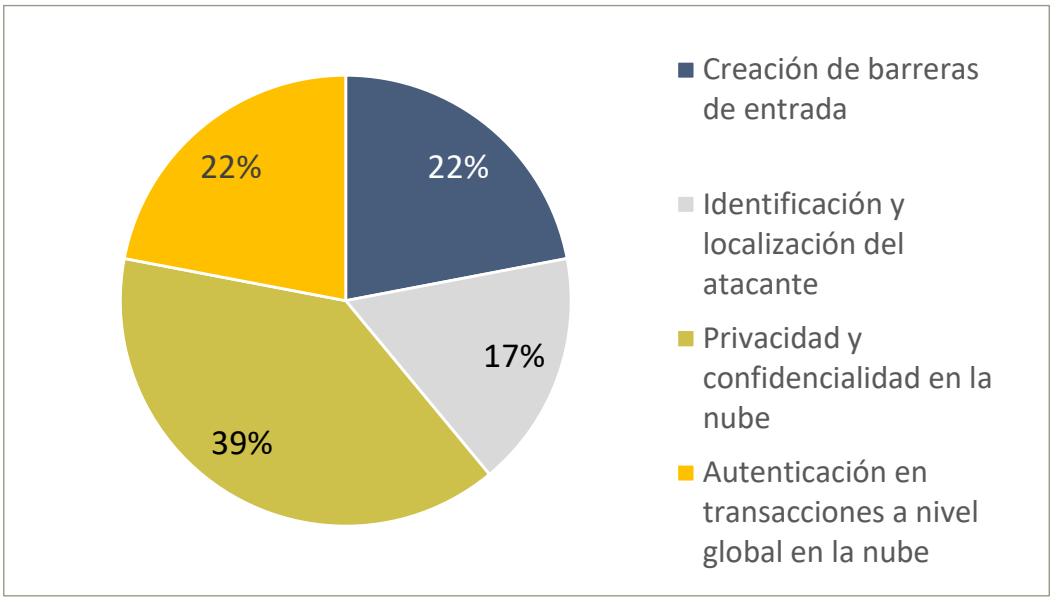


Figura 126. P63: Gráfico. Actividades de cloud y fog computing más relevantes para ciberdefensa

Al permitirse dos respuestas como máximo por entidad los tipos definidos no son excluyentes entre sí.

Se puede observar que el aspecto más importante para esta tecnología es ser capaz de mantener la **privacidad y confidencialidad**, que se corresponde con el 39% de las respuestas. Para apoyar este aspecto se considera también relevante poder **crear barreras de entrada** y **autenticar las transacciones**, con un 22%, mientras que la **identificación y localización de posibles ataques** es la menos votada con un 17% y, por tanto, no es considerada tan crítica, siempre que seamos capaces de garantizar que no tienen éxito.

Modalidad de servicios más utilizada en ciberdefensa

Los datos recogidos en la pregunta 64. *De dichos servicios ofrecidos, ¿Cuál es la modalidad más utilizada para el ámbito de la Ciberdefensa?* se muestran en la siguiente figura:

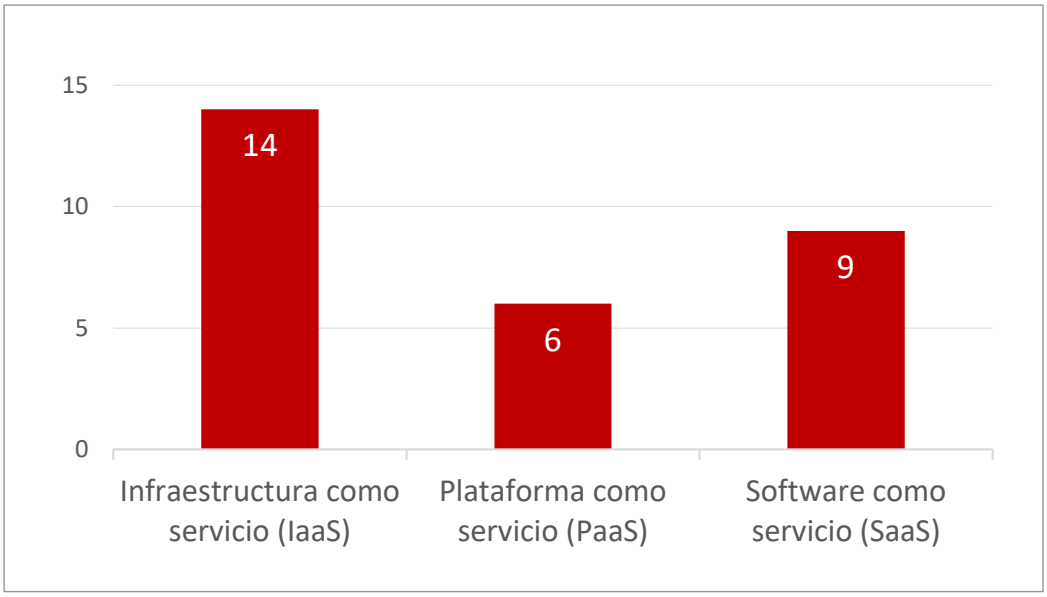


Figura 127, P64: Datos modalidad de cloud y fog computing más utilizado para ciberdefensa

La representación gráfica de estos datos se muestra en la siguiente figura:

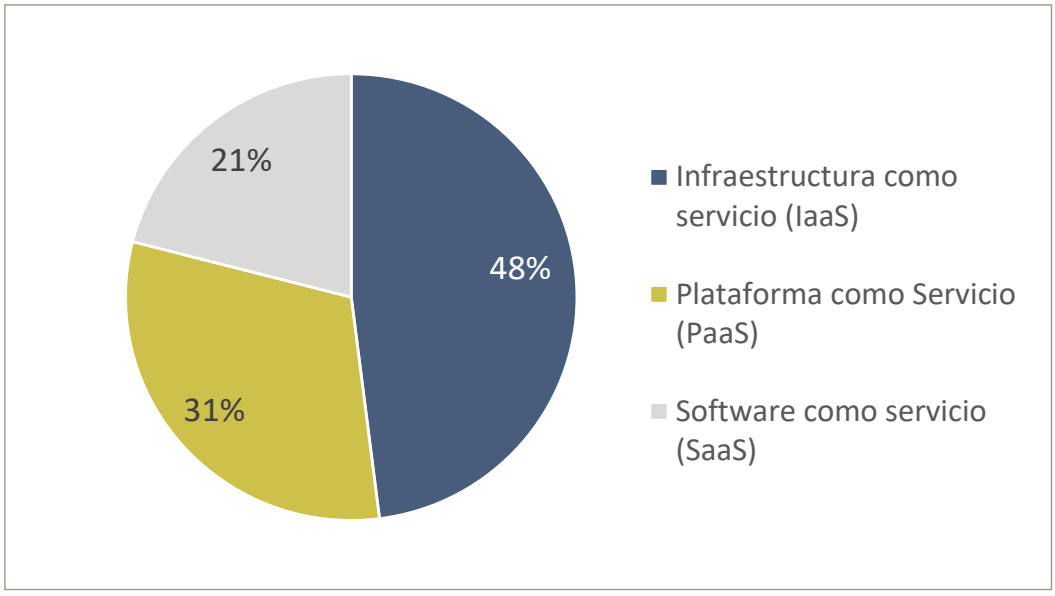


Figura 128. P64: Gráfico. modalidad de cloud y fog computing más utilizado para ciberdefensa

Se puede observar que la modalidad más utilizada para esta tecnología es la de **infraestructura como servicio** (IaaS) con un 48%, seguida por su uso como software **como servicio** (SaaS) con un 31% y por último la opción de **plataforma como servicio** (PaaS) con un 21%. Queda claro que se tiende a considerar más relevantes las aproximaciones más globales que puedan resultar útiles en todos los contextos, mientras que las aplicaciones para plataformas específicas, que hace no muchos años eran la tendencia más extendida, son consideradas las menos relevantes.

Como conclusión de este apartado, es destacable que cada vez más las organizaciones están recurriendo a proveedores externos, incluso para requerimientos con un relevante nivel de seguridad, al contrario del empleo tradicional de elementos propios y dedicados.

7.4. Procesamiento de lenguaje natural

El análisis de las respuestas sobre esta tecnología se desglosa en **dos áreas** que se detallan a continuación:

Actividades más relevantes para ciberdefensa

Los datos recogidos en la pregunta 65. *En su opinión, ¿Cuál de las siguientes actividades considera más relevante para aplicarlas en el sector de la ciberdefensa?* se muestran en la siguiente figura:

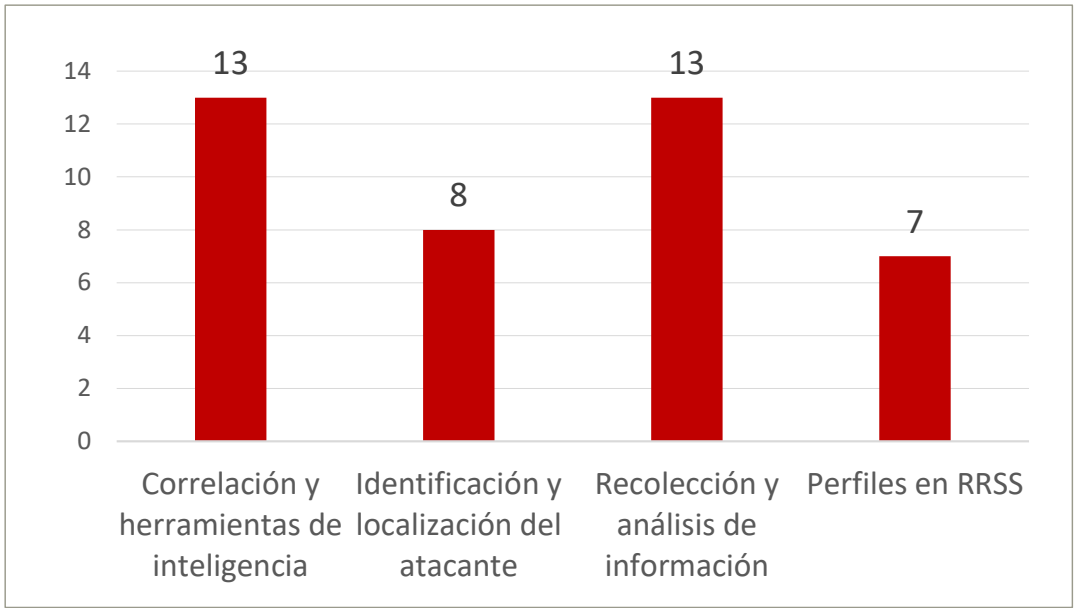


Figura 129. P65: Datos actividades de procesamiento de lenguaje natural más relevantes para ciberdefensa

La representación gráfica de estos datos se muestra en la siguiente figura:

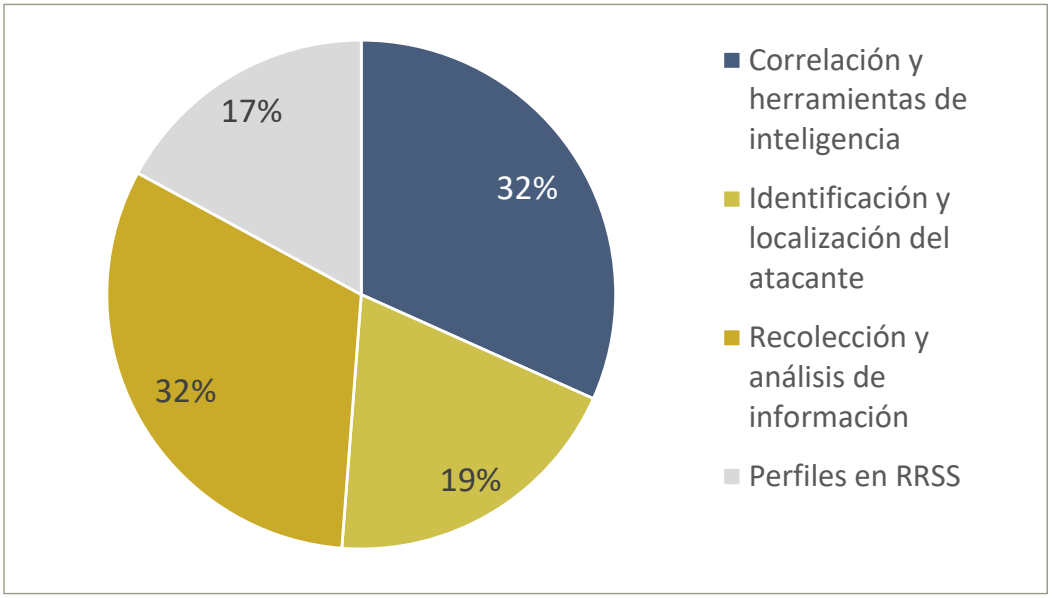


Figura 130. P65: Gráfico. Actividades de procesamiento de lenguaje natural más relevantes para ciberdefensa

Se puede observar que las actividades más relevantes de esta tecnología, con un 32% ambas, son la **recolección y análisis de información**, junto con la capacidad de poder **correlar esta información** usando herramientas de inteligencia. Otras actividades como el **análisis de perfiles en redes sociales**, o la **identificación de posibles atacantes** son consideradas de menos importancia.

Es reseñable que una minoría de las entidades no ha respondido a esta pregunta lo que denota que no utilizan esta tecnología de una forma habitual.

Aplicaciones más relevantes en ciberdefensa

Los datos recogidos en la pregunta 66. *De las siguientes aplicaciones, ¿cuáles considera más relevantes en el ámbito de la Ciberdefensa?* se muestran en la siguiente figura:

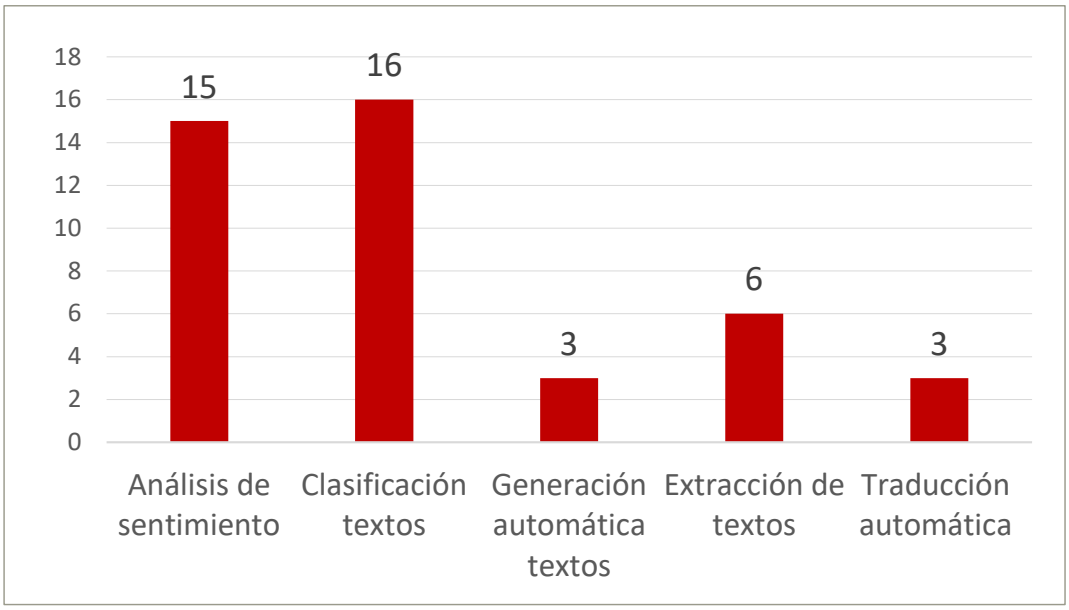


Figura 131- P66: Datos aplicaciones de procesamiento de lenguaje natural más relevantes para ciberdefensa

La representación gráfica de estos datos se muestra en la siguiente figura:

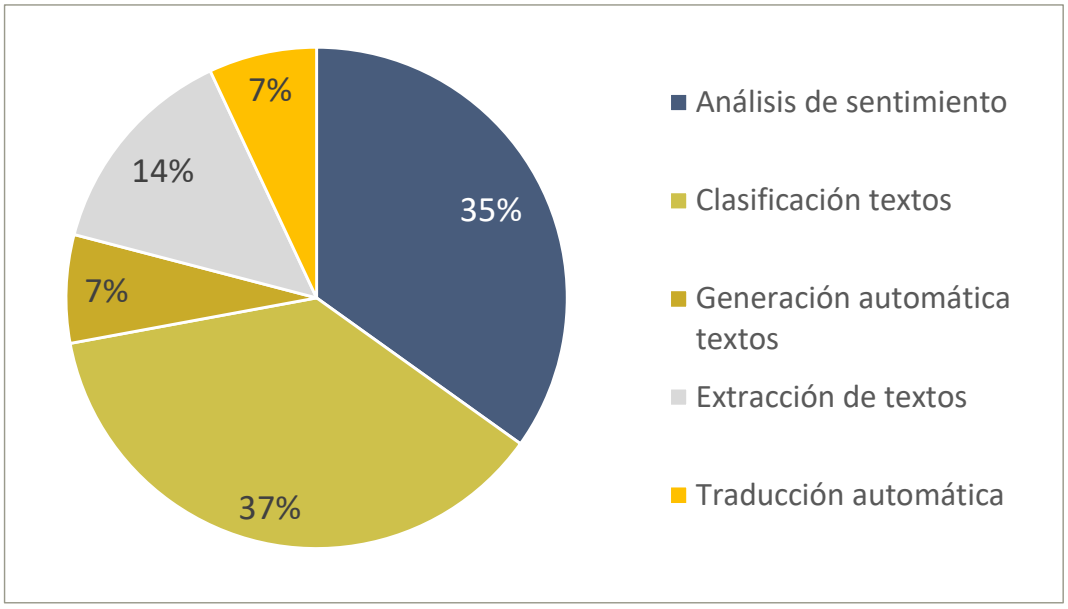


Figura 132- P66: Gráfico.Aplicaciones de procesamiento de lenguaje natural más relevantes para ciberdefensa

Al permitirse dos respuestas como máximo por entidad los tipos definidos no son excluyentes entre sí.

Se puede observar que la opción más relevante para esta tecnología, con un 37%, es la de **clasificación de textos**, seguida muy de cerca por el **análisis de sentimiento** con un 35%. La **extracción de textos** también es seleccionada con un 14%, lo que junto a la primera selección indica que esta tecnología está muy orientada al procesamiento automático de textos para poder realizar un primer filtrado de las grandes cantidades de información disponibles, con el objetivo de permitir un análisis posterior por parte de los analistas. La **generación automática de textos** y la **traducción automática** son las menos nombradas, lo que indica un papel secundario en el contexto actual.

Es destacable que solo una parte pequeña de las entidades no ha respondido a esta pregunta lo que denota que la mayoría de las entidades consideran de interés la aplicación de esta tecnología.

Esta capacidad se emplea esencialmente para automatizar parcialmente las tareas de los analistas. Dada la cada vez más creciente cantidad de información que se debe analizar, el uso de herramientas automáticas capaces de realizar una selección preliminar que se considera de gran utilidad. Esto podría, además, hacer más productivas sus funcionalidades.

7.5. RPA y automatización

El análisis de las respuestas sobre esta tecnología se desglosa en **dos áreas** que se detallan a continuación:

Actividades más relevantes para ciberdefensa

Los datos recogidos en la pregunta 67. *¿En cuáles de las siguientes actividades relacionadas con la Ciberdefensa cree que su organización desarrollará capacidades avanzadas en los próximos 2 años?* en relación con RPA (*robotic process automation*) y automatización de auditorias, se muestran en la siguiente figura:

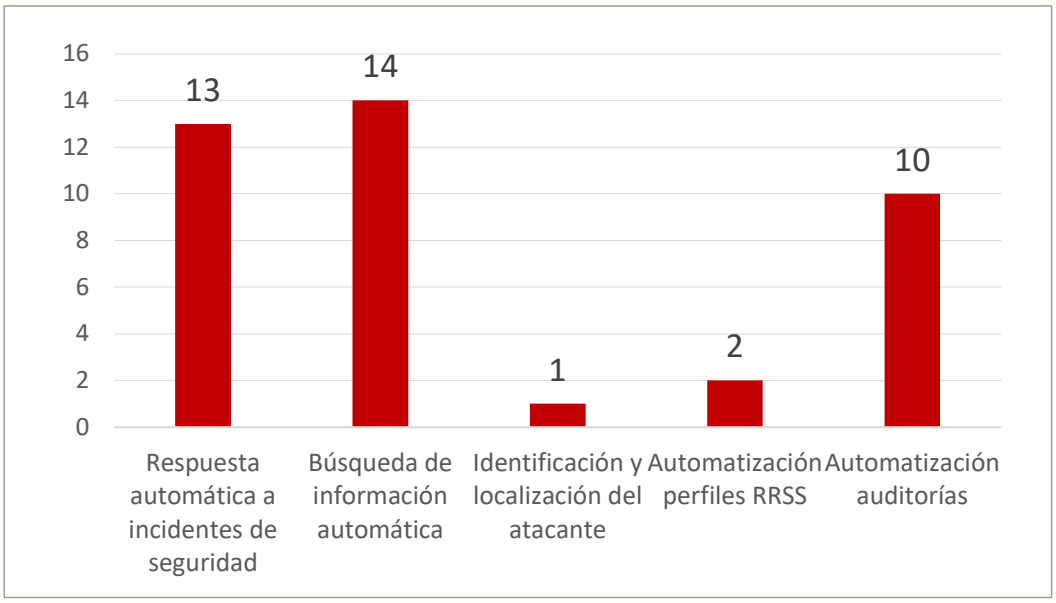


Figura 133. P67: Datos RPA y automatización. Actividades más relevantes para ciberdefensa

La representación gráfica de estos datos se muestra en la siguiente figura:

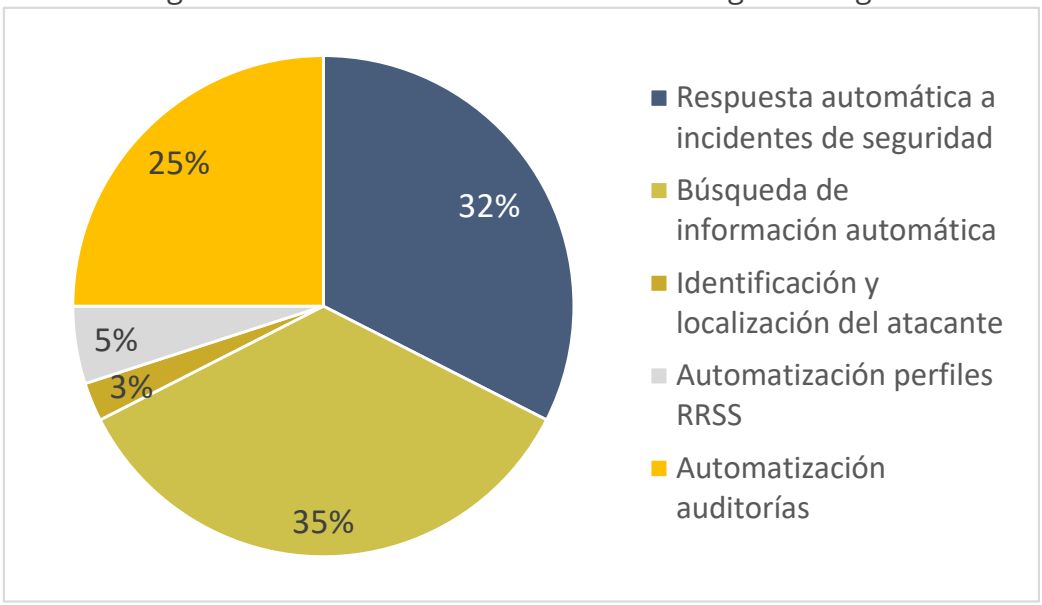


Figura 134. P67: Gráfico. RPA y automatización. Actividades más relevantes para ciberdefensa

Analizando las respuestas, las entidades se centran en las capacidades de **búsqueda de información automática**, de **respuesta automática a incidentes** y **automatización de auditorías**, todas con más de un 25%. Se descartan actividades relacionadas con la **automatización de perfiles en RRSS** y la **identificación y localización del atacante.** Esto indica que su estrategia está más orientada a prevenir y reaccionar a estos incidentes.

