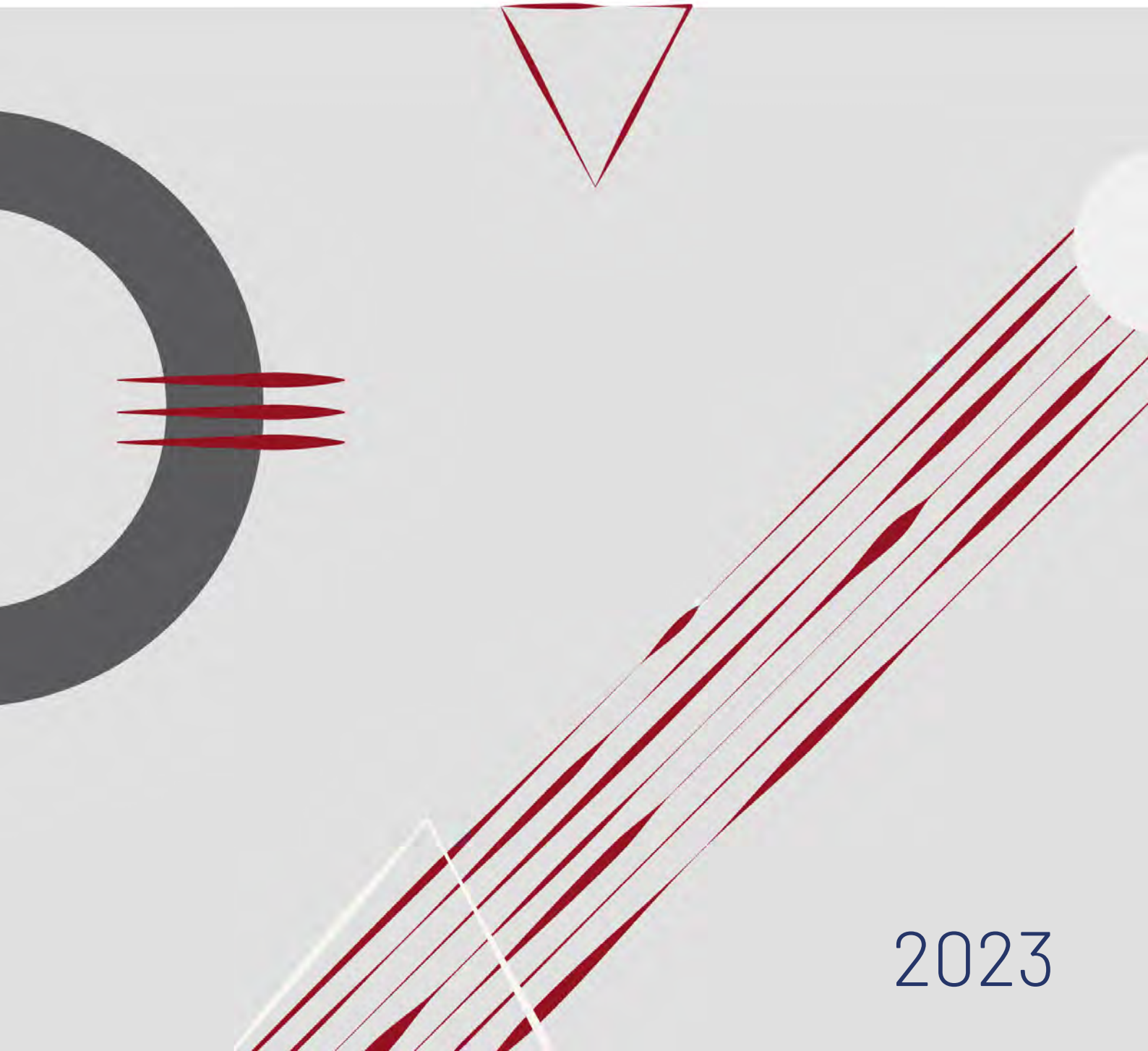
FORO NACIONAL DE CIBERSEGURIDAD

MARCO DE COMPETENCIAS PARA PROGRAMAS SUPERIORES DE FORMACIÓN ESPECIALIZADA EN CIBERSEGURIDAD



2023

Coordinadores sociedad civil:

Víctor A. Villagrá (CRUE Universidades Españolas)

Marta Beltrán Pardo (CRUE Universidades Españolas)

Coordinador institucional:

Pablo López (Centro Criptológico Nacional)

Autores y colaboradores:

Cristina Alcaraz Tello

Eduardo Fernández-Medina Patón

Ana Fernández-Vilas

Lorena González Manzano

Jesús Lizárraga

Gabriel Maciá Fernández

Iván Marsá Maestre

José Javier Martínez Herráiz

Elena Matilla Rodríguez

Helena Rifà Pous

Ricardo Rodríguez Fernández

Francisco J. Sampalo Lainz

Antonio Skármeta

Índice

Acrónimos y terminología

00

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

Objeto

01

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

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

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

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

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

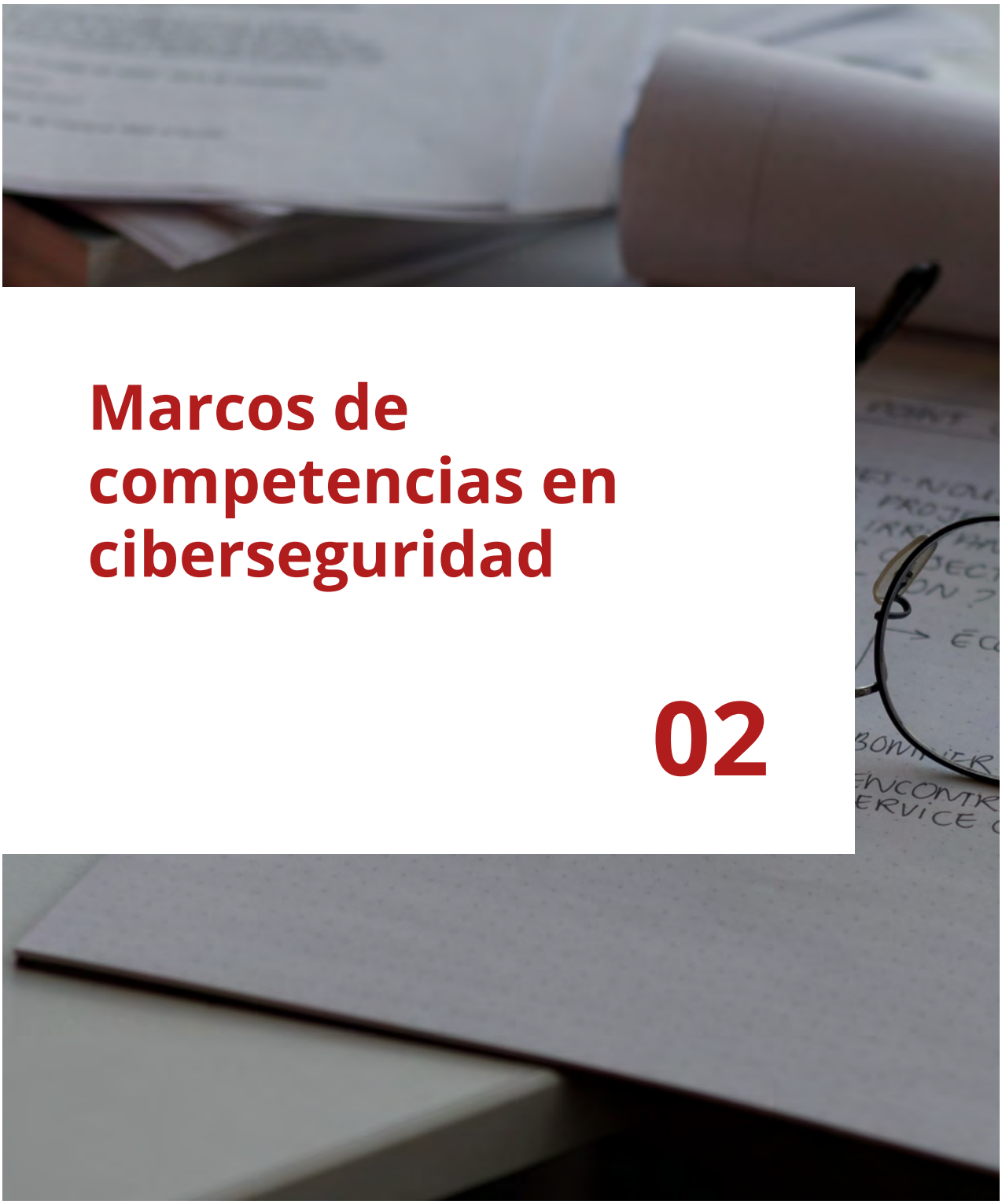
· La sección 2 identifica y analiza los marcos de competencias en ciberseguridad existentes en la actualidad en el ámbito internacional, que pueden ser tomados como base para la identificación de competencias que se pretende realizar.

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

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

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

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



Marcos de competencias en ciberseguridad

02

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

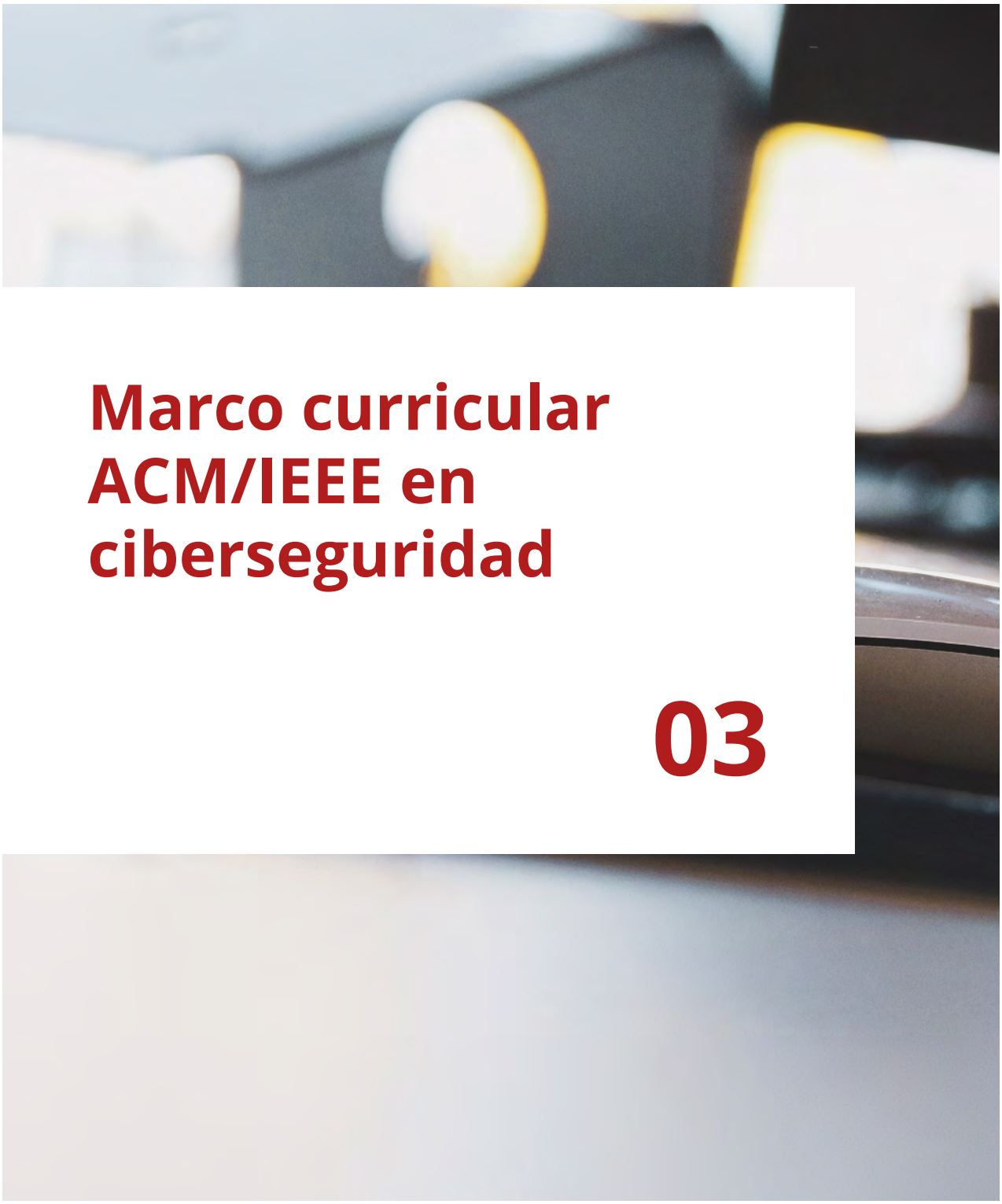
Uno de los marcos referenciales más utilizados es el de NICE (National Initiative for Cybersecurity Education). NICE es un esfuerzo conjunto del gobierno estadounidense junto con instituciones académicas y del sector privado para fortalecer las capacidades formativas en ciberseguridad de los Estados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

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

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

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

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



Marco curricular ACM/IEEE en ciberseguridad

03

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

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

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

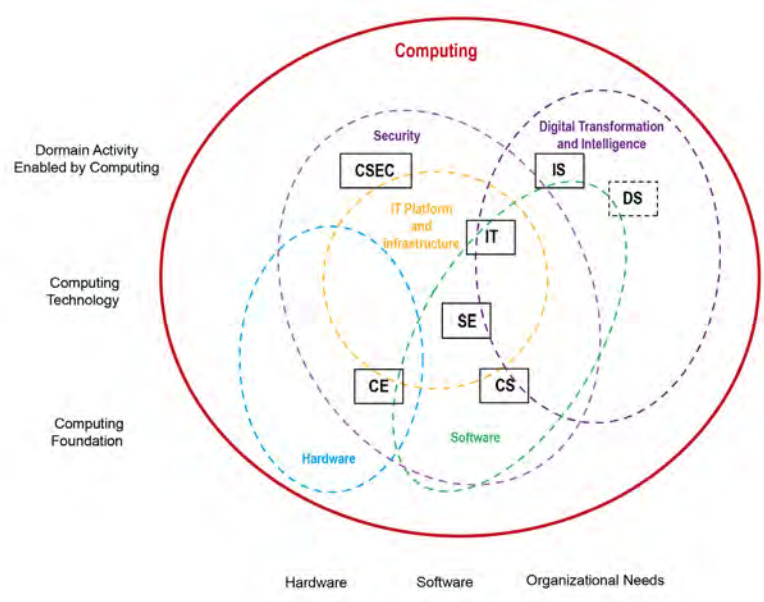


Figura 1. Relación de disciplinas por área de aplicación y tecnología [CC2020]

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

3.1. Modelo CSEC 2017

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

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

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

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

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

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

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

3.2. Áreas de Conocimiento en Ciberseguridad

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

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

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

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

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

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

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

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

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

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

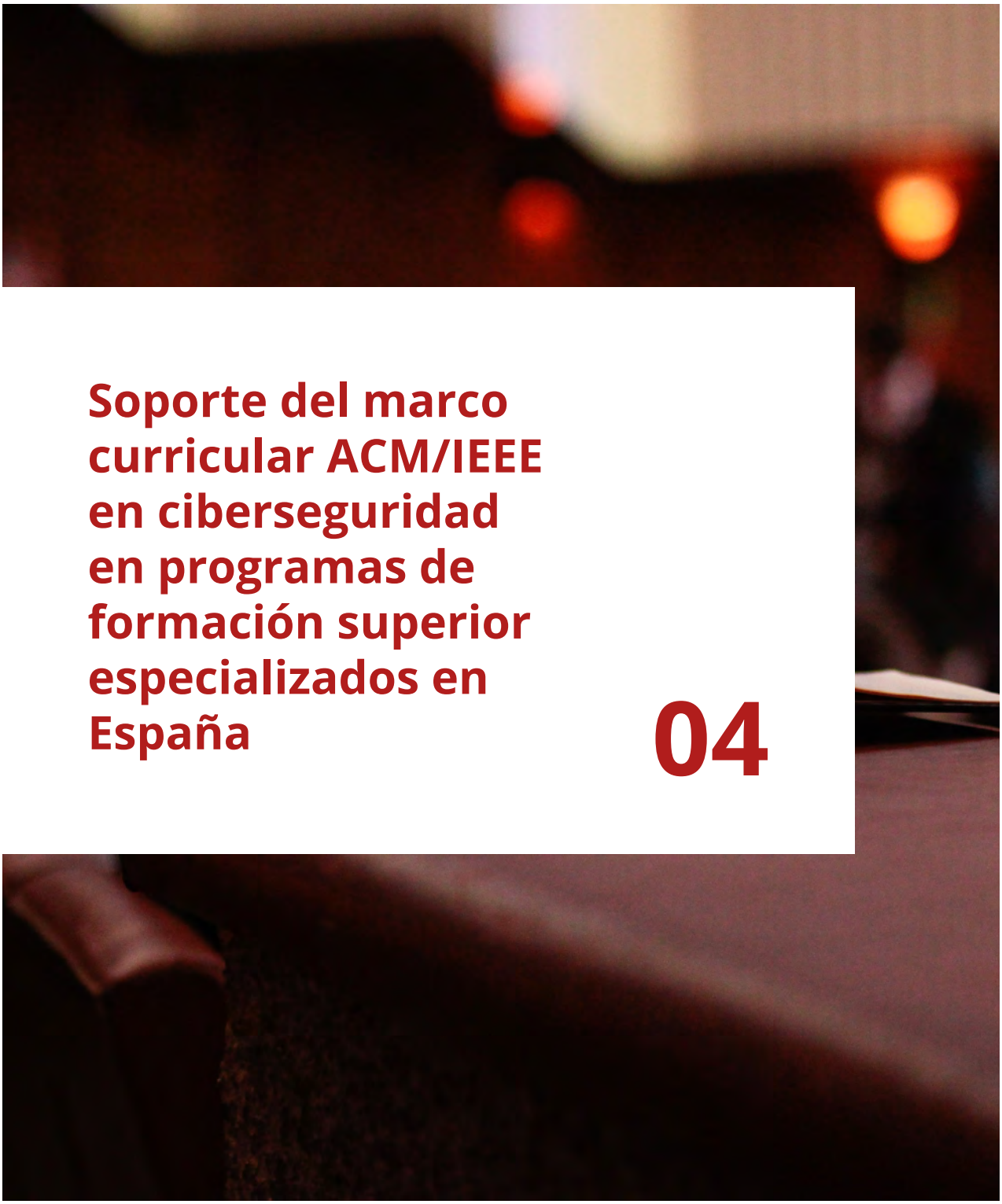
Acceso al sistema	- Métodos de autenticación - Identidad
Control del sistema	- Control de acceso - Modelos de autorización - Detección de intrusos - Ataques - Defensas - Auditoría - Malware - Modelos de vulnerabilidad - Pruebas de penetración - Análisis forense - Recuperación, resiliencia
Retirada del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

