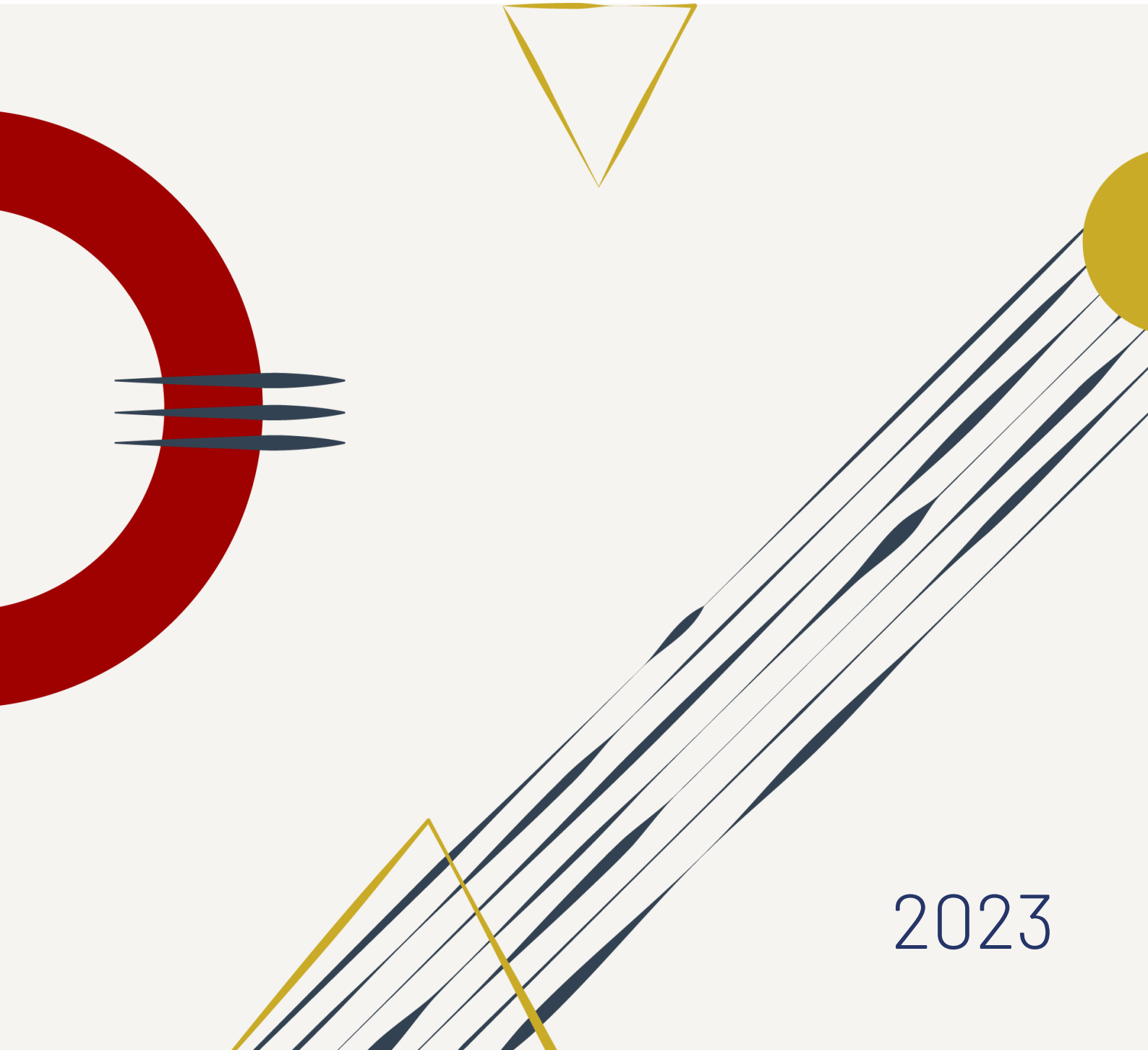
FORO NACIONAL DE CIBERSEGURIDAD

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:

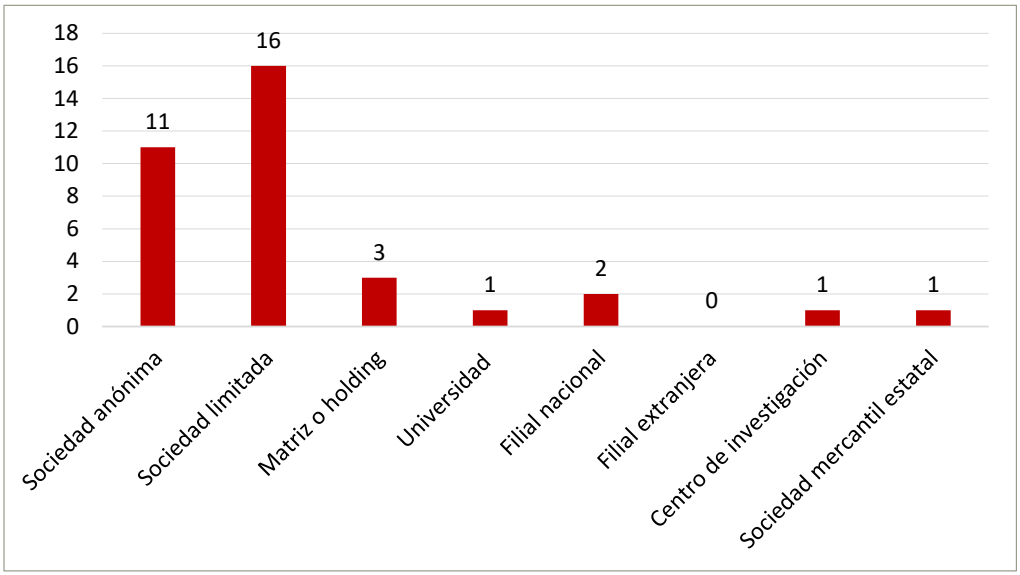


Figura 2. P1: Datos Tipo de organización

La representación gráfica de estos datos se muestra en la siguiente figura:

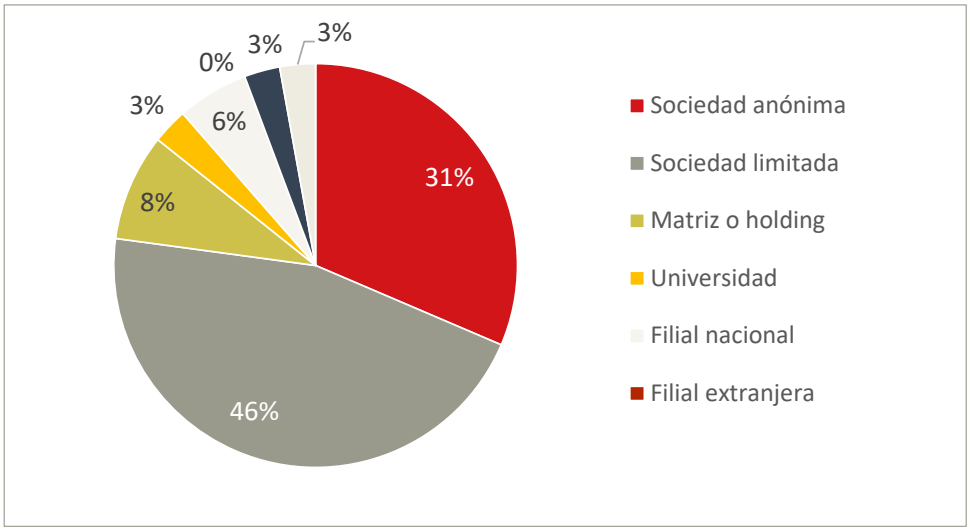


Figura 3. P1: Gráfico. Tipo de organización

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:

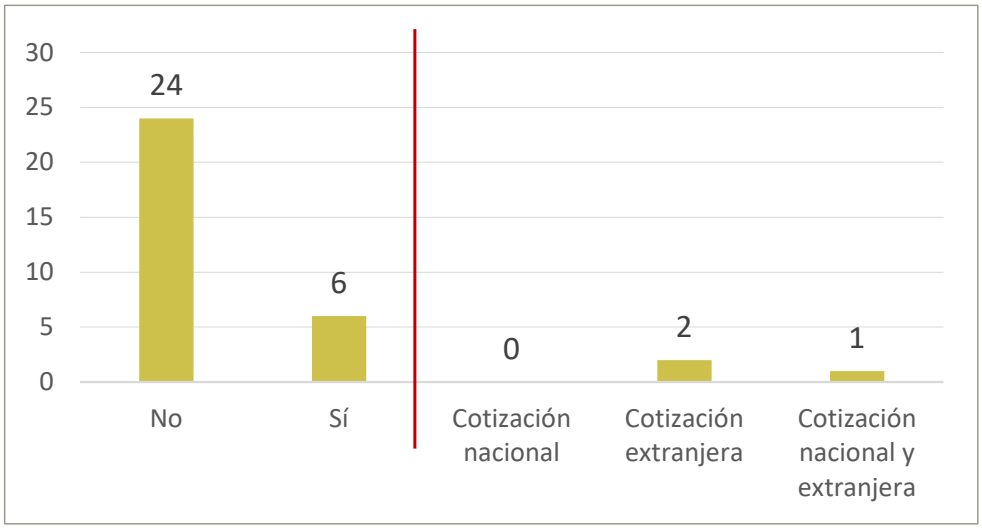


Figura 4. P2: Datos Pertenencia mercado bursátil

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:

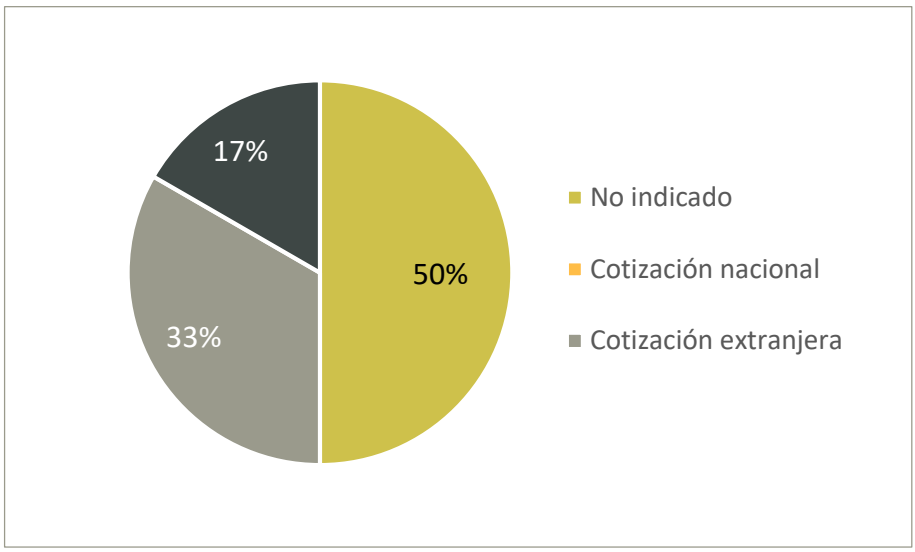


Figura 5. P2: Gráfico. Tipo mercado bursátil

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:

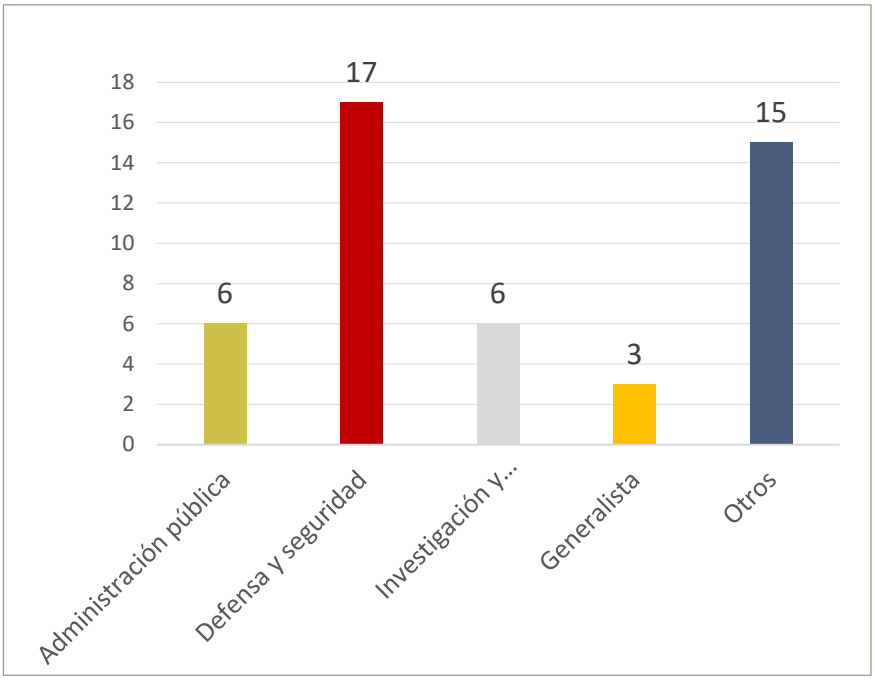


Figura 6. P3: Datos Actividad principal

La representación gráfica de los datos se muestra en la siguiente figura:

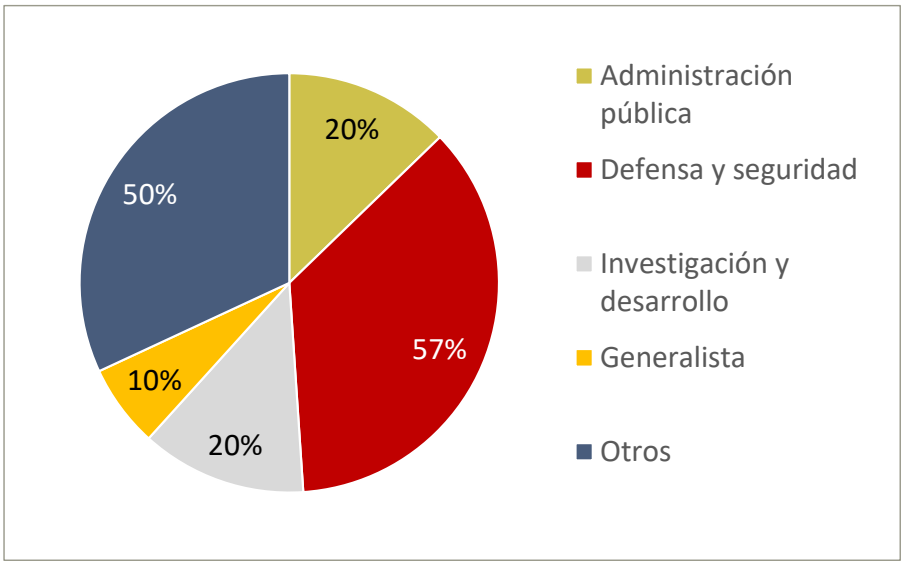


Figura 7. P3: Gráfico. Actividad principal

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:

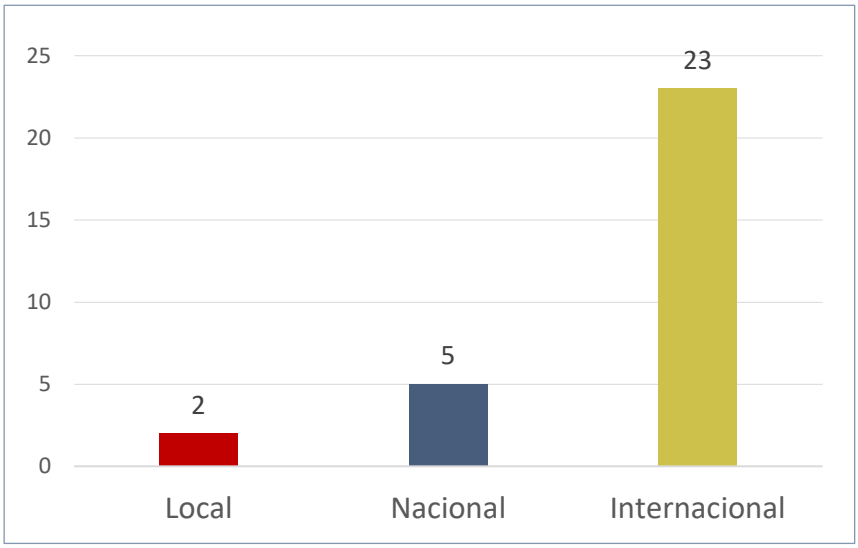


Figura 8. P4: Datos Grado de implantación de entidades

La representación gráfica de los datos se muestra en la siguiente figura:

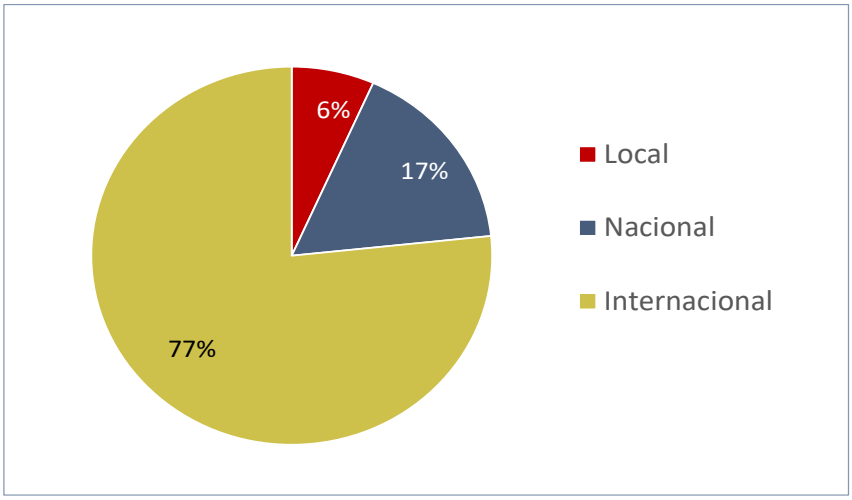


Figura 9. P4: Gráfico. Grado de implantación de las entidades

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:

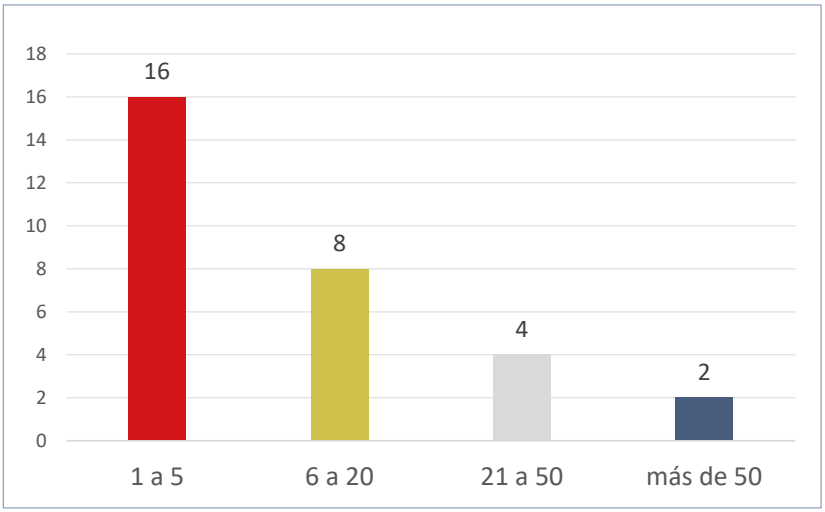


Figura 10. P5: Datos Número de sedes

La representación gráfica de los datos se muestra en la siguiente figura:

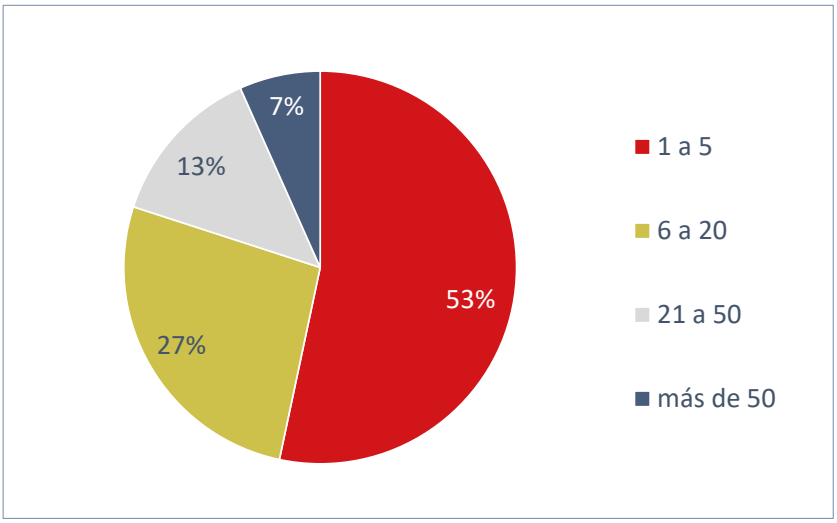


Figura 11. P5: Gráfico. Número de sedes

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:

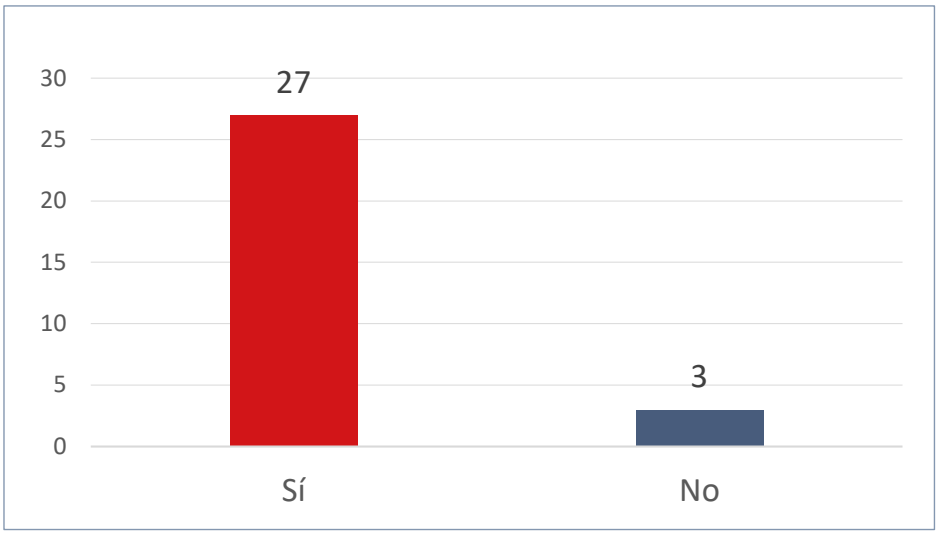


Figura 12. P6: Datos Familiarización con la Ley de Contratos del Sector Público

La representación gráfica de los datos se muestra en la siguiente figura:

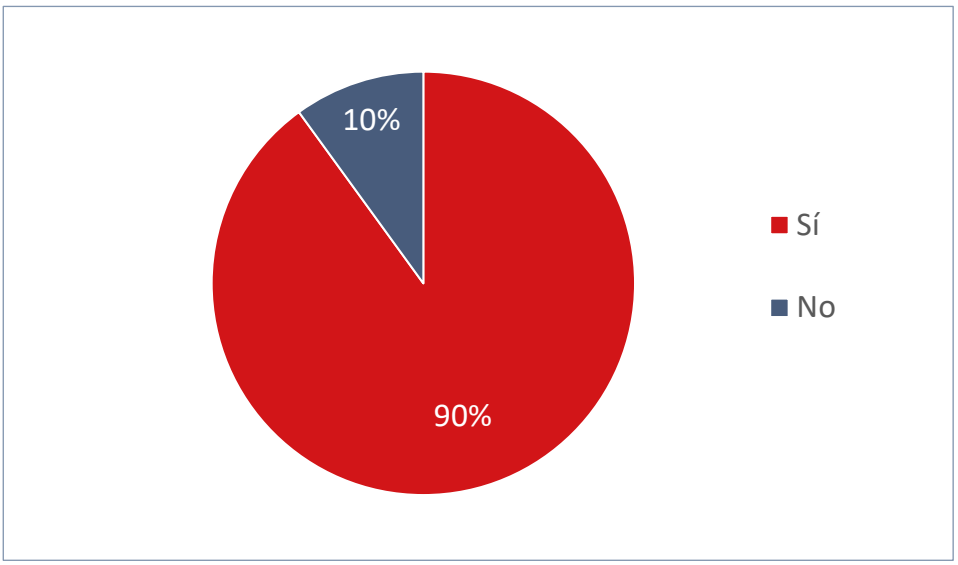


Figura 13. P6: Gráfico. Familiarización con la Ley de Contratos del Sector Público

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:

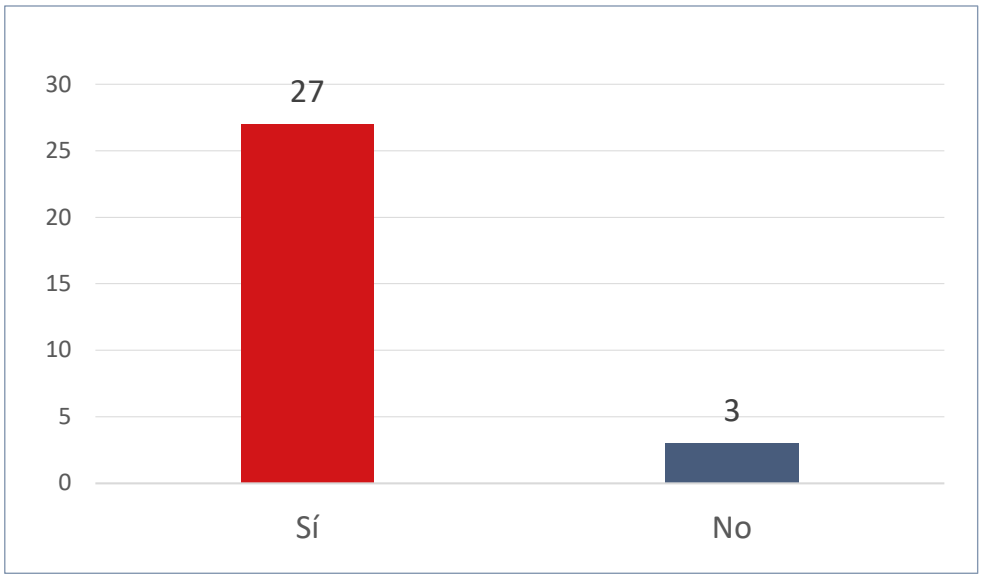


Figura 14. P7: Datos Alta en Plataforma de Contratación del Sector Público

La representación gráfica de los datos se muestra en la siguiente figura:

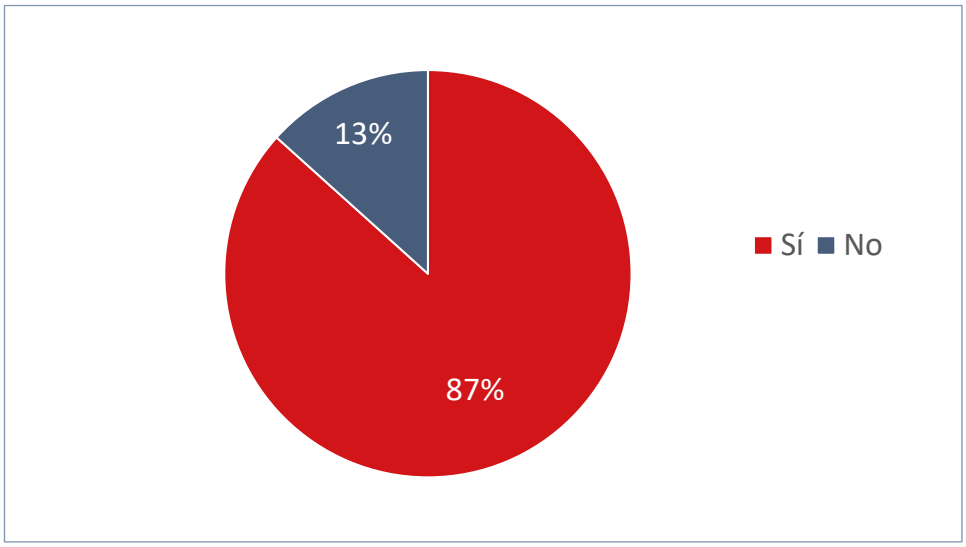


Figura 15. P7: Gráfico. Alta en Plataforma de Contratación del Sector Público

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:

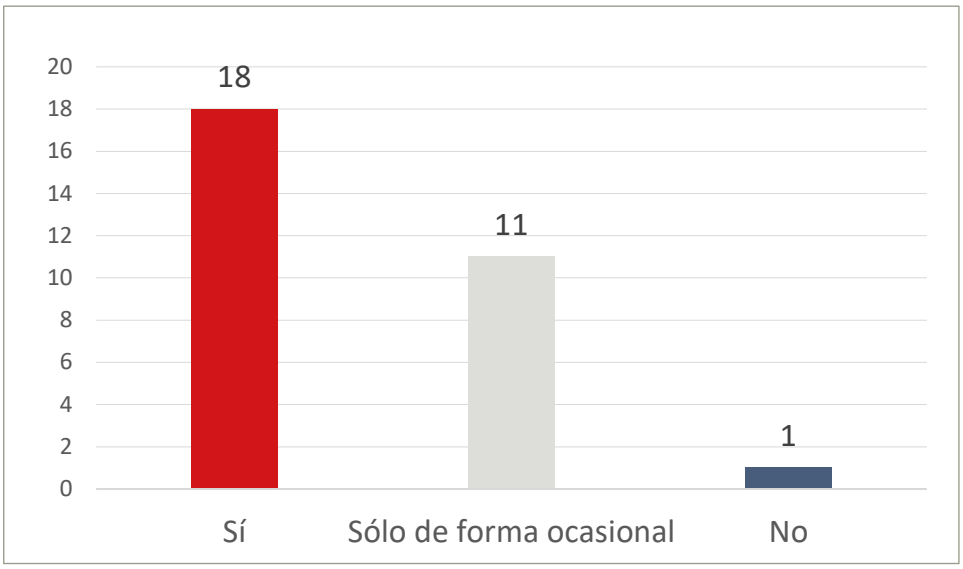


Figura 16. P8: Datos Expertos con conocimiento de la estructura y procesos del Ministerio de Defensa

La representación gráfica de los datos se muestra en la siguiente figura:

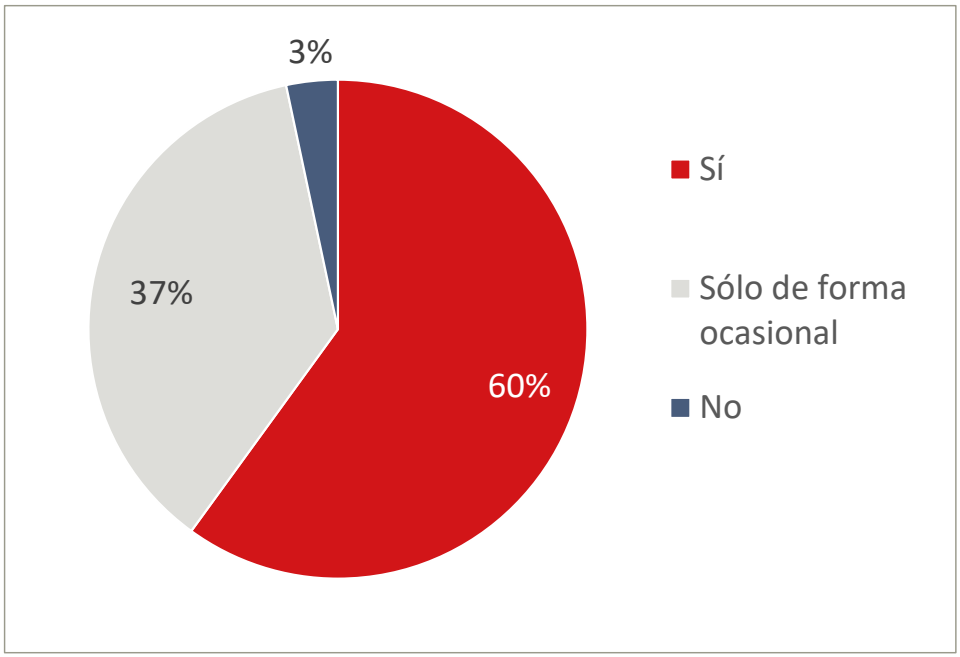


Figura 17. P8: Gráfico. Expertos con conocimiento de la estructura y procesos del Ministerio de Defensa

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:

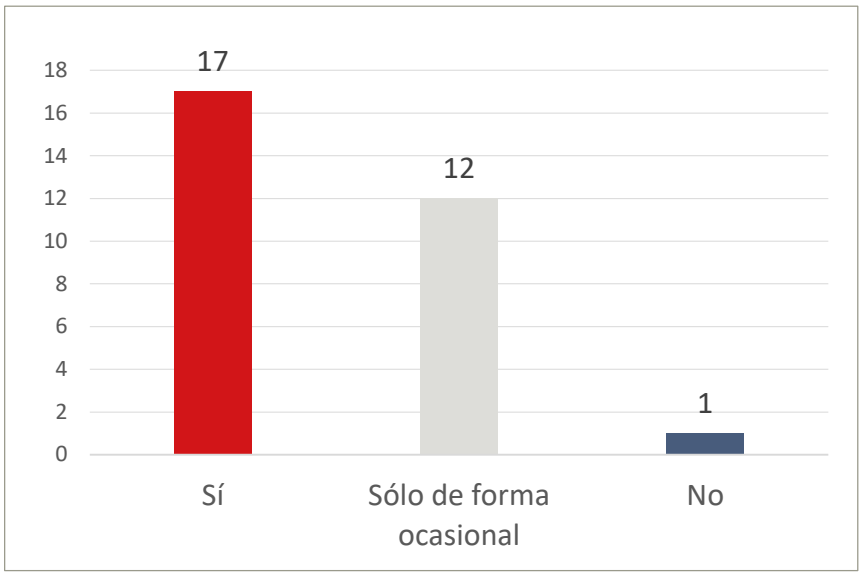


Figura 18. P9: Datos Expertos con conocimientos de la estructura y procesos de Ministerio de las Fuerzas Armadas

La representación gráfica de los datos se muestra en la siguiente figura:

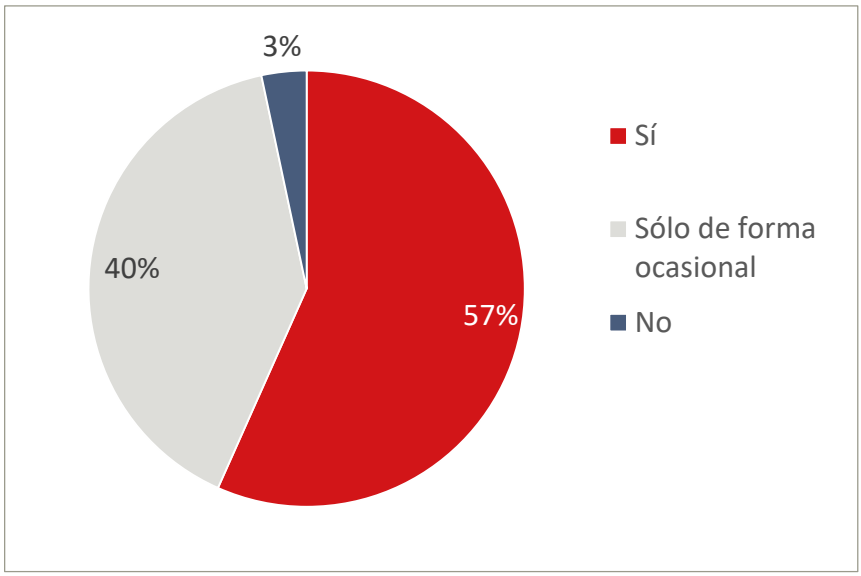


Figura 19. P9: Gráfico. Expertos con conocimientos de la estructura y procesos de Ministerio de las Fuerzas Armadas

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:

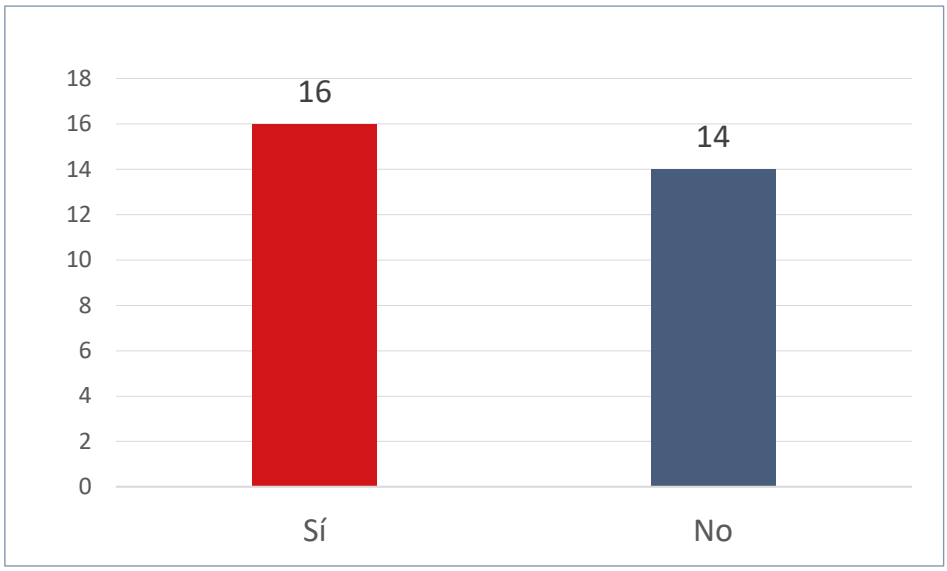


Figura 20. P10: Datos Experiencia en proyectos OTAN/EDA

La representación gráfica de los datos se muestra en la siguiente figura:

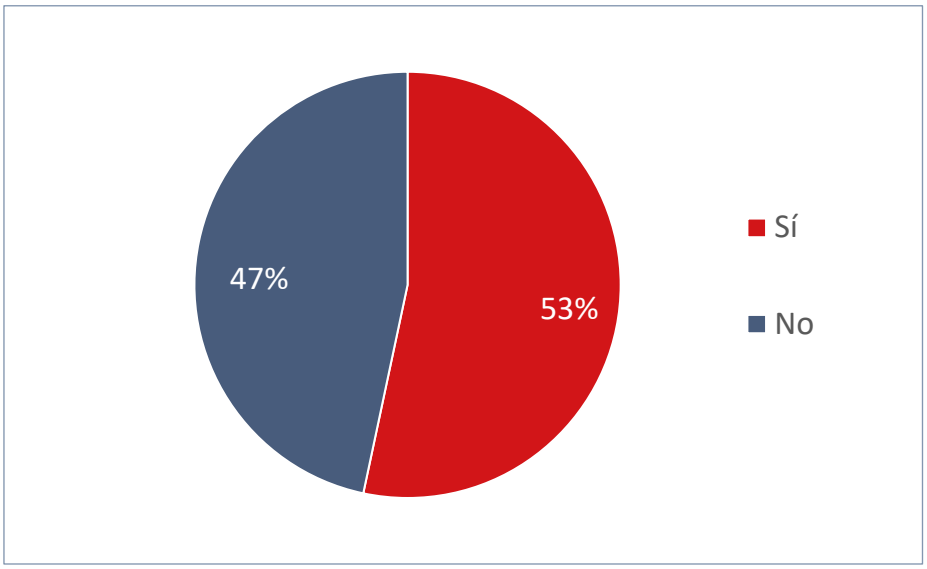


Figura 21. P10: Gráfico. Experiencia en proyectos OTAN/EDA

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:

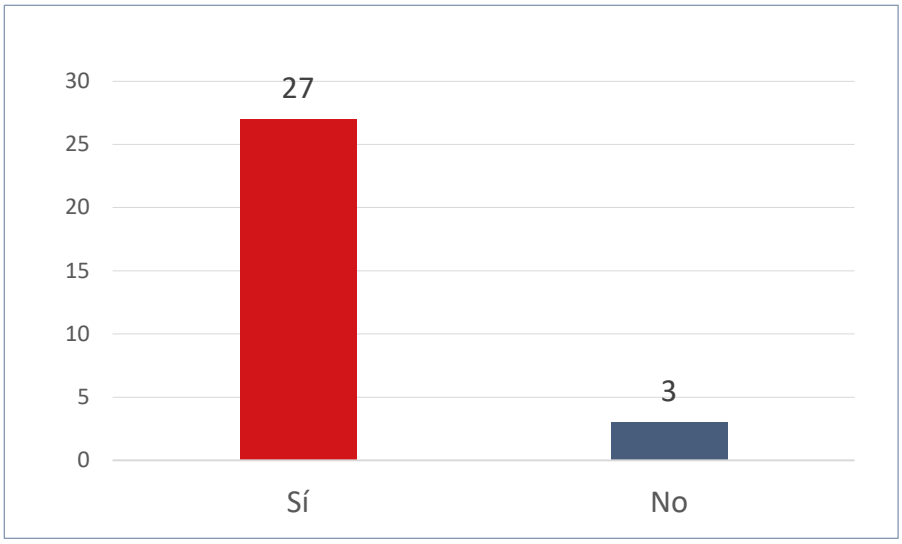


Figura 22. P11: Datos Plan de Gestión de Seguridad de la Información

La representación gráfica de los datos se muestra en la siguiente figura:

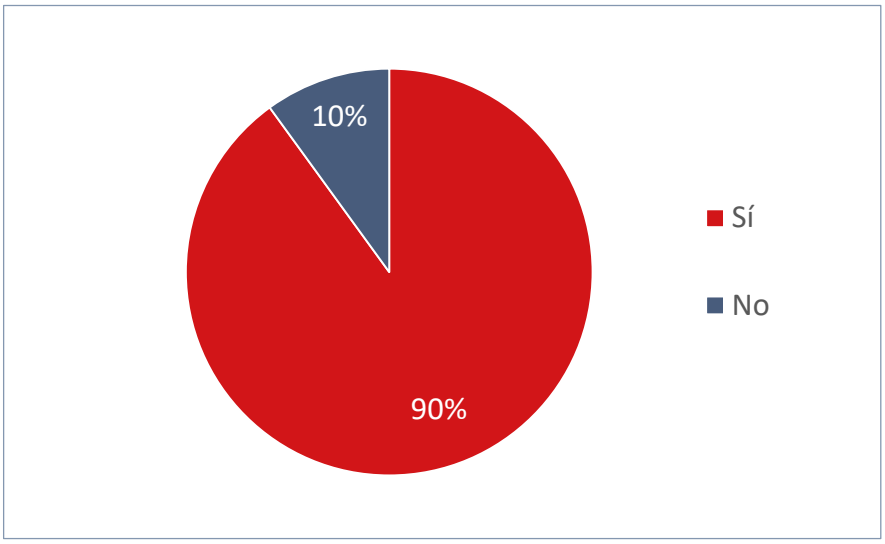


Figura 23. P11: Gráfico. Plan de Gestión de Seguridad de la Información

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:

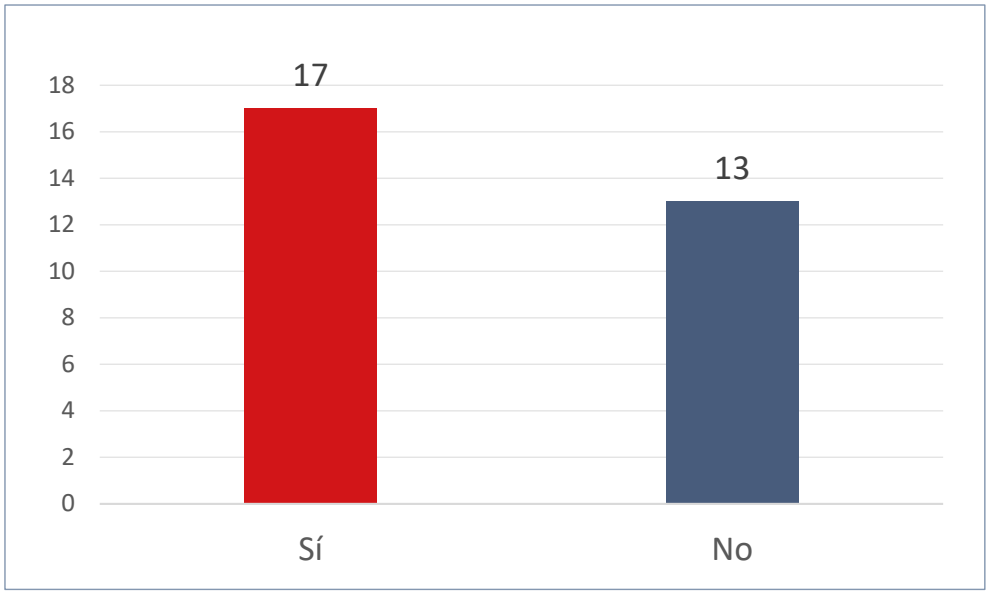


Figura 24. P12: Datos Certificación ISO 27K o similar

La representación gráfica de los datos se muestra en la siguiente figura:

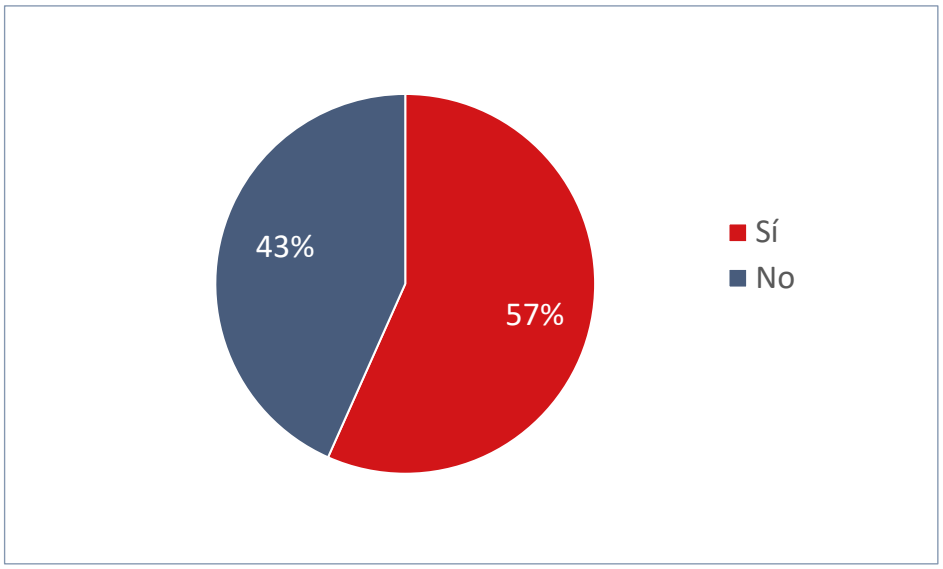


Figura 25. P12: Gráfico. Certificación ISO 27K o similar

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:

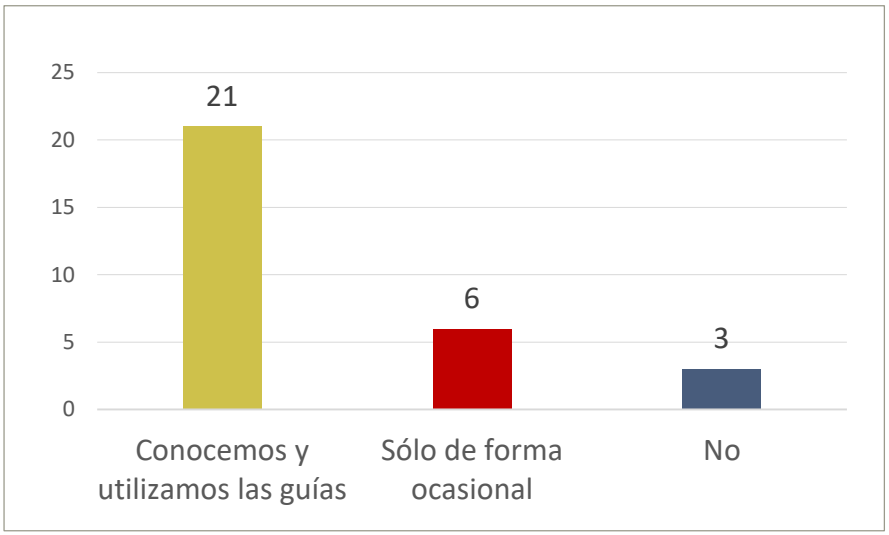


Figura 26. P13: Datos Familiarización con guías de seguridad de la serie CCN-STIC

La representación gráfica de los datos se muestra en la siguiente figura:

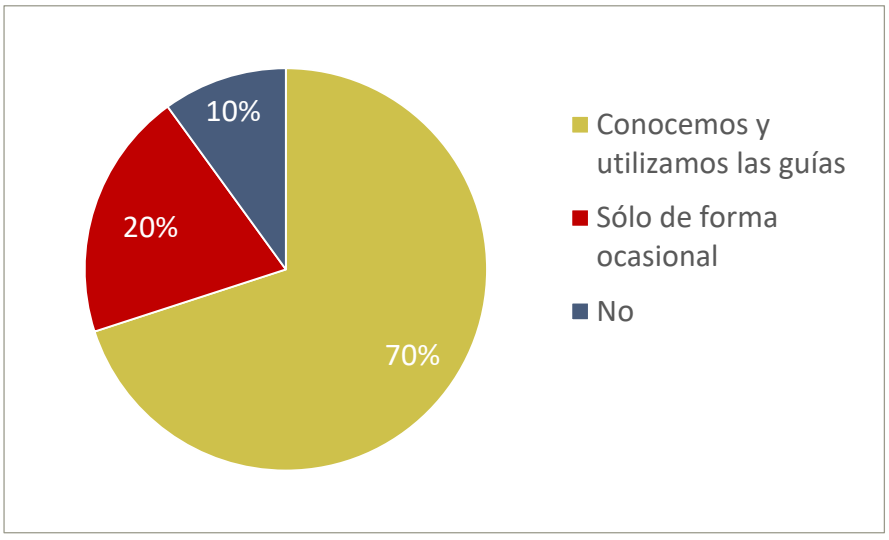


Figura 27. P13: Gráfico. Familiarización con guías de seguridad de la serie CCN-STIC

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:

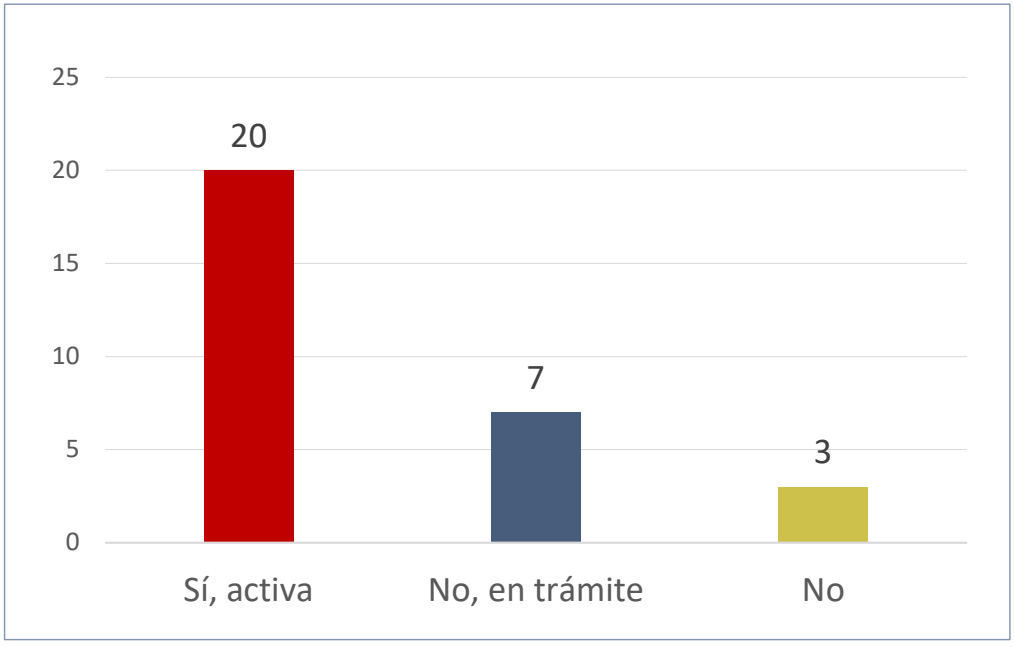


Figura 28. P14: Datos Disposición de HSEM

La representación gráfica de los datos se muestra en la siguiente figura:

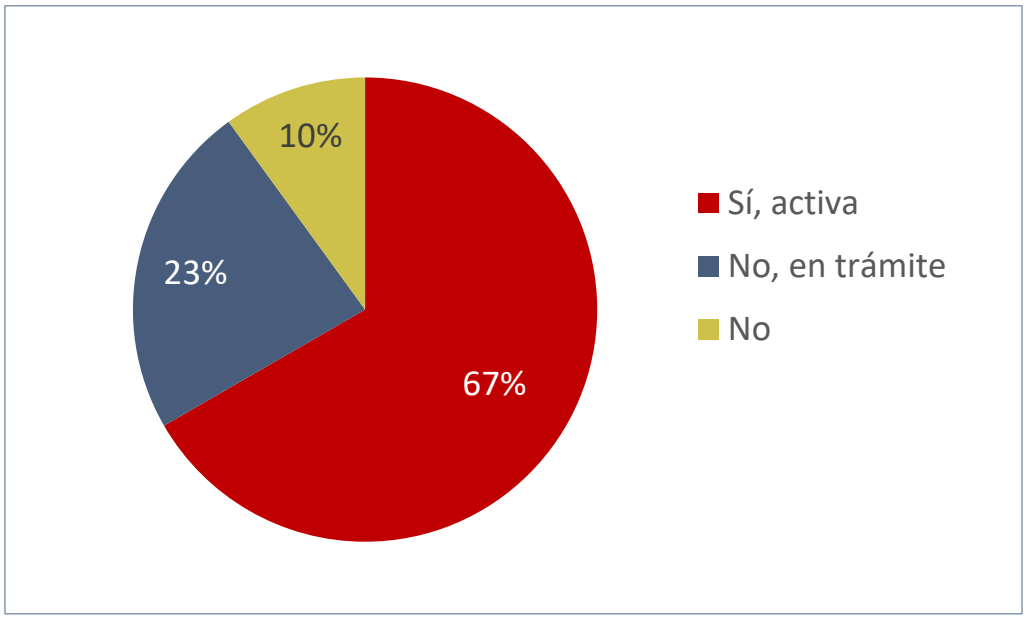


Figura 29. P14: Gráfico. Disposición de HSEM

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:

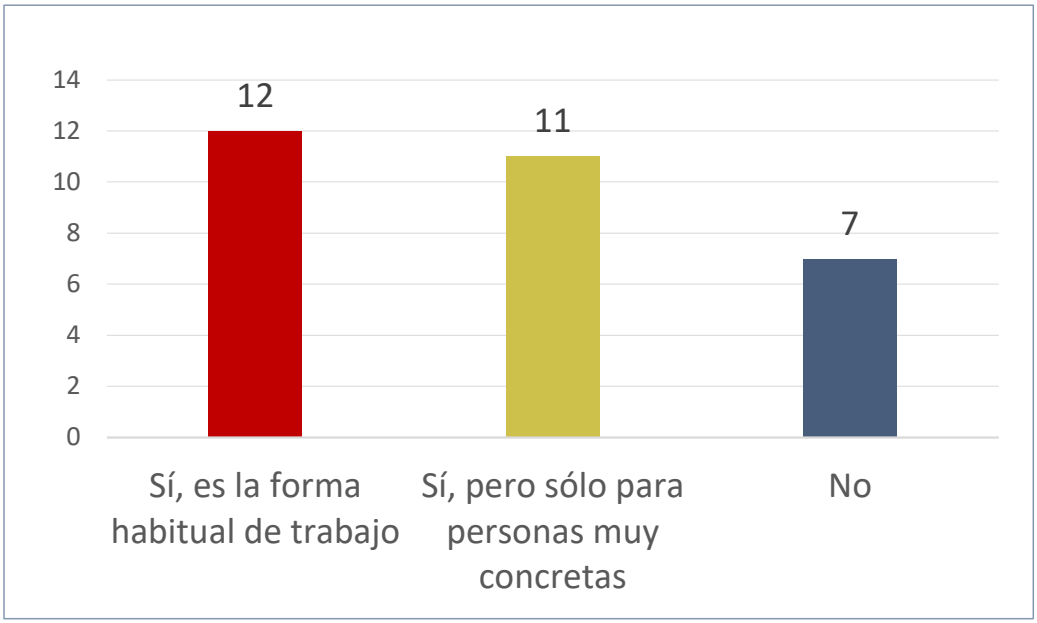


Figura 30. P15: Datos Disposición de personal HPS

La representación gráfica de los datos se muestra en la siguiente figura:

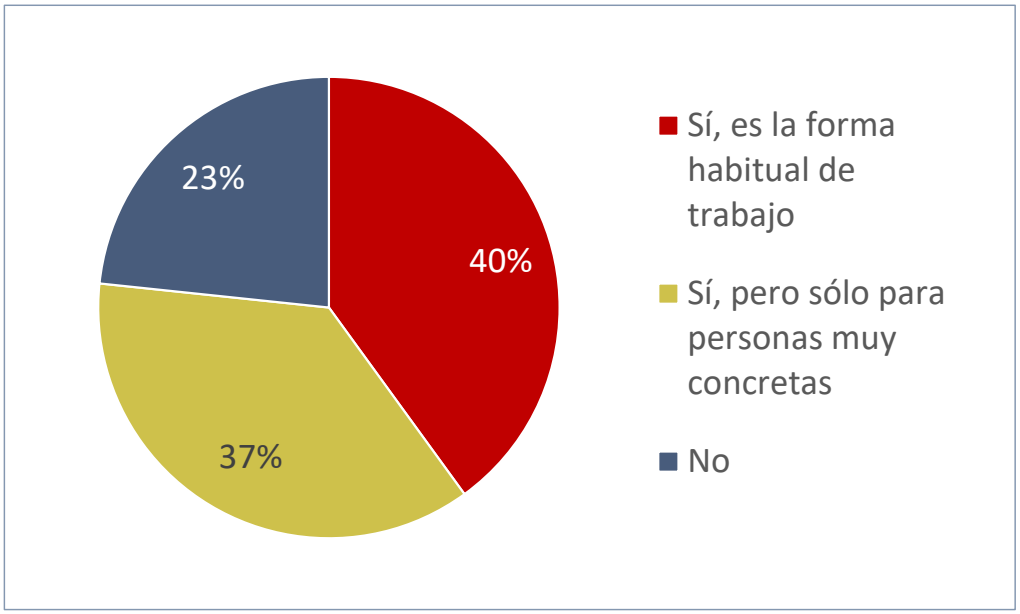


Figura 31. P15: Gráfico. Disposición de personal HPS

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:

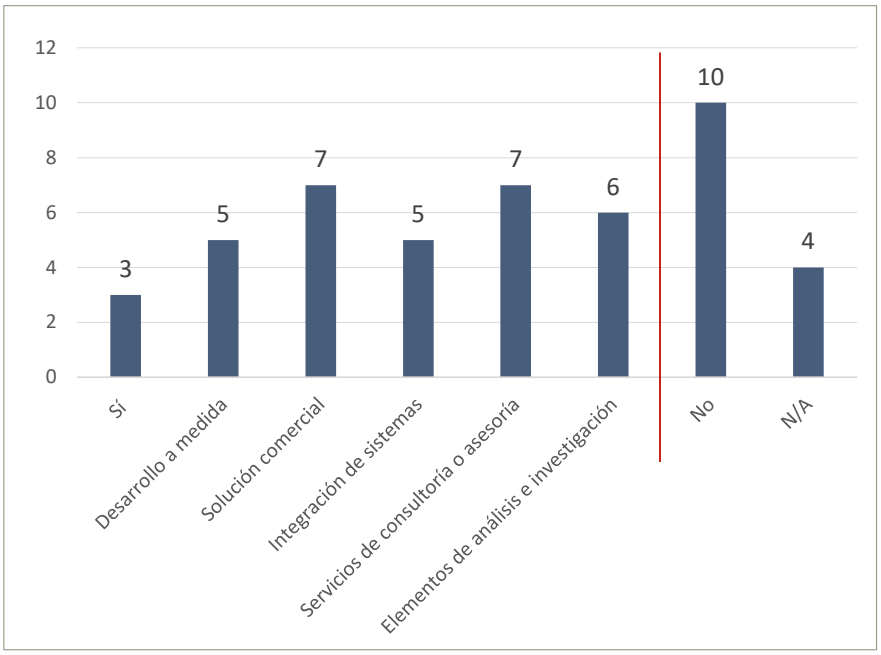


Figura 32. P16: Datos Control de la conducción y ejecución de ciberoperaciones

La representación gráfica de los datos positivos se muestra en la siguiente figura:

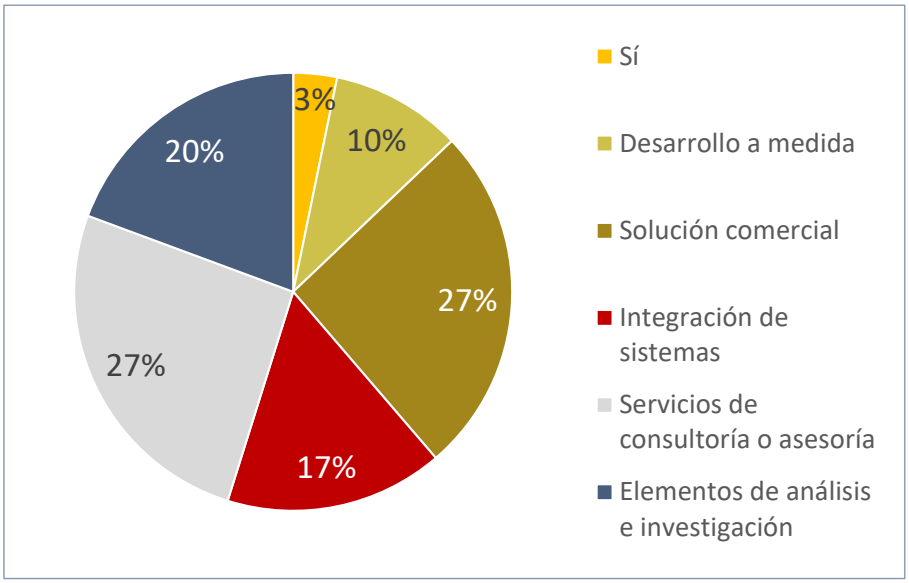


Figura 33. P16: Gráfico. Control de la conducción y ejecución de ciberoperaciones

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:

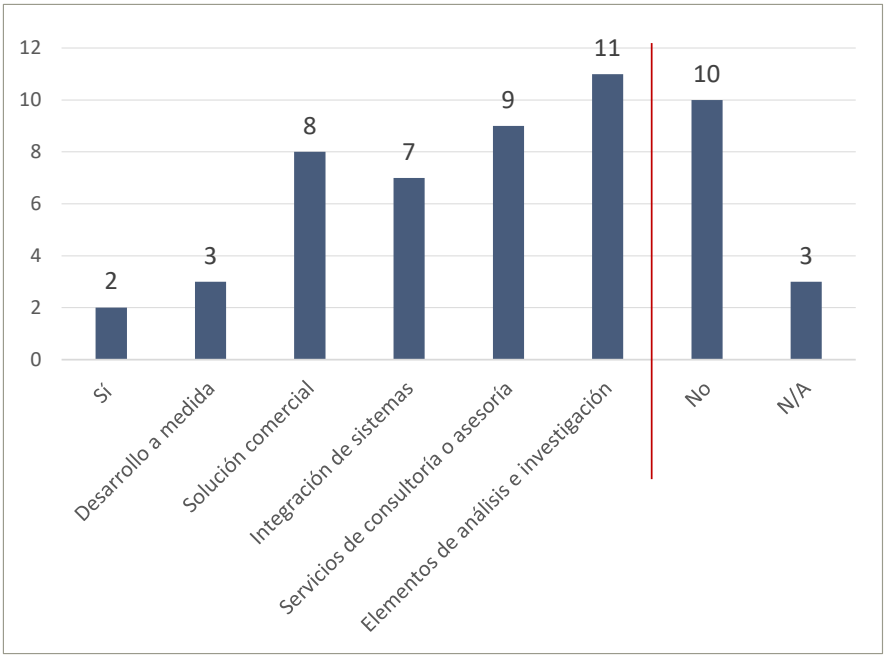


Figura 34- P17: Datos Consciencia situacional en ciberdefensa

La representación gráfica de los datos positivos se muestra en la siguiente figura:

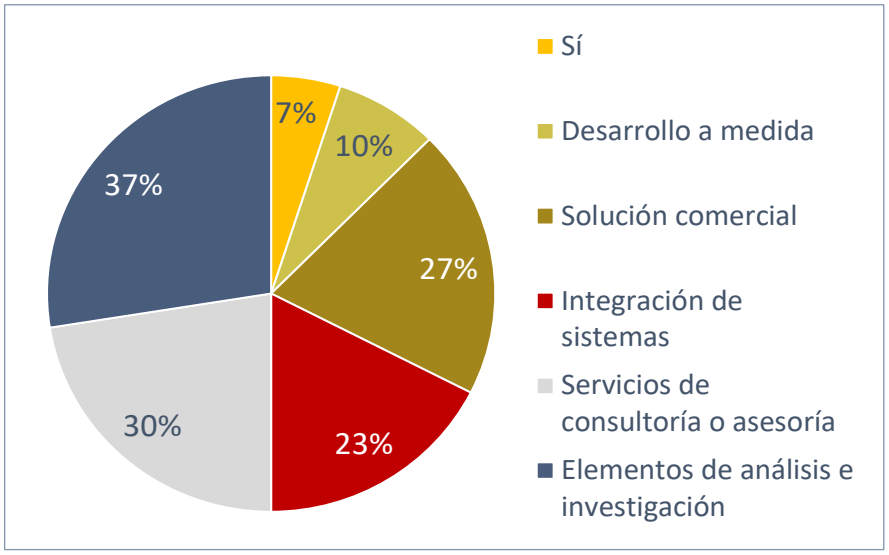


Figura 35- P17: Gráfico. Consciencia situacional ciber en ciberdefensa

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:

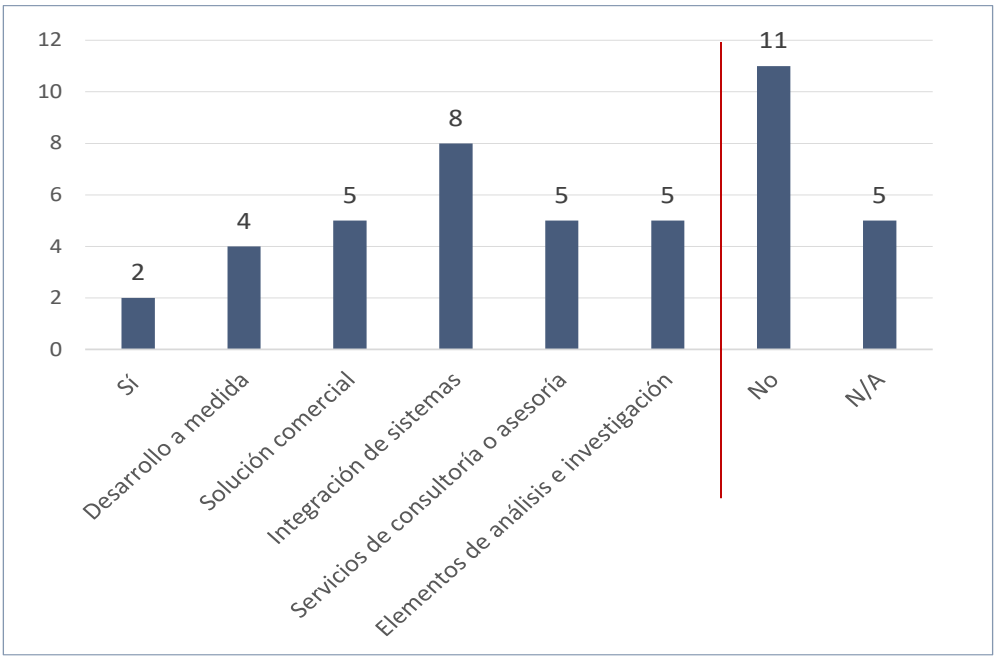


Figura 36. P18: Datos Centro de operaciones del ciberespacio

La representación gráfica de los datos positivos se muestra en la siguiente figura:

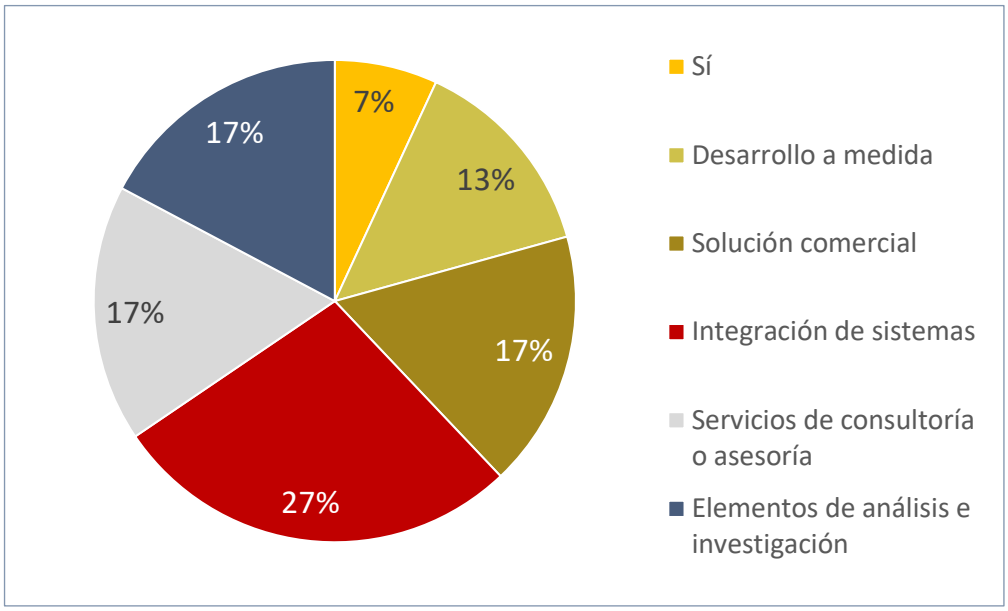


Figura 37. P18: Gráfico. Centro de operaciones del ciberespacio

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:

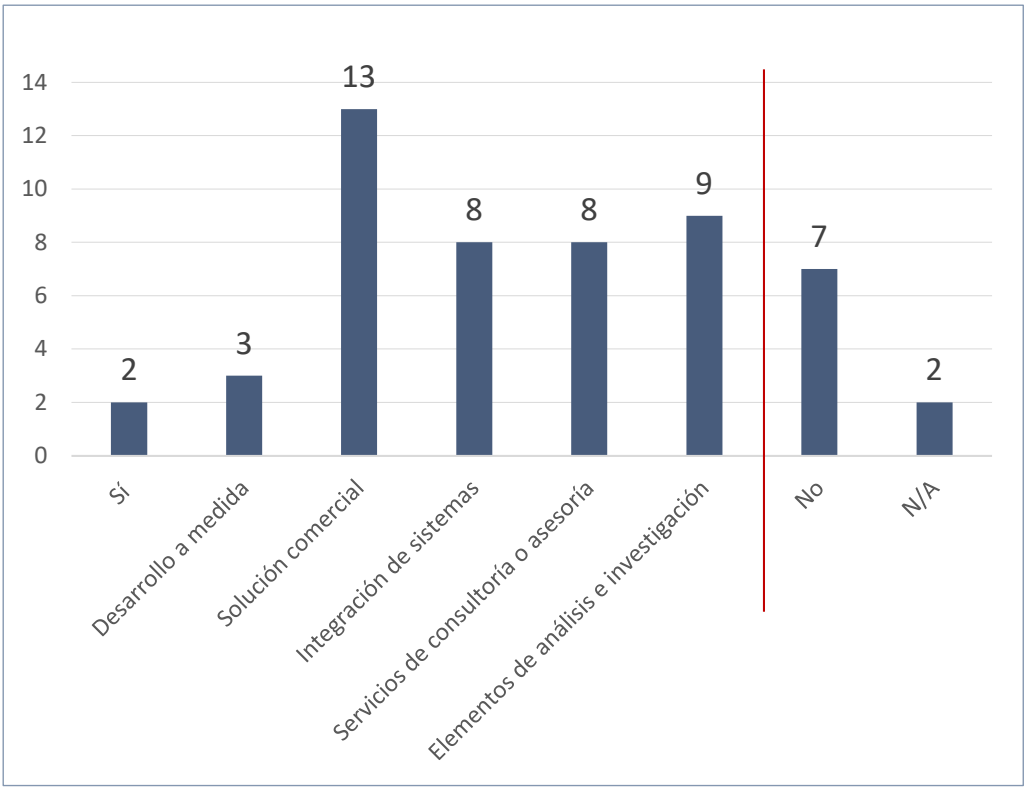


Figura 38. P19: Datos Defensa activa

La representación gráfica de los datos positivos se muestra en la siguiente figura:

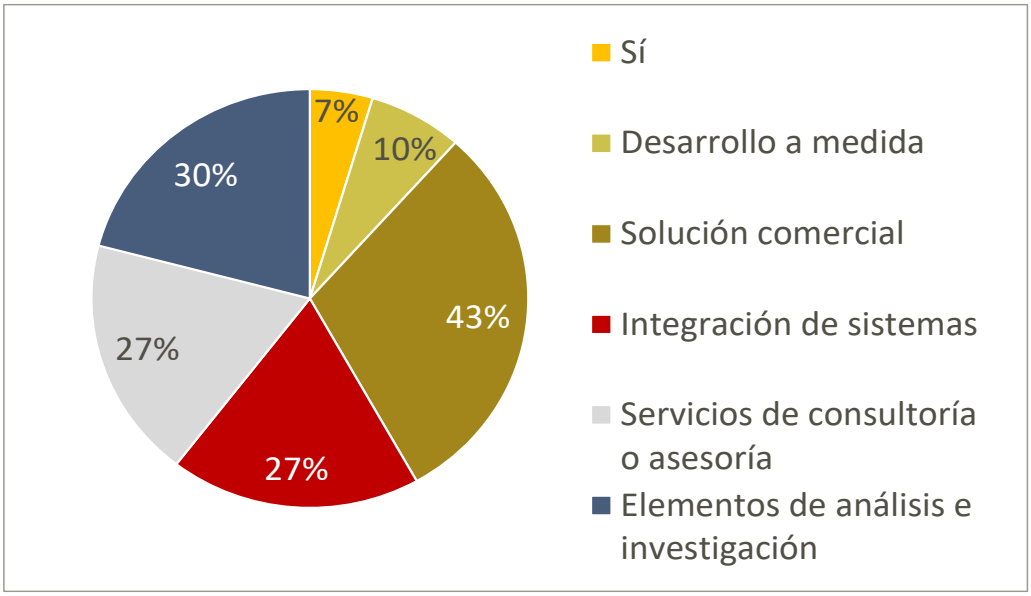


Figura 39. P19: Gráfico. Defensa activa

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:

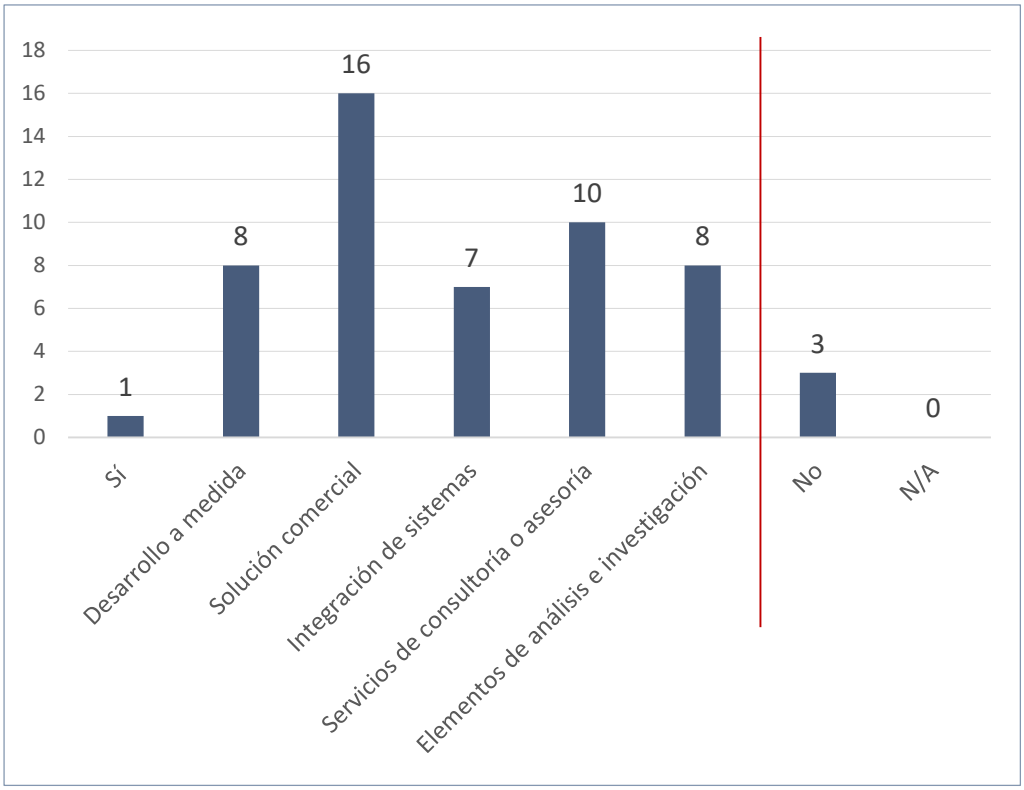


Figura 40. P20: Datos Defensa pasiva

La representación gráfica de los datos positivos se muestra en la siguiente figura:

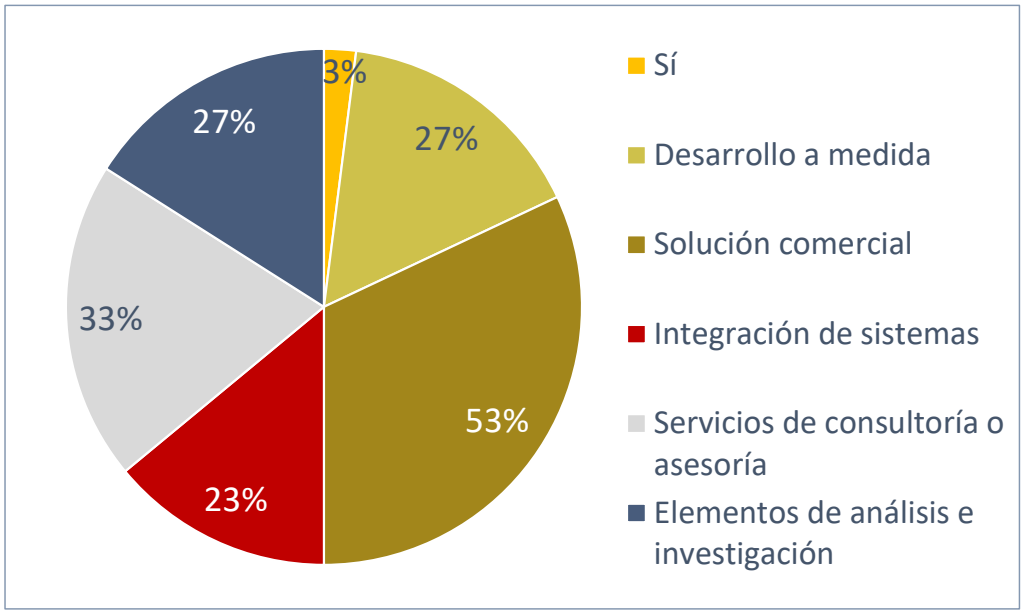


Figura 41. P20: Gráfico. Defensa pasiva

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:

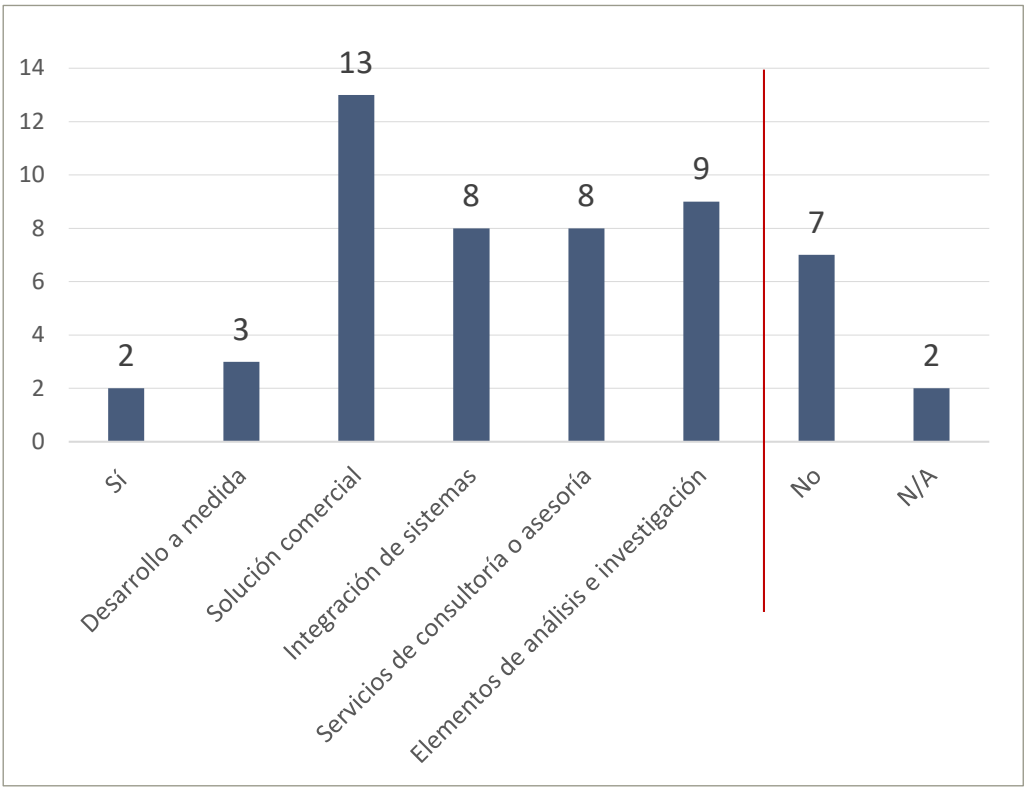


Figura 42. P21: Datos Seguridad perimetral

La representación gráfica de los datos positivos se muestra en la siguiente figura:

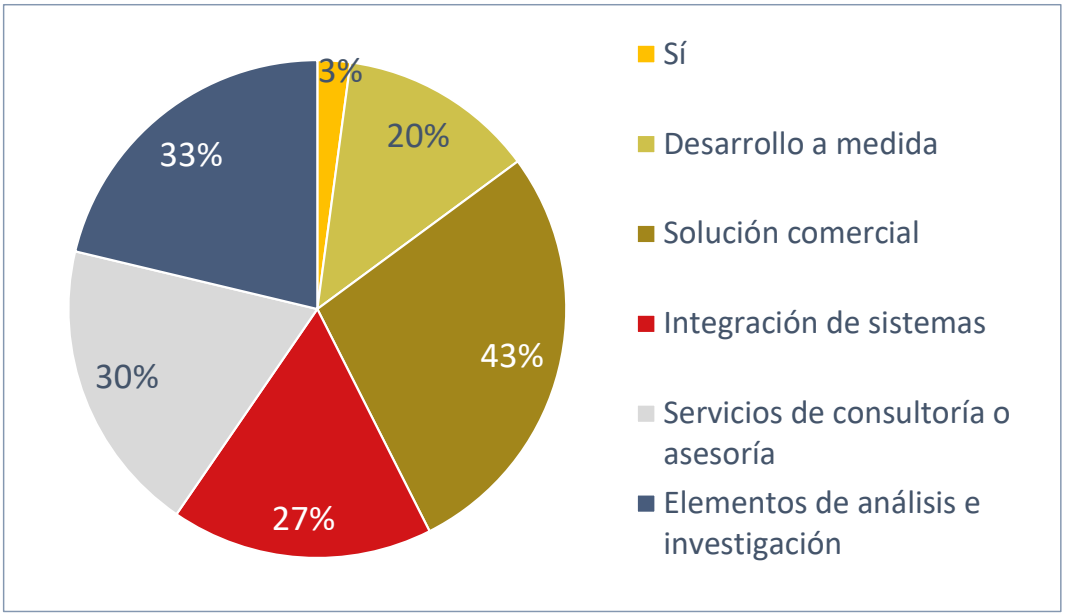


Figura 43. P21: Gráfico. Seguridad perimetral

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:

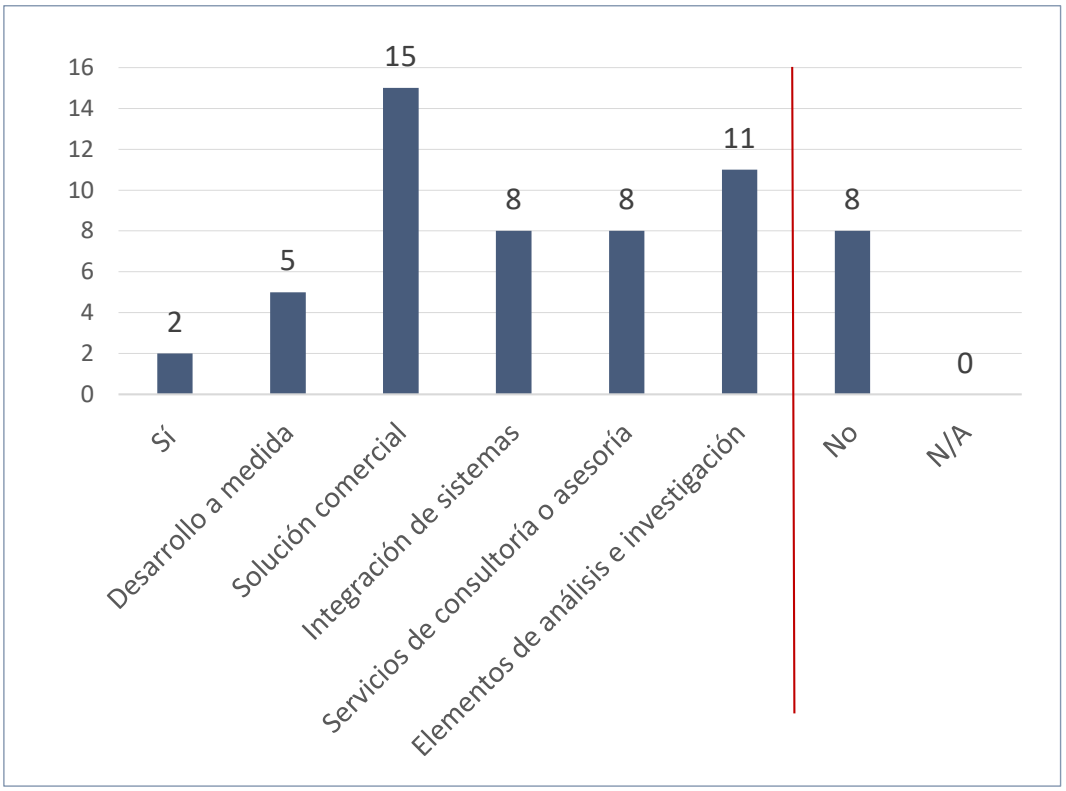


Figura 44. P22: Datos Monitorización y detección de amenazas

[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:

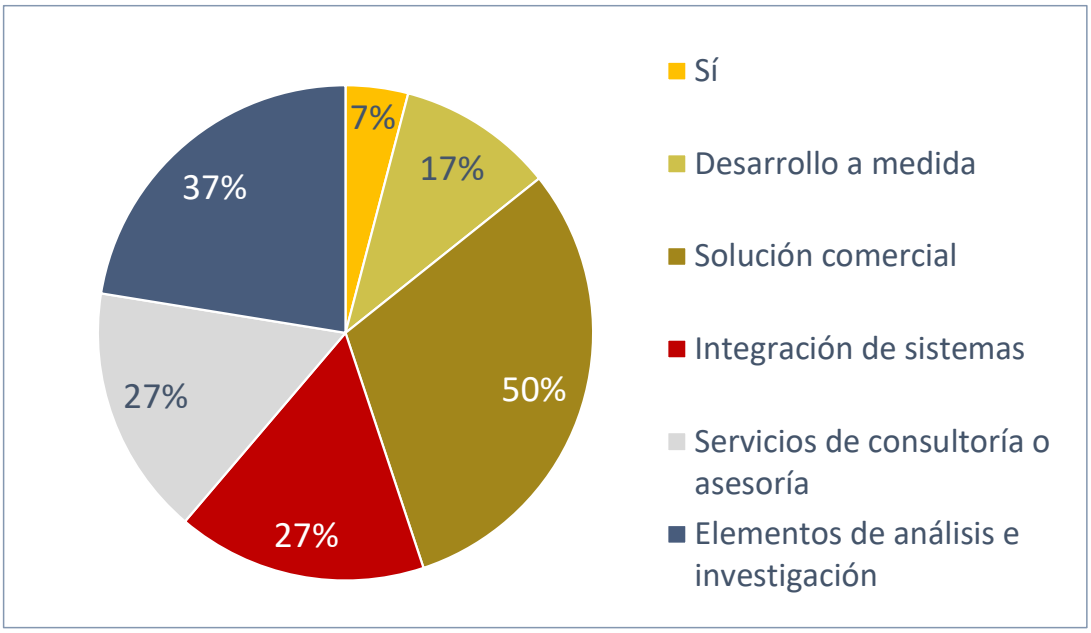


Figura 45. P22: Gráfico. Monitorización y detección de amenazas

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:

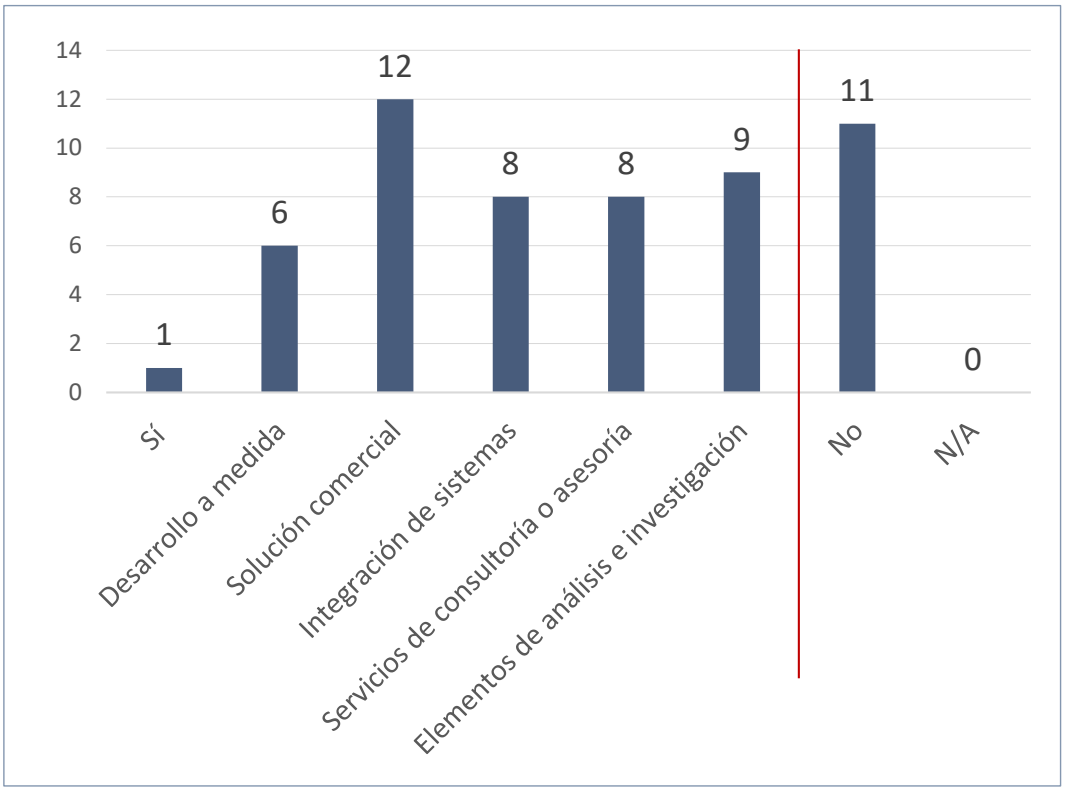


Figura 46. P23: Datos Recolección de información

La representación gráfica de los datos positivos se muestra en la siguiente figura:

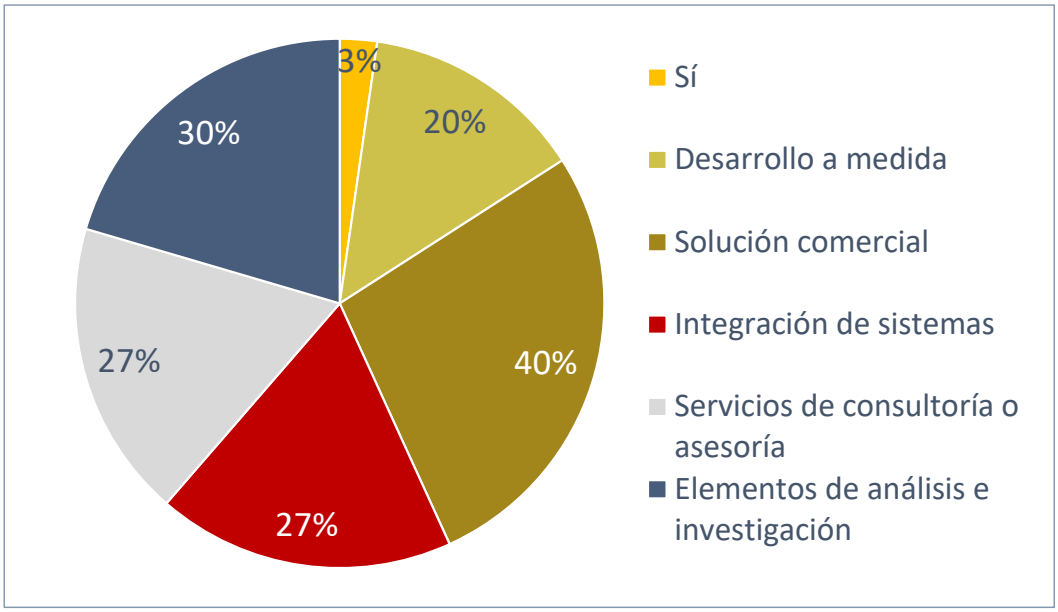


Figura 47. P23: Gráfico. Recolección de información

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:

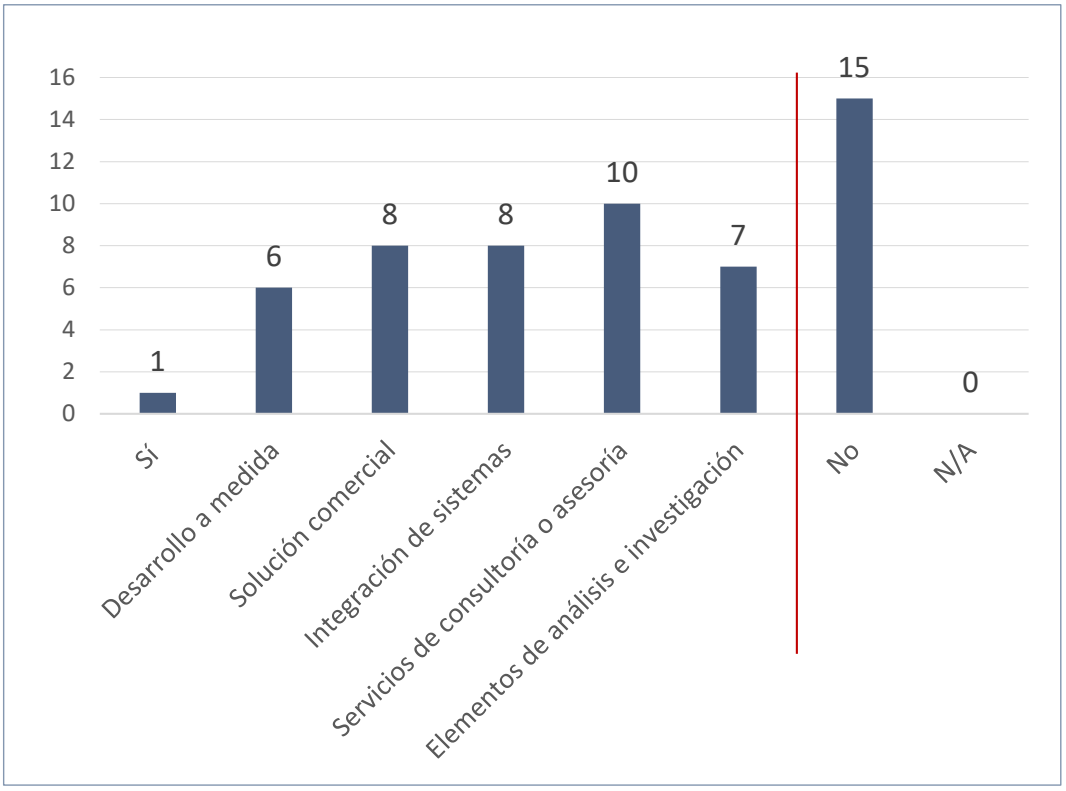


Figura 48. P24: Datos análisis y gestión de riesgos de ciberdefensa

La representación gráfica de los datos positivos se muestra en la siguiente figura:

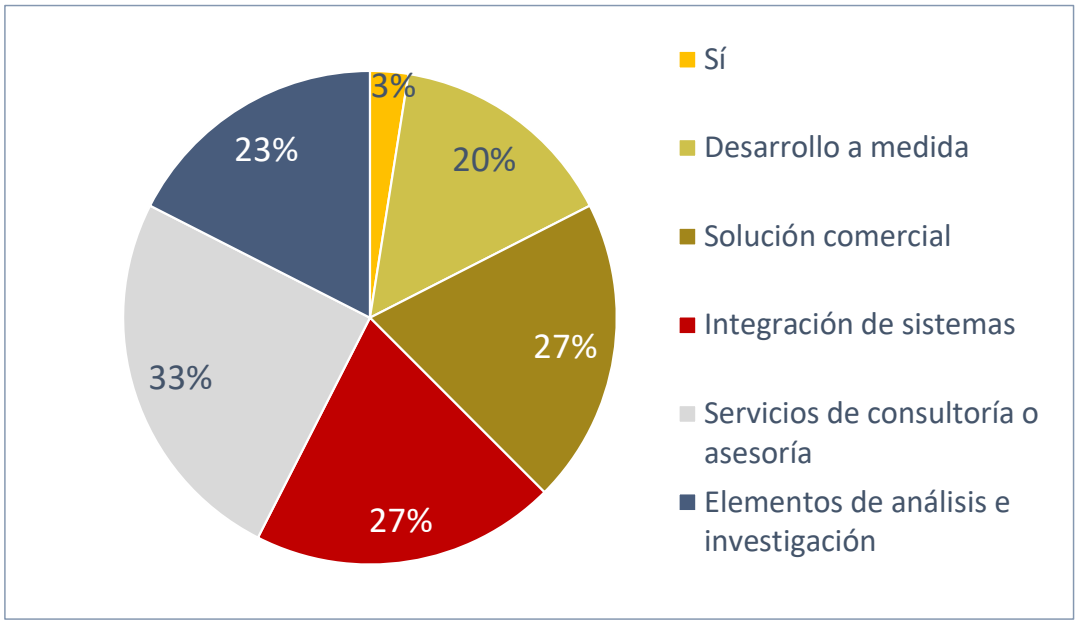


Figura 49. P24: Gráfico. Datos análisis y gestión de riesgos de ciberdefensa

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:

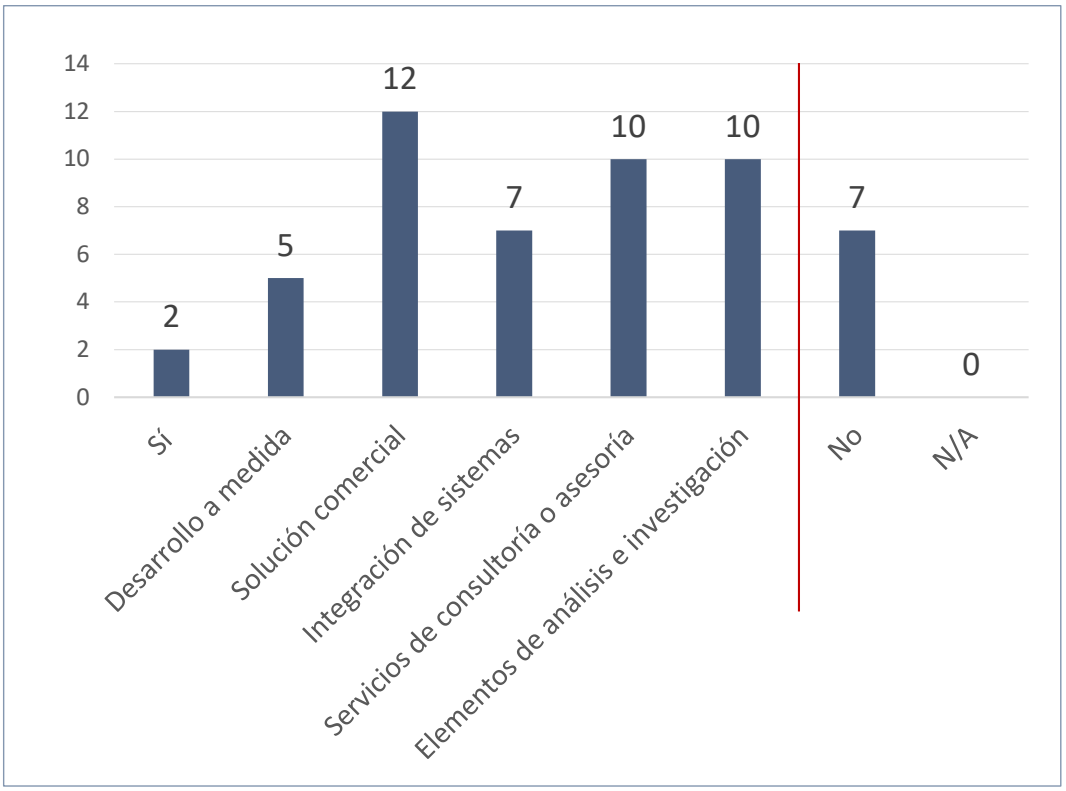


Figura 50. P25: Datos reacción y recuperación ante ataques

La representación gráfica de los datos positivos se muestra en la siguiente figura:

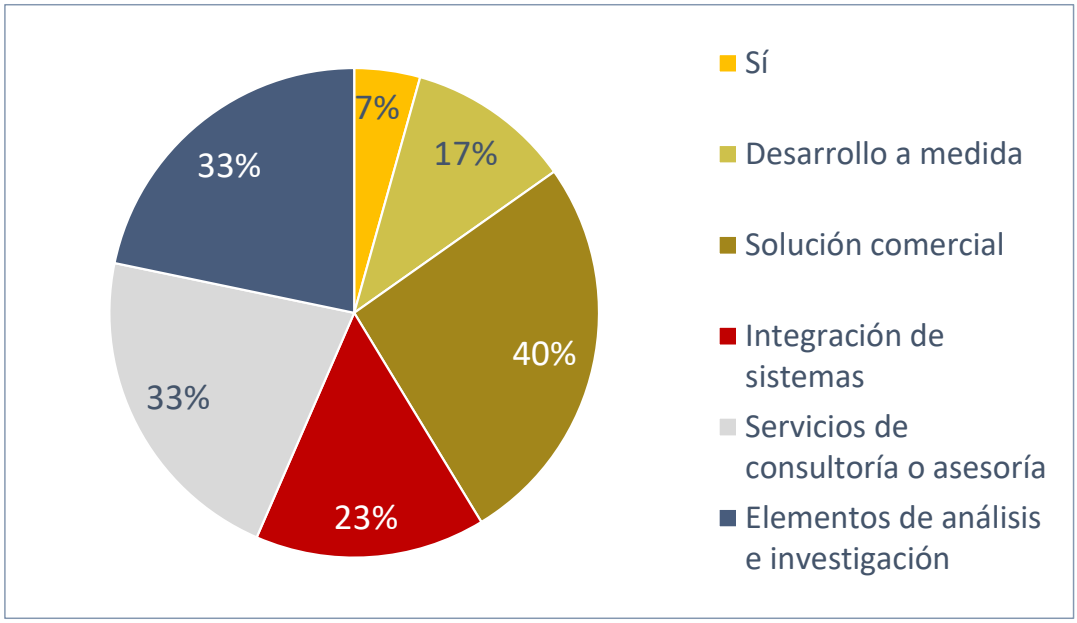


Figura 51. P25: Gráfico. Reacción y recuperación ante ataques

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:

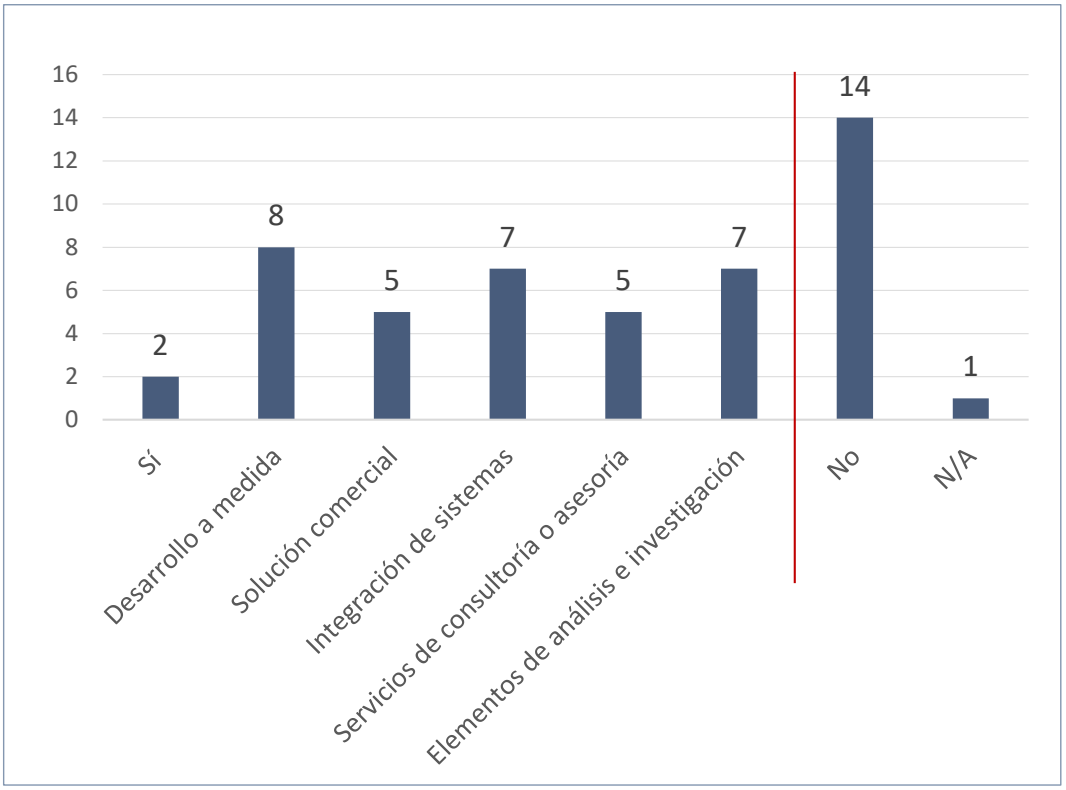


Figura 52. P26: Datos intercambio de información de ciberseguridad

[15] Como AI4CYBER.

La representación gráfica de los datos positivos se muestra en la siguiente figura:

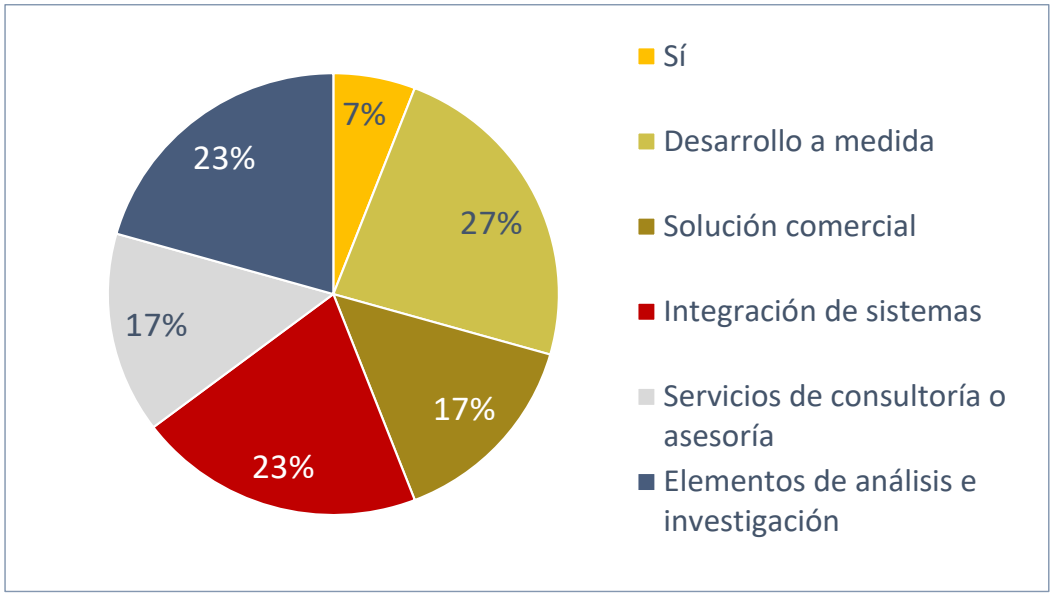


Figura 53. P26: Gráfico.Intercambio de información de ciberseguridad

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:

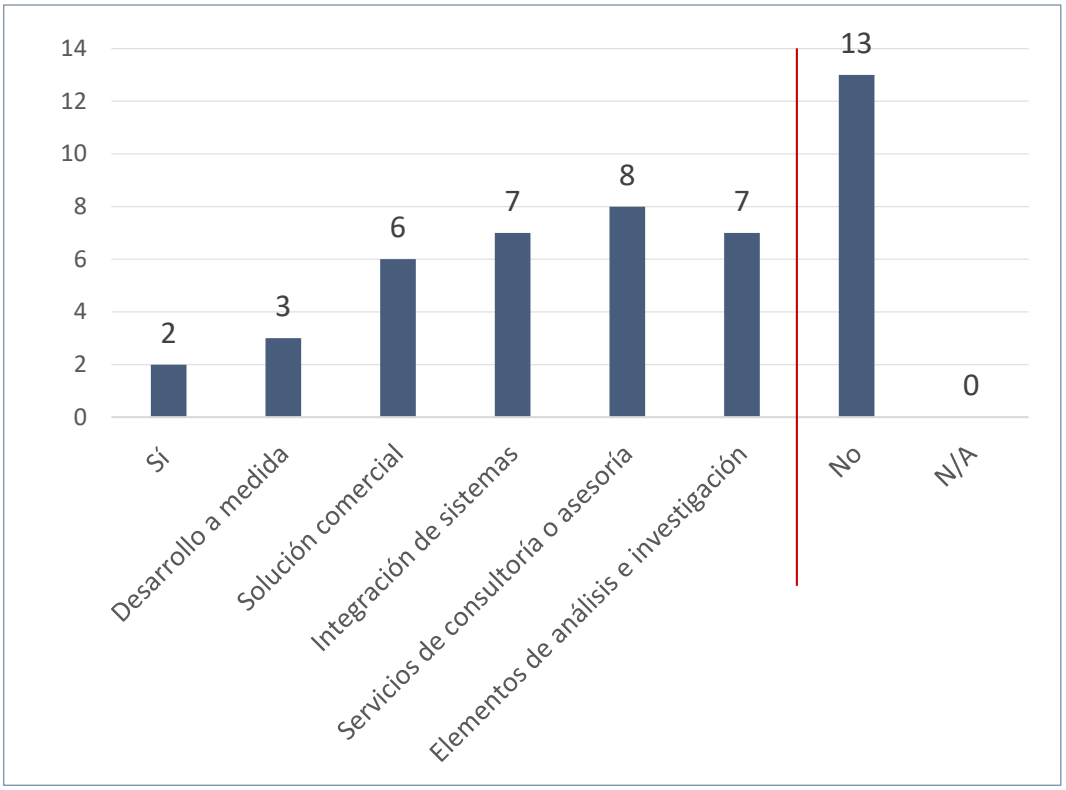


Figura 54. P27: Datos Despliegue de Centro de operaciones de seguridad

La representación gráfica de los datos positivos se muestra en la siguiente figura:

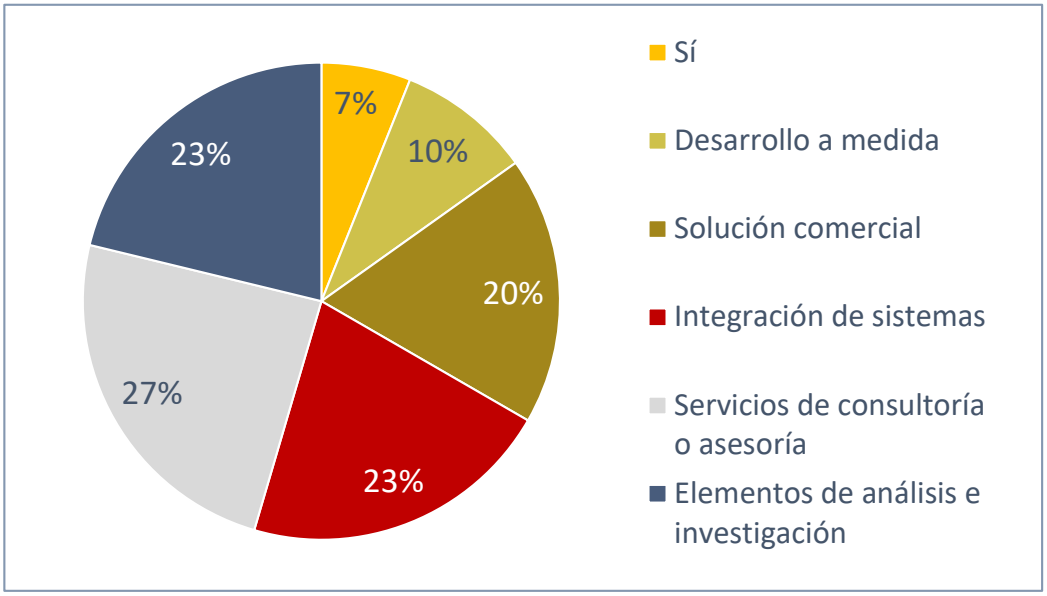


Figura 55, P27: Gráfico. Despliegue de centro de operaciones de seguridad

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:

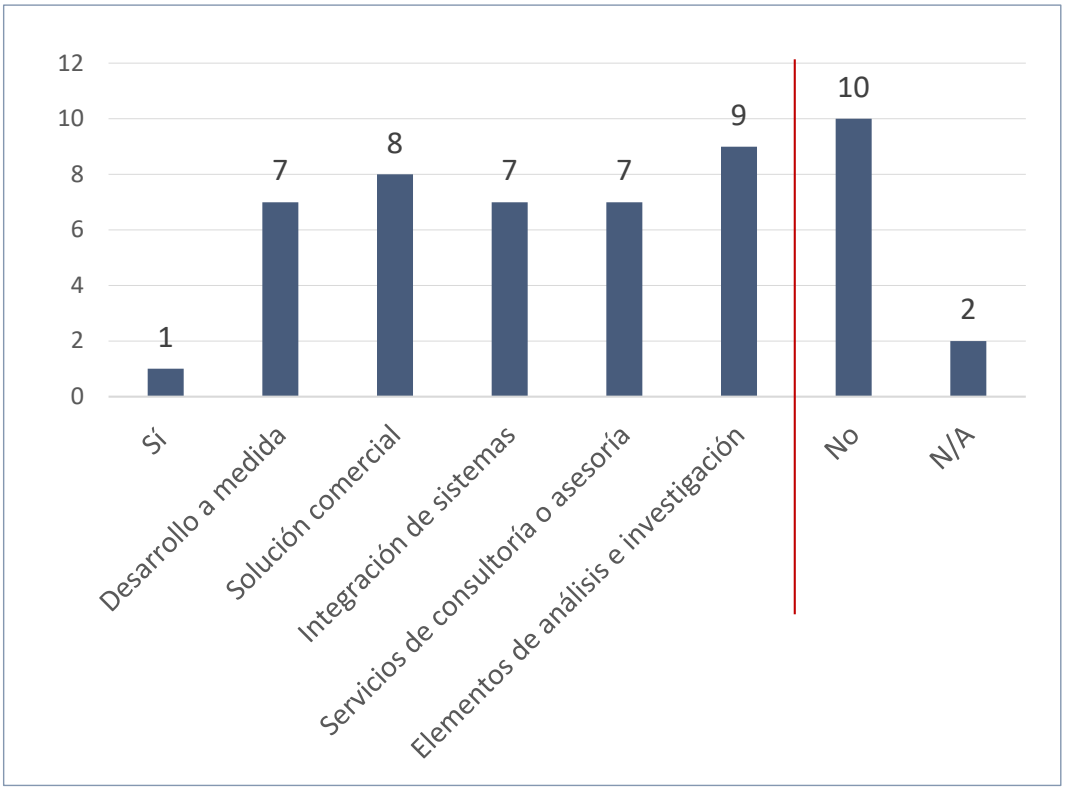


Figura 56. P28: Datos recolección de inteligencia de fuentes abiertas

La representación gráfica de los datos positivos se muestra en la siguiente figura:

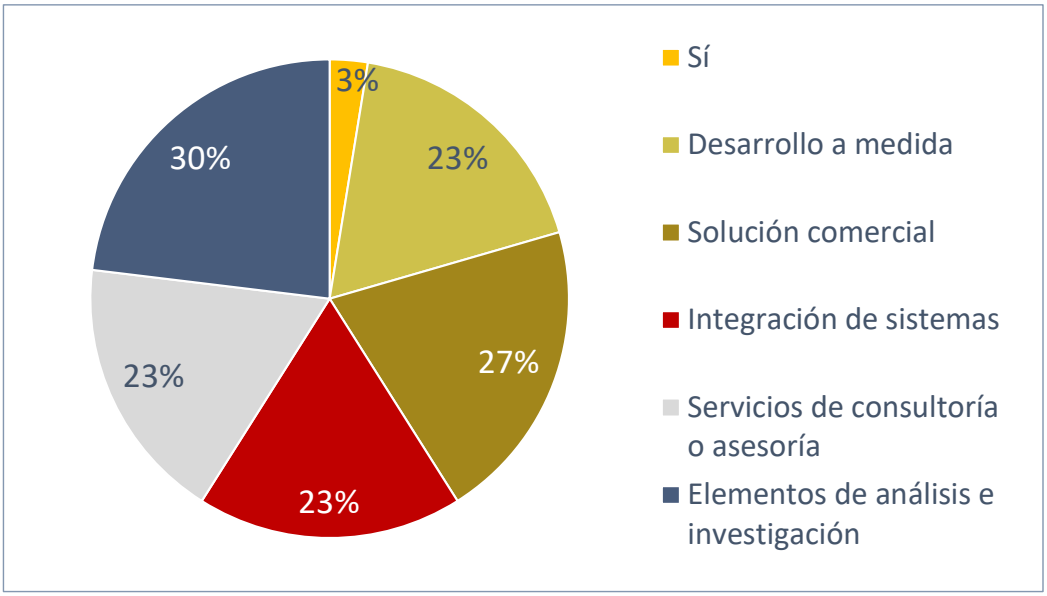


Figura 57. P28: Gráfico. Recolección de inteligencia de fuentes abiertas

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:

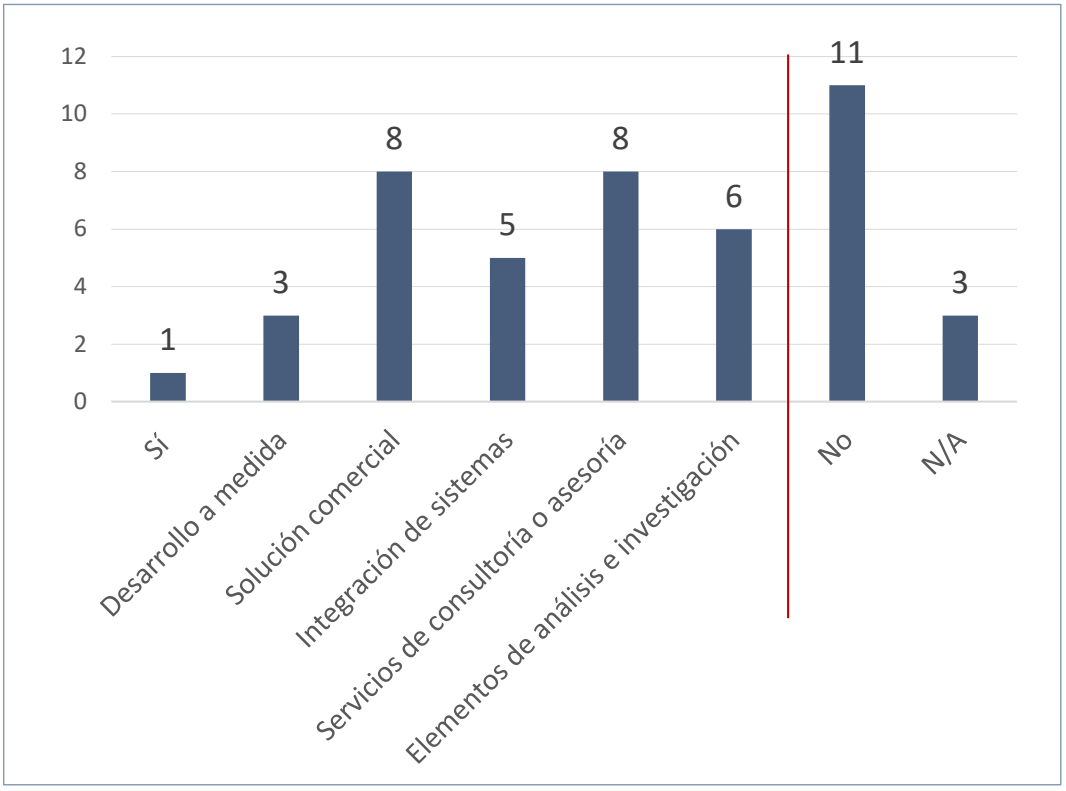


Figura 58. P29: Datos Reconocimiento

La representación gráfica de los datos positivos se muestra en la siguiente figura:

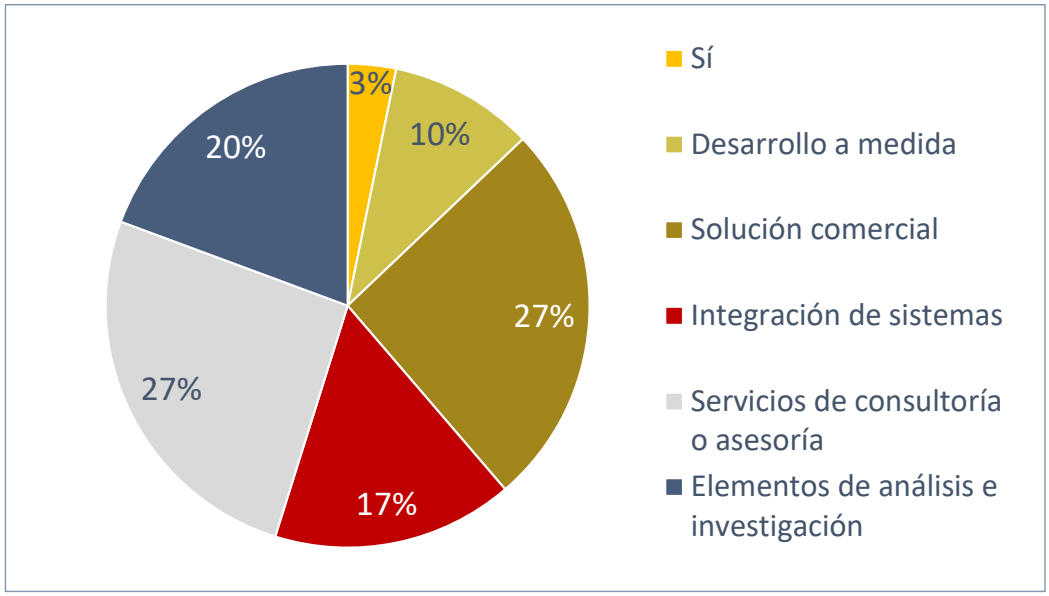


Figura 59. P29: Gráfico.Reconocimiento

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:

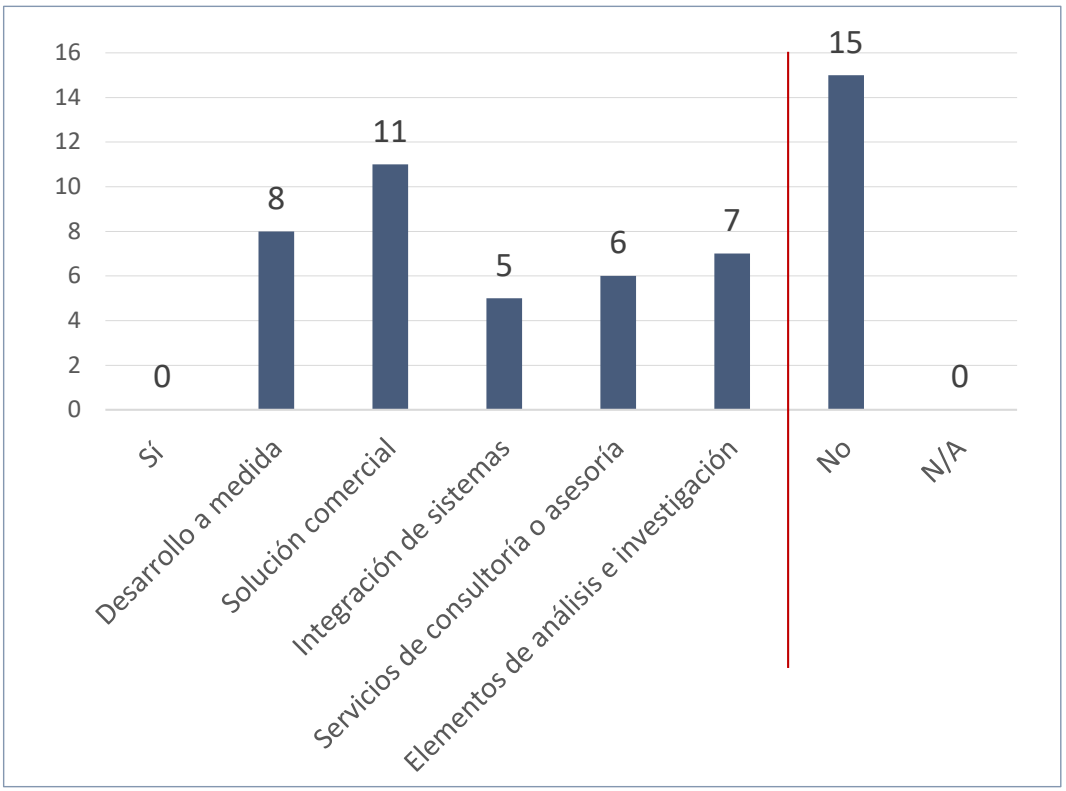


Figura 60. P30: Datos Transformación, integración y ennumeración de la información

La representación gráfica de los datos positivos se muestra en la siguiente figura:

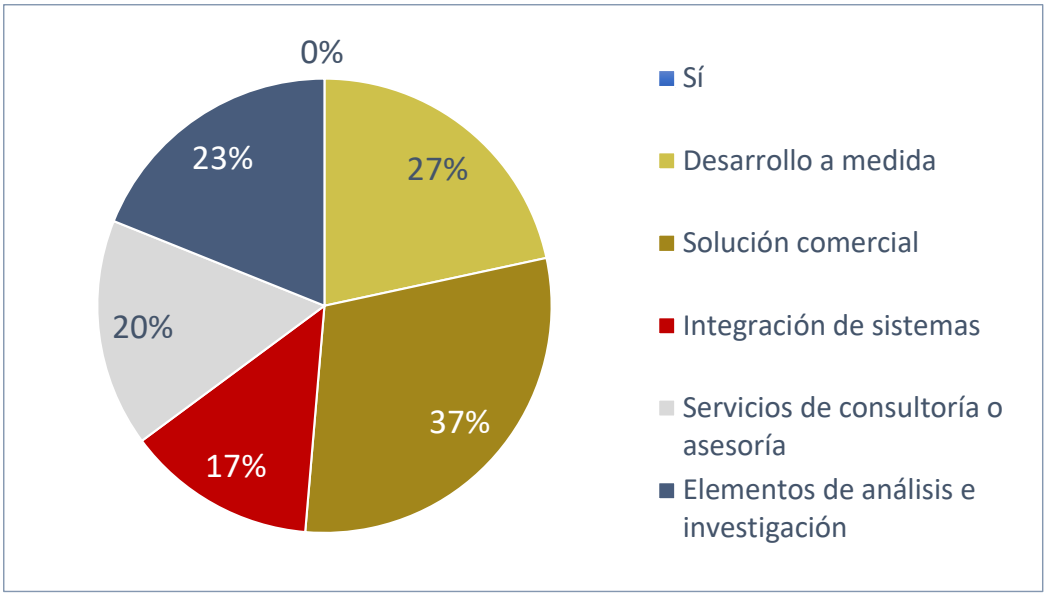


Figura 61. P30: Gráfico. Transformación, integración y ennumeración de la información

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:

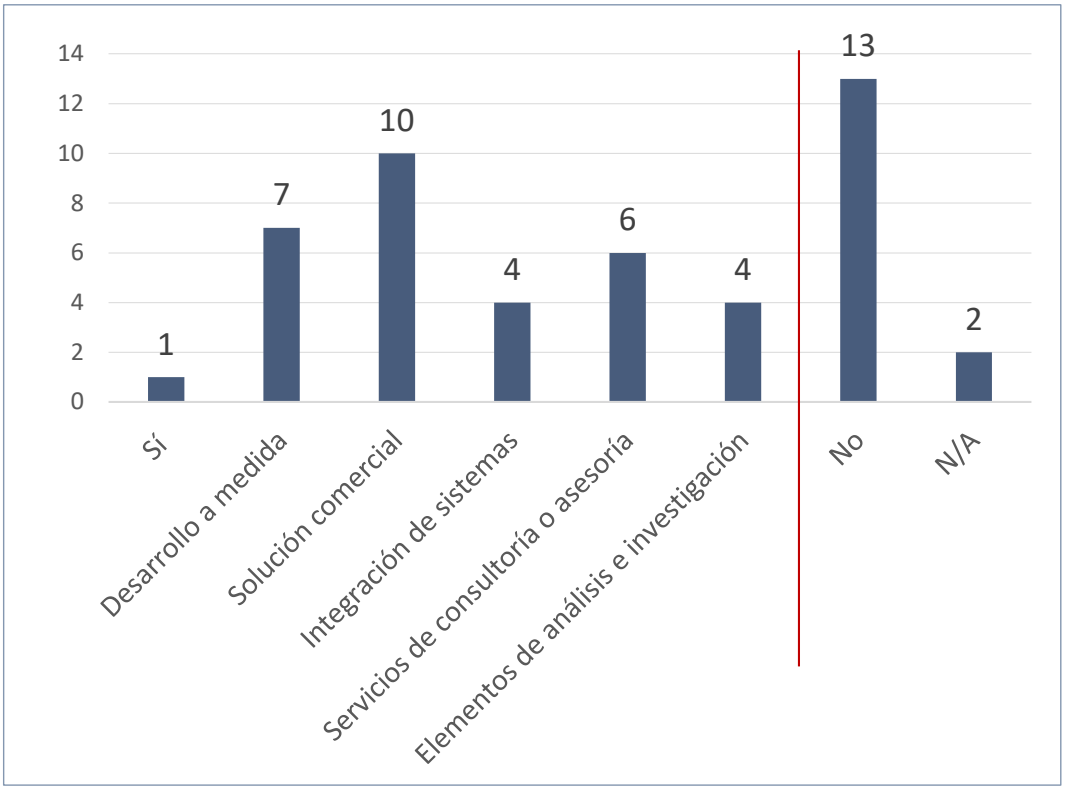


Figura 62. P31: Datos Representación de la información

La representación gráfica de los datos positivos se muestra en la siguiente figura:

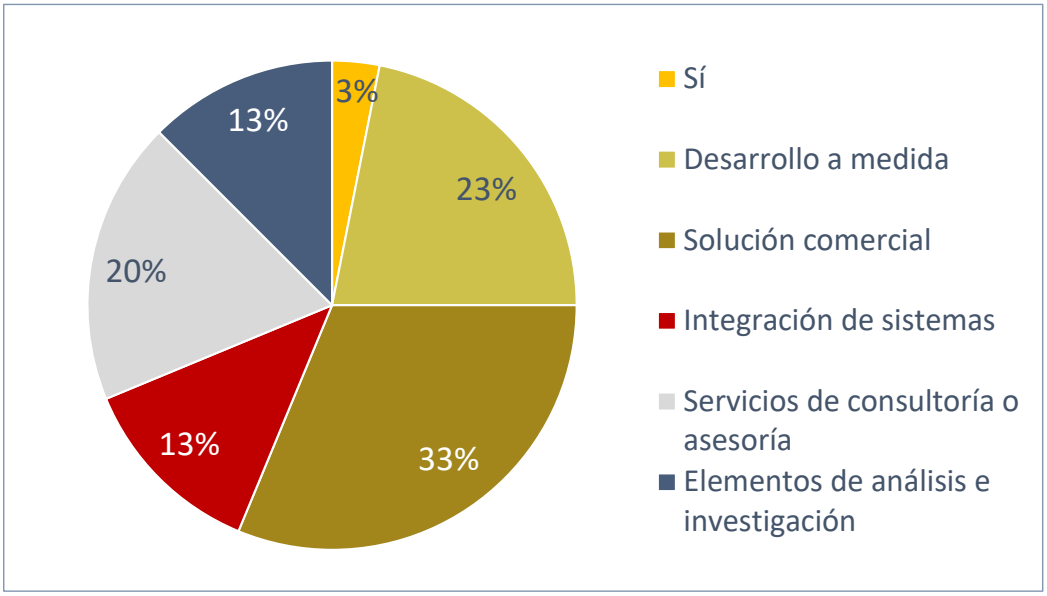


Figura 63. P31: Gráfico. Representación de la información

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:

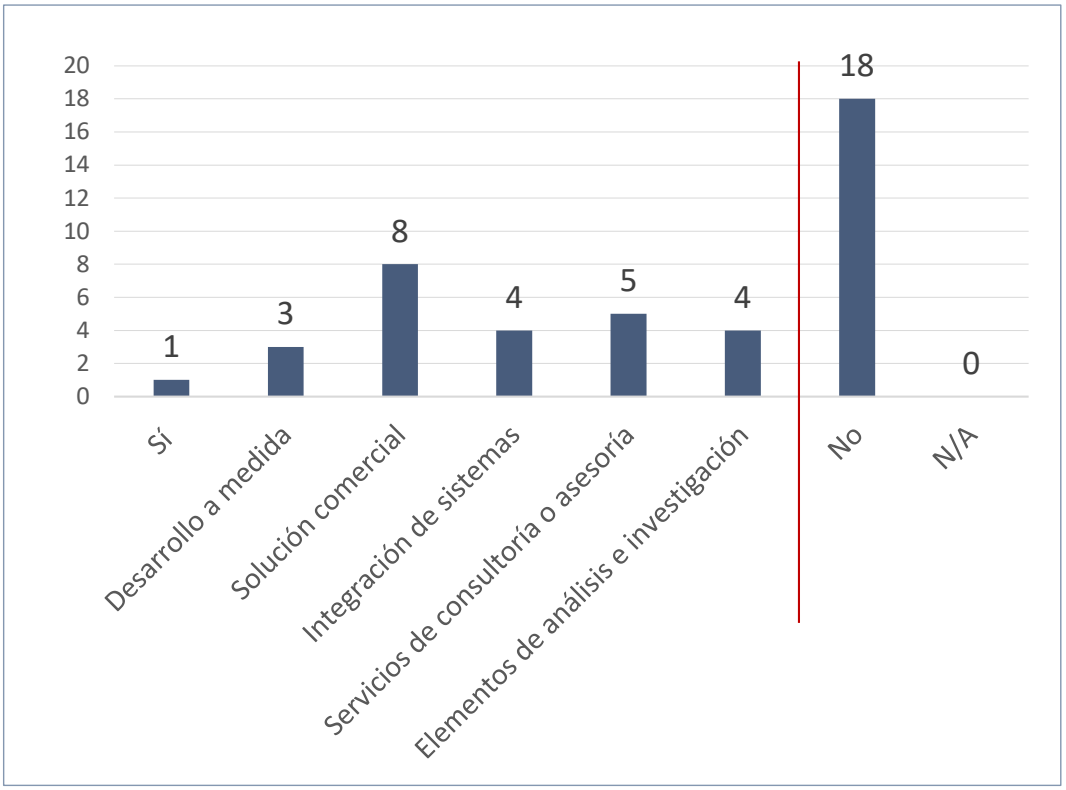


Figura 64. P32: Datos Gestor de mapeo de identidades y vínculos de red en internet

La representación gráfica de los datos positivos se muestra en la siguiente figura:

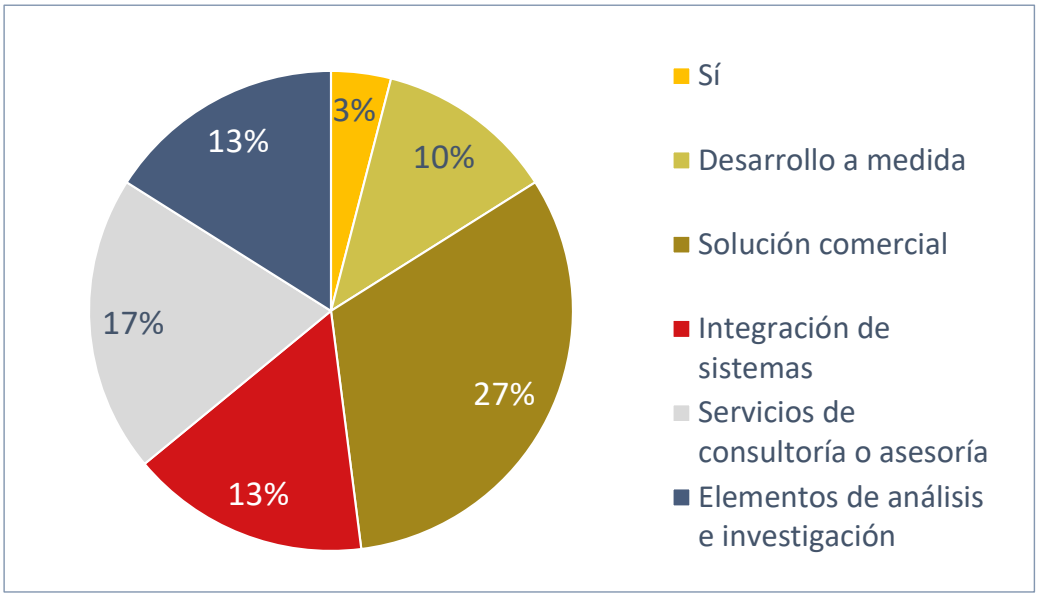


Figura 65. P32: Gráfico. Gestor de mapeo de identidades y vínculos de red en internet

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:

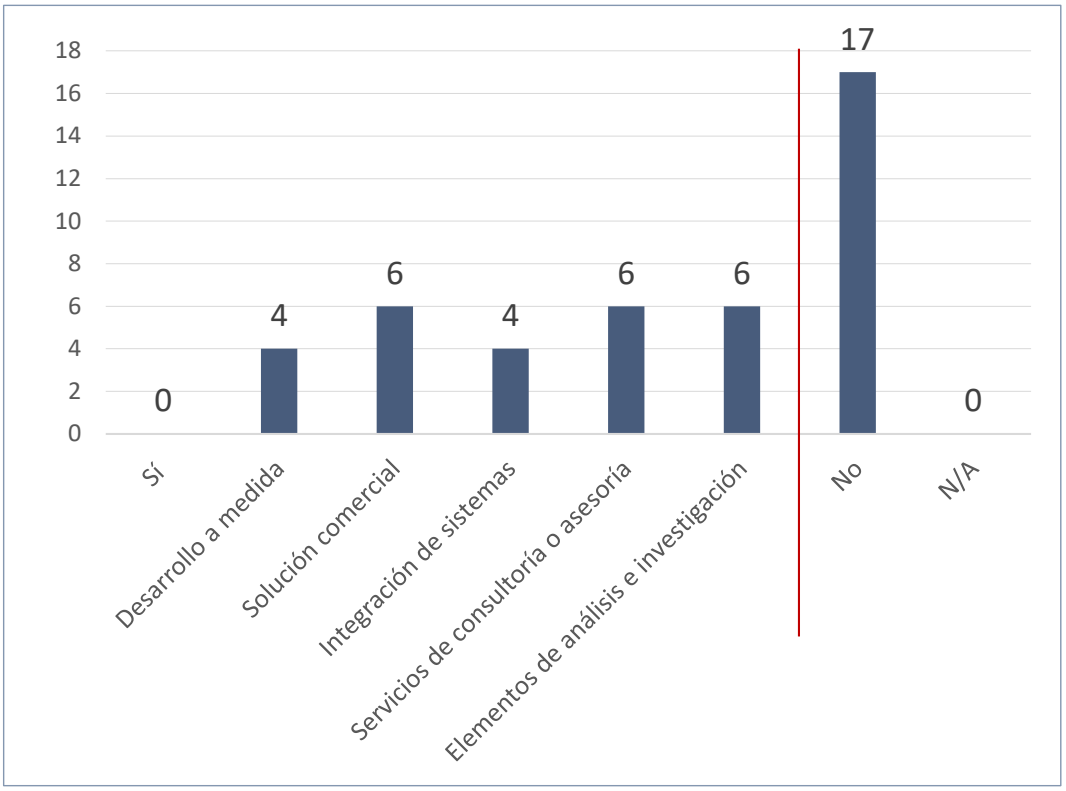


Figura 66. P33: Datos Análisis de redes sociales

La representación gráfica de los datos positivos se muestra en la siguiente figura:

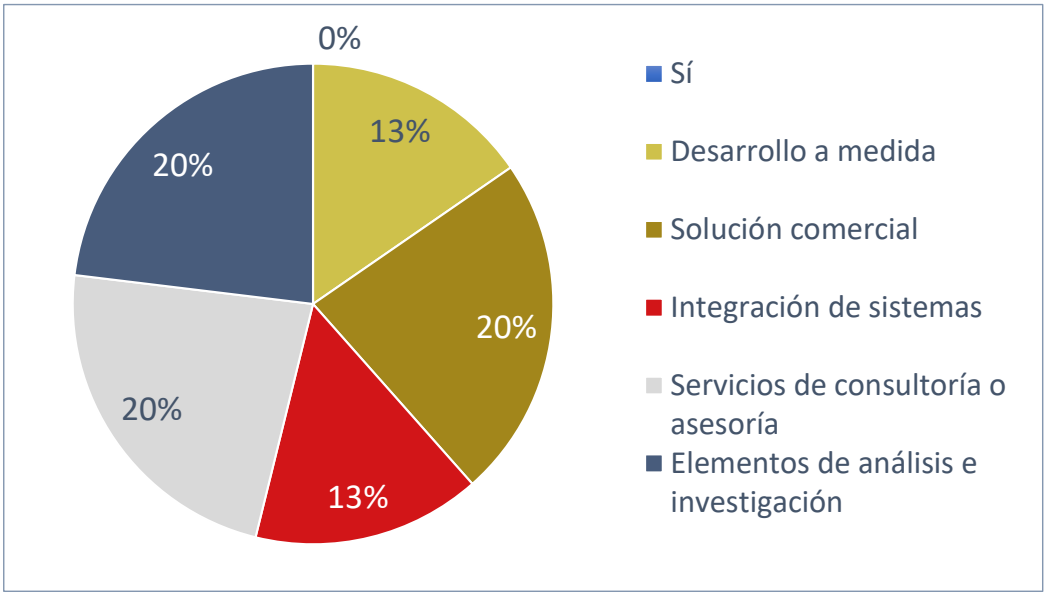


Figura 67. P33: Gráfico. Análisis de redes sociales

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:

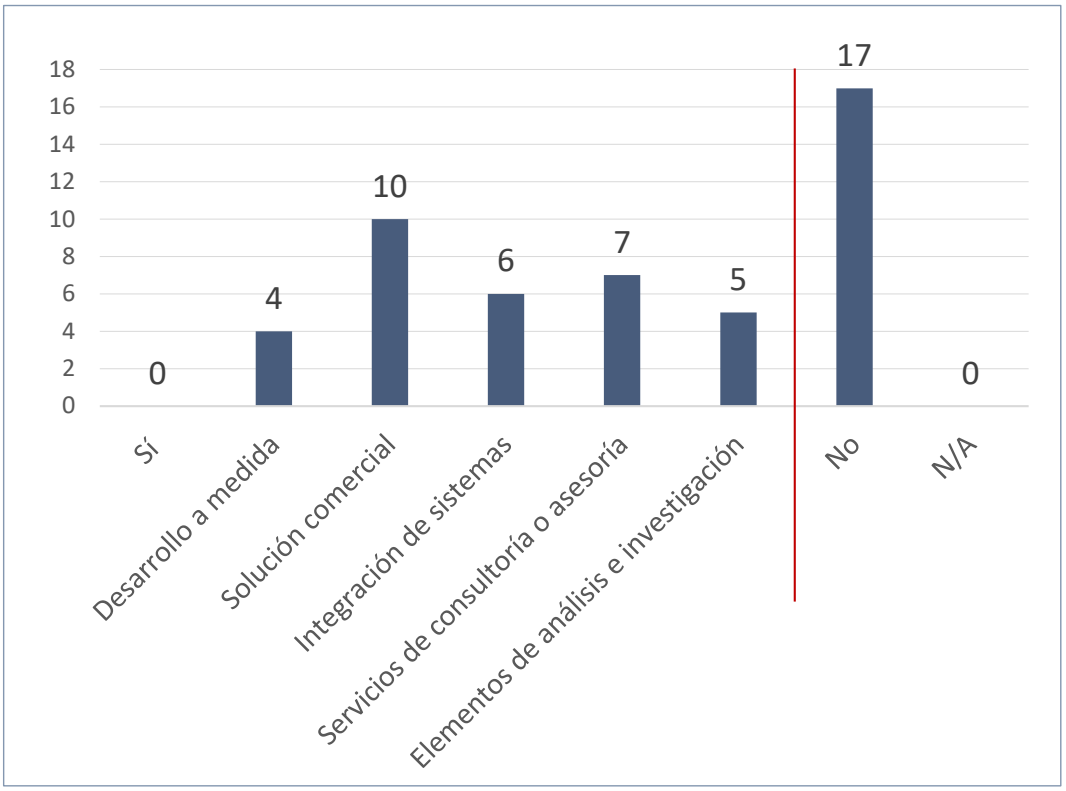


Figura 68. P34: Datos Gestor de feeds de inteligencia de pago y proveedores de datos

La representación gráfica de los datos positivos se muestra en la siguiente figura:

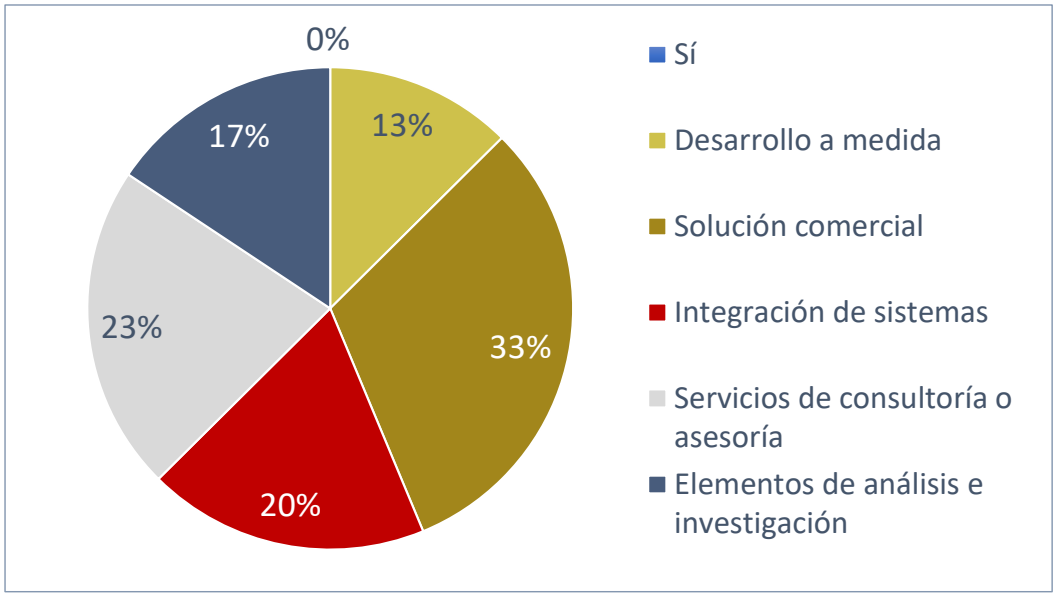


Figura 69. P34: Gráfico. Gestor de feeds de inteligencia de pago y proveedores de datos

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:

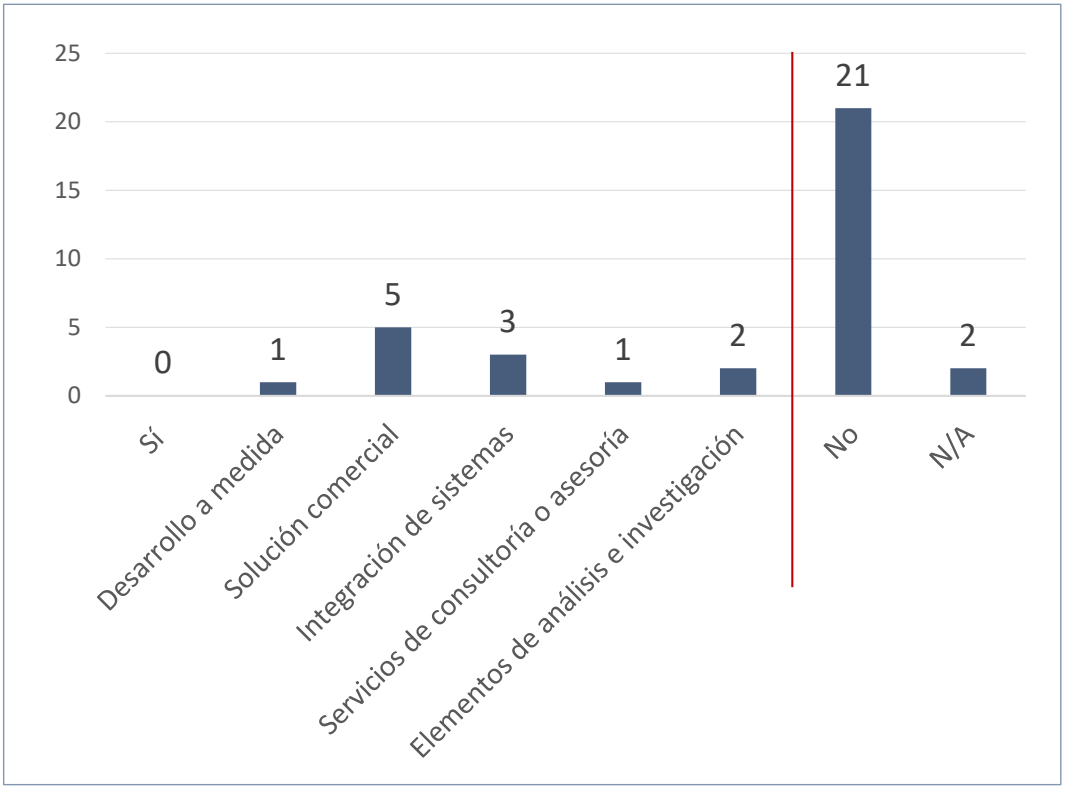


Figura 70. P35: Datos Anonimización

La representación gráfica de los datos positivos se muestra en la siguiente figura:

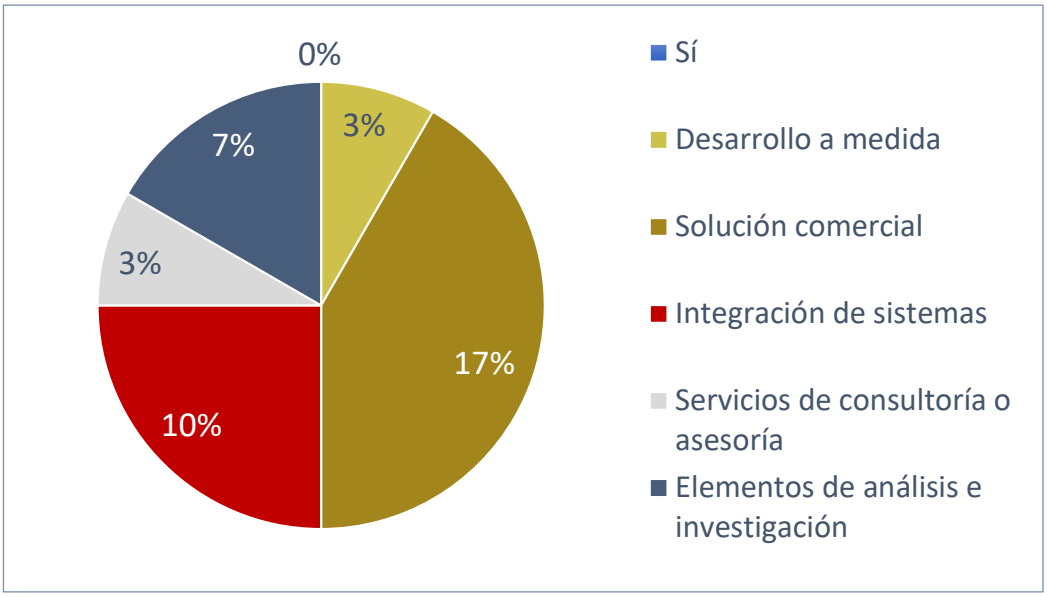


Figura 71. P35: Gráfico. Anonimización

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:

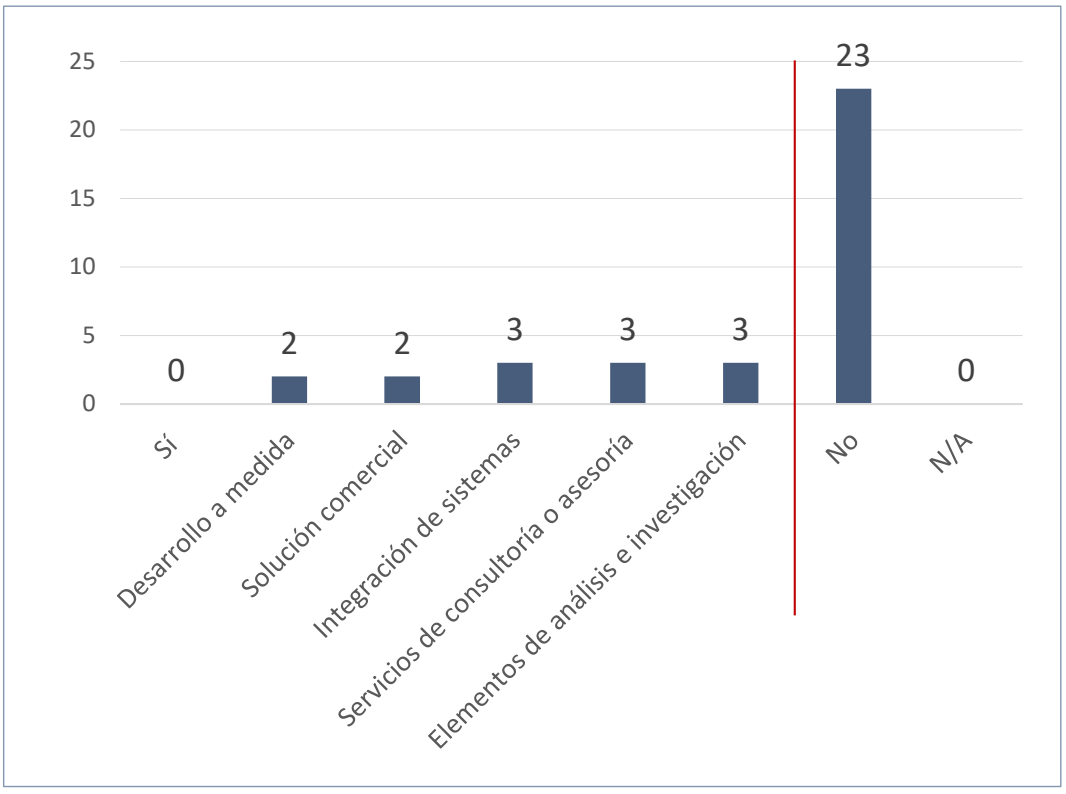


Figura 72. P36: Datos Generación de avatares e identidades digitales

La representación gráfica de los datos positivos se muestra en la siguiente figura:

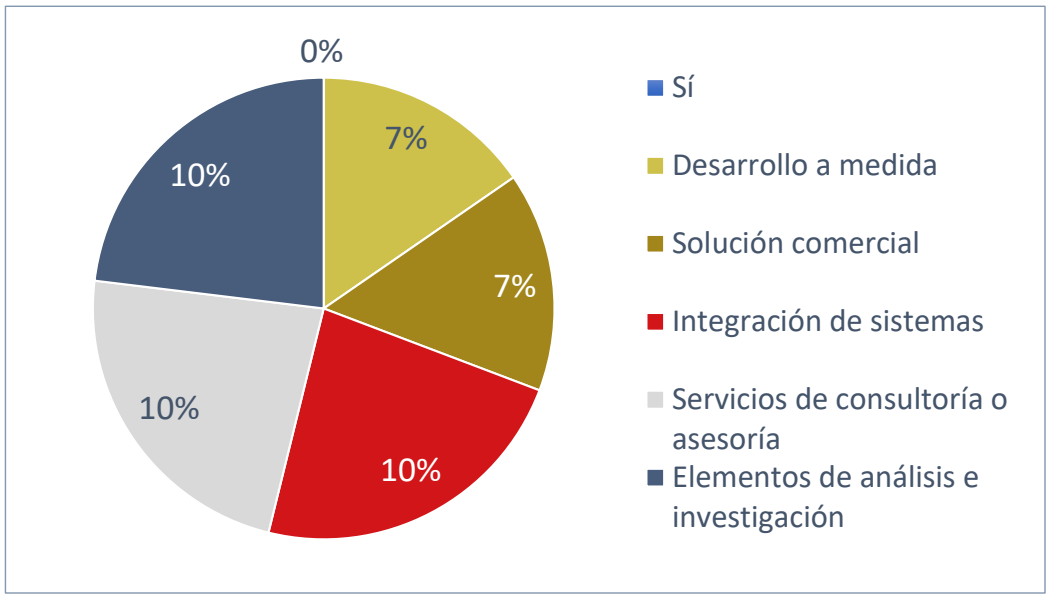


Figura 73. P36: Gráfico. Generación de avatares e identidades digitales

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:

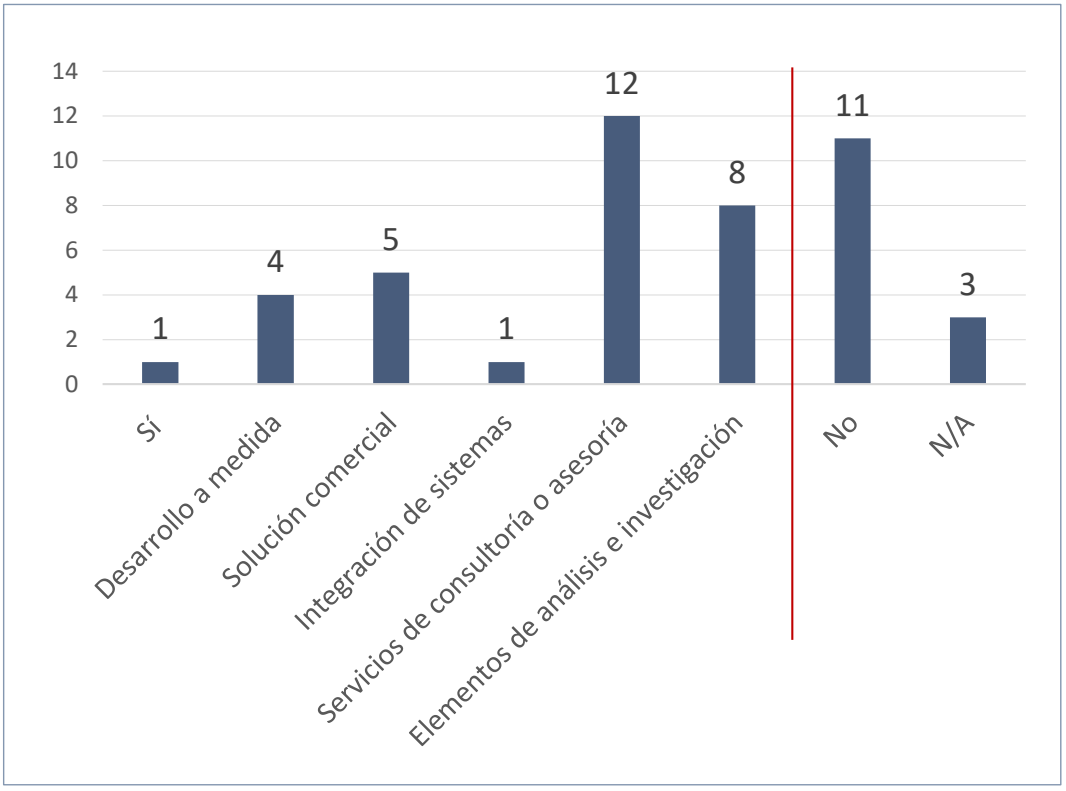


Figura 74. P37: Datos gestión de recursos para operaciones de respuesta

[21] https://attack.mitre.org/

La representación gráfica de los datos positivos se muestra en la siguiente figura:

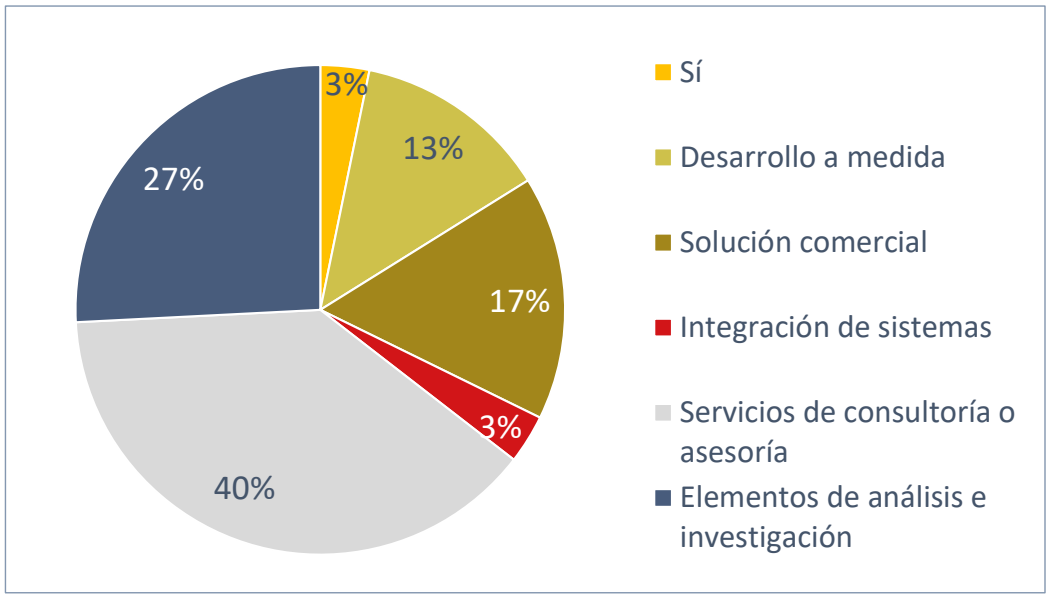


Figura 75. P37: Gráfico. Gestión de recursos para operaciones de respuesta

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:

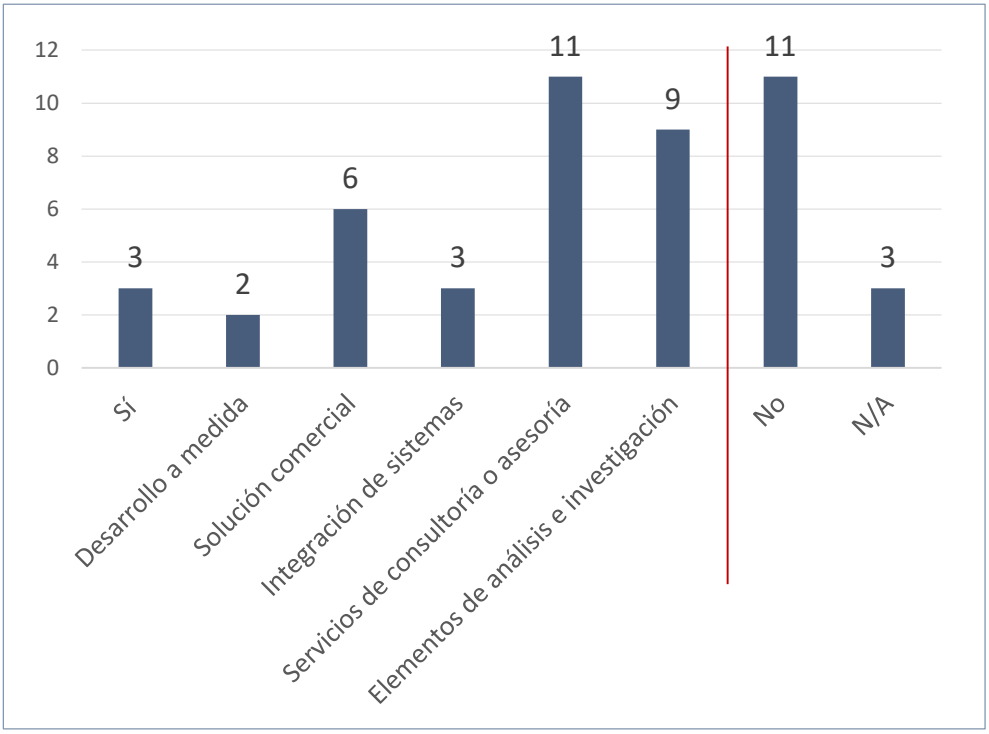


Figura 76. P38: Datos Acceso inicial

La representación gráfica de los datos positivos se muestra en la siguiente figura:

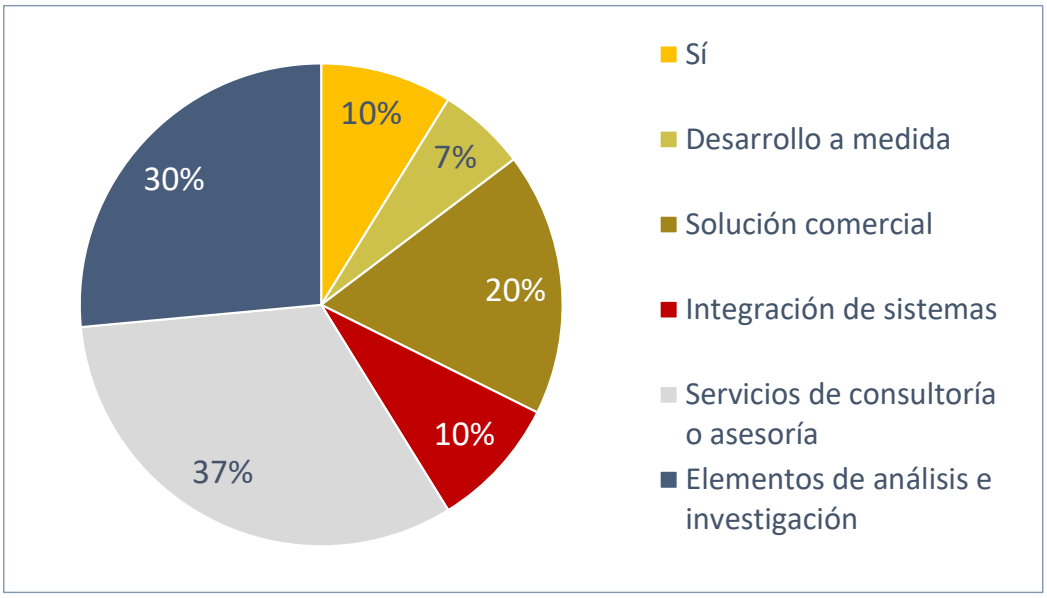


Figura 77. P38: Gráfico. Acceso inicial

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:

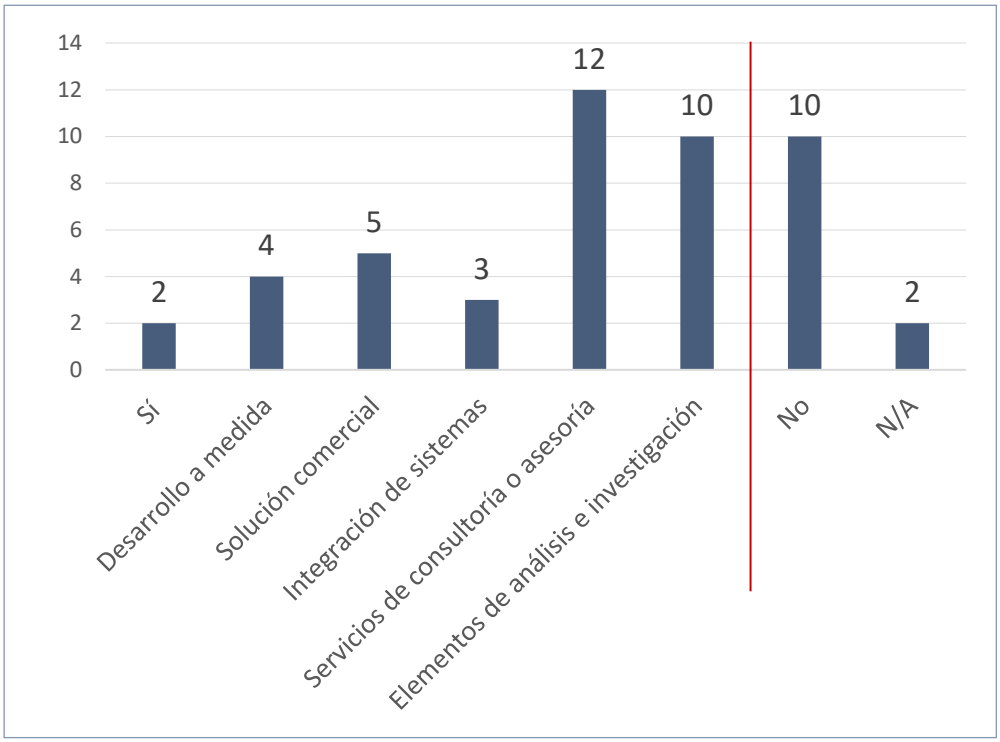


Figura 78. P39: Datos Ejecución

La representación gráfica de los datos positivos se muestra en la siguiente figura:

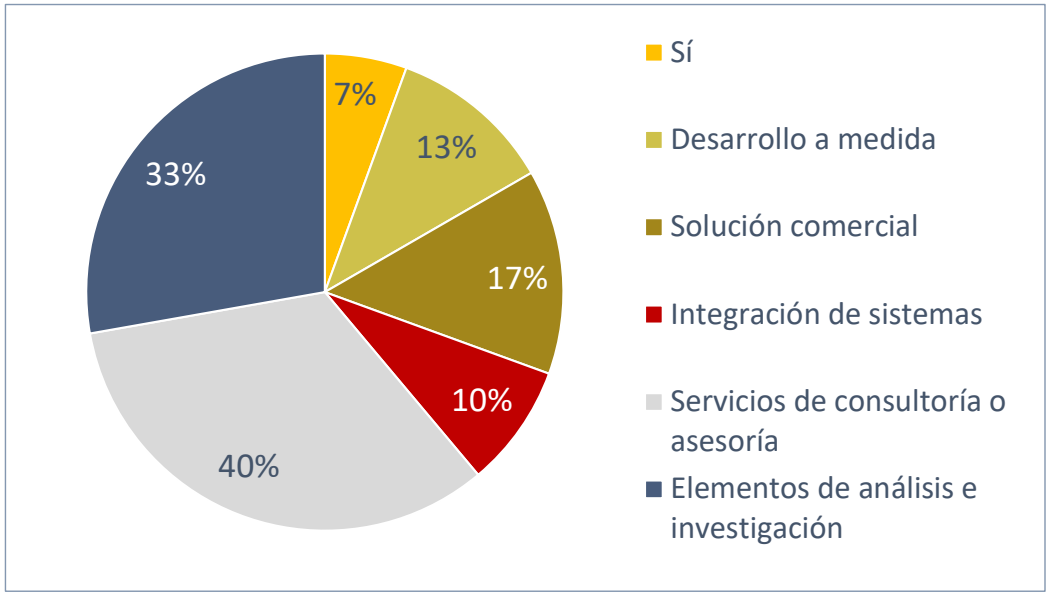


Figura 79. P39: Gráfico. Ejecución

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:

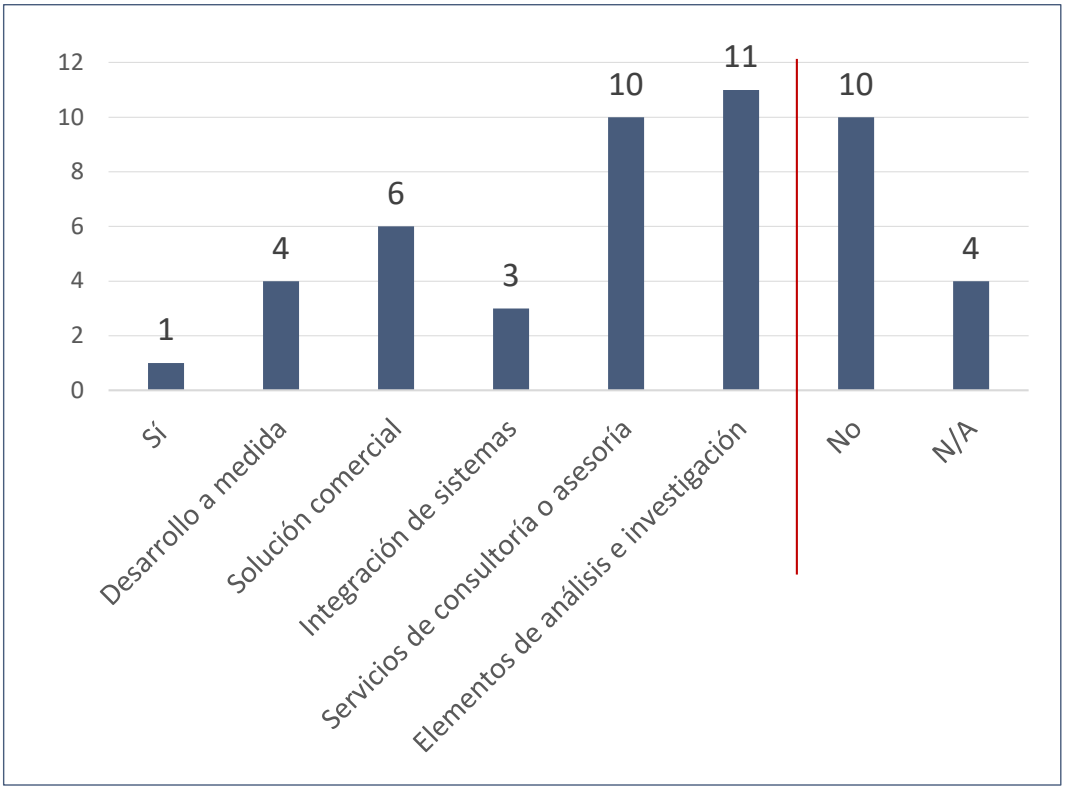


Figura 80. P40: Datos Persistencia

La representación gráfica de los datos positivos se muestra en la siguiente figura:

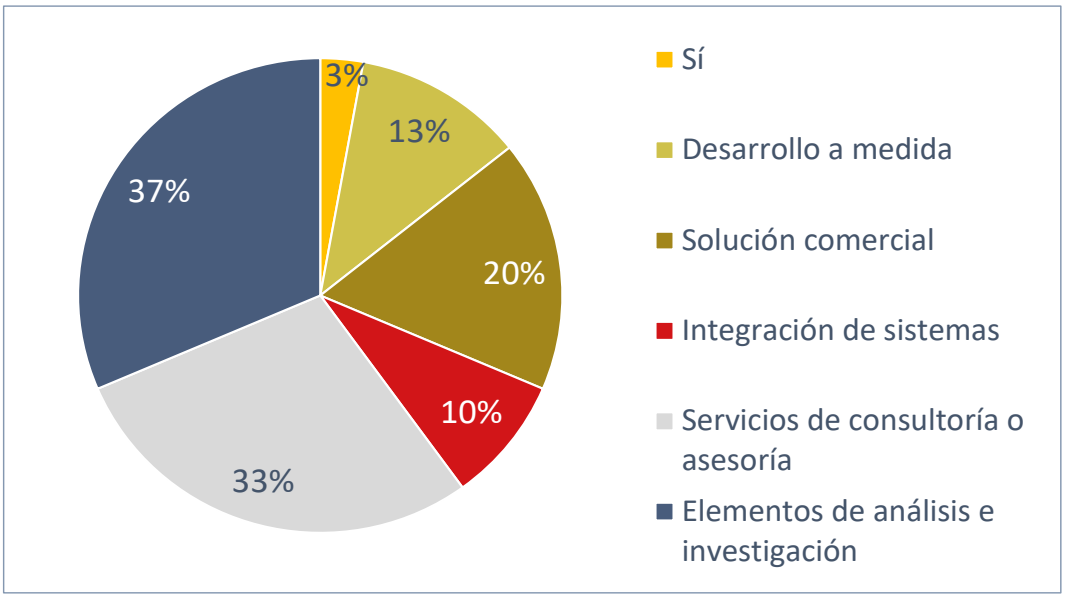


Figura 81. P40. Gráfico. Persistencia

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:

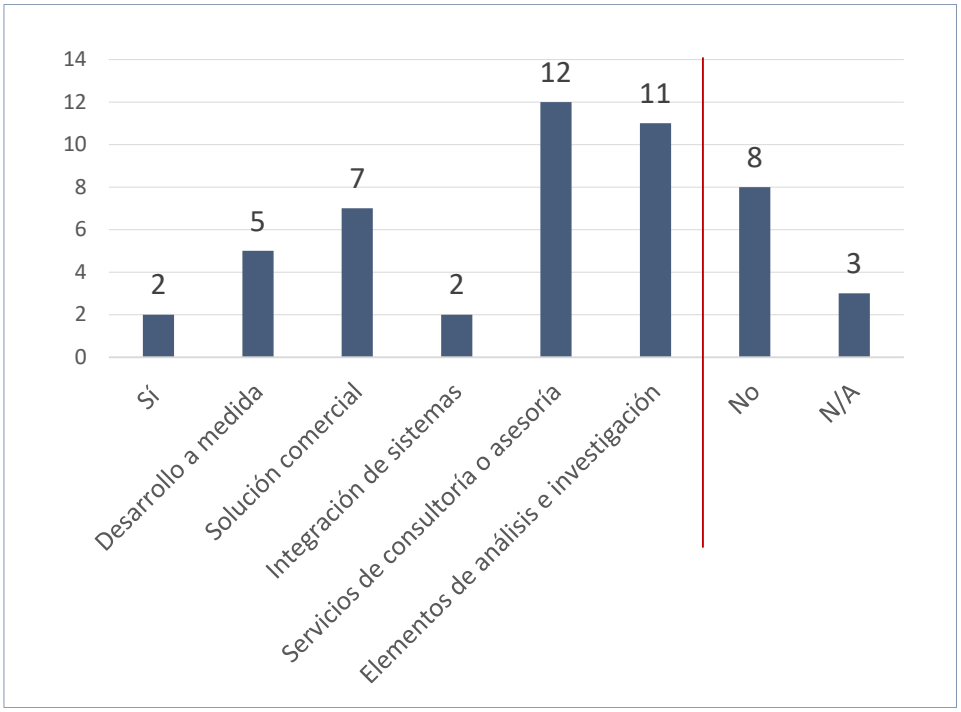


Figura 82. P41: Escalada de privilegios

La representación gráfica de los datos positivos se muestra en la siguiente figura:

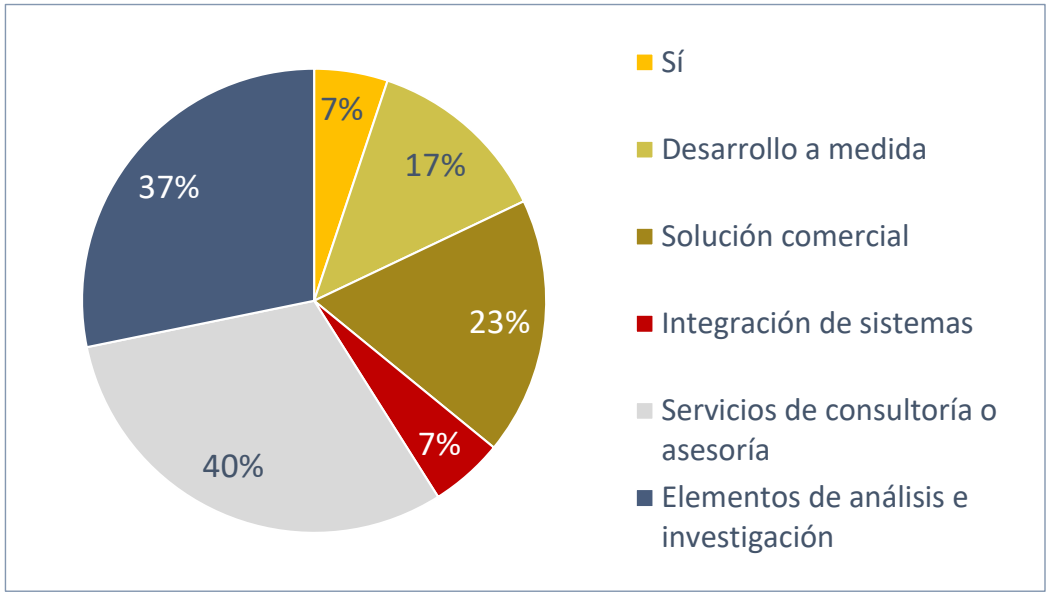


Figura 83. P41: Gráfico. Escalada de privilegios

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:

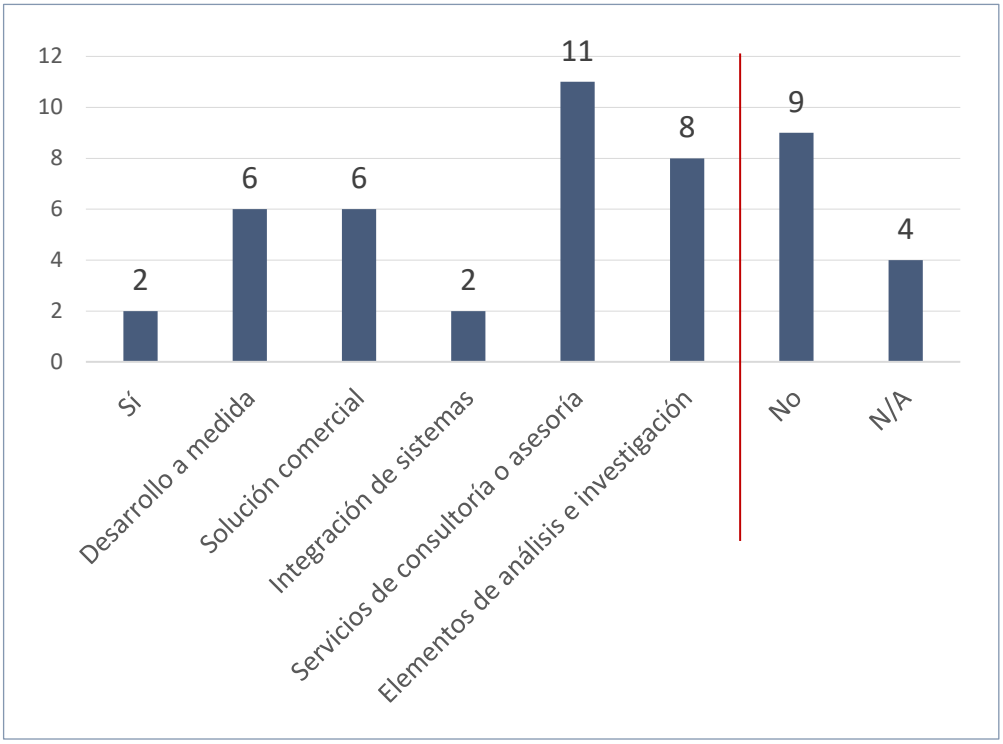


Figura 82. P42: Datos Evasión de defensas

La representación gráfica de los datos positivos se muestra en la siguiente figura:

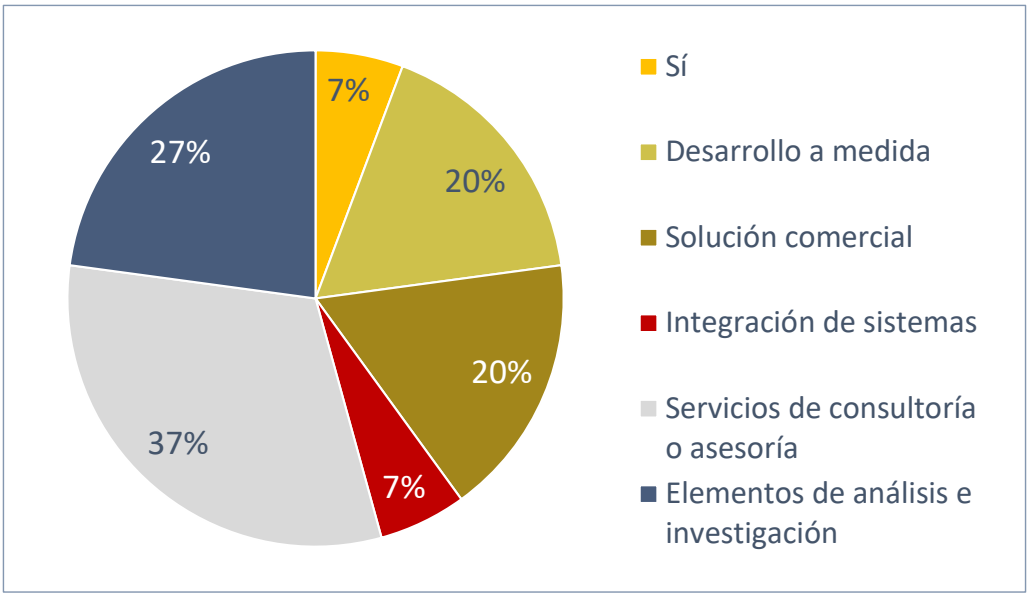


Figura 82. P42: Gráfico. Evasión de defensas

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:

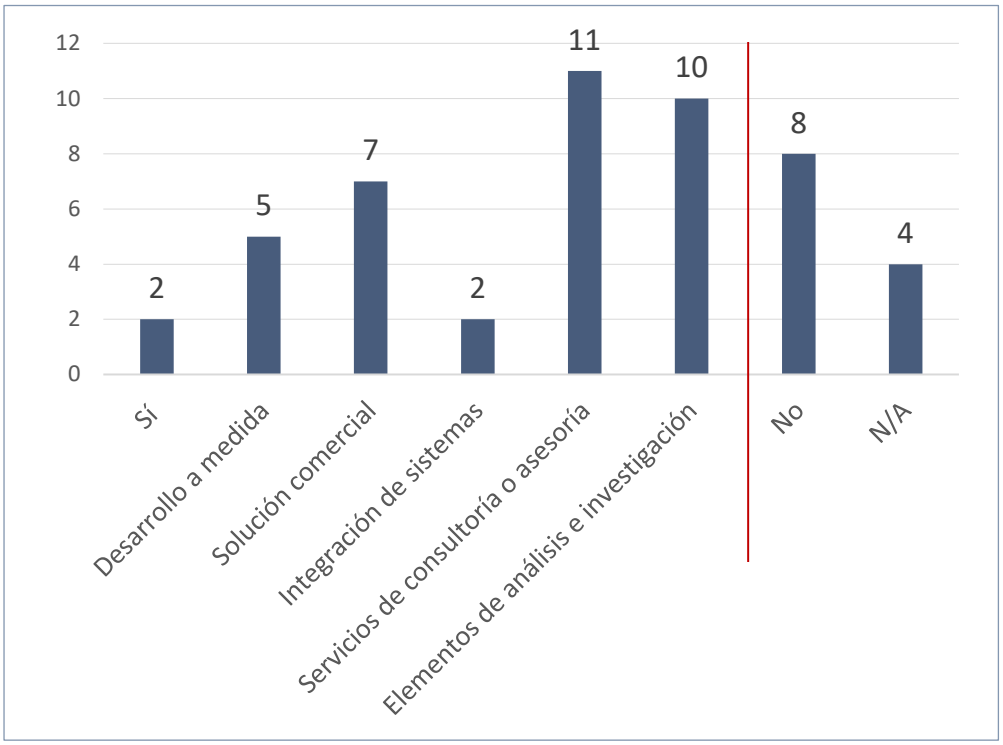


Figura 86. P43: Datos Acceso a credenciales

La representación gráfica de los datos positivos se muestra en la siguiente figura:

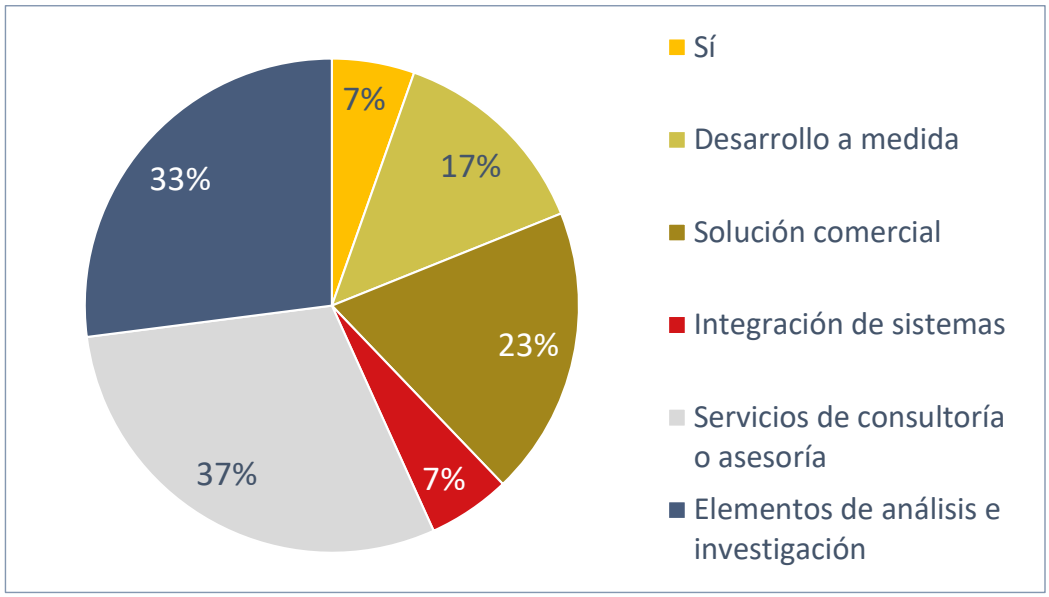


Figura 87. P43: Gráfico. Acceso a credenciales

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:

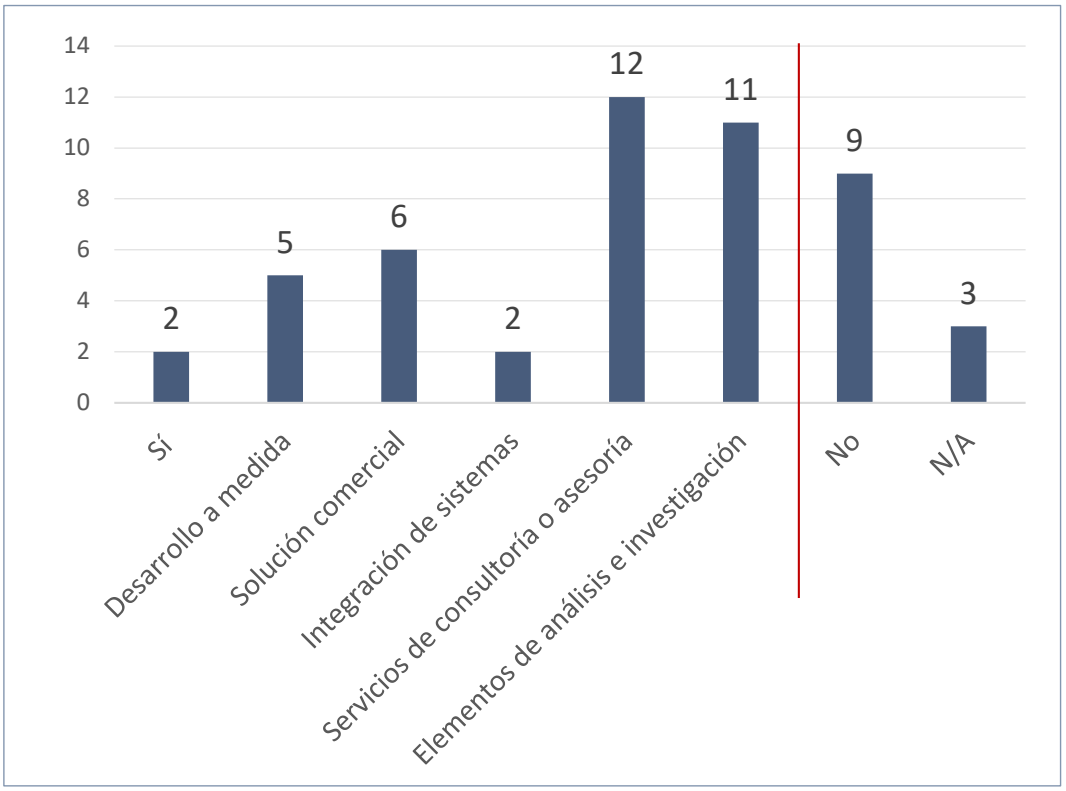


Figura 88. P44: Datos Descubrimiento

La representación gráfica de los datos positivos se muestra en la siguiente figura:

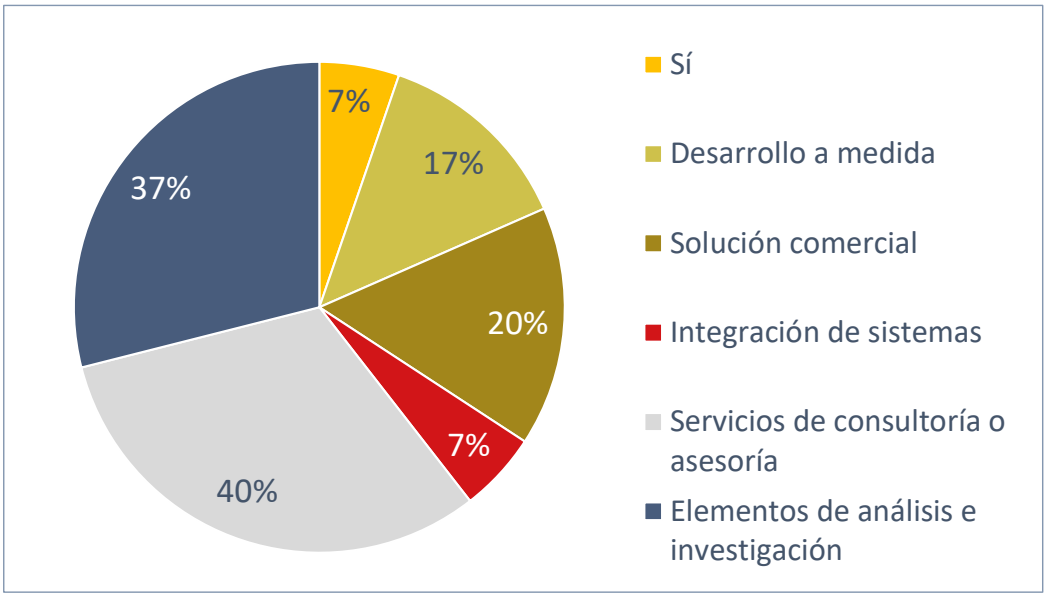


Figura 89. P44: Gráfico. Descubrimiento

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:

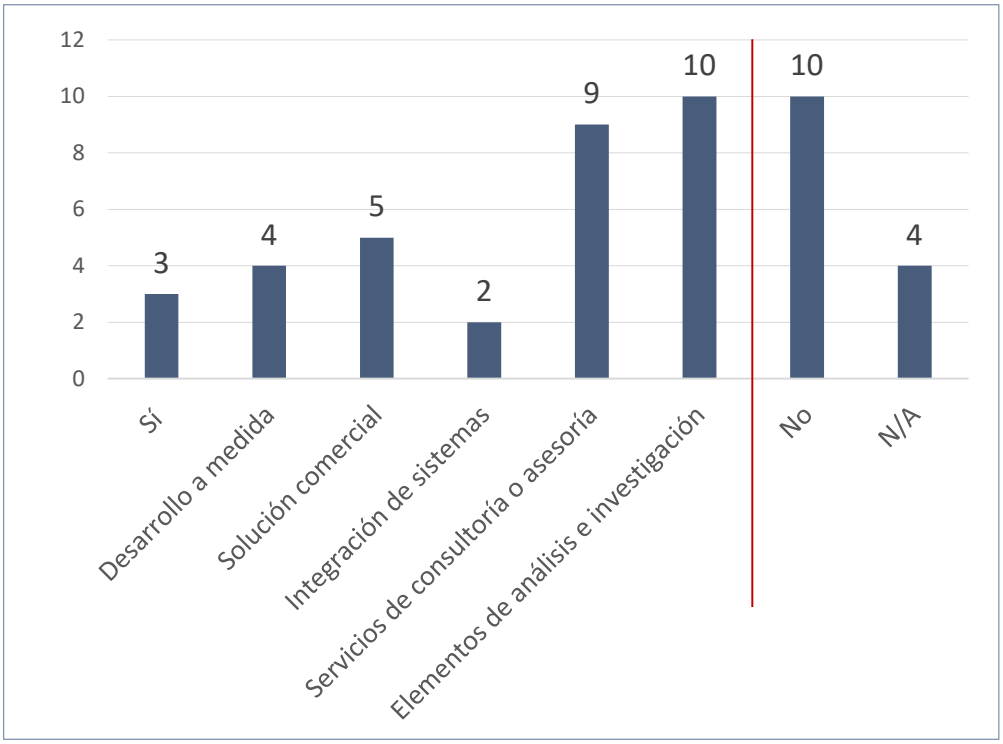


Figura 90. P45: Datos Movimiento lateral

La representación gráfica de los datos positivos se muestra en la siguiente figura:

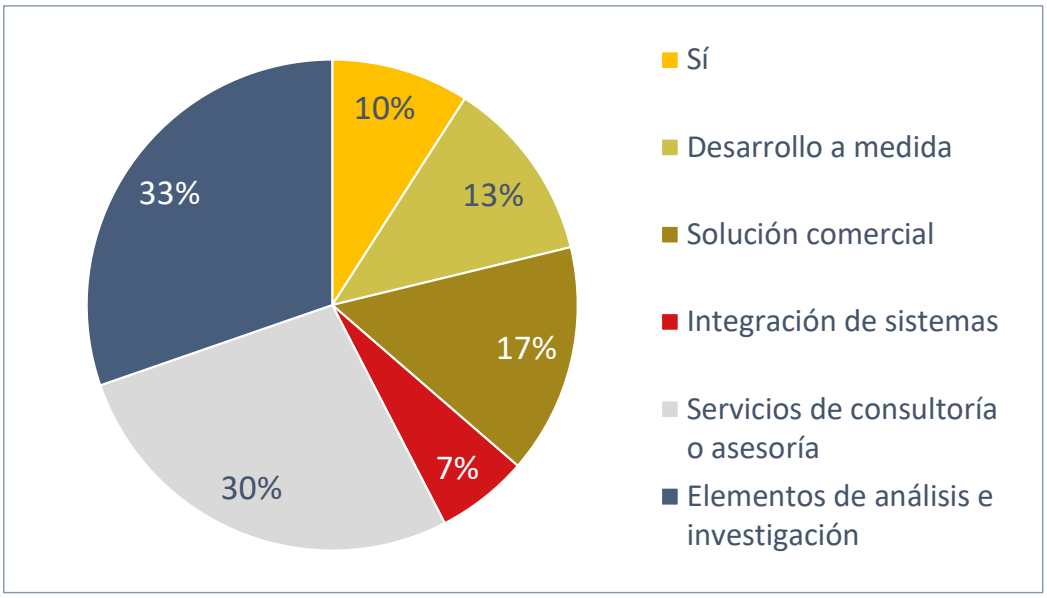


Figura 91. P45: Gráfico. Movimiento lateral

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:

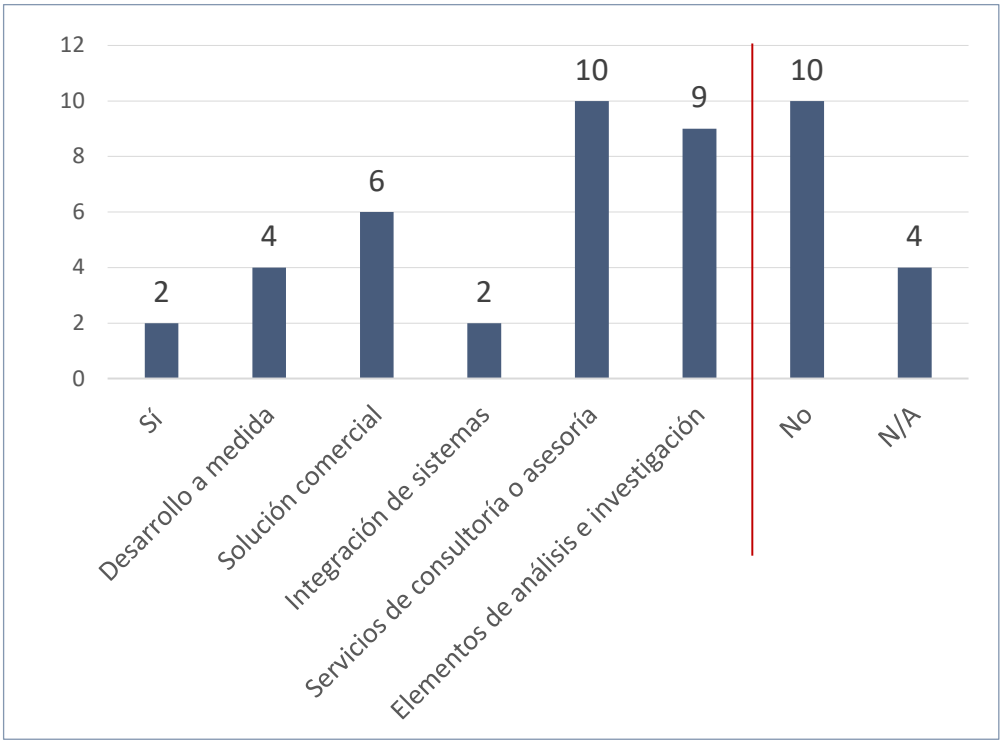


Figura 92. P46: Datos Recogida

La representación gráfica de los datos positivos se muestra en la siguiente figura:

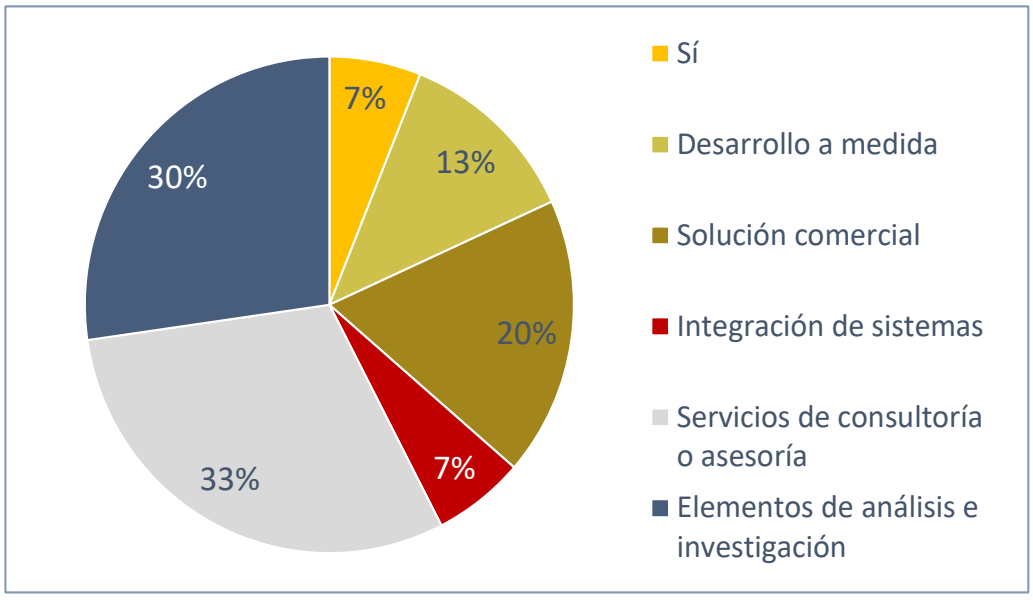


Figura 93. P46: Gráfico. Recogida

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:

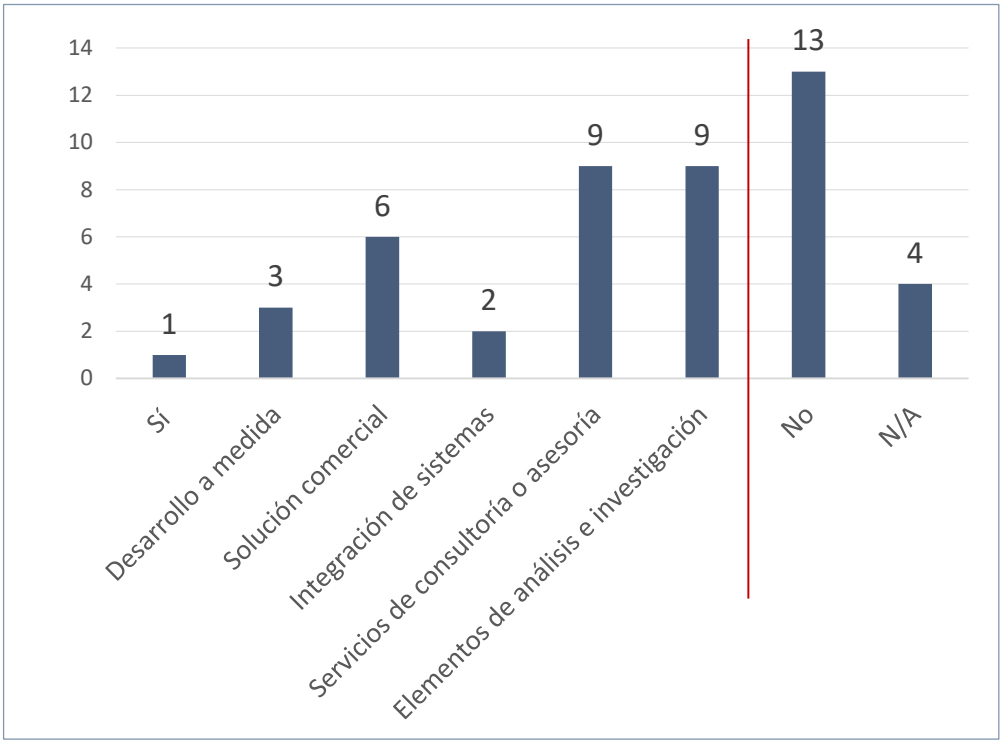


Figura 94. P47: Datos Mando y control

La representación gráfica de los datos positivos se muestra en la siguiente figura:

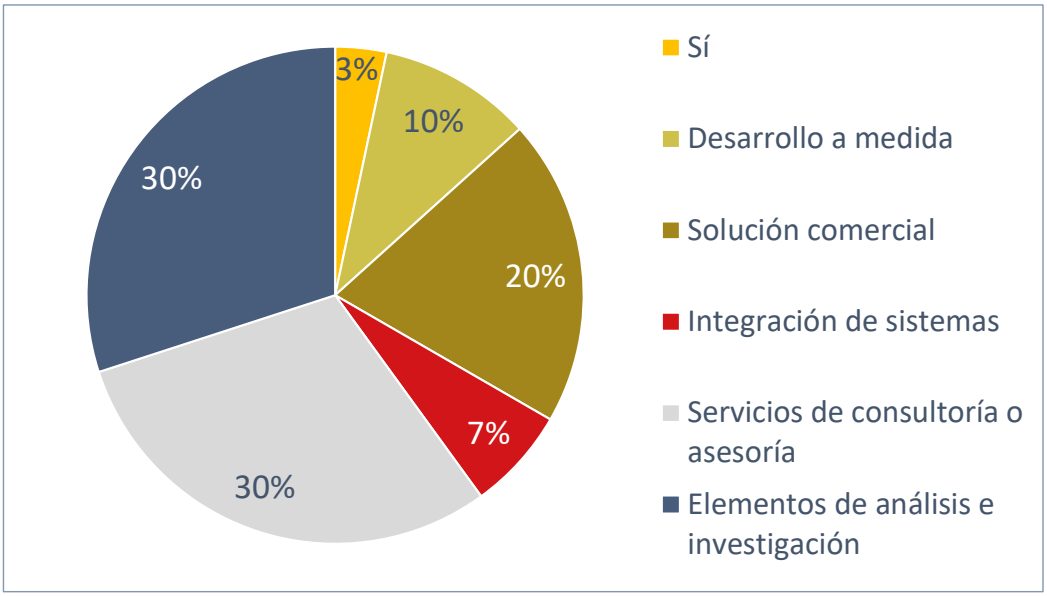


Figura 95. P47: Gráfico. Mando y control

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:

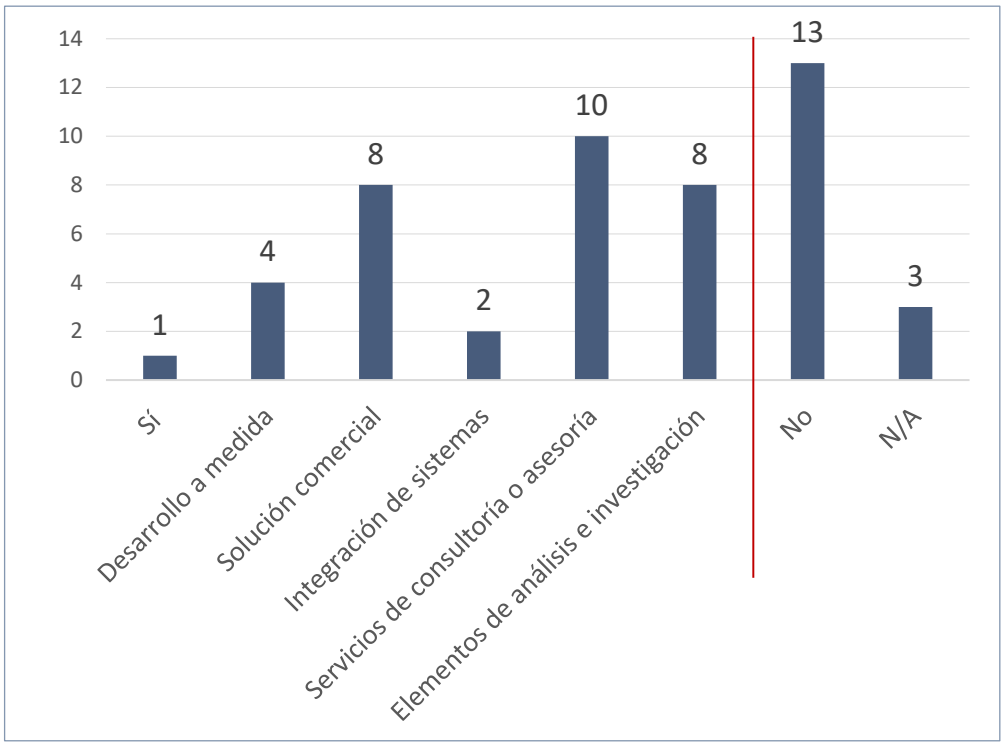


Figura 96. P48: Datos Exfiltración

La representación gráfica de los datos positivos se muestra en la siguiente figura:

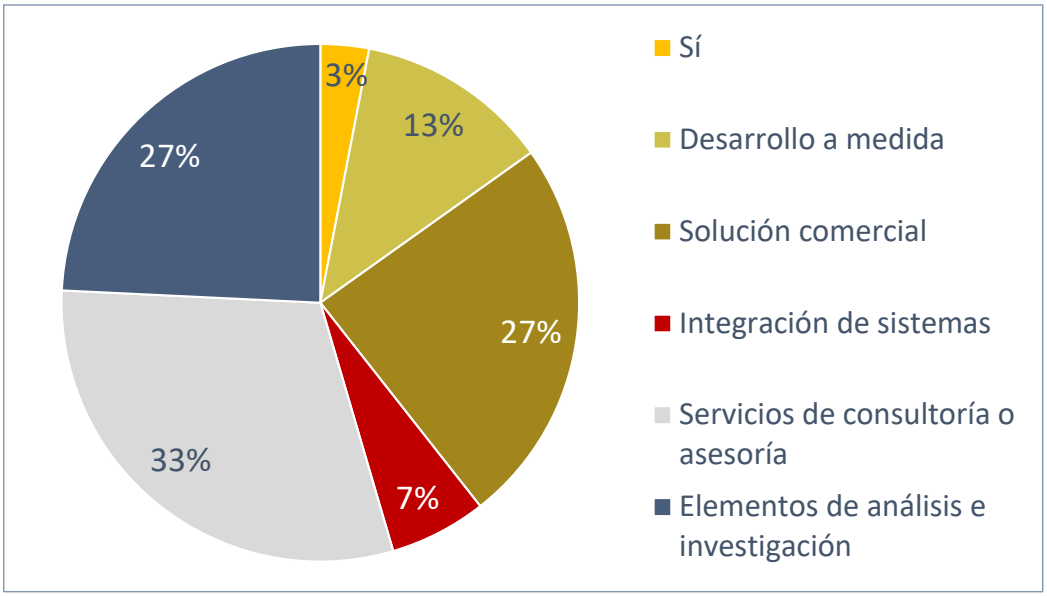


Figura 98. P48: Gráfico. Exfiltración

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:

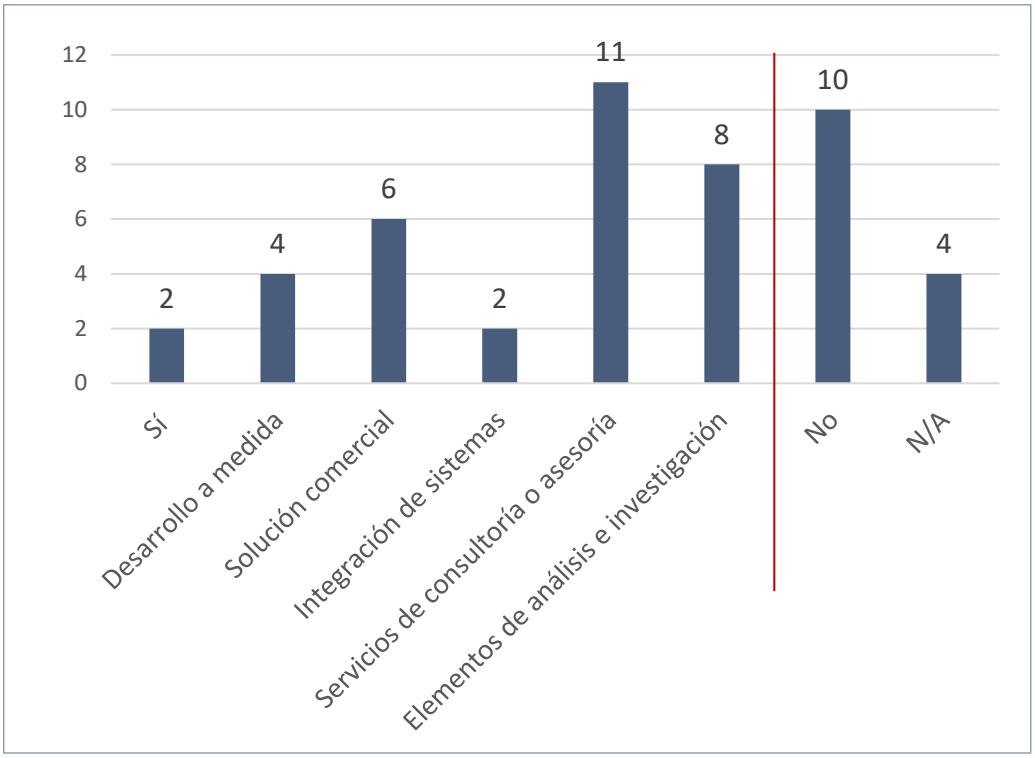


Figura 97. P49: Datos Impaqcto

La representación gráfica de los datos positivos se muestra en la siguiente figura:

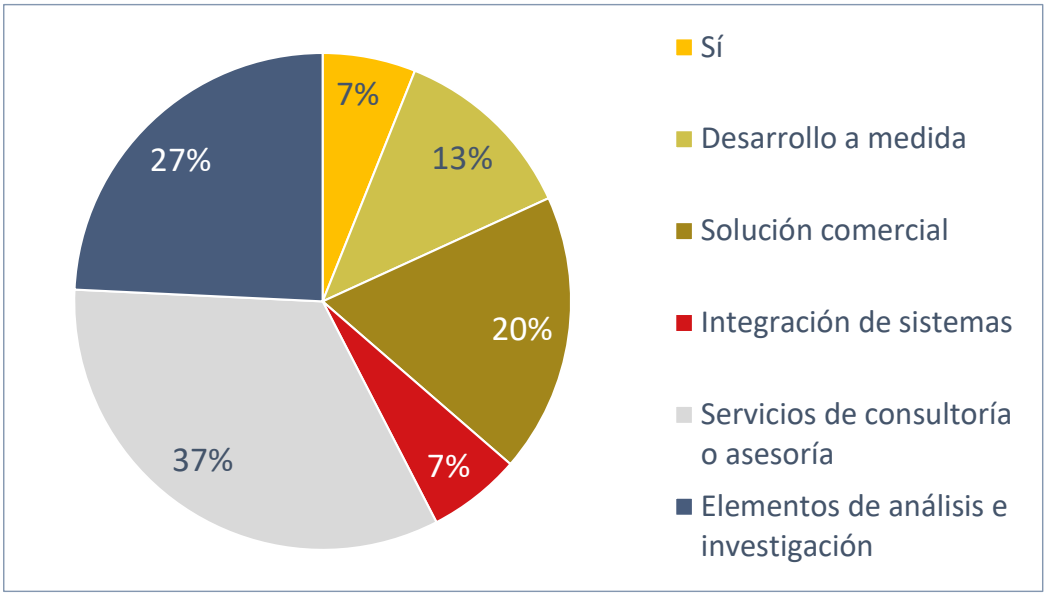


Figura 98. P49: Gráfico. Impacto

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:

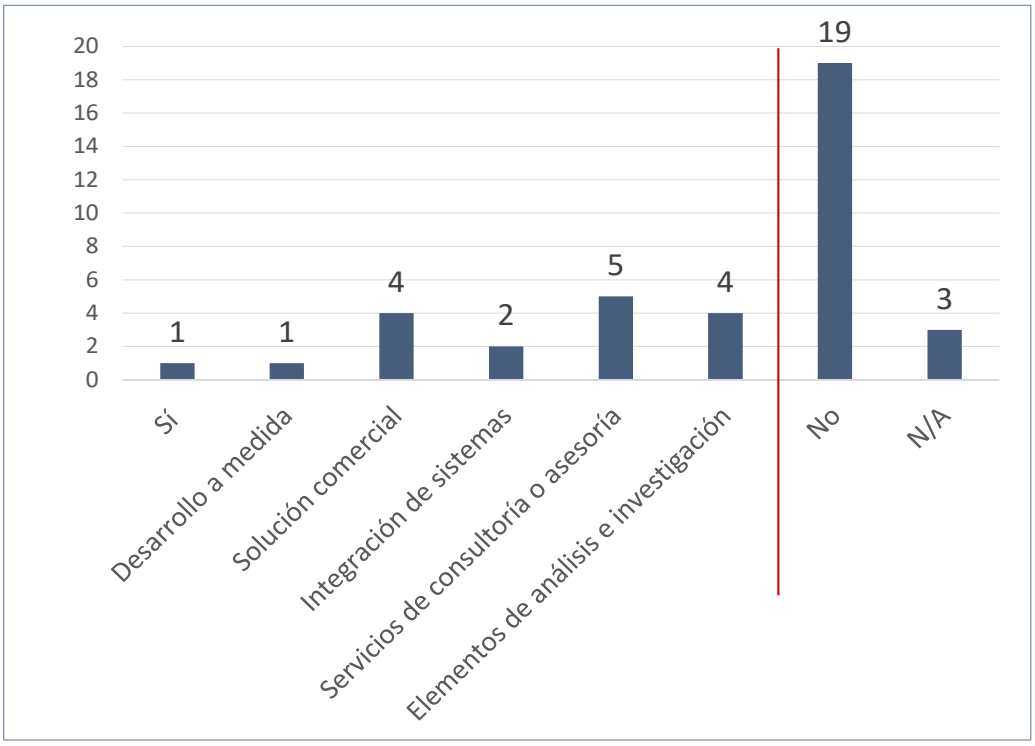


Figura 99. P50: Datos Efectos en la red (móviles)

La representación gráfica de los datos positivos se muestra en la siguiente figura:

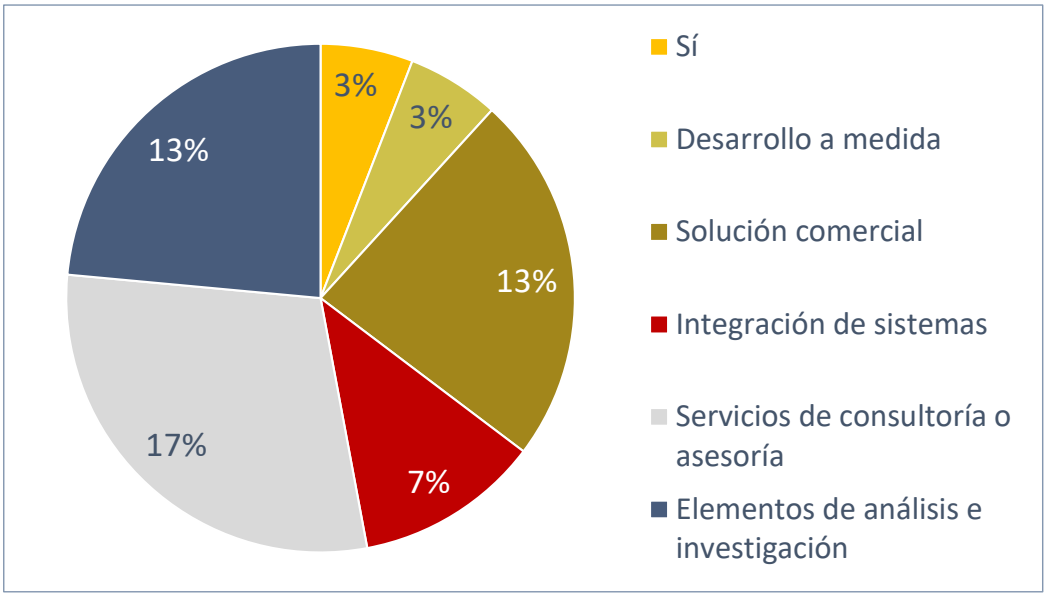


Figura 100. P50: Gráfico. Efectos en la red (móviles)

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:

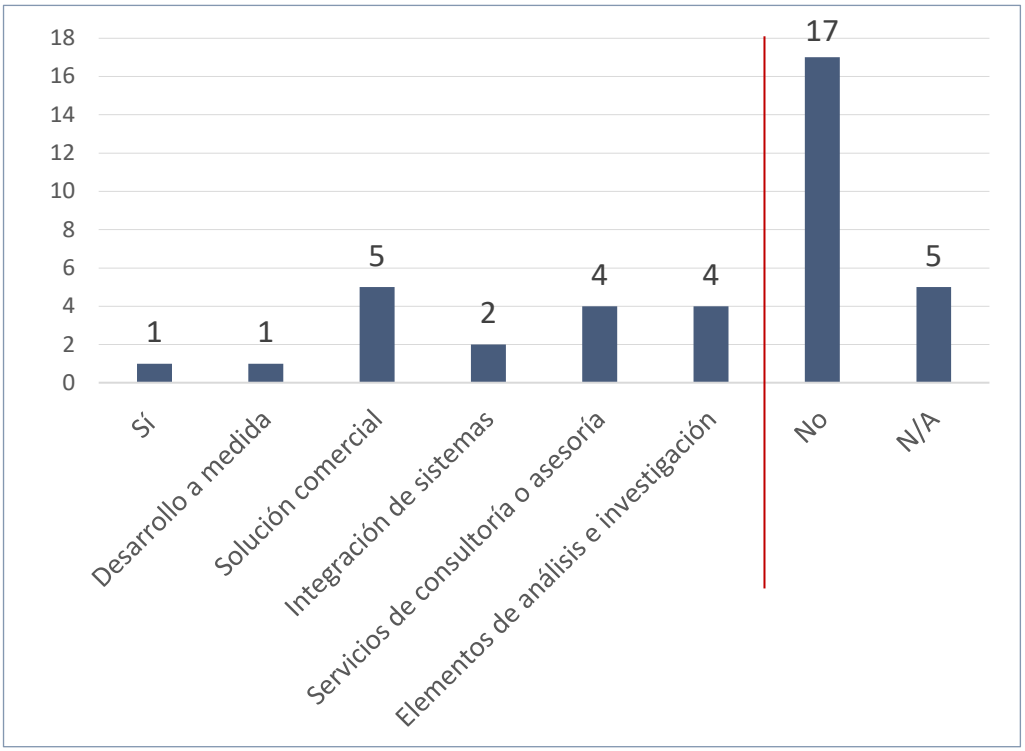


Figura 101. P51: Datos Efectos en los servicios remotos (móviles)

La representación gráfica de los datos positivos se muestra en la siguiente figura:

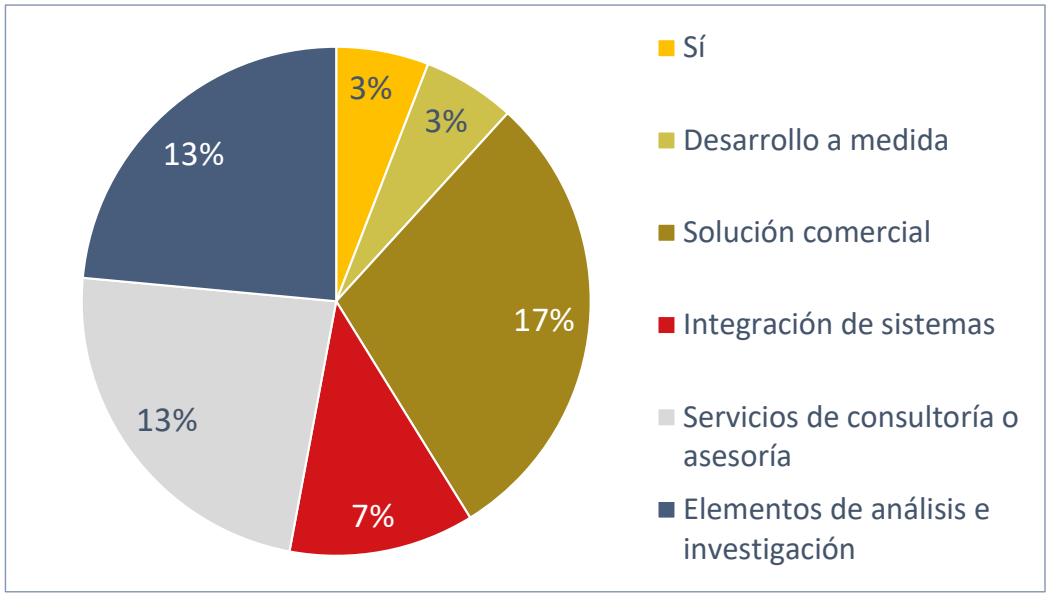


Figura 102. P51: Gráfico. Efectos en los servicios remotos (móviles)

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:

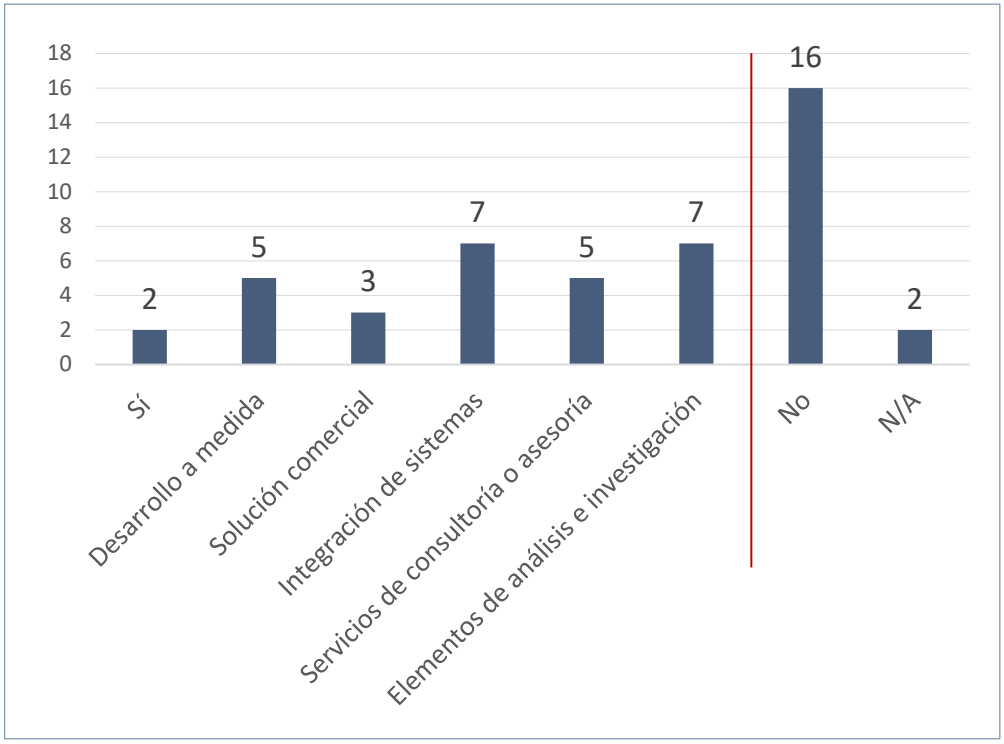


Figura 103. P52: Datos Cyberrange

La representación gráfica de los datos positivos se muestra en la siguiente figura:

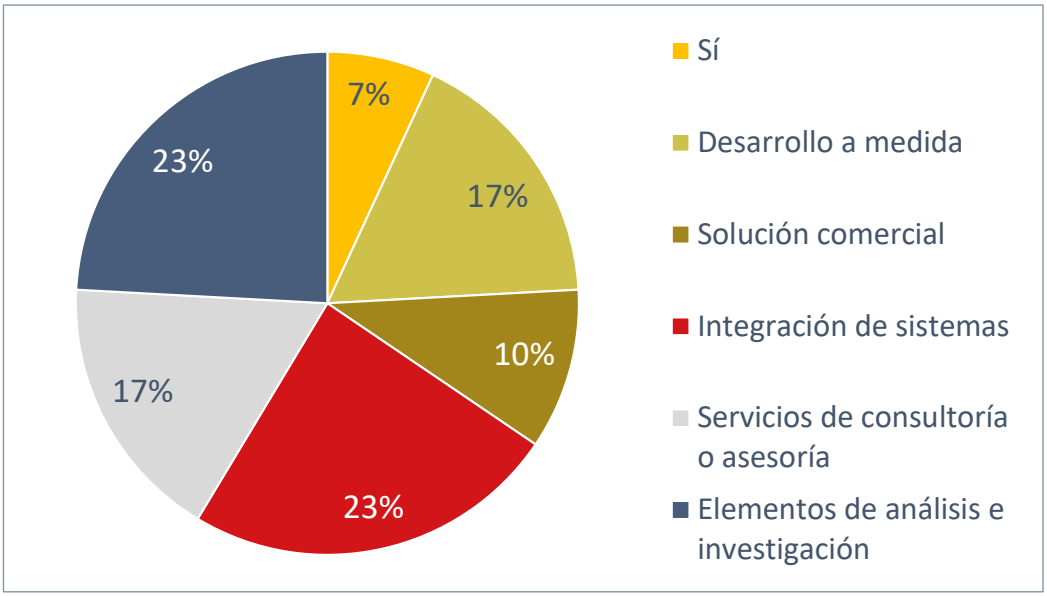


Figura 104. P52: Gráfico. Cyberrange

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:

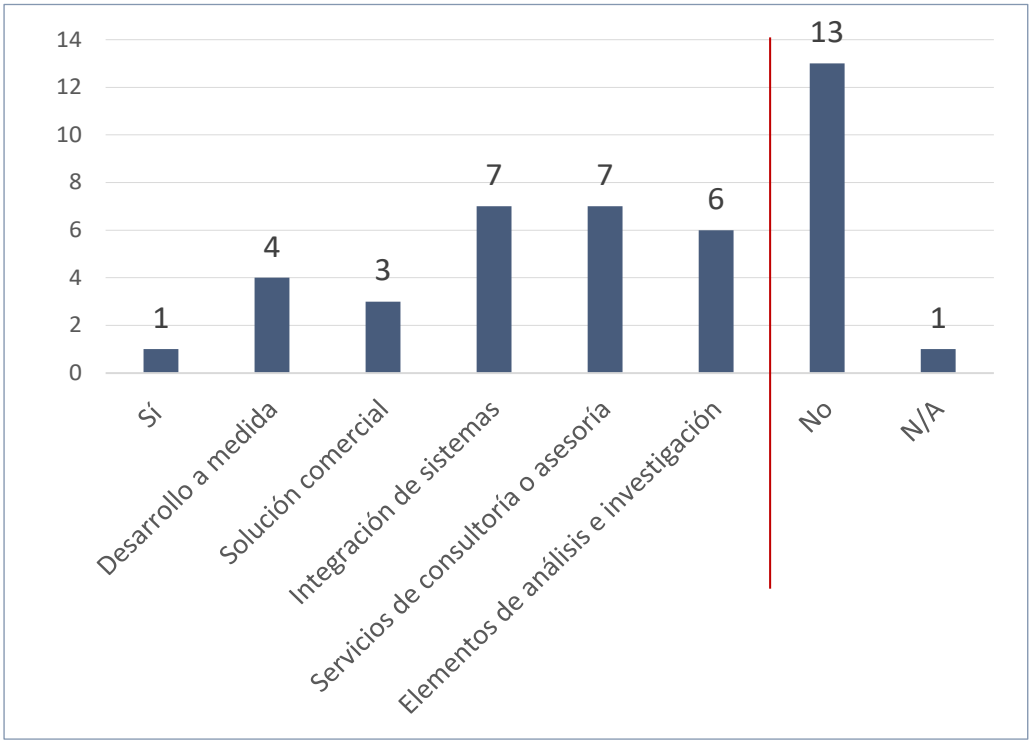


Figura 105. P53: Datos Laboratorio de análisis digital

[22] Como por ejemplo Proofpoint Awareness con Mellivora

La representación gráfica de los datos positivos se muestra en la siguiente figura:

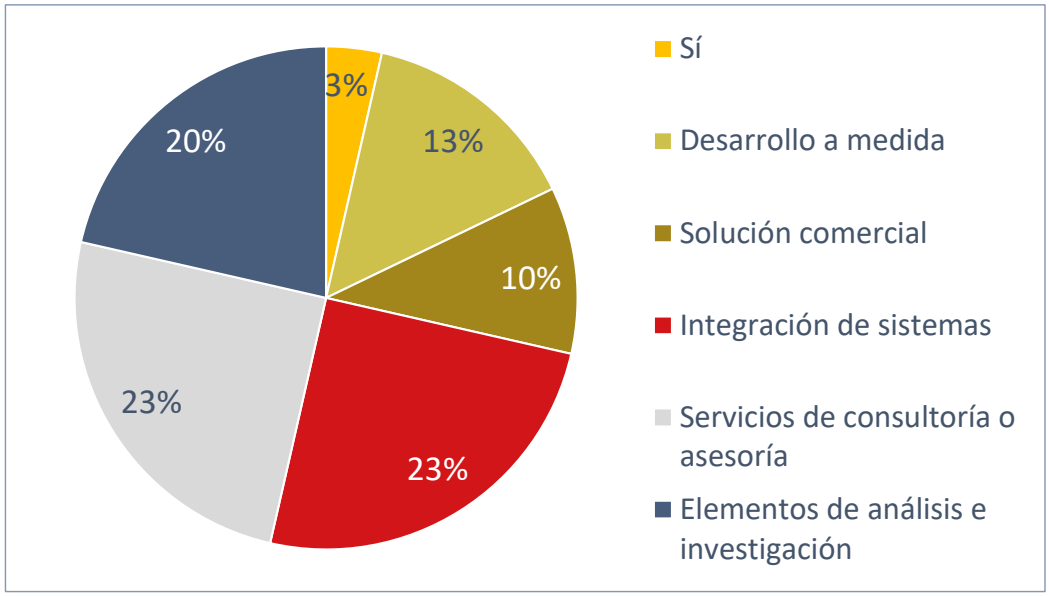


Figura 106. P53: Gráfico. Laboratorio de análisis digital

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:

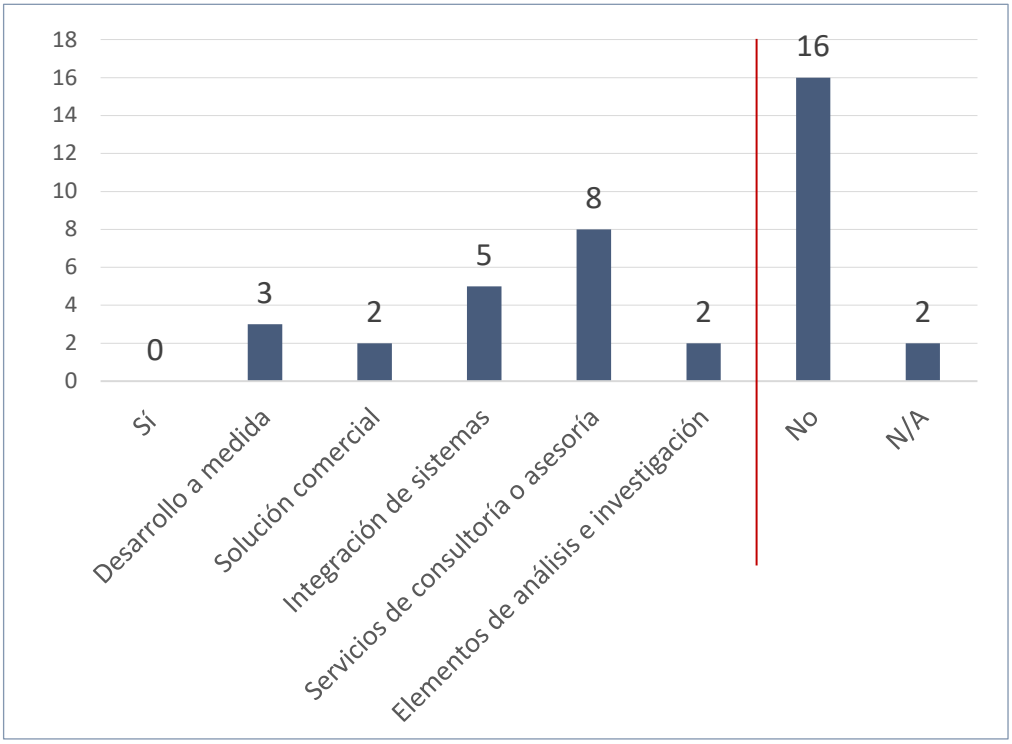


Figura 107. P54: Datos Despliegue automático de sistemas seguros

La representación gráfica de los datos positivos se muestra en la siguiente figura:

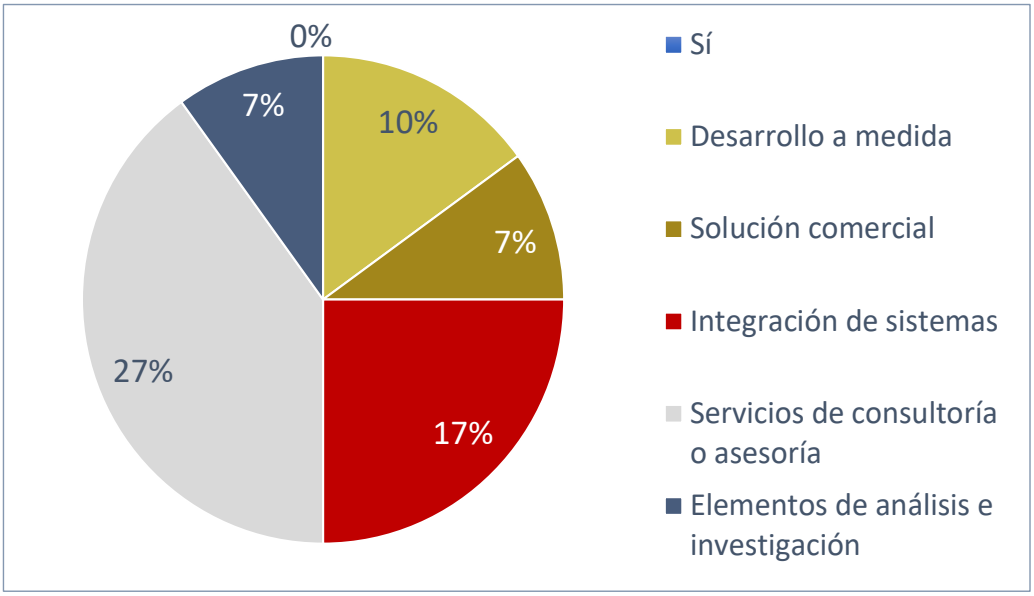


Figura 108. P54: Gráfico. Despliegue automático de sistemas seguros

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:

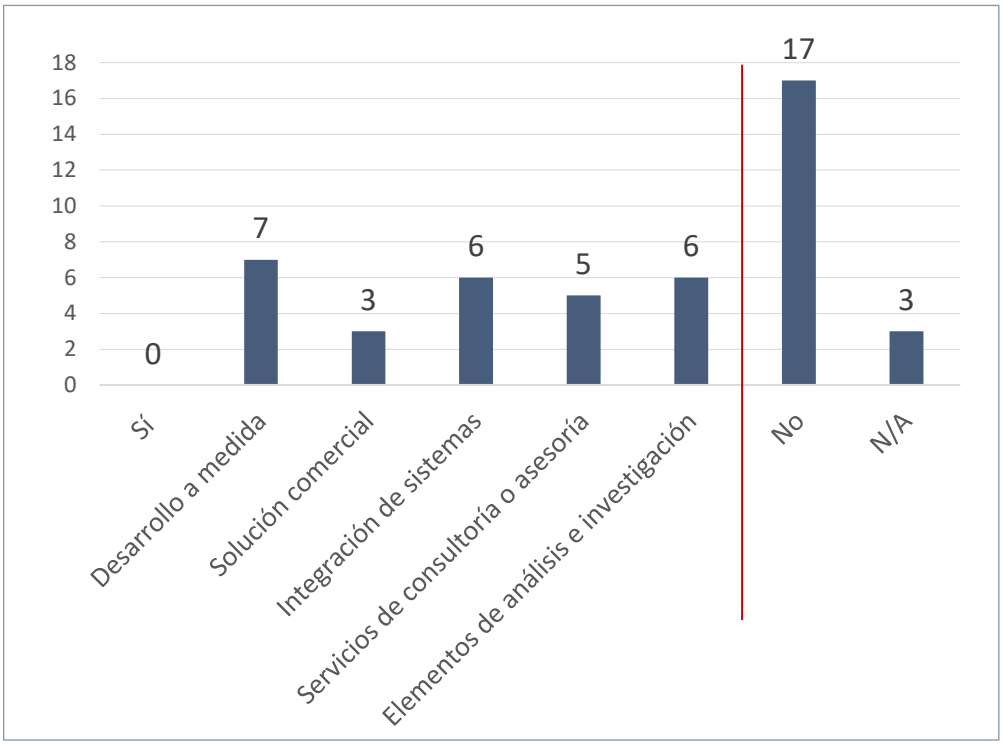


Figura 109. P55: Datos Combat cloud

La representación gráfica de los datos positivos se muestra en la siguiente figura:

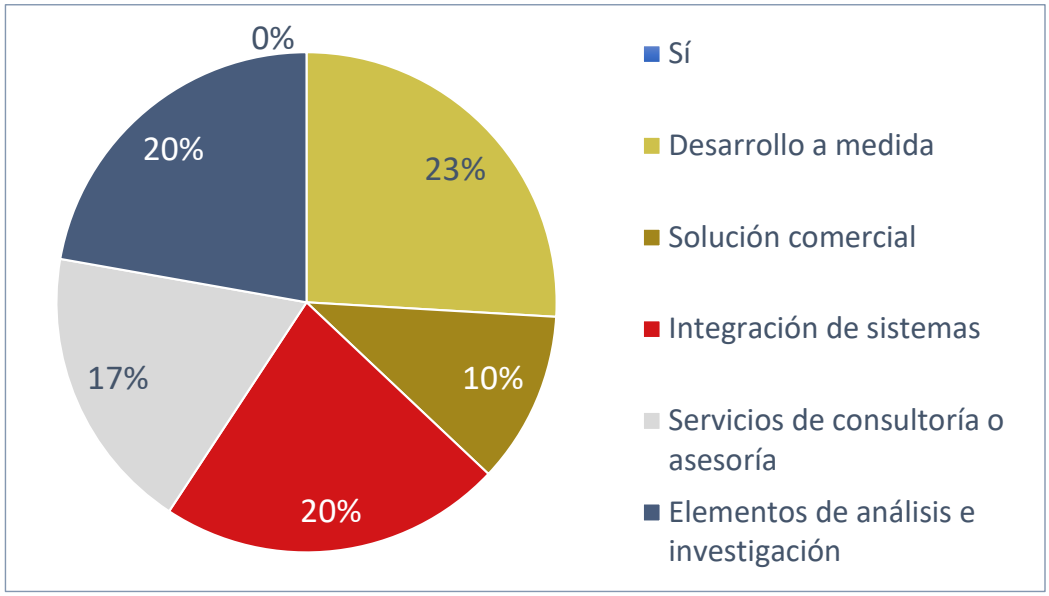


Figura 110. P55: Gráfico. Combat cloud

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:

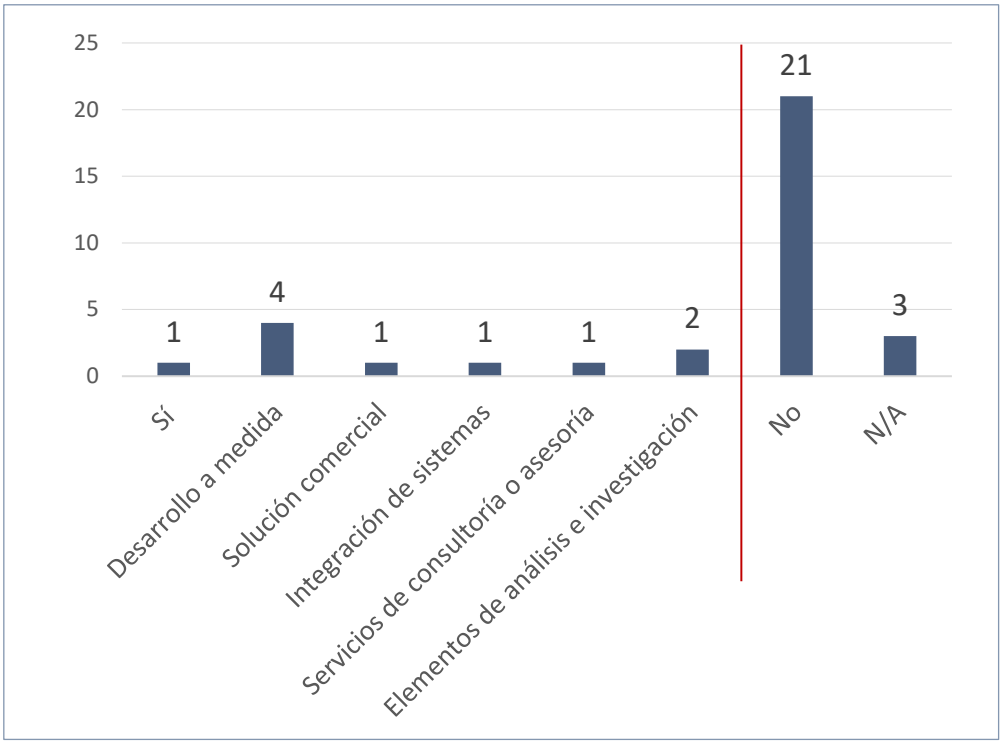


Figura 111. P56: Datos Producción de malware específico

[25] Como Fortinet, Proofpoint o Netskope.

La representación gráfica de los datos positivos se muestra en la siguiente figura:

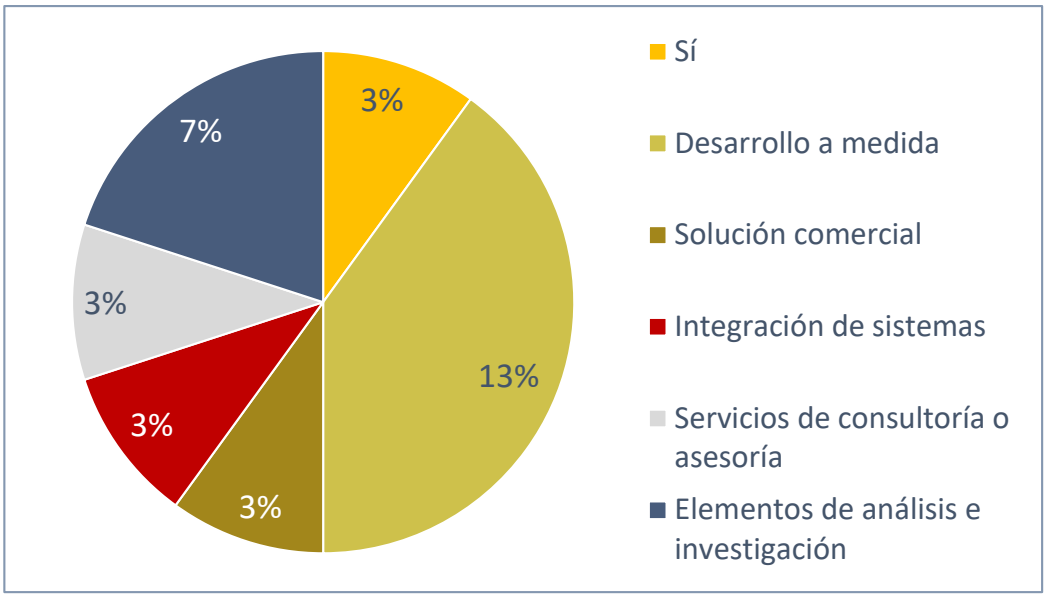


Figura 112. P56: Gráfico. Producción de malware específico

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:

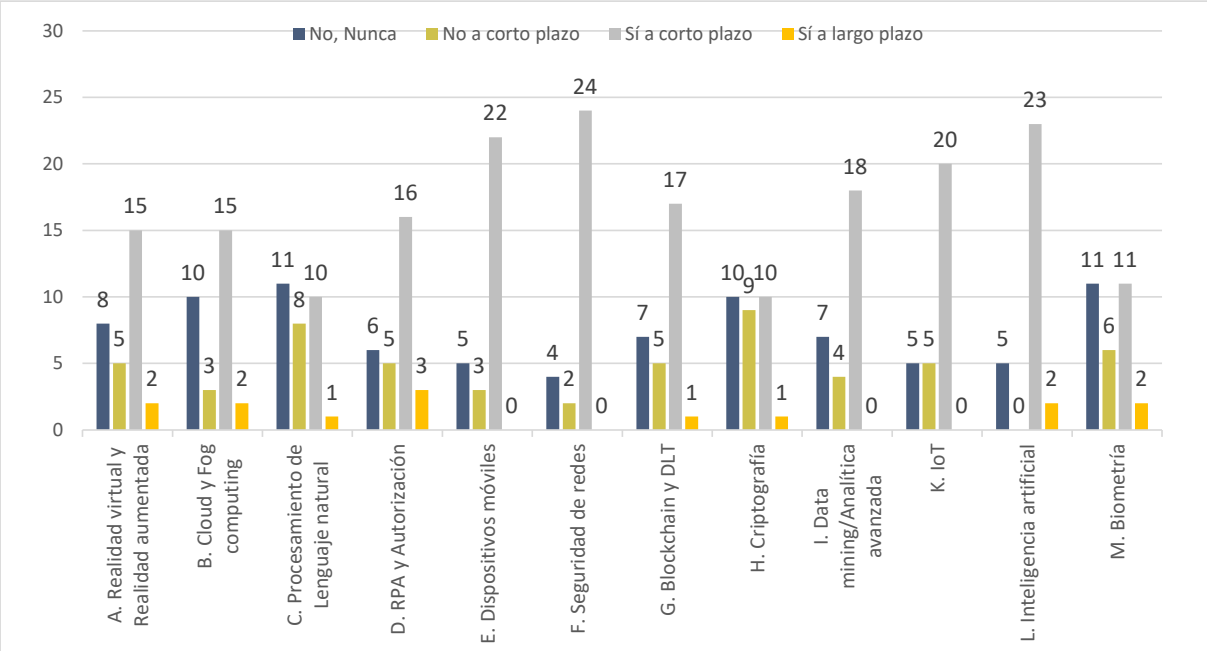


Figura 113. P57: Datos tecnologías: Trabajos y desarrollos por la organización

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:

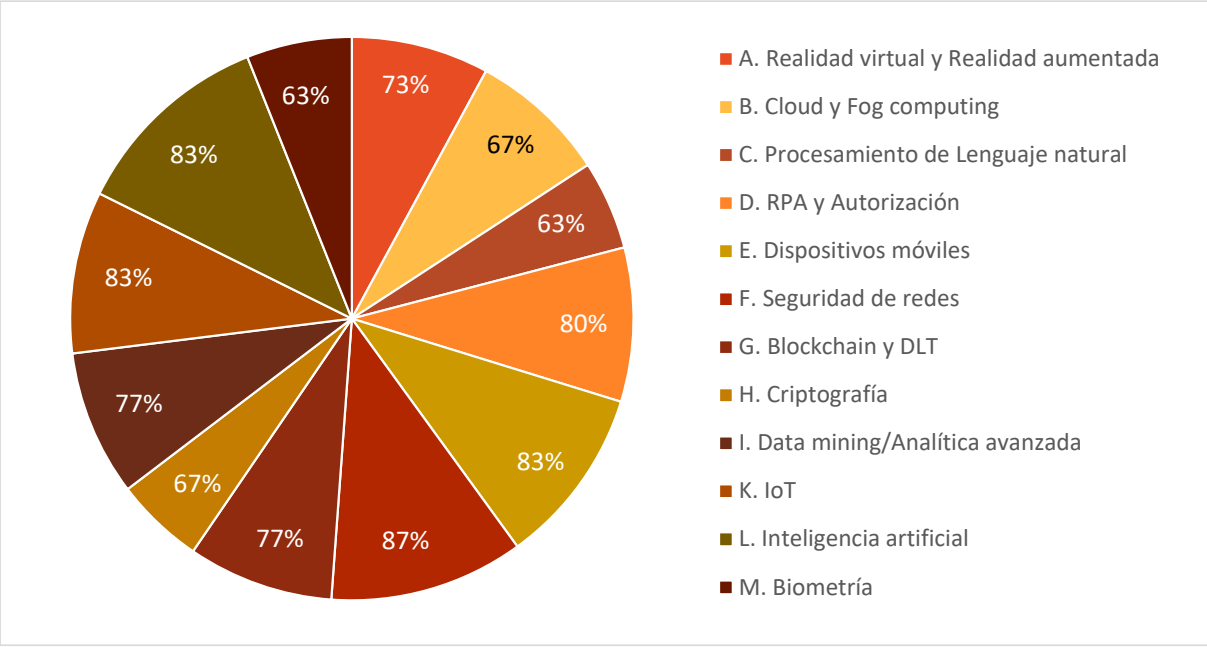


Figura 114. P57: Gráfico. Tecnologías: Trabajos y desarrollos por la organización

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 natural**, 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:

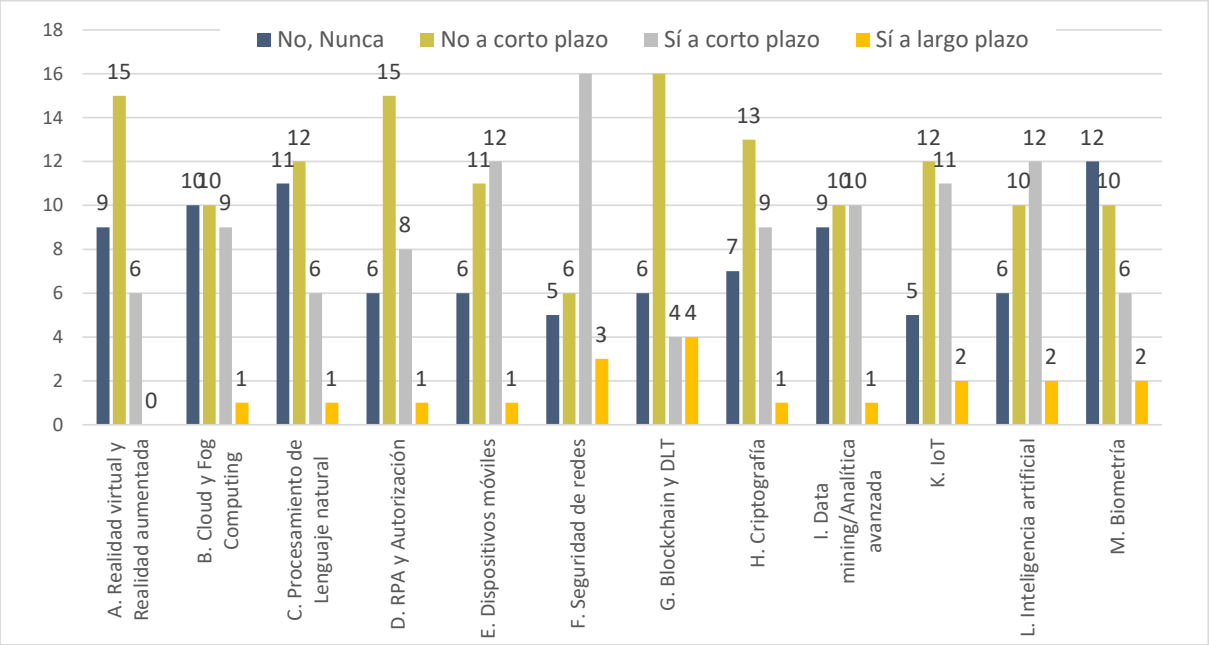


Figura 115. P58: Datos Tecnologías: Aplicación de las tecnologías a la ciberdefensa

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:

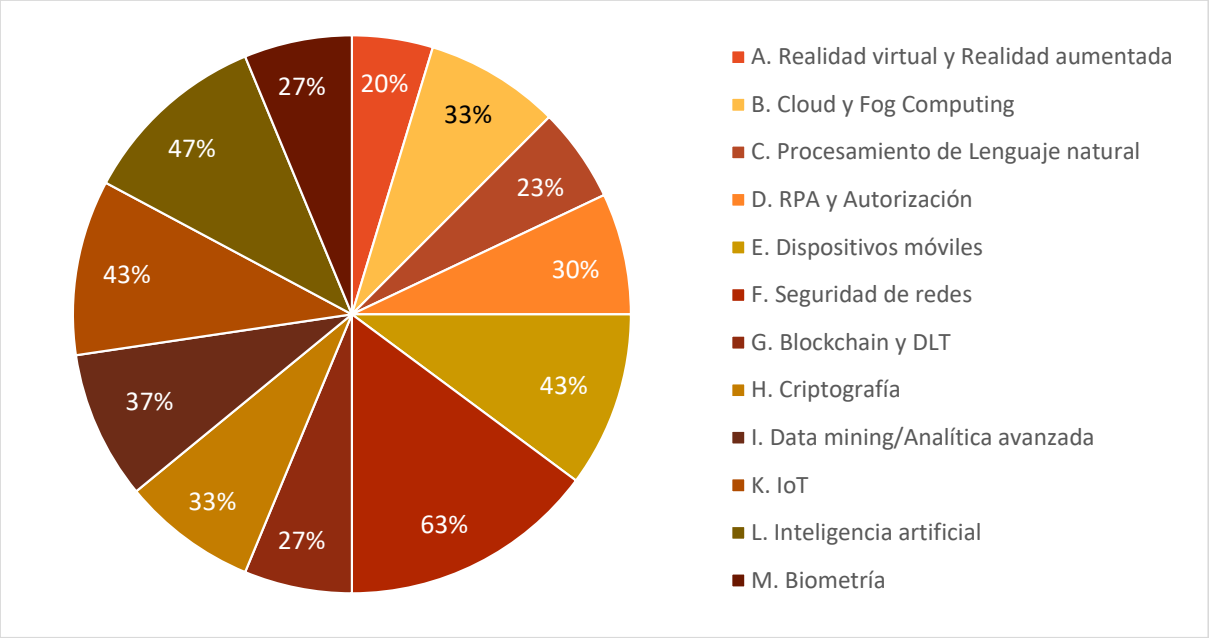


Figura 116. P58: Datos Tecnologías: Aplicación de las tecnologías a la ciberdefensa (corto o largo plazo)

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:

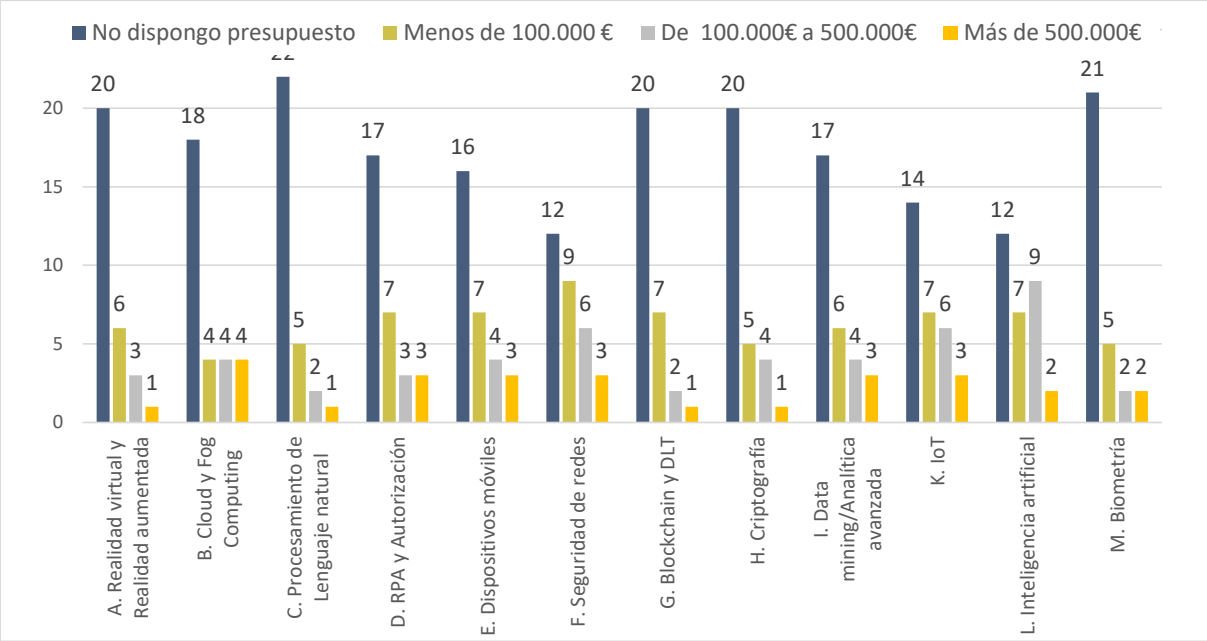


Figura 117. P59: Datos I+D+I: Inversiones en I+D+i en las diferentes tecnologías

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:

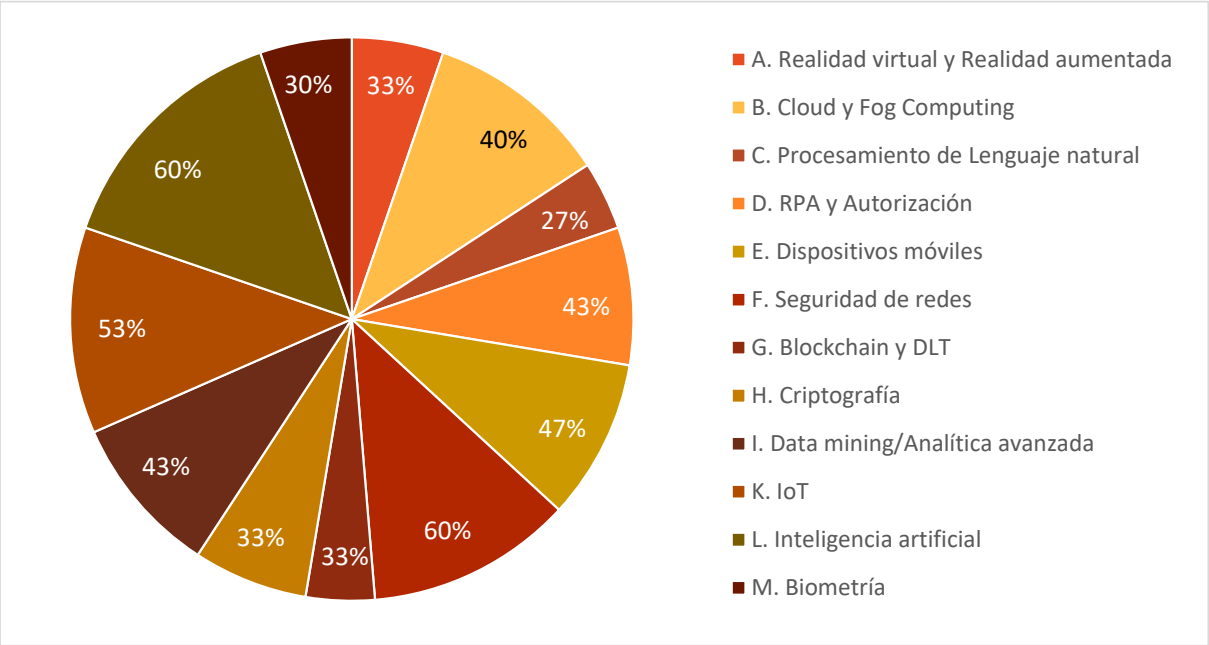


Figura 118. P59: Gráfico. I+D+I: Inversiones en I+D+i en las diferentes tecnologías (Disponen de inversión)

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:

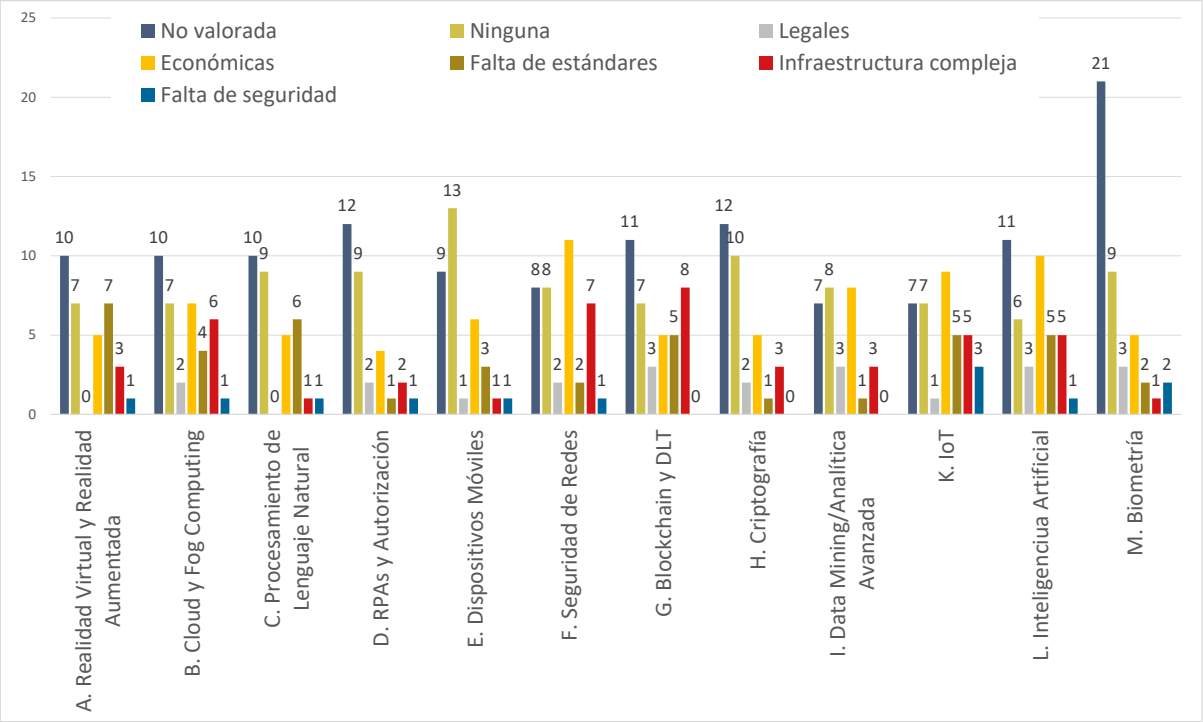


Figura 119. P60: Datos barreras tecnológicas

La representación gráfica de los datos de las barreras tecnológicas encontradas en el conjunto de tecnologías tratadas se muestra en la siguiente figura:

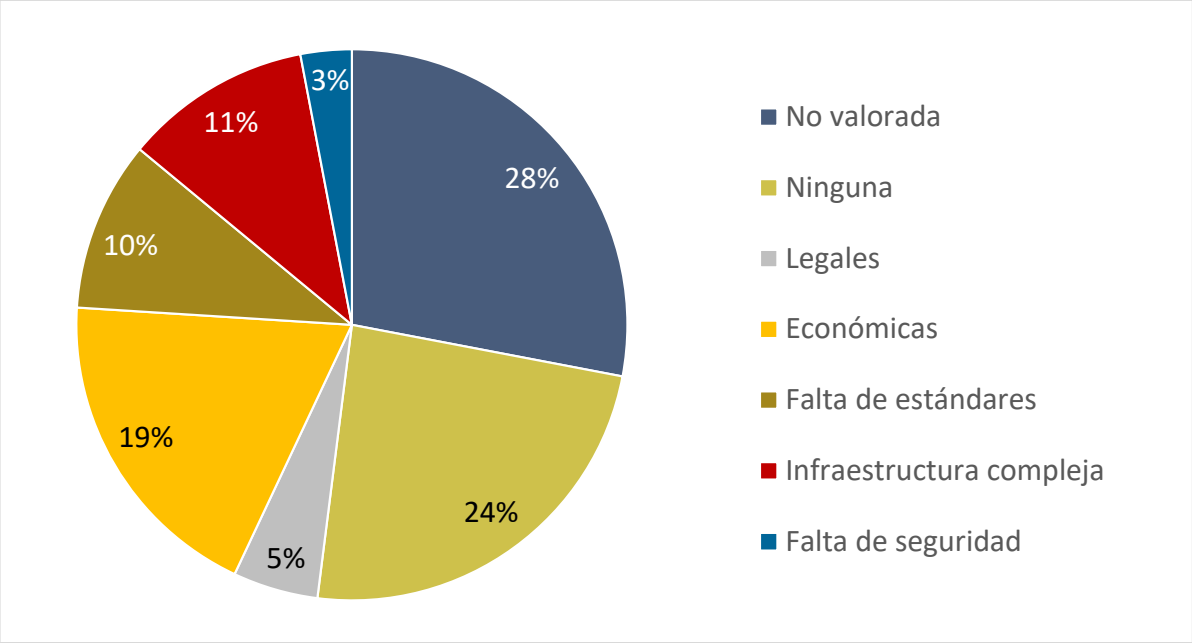


Figura 120. P60: Gráfico. Barreras tecnológicas

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:

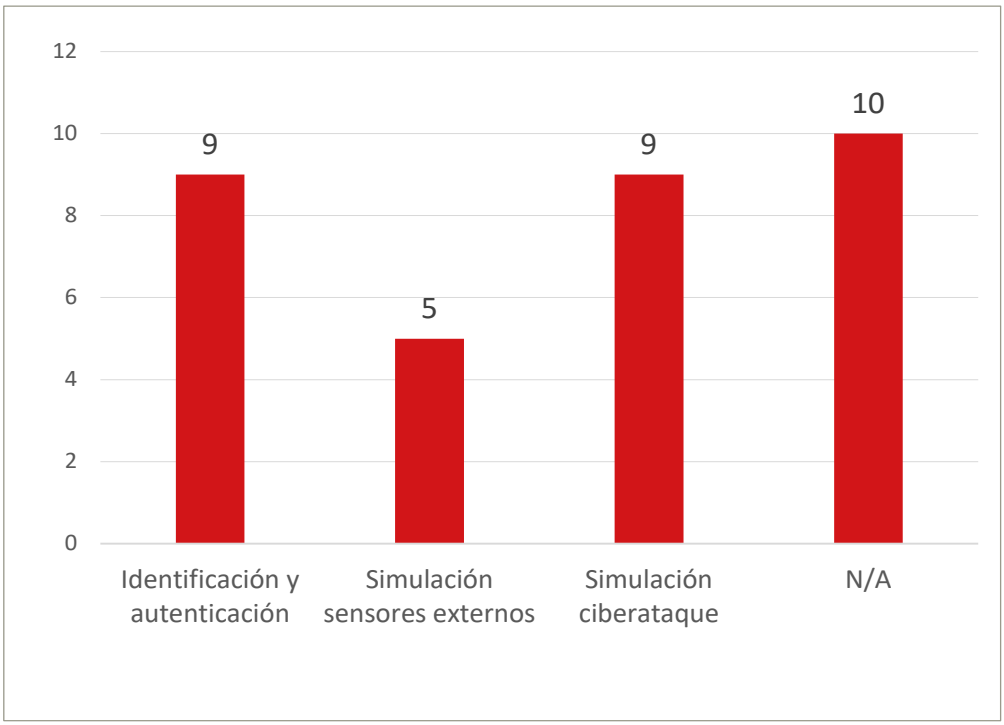


Figura 121. P61: Datos Actividades de la realidad virtual o la realidad aumentada más relevantes para su organización

La representación gráfica de estos datos se muestra en la siguiente figura:

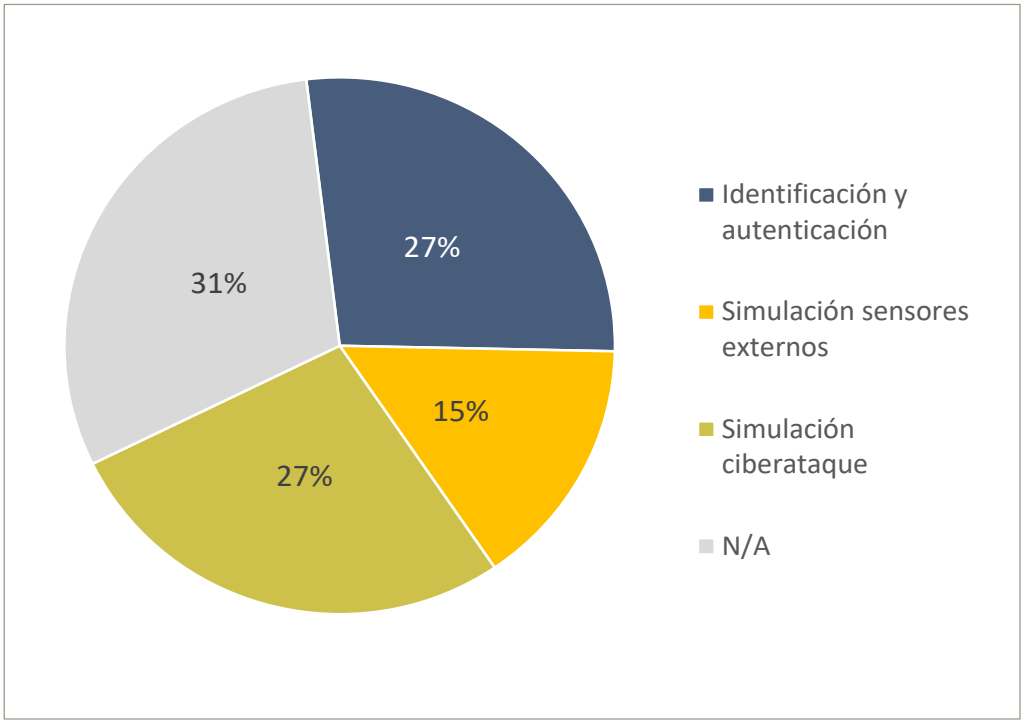


Figura 122. P61: Gráfico. Actividades de la realidad virtual o la realidad aumentada más relevantes para su organización

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:

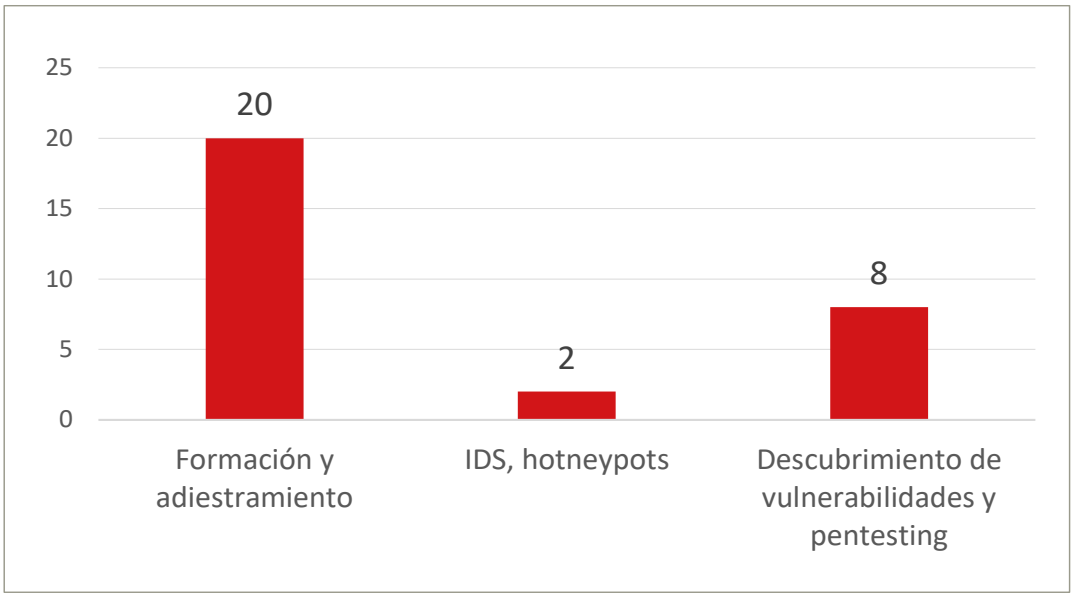


Figura 123. P62: Datos actividades de la realidad virtual o la realidad aumentada más relevantes para ciberdefensa

La representación gráfica de estos datos se muestra en la siguiente figura:

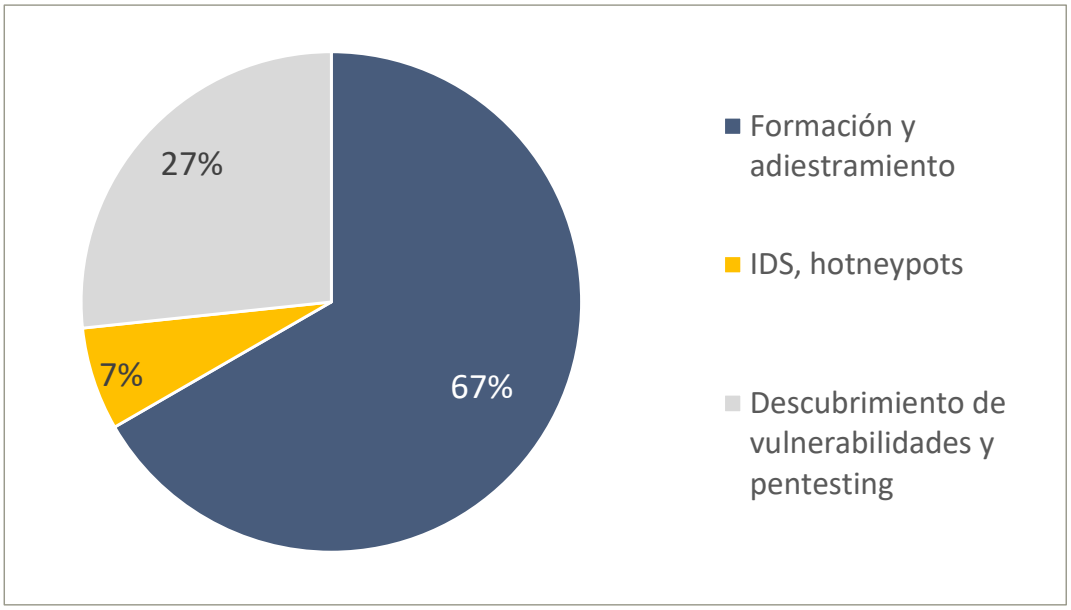


Figura 124. P62: Gráfico. Actividades de la realidad virtual o la realidad aumentada más relevantes para ciberdefensa

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:

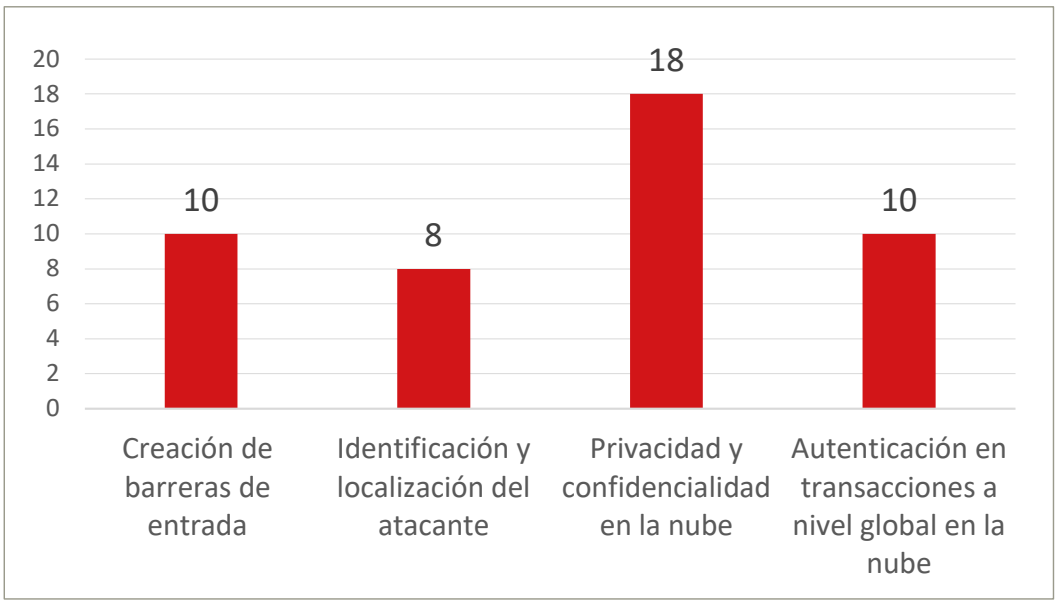


Figura 125. P63: Datos actividades de cloud y fog computing más relevantes para ciberdefensa

La representación gráfica de estos datos se muestra en la siguiente figura:

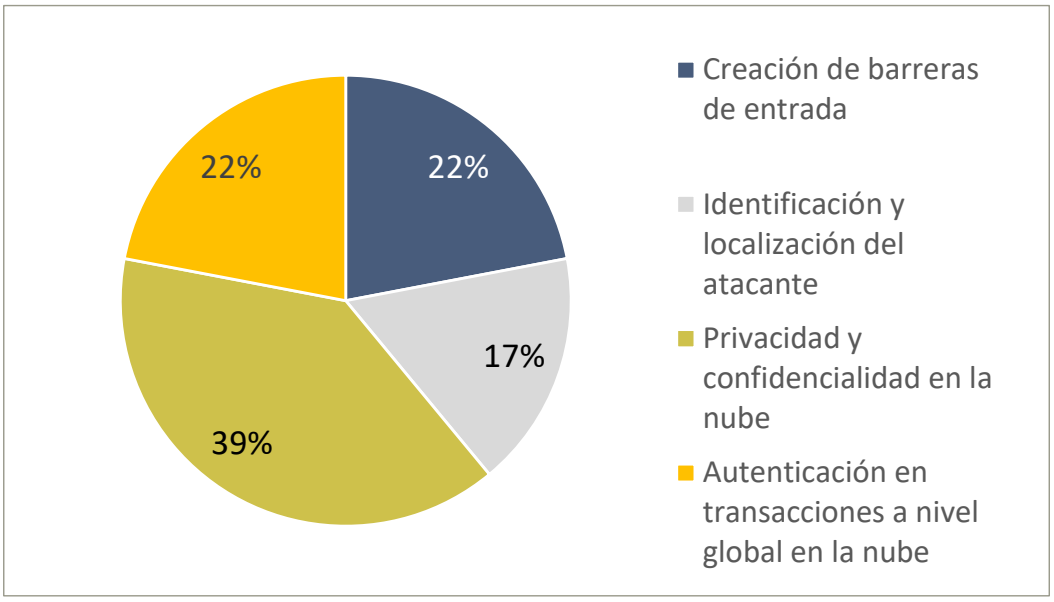


Figura 126. P63: Gráfico. Actividades de cloud y fog computing más relevantes para ciberdefensa

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:

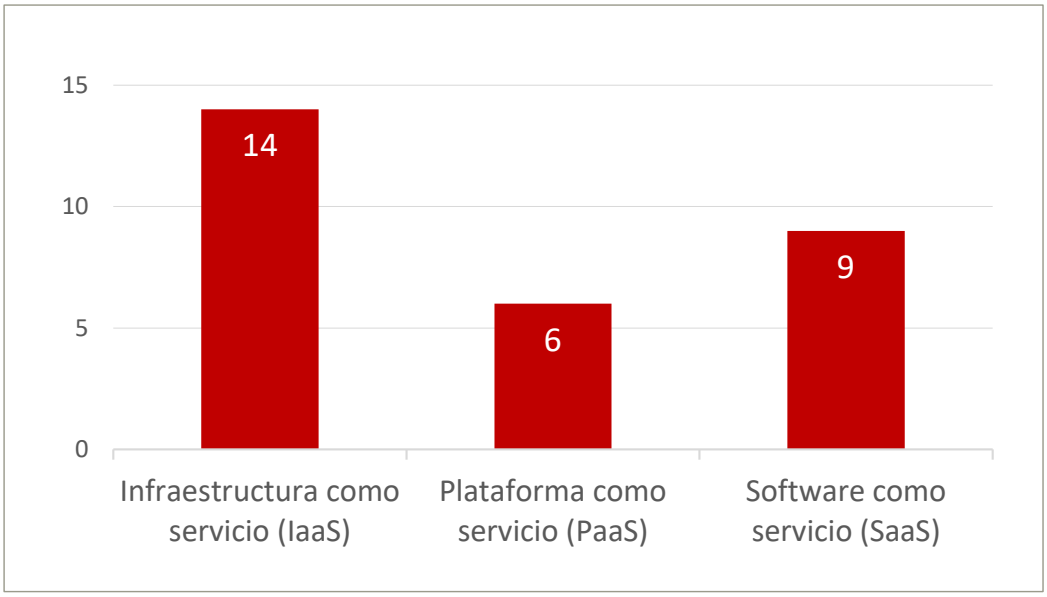


Figura 127, P64: Datos modalidad de cloud y fog computing más utilizado para ciberdefensa

La representación gráfica de estos datos se muestra en la siguiente figura:

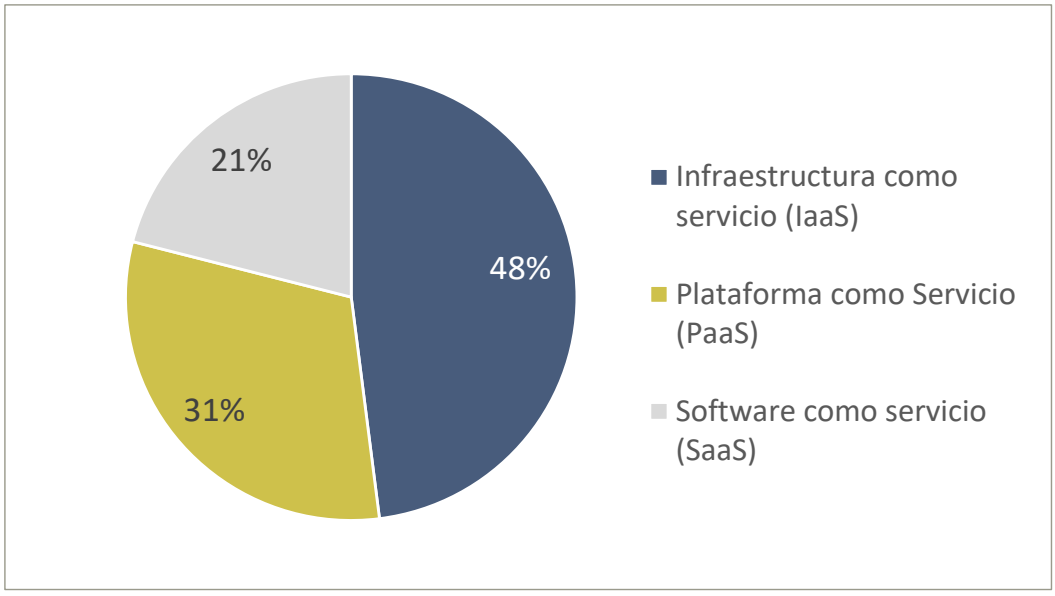


Figura 128. P64: Gráfico. modalidad de cloud y fog computing más utilizado para ciberdefensa