Tecnologías con mayor impacto frente a los sistemas de defensa en operaciones

A continuación, se muestran los análisis realizados para las respuestas recibidas para la pregunta 68. *De las siguientes tecnologías, indique cuál de ellas tiene un mayor impacto referente a los sistemas de defensa en operaciones*, relacionado con RPA y automatización para cada tecnología.

En los siguientes subapartados se analizan las respuestas recibidas para las **tres tecnologías** relacionadas:

- **RPA *(Robotic Process Automation)***

Los datos recogidos para la tecnología RPA se muestran en la siguiente figura:

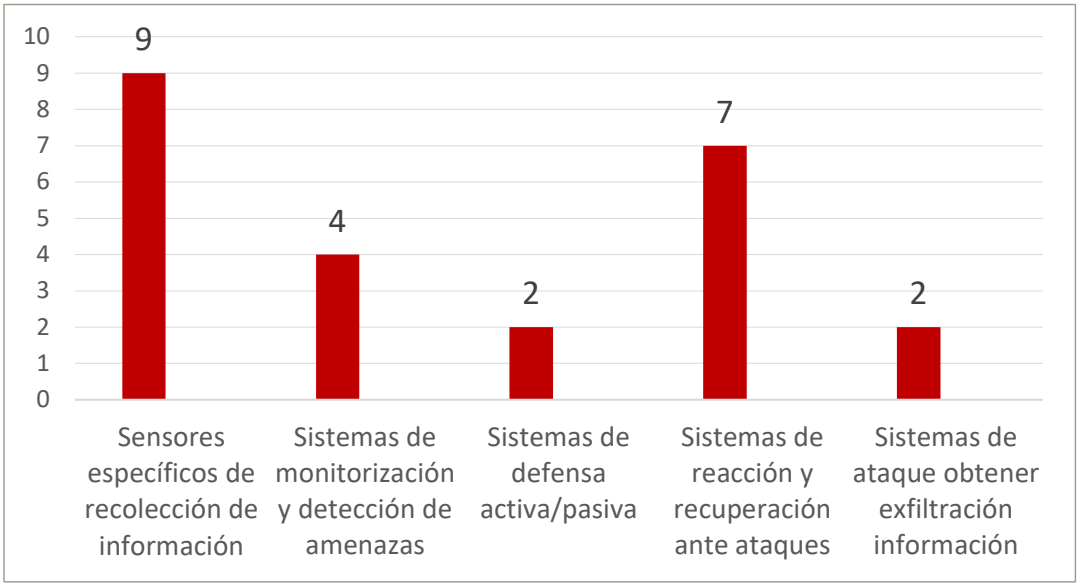


Figura 135. P68 Datos RPA y automatización. Tecnologías con mayor impacto a los sistemas de defensa en operaciones RPA

La representación gráfica de estos datos se muestra en la siguiente figura:

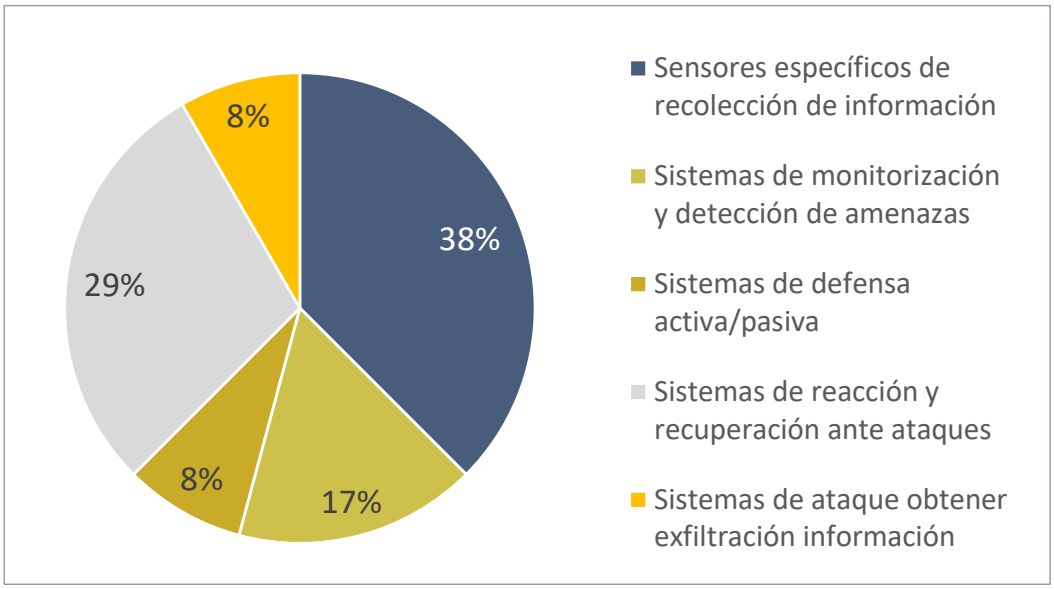


Figura 136. P68: Gráfico. RPA y automatización. Tecnologías con mayor impacto a los sistemas de defensa en operaciones RPA

Más de un tercio de las entidades, con un 38%, prioriza los **sensores de recolección de información** en RPA como tecnología de mayor impacto, seguida por los **sistemas de reacción y recuperación ante ataques** y de **monitorización y detección de amenazas.**

Dado que las respuestas a los ciberincidentes son principalmente reactivas, se deberían potenciar sistemas preventivos que se adelanten a estos problemas para lograr una mejor defensa.

- **Automatización ITPA y tecnologías SOAR**

Los datos recogidos para la tecnología de automatización ITPA y las tecnologías SOAR se muestran en la siguiente figura:

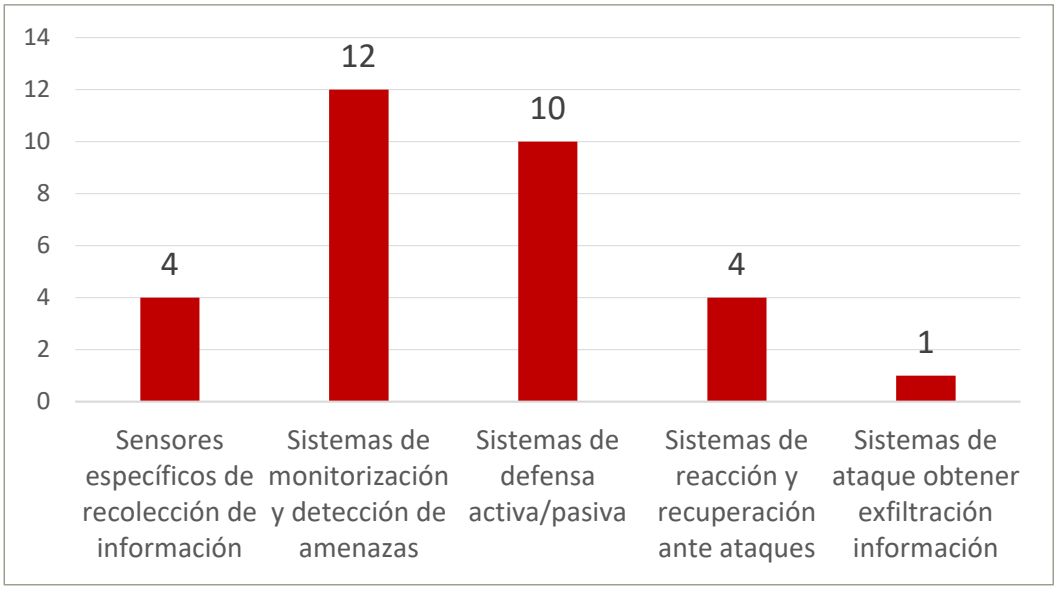


Figura 137. P68 Datos RPA y automatización. Tecnologías con mayor impacto a los sistemas de defensa en operaciones. Automatización ITPA y tecnologías SOAR

La representación gráfica de estos datos se muestra en la siguiente figura:

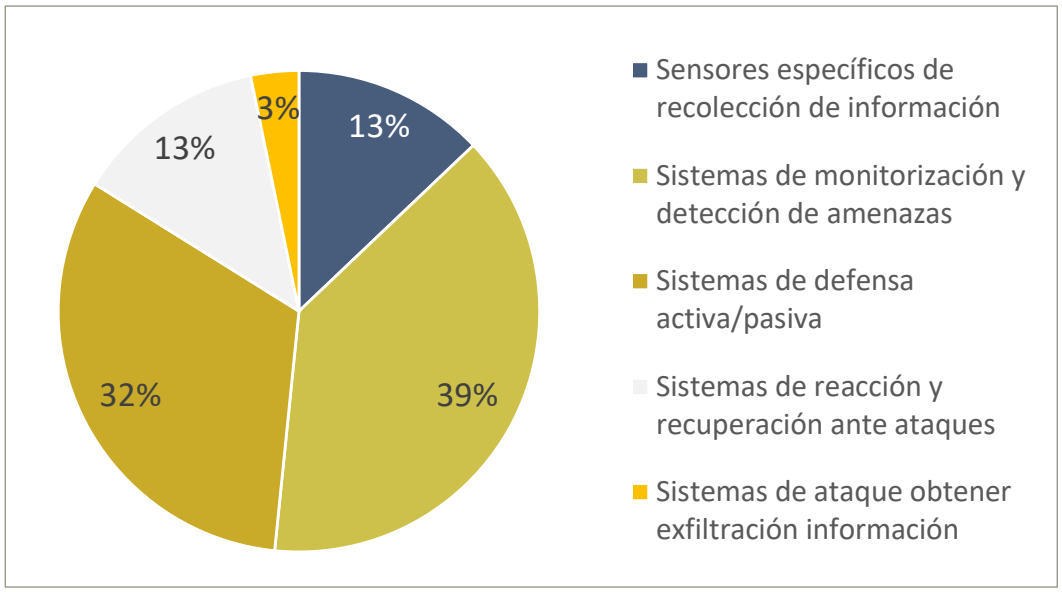


Figura 138. P68: Gráfico. RPAs y automatización. Tecnologías con mayor impacto a los sistemas de defensa en operaciones. Automatización ITPA y tecnologías SOAR

En cuanto a la tecnología de automatización ITPA y SOAR, las entidades priorizan los **sistemas de monitorización y detección de amenazas** con un 39% y los **sistemas de defensa activa y pasiva** con un 32%, que contrasta con el uso de las tecnologías RPA donde no eran las opciones preferentes.

- ***Scripting* y macros**

Los datos recogidos para la tecnología *scripting* y macros se muestran en la siguiente figura:

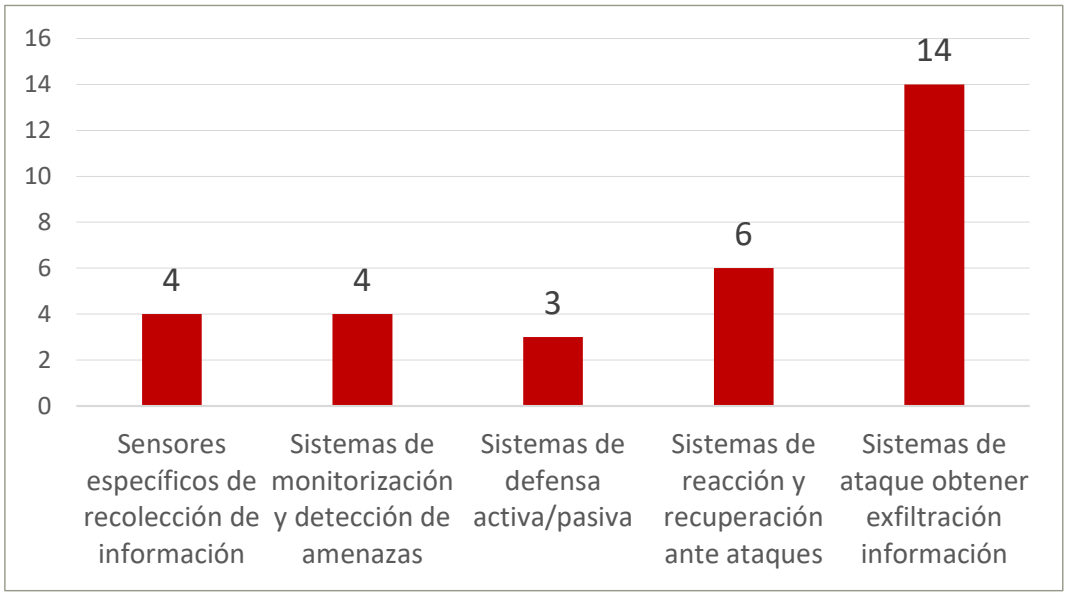


Figura 139. P68: Datos RPA y automatización. Tecnologías con mayor impacto a los sistemas de defensa en operaciones scripting y macros

La representación gráfica de estos datos se muestra en la siguiente figura:

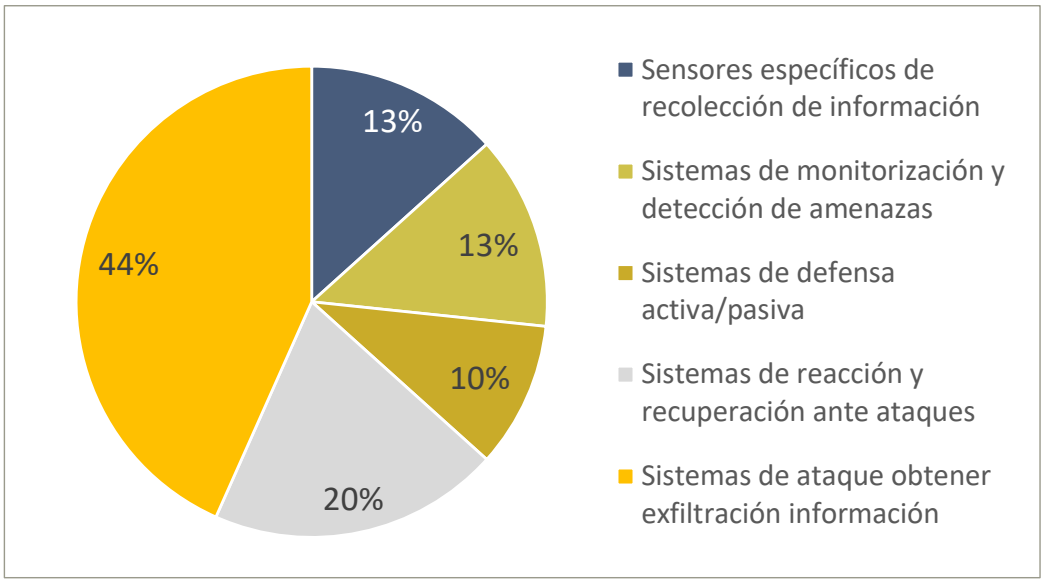


Figura 140. P68: Gráfico. RPA y automatización. Tecnologías con mayor impacto a los sistemas de defensa en operaciones scripting y macros

En las tecnologías relacionadas con *scripting* y macros destacan los **sistemas de ataque para exfiltración** con un 44%, lo que contrasta con el caso de RPA y automatización ITPS y SOAR donde era una opción residual.

La RPA permitirá a las entidades realizar tareas repetitivas que requieren precisión, con una exactitud del 100%. Del mismo modo, la RPA permitirá la estandarización y la optimización de procesos reduciendo el tiempo de entrega en más de una tercera parte, con el beneficio adicional de una mejora en calidad. La automatización de tareas manuales repetitivas hace que los RPA incrementen la productividad y minimiza los errores humanos, lo que a su vez ayuda a reducir el riesgo en ciberdefensa.

La RPA en respuesta a incidentes y la localización de los atacantes serían para las entidades las actividades que ayudarían a la ciberdefensa. Es decir, con el apoyo de esta tecnología y la integración con sistemas SOAR, todas las áreas que ofrecen servicios de ciberdefensa pueden tener más claro los orígenes de posibles ataques o amenazas, y así se pueden dedicar a las actividades urgentes, de modo que pueden dejar en segundo lugar las actividades menos prioritarias.

7.6. Dispositivos móviles

El análisis de las respuestas sobre esta tecnología se desglosa en **dos áreas** que se detallan a continuación:

Actividades más relevantes para ciberdefensa

La siguiente figura muestra los datos recogidos en la pregunta 69. *¿En cuáles de las siguientes actividades relacionadas con la seguridad en dispositivos móviles cree que su organización desarrollará capacidades avanzadas en los próximos 2 años, que tenga aplicabilidad en el ámbito de la ciberdefensa?*, se muestran en la siguiente figura:

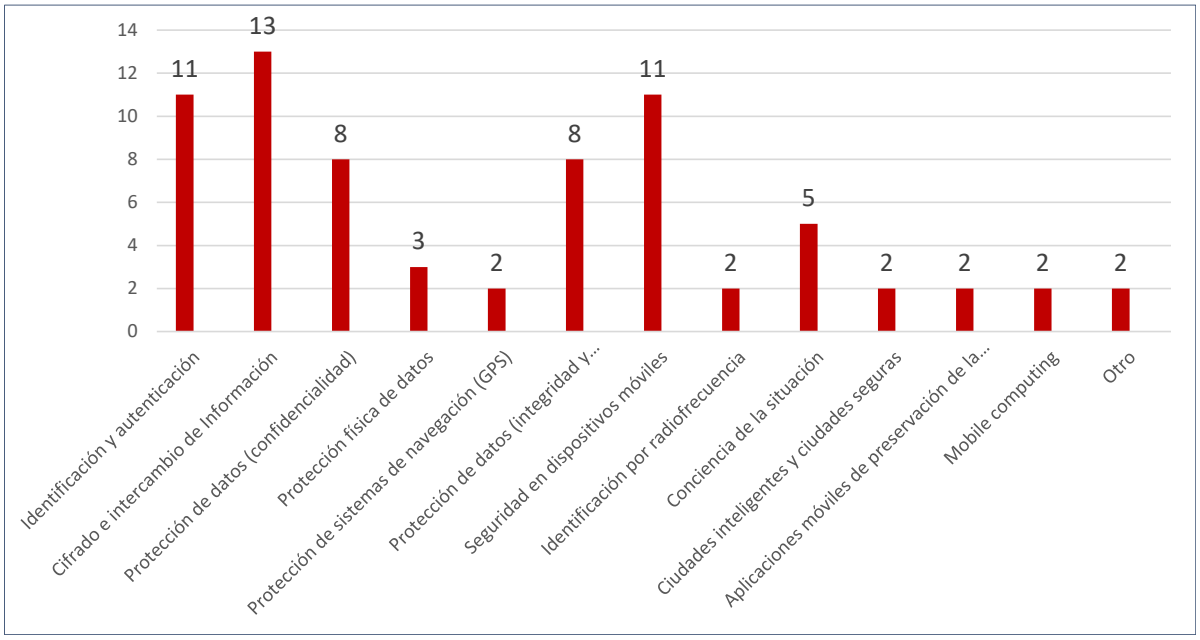


Figura 141. P69: Datos dispositivos móviles. Actividades más relevantes para ciberdefensa

La representación gráfica de estos datos se muestra en la siguiente figura:

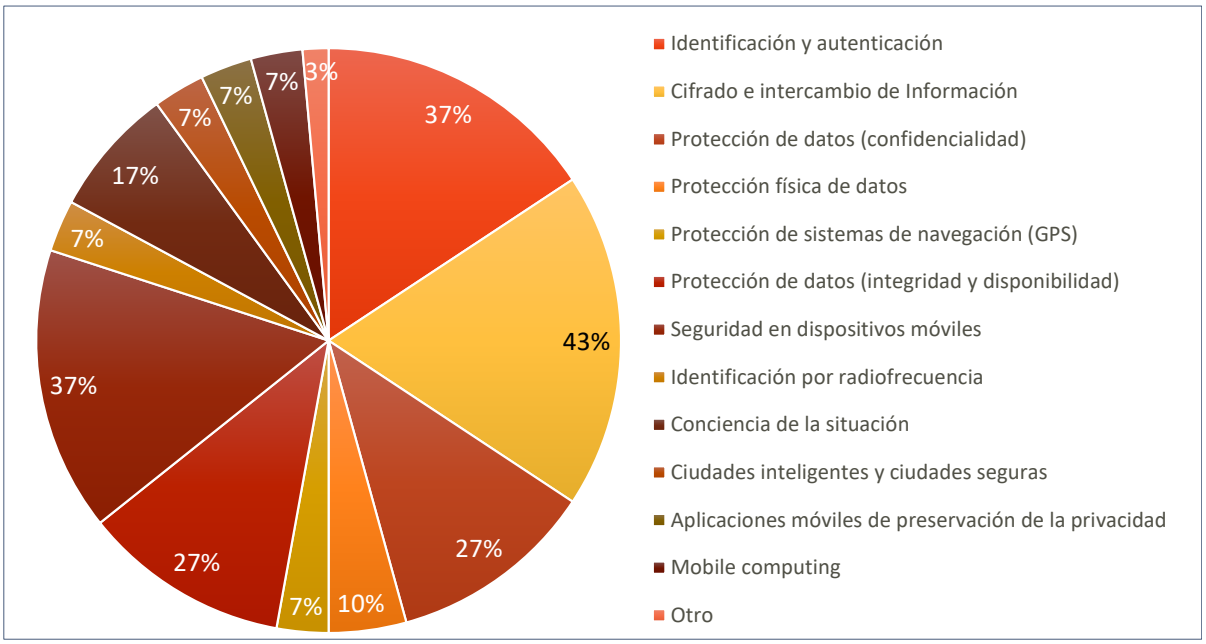


Figura 142. P69: Gráfico. Dispositivos móviles. Actividades más relevantes para ciberdefensa

Se trata de una pregunta con respuestas múltiples. Los resultados obtenidos indican que casi la mitad de las entidades esperan desarrollar capacidades avanzadas relacionadas con el **cifrado e intercambio de la información** para su aplicación en el ámbito de la ciberdefensa. Más de un tercio cree que desarrollará las relacionadas con **identificación, autenticación y seguridad** en los propios terminales móviles. La cuarta parte piensa potenciar las capacidades de **protección de datos** en las principales dimensiones de la información.