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

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

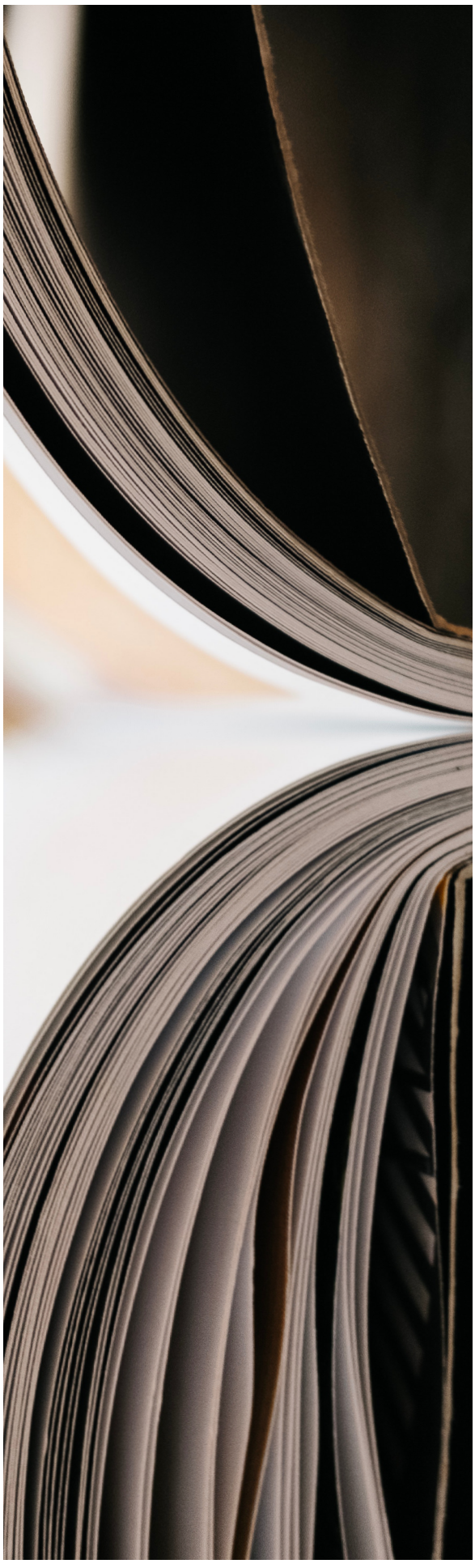
Seguridad del personal	- Concienciación, formación y educación en materia de seguridad - Prácticas de contratación de seguridad - Prácticas de despido por motivos de seguridad - Seguridad de terceros - Seguridad en los procesos de revisión - Cuestión especial en la privacidad de la información personal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

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



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

04



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

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

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

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

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

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

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

De esta consulta, se recibieron informes provenientes de:

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

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

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

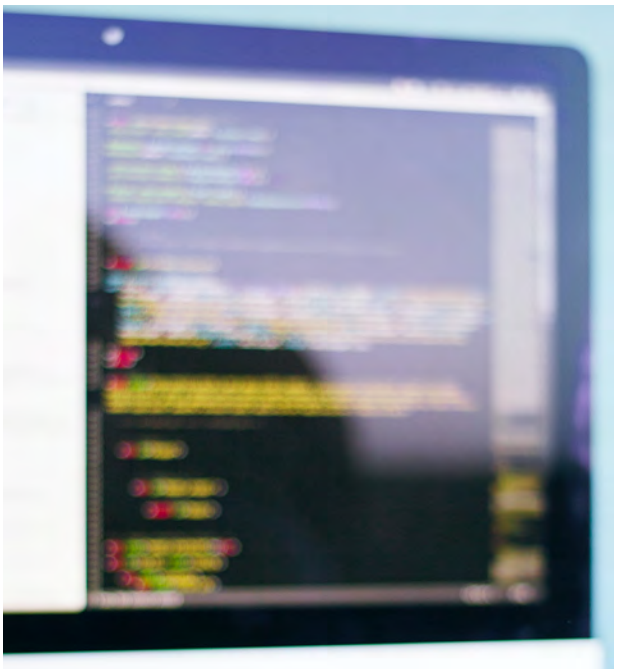
En las siguientes secciones se detalla el análisis agregado sobre el nivel de soporte de todas estas ofertas formativas respecto a los distintos componentes del marco curricular ACM/IEEE en Ciberseguridad. Para cada unidad de conocimiento se incluye un gráfico con el soporte encontrado en cada uno de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

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

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

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

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



4.1.1. Criptografía

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

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

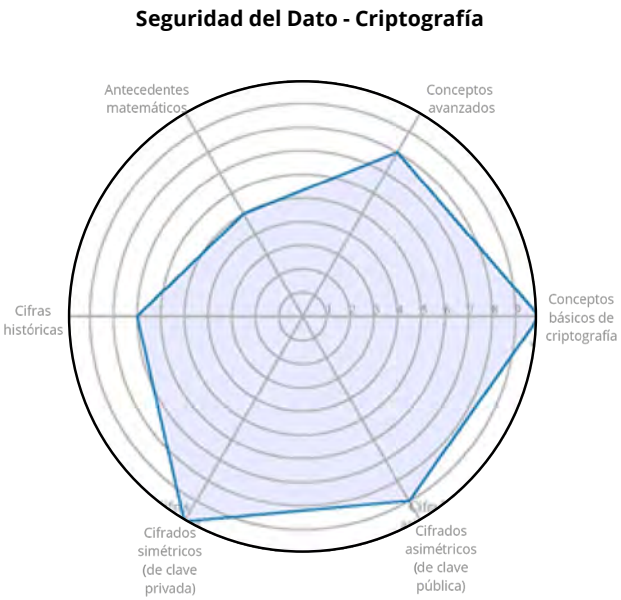


Figura 2: Soporte de temas de Criptografía

4.1.2. Análisis forense digital

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

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

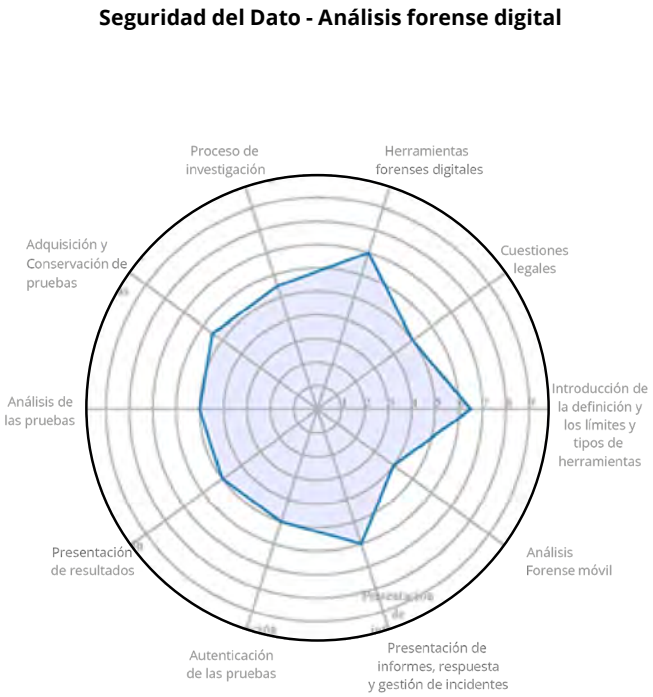


Figura 3: Soporte de temas de Análisis Forense Digital

4.1.3. Integridad y autenticación de datos

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

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

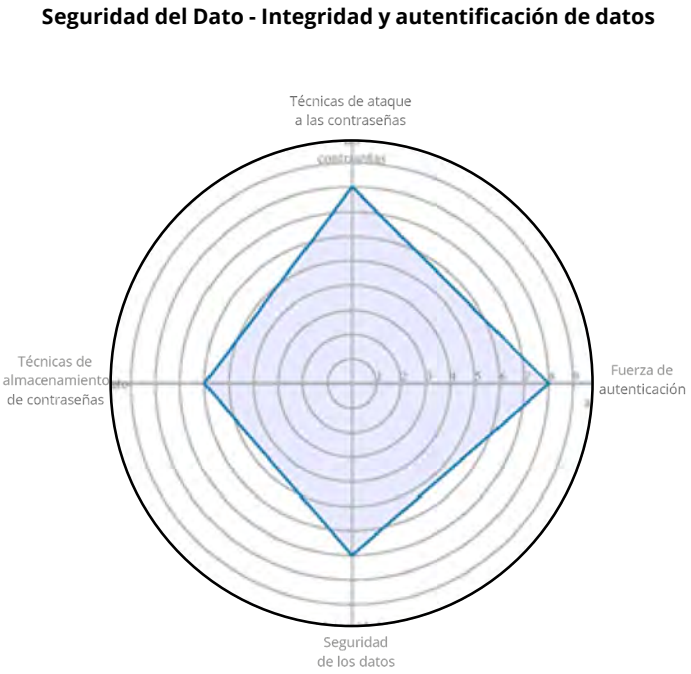


Figura 4: Soporte de temas de Integridad y autenticación de datos

4.1.4. Control de acceso

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

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

Seguridad del Dato - Control de acceso

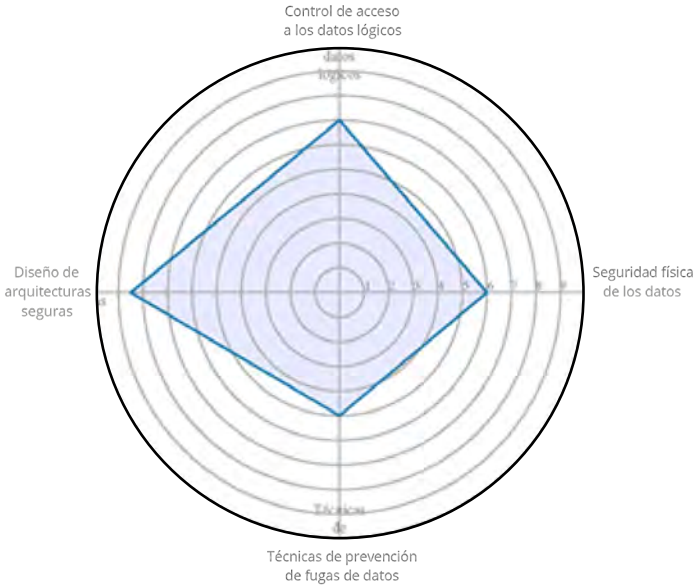


Figura 5: Soporte de temas de Control de Acceso

4.1.5. Protocolos de comunicación seguros

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

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

Seguridad del Dato - Protocolos de comunicación seguros

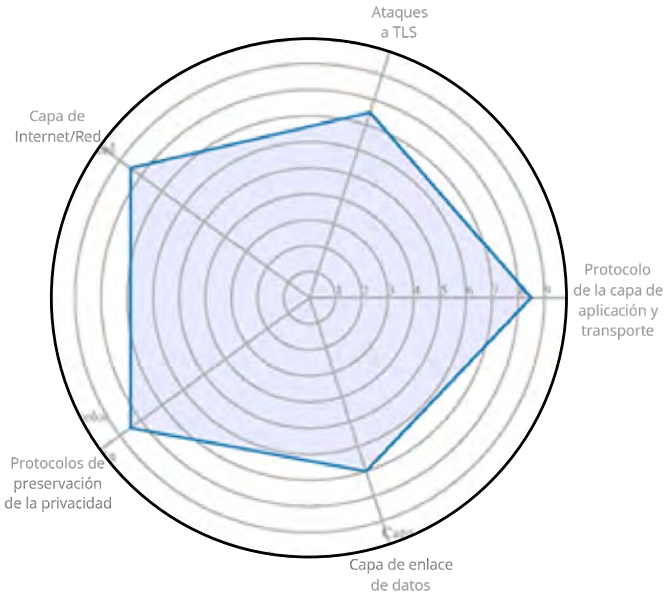


Figura 6: Soporte de temas de Protocolos de comunicación seguros

4.1.6. Criptoanálisis

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

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

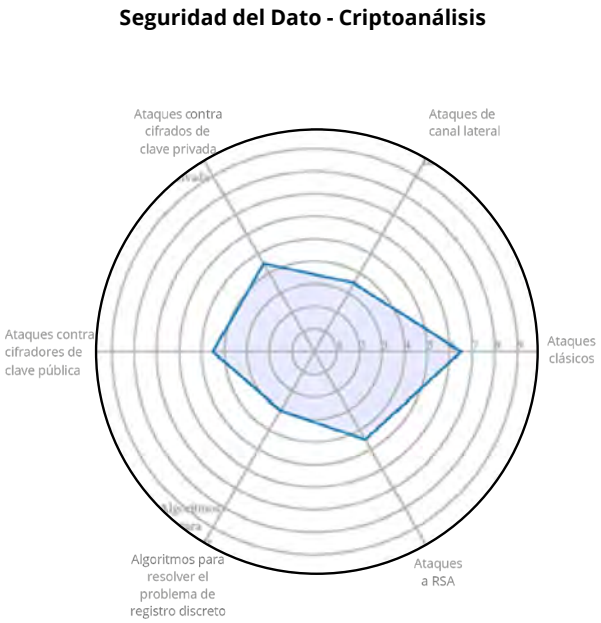


Figura 7: Soporte de temas de Criptoanálisis

4.1.7. Privacidad de datos

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

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

4.1.8. Seguridad del almacenamiento de la información

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

El estudio refleja un soporte **medio/alto** de los temas de esta unidad de conocimiento, exceptuando el enmascaramiento de datos, que tiene un soporte **bajo**. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 8: Soporte de temas de seguridad del almacenamiento de la información

4.2. Área de Conocimiento KA-2: Seguridad del software

Se centra en el desarrollo y la utilización de programas informáticos que preserven de forma fiable las propiedades de seguridad de la información y los sistemas que éstos aplican.

Esta área cubre como contenidos esenciales principios fundamentales de diseño, incluyendo el mínimo privilegio, el diseño abierto y la abstracción, requisitos de seguridad y su rol en el diseño, cuestiones de implementación, pruebas / testing estáticas y dinámicas, configuración y aplicación de parches y ética, especialmente en el desarrollo, las pruebas y la divulgación de vulnerabilidades. Por ello, se divide en las siguientes unidades de conocimiento:

- Principios fundamentales
- Diseño
- Implementación
- Análisis y pruebas
- Despliegue y mantenimiento
- Documentación
- Ética

4.2.1. Principios fundamentales

La unidad de conocimiento de principios fundamentales incluye los aspectos de mínimo privilegio, fallo seguro (por defecto), mediación completa, separación de privilegios, minimizar la superficie de confianza, economía de mecanismo, minimización de la implementación (mecanismo menos común), mínima sorpresa (aceptación psicológica), diseño abierto, diseño por capas (defensa en profundidad), abstracción, modularidad, vinculación completa y diseño para la iteración.

El estudio refleja un soporte **medio/alto** en la mayor parte de los temas de esta unidad de conocimiento, exceptuando algunos de ellos que tienen un soporte **medio/bajo**. El detalle de soporte de cada tema se muestra en la figura siguiente.

Seguridad del Software - Principios fundamentales

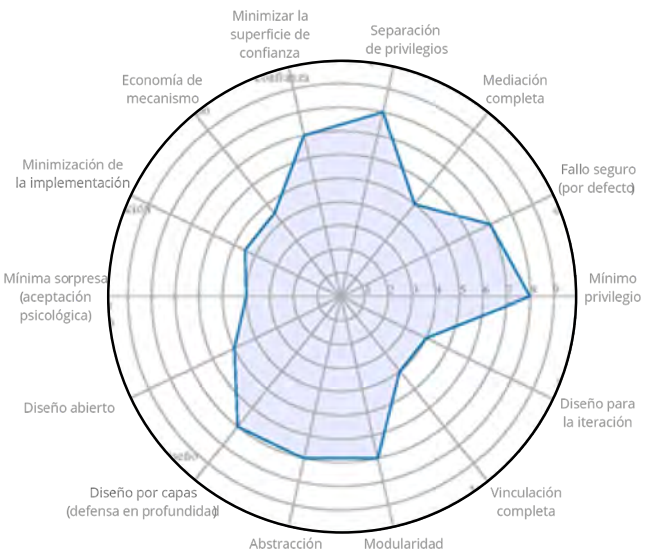


Figura 9: Soporte de temas de principios fundamentales

4.2.2. Diseño

La unidad de conocimiento de diseño incluye los aspectos de derivación de los requisitos de seguridad, especificación de los requisitos de seguridad, ciclo de vida del desarrollo del software ciclo de vida del desarrollo de la seguridad y lenguajes de programación y lenguajes de tipo seguro.