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:

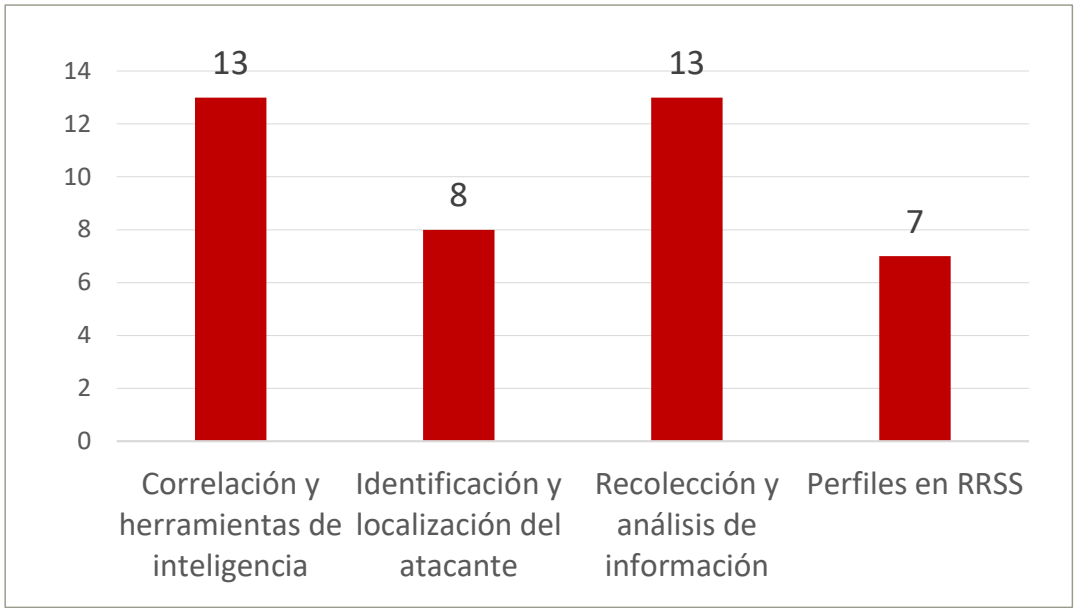


Figura 129. P65: Datos actividades de procesamiento de lenguaje natural más relevantes para ciberdefensa

La representación gráfica de estos datos se muestra en la siguiente figura:

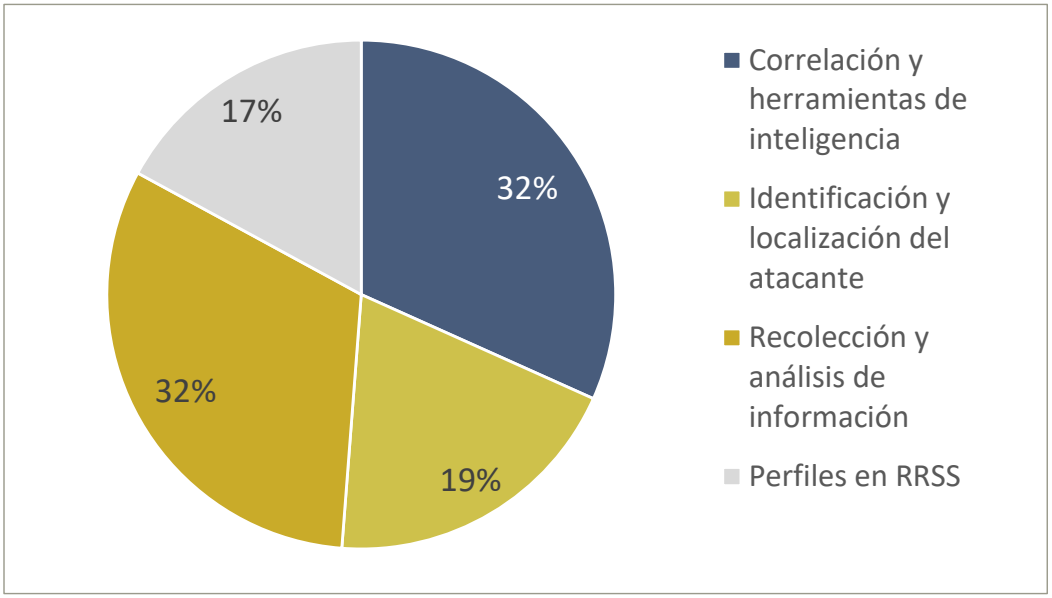


Figura 130. P65: Gráfico. Actividades de procesamiento de lenguaje natural más relevantes para ciberdefensa

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:

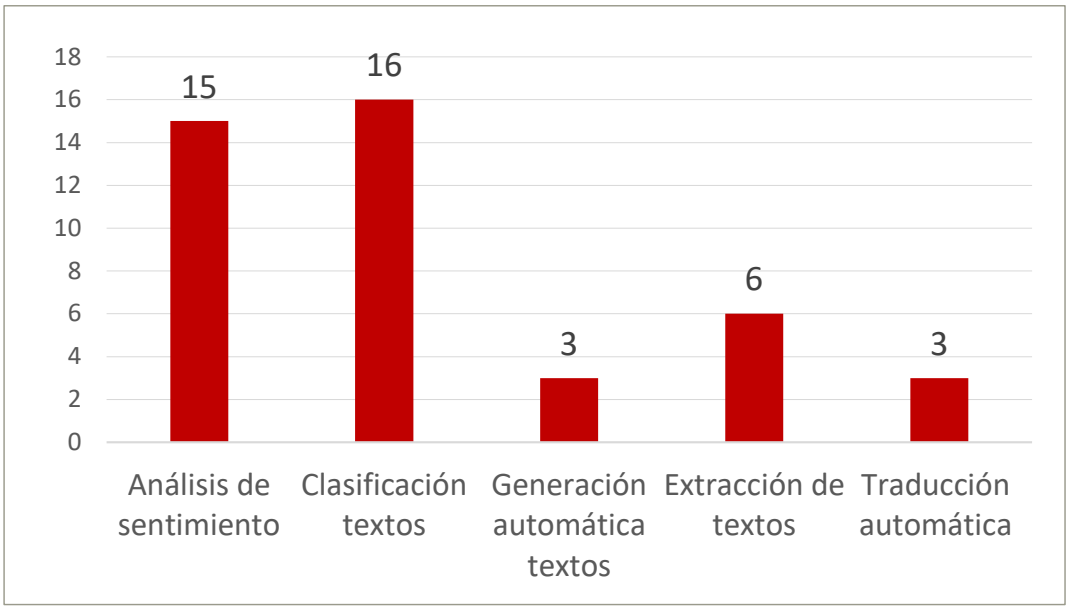


Figura 131- P66: Datos aplicaciones de procesamiento de lenguaje natural más relevantes para ciberdefensa

La representación gráfica de estos datos se muestra en la siguiente figura:

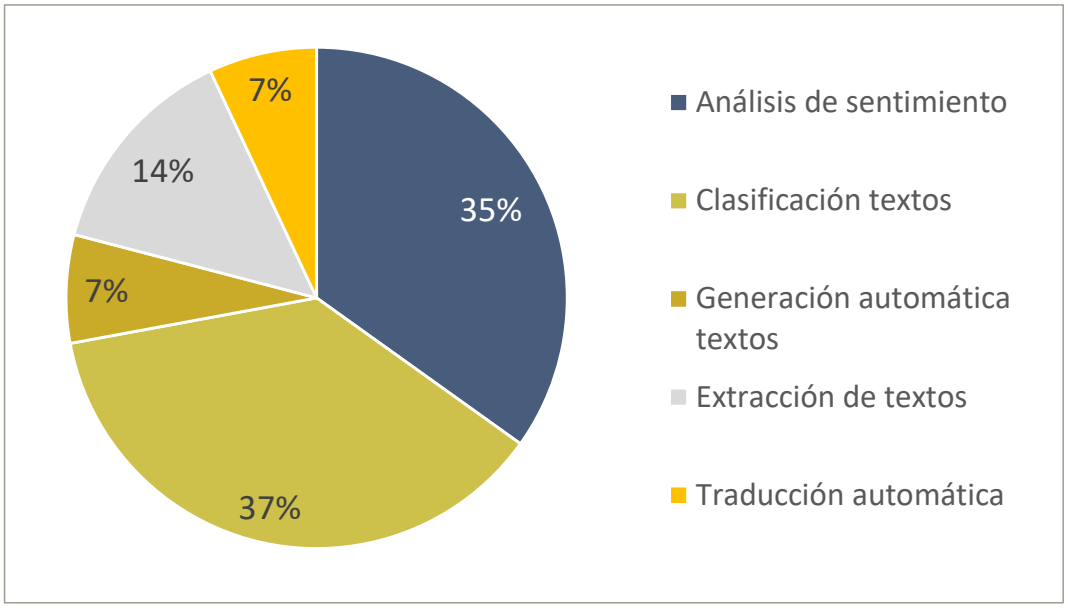


Figura 132- P66: Gráfico.Aplicaciones de procesamiento de lenguaje natural más relevantes para ciberdefensa

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:

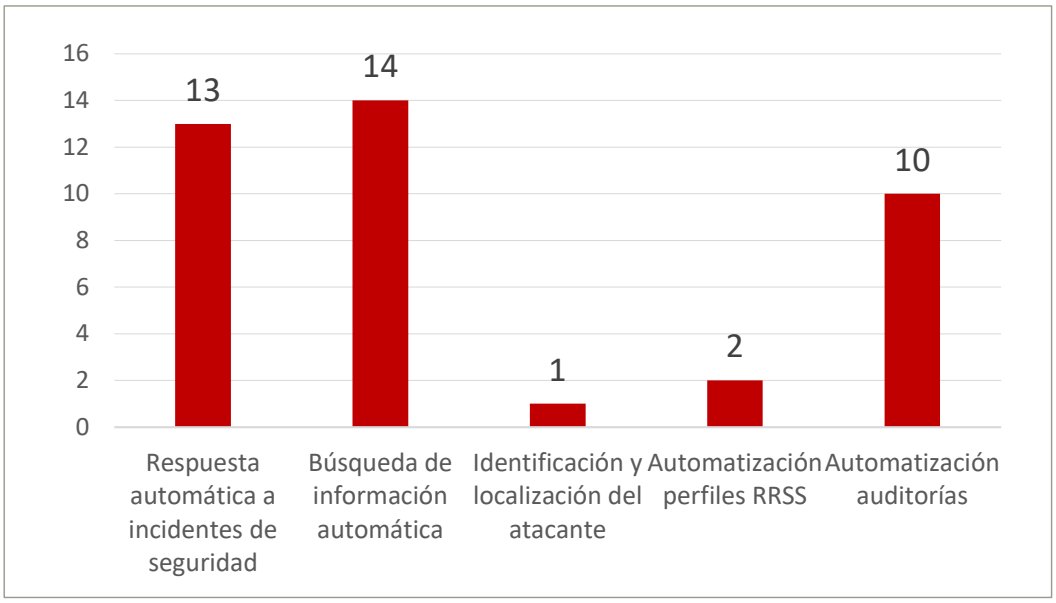


Figura 133. P67: Datos RPA y automatización. Actividades más relevantes para ciberdefensa

La representación gráfica de estos datos se muestra en la siguiente figura:

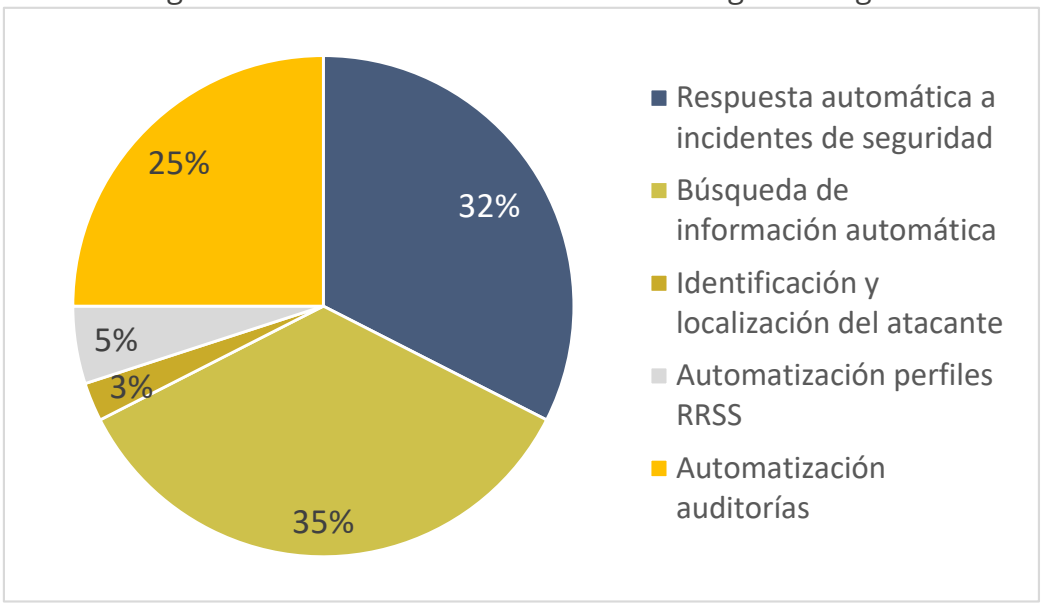


Figura 134. P67: Gráfico. RPA y automatización. Actividades más relevantes para ciberdefensa

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:

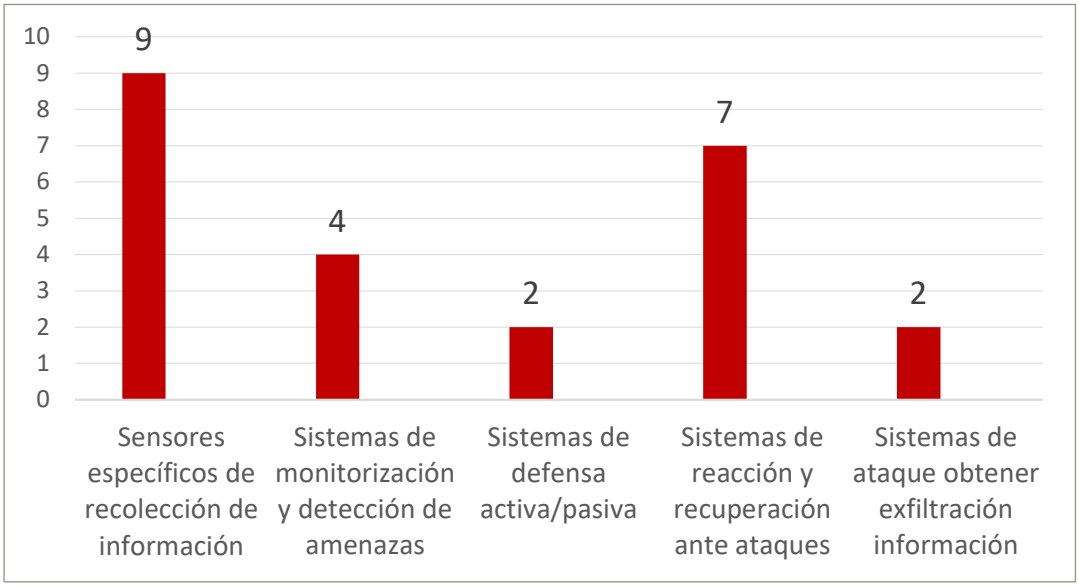


Figura 135. P68 Datos RPA y automatización. Tecnologías con mayor impacto a los sistemas de defensa en operaciones RPA

La representación gráfica de estos datos se muestra en la siguiente figura:

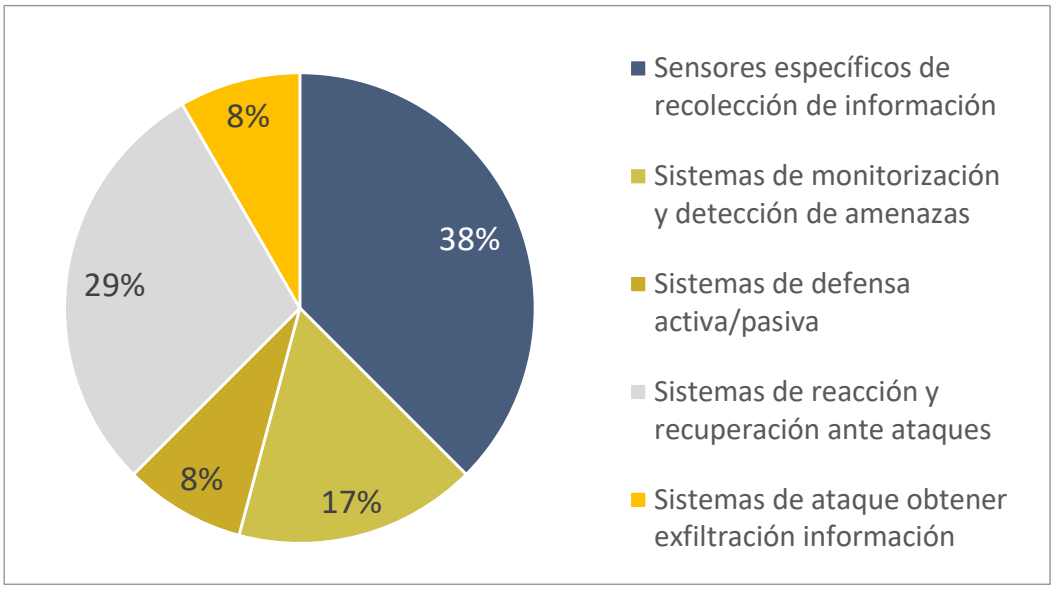


Figura 136. P68: Gráfico. RPA y automatización. Tecnologías con mayor impacto a los sistemas de defensa en operaciones RPA

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:

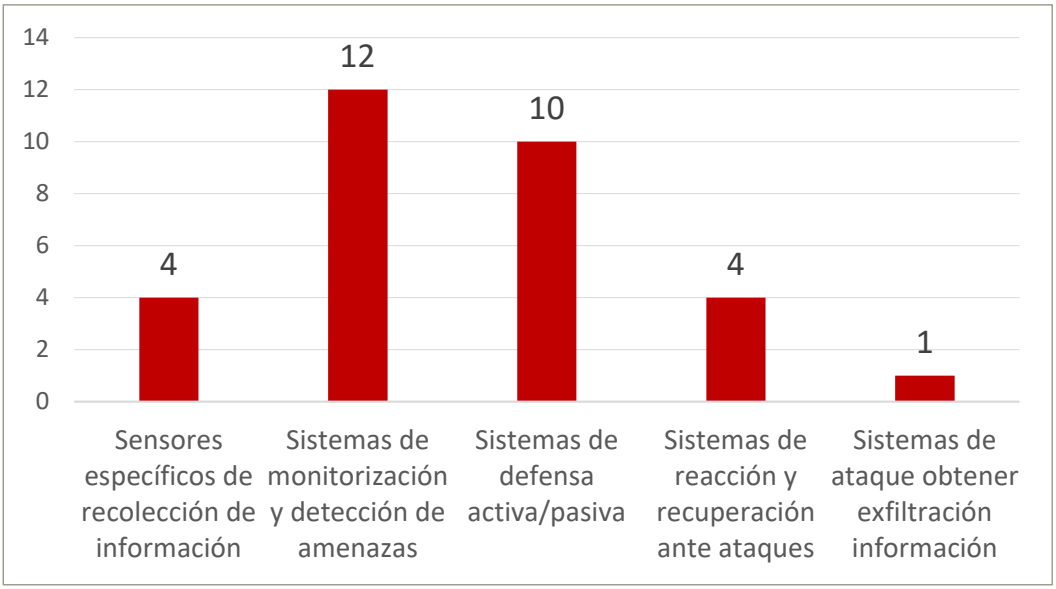


Figura 137. P68 Datos RPA y automatización. Tecnologías con mayor impacto a los sistemas de defensa en operaciones. Automatización ITPA y tecnologías SOAR

La representación gráfica de estos datos se muestra en la siguiente figura:

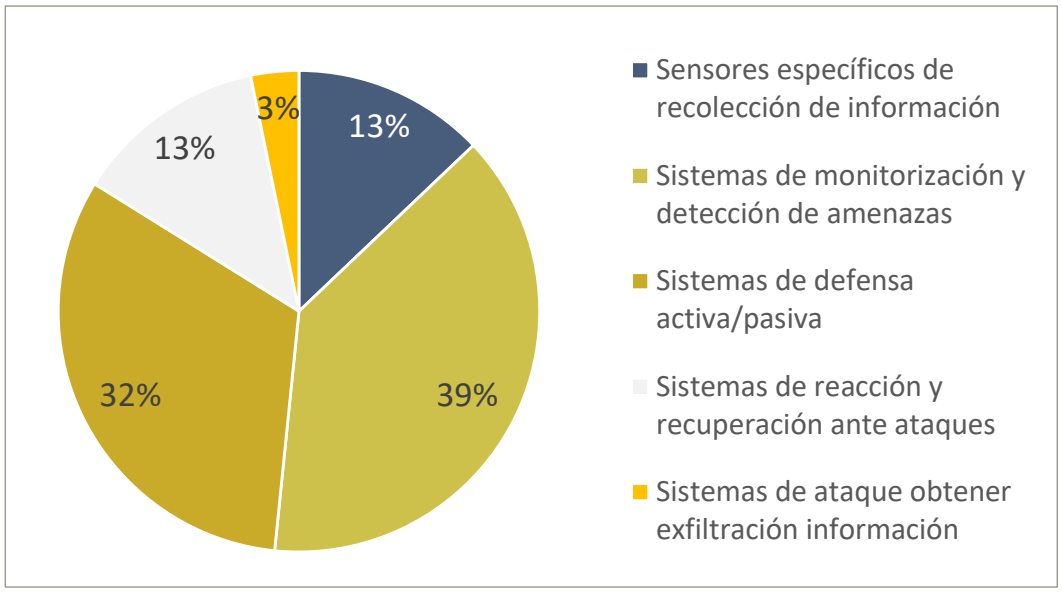


Figura 138. P68: Gráfico. RPAs y automatización. Tecnologías con mayor impacto a los sistemas de defensa en operaciones. Automatización ITPA y tecnologías SOAR

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:

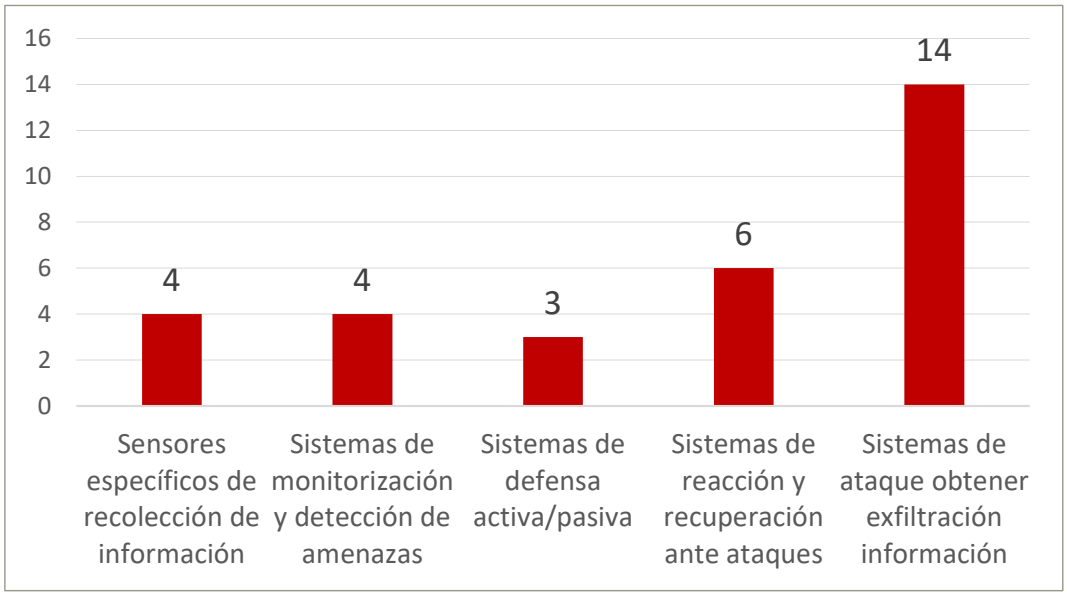


Figura 139. P68: Datos RPA y automatización. Tecnologías con mayor impacto a los sistemas de defensa en operaciones scripting y macros

La representación gráfica de estos datos se muestra en la siguiente figura:

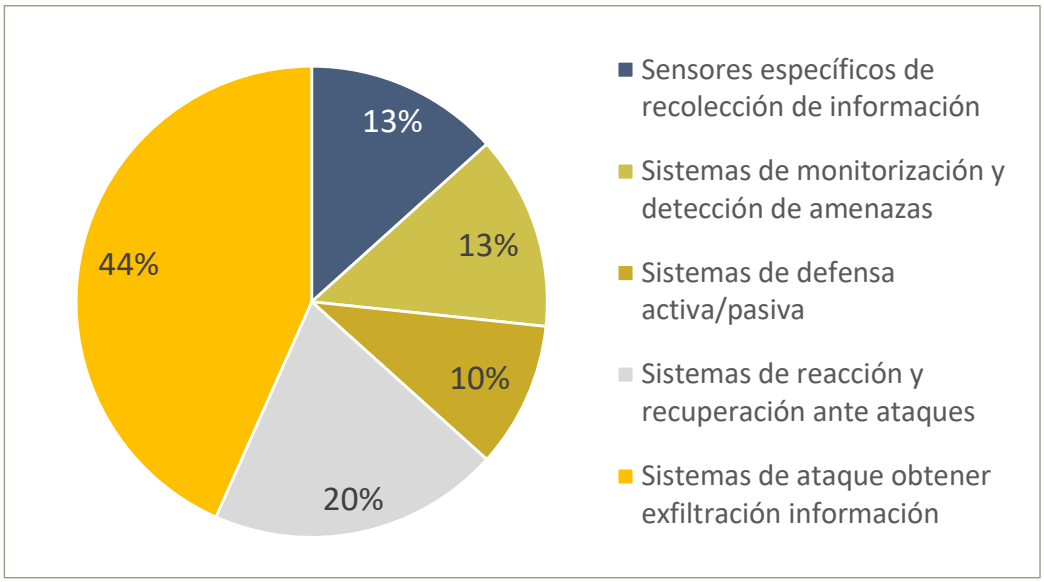


Figura 140. P68: Gráfico. RPA y automatización. Tecnologías con mayor impacto a los sistemas de defensa en operaciones scripting y macros

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:

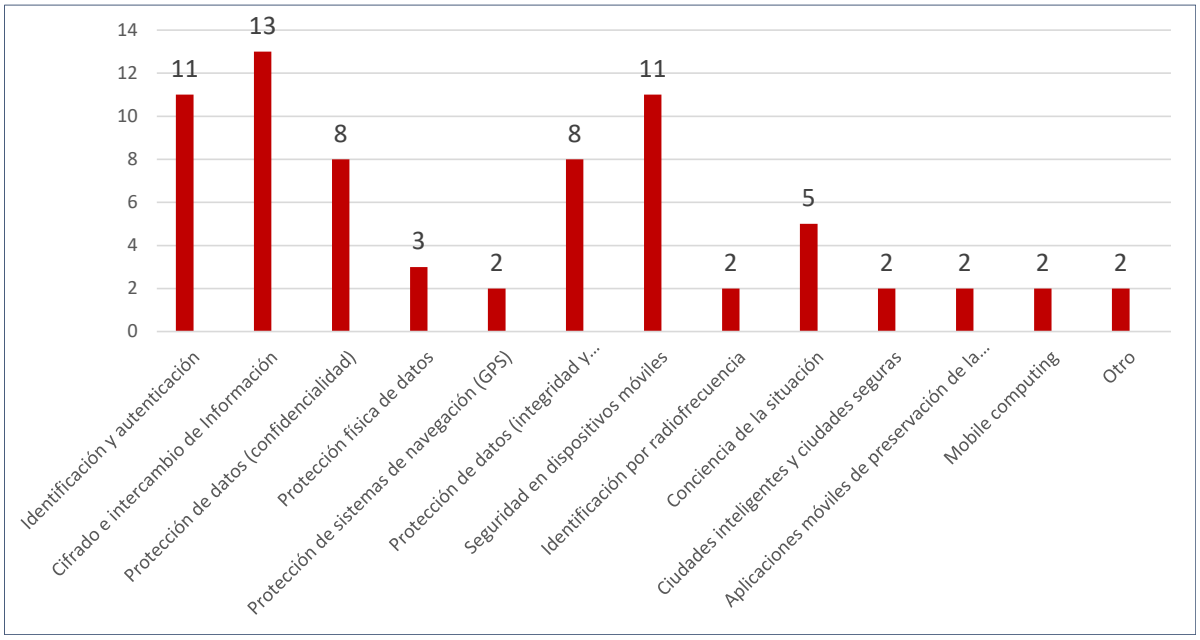


Figura 141. P69: Datos dispositivos móviles. Actividades más relevantes para ciberdefensa

La representación gráfica de estos datos se muestra en la siguiente figura:

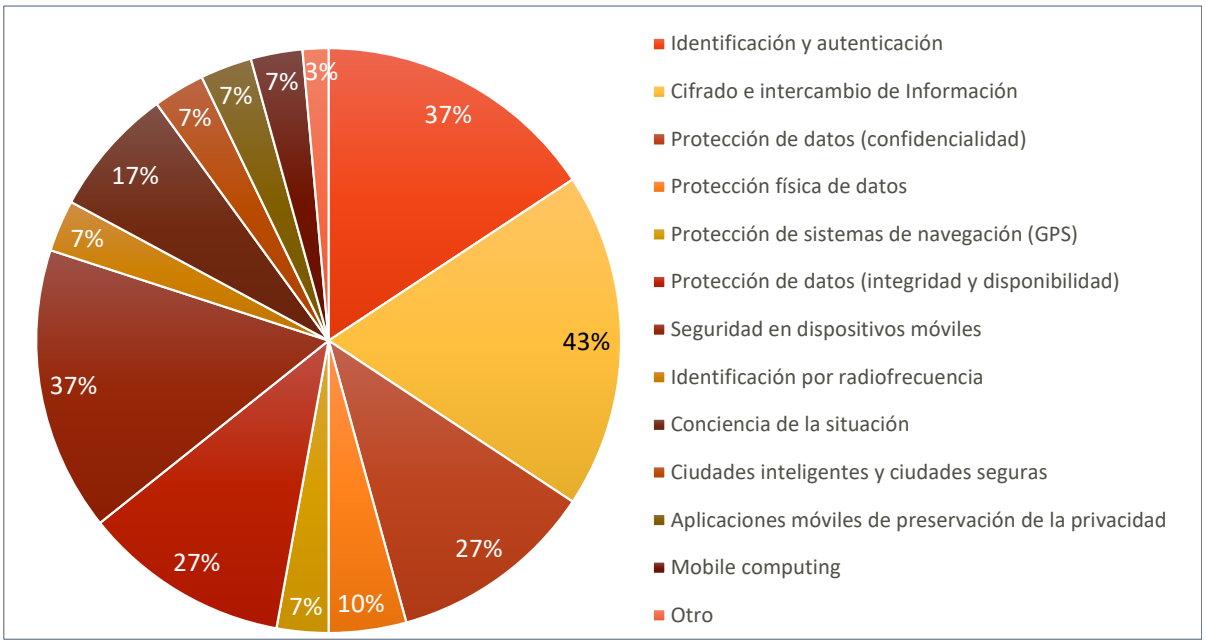


Figura 142. P69: Gráfico. Dispositivos móviles. Actividades más relevantes para ciberdefensa

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:

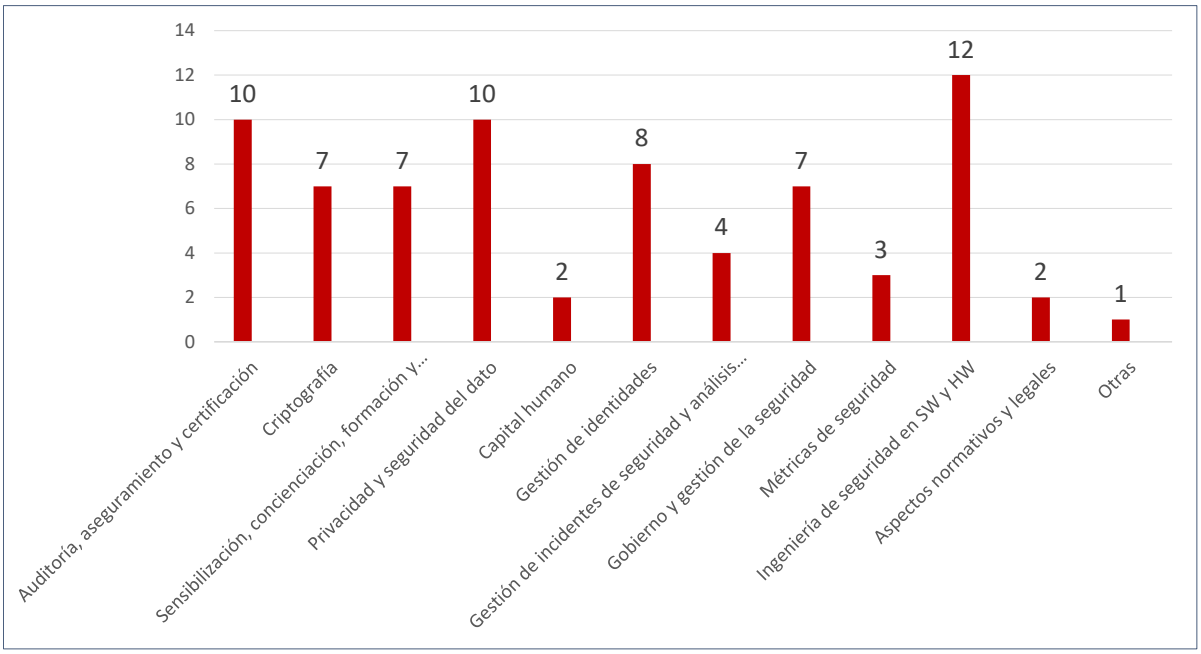


Figura 143. P70: Datos dispositivos móviles. Dominios de conocimiento para desarrollar capacidades en ciberdefensa

La representación gráfica de estos datos se muestra en la siguiente figura:

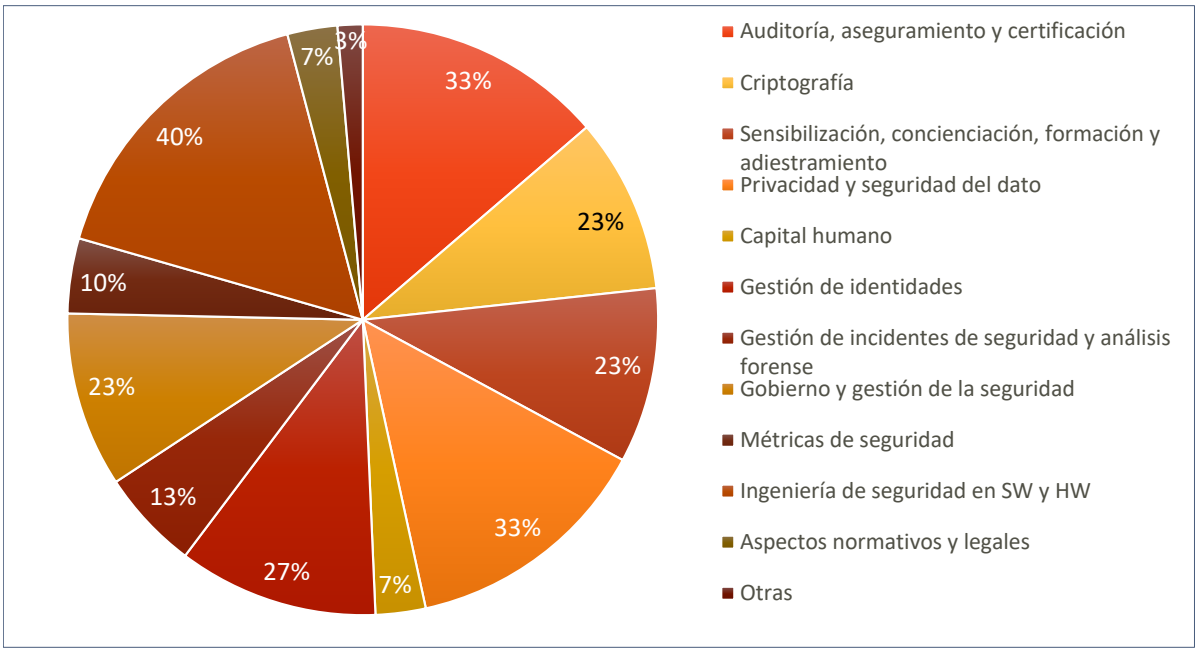


Figura 144. P70: Gráfico. Dispositivos móviles. Dominios de conocimiento para desarrollar capacidades en ciberdefensa

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:

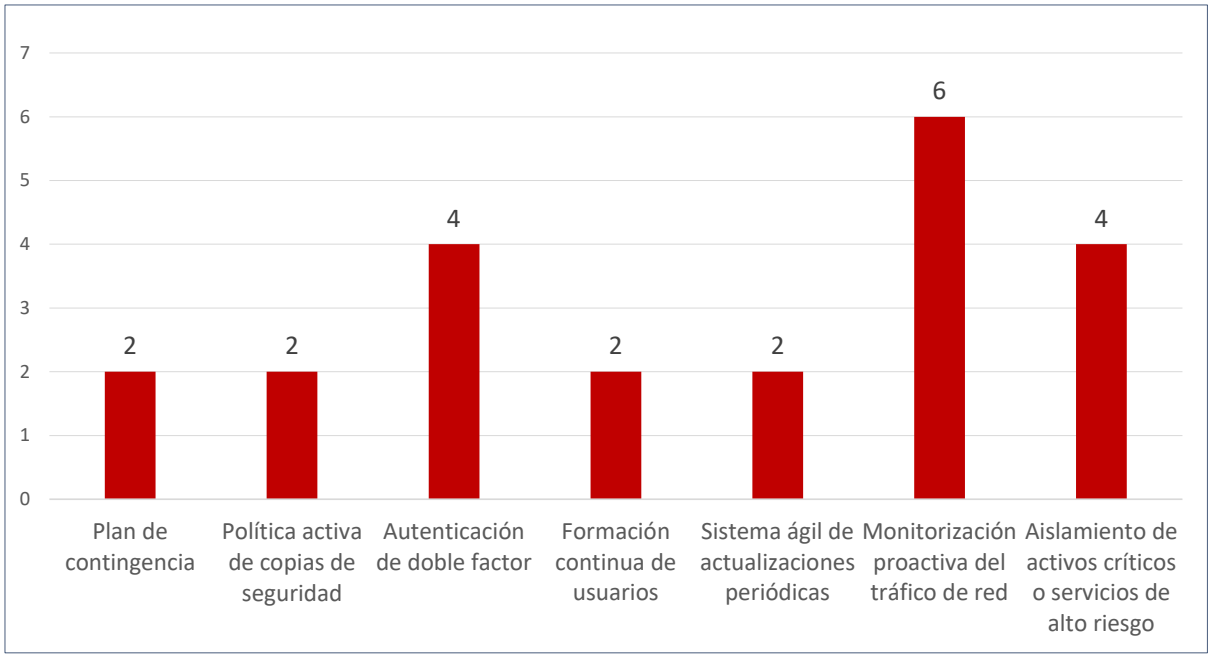


Figura 145. P71: Datos seguridad en redes. Mecanismo de ciberseguridad

La representación gráfica de los datos se muestra en la siguiente figura:

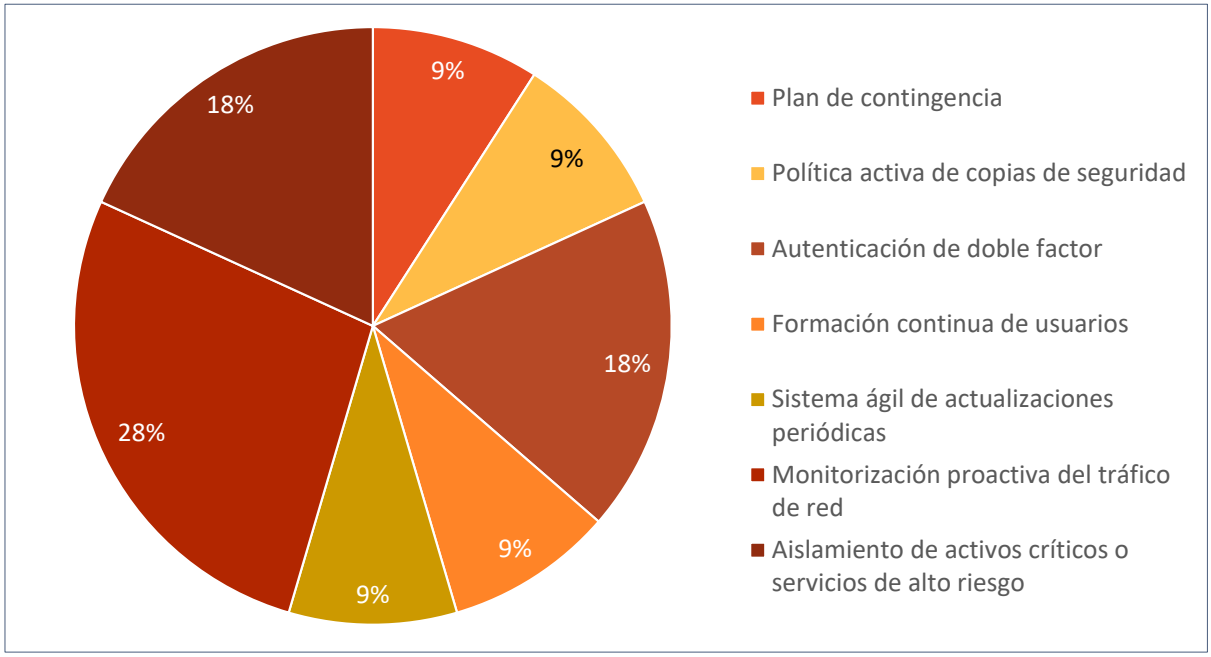


Figura 146. P71: Gráfico. Seguridad en redes. Mecanismo de ciberseguridad

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:

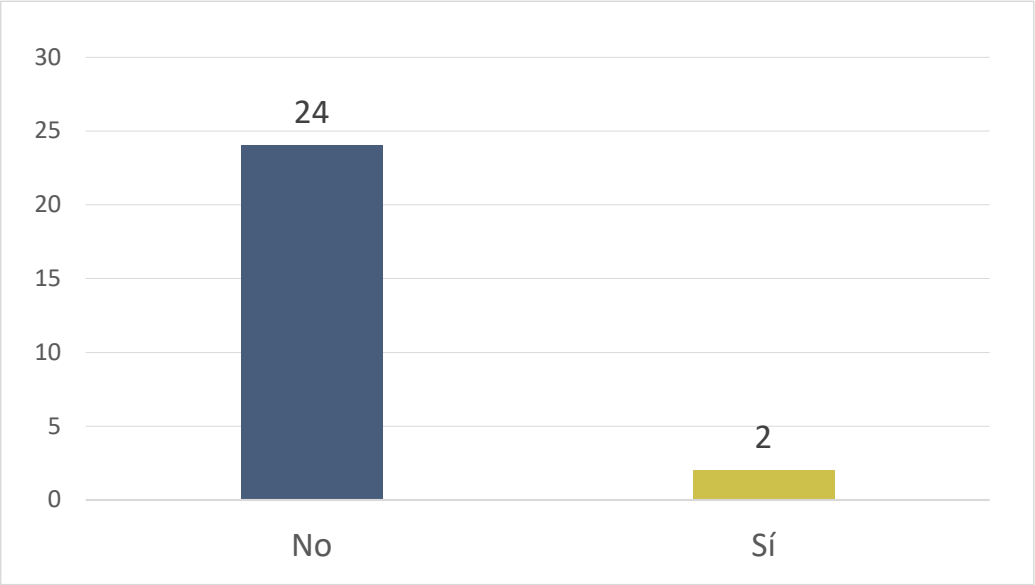


Figura 147. P72: Datos seguridad en redes. Capacidades esteganografía

La representación gráfica de los datos se muestra en la siguiente figura:

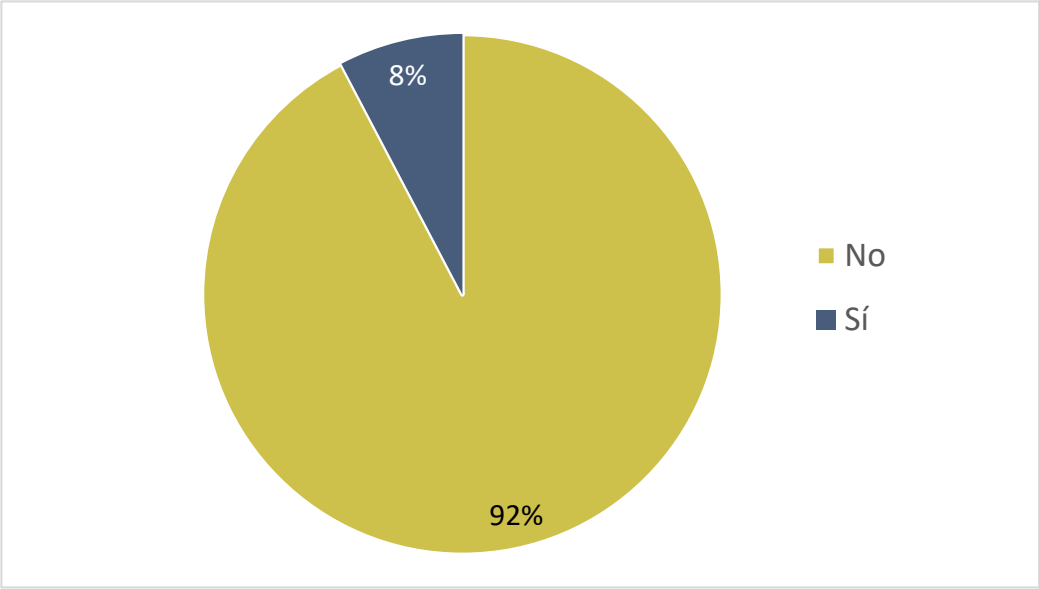


Figura 148. P72: Grafico. Seguridad en redes. Capacidades esteganografía

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:

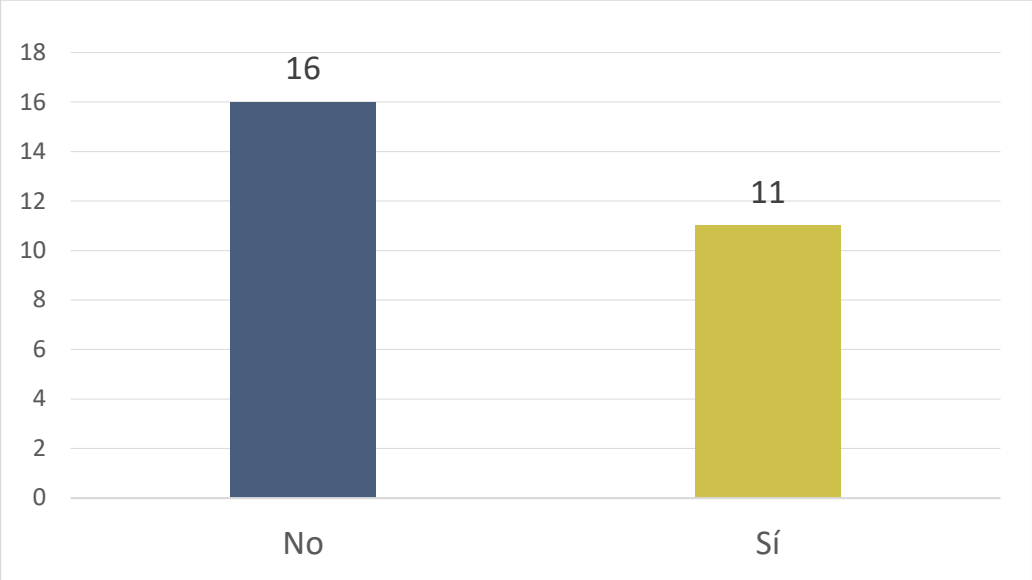


Figura 149. P73: Datos seguridad en redes. Capacidades defensa ante ataques propagables

La representación gráfica de los datos se muestra en la siguiente figura:

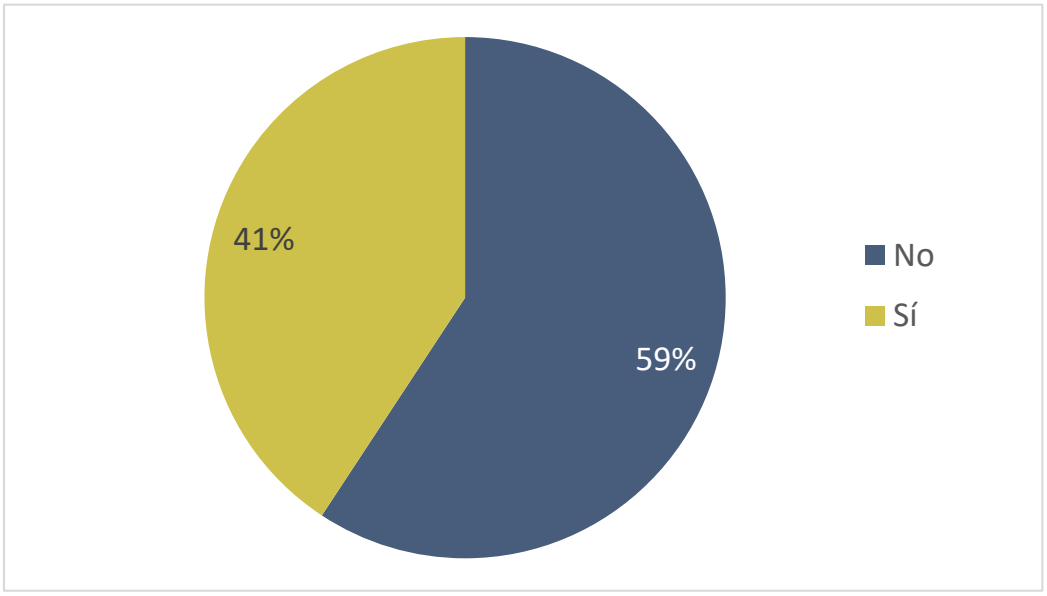


Figura 150. P73: Gráfico. seguridad en redes. Capacidades defensa ante ataques propagables

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:

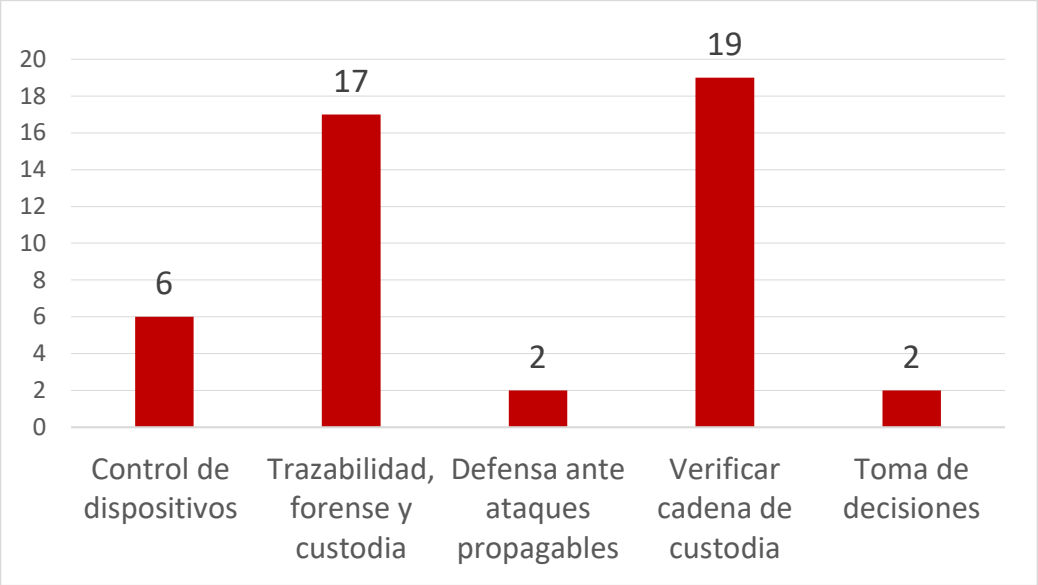


Figura 151. P76: Datos Actividades de blockchain y DLT más relevantes relacionadas con la ciberdefensa

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.