Cabe mencionar, aunque no es significativo, que existe alguna entidad que indica disponer de otro tipo de capacidades, no identificadas anteriormente, que pueden ser orientadas a la mejora de la seguridad en dispositivos móviles.

La mayoría de las entidades son conscientes de la necesidad e importancia de desarrollar determinadas capacidades avanzadas relacionadas con la implementación de medidas de seguridad en los propios terminales y de la información gestionada.

En lo que respecta a la seguridad de dispositivos destaca que las entidades no desarrollarán a corto plazo capacidades avanzadas relacionadas con la **protección de sistemas de navegación (GPS), identificación por radio frecuencia, aplicaciones móviles de preservación de la privacidad,** mobile computing o con las **ciudades inteligentes.**

Dominios de conocimiento para desarrollar capacidades en ciberdefensa

La siguiente figura muestra los datos recogidos en la pregunta 70. ¿En qué dominios de conocimiento cree que su organización puede llegar a ofrecer un mayor valor añadido de cara a desarrollar capacidades de ciberdefensa sustentadas en dispositivos móviles?, se muestran en la siguiente figura:

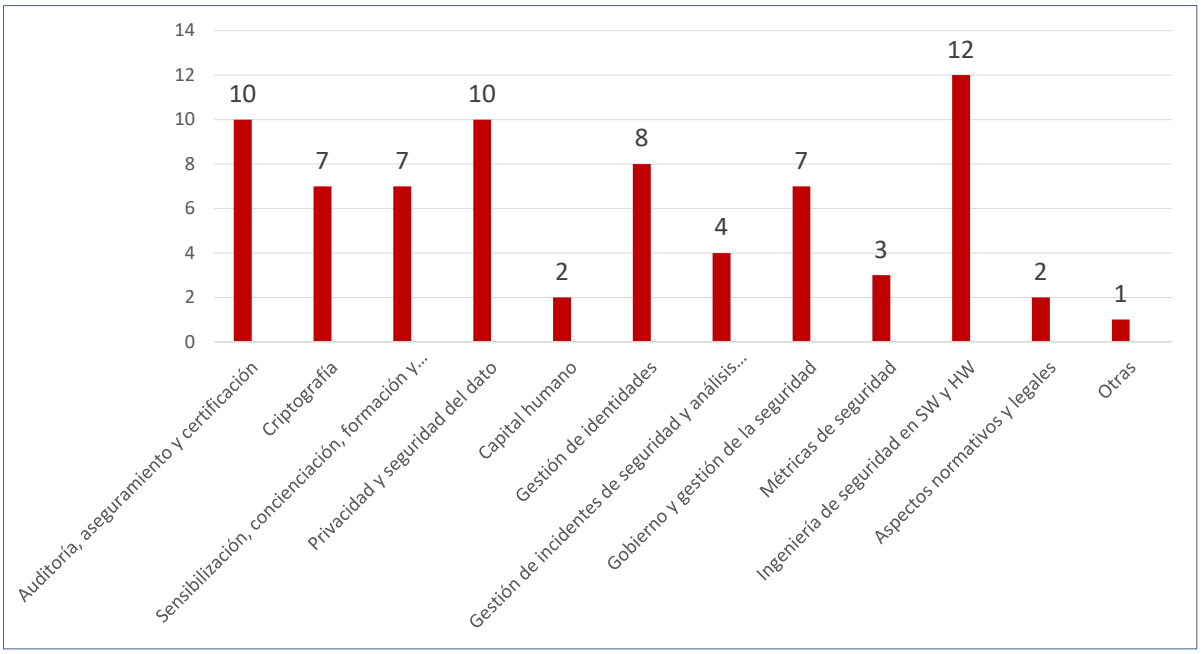


Figura 143. P70: Datos dispositivos móviles. Dominios de conocimiento para desarrollar capacidades en ciberdefensa

La representación gráfica de estos datos se muestra en la siguiente figura:

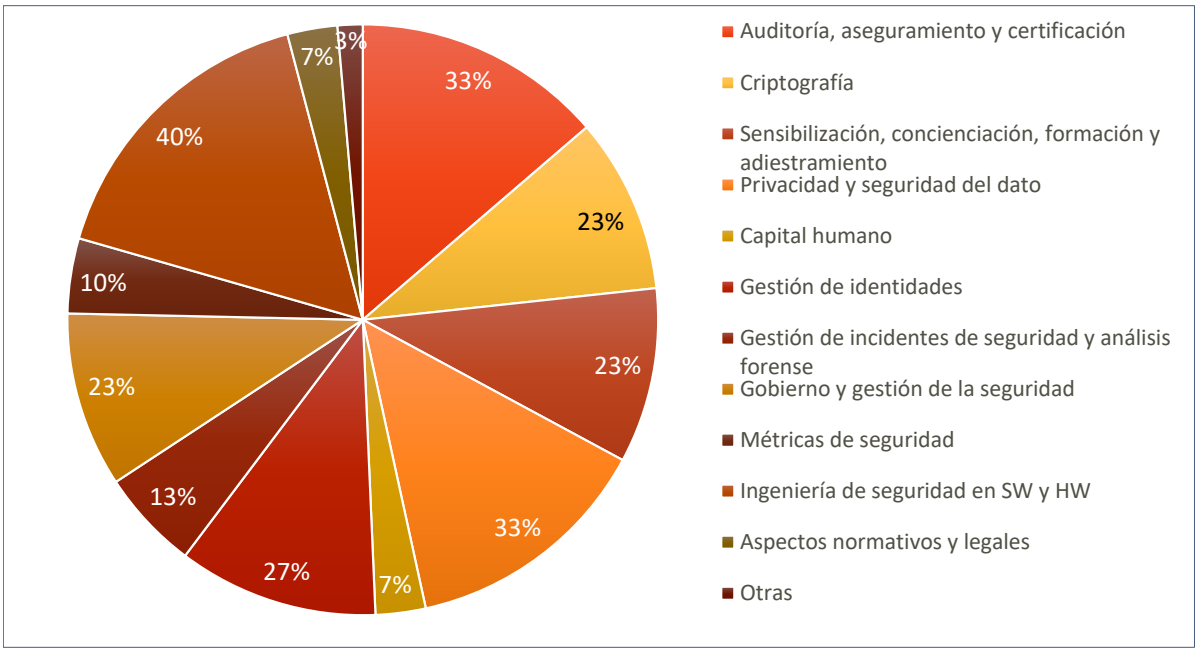


Figura 144. P70: Gráfico. Dispositivos móviles. Dominios de conocimiento para desarrollar capacidades en ciberdefensa

También se trata de una pregunta con respuesta múltiple. Los resultados obtenidos indican que el 40% de las entidades considera que debe tener conocimientos para desarrollar capacidades relacionadas con la **Ingeniería de seguridad en** software **y** hardware. Un 33% cree que debe tener conocimiento para desarrollar las vinculadas con **auditoría, aseguramiento y certificación**. Otro 33%, cree tener conocimiento en las asociadas a la **privacidad y seguridad del dato**. El 27% considera necesario tener conocimiento en las relacionadas con la **gestión de identidades**.

La mayoría de las entidades cree relevante tener dominio de conocimiento para desarrollar capacidades de ciberdefensa en dispositivos móviles relacionadas con la seguridad tanto del *software* y *hardware* como de los datos.

También de deduce de las respuestas que las entidades no consideran relevante tener conocimientos para desarrollar capacidades relacionadas con **aspectos normativos y legales** ni con **métricas de seguridad**. Tampoco dan una importancia significativa a disponer del **capital humano** suficiente.

7.7. Seguridad en redes

El análisis de las respuestas sobre esta tecnología se desglosa en **tres áreas** que se detallan a continuación:

Mecanismos de ciberseguridad

Los datos recogidos en la pregunta *71. En el ámbito de los Sistemas de Defensa de Operaciones en el Ciberespacio, ¿qué mecanismos de Ciberseguridad no está utilizando su organización?,* se muestran en la siguiente figura:

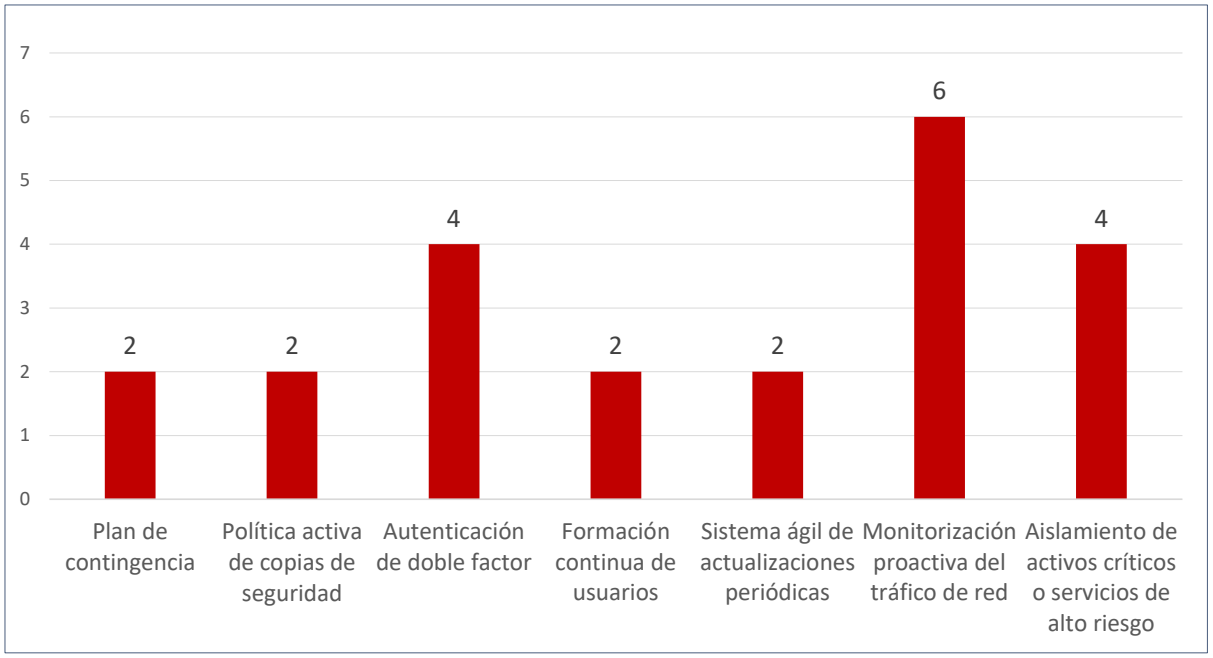


Figura 145. P71: Datos seguridad en redes. Mecanismo de ciberseguridad

La representación gráfica de los datos se muestra en la siguiente figura:

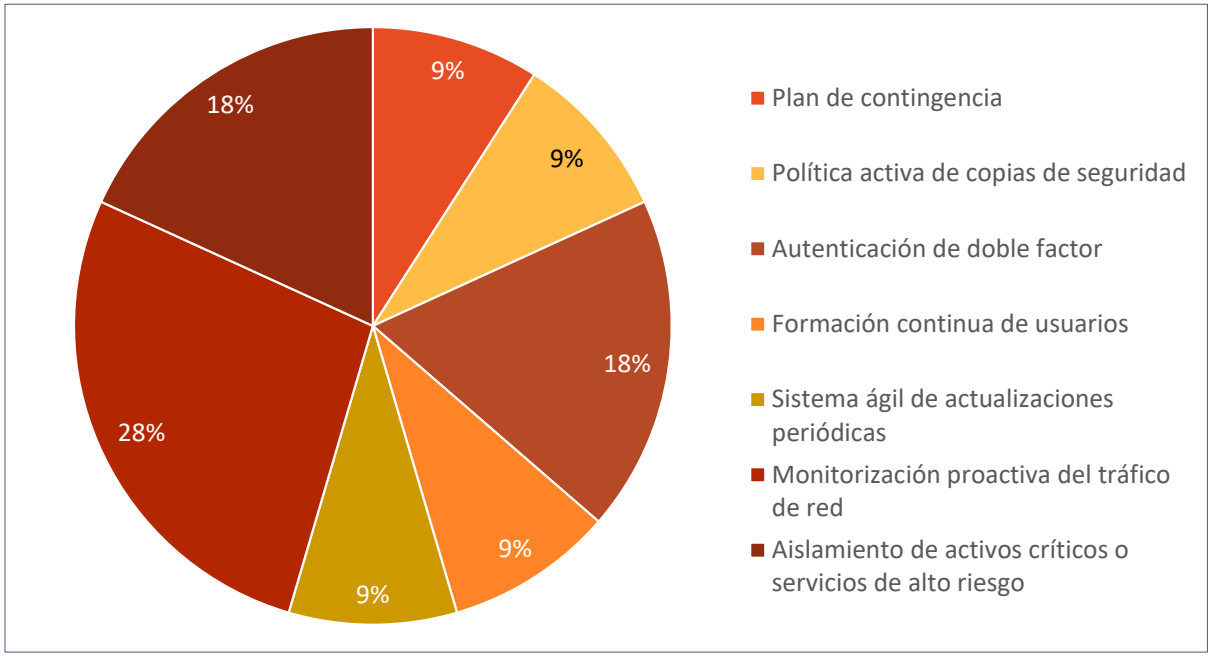


Figura 146. P71: Gráfico. Seguridad en redes. Mecanismo de ciberseguridad

Se trata de una pregunta con respuestas múltiples. Los resultados obtenidos indican que el 67% de las entidades que han respondido utiliza todos los mecanismos de ciberseguridad propuestos. Sobre la aplicación de los mecanismos de ciberseguridad propuestos, un 28% indica que no **monitoriza de manera proactiva el tráfico de red**, un 18% indica que no realiza la **autenticación de doble factor de usuario** y otro 18% no tiene **segmentación fuerte** relativa al aislamiento de los activos críticos o servicios de alto riesgo.

Cabe mencionar, aunque no es significativo, que existe alguna entidad que no utiliza ninguno de los mecanismos de ciberseguridad propuestos en su organización.

A pesar de poder haberse incluido muchos otros mecanismos de ciberseguridad, **más de un 30% de** las entidades aún no aplica todos los mecanismos propuestos en la pregunta.. Se debe seguir concienciando a las organizaciones para que inviertan más en herramientas y soluciones de ciberseguridad que mejoren la continuidad del negocio. Asimismo, las entidades deberían disponer del talento humano cualificado para gestionarlas y administrarlas, así como nunca olvidar la concienciación y formación de los usuarios.

Capacidades de esteganografía

Los datos recogidos en la pregunta 72. *¿Está desarrollando capacidades referentes a la esteganografía en la red?,* se muestran en la siguiente figura:

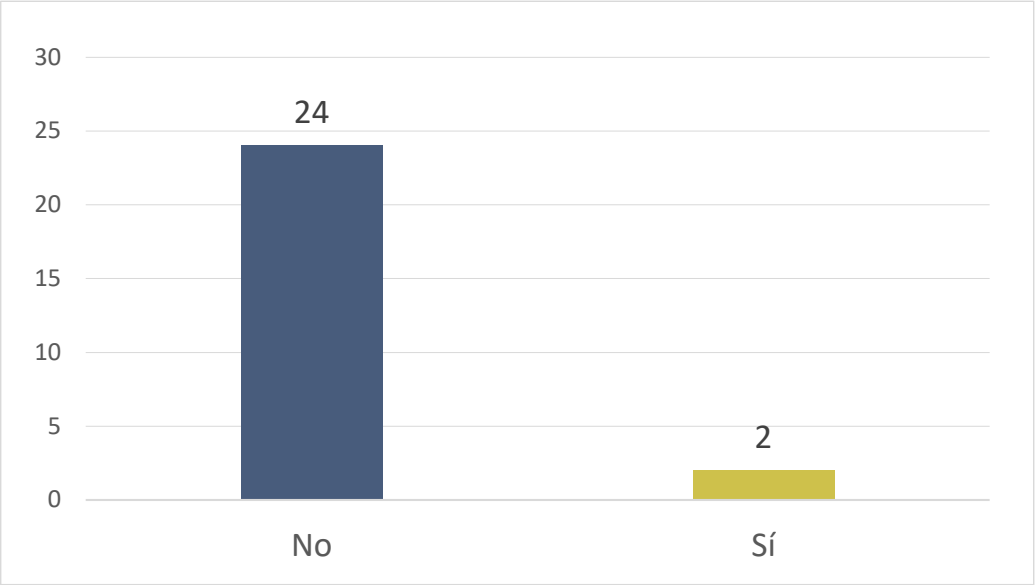


Figura 147. P72: Datos seguridad en redes. Capacidades esteganografía

La representación gráfica de los datos se muestra en la siguiente figura:

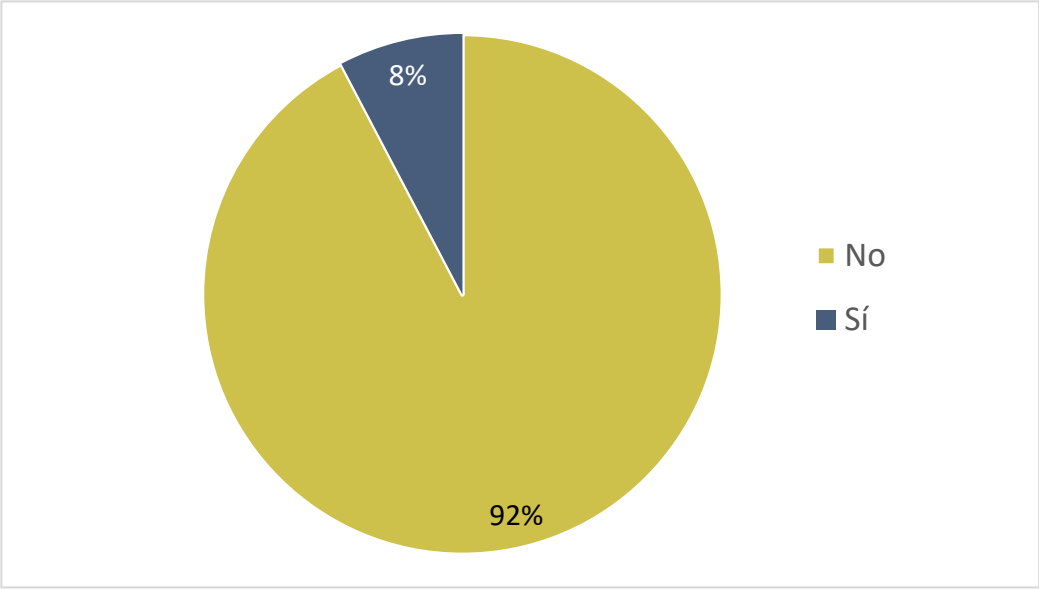


Figura 148. P72: Grafico. Seguridad en redes. Capacidades esteganografía

Los resultados obtenidos indican que el 92% de las entidades que ha respondido no está desarrollando capacidades de esteganografía. La minoría que sí lo hace se dedica a temas de investigación, análisis, enmascaramiento y algoritmia.

La esteganografía es una técnica con la que la mayoría de las entidades no está familiarizada o no considera útil usarla para el desarrollo de su actividad, como sí sucede con la criptografía que se tratará en el siguiente apartado.

Capacidades defensa ante ataques propagables

Los datos recogidos en la pregunta *73. ¿Está desarrollando capacidades referentes a la defensa ante ataques propagables?*, se muestran en la siguiente figura:

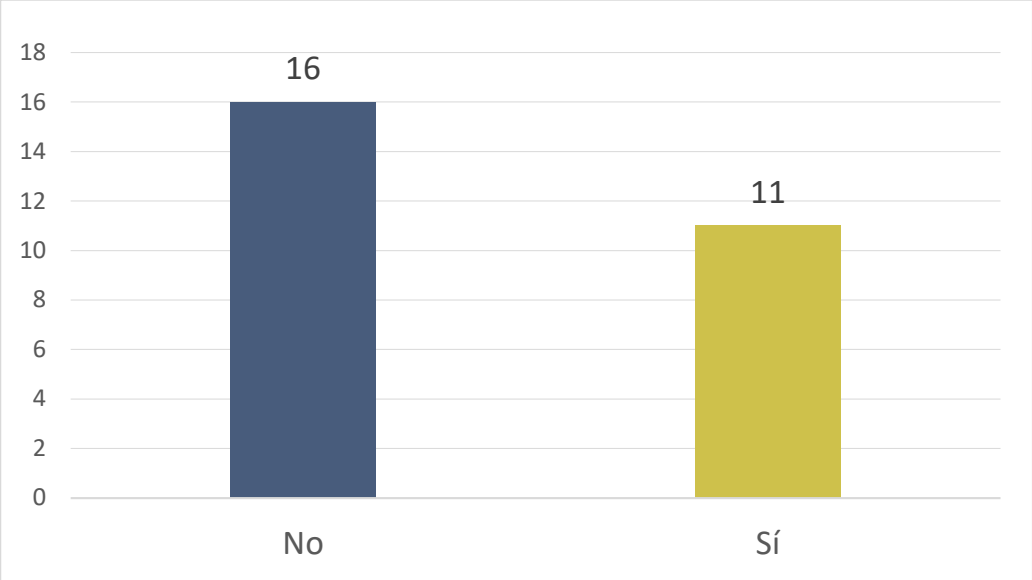


Figura 149. P73: Datos seguridad en redes. Capacidades defensa ante ataques propagables

La representación gráfica de los datos se muestra en la siguiente figura:

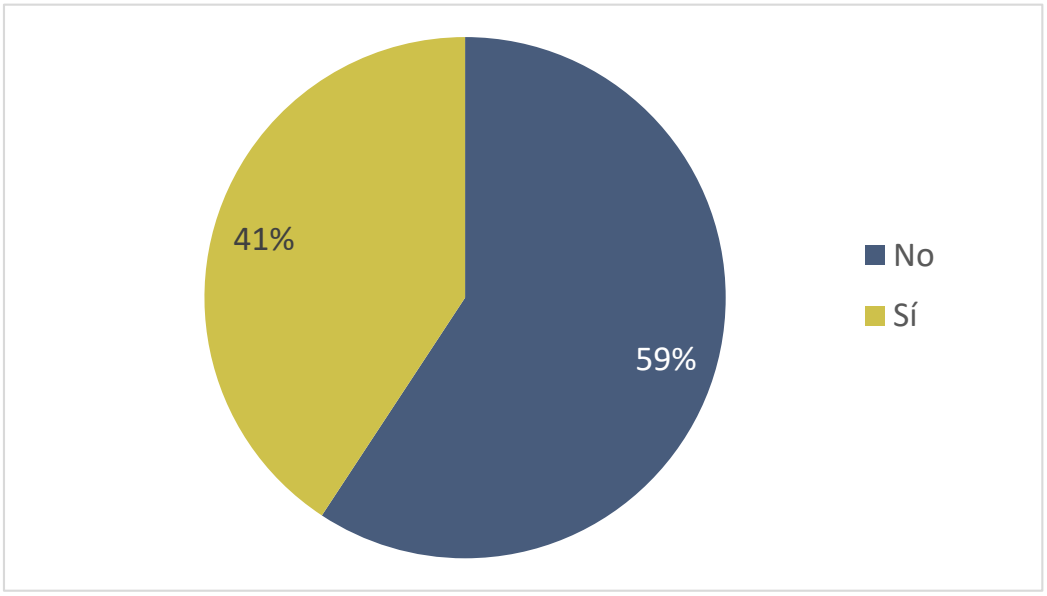


Figura 150. P73: Gráfico. seguridad en redes. Capacidades defensa ante ataques propagables

Los resultados obtenidos indican que un 59% de las entidades que ha respondido no está desarrollando capacidades de defensa ante ataques propagables y un 41% declara que las están desarrollando. Las acciones que están llevando a cabo para reducir la posibilidad de un ataque son, entre otras, la segmentación de redes, *ciberkill chain*, los desarrollos específicos de sistemas de ciberdefensa, la implantación de herramientas SIEM y APT o el uso de tecnologías EDR, así como la protección de *firmware*. Sólo un 10% no ha contestado.