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

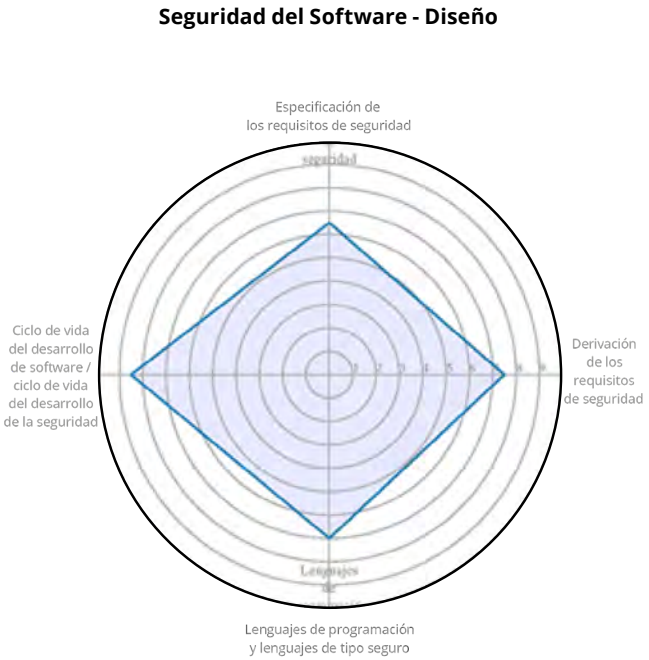


Figura 10: Soporte de temas de diseño

4.2.3. Implementación

La unidad de conocimiento de implementación incluye los aspectos de validación de la entrada y comprobación de su representación, utilización correcta de las API, uso de las funciones de seguridad, comprobación de las relaciones de tiempo y estado, manejar adecuadamente las excepciones y los errores, programación robusta, encapsular estructuras y módulos así como tener en cuenta el entorno.

El estudio refleja un soporte **alto** en la mayor parte de los temas de esta unidad de conocimiento, exceptuando algunos de ellos que tienen un soporte medio. El detalle de soporte de cada tema se muestra en la figura siguiente.

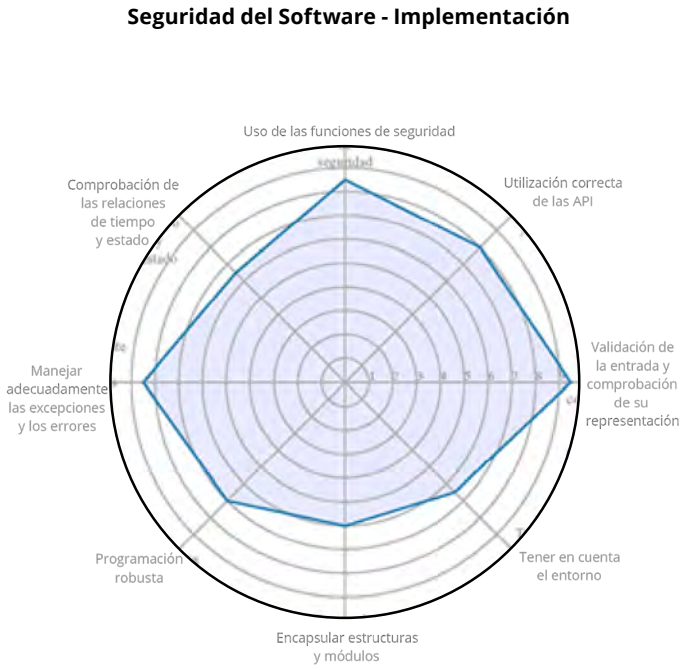


Figura 11: Soporte de temas de implementación

4.2.4. Análisis y pruebas

La unidad de conocimiento de análisis y pruebas incluye los aspectos de análisis estático y dinámico, pruebas unitarias, pruebas de integración y pruebas de software.

El estudio refleja un soporte **medio** en los temas de esta unidad de conocimiento, excepto el tema de análisis estático y dinámico, que tiene un soporte **alto**. El detalle de soporte de cada tema se muestra en la figura siguiente.

Seguridad del Software - Análisis y pruebas

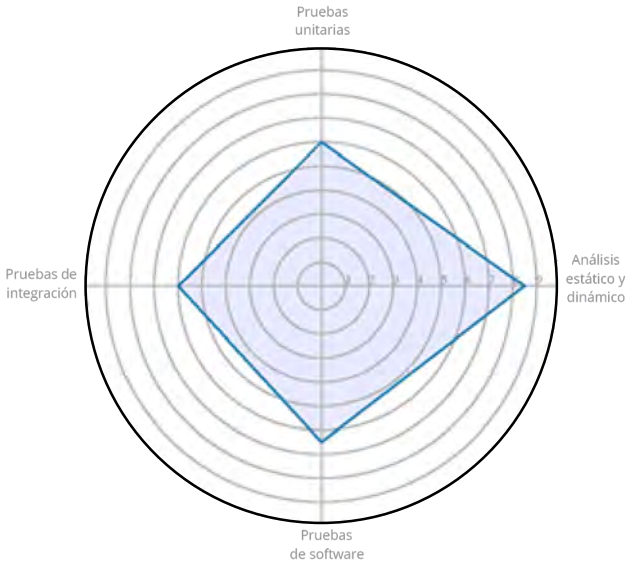


Figura 12: Soporte de temas de análisis y pruebas

4.2.5. Despliegue y mantenimiento

La unidad de conocimiento de despliegue y mantenimiento incluye los aspectos de configuración, parcheado y ciclo de vida de la vulnerabilidad, comprobación del entorno, DevOps y desmantelamiento/retirada.

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

Seguridad del Software - Despliegue y mantenimiento

Figura 13: Soporte de temas de despliegue y mantenimiento

4.2.6. Documentación

La unidad de conocimiento de documentación incluye los aspectos de documentos de instalación, guías y manuales de usuario, documentación de aseguramiento/garantía y documentación sobre seguridad.

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

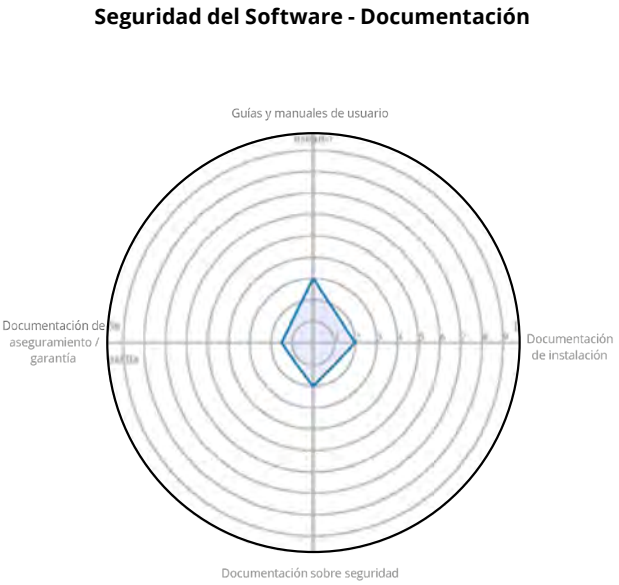


Figura 14: Soporte de temas de documentación

4.2.7. Ética

La unidad de conocimiento de ética incluye los aspectos de cuestiones éticas en el desarrollo de software, aspectos sociales del desarrollo de software, aspectos legales del desarrollo de software, revelación de vulnerabilidades y qué, cuándo y por qué probar.

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

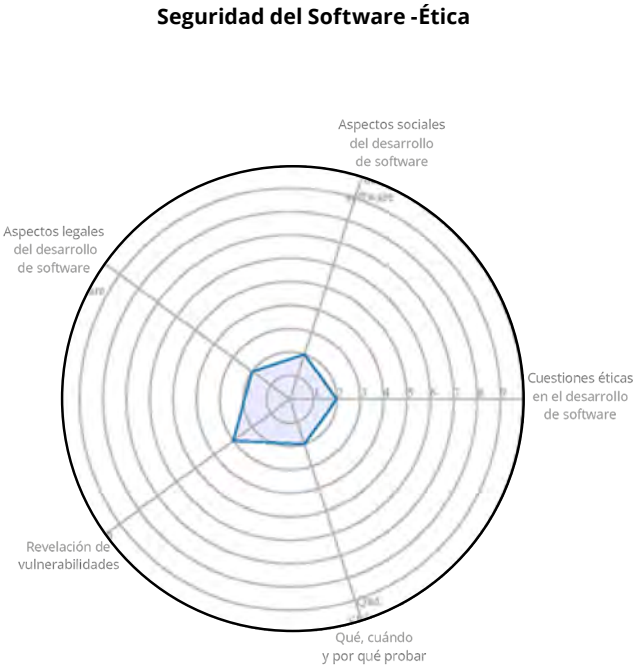


Figura 15: Soporte de temas de ética

4.3. Área de Conocimiento KA-3: Seguridad de los componentes

Se centra en el ciclo de vida de los componentes, desde el diseño, la adquisición, las pruebas, y el análisis hasta el mantenimiento de componentes integrados en sistemas.

Esta área cubre como contenidos esenciales las vulnerabilidades de los componentes del sistema, ciclo de vida de los componentes, principios de diseño de componentes seguros, seguridad en la gestión de la cadena de suministro, pruebas de seguridad e ingeniería inversa. Por ello, se divide en las siguientes unidades de conocimiento:

- Diseño de componentes
- Adquisición de componentes
- Pruebas de componentes
- Ingeniería inversa de componentes

4.3.1. Diseño de componentes

La unidad de diseño de componentes incluye los aspectos de seguridad en el diseño de componentes, principios de diseño seguro de componentes, Identificación de componentes, técnicas de ingeniería inversa, mitigación de ataques de canal lateral y tecnologías antimanipulación.

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

Seguridad de los Componentes -Diseño de componentes

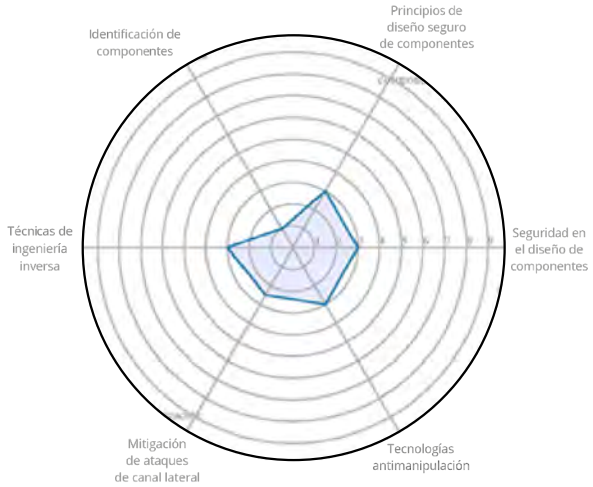


Figura 16: Soporte de temas de diseño de componentes

4.3.2. Adquisición de componentes

La unidad de adquisición de componentes incluye los aspectos de riesgos de la cadena de suministro, seguridad de la cadena de suministro e investigación de proveedores.

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

Seguridad de los Componentes -Adquisición de componentes

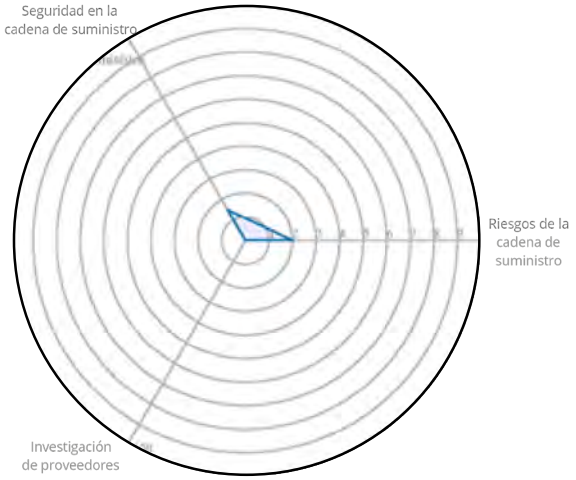


Figura 17: Soporte de temas de adquisición de componentes

4.3.3. Pruebas de componentes

La unidad de pruebas de componentes incluye los aspectos de principios de las pruebas unitaria y pruebas de seguridad.

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

Seguridad de los Componentes -Pruebas de componentes

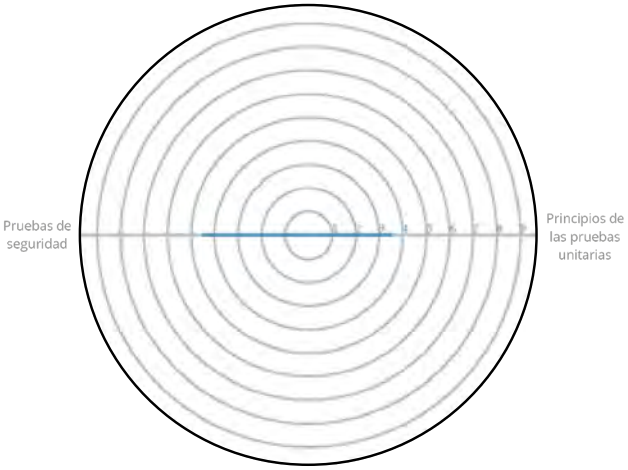


Figura 18: Soporte de temas de pruebas de componentes

4.3.4. Ingeniería inversa de componentes

La unidad de Ingeniería inversa de componentes incluye los aspectos de ingeniería inversa del diseño, ingeniería inversa del hardware e ingeniería inversa del software.

El estudio refleja un soporte **bajo** en los temas de esta unidad de conocimiento, exceptuando el tema de ingeniería inversa del software que cuenta con un soporte **medio**. El detalle de soporte de cada tema se muestra en la figura siguiente.

Seguridad de los Componentes - Ingeniería inversa de componentes

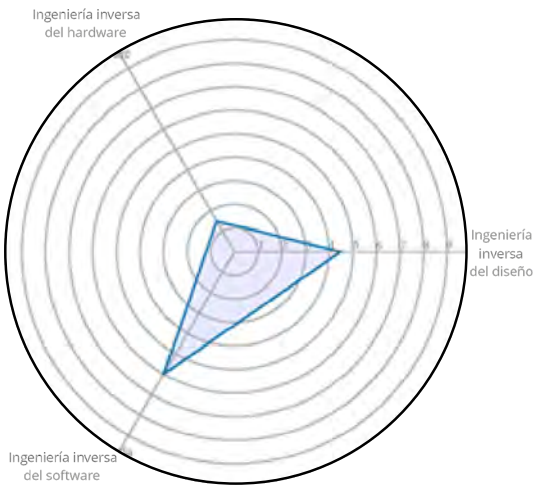


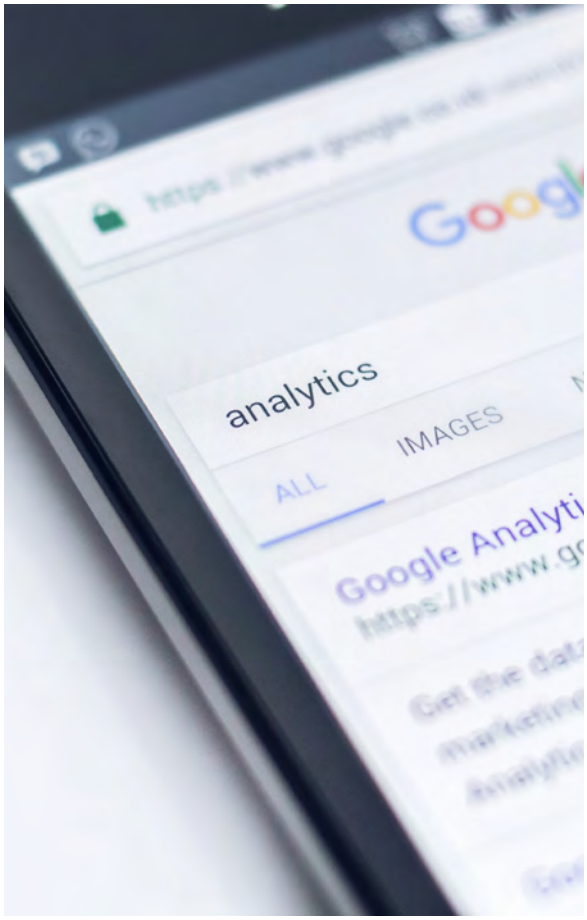
Figura 19: Soporte de temas de ingeniería inversa de componentes

4.4. Área de Conocimiento KA-4: Seguridad de las conexiones

Se centra en la seguridad de las conexiones establecidas entre componentes, incluyendo las conexiones físicas y lógicas.

Esta área cubre como contenidos esenciales los sistemas, arquitectura, modelos y normas, interfaces de componentes físicos, interfaces de componentes de software, ataques de conexión y ataques de transmisión. Por ello, se divide en las siguientes unidades de conocimiento:

- Medios físicos
- Interfaces físicas y conectores
- Arquitectura de hardware
- Arquitectura de sistemas distribuidos
- Arquitectura de red
- Implementación de redes
- Servicios de red
- Defensa de la red



4.4.1. Medios físicos

La unidad de medios físicos incluye los aspectos de transmisión en un medio, medios compartidos y punto a punto, modelos de compartición y tecnologías comunes.

El estudio refleja un soporte **nulo** en los temas de esta unidad de conocimiento como se ve en el detalle de soporte de cada tema mostrado en la figura siguiente. Estos temas son asumidos como conocimientos previos para estos estudios superiores especializados.