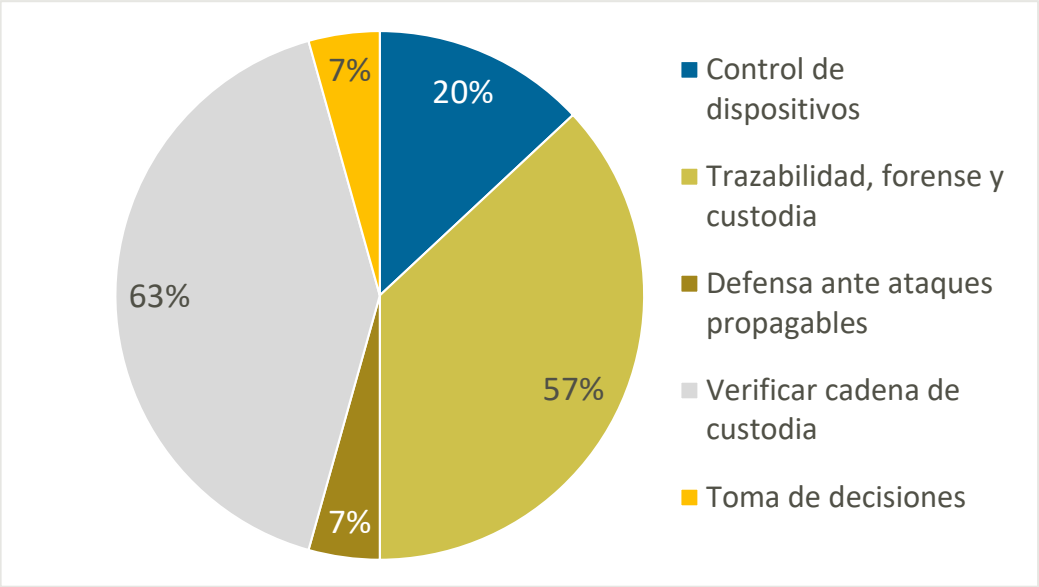


Figura 152.P76: Gráfico. Actividades de blockchain y DLT más relevantes relacionadas con la ciberdefensa

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:

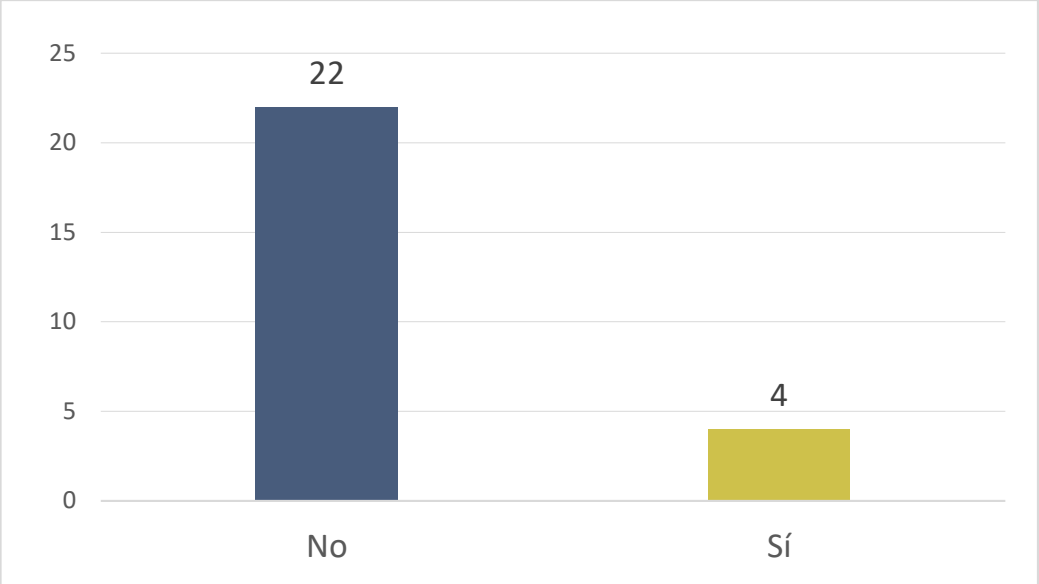


Figura 153. P77: Datos Capacidades referentes a la privacidad y seguridad del dato con técnicas de blockchain para ciberdefensa

La representación gráfica de estos datos se muestra en la siguiente figura:

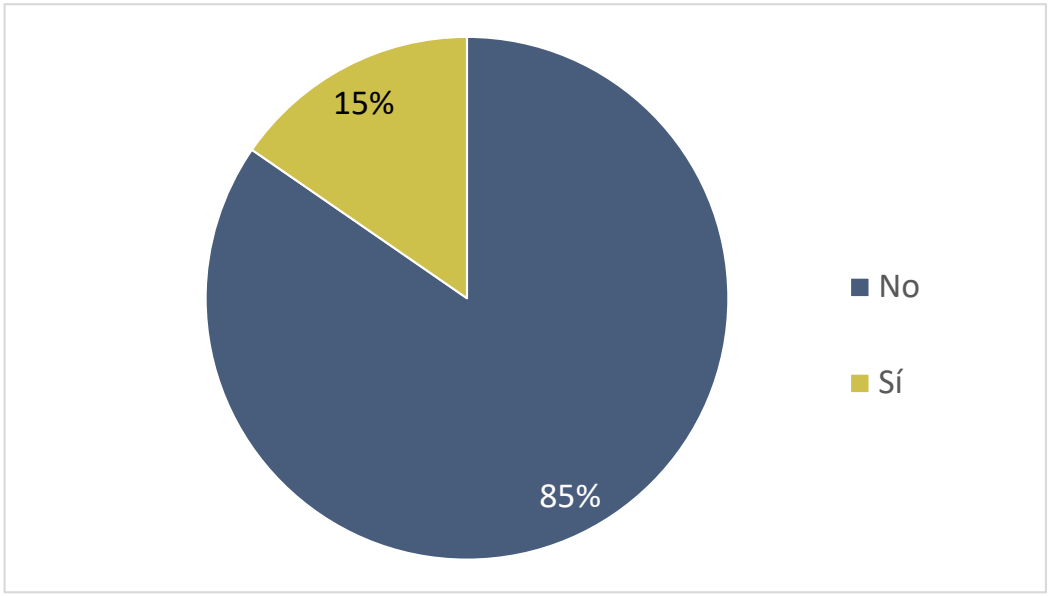


Figura 154. P77: Gráfico. Capacidades referentes a la privacidad y seguridad del dato con técnicas de blockchain para ciberdefensa

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:

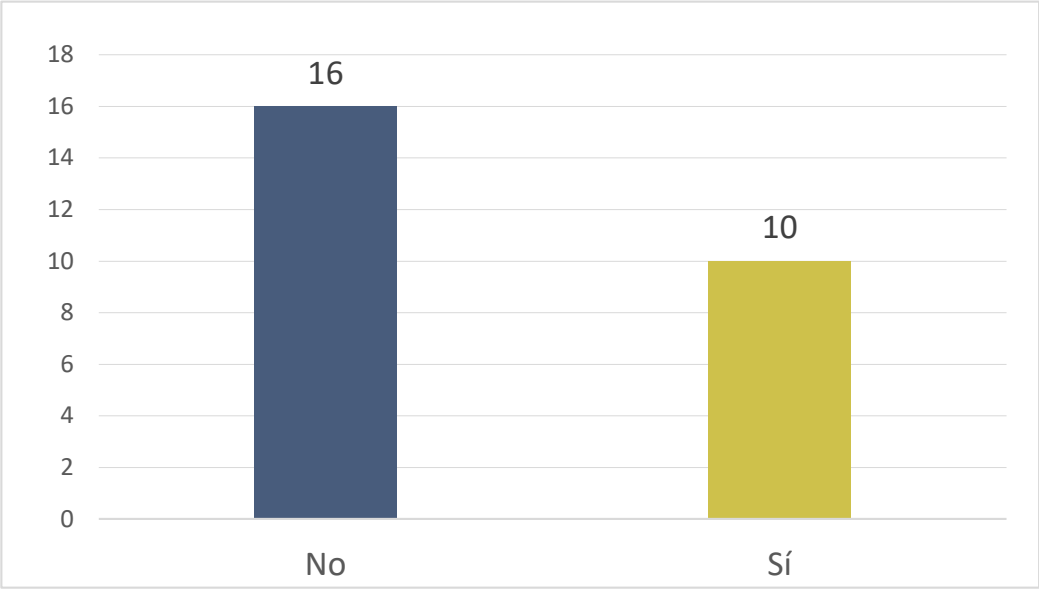


Figura 155. P78: Datos criptografía. Tecnologías y postcuánticas

La representación gráfica de los datos se muestra en la siguiente figura:

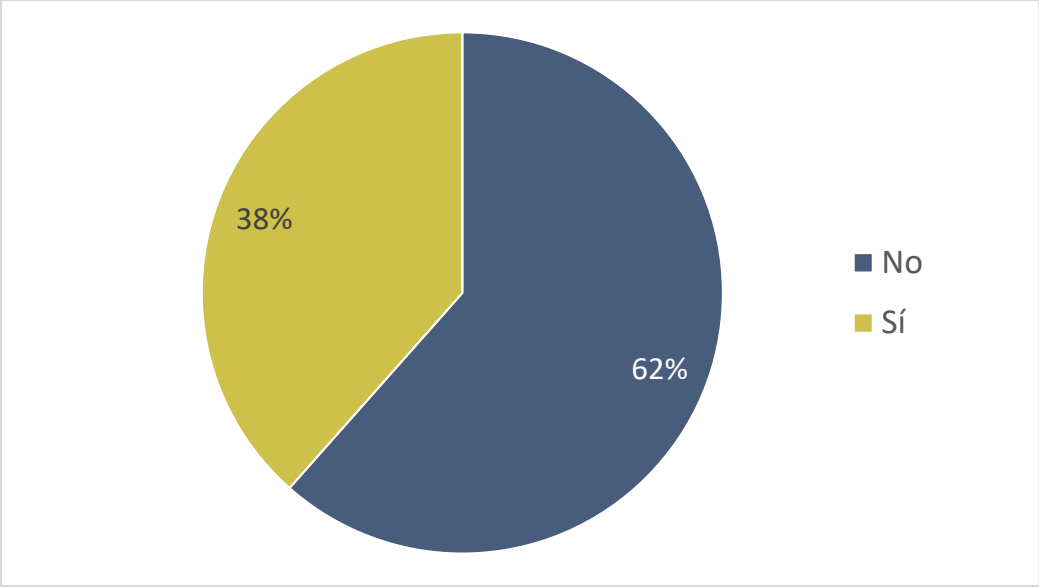


Figura 156. P78: Gráfico. Criptografía. Tecnologías y postcuánticas

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:

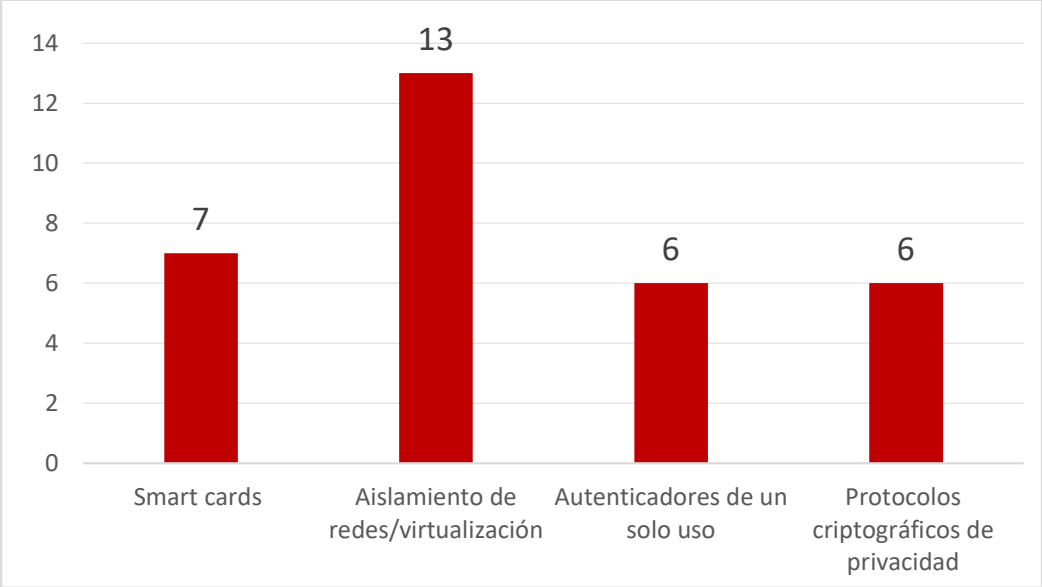


Figura 157. P79: Datos criptografía.Mecanismos criptográficos avanzados

La representación gráfica de los datos se muestra en la siguiente figura:

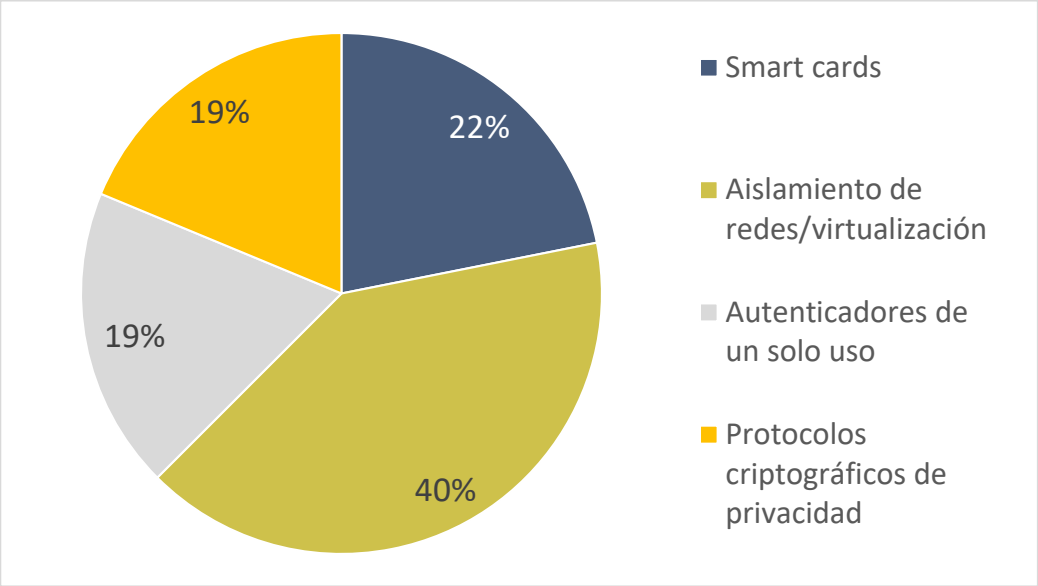


Figura 158. P79: Gráfico. Criptografía.Mecanismos criptográficos avanzados

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:

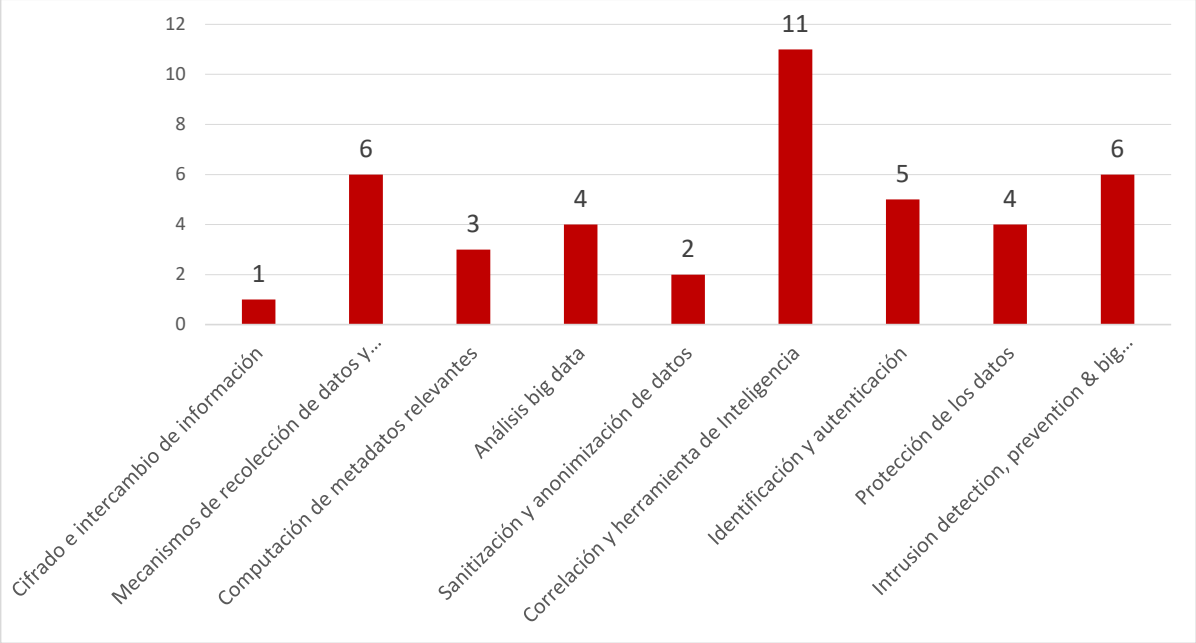


Figura 159. P80: Datos data minig y analítica avanzada

La representación gráfica de estos datos se muestra en la siguiente figura:

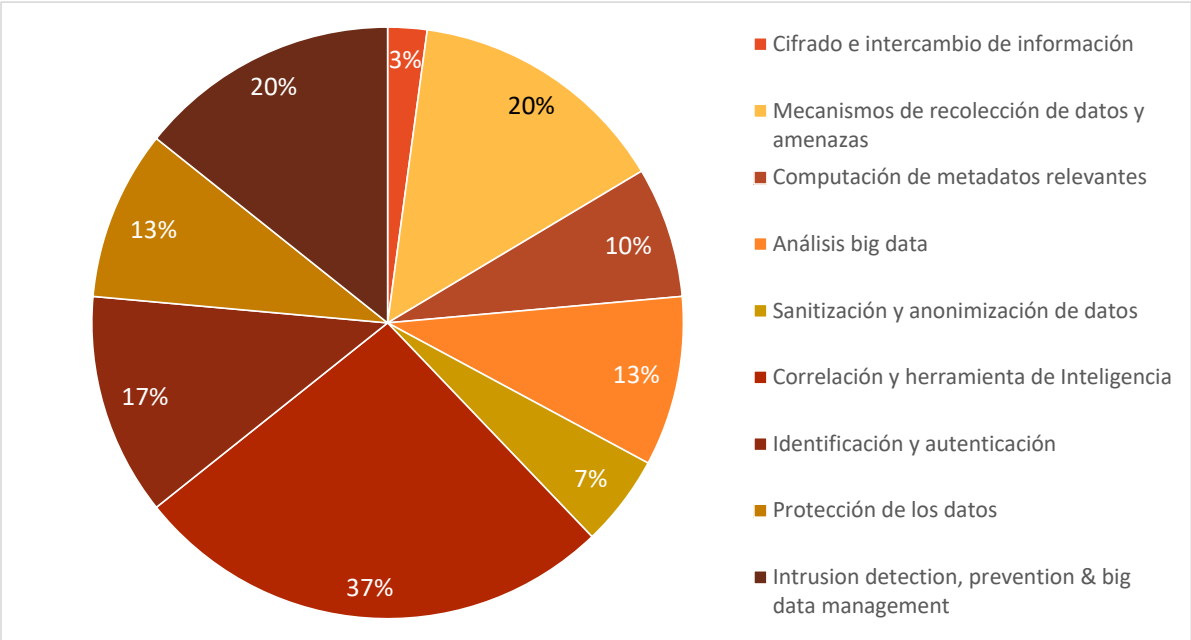


Figura 160. P80: Gráfico. Data minig y analítica avanzada

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:

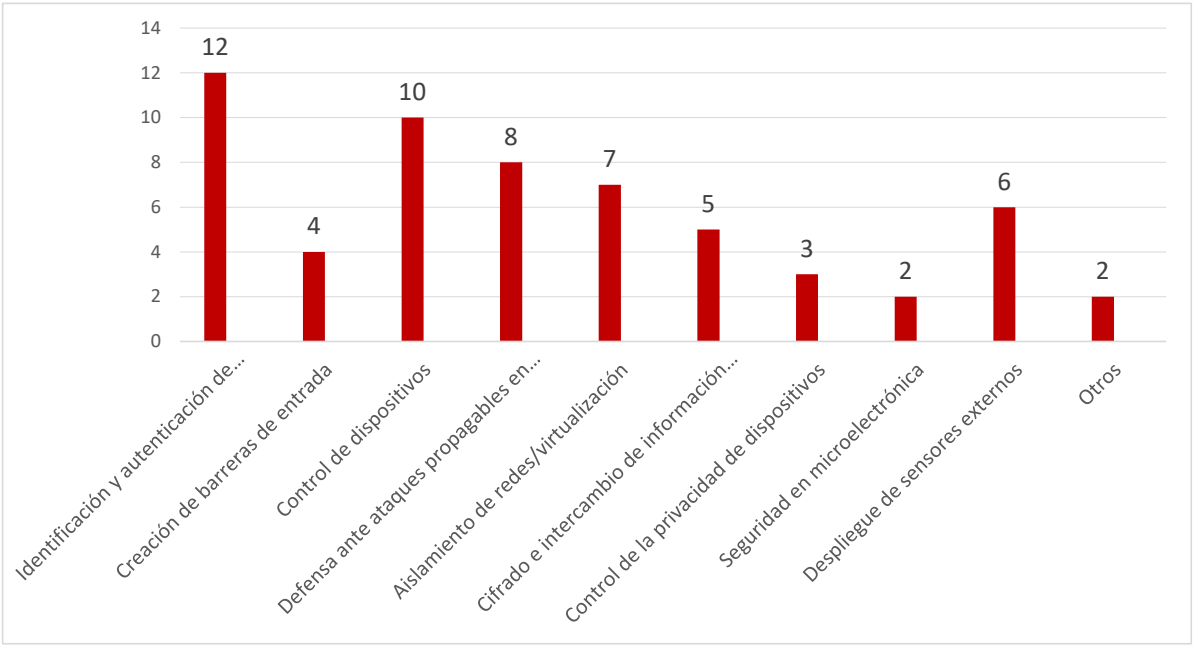


Figura 161. P81: Datos IoT. Actividades más relevantes para ciberdefensa

La representación gráfica de estos datos se muestra en la siguiente figura:

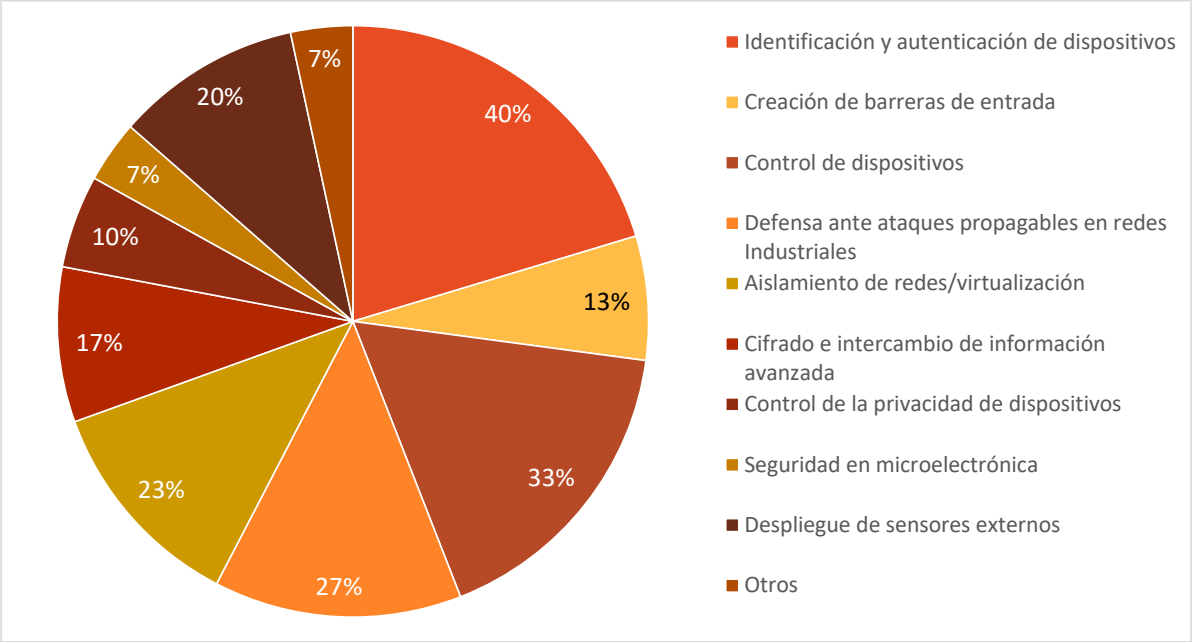


Figura 162. P81: Gráfico. IoT. Actividades más relevantes para ciberdefensa

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:

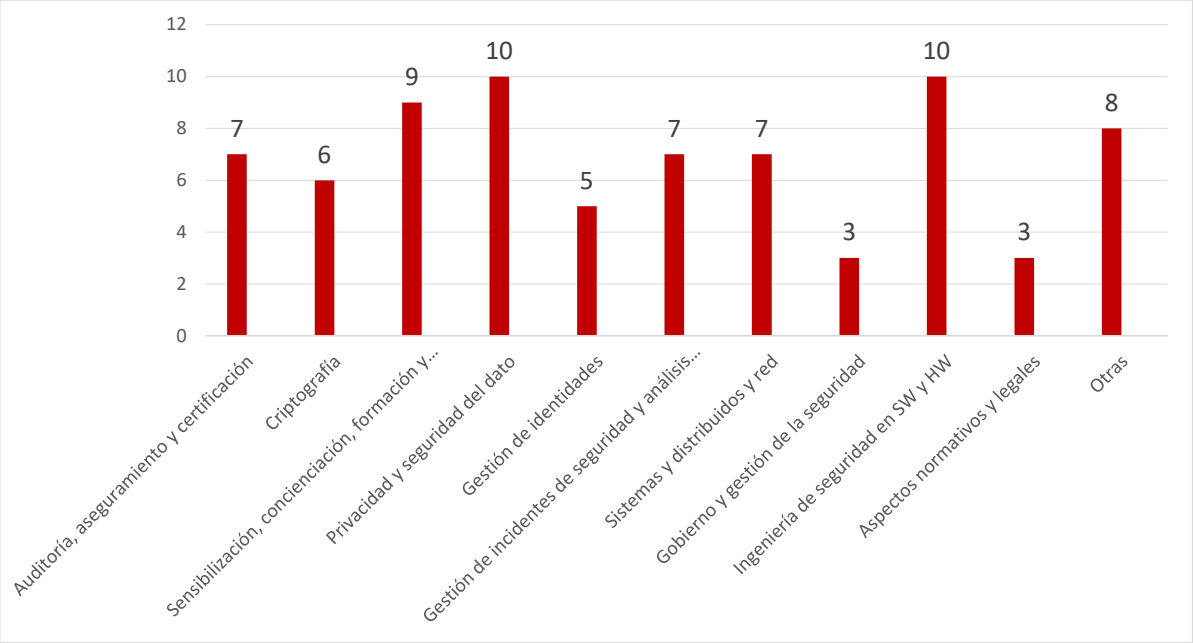


Figura 163. P82: Datos IoT. Tecnologías con mayor impacto para ciberdefensa

La representación gráfica de estos datos se muestra en la siguiente figura:

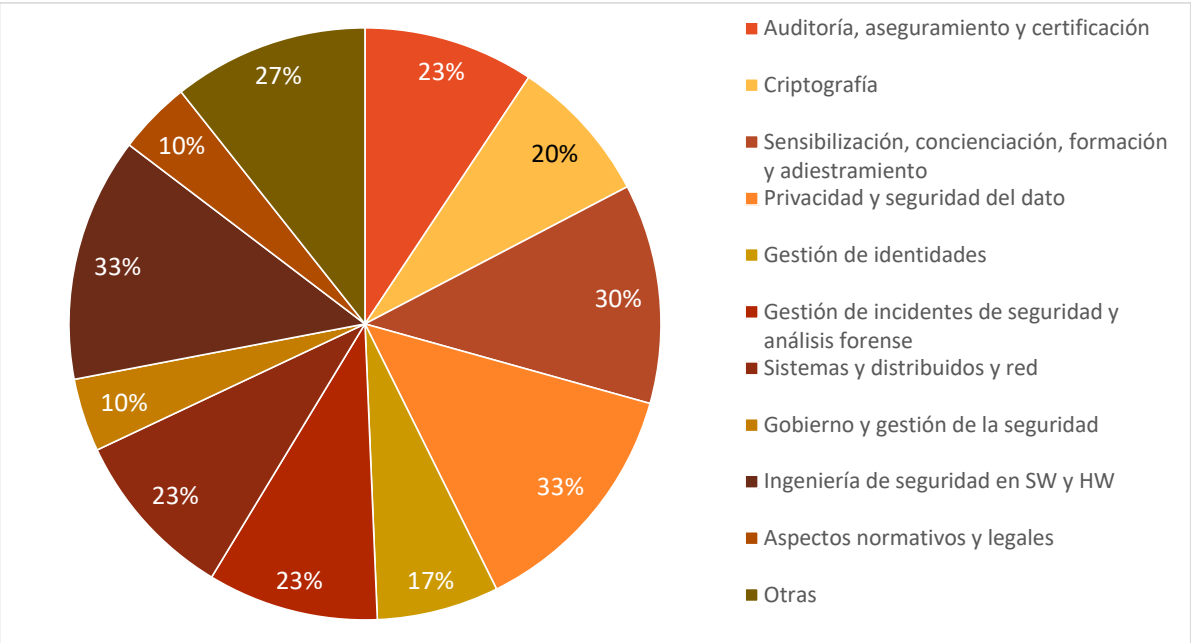


Figura 164. P82: Gráfico. IoT. Tecnologías con mayor impacto para ciberdefensa

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:

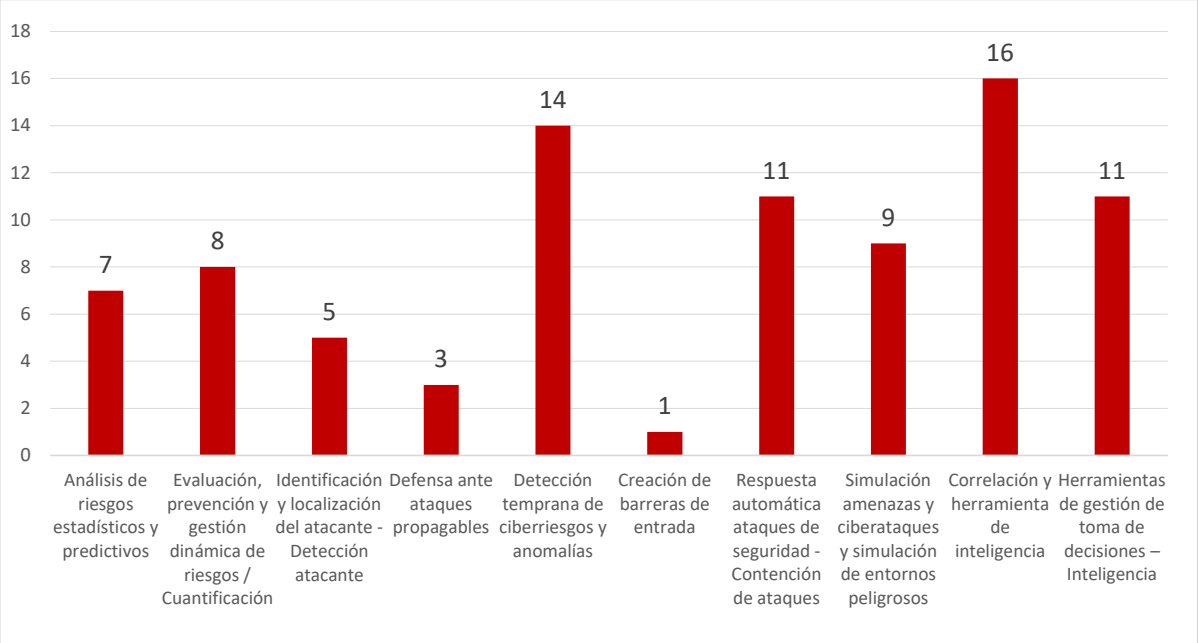


Figura 165. P83: Datos Inteligencia artifical

La representación gráfica de los datos se muestra en la siguiente figura:

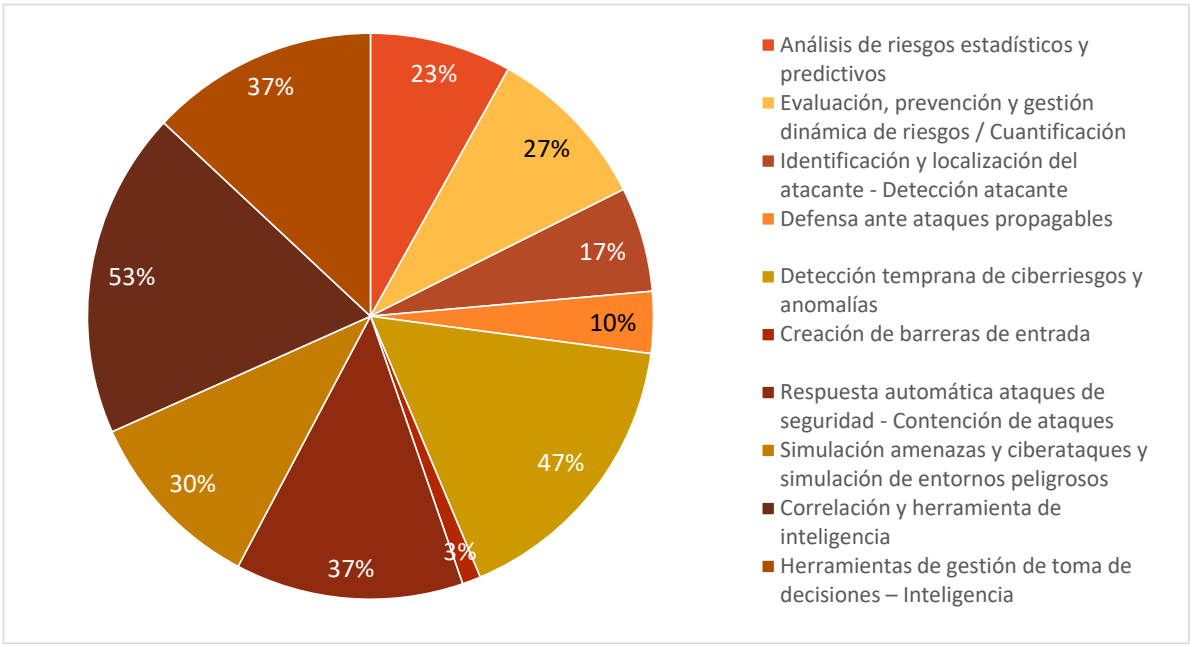


Figura 166. P83: Gráfico. Inteligencia artifical

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:

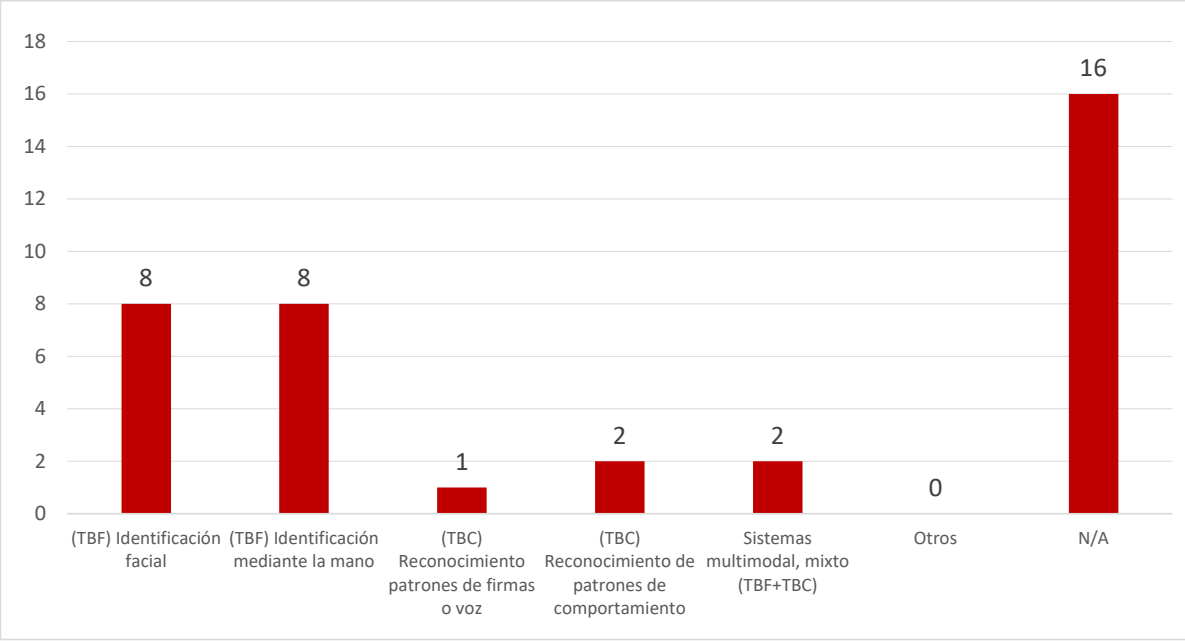


Figura 167. P84: Datos biometría. Técnicas utilizadas

La representación gráfica de los datos se muestra en la siguiente figura:

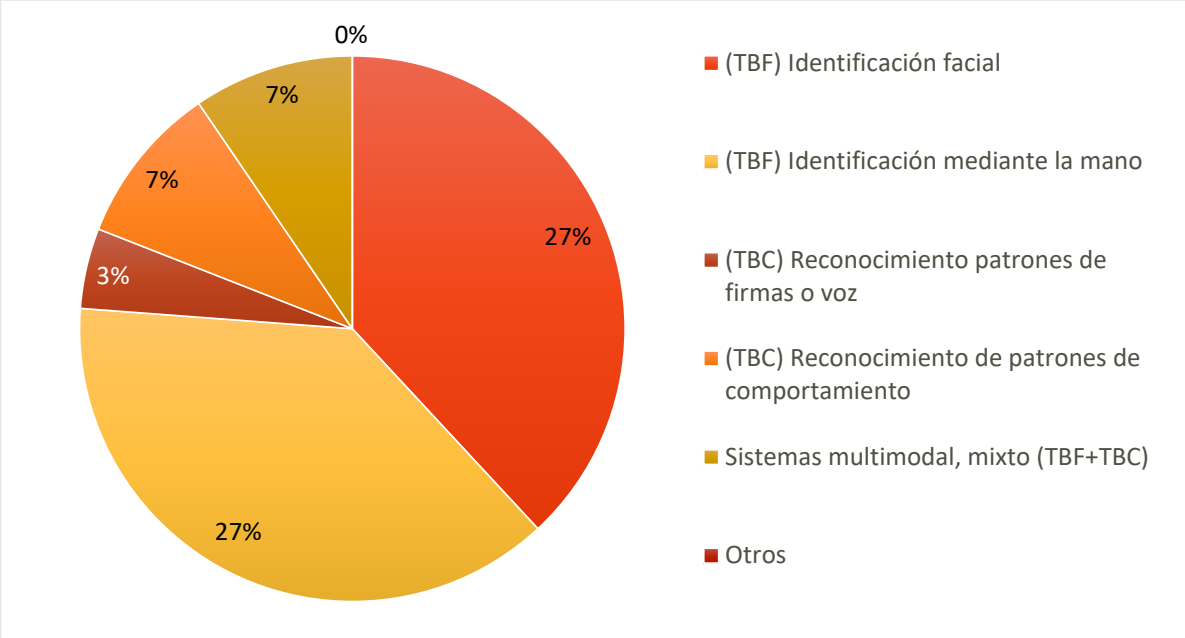


Figura 168. P84: Gráfico. Biometría. Técnicas utilizadas

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:

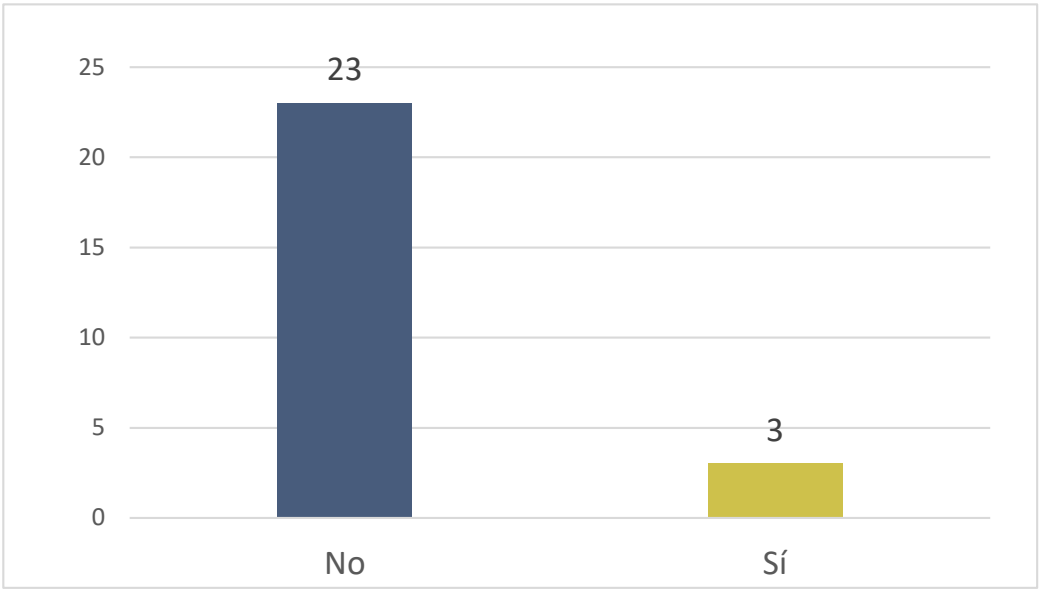


Figura 169. P85: Datos biometría. Capacidades de cifrado

La representación gráfica de los datos se muestra en la siguiente figura:

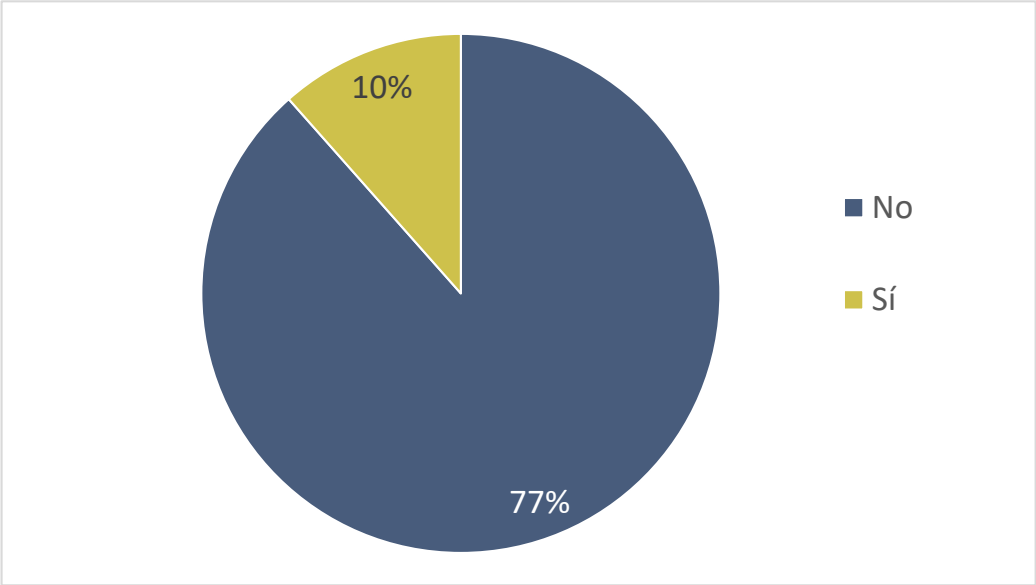


Figura 170. P85: Gráfico. Biometría. Capacidades de cifrado

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

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

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA, RELACIONES CON LAS CORTES Y MEMORIA DEMOCRÁTICA

NIPO (edición online): 089-23-018-6
Fecha de edición: junio 2023

FORO
NACIONAL DE
CIBERSEGURIDAD

2023