Sólo el 37% de las entidades que ha respondido indica que está desarrollando capacidades de defensa ante ataques propagables, mientras que en la pregunta 71 el 67% de las entidades indican que utilizan todos los mecanismos de ciberseguridad. Llama la atención esta diferencia de porcentaje ya que los mecanismos de ciberseguridad contemplados pueden ayudar a mitigar la propagación de los ataques.

Sería recomendable que las entidades que no lo hacen aún, desarrollaran e implementaran mecanismos que impidan la propagación dentro de la organización y de la cadena de suministro. Esto les permitiría reaccionar rápidamente ante un posible ciberincidente que afecte a la continuidad de negocio.

7.8. *Blockchain* y DLT

El análisis de las respuestas sobre esta tecnología se desglosa en **dos áreas** que se detallan a continuación:

Actividades más relevantes para ciberdefensa

Los datos recogidos en la pregunta 76[26]. *¿Cuál de las siguientes actividades de blockchain y DLT relacionadas con la ciberdefensa considera más relevante?,* se muestran en la siguiente figura:

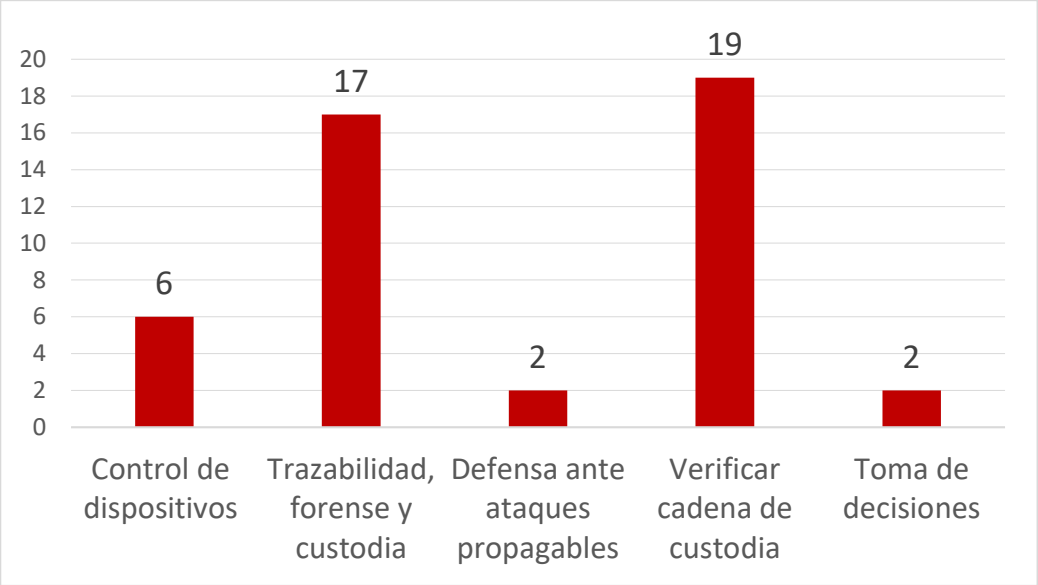


Figura 151. P76: Datos Actividades de blockchain y DLT más relevantes relacionadas con la ciberdefensa

La representación gráfica de estos datos se muestra en la siguiente figura:

[26] Se ha detectado una errata en la numeración de las preguntas pasando de la 73 a la 76 directamente.

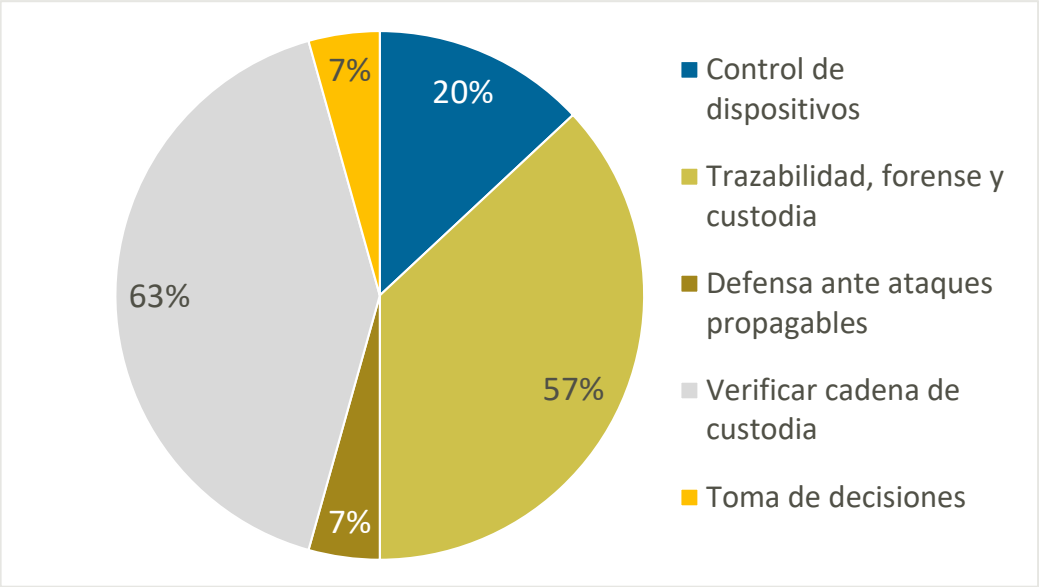


Figura 152.P76: Gráfico. Actividades de blockchain y DLT más relevantes relacionadas con la ciberdefensa

Como puede observarse en el gráfico, el 63% de las entidades consideran que **verificar la cadena de custodia** es la actividad de *blockchain y* DLT más relevante para la ciberdefensa, mientras el 57% consideran que lo es la **trazabilidad, forense y custodia**. El 20% consideran que es el **control del dispositivo** y una minoría del 7% considera la **defensa ante ataques propagables** y la **toma de decisiones**.

Utilización de *blockchain* para la privacidad y seguridad del dato en el ámbito de la ciberdefensa

Los datos recogidos en la pregunta 77. *¿Está desarrollando capacidades referentes a la privacidad y seguridad del dato con técnicas de blockchain en el ámbito de la ciberdefensa?* se muestran en la siguiente figura:

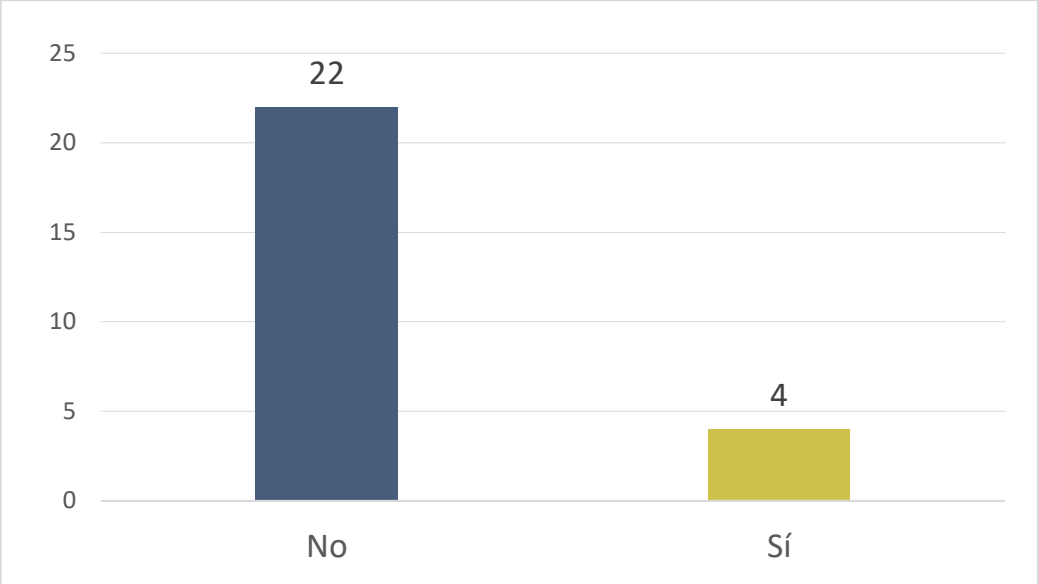


Figura 153. P77: Datos Capacidades referentes a la privacidad y seguridad del dato con técnicas de blockchain para ciberdefensa

La representación gráfica de estos datos se muestra en la siguiente figura:

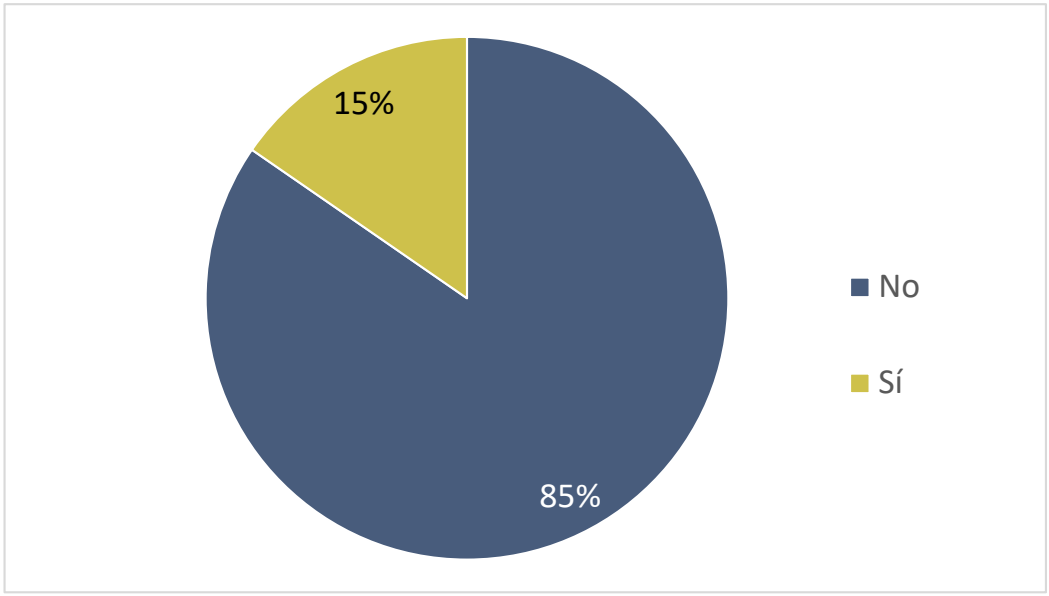


Figura 154. P77: Gráfico. Capacidades referentes a la privacidad y seguridad del dato con técnicas de blockchain para ciberdefensa

Como puede observarse en el gráfico, el 85% de las entidades que han respondido indica no estar desarrollando capacidades referentes a privacidad y seguridad del dato. Las entidades que afirman estar desarrollando este tipo de capacidades, el 15%, mencionan los siguientes ámbitos de interés:

- Gestión de la identidad.
- Registro y trazabilidad inmutables.
- Privacidad y seguridad del dato (no aplicándolo por el momento al ámbito de la ciberdefensa).
- Aseguramiento de mensajería en IoT.
- Inmutabilidad de objetos digitales.

Es destacable el elevado número de entidades que creen que la tecnología del *blockchain* y DLT es relevante, para los distintos usos propuestos para la ciberdefensa, especialmente para la verificación de la cadena de custodia, la trazabilidad o el forense, aunque posteriormente muy pocas realizan desarrollos relacionados con la privacidad y seguridad del dato.

7.9. Criptografía

El análisis de las respuestas esta tecnología se desglosa en **dos áreas** que se detallan a continuación:

Tecnologías cuánticas y postcuánticas

Los datos recogidos en la pregunta *78.* ¿Está su organización *trabajando en desarrollos relacionados con técnicas o tecnologías cuánticas y postcuánticas que pudieran ser de aplicación en el ámbito de la Ciberdefensa?,* se muestran en la siguiente figura:

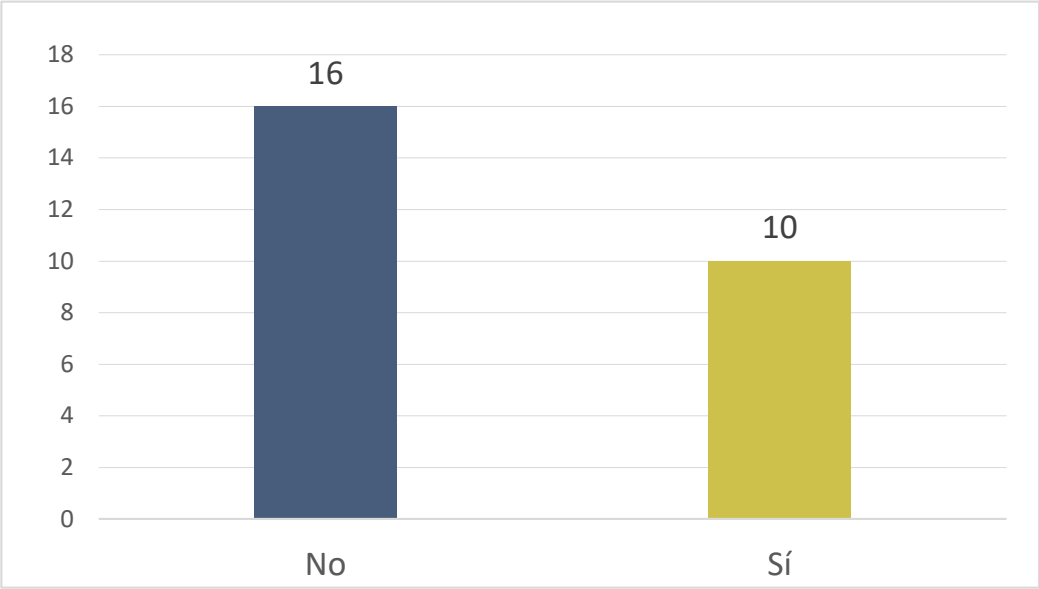


Figura 155. P78: Datos criptografía. Tecnologías y postcuánticas

La representación gráfica de los datos se muestra en la siguiente figura:

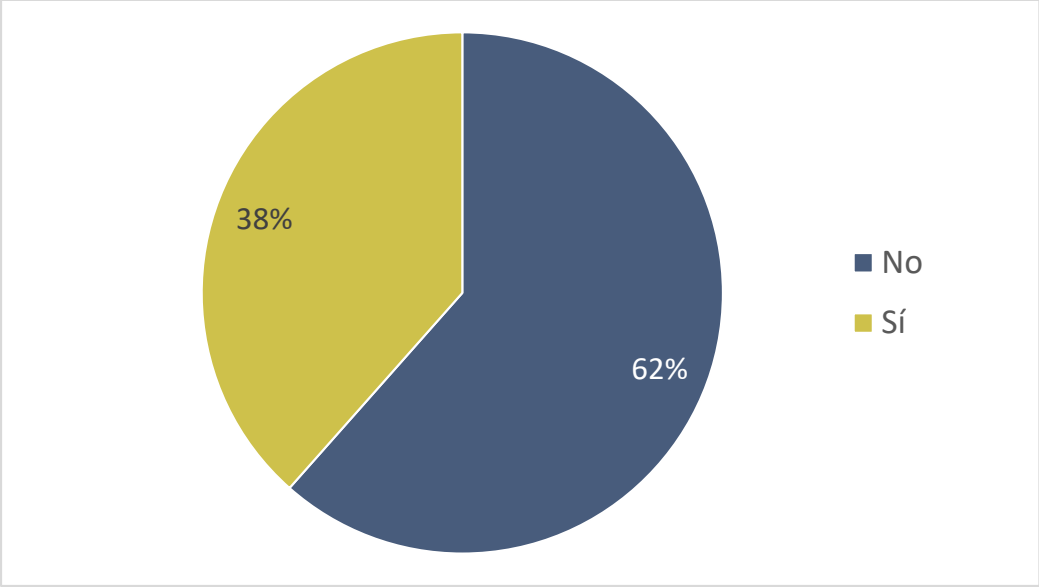


Figura 156. P78: Gráfico. Criptografía. Tecnologías y postcuánticas

Los resultados obtenidos muestran que un 62% de las entidades que ha respondido indica que no están trabajando en desarrollos relacionados con estas tecnologías que pudieran ser de aplicación en el ámbito de la ciberdefensa.

De entre el 38% de entidades que sí lo hace, algunas indican estar trabajando en proyectos relacionados con la criptografía postcuántica (PQC: *Post-Quantum Cryptograph*) y la distribución cuántica de claves (QKD: *Quantum Key Distribution*). Entre sus labores destacan el análisis de criptosistemas, la identificación y migración de aplicaciones clásicas a las tecnologías PQC, así como la verificación y validación de distintos *software* cuánticos.

Destaca una entidad que participa en el proyecto ESA DISCRETION, dedicado al desarrollo de redes de comunicaciones seguras para uso en defensa, definidas por *software* y cuyas claves criptográficas son distribuidas mediante enlaces cuánticos.

Mecanismos criptográficos avanzados

La siguiente figura muestra los datos recogidos en la pregunta 79. En el ámbito de los sistemas de defensa en operaciones en el ciberespacio (sistemas de intercambio de información, sistemas de defensa activa y pasiva, sistemas de anonimización…), ¿qué mecanismos criptográficos más avanzados están utilizando/desarrollando?, se muestran en la siguiente figura:

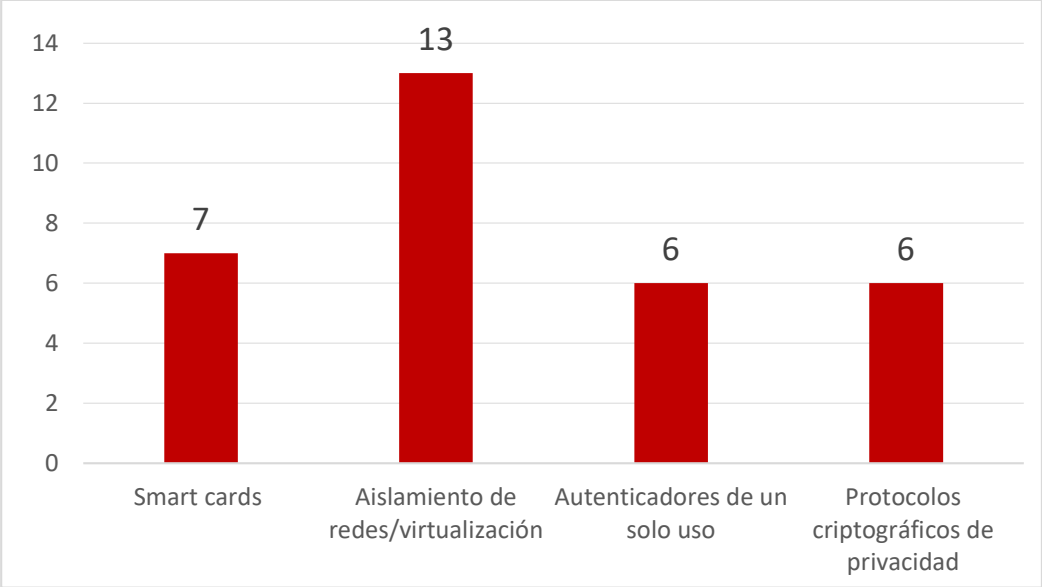


Figura 157. P79: Datos criptografía.Mecanismos criptográficos avanzados

La representación gráfica de los datos se muestra en la siguiente figura:

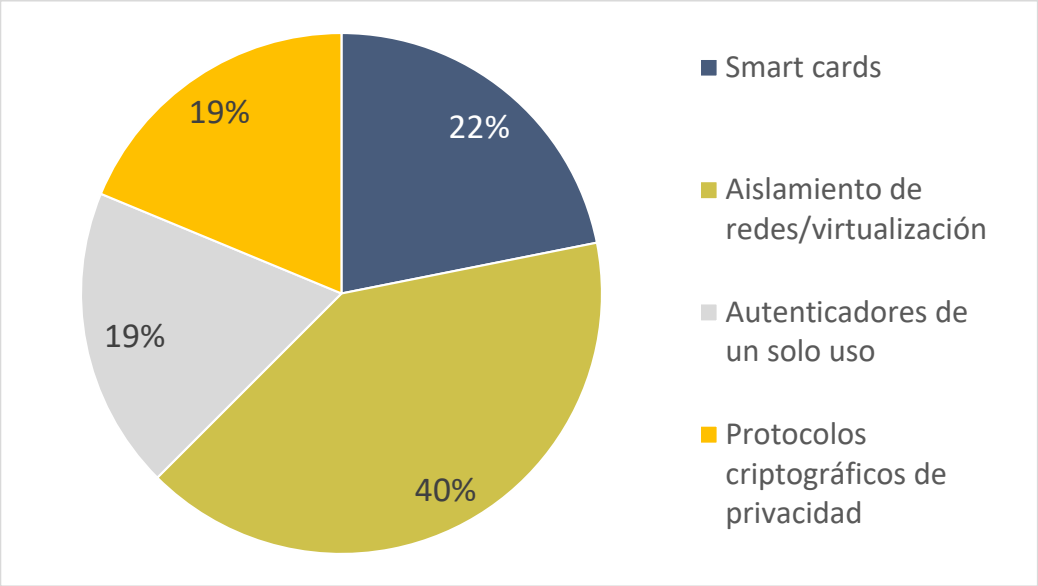


Figura 158. P79: Gráfico. Criptografía.Mecanismos criptográficos avanzados

En el ámbito de los sistemas de defensa en operaciones en el ciberespacio, los resultados obtenidos muestran que un 40% de las respuestas indica que aplican los mecanismos criptográficos avanzados para el **aislamiento de redes y virtualización** y un 22% para el desarrollo de smart cards (de última generación). Finalmente, un 19% aplica **autenticadores** y **protocolos criptográficos** de preservación de la privacidad en este ámbito, que aun siendo técnicas más avanzadas son menos empleadas. Se aprecia que se continúa abordando la protección y defensa en estos entornos desde un punto de vista IT y menos desde un enfoque de ciberseguridad, empleando los nuevos mecanismos criptográficos avanzados.