Seguridad de las Conexiones -Medios físicos

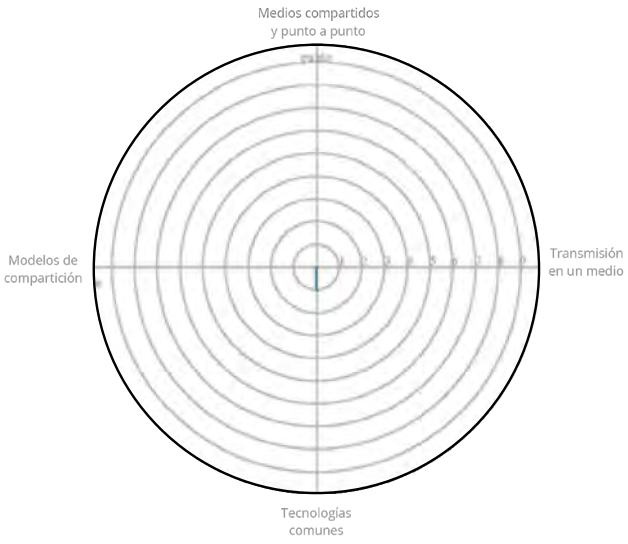


Figura 20: Soporte de temas de medios físicos

4.4.2. Interfaces físicas y conectores

La unidad de interfaces físicas y conectores incluye los aspectos de características y materiales del hardware, estándares y conectores comunes.

El estudio refleja un soporte **nulo** en los temas de esta unidad de conocimiento como se ve en el detalle de soporte de cada tema mostrado en la figura siguiente. Estos temas son asumidos como conocimientos previos para estos estudios superiores especializados.

Seguridad de las Conexiones - Interfaces físicas y conectores

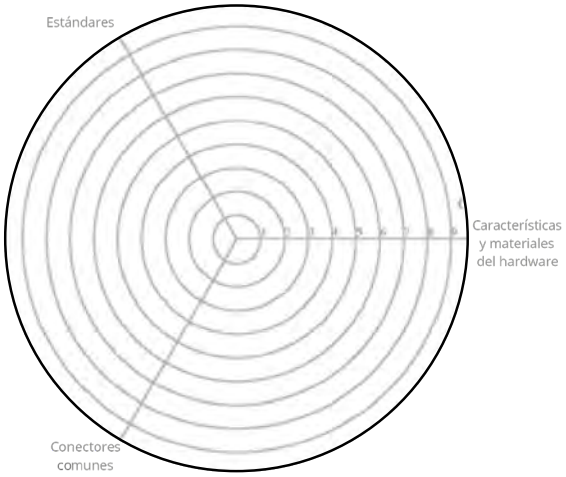
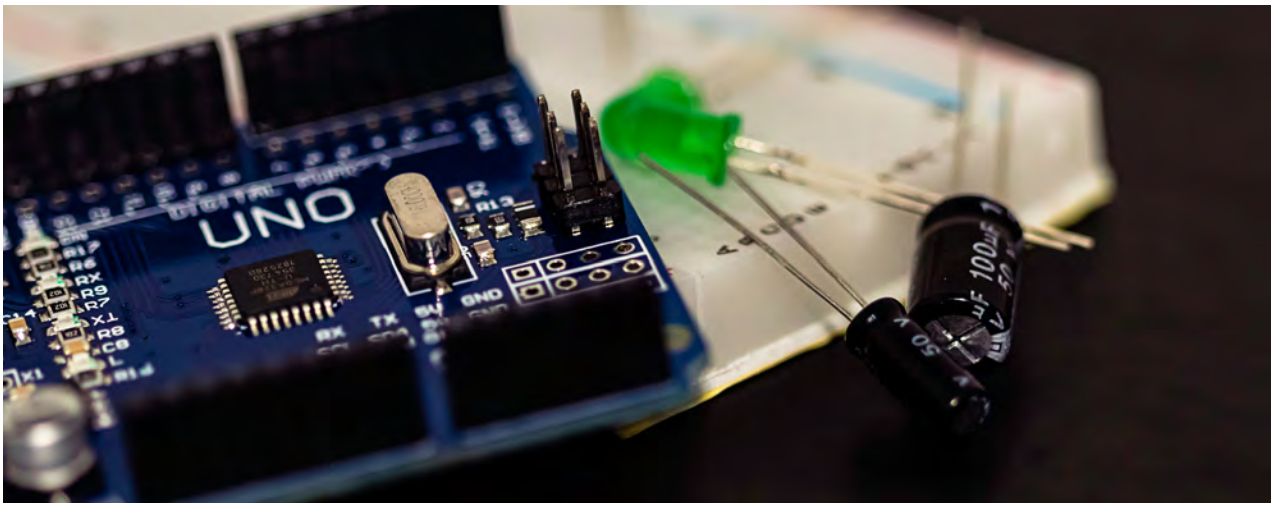


Figura 21: Soporte de temas de Interfaces físicas y conectores



4.4.3. Arquitectura de hardware

La unidad de arquitectura de hardware incluye los aspectos de arquitecturas estándar, estándares de interfaz de hardware y arquitecturas comunes.

El estudio refleja un soporte **nulo** en los temas de esta unidad de conocimiento, como se ve en el detalle de soporte de cada tema mostrado en la figura siguiente. Estos temas son asumidos como conocimientos previos para estos estudios superiores especializados.

Seguridad de las Conexiones - Arquitectura de hardware

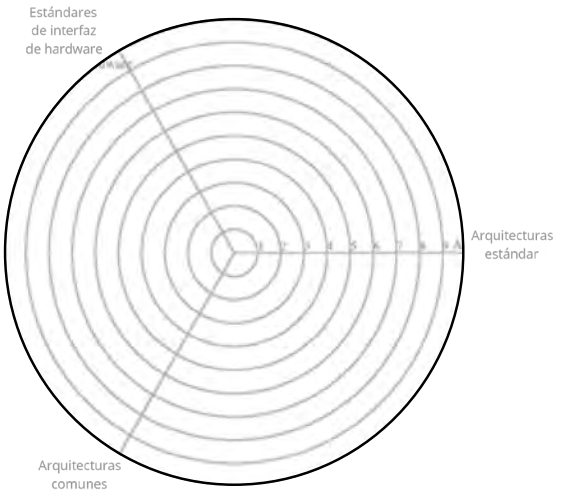


Figura 22: Soporte de temas de arquitectura de hardware

4.4.4. Arquitectura de sistemas distribuidos

La unidad de arquitectura de sistemas distribuidos incluye los aspectos de conceptos generales, web global, internet; protocolos y estratificación, computación de alto rendimiento (superordenadores), hipervisores e implementaciones de computación en la nube y vulnerabilidades y ejemplos de explotaciones.

El estudio refleja un soporte desigual en los temas de esta unidad de conocimiento como se ve en el detalle de soporte de cada tema mostrado en la figura siguiente. El tema de vulnerabilidades tiene un soporte **completo**, mientras que los temas de conceptos generales e Internet tienen un soporte **medio/alto** y el resto un soporte **bajo**. La mayor parte de estos temas son asumidos como conocimientos previos para estos estudios superiores especializados.

Seguridad de las Conexiones - Arquitectura de sistemas distribuidos

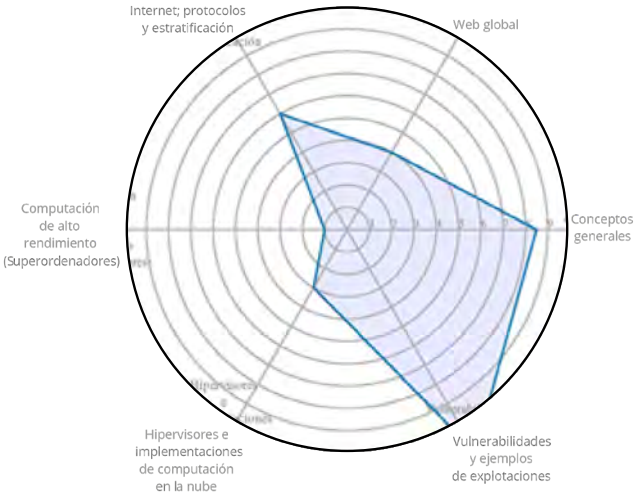


Figura 23: Soporte de temas de arquitectura de sistemas distribuidos

4.4.5. Arquitectura de red

La unidad de arquitectura de red incluye los aspectos de conceptos generales, arquitecturas comunes, reenvío / enrutamiento, conmutación/recuperación, tendencias emergentes y virtualización y arquitectura de hipervisor virtual.

El estudio refleja un soporte **medio/bajo** en los temas de esta unidad de conocimiento como se ve en el detalle de soporte de cada tema mostrado en la figura siguiente. La mayor parte de estos temas son asumidos como conocimientos previos para estos estudios superiores especializados.

Seguridad de las Conexiones - Arquitectura de red

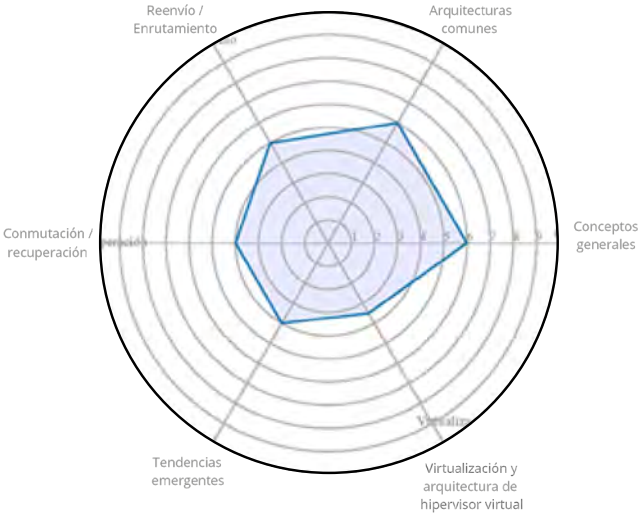


Figura 24: Soporte de temas de arquitectura de red

4.4.6. Implementación de redes

La unidad de implementación de redes incluye los aspectos de redes IEEE 802/ISO, redes IETF y TCP/IP, integración práctica y protocolos de cola y vulnerabilidades y ejemplos de explotaciones.

El estudio refleja un soporte desigual en los temas de esta unidad de conocimiento como se ve en el detalle de soporte de cada tema mostrado en la figura siguiente. El tema de vulnerabilidades tiene un soporte **alto**, mientras que el resto de temas tienen un soporte **medio/bajo**. La mayor parte de estos temas son asumidos como conocimientos previos para estos estudios superiores especializados.

Seguridad de las Conexiones - Implementación de redes

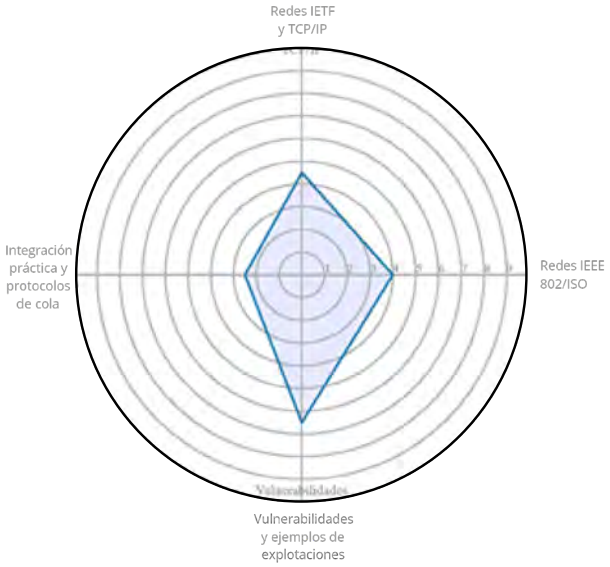


Figura 25: Soporte de temas de implementación de redes

4.4.7. Servicios de red

La unidad de servicios de red incluye los aspectos de concepto de servicio, modelos de servicio (cliente-servidor, peer-to-peer), conceptos de protocolo de servicio (IPC, API, IDL), arquitecturas comunes de comunicación de servicios, virtualización de servicios y vulnerabilidades y ejemplos de explotaciones.

El estudio refleja un soporte desigual en los temas de esta unidad de conocimiento como se ve en el detalle de soporte de cada tema mostrado en la figura siguiente. El tema de vulnerabilidades tiene un soporte **completo**, mientras que el resto de temas tienen un soporte **medio/bajo**. La mayor parte de estos temas son asumidos como conocimientos previos para estos estudios superiores especializados.

Seguridad de las Conexiones - Servicios de red

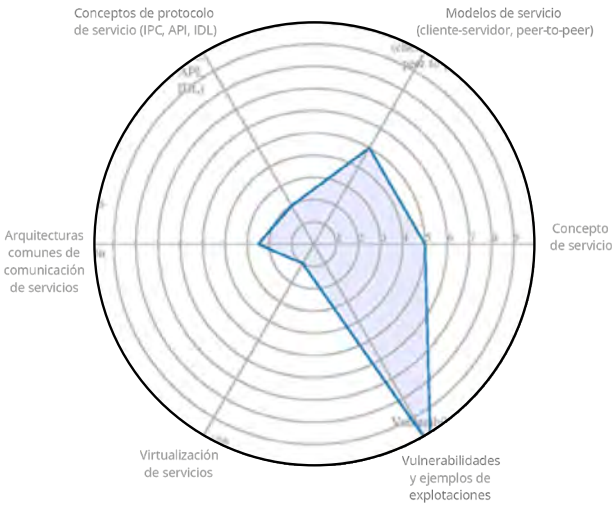


Figura 26: Soporte de temas de servicios de red

4.4.8. Defensa de la red

La unidad de defensa de red incluye los aspectos de endurecimiento de la red, Implantación de IDS/IPS, implantación de cortafuegos y redes privadas virtuales (VPN), defensa en profundidad, Honeypots y honeynets, monitorización de la red, análisis del tráfico de la red, minimización de la exposición (superficie de ataque y vectores), control de acceso a la red (interno y externo), redes perimetrales (zonas desmilitarizadas o DMZ)/servidores proxy, desarrollo y aplicación de políticas de red, procedimientos de ataque (por ejemplo, secuestro de sesión, hombre en el medio) y búsqueda de amenazas y aprendizaje automático.

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

Seguridad de las Conexiones - Defensa de la red

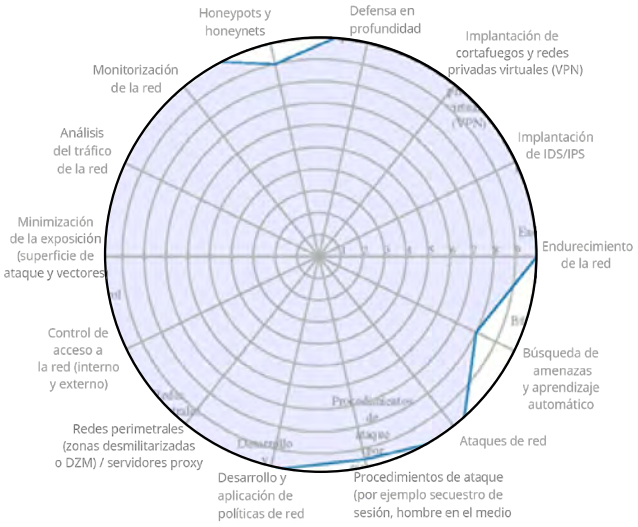


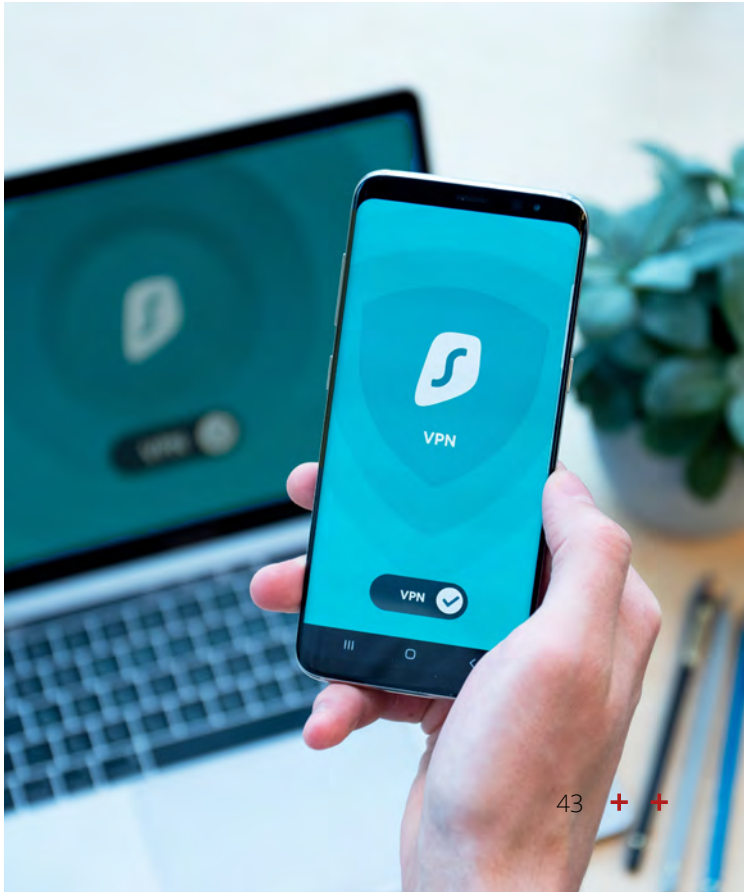
Figura 27: Soporte de temas de defensa de la red

4.5. Área de Conocimiento KA-5: Seguridad de sistemas

Se centra en la seguridad de sistemas compuesto de conexiones, componentes y software.

Esta área cubre como contenidos esenciales un enfoque holístico, política de seguridad, autenticación, control de acceso, supervisión, recuperación, pruebas y documentación. Por ello, se divide en las siguientes unidades de conocimiento:

- Pensamiento sistémico
- Gestión de sistemas
- Acceso al sistema
- Control del sistema
- Retirada del sistema
- Prueba del sistema
- Ejemplos de arquitecturas de sistemas



4.5.1. Pensamiento sistémico

La unidad de pensamiento sistémico incluye los aspectos de definición de sistemas: aproximaciones globales al diseño de sistemas, seguridad de sistemas de propósito general, seguridad de Sistemas de propósito específico, modelos de amenazas, análisis de requisitos, principios fundamentales de seguridad de sistemas, y desarrollo de pruebas.

El estudio refleja un soporte **bajo** en los temas de esta unidad de conocimiento. La mayor parte de estos temas son asumidos como conocimientos previos para estos estudios superiores especializados El detalle de soporte de cada tema se muestra en la figura siguiente.

Seguridad de Sistemas - Pensamiento sistémico

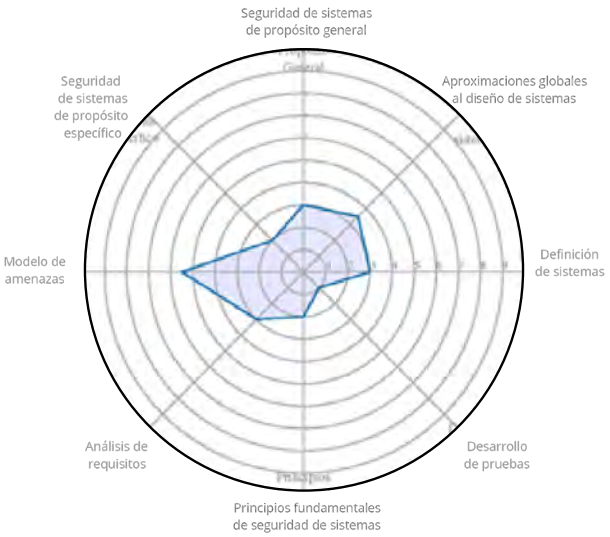


Figura 28: Soporte de temas de pensamiento sistémico

4.5.2. Gestión de sistemas

La unidad de gestión de sistemas incluye los aspectos de modelos de política, composición de políticas, uso de la automatización, parcheo y ciclo de vida de la vulnerabilidad, operación, puesta en marcha y desmantelamiento, amenaza interna, documentación y sistemas y procedimientos.

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

Seguridad de Sistemas - Gestión de sistemas

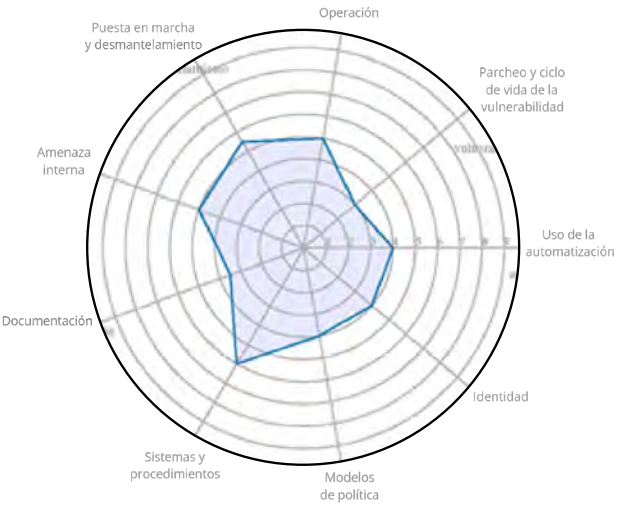


Figura 29: Soporte de temas de gestión de sistemas

4.5.3. Acceso al sistema

La unidad de acceso al sistema incluye los aspectos de métodos de autenticación e identidad.

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

Figura 30: Soporte de temas de acceso al sistema

4.5.4. Control del sistema

La unidad de control del sistema incluye los aspectos de control de acceso, modelos de autorización, detección de intrusos, ataques, defensas, auditoría, malware, modelos de vulnerabilidad, pruebas de penetración, análisis forense y recuperación, resiliencia.

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

Figura 31: Soporte de temas de control del sistema

4.5.5. Retirada del sistema

La unidad de retirada del sistema incluye los aspectos de desmantelamiento y eliminación.

El estudio refleja un soporte nulo en los temas de esta unidad de conocimiento.

4.5.6. Prueba del sistema

La unidad de prueba del sistema incluye los aspectos de validación de los requisitos, validación de la composición de los componentes, pruebas unitarias frente a pruebas del sistema y verificación formal de sistemas.

El estudio refleja un soporte **muy bajo** en los temas de esta unidad de conocimiento. La mayor parte de estos temas son asumidos como conocimientos previos para estos estudios superiores especializados. El detalle de soporte de cada tema se muestra en la figura siguiente.

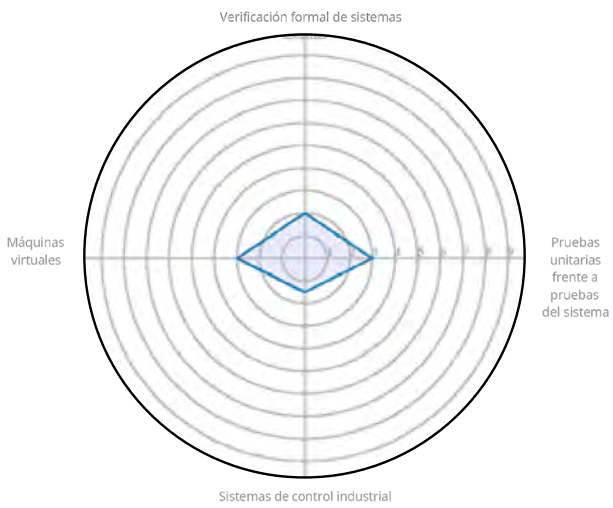


Figura 32: Soporte de temas de prueba del sistema

4.5.7. Ejemplos de arquitecturas de sistemas

La unidad de ejemplos de arquitecturas de sistemas incluye los aspectos de máquinas virtuales, sistemas de control industrial, internet de las cosas, sistemas embebidos, sistemas móviles, sistemas autónomos y sistemas de propósito general.

El estudio refleja un soporte **medio/bajo** en los temas de esta unidad de conocimiento. La mayor parte de estos temas son asumidos como conocimientos previos para estos estudios superiores especializados. El detalle de soporte de cada tema se muestra en la figura siguiente.

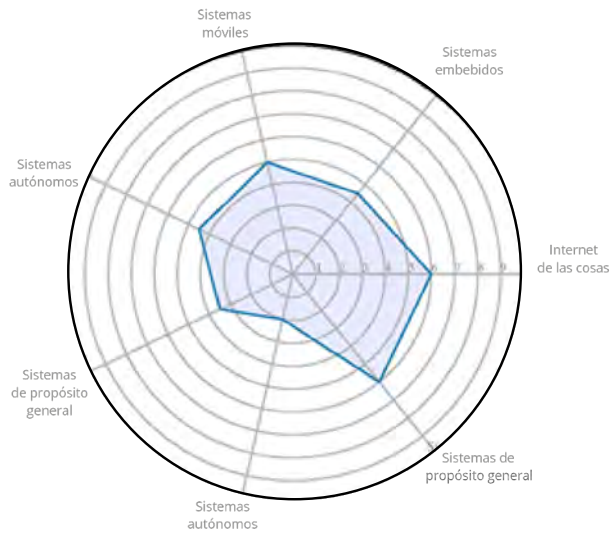


Figura 33: Soporte de temas de ejemplos de arquitecturas de sistemas

4.6. Área de Conocimiento KA-6: Seguridad del ser humano

Se centra en garantizar la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos pertenecientes a una persona (dispositivos personales) o a una organización.

Esta área cubre como contenidos esenciales la gestión de la identidad, ingeniería social, conciencia y comprensión. privacidad y seguridad del comportamiento social y privacidad y seguridad de los datos personales. Por ello, se divide en las siguientes unidades de conocimiento:

- Gestión de la identidad
- Ingeniería social
- Cumplimiento de las reglas/políticas/normas éticas de ciberseguridad
- Conciencia y comprensión
- Privacidad social y de comportamiento
- Privacidad y seguridad de los datos personales
- Seguridad y privacidad aplicables

4.6.1. Gestión de la identidad

La unidad de Gestión de la identidad incluye los aspectos de identificación y autenticación de personas y dispositivos, control de activos físicos y lógicos, identidad como servicio (Identity as a Service, IaaS), servicios de identidad de terceros y ataques al control de acceso y medidas de mitigación.

El estudio refleja un soporte desigual en los temas de esta unidad de conocimiento con soporte **alto** de identificación y autenticación de personas y dispositivos y ataques al control de acceso y medidas de mitigación y un soporte **medio/bajo** en el resto. El detalle de soporte de cada tema se muestra en la figura siguiente.

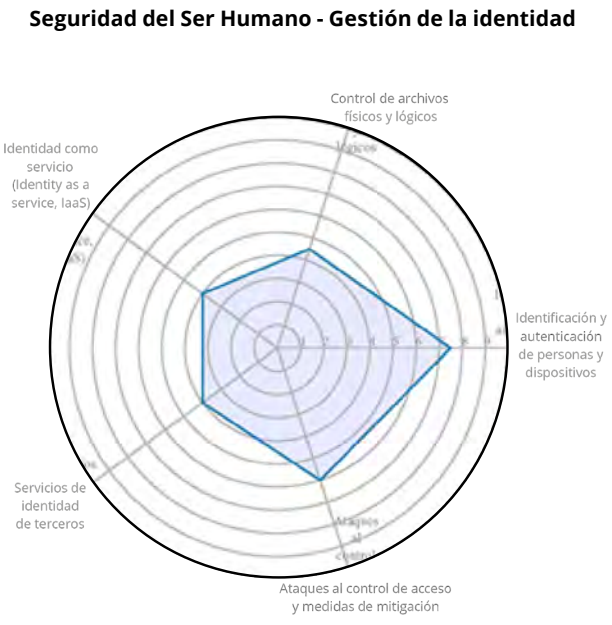


Figura 34: Soporte de temas de gestión de la identidad

4.6.2. Ingeniería social

La unidad de ingeniería social incluye los aspectos de tipos de ataques de ingeniería social, psicología de los ataques de ingeniería social, engañar a los usuarios y detección y mitigación de los ataques de ingeniería social.

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

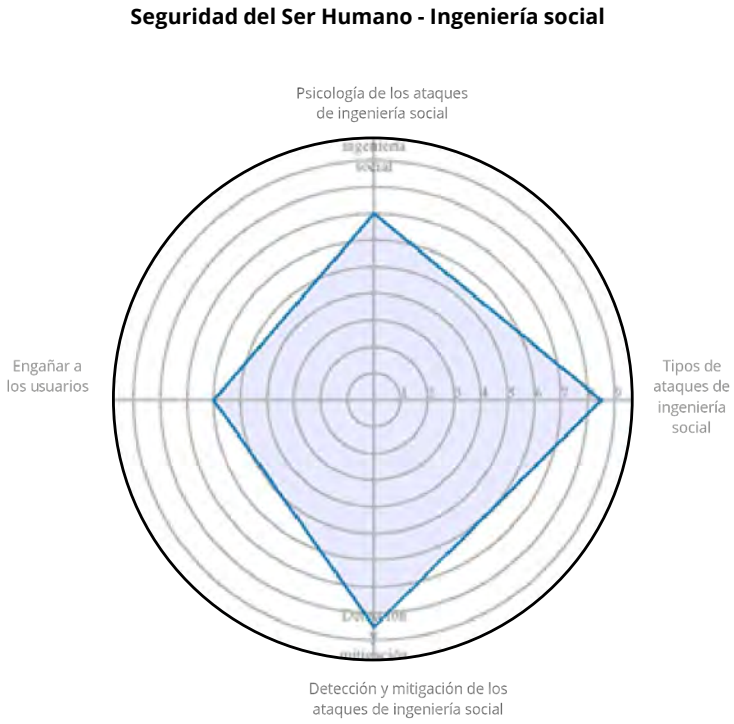


Figura 35: Soporte de temas de Ingeniería social

4.6.3. Cumplimiento de las reglas/políticas/normas éticas de ciberseguridad

La unidad de cumplimiento de las reglas/políticas/normas éticas de ciberseguridad incluye los aspectos de mal uso del sistema y mal comportamiento de los usuarios, aplicación y normas de comportamiento y comportamiento adecuado en condiciones de incertidumbre.

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

Figura 36: Soporte de temas de cumplimiento de las reglas/políticas/ normas éticas de ciberseguridad

4.6.4. Conciencia y comprensión

La unidad de conciencia y comprensión incluye los aspectos de percepción del riesgo y comunicación, ciberhigiene, educación de los usuarios en materia de ciberseguridad y conocimiento de las cibervulnerabilidades y amenazas.

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

Seguridad del Ser Humano - Conciencia y comprensión

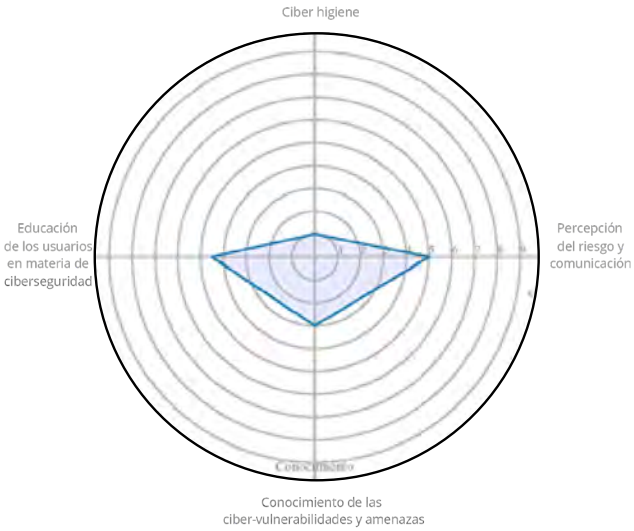


Figura 37: Soporte de temas de conciencia y comprensión

4.6.5. Privacidad social y de comportamiento

La unidad de privacidad social y de comportamiento incluye los aspectos de teorías sociales de la privacidad y seguridad en las redes sociales.

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

Seguridad del Ser Humano - Privacidad social y de comportamiento

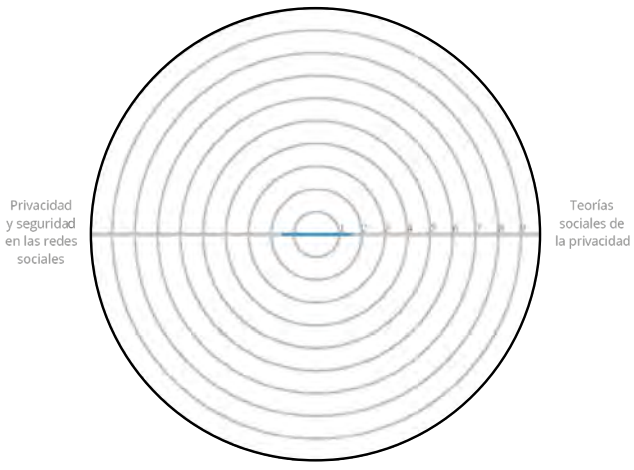


Figura 38: Soporte de temas de privacidad social y de comportamiento

4.6.6. Privacidad y seguridad de los datos personales

La unidad de privacidad y seguridad de los datos personales incluye los aspectos de datos personales sensibles y seguimiento personal y huella digital.

El estudio refleja un soporte desigual en los temas de esta unidad de conocimiento, siendo **alto** para datos personales sensibles y **bajo** para seguimiento personal y huella digital. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 39: Soporte de temas de privacidad y seguridad de los datos personales.

4.6.7. Seguridad y privacidad aplicables

La unidad de seguridad y privacidad aplicables incluye los aspectos de usabilidad y experiencia del usuario, factores de seguridad humana, conocimiento y comprensión de la política, política de privacidad y orientación e implicaciones del diseño.