Si bien las tecnologías cuánticas y postcuánticas no son tecnologías muy maduras, se ha identificado un buen número de entidades trabajando en ellas, principalmente en temas de distribución cuántica de claves y criptografía postcuántica. Algunas incluso participan en proyectos europeos relacionados para el desarrollo de redes de comunicaciones seguras para defensa. Por otro lado, aunque existen mecanismos criptográficos avanzados, todavía no son empleados por todas las entidades.

7.10. *Data mining* y analítica avanzada

Los datos recogidos en la pregunta 80. *¿Está su organización trabajando en desarrollos relacionados con analítica y minería de datos que pudieran tener aplicación en el ámbito de la Ciberdefensa?*, se muestran en la siguiente figura:

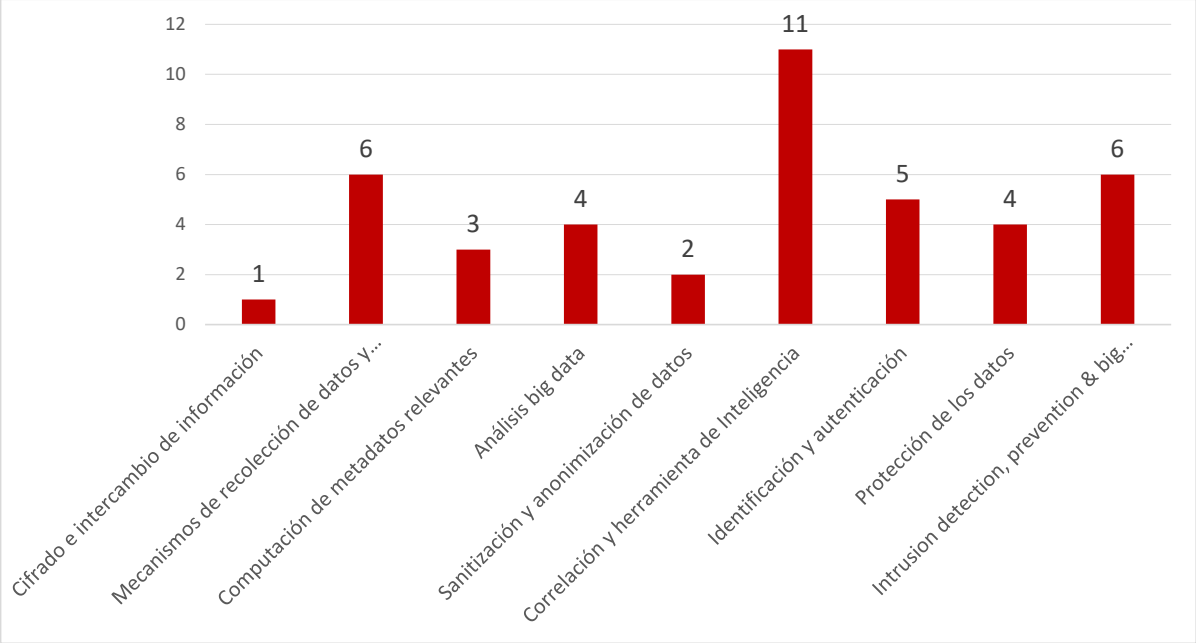


Figura 159. P80: Datos data minig y analítica avanzada

La representación gráfica de estos datos se muestra en la siguiente figura:

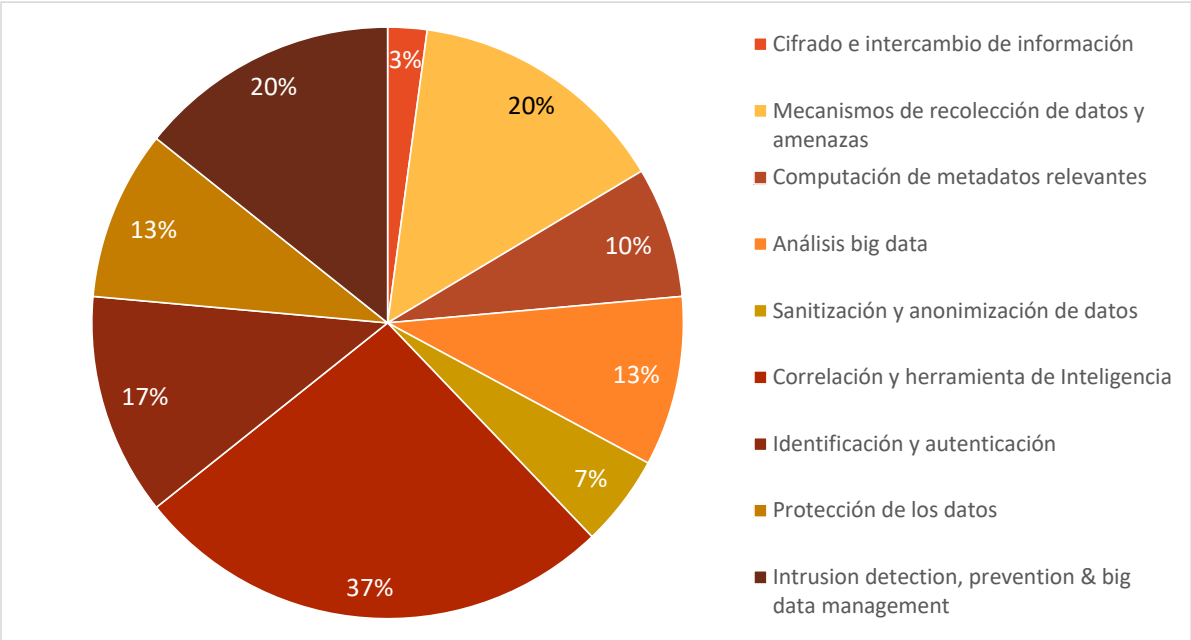


Figura 160. P80: Gráfico. Data minig y analítica avanzada

Los resultados obtenidos muestran que los desarrollos relacionados con la analítica y la minería de datos con aplicación en el ámbito de la ciberdefensa más empleados por las entidades son **correlación y herramienta de Inteligencia**, con un 37% de las entidades que han respondido, **intrusion, detection, prevention &** big data management y los **mecanismos de recolección de datos** y, ambas con un 20% e **identificación y autenticación** con un 17%.

Se observan múltiples posibilidades y respuestas de los desarrollos relacionados con analítica y minería de datos que pudieran tener aplicación en el ámbito de la ciberdefensa, siendo la mayoría para correlación y herramienta de Inteligencia, detección de anomalías, y la minoría para **cifrado e intercambio de Información**, no siendo por ello menos importantes. En menor medida, las entidades también han indicado dedicarse a otros sectores propuestos como cifrado, protección de datos, Inteligencia y autentificación, *big data* o computación que pudieran tener aplicación en el ámbito de la ciberdefensa**.**

7.11 Internet de las cosas (IoT)

El análisis de las respuestas esta tecnología se desglosa en **dos áreas** que se detallan a continuación:

Actividades más relevantes para ciberdefensa

Los datos recogidos en la pregunta 81.*¿En cuáles de las siguientes actividades relacionadas con la seguridad en IoT cree que su organización desarrollará capacidades avanzadas en los próximos 2 años y pueden ser de aplicabilidad en el ámbito de la ciberdefensa?*, se muestran en la siguiente figura:

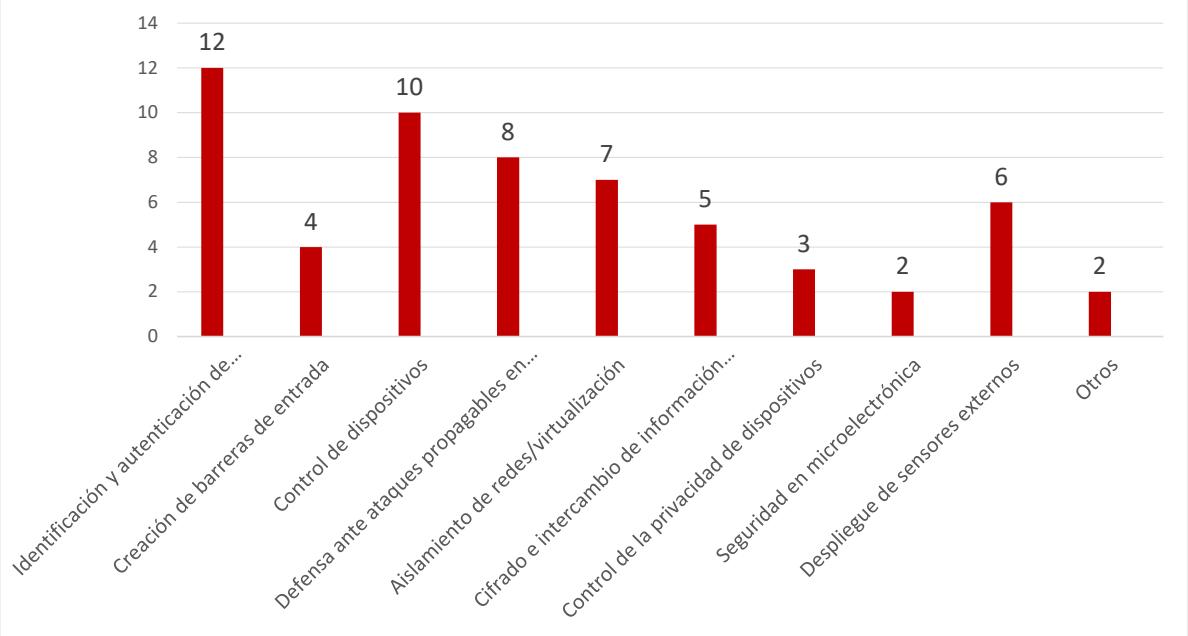


Figura 161. P81: Datos IoT. Actividades más relevantes para ciberdefensa

La representación gráfica de estos datos se muestra en la siguiente figura:

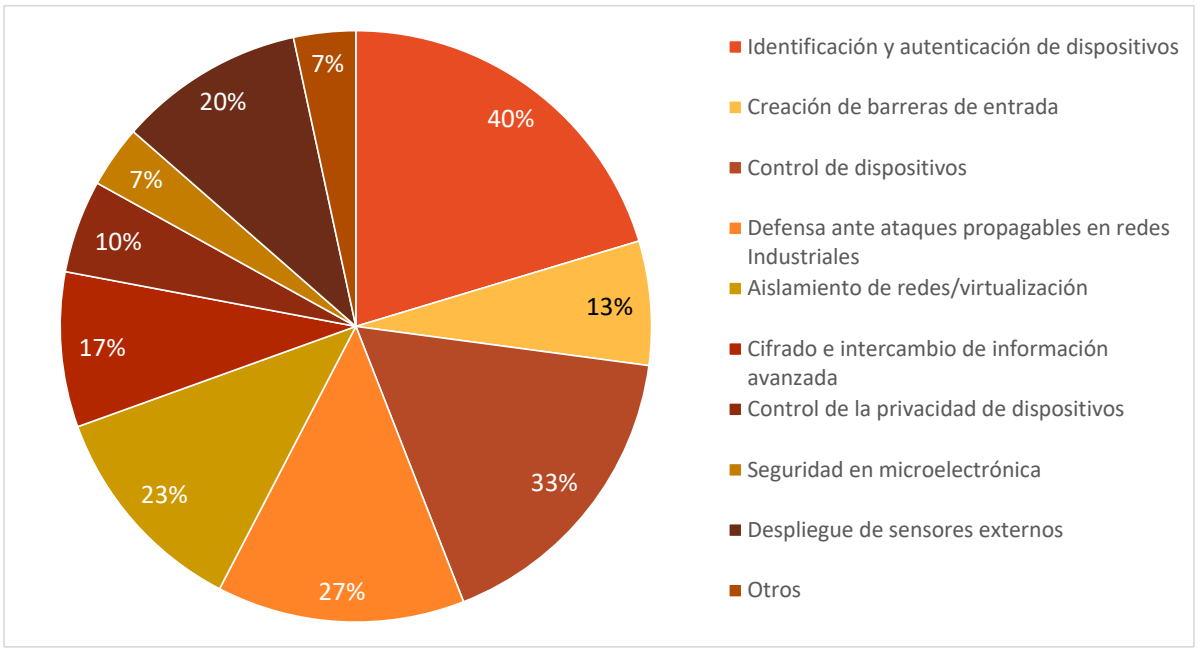


Figura 162. P81: Gráfico. IoT. Actividades más relevantes para ciberdefensa

Las entidades prevén una amplia capacidad en el desarrollo de seguridad en IoT, especialmente las orientadas a la **identificación, autenticación** y **privacidad de los dispositivos IoT** conectados. Esta posible extensa aplicación a diferentes ámbitos, entre ellos el de la ciberdefensa, es coherente con el crecimiento esperado de los dispositivos IoT en los próximos años. No obstante, cabe resaltar la escasa dedicación esperada en aspectos relacionados con las capacidades de **protección**, desde la microelectrónica, pasando por el **desarrollo de barreras** de entrada hasta la **privacidad**; Estos últimos se consideran elementos clave para garantizar la seguridad operacional.

Tecnologías con mayor impacto para ciberdefensa

Los datos recogidos en la pregunta 82. *¿En qué dominios de conocimiento cree que su organización puede llegar a ofrecer un mayor valor añadido de cara a desarrollar capacidades sustentadas en IoT de aplicabilidad en la ciberdefensa?*, se muestran en la siguiente figura:

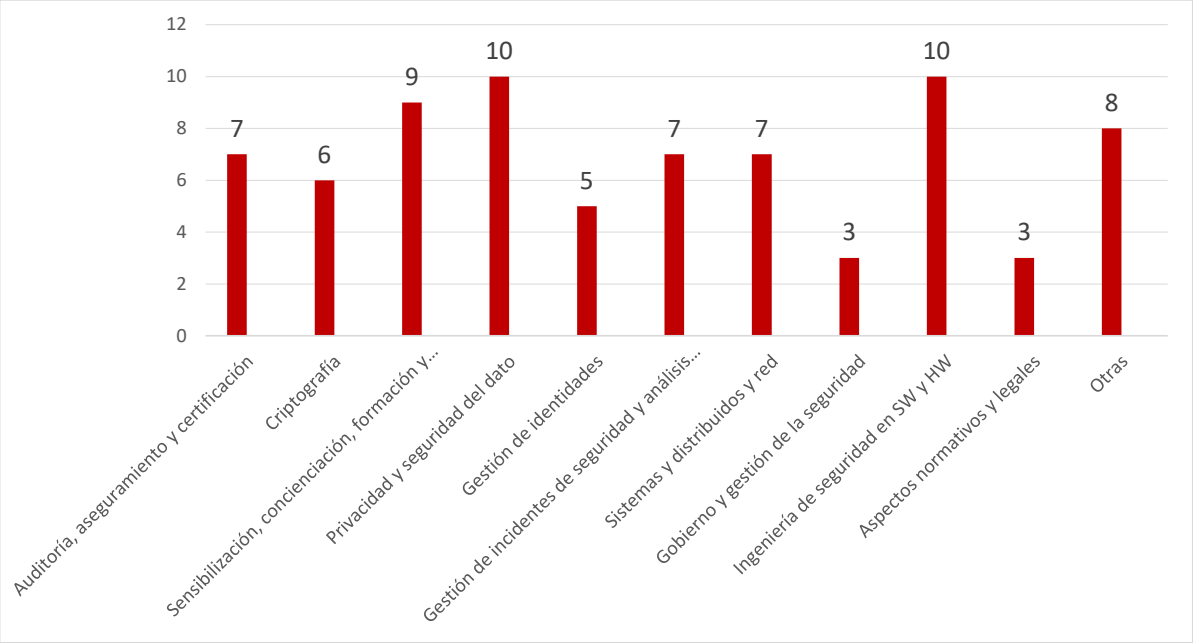


Figura 163. P82: Datos IoT. Tecnologías con mayor impacto para ciberdefensa

La representación gráfica de estos datos se muestra en la siguiente figura:

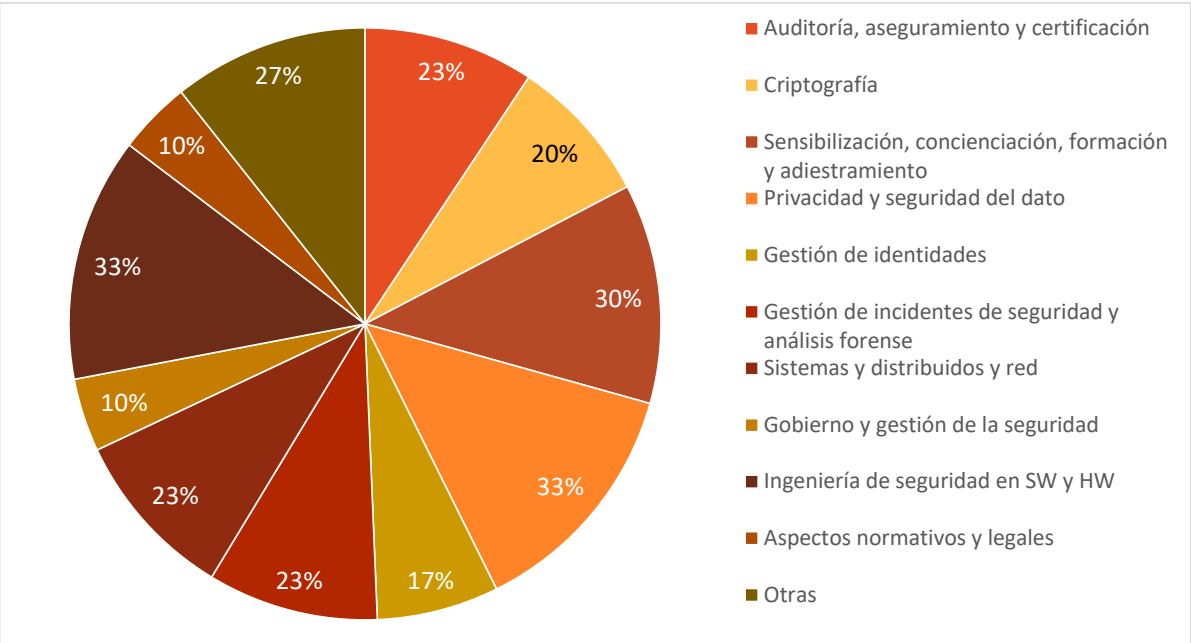


Figura 164. P82: Gráfico. IoT. Tecnologías con mayor impacto para ciberdefensa

Las entidades encuestadas afirman ser capaces de ofrecer valor añadido en un amplio espectro de aplicaciones de las tecnologías IoT para la ciberdefensa, especialmente en las que tienen que ver con la **privacidad y seguridad del dato**, la **Ingeniería de seguridad** hardware **y** software, o la **sensibilización, concienciación, formación y el adiestramiento**. Dentro de estas capacidades, alguna entidad indica estar realizando trabajos relacionados con la **protección del** firmware y las **comunicaciones seguras** IoT.

En menor medida, creen no ser tan capaces de aportar capacidades para el **gobierno y la gestión** de la seguridad del dispositivo, o en el **cumplimento de aspectos normativos y legales.**

En general, las entidades han indicado tener una buena capacidad para realizar desarrollos en los ámbitos de la seguridad de los elementos IoT, sus comunicaciones y de los datos gestionados; no así en otros más propios de la gestión y el cumplimiento normativo.

Destaca la capacidad de las entidades en el desarrollo de seguridad en IoT, especializándose en la seguridad y protección de las **comunicaciones** de los dispositivos IoT conectados y de los **datos** tratados por estos.