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

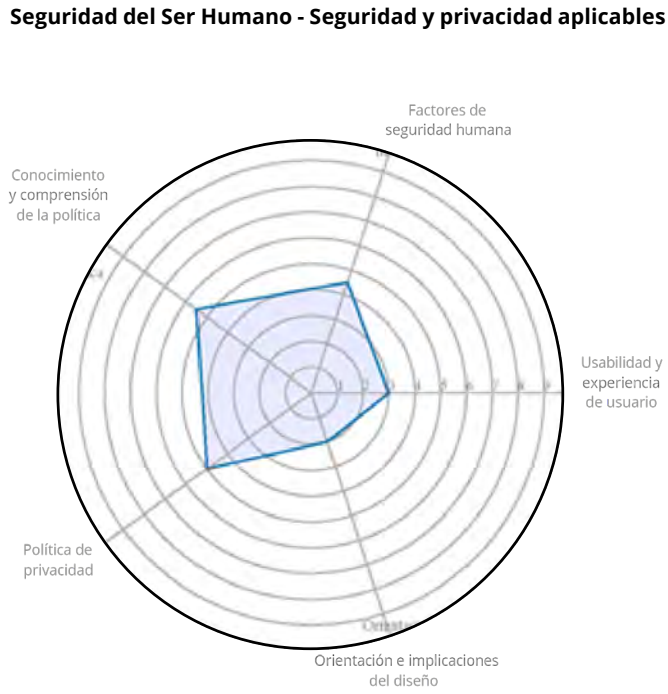
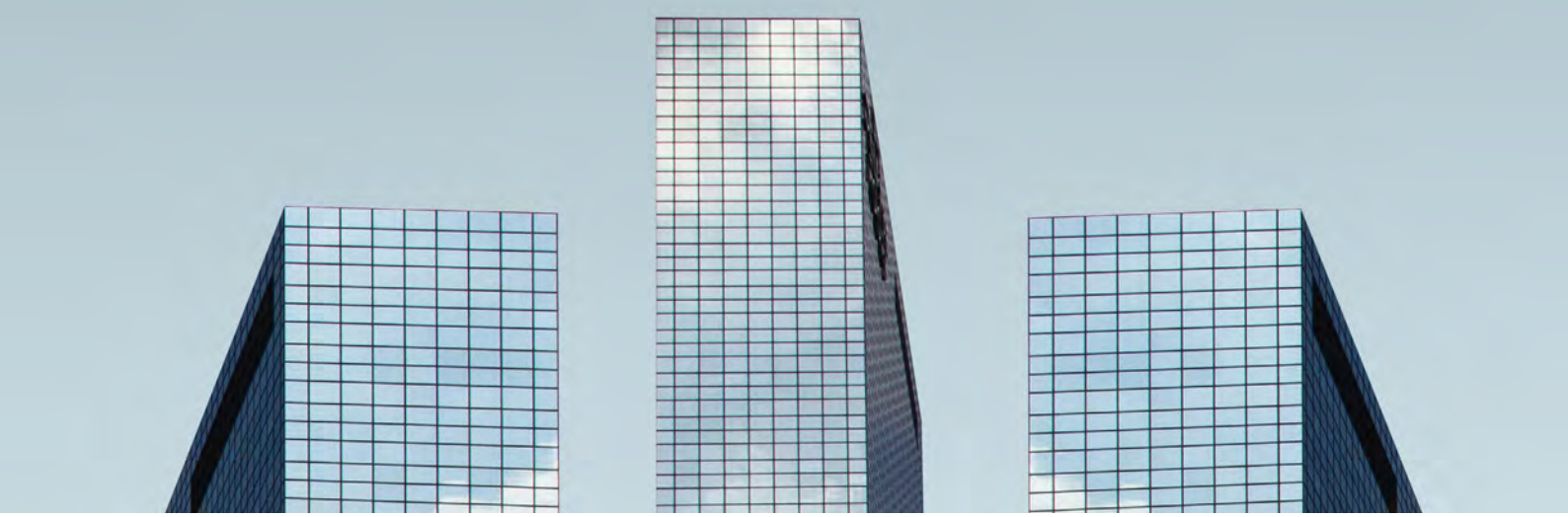


Figura 40: Soporte de temas de seguridad y privacidad aplicables



4.7. Área de Conocimiento KA-7: Seguridad de la organización

Se centra en proteger la información de las organizaciones y conlleva temas relativos a la gestión de riesgo.

Esta área cubre como contenidos la gestión de riesgos, la gobernanza y política, leyes, ética y cumplimiento y estrategia y planificación. Por ello, se divide en las siguientes unidades de conocimiento:

- Gestión de riesgos
- Gobernanza y política de seguridad
- Herramientas analíticas
- Administración de sistemas
- Planificación de la ciberseguridad
- Continuidad de negocio, recuperación de desastres y gestión de incidentes
- Gestión de programas de seguridad
- Seguridad del personal
- Operaciones de seguridad

4.7.1. Gestión de riesgos

La unidad de gestión de riesgos incluye los aspectos de identificación de riesgos, evaluación y análisis de riesgos, amenazas internas, modelos y metodologías de medición y evaluación de riesgos y control de riesgos.

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

Figura 41: Soporte de temas de gestión de riesgos

4.7.2. Gobernanza y política de seguridad

La unidad de gobernanza y política de seguridad incluye los aspectos de contexto organizativo, privacidad, leyes, ética y cumplimiento, gobernanza de la seguridad, comunicación a nivel ejecutivo y del consejo de administración y política de gestión.

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

Seguridad de la Organización - Gobernanza y política de seguridad

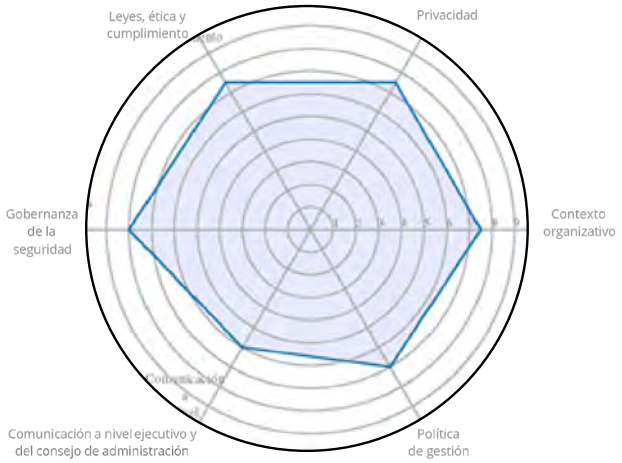


Figura 42: Soporte de temas de gobernanza y política de seguridad

4.7.3. Herramientas analíticas

La unidad de herramientas analíticas incluye los aspectos de medidas de rendimiento (métricas), análisis de datos e inteligencia de seguridad.

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

Seguridad de la Organización - Herramientas analíticas

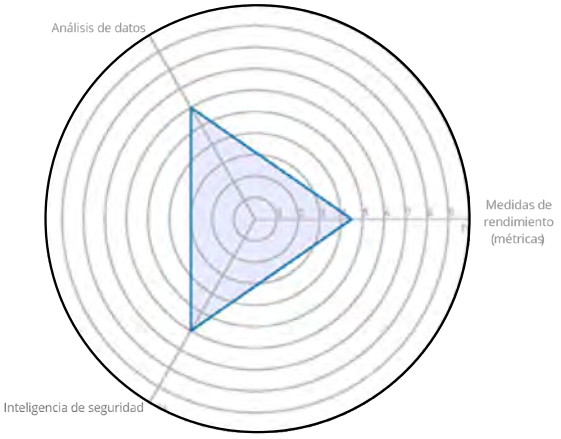


Figura 43: Soporte de temas de herramientas analíticas

4.7.4. Administración de sistemas

La unidad de administración de sistemas incluye los aspectos de administración de sistemas operativos, administración de sistemas de bases de datos, administración de redes, administración de la nube, administración de sistemas ciberfísicos, bastionado del sistema y disponibilidad.

El estudio refleja un soporte desigual en los temas de esta unidad de conocimiento, siendo **alto** para bastionado del sistema y **medio/bajo** para el resto. El detalle de soporte de cada tema se muestra en la figura siguiente.

Seguridad de la Organización - Administración de sistemas

Figura 44: Soporte de temas de administración de sistemas

4.7.5. Planificación de la ciberseguridad

La unidad de planificación de la ciberseguridad incluye los aspectos de planificación estratégica y gestión operativa y táctica.

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

Seguridad de la Organización - Planificación de la ciberseguridad

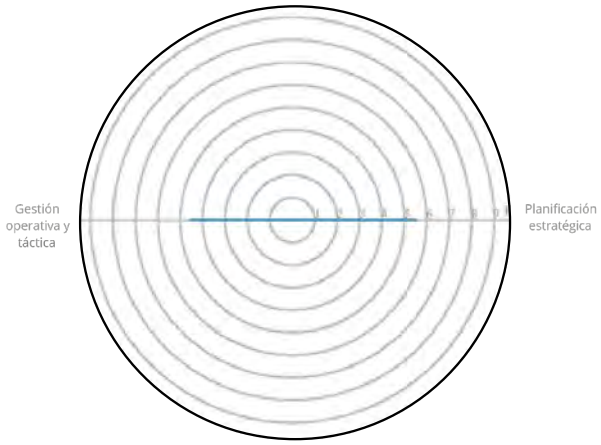


Figura 45: Soporte de temas de planificación de la ciberseguridad

4.7.6. Continuidad de negocio, recuperación de desastres y gestión de incidentes

La unidad de continuidad de negocio, recuperación de desastres y gestión de incidentes incluye solo un tema sobre ese aspecto, y el estudio refleja un soporte **alto** de dicho tema.

4.7.7. Gestión de programas de seguridad

La unidad de gestión de programas de seguridad incluye los aspectos de gestión de proyectos, gestión de recursos, métricas de seguridad y garantía y control de calidad.

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

Seguridad de la Organización - Gestión de programas de seguridad

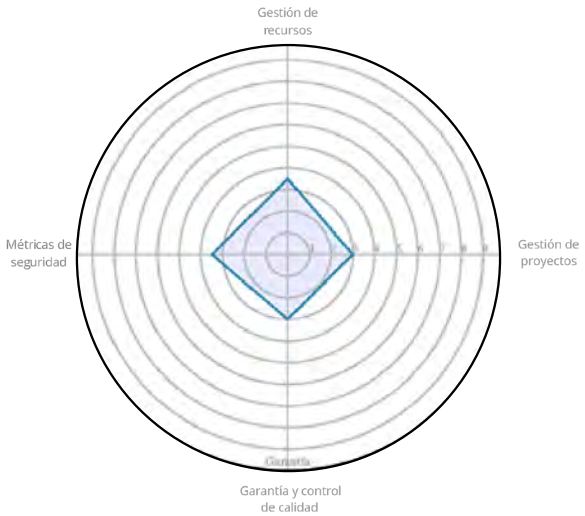


Figura 46: Soporte de temas de gestión de programas de seguridad

4.7.8. Seguridad del personal

La unidad de seguridad del personal incluye los aspectos de concienciación, formación y educación en materia de seguridad, prácticas de contratación de seguridad, prácticas de despido por motivos de seguridad, seguridad de terceros, seguridad en los procesos de revisión y cuestión especial en la privacidad de la información personal de los empleados.

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

Seguridad de la Organización - Seguridad del personal

Figura 47: Soporte de temas de seguridad del personal

4.7.9. Operaciones de seguridad

La unidad de operaciones de seguridad incluye los aspectos de convergencia de la seguridad y centros de operaciones de seguridad global (Global Security Operations Centers, GSOC).

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

Seguridad de la Organización - Operaciones de seguridad

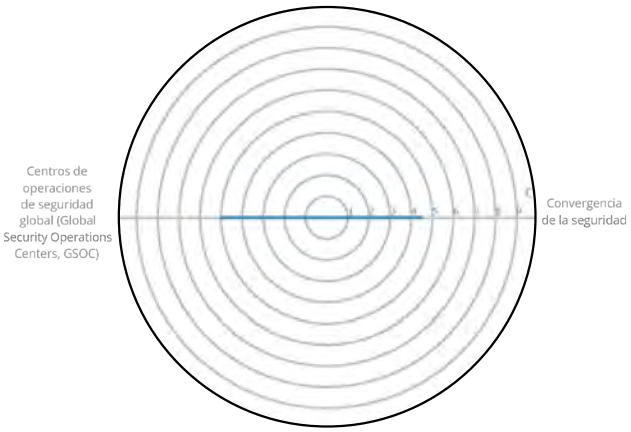


Figura 48: Soporte de temas de operaciones de seguridad

4.8. Área de Conocimiento KA-8: Seguridad en la sociedad

Se centra en aspectos de la ciberseguridad que repercuten de manera positiva o negativa al conjunto de la sociedad.

Esta área cubre como contenidos la ciberdelincuencia (Cibercrimen), ciberderecho (cyber law), ciberética, ciberpolítica y privacidad. Por ello, se divide en las siguientes unidades de conocimiento:

- Ciberdelincuencia
- Ciberderecho
- Ciberética
- Ciberpolítica
- Privacidad

4.8.1. Ciberdelincuencia

La unidad de ciberdelincuencia incluye los aspectos de comportamiento cibercriminal, ciberterrorismo, Investigaciones cibercriminales y economía de la ciberdelincuencia.

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

Figura 49: Soporte de temas de ciberdelincuencia

4.8.2. Ciberderecho

La unidad de ciberderecho incluye los aspectos de fundamentos constitucionales del ciberderecho, propiedad intelectual relacionada con la ciberseguridad, leyes de privacidad, derecho de la seguridad de los datos, leyes de piratería informática, pruebas digitales, contratos digitales, convenios multinacionales (acuerdos) y leyes transfronterizas de privacidad y seguridad de datos.

El estudio refleja un soporte desigual en los temas de esta unidad de conocimiento, siendo **altos** para los temas de leyes de privacidad, seguridad de datos y piratería informática y pruebas digitales y **bajos** para el resto de temas. El detalle de soporte de cada tema se muestra en la figura siguiente.

Figura 50: Soporte de temas de ciberderecho

4.8.3. Ciberética

La unidad de ciberética incluye los aspectos de definición de la ética, ética profesional y códigos de conducta, ética y equidad/diversidad, ética y derecho, autonomía/ética de los robots, ética y conflicto, hacking ético y marcos éticos y teorías normativas

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

Figura 51: Soporte de temas de ciberética

4.8.4. Ciberpolítica

La unidad de ciberpolítica incluye los aspectos de ciberpolítica internacional, ciberpolítica de la UE, impacto global, política de ciberseguridad y seguridad nacional, implicaciones económicas nacionales de la ciberseguridad y nuevas adyacencias a la diplomacia.

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

Figura 52: Soporte de temas de ciberpolítca

4.8.5. Privacidad

La unidad de privacidad incluye los aspectos de definición de la privacidad, derecho a la intimidad, protección de la intimidad, normas y actitudes en materia de privacidad, violación de la intimidad y la privacidad en las sociedades.

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

Figura 53: Soporte de temas de privacidad

4.9. Conclusiones y resumen del soporte del marco curricular ACM/IEEE

En las secciones anteriores se han proporcionado los datos más relevantes sobre el soporte que tiene el Marco Curricular ACM/IEEE en Ciberseguridad en los programas de formación superior con especialización en el área de ciberseguridad en España. Este soporte se ha basado en una consulta a una muestra significativa de universidades públicas y privadas participantes en este grupo de trabajo del Foro Nacional de Ciberseguridad, a través de CRUE y RENIC (Red de Excelencia Nacional de Investigación en Ciberseguridad). La consulta incluía:

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

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

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

De esta consulta, se recibieron informes provenientes de:

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

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

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

Las principales conclusiones de este estudio pueden resumirse de la siguiente forma:

• **Área de Seguridad del Dato**, con sus unidades de conocimiento de criptografía, análisis forense digital, integridad y autenticación de datos, control de acceso, protocolos de comunicación seguros, criptoanálisis, privacidad de datos, seguridad del almacenamiento de la información.

En general, todas las unidades de conocimiento tienen un soporte **alto o medio** por parte de los programas de formación superior. Solo temas concretos no son cubiertos, sobre todo aquellos relacionados con los modelos matemáticos, como los aspectos matemáticos relacionados con la criptografía, y aspectos de criptoanálisis.

• **Área de Seguridad del Software**, con sus unidades de conocimiento de principios fundamentales, diseño, implementación, análisis y pruebas, despliegue y mantenimiento, documentación y ética.

En general, las unidades de conocimiento principales tienen un soporte **alto o medio/alto** por parte de los programas de formación superior. Solo los temas relacionados con el despliegue y mantenimiento, documentación y ética tienen un soporte **bajo**.

• **Área de Seguridad de los Componentes**, con sus unidades de conocimiento de diseño de componentes, adquisición de componentes, pruebas de componentes e ingeniería inversa de componentes.

En general, las unidades de conocimiento tienen un soporte **bajo** por parte de los programas de formación superior, exceptuando el tema de ingeniería inversa software que es soportado con un nivel **medio**.

• **Área de Seguridad de las Conexiones**, con sus unidades de conocimiento de medios físicos, interfaces físicas y conectores, arquitectura de hardware, arquitectura de sistemas distribuidos, arquitectura de red, implementación de redes, servicios de red y defensa de la red.

Las unidades de conocimiento relacionadas con medios físicos, interfaces físicas y conectores y arquitectura de hardware tienen un soporte **nulo** por parte de los programas de formación superior ya que son considerados como conocimientos previos requeridos. Los temas de arquitectura de sistemas distribuidos, arquitectura de red, implementación de redes y servicios de red tienen un soporte **medio**, ya que se imparten, pero siguen siendo considerados como conocimientos previos. Sin embargo, los temas relacionados con las vulnerabilidades y la unidad de conocimiento de defensa de la red tienen un soporte **completo** en estos programas superiores de formación.

• **Área de Seguridad de Sistemas**, con sus unidades de conocimiento de pensamiento sistémico, gestión de sistemas, acceso al sistema, control del sistema, retirada del sistema, prueba del sistema y ejemplos de arquitecturas de sistemas.

El soporte de estas unidades de conocimiento es dispar. Por un lado, existen unidades de conocimientos con un soporte **nulo o muy bajo** ya que son consideradas como conocimientos previos, tales como pensamiento sistémico, pruebas del sistema y ejemplos de arquitecturas de sistemas. Por otro, se aprecia un soporte **medio** de la unidad de conocimiento de gestión de sistemas y un soporte **alto o muy alto** de las unidades de conocimiento de acceso al sistema y control del sistema. La unidad de conocimiento de retirada del sistema tiene un soporte **nulo**, no es tratada por ninguno de los programas consultados.

• **Área de Seguridad del Ser Humano**, con sus unidades de conocimiento de gestión de la identidad, ingeniería social, cumplimiento de las reglas / políticas / normas éticas de ciberseguridad, conciencia y comprensión, privacidad social y de comportamiento, privacidad y seguridad de los datos personales y seguridad y privacidad aplicables.