7.12. Inteligencia artificial

Los datos recogidos en la pregunta 83. *¿Cuál de las siguientes actividades relacionadas con la inteligencia artificial considera más relevante para el ámbito de la ciberdefensa?*, se muestran en la siguiente figura:

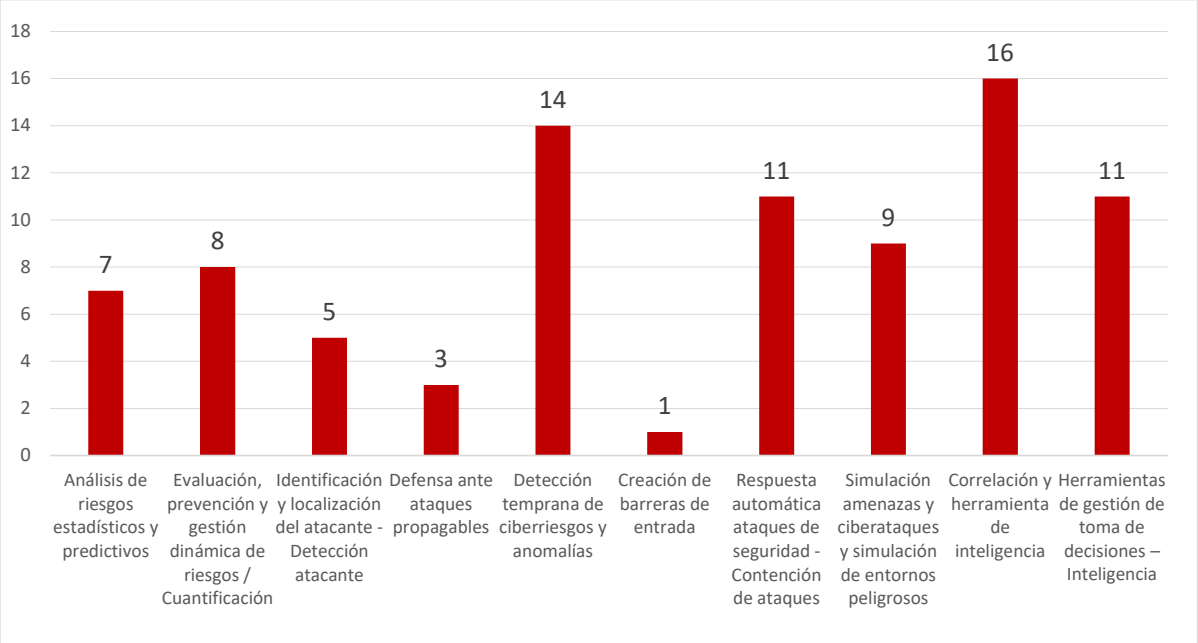


Figura 165. P83: Datos Inteligencia artifical

La representación gráfica de los datos se muestra en la siguiente figura:

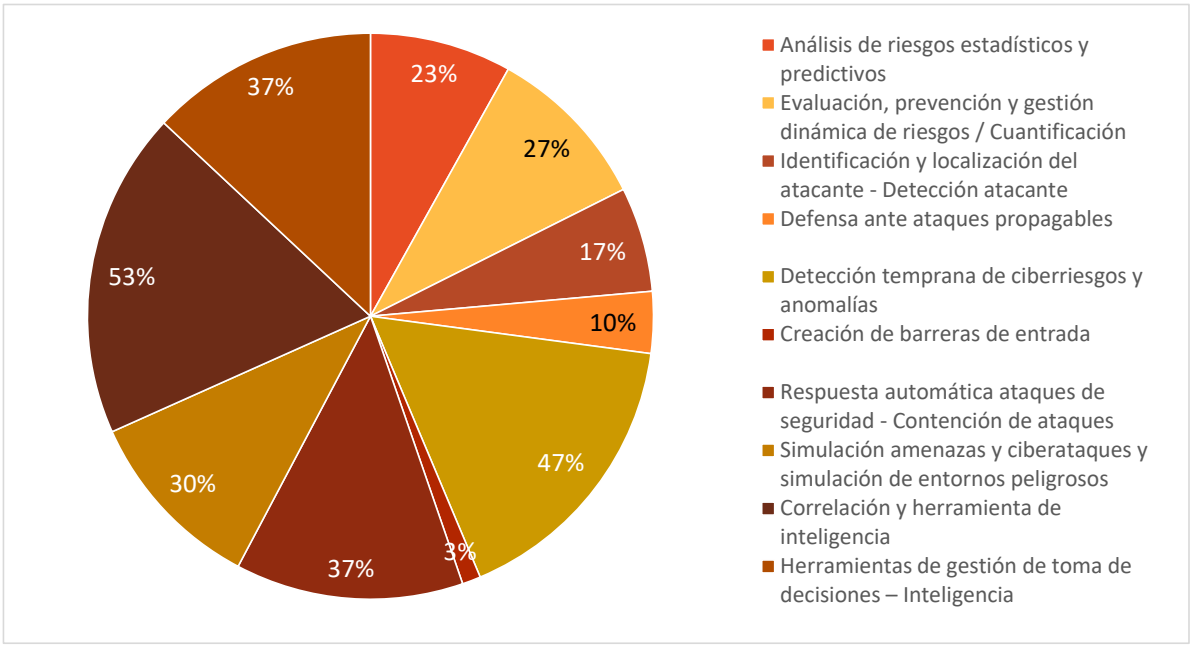


Figura 166. P83: Gráfico. Inteligencia artifical

El 53% de las entidades destaca el beneficio que permitiría el uso de esta tecnología para la **correlación y herramienta de inteligencia,** mientras que el 47% indica el avance que podría suponer para la **detección temprana de ciberriesgos y anomalías**.

Al mismo tiempo vemos como en un porcentaje similar, en torno al 37%, se identifican el **apoyo a la toma de decisiones** y las **respuestas automáticas frente ataques** como otras dos actividades que mejorarían sustancialmente la protección y defensa frente a ciberamenazas.

La respuesta menos seleccionada por las entidades ha sido la asociada a la **creación de barreras de entrada**.

Los resultados obtenidos en esta pregunta indican que las actividades más relevantes asociadas a la IA para las entidades consultadas son las que se enmarcan en capacidades para la detección del atacante, la detección temprana de ciberriesgos, gestión de decisiones y respuestas automáticas.

7.13. Biometría

El análisis de las respuestas sobre esta tecnología se desglosa en dos áreas que se detallan a continuación:

Técnicas biométricas utilizadas para desarrollar productos o servicios

Los datos recogidos en la pregunta 84. *¿Qué técnicas biométricas más avanzadas están utilizando o desarrollando en sus productos o servicios?*, se muestran en la siguiente figura:

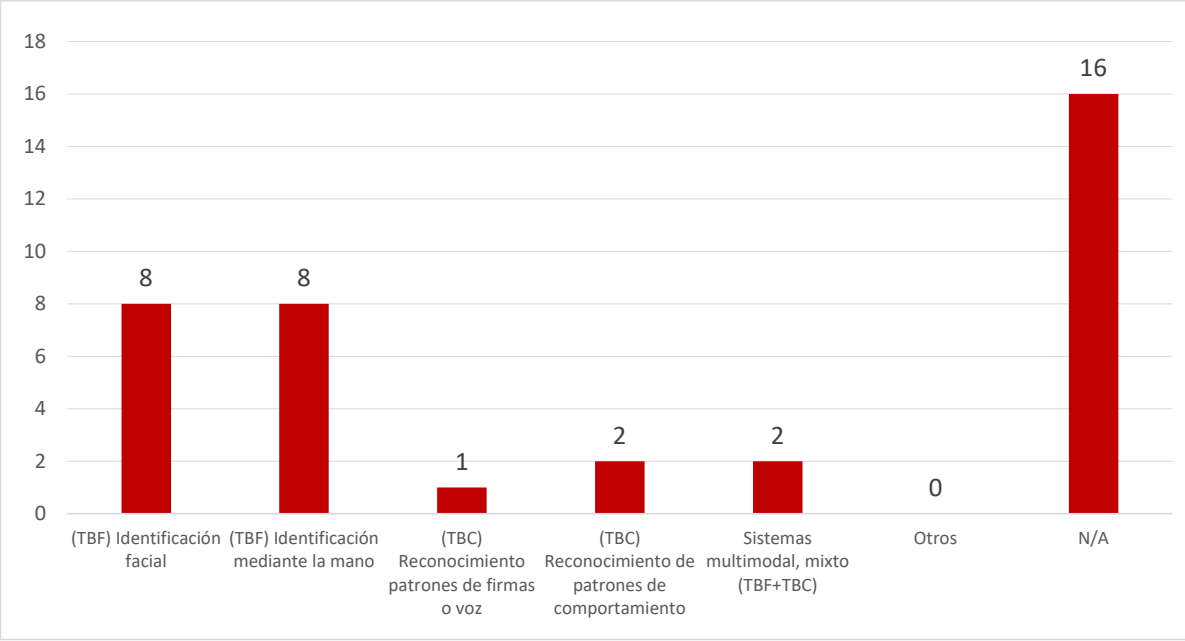


Figura 167. P84: Datos biometría. Técnicas utilizadas

La representación gráfica de los datos se muestra en la siguiente figura:

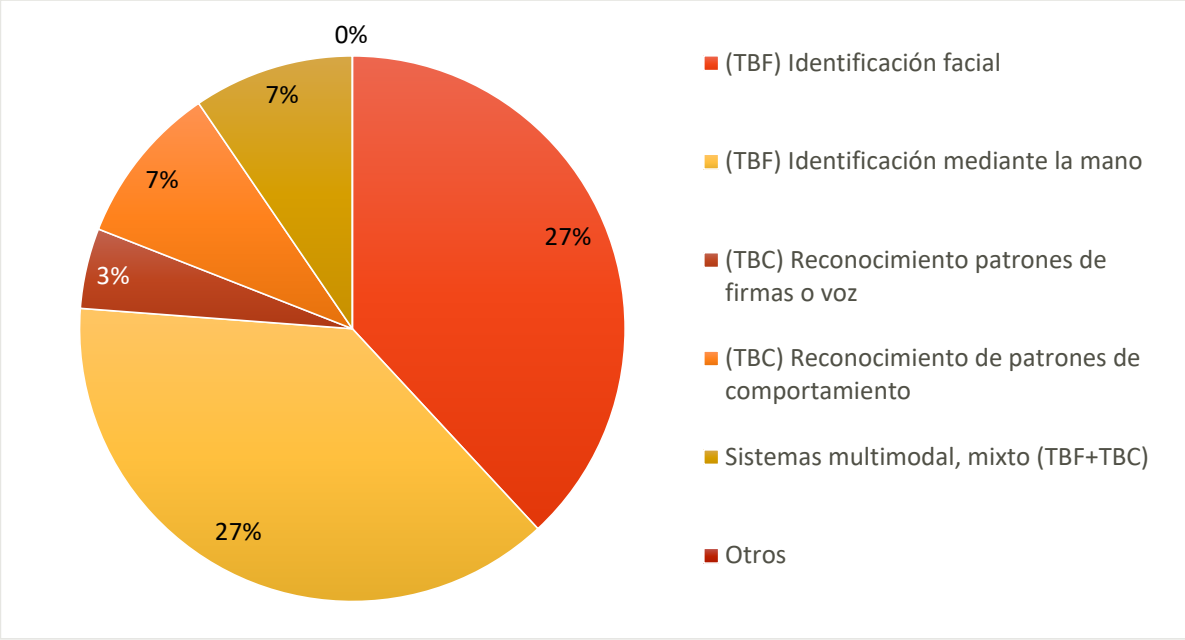


Figura 168. P84: Gráfico. Biometría. Técnicas utilizadas

Atendiendo a los resultados de la primera pregunta sobre esta tecnología, podemos observar que el 27% de las entidades que están integrando esta capacidad en el ámbito de la ciberseguridad, lo hacen para la **identificación** y **acceso de personas** mediante **tecnologías TBF**.

Capacidades de cifrado con técnicas biométricas

Los datos recogidos en la pregunta 85. *¿Está desarrollando capacidades de cifrado con técnicas biométricas?*, se muestran en la siguiente figura:

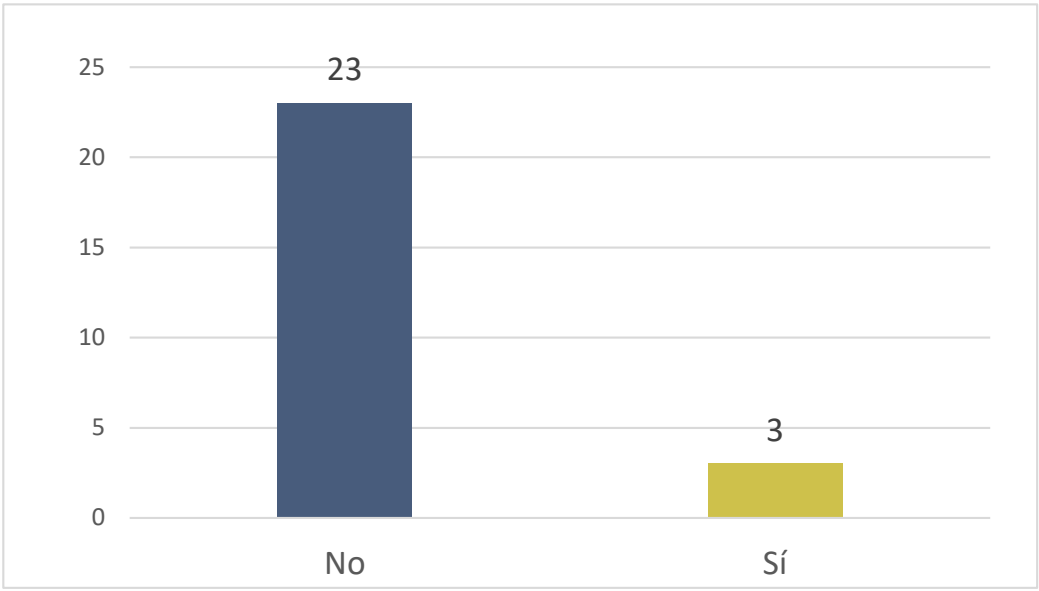


Figura 169. P85: Datos biometría. Capacidades de cifrado

La representación gráfica de los datos se muestra en la siguiente figura:

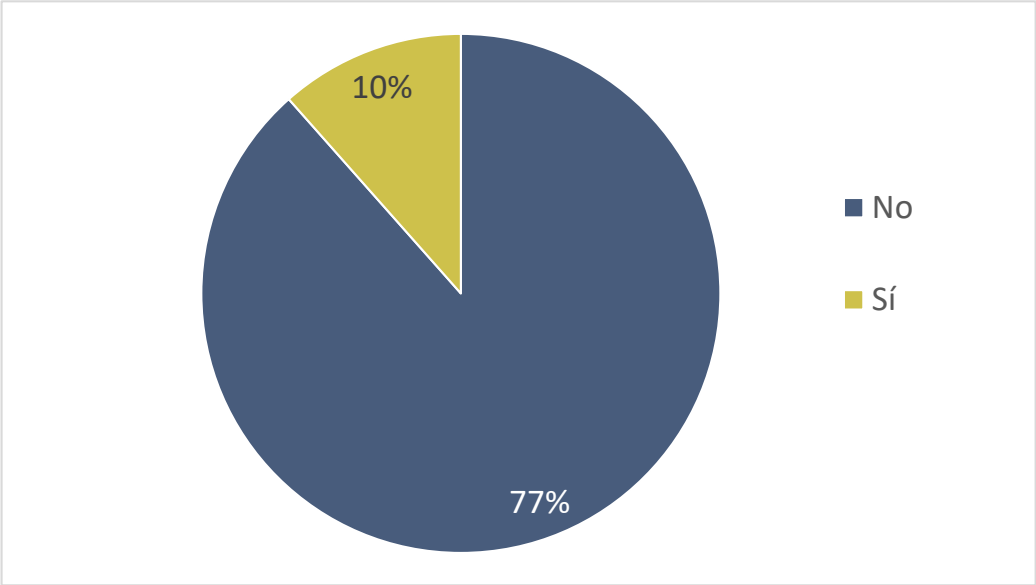


Figura 170. P85: Gráfico. Biometría. Capacidades de cifrado

En cuanto a técnicas de comportamiento, son muy pocas entidades, apenas un 10%, las que las integran.

Como conclusión del apartado, cabe destacar que más de la mitad de las entidades aplican actualmente la tecnología TBF para identificación y acceso, mientras que una cuarta parte sólo usa las tecnologías TBC ocasionalmente.

Además, el desarrollo de la tecnología de cifrado con biometría por parte de las entidades participantes de este estudio es muy bajo, siendo principalmente consumidores de soluciones. Solo un 10% de las que las usan desarrollan aplicaciones para *onboarding digital* o protección de información en aplicaciones móviles integradas con biometría para diferentes plataformas como Android o IOS.

8. CONCLUSIONES

A continuación, se presentan las principales conclusiones alcanzadas tras el análisis de los datos estudiados y de los resultados obtenidos. Se han agrupado según los apartados analizados.

Capacidades operativas

Las conclusiones que se muestran a continuación están orientadas al desarrollo de las capacidades operativas identificadas para la ejecución de operaciones militares de ciberdefensa.

Oferta limitada de desarrollos y productos para su empleo por parte del MINISDEF

El sector industrial cuenta con buenas capacidades de desarrollo de ciberdefensa, pero carece de un buen catálogo de productos concretos. Esta oferta se podría ver ampliada con un incremento de la inversión por parte de las empresas del sector y un mayor apoyo del MINISDEF, lo que aumentaría la capacidad de la Industria nacional en este mercado y mejoraría su posicionamiento en un entorno multinacional.

Es un hecho que dicha limitación también está condicionada por el exigente modelo de contratación, inherente al sector de la defensa.

Potencial para el desarrollo de soluciones aplicables en el ámbito de coordinación y control

Si bien la mayor parte de las soluciones existentes están orientadas a las necesidades de los centros de operaciones de seguridad, también suponen una base importante para el desarrollo de soluciones que cubran las necesidades y características más avanzadas y específicas requeridas para la coordinación y control de las operaciones en el ciberespacio. La solvencia técnica y experiencia de las entidades españolas en el desarrollo de este tipo de herramientas para el resto de los ámbitos de las operaciones (tierra, mar, aire y espacio) hace que este sea también un buen punto de partida.

Buen nivel de desarrollo de soluciones de capacidades de defensa

Por tratarse del área más extendida, existe un buen número de entidades enfocadas en este campo qde los resultados obtenidos. Se han agrupado según los apartados analizados. Por ello, es recomendable lograr un mayor aprovechamiento de las fortalezas y experiencias adquiridas en este ámbito para aumentar las soluciones nacionales en cada una de las subcapacidades. Se aprecia en todas ellas un incipiente interés en el desarrollo

de soluciones propietarias. Además, sería deseable conseguir la interoperabilidad entre estas soluciones para contribuir a una capacidad nacional global.

Limitada capacidad nacional para el desarrollo de soluciones aplicables al ámbito de explotación

Dentro de la capacidad de explotación, se aprecia una desigual oferta de soluciones en función de la subcapacidad considerada. Por una parte, la respuesta es amplia en lo relativo a subáreas a subáreas tales como recolección de inteligencia de fuentes abiertas, reconocimiento o representación de la información. Mientras en las subcapacidades donde apenas existen desarrollos propios, como en análisis de redes sociales, anonimización o generación de avatares e identidades digitales, las entidades se apoyan en soluciones y servicios de terceros.

Escaso catálogo de desarrollos aplicables a la capacidad de respuesta

Por lo general, el número de entidades que declara poseer capacidades de desarrollo en las distintas subcapacidades relacionadas con la capacidad de respuesta (como persistencia, escalada de privilegios o exfiltración) es bastante más reducido que en el resto. Esto era lo previsible, dado que se trata de un ámbito de actuación muy restringido y de menor demanda. Asimismo, debe entenderse que la orientación de estos desarrollos está dirigida al ámbito civil y, más concretamente, al de las auditorías de sistemas (*hacking* ético, *pentesting*, *red team*, ...). No obstante, estas capacidades tienen una naturaleza dual y podrían ser aprovechables en el ámbito de las operaciones militares en el ciberespacio.

Gran margen de desarrollo y mejora en la capacidad de apoyo técnico

En el área de apoyo técnico a las operaciones destaca un desarrollo desigual en función de las subcapacidades. Si bien todos los desarrollos relativos a la generación y uso de *cyberranges* son punteros y muy extendidos, no ocurre lo mismo con las áreas relativas al desarrollo específico de *malware* o al despliegue automático de sistemas.

En el resto de las tecnologías que se han analizado y que se recogen en el presente informe existe potencial para poder seguir mejorando en el desarrollo de estas áreas y y en su conocimiento profundo.

Cuestiones generales y datos de las entidades

Buen nivel de colaboración público-privada entre entidades de ciberseguridad y ciberdefensa con el sector público

El sector público cuenta con el apoyo de la industria nacional de ciberseguridad y ciberdefensa a raíz de los datos obtenidos. La mayoría de las entidades ha colaborado con él en algún momento, participando en algún proyecto o licitación. Además, la mayoría de las entidades cuenta con personal que conoce las estructuras y procesos del MINISDEF y de las Fuerzas Armadas, lo que facilita su buena relación.

Necesidad de concienciar a las entidades sobre la importancia de dar visibilidad a sus capacidades

Es importante recalcar que este informe aporta el valor de ser el primero en tratar de identificar las empresas nacionales con capacidades específicas de Ciberdefensa, y que en él se incluye un porcentaje muy significativo de este segmento industrial.

Este trabajo se ha basado principalmente en la alta participación de las empresas relacionadas con el ámbito de la ciberdefensa asociadas a TEDAE y de las inscritas en el registro de empresas de la DGAM. Además, se decidió incrementar al máximo el espectro de las entidades a las que se distribuyó el cuestionario para ampliar, en la medida de lo posible, la información recopilada. Por eso se completó con centros tecnológicos y universidades asociadas a RENIC, junto con otras empresas inicialmente identificadas que pudieran tener alguna implicación o aportación en el sector que colaboran habitualmente con el MINISDEF.

De las 120 entidades invitadas a participar en el estudio, 88 mostraron interés y finalmente treinta han compartido sus cuestionarios con el GT4 con distinto nivel de detalle. Estas respuestas han ayudado a profundizar en el análisis y a detectar los retos, a la vez que han mostrado la necesidad de concienciar a las entidades sobre la importancia de visibilizar sus capacidades y su participación en proyectos similares.

Concienciación en ciberseguridad

A pesar de que casi la totalidad de las entidades dispone de un plan de gestión de seguridad de la información, sólo la mitad de las entidades ha realizado las gestiones necesarias para obtener un certificado ISO 27K o similar que confirme la idoneidad de su implantación. Este es un aspecto importante que se debe revisar para mejorar la concienciación en ciberseguridad en las entidades.

Cabe destacar que la mayoría de las entidades conoce y aplica las guías del CCN-STIC. Este es un aspecto importante en la gestión de la ciberseguridad de los sistemas y de los servicios prestados en el ámbito del MINISDEF que, aun no siendo de aplicación habitual en el ámbito civil, ayudaría a mejorar su concienciación.

Disponibilidad de HSEM/HPS

A pesar de que la mayoría de las entidades que responden al cuestionario dispone de las habilitaciones de seguridad de empresa y del personal para poder participar en proyectos clasificados del MINISDEF, sería recomendable que más entidades siguieran su ejemplo para asegurarse de poder cubrir todas las necesidades de defensa con las garantías suficientes.

Una posible causa es que el procedimiento de obtención de estas habilitaciones de seguridad no es sencillo ni rápido. Existe margen para mejorar y simplificar este procedimiento, lo que facilitaría la incorporación de más entidades a proyectos de defensa y que permita aumentar la masa crítica de personal cualificado para trabajar en el sector de la defensa.