El soporte de estas unidades de conocimiento es dispar: Por un lado, existen unidades de conocimientos con un soporte **alto o medio**, como la gestión de la identidad, ingeniería social y privacidad y seguridad de los datos personales, y un soporte **bajo o medio/bajo** en el resto de unidades de conocimiento: cumplimiento de las reglas/políticas/normas éticas de ciberseguridad, conciencia y comprensión, privacidad social y de comportamiento y seguridad y privacidad aplicables.

• **Área de Seguridad de la Organización**, con sus unidades de conocimiento de gestión de riesgos, gobernanza y política de seguridad, herramientas analíticas, administración de sistemas, planificación de la ciberseguridad, continuidad de negocio, recuperación de desastres y gestión de incidentes, gestión de programas de seguridad, seguridad del personal y operaciones de seguridad.

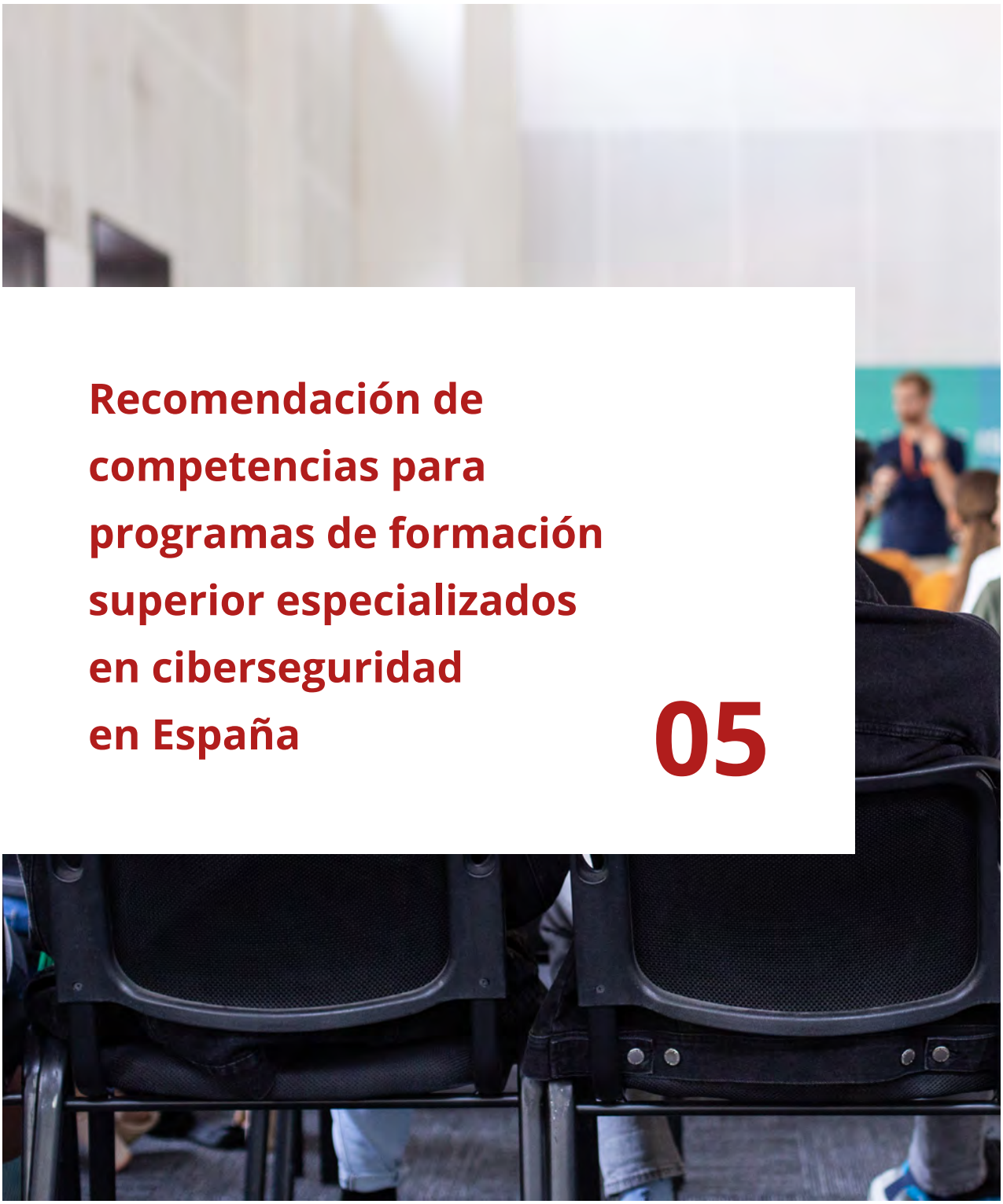
En general, las unidades de conocimiento principales tienen un soporte **alto o medio/alto** por parte de los programas de formación superior, con la salvedad de las unidades de conocimiento de administración de sistemas, cuyos temas son considerados como conocimientos previos (excepto el bastionado), la gestión de programas de seguridad y la seguridad del personal, que tienen un soporte **bajo**.

• **Área de Seguridad en la Sociedad**, con sus unidades de conocimiento de ciberdelincuencia, ciberderecho, ciberética, ciberpolítica y privacidad.

En general, las unidades de conocimiento tienen un soporte **medio** por parte de los programas de formación superior, aunque las unidades de conocimiento de ciberética y ciberpolítica tienen un soporte **bajo**.

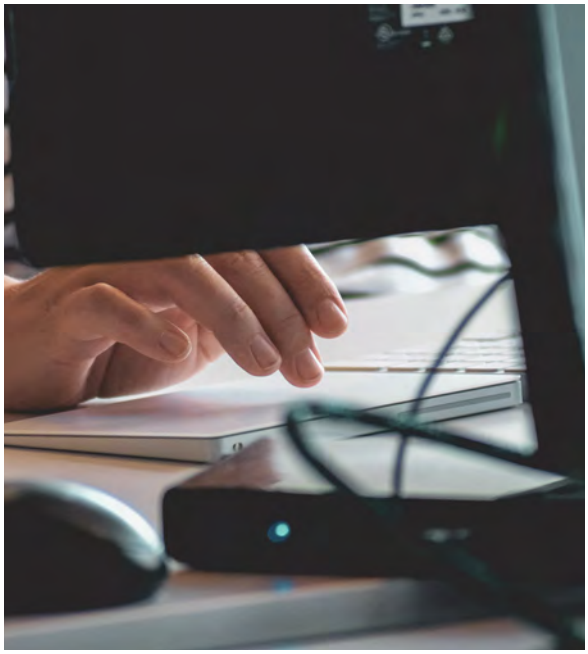
Por último, destacar que las consultas a estos programas de formación superior incluyen el soporte a la formación en algunas áreas que no están incluidas expresamente en el marco curricular ACM/IEEE en Ciberseguridad, y que son las siguientes:

- Seguridad Ofensiva:
  - Análisis de Vulnerabilidades
  - Técnicas de Explotación
  - Análisis de Amenazas
- Auditoría:
  - Papel de la auditoría
  - Ámbito y objetivos de la auditoría
  - Tipos de auditoría, marcos, técnicas y herramientas
  - Acuerdos y documentación
- Otros:
  - Protección de los perímetros
  - Vigilancia e Inteligencia
  - Detección de Intrusiones
  - Esteganografía



Recomendación de competencias para programas de formación superior especializados en ciberseguridad en España

05



Las secciones anteriores de este documento han servido para analizar el soporte que tiene el Marco Curricular ACM/IEEE en Ciberseguridad en los programas de formación superior con especialización en el área de ciberseguridad que se imparten actualmente en España. Este análisis permite comprender que la cobertura de ciertos temas (clasificados por áreas de conocimiento y unidades de conocimiento) es alta o media, mientras que la de otros es baja o nula ya que se identifican como conocimientos previos. Incluso se han identificado algunos temas que suelen incluirse en los programas formativos, a pesar de que no estén incluidos en el marco curricular ACM/IEEE.

La elección de los temas que se incluyen en los programas formativos analizados se fundamenta en las competencias que se pretende que tengan los egresados de dichos programas. Pero no existe un marco de competencias específicas del que se pueda partir para diseñar los planes de estudios especializados en ciberseguridad. Es por este motivo que las competencias de los programas analizados varían considerablemente, tanto en su redacción como en su contenido. El objetivo del resto del presente documento es justo éste: proponer un marco de competencias que facilite el diseño de planes de estudios especializados.

Este marco de referencia permitirá a los centros de formación superior escoger aquellas competencias que consideren más oportunas para el perfil de egresado que desean formar y a partir de ellas, por ejemplo, utilizando el marco curricular ACM/IEEE, proponer los temas y unidades de conocimiento que deben incluirse en los planes de estudios. Es decir, se pretende proporcionar una herramienta que reduzca la dificultad de los procesos de diseño de planes de estudios especializados, permitiendo a las instituciones responsables de este proceso seleccionar las competencias de entre un conjunto compartido o común, completo y actualizado, validado por expertos en la materia y ajustado a las necesidades del mercado laboral a medio plazo.

Se persigue además un objetivo adicional, que el marco de competencias propuesto permita mejorar la colaboración entre la academia y la industria. Mientras que en el primer ámbito las competencias son el punto de partida para el diseño de los planes de estudios, en el segundo son el punto de partida para la definición de perfiles y roles dentro de las organizaciones. El marco de competencias propuesto permitirá, gracias a la estandarización proporcionada, aproximar el lenguaje que se utiliza en ambos contextos, permitiendo a las universidades que los estudiantes egresados de sus títulos respondan mejor a las necesidades del mercado laboral y a las organizaciones tener expectativas realistas respecto a las actividades y tareas que estos egresados puedan llevar a cabo con garantías cuando finalizan sus estudios.

5.1. Metodología

Para proponer el marco de competencias se ha partido de una consulta a los futuros empleadores de los egresados de programas formativos especializados en ciberseguridad, tanto en el sector público como en el privado.

Esta consulta se ha realizado mediante un formulario de recogida de información (anexo I de este documento) que debían responder personas con perfiles concretos dentro de estos potenciales empleadores (personas con responsabilidad técnica en departamentos de IT, seguridad o similares). Contestar el cuestionario requería de un tiempo aproximado entre los 30 y 40 minutos.

El objetivo era recoger información sobre las actividades y tareas que necesitarán realizar los profesionales de la ciberseguridad en el medio o largo plazo. El objetivo no era analizar el mercado laboral ni el organigrama actual de las organizaciones, sino investigar acerca de las competencias más adecuadas para los futuros planes de estudios especializados en función de los perfiles que los empleadores van a necesitar.

En este formulario se mostraban diez funciones/áreas diferentes de la ciberseguridad (tabla 5.1). Para cada una de ellas se identificaban una serie de tareas o actividades inspiradas en el marco propuesto por el NICE [NICE2017]. La persona que respondía el formulario debía usar la escala de Likert (1- nunca, 2 -casi nunca, 3 -ocasionalmente, 4 - a menudo, 5 - constantemente) para indicar si esa tarea o actividad se desarrolla en su organización, independientemente de la denominación que tenga el puesto o rol de la persona que la desempeñe o de si se centra en activos IT, OT, en la nube, etc. Se pedía que la respuesta no tuviera en cuenta sólo lo que ocurre actualmente, sino también la tendencia a medio o largo plazo. Es decir, lo que se espera que ocurra en los próximos años.

Arquitectura
Desarrollo y producto
Ingeniería y administración
Análisis
Detección y respuesta
Investigación
Responsabilidad y dirección
Ingeniería de la confiabilidad
Auditoría
Formación, concienciación y sensibilización

Tabla 5.1. Funciones/áreas consideradas para la definición del marco de competencias

Aunque la mayor parte de estas funciones o áreas son auto-explicativas dada su denominación, cabe aclarar que la función o área de Ingeniería de la confiabilidad incluye todos los aspectos relativos a privacy, reliability, resilience y safety.

En una última sección se pedía que, una vez comprendidas las tareas y actividades que se asocian a cada función/área, se priorizaran las diez que habían identificado teniendo en cuenta la importancia para la organización.

Para que la muestra fuera representativa, el formulario se hizo llegar en el mes de septiembre del 2021 a representantes de los sectores de actividad mostrados en la tabla 5.2. El tamaño de la muestra fue de 95 personas, durante el mes de octubre se analizaron y procesaron las 46 respuestas completas recibidas en ese momento.

En paralelo a este proceso, se trabajó en identificar un conjunto plano de competencias específicas asociadas a las tareas y actividades listadas dentro de cada función/área. Es decir, se analizaron las competencias esenciales para que un profesional lleve a cabo cada una de estas tareas o actividades. Una vez recibidas las respuestas de los formularios, se priorizaron unas competencias frente a otras (teniendo en cuenta las necesidades de los potenciales empleadores) de manera que se listaran entre 10 y 20 competencias por función/área, aquellas necesarias para poder realizar las tareas y actividades más importantes para las organizaciones que habían respondido al formulario de recogida de información.

Sector privado	Sector público
Big Four (consultoras de mayor tamaño)	Administración central
Consultoras especializadas	Administración autonómica
Ingenierías	Administración local
Fabricantes de software y empresas de desarrollo	Justicia
Fabricantes/proveedores del sector de la ciberseguridad	Sanidad
Banca	Educación y universidades
Seguros, mutuas y sanidad privada	Fuerzas Armadas
Operadores de telecomunicaciones	Fuerzas y cuerpos de seguridad del Estado y policías autonómicas
Otros proveedores tecnológicos	Centros de investigación y tecnológicos
Centros de investigación y tecnológicos	
Defensa	
Logística	
Energía	
Transporte	
Aeroespacial	
Aguas	
Industria y manufactura	
Marketing y medios de comunicación	

Tabla 5.2. Sectores de actividad consultados para la definición del marco de competencias

5.2. Listado de competencias específicas

Una vez realizado el proceso explicado en la sección anterior, se propone el siguiente marco de competencias específicas para programas formativos en seguridad, categorizando las competencias según la función/área con la que están más relacionadas.

Cabe exponer algunas aclaraciones sobre este marco de competencias. La primera, se ha tenido en cuenta la definición de competencias de la Organización para la Cooperación y Desarrollo Económico que se ha trasladado al Espacio Europeo de Educación Superior. Esto implica que las competencias son habilidades y capacidades adquiridas a través de un esfuerzo deliberado y sistemático por realizar actividades complejas. De esta forma, no se limitan a comportamiento observables, sino que combinan conocimientos, habilidades, actitudes y motivaciones. Una competencia no se centra sólo en los elementos cognitivos (teorías, conceptos o conocimientos), sino que abarca tanto habilidades técnicas como atributos interpersonales [OECD2001].

En resumen, las competencias que se proponen a continuación permiten al egresado de un título universitario realizar con garantías de éxito las tareas y actividades por las que se preguntó en el formulario disponible en el anexo I para cada área o función.

La segunda, se han empleado para la redacción de las competencias verbos que reflejen esta consideración y que se ajusten a los niveles 3 y 4 de la taxonomía de Bloom en su mayoría, Aplicación y Análisis respectivamente [P2018]. En algunos casos excepcionales, se ha recurrido a verbos en los niveles 5 y 6 (Síntesis y Evaluación) o en los niveles 1 y 2 (Conocimiento y Comprensión). Pero dado que el objetivo es definir competencias para programas universitarios, estos dos niveles, el 3 y el 4 se han considerado los más adecuados, por norma general, para títulos tanto de grado como de post-grado.

5.2.1. Competencias asociadas con el área de ARQUITECTURA

CE1	Recolectar y definir las capacidades y requisitos de seguridad de los sistemas.
CE2	Realizar procesos de análisis del riesgo y seleccionar las estrategias más adecuadas para gestionar los riesgos identificados en función de la tolerancia de la organización.
CE3	Aplicar y analizar la aplicación de los principios básicos de la ciberseguridad y la privacidad durante el desarrollo, despliegue, instalación, integración, mantenimiento y optimización de sistemas.
CE4	Conocer y aplicar métodos y técnicas específicas de depuración, prueba, validación y evaluación de la seguridad de los sistemas, y documentar adecuadamente el diseño, implementación, mantenimiento y operación de la seguridad de dichos sistemas.
CE5	Supervisar la integración de las metas y los objetivos de la organización en la arquitectura de seguridad y en su configuración.
CE6	Comprender las tendencias y los conceptos arquitectónicos de las tecnologías de la información para el diseño de la arquitectura de seguridad.
CE7	Determinar cómo debe funcionar un sistema de seguridad (incluidas sus capacidades de resiliencia y confiabilidad) y cómo los cambios en las condiciones, las operaciones o el entorno afectarán a este funcionamiento.
CE8	Comprender y categorizar los impactos operativos específicos de las debilidades y vulnerabilidades de los activos.
CE9	Conocer y aplicar mecanismos de cifrado de datos y de gestión de claves.
CE10	Diseñar y aplicar adecuadamente los distintos métodos de autenticación, autorización y control de acceso.
CE11	Conocer y analizar los métodos y mejores prácticas para realizar gestión segura de configuraciones.
CE12	Diseñar la arquitectura de la red, en relación con los objetivos de seguridad y los objetivos operativos.
CE13	Apoyar en la adquisición y contratación de mecanismos y servicios de seguridad, garantizando una gestión adecuada de la cadena de suministro.
CE14	Conocer la naturaleza y la función de la Estructura de Información pertinente (por ejemplo, Computer Emegency Response Team de referencia).
CE15	Conocer y aplicar conceptos de mejora de procesos organizativos y modelos de madurez de procesos.

CE16	Interpretar y aplicar las leyes, las regulaciones, las políticas y principios éticos en relación con la ciberseguridad y la confiabilidad.
CE17	Diferenciar los modelos de seguridad y su relación con los estándares del sector de la ciberseguridad.