Ámbitos tecnológicos

Margen de mejora en la investigación y desarrollo de las tecnologías identificadas para el ámbito de la ciberdefensa

La seguridad en las redes, la inteligencia artificial, la criptografía, los dispositivos móviles y el procesamiento de lenguaje natural son las tecnologías en las que más se están enfocando en el corto plazo las entidades consultadas. De estas, las tres primeras son las que más aplicación a la ciberdefensa encuentran las entidades, y las dos primeras en las que más están invirtiendo, habitualmente cantidades inferiores a 100.000€. En el largo plazo, una pequeña parte de las entidades muestra interés en otras tecnologías, entre las que destacan *blockchain* y seguridad en redes.

El aspecto económico, la falta de estándares relacionados y la compleja infraestructura requerida son las barreras tecnológicas destacadas en el desarrollo e implementación de las tecnologías propuestas por las entidades.

Tecnologías de gran potencial infrautilizadas

Se han identificado tecnologías con funcionalidades muy potentes que en un futuro serán imprescindibles, aunque las entidades no las están desarrollando a corto plazo o se están aplicando para tareas básicas y sus funcionalidades podrían ser mejor aprovechadas. No obstante, las entidades han mostrado interés en su desarrollo a largo plazo.

Ejemplos de estas tecnologías son el procesamiento de lenguaje natural, empleado para automatizar parcialmente las tareas de los analistas, el *data mining* y analítica avanzada que se emplea solo para la correlación de eventos y la detección de anomalías, o la realidad virtual y realidad aumentada, que se usa para tareas de formación.

Incremento del uso de servicios en la nube proporcionados por proveedores externos

Se aprecia que cada vez más las organizaciones están recurriendo a proveedores externos, incluso para requerimientos con un relevante nivel de seguridad, al contrario de lo que se hacía tradicionalmente cuando se empleaban elementos propios y dedicados. Un buen ejemplo de esto es el uso de diferentes modalidades de tecnologías *cloud* proporcionadas como servicio.

La RPA facilitará la gestión de ciberincidentes en el futuro

La RPA (*Robotic Process Automation*) aplicada a incidentes y a la localización de los atacantes serán capacidades que apoyarán a la ciberdefensa. Esta tecnología y su integración con sistemas SOAR (*Security Orchestration, Automation and Response*) ayudarán a los servicios de ciberdefensa, facilitando la identificación de posibles ataques y amenazas, y permitiendo priorizar otras actividades más urgentes.

Formación y necesidad de mejora en los desarrollos relacionados con seguridad móvil

La mayoría de las entidades son conscientes de la necesidad e importancia de disponer de conocimiento específico y desarrollar determinadas capacidades avanzadas relacionadas con la implementación de medidas de seguridad *software* y *hardware* en los propios terminales y así como en la información y los datos.

Necesaria aplicación de mecanismos de ciberseguridad para apoyar las capacidades de defensa ante ataques propagables

Los mecanismos de ciberseguridad están ayudando a las entidades a mitigar la propagación de los ciberataques, siempre y cuando tengan una idea clara del perímetro que se debe proteger,, ya que este se ha difuminado y ampliado debido a la movilidad, los entornos *cloud* y la virtualización.

Estado incipiente de aplicación del *blockchain* y DLT al ámbito de la ciberdefensa

La mayoría de entidades creen que la tecnología del *blockchain* y DLTs es muy relevante para la ciberdefensa a raíz del interés mostrado en los distintos usos propuestos, especialmente en la verificación de la cadena de custodia, la trazabilidad o el forense. Sin embargo, este dato contrasta con el escaso número de entidades que finalmente realiza desarrollos relacionados con la privacidad y seguridad del dato.

Margen de mejora de las tecnologías cuánticas y postcuánticas y los mecanismos criptográficos avanzados

Las tecnologías cuánticas y postcuánticas no son una tecnología madura. Aun así, contamos con un grupo de entidades que trabaja en ellas, principalmente en temas de distribución cuántica de claves y criptografía postcuántica, y que incluso participa en proyectos europeos relacionados con el desarrollo de redes de comunicaciones seguras para defensa.

Por otro lado, aunque existen mecanismos criptográficos avanzados, todavía no son empleados por todas las entidades.

Buena capacidad en desarrollos de seguridad de ciertos ámbitos IoT y posibilidad de mejora en otros

Existe buena capacidad por parte de las entidades en el desarrollo de seguridad en IoT, especializándose en la seguridad y protección de las comunicaciones de los dispositivos IoT conectados y de los datos tratados por estos, con margen de mejora en otras capacidades como el gobierno y gestión de la seguridad del dispositivo o el cumplimento normativo y legal.

Bajo desarrollo de capacidades basadas en tecnologías biométricas

Destaca que solo una pequeña parte de las entidades emplea las tecnologías biométricas para el desarrollo de aplicaciones, siendo principalmente consumidores de soluciones de terceros. Relacionado con estas tecnologías, las TBF son las más aplicadas en sus desarrollos y las TBC las menos.

9. RETOS Y OPORTUNIDADES DE FUTURO

En esta sección de retos y oportunidades de futuro se abordan tanto las necesidades identificadas para la mejora como la la falta de desarrollos o herramientas en ciertas áreas que se ha estimado que es necesario tener cubiertas con las capacidades de las entidades nacionales. A continuación, se muestran los resultados más relevantes sobre dichas necesidades agrupados por los apartados analizados.

Capacidades operativas

Según hemos visto, la ciberdefensa está en plena evolución y requiere de una amplia potenciación de la industria nacional con las capacidades necesarias para hacer realidad los siguientes desarrollos:

- Sistemas de **planificación, mando, coordinación y control** de operaciones en el ciberespacio, especialmente en las subcapacidades de control de Ejecución de ciberoperaciones y consciencia situacional en ciberdefensa.
- Sistemas de **defensa**, especialmente en las subcapacidades de defensa activa y pasiva, recolección de información y despliegue de centros de operaciones de seguridad.
- Sistemas de **explotación** para extraer datos e información de las redes y sistemas, y elaborar inteligencia especifica en el ciberespacio, especialmente en las subcapacidades de recolección de inteligencia de fuentes abiertas, reconocimiento, representación de la información, análisis de redes sociales, anonimización o generación de avatares e identidades digitales.
- Sistemas de **respuesta** para lograr un efecto sobre los activos del adversario en el ciberespacio o a través de él, especialmente en las subcapacidades de persistencia, escalada de privilegios o exfiltración.
- Sistemas de **apoyo técnico a las operaciones** en el ciberespacio, especialmente en las subcapacidades de laboratorio de análisis forense digital, despliegue automático de sistemas seguros o *combat cloud*.

En definitiva, es la hora de aprovechar el nuevo ciclo de incremento de los presupuestos en defensa, derivados de los importantes cambios geoestratégicos, para consolidar unas disciplinas que son parte de la piedra angular que tiene que soportar la Seguridad Nacional, lo que deriva en inversiones sostenibles en el tiempo para la adquisición de capacidades.

Cuestiones generales y datos de las entidades

En la primera parte del cuestionario se ha consultado a las entidades sobre datos generales y sobre asuntos relacionados con la seguridad propia y su relación con el sector público, especialmente con el de defensa. Se han encontrado ciertas deficiencias que podrían resolverse con las siguientes acciones:

- Fomentar que las entidades se interesen en las **licitaciones** y se incremente el número de entidades registradas en la **Plataforma de Contratación del Sector Público**.
- Como se ha comentado, la ciberseguridad es un ámbito de especial interés para la Seguridad Nacional, que tiene singularidades muy específicas en el ámbito de la defensa. Esto requiere conseguir un mayor número de entidades especializadas en Ciberseguridad con **expertos** que conozcan las **necesidades, estructura y procesos** del Ministerio de Defensa y de las Fuerzas Armadas entre su personal fijo.
- Promover y facilitar la **internacionalización de las entidades españolas** del sector, fomentando su participación en proyectos de cooperación internacionales del ámbito OTAN y UE, como forma de adquisición y fortalecimiento de las capacidades propias.
- Conseguir que el 100% de las entidades cuenten con un **SGSI implantado** y una **certificación** de la serie ISO 27K o similar, e implanten **Planes de Concienciación** en Ciberseguridad a todos los empleados.
- Conseguir que el 100% de las entidades conozcan y apliquen las **guías CCN-STIC**, y participen activamente en la formación del CCN sobre sus guías, requeridas en las licitaciones de defensa.
- Mejorar y simplificar el **procedimiento de obtención de las habilitaciones de seguridad** (HSEM/HPS) logrando que sea más sencillo y rápido, de forma que facilite la incorporación de más entidades a proyectos de defensa y que permita aumentar la masa crítica de personal cualificado para trabajar en el sector de la defensa.
- Realizar acciones que fomenten que las entidades vean la **Ciberdefensa** como un dominio de aplicación de todas las tecnologías tratadas en el presente informe.
- Derivada del número de respuestas, se concluía que la **participación** de entidades en el estudio ha sido **baja**, lo que ha dificultado extraer resultados concluyentes. Por ello, uno de los retos que debemos plantearnos es la difusión del Foro y sus objetivos para conseguir una mayor participación de entidades en futuros estudios similares, con especial énfasis en la academia y centros de investigación o tecnológicos. La obtención de capacidades de ciberdefensa se considera básica para la Seguridad Nacional y una adecuada colaboración público-privada es la forma más eficiente de conseguirlo.

Ámbitos tecnológicos

Los resultados de este primer estudio, proyectan la necesidad de fomentar la incorporación de las nuevas tecnologías en el desarrollo de las capacidades de ciberdefensa. Esto nos lleva a la urgente necesidad de **definir un plan estratégico** que priorice un conjunto de estas tecnologías según su adecuación al desarrollo de las capacidades operativas de ciberdefensa y un **plan de acción** que proporcione las palancas necesarias para su rápido desarrollo. Este plan debe contemplar, entre otros, los siguientes objetivos:

Incentivar la **incorporación de las tecnologías** de interés y con mayores limitaciones en el hoja de ruta de las entidades.

- Establecer la necesidad de **desarrollos** de aplicaciones para el uso en el **ámbito de la defensa**, que incorporen las diferentes tecnologías analizadas, identificando su prioridad.
- Potenciar e incentivar la **inversión en I+D+i** de las entidades para las diferentes tecnologías analizadas, estableciendo líneas estratégicas priorizadas según su importancia para el desarrollo de la ciberdefensa.
- Proporcionar **mecanismos** ágiles de **financiación y cofinanciación y subvención**, orientadas a iniciativas relacionadas con las líneas estratégicas para las diferentes tecnologías.
- Colaborar en el **desarrollo de estándares** de las distintas tecnologías que adolecen de estos para facilitar su implantación.
- Utilizar la tecnología de **realidad virtual** para simulaciones de ataques complejos que permitan evolucionar sistemas como los IDS o *Honeypots*.
- Evolucionar los sistemas **RPA** para predecir e interactuar como un humano en RRSS, apoyar en la identificación, localización y exfiltración de la información de los atacantes.
- Priorizar el empleo de los **mecanismos criptográficos** más avanzados frente a la securización de las comunicaciones con mecanismos más característicos de IT.
- **Reto general**: Dar mayor difusión a las **posibilidades y funcionalidades** que ofrecen las distintas tecnologías tratadas en el presente informe con aplicación en el sector de la ciberdefensa y que le puedan ser desconocidas a las entidades. Además, se debe promover la **formación** para adquirir los conocimientos específicos que permitan el desarrollo de las capacidades relativas a este ámbito. Asimismo, se debe potenciar el desarrollo nacional de dichas capacidades, de forma coordinada entre los diferentes actores, buscando su interoperabilidad y evitando una dependencia tecnológica de terceros.

ANEXO I: Descripción de los ámbitos tecnológicos

A continuación, se amplía la información relativa a los diferentes ámbitos tecnológicos que se contemplan en el estudio:

Realidad virtual y realidad aumentada

A efectos del presente estudio, se entiende realidad virtual como el uso de la tecnología informática para crear un entorno simulado de manera lo suficientemente realista como para engañar al cerebro humano para que los acepte como realidad y realidad aumentada como un conjunto de tecnologías que combinan imágenes reales y virtuales, de forma interactiva y en tiempo real, de manera que permite añadir la información virtual a los elementos que el usuario dispone dentro del mundo real.

En el estudio se pretenden analizar la aplicación de la realidad virtual y realidad aumentada como elementos claves en la formación ante situaciones de emergencia y crisis, así como la asistencia virtual en las operaciones de ciberdefensa. Esto aplica tanto al plano defensivo como ofensivo.

En el ámbito de la ciberdefensa, se contempla principalmente el desarrollo de las siguientes capacidades:

- Identificación y autenticación: de cara a permitir visualizar gráficamente las amenazas en curso (con su nivel de riesgo asociado) o el grado de efectividad de las protecciones (permitiendo la identificación de los puntos débiles) o disponer distintas vistas gráficas con agrupaciones por tipos de actividades, servicios o adversarios (que facilite la explotación de la información), facilitando así la toma de decisiones,
- Simulación sensores externos: para permitir disponer de entornos de pruebas para la capacitación de los analistas.
- Simulación de ciberataque: para permitir disponer de simulaciones de ciberataques que permitan la capacitación de los analistas y realizar pruebas sobre los entornos simulados de las TTP (táctica, técnicas y procedimientos).

Cloud y fog computing

La computación en la nube (*cloud computing*) se ha convertido en la última década en un paradigma informático ampliamente adoptado por muchas organizaciones, debido a sus características dinámicas como la elasticidad y el pago por uso.

Para poder ofrecer estas características, la virtualización es uno de los pilares de gestión de los proveedores de la nube. Las máquinas virtuales y los contenedores permiten a los proveedores compartir porciones de sus recursos informáticos, normalmente desplegados en grandes centros de datos, entre los usuarios, dando lugar a un sistema aislado lógicamente para cada cliente.

La computación bajo demanda se ofrece en tres modalidades: Infraestructura como servicio (IaaS), Plataforma como servicio (PaaS) y *Software* como servicio (SaaS).

Aunque la computación en nube ha contribuido a hacer accesible la computación, el tiempo necesario para acceder a las aplicaciones basadas en la nube puede ser demasiado elevado y no resultar práctico para algunas aplicaciones de misión crítica, o aplicaciones con requisitos de latencia ultra baja. Además, el rápido crecimiento de la cantidad de datos generados en el borde de la red por un número creciente de dispositivos conectados requiere que los recursos de la nube estén más cerca de donde se generan los datos. La mayor demanda de procesamiento de datos de gran ancho de banda, geográficamente dispersos, de baja latencia y sensibles a la privacidad ha hecho surgir una necesidad esencial de paradigmas informáticos que tengan lugar más cerca de los dispositivos conectados y que admitan aplicaciones descentralizadas de baja latencia y gran ancho de banda. Para responder a estas necesidades, tanto la industria como el mundo académico han propuesto la computación en la niebla, más conocido por su nombre en inglés *fog computing* cuyo objetivo principal es proporcionar servicios similares a los de la nube, pero cerca de los suscriptores en el borde (*edge*) de la red.

Teniendo en cuenta que cada vez más entidades completan su transformación digital y migran sus servicios a la nube, la ciberseguridad cobra mayor importancia. Además, la descentralización de los datos en infraestructuras no controladas por los propietarios que incluso geográficamente pueden estar fuera del territorio nacional conlleva nuevos problemas que requieren adaptaciones en los procedimientos y en el marco legal. En el ámbito específico de la defensa esto cobra especial importancia incluyendo otras consideraciones que son especialmente relevantes en el ámbito de la *combat cloud* o la *tactical cloud*.

En el ámbito de la ciberdefensa, se contempla principalmente el desarrollo de las siguientes capacidades:

- Creación de barreras de entrada: proporcionando mecanismos de defensa avanzados para las soluciones desplegadas en la nube.
- Identificación y localización del atacante: creando herramientas para permitir conocer la identidad del atacante y la localización desde donde se realizó.
- Privacidad y confidencialidad en la nube: actualizando y completando los procedimientos y el marco legal, contribuyendo a asegurar que la información se almacena de forma segura.
- Autenticación en transacciones a nivel global en la nube: mejorando los mecanismos actuales de autenticación.

Procesamiento de lenguaje natural

A efectos del presente estudio, se considera el procesamiento de lenguaje Natural (NLP: Natural Language Processing) como el campo de la inteligencia artificial en el que los ordenadores analizan, comprenden y obtienen el significado del lenguaje humano de forma inteligente y útil. Al utilizar NLP, se puede organizar y estructurar el conocimiento para realizar tareas como el resumen automático, la traducción, el reconocimiento de entidades con nombre, la extracción de relaciones, el análisis de sentimientos, el reconocimiento del habla, la segmentación de tópicos, etc. El objetivo de NLP es que las máquinas comprendan cómo nos comunicamos los humanos por vía oral o escrita.

En este estudio se desea investigar sobre la aplicación de técnicas de NLP en el ámbito de la ciberdefensa. En los últimos años el crecimiento de aplicaciones e investigaciones sobre NLP ha sido exponencial, por tanto, puede deducirse que el aprendizaje automático para el procesamiento del lenguaje desempeña un papel cada vez más relevante en la interacción hombre máquina. Sus capacidades analíticas y de generación automática de lenguaje, tanto escrito como hablado, lo están convirtiendo en una importante herramienta en manos de todo tipo de actores con fines de información o desinformación en torno a la ciberseguridad.

En el ámbito de la ciberdefensa, se contempla principalmente el desarrollo de las siguientes capacidades:

- Correlación y herramienta de Inteligencia: incluye las técnicas para fusionar y explotar de forma automatizada información textual o hablada permitiendo la obtención ágil de inteligencia.
- Identificación y localización del atacante, detección del atacante: comprende el análisis, procesamiento y transmisión de información valiéndose de los principios y efectos de la mecánica cuántica. El objetivo es tanto complicar al máximo la vulneración de la confidencialidad de la comunicación como la obtención de información del enemigo gracias a la computación cuántica.
- Recolección y análisis de información: proporcionando herramientas que reduzcan el tiempo y esfuerzo empleado por los analistas y por tanto contribuyendo al proceso de toma de decisiones.
- Perfiles en RRSS: NLP puede aplicarse para realizar análisis de sentimiento y de intenciones en redes sociales, facilitando un indicador más para los cuadros de mando de los sistemas de ciberdefensa.

RPA y automatización

A efectos del presente estudio, se entienden como RPA (*Robotic Process Automation*) aquellas tecnologías basadas en un robot *software* o *soft-bot*, que procesa automáticamente aquellas tareas repetitivas o basadas en reglas.

La necesidad acuciante de recursos especializados en el ámbito de la ciberdefensa, así como la posibilidad de asignar las tareas más importantes a las personas más valiosas, están impulsando ampliamente las tecnologías de automatización.

Otro hecho relevante viene de la mano de poder minimizar los errores relacionados con labores manuales a través del uso de RPA.

En el ámbito de la ciberdefensa, se contempla principalmente el desarrollo de las siguientes capacidades:

- Respuesta automática incidentes seguridad, tomando decisiones autónomas y minimizando los falsos positivos fundamentalmente en el ámbito de la gestión de incidentes de seguridad y análisis forense.
- Identificación y localización del atacante, detección automática de la identidad del atacante basado en algoritmos avanzados, cuando se está gestionando un incidente de seguridad.
- Automatización perfiles RRSS, generación de perfiles en RRSS de forma automática consiguiendo el máximo de personalización y evitando técnicas de detección de falsos avatares.
- Automatización de auditorías, proporcionando una búsqueda de información avanzada de las vulnerabilidades permitiendo generar información compleja basada en el impacto de la misma en la organización.
- Búsqueda de información automática, seleccionando la información más valiosa tanto para casos de prevención en donde se hace foco en la privacidad y seguridad del dato cómo en caso de respuesta en un incidente real.

Dispositivos móviles

A efectos del presente estudio, se entienden como dispositivos móviles, aquellas tecnologías que posibilitan la recolección y movilidad de datos, activos de información, comunicaciones, sincronización de planificaciones.

La necesidad permanente de una gestión integral de todos los aspectos de seguridad física (espectro incluido) y lógica, y de aprovisionamiento requiere una innovación y mejora constante en procesos y tecnologías que soporten dichas necesidades.

Para el presente estudio, con respecto a RPA, se contempla principalmente el desarrollo de las siguientes capacidades en el ámbito de la ciberdefensa:

- Identificación y autenticación: fortalecer y modernizar actividades básicas de control de la información.
- Cifrado e intercambio de Información: la criptografía es esencial para salvaguardar el secreto e integridad de las comunicaciones.
- Protección de datos (confidencialidad): la confidencialidad es parte esencial del ciclo de vida de la Información.
- Protección de datos (integridad y disponibilidad): la integridad y disponibilidad son otras dimensiones esenciales de la seguridad de la información.
- Protección de sistemas de navegación (GPS): el posicionamiento de los activos es esencial en cualquier planificación operativa y táctica.

- Protección física de datos: la seguridad física de la información es condición necesaria para la integridad de los datos.
- Seguridad en dispositivos móviles: un campo multidisciplinar que integra varias de las habilidades mencionadas en el presente documento.
- Conciencia de la situación: la consciencia situacional es un estado mental que posibilita el ciclo de toma de decisiones.
- Ciudades inteligentes y ciudades seguras: la instrumentación de las ciudades inteligentes habilita la colaboración entre sector militar y civil, además de posibilitar un inicio de defensa ante ataques híbridos.
- Aplicaciones móviles de preservación de la privacidad: los fallos en cadenas de suministro y fabricación a menudo comprometen la privacidad de los datos. Es importante desarrollar aplicaciones que posibiliten, entre otras cosas, fortalecer la privacidad de la información en todo dispositivo móvil.
- *Mobile computing*: el paradigma de *mobile computing* tiene una amplia adopción el sector civil. también puede ser orientado hacia el concepto de *edge computing*.

Seguridad de redes

A efectos del presente estudio, se entiende como seguridad de redes la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

En el estudio se desea conocer el estado de la seguridad de las redes de las organizaciones para medir el grado de madurez de sus sistemas de defensa en operaciones en el ciberespacio. Resulta una parte básica y crítica de la ciberdefensa para fortalecer sus capacidades de reacción y respuesta, y poder desarrollar así sus sistemas de staque.

En el ámbito de la ciberdefensa, se contempla principalmente el desarrollo de las siguientes capacidades:

- Arquitectura de protección de redes y arquitectura resiliente: cubre los servicios de seguridad que se le exigen a una red, los componentes necesarios para proporcionar dichos servicios y las características que se requieren de dichos componentes para enfrentarse eficazmente a las amenazas sean o no previsibles. Además, las redes han de seguir operando pese a estar sometidas a un ataque, aunque sea en un estado degradado o debilitado. Asimismo, incluye la capacidad de restaurar con rapidez sus funciones esenciales después de un ataque.
- Monitorización de la red: es necesaria para tener visibilidad de lo que está pasando y poder reaccionar. Hay que monitorizar los posibles elementos que puedan generar situaciones que comprometan la seguridad, detectando dichas situaciones y permitiendo a un equipo de personas actuar de la forma conveniente en cada caso. Aunque los elementos que se deben monitorizar son muchos, debe considerarse obligatoria al menos la monitorización del entorno tecnológico propio, sobre todo de los elementos necesarios para garantizar los servicios que la

organización presta, en los términos y umbrales necesarios para garantizar la calidad del servicio ofrecido.

- Seguridad de la red: es el conjunto de técnicas y controles de seguridad que se implementan en el interior de los propios equipos y sistemas de tecnologías de la información que forman la red, sea en el *hardware*, o sea en el *software*, para proteger, principalmente, los programas y los datos que procesan, almacenan y transmiten, aunque también prevengan de las amenazas sobre el propio *hardware*.
- Detección de amenazas: es necesario realizar un análisis de riesgos para reducir la probabilidad de que se produzca un incidente de seguridad. Se trata de evitar que una amenaza aproveche una vulnerabilidad para producir daños o pérdidas.
- Esteganografía en la red: esteganografía es la técnica que consiste en ocultar un mensaje u objeto dentro de otro, llamado portador, de modo que no se perciba la existencia del mensaje que se quiere ocultar. A diferencia de la criptografía que se utiliza para cifrar información de manera que sea ininteligible para un probable intruso a pesar del conocimiento de su existencia; la esteganografía oculta la información en un portador de modo que no sea advertido el hecho mismo de su existencia y envío.
- Defensa ante ataques propagables: las acciones para reducir la posibilidad de un ataque son, por ejemplo, la concienciación de empleados, los ejercicios de test de intrusión o *hacking* ético para localizar y corregir vulnerabilidades y los servicios de vigilancia digital para adelantarse a posibles amenazas. Para mitigar la propagación de los ataques se debe mantener los sistemas operativos, aplicaciones y *firmware* actualizados, realizar una monitorización proactiva y mejorar la segmentación de red.
- Exfiltración de datos, fuga o robo de información: es la transferencia de información sensible entre la red de una organización y una ubicación externa controlada por atacantes externos a dicha organización. También puede darse desde dentro de la propia organización (*insiders*).
- Ciencia forense y gestión de evidencias electrónicas: la ciencia forense es la aplicación de herramientas de investigación y técnicas de análisis para recolectar evidencia a partir de recursos informáticos a fin de determinar la causa del incidente de seguridad. Además, se debe garantizar la validez e integridad de las evidencias electrónicas desde su recogida hasta su utilización final.

Blockchain y DLT

El *blockchain* puede describirse como un registro descentralizado de transacciones y eventos digitales, cuya información es aprobada por consenso y almacenada en bloques de transacciones vinculados criptográficamente para hacerlos inalterables, por lo que el más mínimo cambio rompería la cadena.

Confianza y descentralización son dos de las características clave de *blockchain*. La confianza se basa en tres pilares como son la transparencia que reduce las fricciones favoreciendo la interacción, la integridad de los datos a través de la verificación de las transacciones por *peers*, junto con la utilización de la criptografía y la inmutabilidad de las

transacciones acordadas. Por su parte la descentralización se basa en la privacidad y el pseudoanonimato de los participantes, su fiabilidad a través de la redundancia de los datos y su potencial de automatización y su versatilidad.

Los tipos de *blockchain* pueden clasificarse en permisionadas y no permisionadas. En el caso de las permisionadas los miembros de la red son preseleccionados por el administrador del *ledger* que controlará el acceso a la red y reforzará las reglas del *ledger*. En el caso no permisionado no existe un propietario central que controla el acceso a la red. También podemos hablar de tres tipologías de *blockchain*: públicas, si cualquiera puede acceder a ella, privadas si sólo pueden acceder los nodos pertenecientes a la red, e híbridas. La selección de uno u otro tipo depende fundamentalmente del tipo de problema que busca resolverse mediante *blockchain*.

Distributed Ledger Technology o DLT es una aproximación al registro y compartición de datos entre múltiples almacenes de datos denominados *ledgers* y permite registrar, compartir y sincronizar datos y transacciones en una red distribuida de participantes diferentes de la red. *blockchain* es un tipo particular de DLT que almacena y transmite datos en paquetes denominados bloques que están conectados unos a otros en una cadena digital, empleando métodos criptográficos y algorítmicos para registrar y sincronizar de forma inmutable en una red.

Según señala la EDA[27], la confidencialidad y privacidad que posibilita *blockchain* y otros DLT dificultan el objetivo de comprometer la red por parte de los adversarios. También contribuye a crear confianza en los datos digitales ya que la red descentralizada certifica la validez de los datos y guarda un registro digital seguro que no permite la manipulación de los datos, protegiéndolos. Otra posible aplicación en defensa está ligada a la protección de la identidad.

En el ámbito de la ciberdefensa, se contempla principalmente el desarrollo de las siguientes capacidades:

- Control de dispositivos: gestiona el acceso de los usuarios y de otros equipos al dispositivo.
- Defensa ante ataques propagables: evita que un ataque a una determinada zona puede extenderse a otras.
- Trazabilidad, forense y custodia: guarda el registro de lo que ha sucedido en un determinado sistema o red con el objetivo de analizar las causas que lo han provocado y poder custodiar las evidencias y las pruebas para su posterior tratamiento judicial.
- Verificar cadena de custodia: comprobación de que las evidencias y las pruebas no han sido manipuladas durante la cadena de custodia.
- Toma de decisiones: utilización de datos no manipulados para tomar decisiones informadas por parte de las personas pertinentes.

[27] https://eda.europa.eu/webzine/issue14/cover-story/blockchain-technology-in-defence

Criptografía

A efectos del presente estudio, se entienden como criptografía aquellas técnicas orientadas a mantener la información segura transformándola en algo que los receptores no deseados no pueden entender, así como los mecanismos inversos que buscan conseguir transcribir la información que se encuentra cifradas en información accesible.

En el estudio se desea analizar la aplicación de algoritmos, metodologías y herramientas criptológicas modernas para la creación de *software* malicioso y puertas traseras, como así también indagar en técnicas de prevención, detección y protección para ser consideradas en el ámbito de la ciberdefensa. Esto se aplica tanto al plano defensivo como de ataque.

En el ámbito de la ciberdefensa, se contempla principalmente el desarrollo de las siguientes capacidades

- Defensa y protección a ataques con técnicas cuánticas: incluye las técnicas para proteger y quebrantar los sistemas de información en gracias a la computación cuántica
- Comunicaciones cuánticas (*Quantum Key Distribution)*: comprende el análisis, procesamiento y transmisión de información valiéndose de los principios y efectos de la mecánica cuántica. El objetivo es tanto complicar al máximo la vulneración de la confidencialidad de la comunicación como la obtención de información del enemigo en gracias a la computación cuántica.
- Protocolos criptográficos de preservación de la privacidad en ciberdefensa: son los protocolos de seguridad aplicando mecanismos criptográficos, incluyendo protocolos de gestión y distribución de claves, protocolos de autenticación...
- Computación segura multiparte: permite el intercambio de información segura manteniendo cada una de las partes sus claves privadas mientras las partes calculan conjuntamente una función criptográfica.
- Computación verificable: una entidad central puede delegar la computación de datos a otra entidad potencialmente desconocida, no verificada previamente, mientras mantiene resultados verificables.
- Autenticadores de un solo uso: en donde el usuario comparte una clave criptográfica con el verificador una sola vez (OTP, TOTP...).
- Aislamiento de redes y virtualización: se realiza con el uso de criptografía y presta especial atención a la microsegmentación y al aislamiento de redes en entornos distribuidos y *Cloud*.
- *Smart cards*: de última generación incluyen técnicas sin contacto, *Smart cards software*...

Data mining y analítica avanzada

A efectos del presente estudio, se entiende como *data mining* el conjunto de métodos estadísticos que, de forma automática o semiautomática, proporcionan información (correlacionada o por patrones) para la extracción de conocimiento e información útil a partir de grandes bases de datos desde diferentes perspectivas. Una de las formas de análisis de los datos es la utilización de técnicas estadísticas avanzadas, analítica avanzada, cuando el volumen de datos es muy elevado y no se puede utilizar la estadística tradicional, momento en el que se recurre a la minería de datos.

La minería de datos es la herramienta que nos permite aprovechar de una forma útil, válida y comprensible, el activo disponible en las bases de datos (*big data*).

Los modelos de minería de datos se pueden clasificar, en función de su propósito general, en modelos **descriptivos,** que son los que describen el comportamiento de los datos de forma que sea perfectamente interpretable por un usuario experto para la identificación de patrones. Los modelos **predictivos**, por su parte, además de describir los datos, se utilizan para predecir el valor futuro de algún atributo desconocido.

Para este estudio sobre *data mining*, se contempla principalmente el desarrollo de las siguientes capacidades en el ámbito de la ciberdefensa:

- Cifrado e intercambio de información: cubre las técnicas orientadas a mantener la información segura tanto en su lugar de origen como en el destino, así como en los distintos intercambios entre los diferentes lugares y usuarios.
- Análisis *big data:* enfocado al respeto de la privacidad y confidencialidad. Los procesos de minería o análisis de datos también van acompañados de riesgos. Quizás uno de los más relevantes el riesgo que este análisis masivo de datos posa sobre la privacidad de las personas sobre la privacidad de las personas. Es imprescindible proteger el origen de los datos subyacentes para evitar que usuarios no autorizados puedan poner en riesgo la información confidencial.
- Identificación y autenticación: se define la identificación como la capacidad de identificar de forma **exclusiva** a un usuario de un sistema o una aplicación que se está ejecutando en el sistema. Para evitar el acceso no autorizado al sistema y a los datos, la identificación por sí sola no es suficiente, por lo tanto, se utiliza la autenticación. La autenticación es la capacidad de demostrar que este usuario o esa aplicación es realmente quién asegura ser.
- Mecanismos de recolección de datos y amenazas (estudio de patrones ciberriesgos): la aplicación de la minería de datos en bases de datos referentes a amenazas actuales es una parte importante de la evaluación y definición de patrones para la implementación de las prioridades a tener en cuenta para los crecientes riesgos en ciberseguridad y ciberdefensa. Será preciso obtener para el futuro información útil y valiosa que nos aporte mecanismos para la prevención, detección, respuesta, mitigación y recuperación de los sistemas.
- Sanitización y anonimización de datos: la sanitización de datos se refiere a un proceso que no permite el acceso a los datos sobre los medios para un determinado nivel de esfuerzo, es decir, que los datos no se recuperen fácilmente. Algunas de

las razones por las que se requiere sanitizar los medios de almacenamiento son: reutilizar, revender, reparar, eliminar, regular y destruir. Por su parte la anonimización de datos tiene como finalidad eliminar o reducir al mínimo los riesgos de reidentificación de los datos anonimizados manteniendo la veracidad de los resultados del tratamiento de estos, es decir, además de evitar la identificación de las personas, los datos anonimizados deben garantizar que cualquier operación o tratamiento que pueda ser realizado con posterioridad a la anonimización no conlleve una distorsión de los datos reales.

- Computación de metadatos relevantes: considerando que los metadatos ponen en contexto la calidad, la relevancia y el valor de los datos primarios, es fundamental la utilización de los metadatos más relevantes y su posterior análisis y estudio con técnicas de computación avanzada.
- Correlación y herramienta de inteligencia y detección de anomalías: la detección de anomalías es clave para la supervivencia de los sistemas, ya que la detección temprana de fallos y amenazas puede evitar males mayores. Aporta un nivel de protección preventivo que reduce la implementación real de posibles riesgos antes de que se materialicen. El uso de herramientas de inteligencia en la búsqueda de anomalías reduce los falsos positivos, detecta los valores anómalos y aporta informes sobre el comportamiento y evolución del sistema.
- Intrusion detection, prevention & *big data management*: para una correcta gestión de la prevención y detección de las intrusiones en los sistemas se requiere un análisis pormenorizado del tráfico de la red, así como el contenido y comportamiento de la propia la red. Este proceso requiere el manejo de ingentes cantidades de información, por lo que las tecnologías de *data mining* y analítica avanzada pueden jugar un papel importante a la hora de reducir los tiempos de procesamiento, así como ofrecer información temprana y resultados sobre los datos analizados.

IoT

A efectos del presente estudio, se entiende como IoT aquella red de objetos físicos (*cosas)* que tienen incorporados *software*, sensores y otros tipos de tecnologías cuyo fin es el de intercambiar datos o conectarse con otros dispositivos a través de internet.

Su uso hace que dispositivos físicos tengan capacidad de conectarse a la red y poder empezar a intercambiar información en tiempo real, obteniendo procesos más sostenibles y una comunicación más directa con el entorno más cercano de cara a poder mejorar la toma de decisiones o la productividad.

En el ámbito de la ciberdefensa, se contempla principalmente el desarrollo de las siguientes capacidades:

- Identificación y autenticación de dispositivos: proceso que tiene que ejecutar cualquier dispositivo antes de conectarse a la red o hacer cualquier intercambio de datos.
- Creación de barreras de entrada: para que los objetivos a lo que se apunta no se vean comprometidos.

- Control de dispositivos: para tener una visión de los dispositivos de los que se dispone y además poder acceder a los mismos de múltiples maneras a lo largo del tiempo.
- Defensa ante ataques propagables en redes industriales: ya que es el ataque más usual en este tipo de dispositivos.
- Aislamiento de redes y virtualización: segmentar la capa de red o la utilización de listas de control de acceso a los dispositivos es una práctica usual de seguridad, ya que permiten un control granular de activos y reducen la superficie de ataque.
- Cifrado e intercambio de información avanzada (cuántica y postcuánticas): su uso es esencial para salvaguardar la integridad tanto de las comunicaciones como el de la información que se almacena, se envía o se recibe.
- Control de la privacidad de dispositivos: cuyo enfoque es la mayor preocupación en el uso de esta tecnología.
- Seguridad en microelectrónica: ya que los avances han hecho que el uso de los IOT se haya extendido exponencialmente pudiendo colocarles en ubicaciones remotas con un mantenimiento físico mínimo.
- Despliegue de sensores externos: para expandir la variedad de los datos que los dispositivos pueden recibir.

Inteligencia artificial

A efectos del presente estudio, se entiende como inteligencia artificial la habilidad de una máquina de presentar las mismas capacidades que los seres humanos, como el razonamiento, el aprendizaje, la creatividad y la capacidad de planear.

En el estudio se pretenden analizar la aplicación de la inteligencia artificial como elemento clave en la defensa, ya que permite a un sistema tecnológico percibir su entorno, relacionarse con él, resolver problemas, tomar decisiones y aprender. Todo ello con un fin específico.

Para el presenta estudio, se contempla principalmente el desarrollo de las siguientes capacidades en el ámbito de la ciberdefensa:

- Análisis de riesgos estadísticos y predictivos: permite procesar los datos, clasificar activos y presentar predicciones de los posibles riesgos que permitan plantear y preparar las ciberoperaciones.
- Evaluación, prevención y gestión dinámica de riesgos (cuantificación): permite evaluar riesgos en tiempo real para que se cuente con esta información dinámica para la toma de decisiones.
- Identificación y localización del atacante (detección atacante): permite identificar y localizar de forma automática al atacante.
- Defensa ante ataques propagables: permite desplegar contramedidas o realizar acciones automáticas que ayuden a contener ataques en curso y limitar su propagación.

- Detección temprana de ciberriesgos y anomalías: detecta automáticamente y en tiempo real posibles amenazas y cuantifica su riesgo.
- Creación de barreras de entrada: permite identificar necesidades de protección, su implementación y la valoración del grado de su efectividad.
- Respuesta automática ataques de seguridad (contención de ataques): permite el despliegue automático de barreras adicionales de seguridad, en el caso de detectarse ataques.
- Simulación amenazas y ciberataques y simulación de entornos peligrosos: para permitir disponer de simulaciones de ciberataques que permitan la capacitación de los analistas y de las TTP (tácticas, técnicas y procedimientos).
- Correlación y herramienta de Inteligencia: permite el descubrimiento automático de eventos de seguridad y cuantificar el riesgo.
- Herramientas de gestión de toma de decisiones e inteligencia: permite el análisis automático de la información, presentando valoraciones de posibles amenazas, con sus riesgos asociados que ayuden en la toma de decisiones.

Biometría

A efectos del presente estudio, se entiende como biometría el concepto definido por INCIBE en su documento *Método de reconocimiento de reconocimiento de personas basado en sus características fisiológicas o de comportamiento*.

En el estudio se pretenden analizar la aplicación de técnicas biométricas como elementos claves en la identificación de personas y control de accesos que nos permitan apoyar las técnicas de prevención, detección y protección para ser consideradas en el ámbito de la ciberdefensa. Esto se aplica tanto al plano defensivo como en ataque.

En el ámbito de la ciberdefensa, se contempla principalmente el desarrollo de las siguientes capacidades:

Tecnologías biométricas fisiológicas (TBF):

- Huella dactilar: identificación basada en la búsqueda de coincidencias con la huella dactilar de una persona, bien sea mediante minucias o por correlación.
- Reconocimiento facial: identificación basada en el reconocimiento mediante una imagen o fotografía.
- Reconocimiento ojo (retina, iris): identificación basada en el reconocimiento mediante el análisis de características del globo ocular como la retina o el iris.
- Geometría de la mano: identificación basada en el reconocimiento mediante el análisis de la forma mano, apoyándose en imágenes 3D, desde diferentes ángulos.
- Vascular: identificación basada en el reconocimiento un patrón biométrico interno a partir de la geometría del árbol de venas de la muñeca o un dedo.

Tecnologías biométricas de comportamiento (TBC):

- Análisis de firma: identificación basada en el reconocimiento a través del análisis de la firma manuscrita de una persona mediante comparación simple o verificación dinámica.
- Reconocimiento de voz: identificación basada en el reconocimiento a través del análisis de la Voz de una persona apoyándose en el uso de sistemas de IA (redes neuronales) con aprendizaje.
- Patrón de teclado: identificación basada en el reconocimiento a través del análisis de la escritura de una persona atendiendo a valores como la fuerza al teclear, pulsación, periodo de duración, etc.
- Reconocimiento de comportamiento (formas de andar, escritura, etc.): identificación basada en el reconocimiento de comportamientos específicos de las personas apoyándose en un análisis previo de los que se ha deducido un patrón.

ANEXO II: Acrónimos

ACRÓNIMOS	SIGNIFICADO
ABIDE	*Artificial Intelligence and Big Data for Decision Making in C4ISR*
AGE	Administración General del Estado
AI4DEF	*Artificial Intelligence for Defence*
ANPIC	Autoridad Nacional para la Protección de la Información Clasificada
APT	*Advanced Persistent Threat*
C2, C&C	Mando y Control
CC	*Common Criteria*
CCN	Centro Criptológico Nacional
CEOE	Confederación Española de Organizaciones Empresariales
CERT	*Computer Emergency Response Team*
CIDCC	*Cyber and Information Domain Coordination Centre*
CIS	*Communication and Information System*
CLR	*.Net Common Language Runtime*
CMDB	*Configuration Management Data Base*
CNI	Centro Nacional de Inteligencia
COS	Centro de Operaciones de Seguridad
CSIRT	Equipo de respuesta a incidentes de seguridad informática
CyOC	*Cyberspace Operations Centre*
DFIR	*Digital Forensic & Incident Response*

DGAM	Dirección General de Armamento y Material
DLT	*Distributed Ledger Technology*
DSC	*Desired State Configuration*
ECYSAP	*European Cyber Situation Awareness Package*
EDA	Agencia Europea de Defensa
EDF	*European Defence Fund*
EDIPD	*European Defence Industrial Development Programme*
EDR/XDR	*Endpoint Detection and Response/ Extended Detection & Response*
ENCS	Estrategia Nacional de Ciberseguridad
ENS	Esquema Nacional de Seguridad
FEDER	Fondo Europeo de Desarrollo Regional
FRONTEX	Agencia Europea de la Guardia de Fronteras y Costas
GNSS	*Global Navigation Satellite System*
GPS	*Global Positioning System*
GT4	Grupo de Trabajo 4 (Análisis e impulso a la industria de Ciberdefensa) del Foro Nacional de Ciberseguridad
HPS	Habilitación Personal de Seguridad
HSEM	Habilitación de Seguridad de Empresa
IA	*Artificial Intelligence*
IaaS	Infraestructura como servicio
IAC	*Infrastructure As Code*
ICS	Sistemas de control industrial
INCIBE	Instituto Nacional de Ciberseguridad
IOT	*Internet Of Things*
ISO	*International Organization for Standardization*
ISP	Proveedor de servicios de internet
JISR	*Joint Intelligence, Surveillance and Reconnaissance*

KMS	*Key Management Service*
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
MCCE	Mando Conjunto del Ciberespacio
MILDEC	*Military Deception*
MISP	*Malware Information Sharing Platform*
MITRE	Organización estadounidense sin ánimo de lucro que provee ingeniería de sistemas, investigación y desarrollo, y soporte sobre tecnologías de la información
NCIA	*NATO Communications and Information Agency*
NGWS/FCAS	*Next Generation Weapon System/ Future Combat Air System*
NICE	*National Initiative for Cybersecurity Education*
NIS2	*Network and Information Security*
NLP	*Natural Language Processing*
OPSEC	*Operations security*
OSINT	*Open-Source Intelligence*
OTP /TOTP	*One time password/Time-Based One-Time Password*
PaaS	Plataforma como servicio
PESCO	*Permanent Structured Cooperation* (EU)
PQC	*Post-Quantum Cryptograph*
QKD	*Quantum Key Distribution*
RENIC	Red de Excelencia Nacional de Investigación en Ciberseguridad
RL	*Reinforcement Learning*
RPAs	*Robotic Process Automation*
RRSS	Redes sociales
RV/RA/RM	Realidad virtual/realidad aumentada/realidad mixta
SaaS	*Software* como servicio
SCCM	*System Center Configuration Manager*

SGSI	Sistema de Gestión de Seguridad de la Información
SOAR	*Security Orchestration, Automation and Response*
SOC	Centro de Operaciones de Seguridad
STIC	Seguridad de las tecnologías de la información y las comunicaciones
TBC	Tecnologías biométricas de comportamiento
TBF	Tecnologías biométricas fisiológicas
TEDAE	Asociación Española de Tecnologías de Defensa, Seguridad, Aeronáutica y Espacio
TGVF	*Time and Geodesy Validation Facility*
TTP	Tácticas, Técnicas y Procedimientos

FORO
NACIONAL DE
CIBERSEGURIDAD

2023