5.2.2. Competencias asociadas con el área de DESARROLLO Y PRODUCTO

CE1	Recolectar y definir las capacidades y requisitos de seguridad de los sistemas.
CE18	Conocer y entender los requisitos de funcionalidad, calidad y seguridad, y la manera en que estos se aplican a elementos específicos del suministro.
CE2	Realizar procesos de análisis del riesgo y seleccionar las estrategias más adecuadas para gestionar los riesgos identificados en función de la tolerancia de la organización.
CE3	Aplicar y analizar la aplicación de los principios básicos de la ciberseguridad y la privacidad durante el desarrollo, despliegue, instalación, integración, mantenimiento y optimización de sistemas.
CE4	Conocer y aplicar métodos y técnicas específicas de depuración, prueba, validación y evaluación de la seguridad de los sistemas, y documentar adecuadamente el diseño, implementación, mantenimiento y operación de la seguridad de dichos sistemas.
CE6	Comprender las tendencias y los conceptos arquitectónicos de las tecnologías de la información para el diseño de la arquitectura de seguridad.
CE19	Conocer las vulnerabilidades más frecuentes de las aplicaciones, y los métodos y técnicas para descubrirlas y solventarlas.
CE20	Analizar la superficie de exposición de un software y producir modelos de amenazas dentro de procesos de desarrollo de software.
CE21	Utilizar los principios y métodos de seguridad y confiabilidad en procesos de ingeniería del software para producir software seguro desde el diseño.
CE22	Producir software siguiendo ciclos de vida, metodologías y prácticas de desarrollo seguros.
CE23	Conocer y saber aplicar las mejores prácticas en codificación segura para los lenguajes de programación y plataformas más extendidos.
CE24	Seleccionar, desplegar, configurar y mantener capacidades de protección de aplicaciones como diferentes tipos de filtros, firewalls de aplicación, etc.

CE25	Comprender las implicaciones que la configuración del software, o de su relación con otros componentes de los sistemas, pueden tener para la seguridad.
CE26	Investigar los vectores de ataque y amenazas actuales y emergentes que pueden afectar a una organización, apoyándose en diferentes fuentes de información privadas o públicas (boletines, alertas, etc.).
CE16	Interpretar y aplicar las leyes, las regulaciones, las políticas y principios éticos en relación con la ciberseguridad y la confiabilidad.
CE27	Conocer las principales categorías de incidentes de seguridad y seleccionar las metodologías más adecuadas para responder ante ellos y gestionarlos según el contexto y la responsabilidad.

5.2.3. Competencias asociadas con el área de INGENIERÍA Y ADMINISTRACIÓN

CE2	Realizar procesos de análisis del riesgo y seleccionar las estrategias más adecuadas para gestionar los riesgos identificados en función de la tolerancia de la organización.
CE28	Aplicar los principios básicos de la ciberseguridad y la privacidad para gestionar los riesgos relacionados con el uso, el procesamiento, el almacenamiento y la transmisión de información o datos.
CE4	Conocer y aplicar métodos y técnicas específicas de depuración, prueba, validación y evaluación de la seguridad de los sistemas, y documentar adecuadamente el diseño, implementación, mantenimiento y operación de la seguridad de dichos sistemas.
CE29	Seleccionar e interpretar indicadores de rendimiento y disponibilidad de sistemas.
CE30	Implementar, mantener y supervisar mecanismos de control de acceso a la red o los activos (por ejemplo, listas de control de acceso, capacidades).
CE31	Realizar copias de seguridad y recuperación de datos.
CE32	Realizar procesos de parcheo y actualización de sistemas y aplicaciones y analizar la conveniencia de dichos procesos en diferentes escenarios.
CE11	Conocer y analizar los métodos y mejores prácticas para realizar gestión segura de configuraciones.
CE33	Escoger, configurar y utilizar capacidades y herramientas de prevención y detección de intrusiones en hosts y redes.
CE34	Proteger y fortificar sistemas operativos, aplicaciones y redes aplicando métodos de defensa en profundidad.
CE27	Conocer las principales categorías de incidentes de seguridad y seleccionar las metodologías más adecuadas para responder ante ellos y gestionarlos según el contexto y la responsabilidad.

CE35	Comprender la seguridad de la cadena de suministro de las tecnologías de la información y conocer políticas, requisitos y procedimientos para gestionar los riesgos asociados a la misma.
CE36	Diseñar, desplegar, supervisar y seleccionar políticas, procesos y actividades de formación, concienciación y sensibilización.
CE37	Entender y participar en las operaciones y procesos que gestionan eventos e incidentes.

5.2.4 Competencias asociadas con el área de ANÁLISIS

CE3	Aplicar y analizar la aplicación de los principios básicos de la ciberseguridad y la privacidad durante el desarrollo, despliegue, instalación, integración, mantenimiento y optimización de sistemas.
CE2	Realizar procesos de análisis del riesgo y seleccionar las estrategias más adecuadas para gestionar los riesgos identificados en función de la tolerancia de la organización.
CE4	Conocer y aplicar métodos y técnicas específicas de depuración, prueba, validación y evaluación de la seguridad de los sistemas, y documentar adecuadamente el diseño, implementación, mantenimiento y operación de la seguridad de dichos sistemas.
CE38	Investigar y evaluar la fiabilidad de un servicio o producto y de su proveedor.
CE39	Utilizar herramientas de análisis de tráfico de red para identificar vulnerabilidades y anomalías.
CE19	Conocer las vulnerabilidades más frecuentes de las aplicaciones, y los métodos y técnicas para descubrirlas y solventarlas.
CE40	Llevar a cabo tests de penetración aplicando y utilizando los principios, técnicas y herramientas más adecuadas y conociendo las principales tácticas, técnicas y procedimientos (TTP) utilizadas por los adversarios.
CE41	Analizar y distinguir las diferentes clases de ataques y sus fases o etapas.
CE42	Aplicar principios y técnicas para realizar procesos de hacking ético.
CE43	Simular las tácticas, técnicas y procedimientos (TTP) utilizadas por los adversarios para poder emularlas o anticiparse a sus posibles impactos.
CE26	Investigar los vectores de ataque y amenazas actuales y emergentes que pueden afectar a una organización, apoyándose en diferentes fuentes de información privadas o públicas (boletines, alertas, etc.).
CE44	Investigar los vectores de ataque y amenazas actuales y emergentes que pueden afectar a una organización, apoyándose en diferentes fuentes de información privadas o públicas (boletines, alertas, etc.).

CE20	Aplicar técnicas de ingeniería inversa en activos hardware y software y analizar archivos binarios.
CE45	Entender las técnicas de análisis forense existentes, aplicarlas según proceda y proporcionar recomendaciones tras el análisis realizado.
CE46	Conocer las tácticas, técnicas y procedimientos que pueden ser utilizadas para que un análisis forense no revele la realidad (anti-forense).
CE47	Comprender el malware y generar firmas que resuman su comportamiento.
CE48	Utilizar herramientas de análisis de malware y conocer los conceptos y metodologías asociados a este análisis.

5.2.5. Competencias asociadas con el área de DETECCIÓN Y RESPUESTA

CE41	Analizar y distinguir las diferentes clases de ataques y sus fases o etapas.
CE49	Aplicar los principios de extracción, transformación y almacenamiento de datos y saber automatizarlos.
CE50	Conocer y aplicar métodos estándar para recoger y diseminar información relativa a la evaluación, monitorización, vigilancia y recuperación de la seguridad.
CE4	Conocer y aplicar métodos y técnicas específicas de depuración, prueba, validación y evaluación de la seguridad de los sistemas, y documentar adecuadamente el diseño, implementación, mantenimiento y operación de la seguridad de dichos sistemas.
CE29	Seleccionar e interpretar indicadores de rendimiento y disponibilidad de sistemas.
CE51	Localizar y analizar archivos de sistema con información relevante para la seguridad (archivos de registro de actividad, archivos de configuración, etc.).
CE39	Utilizar herramientas de análisis de tráfico de red para identificar vulnerabilidades y anomalías.
CE52	Seleccionar, preparar o implementar herramientas de correlación de eventos de seguridad.
CE33	Escoger, configurar y utilizar capacidades y herramientas de prevención y detección de intrusiones en hosts y redes.
CE27	Conocer las principales categorías de incidentes de seguridad y seleccionar las metodologías más adecuadas para responder ante ellos y gestionarlos según el contexto y la responsabilidad.
CE26	Investigar los vectores de ataque y amenazas actuales y emergentes que pueden afectar a una organización, apoyándose en diferentes fuentes de información privadas o públicas (boletines, alertas, etc.).
CE31	Realizar copias de seguridad y recuperación de datos.

CE53	Recoger, custodiar y presentar pruebas y evidencias válidos en procedimientos judiciales.
CE45	Entender las técnicas de análisis forense existentes, aplicarlas según proceda y proporcionar recomendaciones tras el análisis realizado.
CE36	Diseñar, desplegar, supervisar y seleccionar políticas, procesos y actividades de formación, concienciación y sensibilización.
CE16	Interpretar y aplicar las leyes, las regulaciones, las políticas y principios éticos en relación con la ciberseguridad y la confiabilidad.

5.2.6. Competencias asociadas con el área de INVESTIGACIÓN

CE54	Identificar problemas y retos de ciberseguridad en las tecnologías de la información actuales y emergentes.
CE55	Conocer el estado del mercado y la industria nacional e internacional de ciberseguridad, así como distinguir las tareas, conocimientos, destrezas y habilidades de los diferentes roles de trabajo asociados.
CE3	Aplicar y analizar la aplicación de los principios básicos de la ciberseguridad y la privacidad durante el desarrollo, despliegue, instalación, integración, mantenimiento y optimización de sistemas.
CE56	Entender cómo aprovechar los centros de investigación y desarrollo, los grupos de reflexión, la investigación académica y los sistemas de protección de propiedad intelectual o industrial, para llevar a cabo proyectos de investigación, innovación y transferencia.
CE57	Usar entornos de trabajo colaborativos empleando herramientas y plataformas de colaboración, y aprovechando y aportando experiencia analítica y técnica en grupos con otros analistas y expertos, tanto internos como externos a la organización.
CE50	Conocer y aplicar métodos estándar para recoger y diseminar información relativa a la evaluación, monitorización, vigilancia y recuperación de la seguridad.
CE58	Definir y liderar los procedimientos pertinentes de publicación y difusión de resultados de investigación teniendo en cuenta la protección la propiedad intelectual e industrial.
CE16	Interpretar y aplicar las leyes, las regulaciones, las políticas y principios éticos en relación con la ciberseguridad y la confiabilidad.

5.2.7. Competencias asociadas con el área de RESPONSABILIDAD Y DIRECCIÓN

CE28	Aplicar los principios básicos de la ciberseguridad y la privacidad para gestionar los riesgos relacionados con el uso, el procesamiento, el almacenamiento y la transmisión de información o datos.
CE27	Conocer las principales categorías de incidentes de seguridad y seleccionar las metodologías más adecuadas para responder ante ellos y gestionarlos según el contexto y la responsabilidad.
CE59	Diseñar, desplegar, supervisar, medir y mejorar planes de continuidad de operaciones, de continuidad de negocio, de contingencia y de recuperación ante desastres, así como programas a diferentes niveles.
CE50	Conocer y aplicar métodos estándar para recoger y diseminar información relativa a la evaluación, monitorización, vigilancia y recuperación de la seguridad.
CE35	Comprender la seguridad de la cadena de suministro de las tecnologías de la información y conocer políticas, requisitos y procedimientos para gestionar los riesgos asociados a la misma.
CE36	Diseñar, desplegar, supervisar y seleccionar políticas, procesos y actividades de formación, concienciación y sensibilización.
CE60	Conocer las leyes, políticas, procedimientos, marcos normativos y reglamentos que de forma explícita describan obligaciones y requerimientos relacionados con la gestión de la ciberseguridad en los diversos entornos en que son de aplicación (incluidas las infraestructuras críticas).
CE61	Conocer y saber aplicar mejores prácticas, guías y recomendaciones para la gobernanza de la seguridad.
CE62	Utilizar normas, marcos y metodologías que permitan categorizar y clasificar las fuentes de información y el uso y características de los datos utilizados en una organización, según su sensibilidad y otros factores de riesgo.
CE63	Planificar el proceso organizativo relacionado con la dotación de recursos y personal dedicado a la ciberseguridad.
CE64	Establecer los requisitos de adquisición y compras de tecnologías de la información.

5.2.8. Competencias asociadas con el área de INGENIERÍA DE LA CONFIABILIDAD

CE16	Interpretar y aplicar las leyes, las regulaciones, las políticas y principios éticos en relación con la ciberseguridad y la confiabilidad.
CE65	Realizar evaluaciones de impacto para la privacidad.
CE28	Aplicar los principios básicos de la ciberseguridad y la privacidad para gestionar los riesgos relacionados con el uso, el procesamiento, el almacenamiento y la transmisión de información o datos.
CE62	Utilizar normas, marcos y metodologías que permitan categorizar y clasificar las fuentes de información y el uso y características de los datos utilizados en una organización, según su sensibilidad y otros factores de riesgo.
CE66	Diseñar y ejecutar los programas y procedimientos de clasificación de la información de una organización, así como los procedimientos en caso de incidentes.
CE9	Conocer y aplicar mecanismos de cifrado de datos y de gestión de claves.
CE67	Conocer y aplicar mecanismos de gestión de identidades y accesos.
CE68	Utilizar los principios y métodos de ciberseguridad y confiabilidad en procesos de ingeniería del software para producir software seguro desde el diseño.
CE60	Conocer las leyes, políticas, procedimientos, marcos normativos y reglamentos que de forma explícita describan obligaciones y requerimientos relacionados con la gestión de la ciberseguridad en los diversos entornos en que son de aplicación (incluidas las infraestructuras críticas).
CE69	Comprender estándares y normas relacionados con la gestión de datos PII (Personally Identifiable Information).
CE7	Determinar cómo debe funcionar un sistema de seguridad (incluidas sus capacidades de resiliencia y confiabilidad) y cómo los cambios en las condiciones, las operaciones o el entorno afectarán a este funcionamiento.
CE70	Analizar los niveles de redundancia y resiliencia de los sistemas asociados a infraestructuras críticas.
CE71	Diseñar, desplegar, mantener y operar la que soporta las tecnologías de la información desplegadas en una organización de manera que se garantice la confiabilidad.
CE72	Conocer y saber aplicar estándares y normas relacionados con la gestión de datos PCI (Payment Card Industry), PHI (Personal Heath Information) o de otros dominios especialmente sensibles.
CE37	Entender y participar en las operaciones y procesos que gestionan eventos e incidentes.
CE53	Recoger, custodiar y presentar pruebas y evidencias válidas en procedimientos judiciales.

5.2.9. Competencias asociadas con el área de AUDITORÍA

CE16	Interpretar y aplicar las leyes, las regulaciones, las políticas y principios éticos en relación con la ciberseguridad y la confiabilidad.
CE73	Habilitar y documentar el proceso de evaluación y autorización de la seguridad.
CE74	Conocer y auditar principios como los de mínimo privilegio o segregación de funciones.
CE28	Aplicar los principios básicos de la ciberseguridad y la privacidad para gestionar los riesgos relacionados con el uso, el procesamiento, el almacenamiento y la transmisión de información o datos.
CE62	Utilizar normas, marcos y metodologías que permitan categorizar y clasificar las fuentes de información y el uso y características de los datos utilizados en una organización, según su sensibilidad y otros factores de riesgo.
CE15	Conocer y aplicar conceptos de mejora de procesos organizativos y modelos de madurez de procesos.
CE75	Conocer y entender los requisitos de funcionalidad, calidad y seguridad, y la manera en que estos se aplican a elementos específicos del suministro.
CE17	Diferenciar los modelos de seguridad y su relación con los estándares del sector de la ciberseguridad.
CE50	Conocer y aplicar métodos estándar para recoger y diseminar información relativa a la evaluación, monitorización, vigilancia y recuperación de la seguridad.
CE60	Conocer las leyes, políticas, procedimientos, marcos normativos y reglamentos que de forma explícita describan obligaciones y requerimientos relacionados con la gestión de la ciberseguridad en los diversos entornos en que son de aplicación (incluidas las infraestructuras críticas).
CE4	Conocer y aplicar métodos y técnicas específicas de depuración, prueba, validación y evaluación de la seguridad de los sistemas, y documentar adecuadamente el diseño, implementación, mantenimiento y operación de la seguridad de dichos sistemas.
CE7	Determinar cómo debe funcionar un sistema de seguridad (incluidas sus capacidades de resiliencia y confiabilidad) y cómo los cambios en las condiciones, las operaciones o el entorno afectarán a este funcionamiento.
CE11	Conocer y analizar los métodos y mejores prácticas para realizar gestión segura de configuraciones.
CE35	Comprender la seguridad de la cadena de suministro de las tecnologías de la información y conocer políticas, requisitos y procedimientos para gestionar los riesgos asociados a la misma.
CE76	Identificar los problemas de ciberseguridad y privacidad que surgen de las conexiones con clientes y socios internos o externos.

5.2.10. Competencias asociadas con el área de FORMACIÓN, CONCIENCIACIÓN Y SENSIBILIZACIÓN

CE8	Comprender y categorizar los impactos operativos específicos de las debilidades y vulnerabilidades de los activos.
CE77	Analizar políticas, procesos y procedimientos de formación, concienciación y sensibilización de la organización, contribuyendo a evaluar sus necesidades presentes y futuras.
CE36	Diseñar, desplegar, supervisar y seleccionar políticas, procesos y actividades de formación, concienciación y sensibilización.
CE78	Seleccionar los principios y métodos de enseñanza-aprendizaje más adecuados para diferentes personas y grupos, e interpretar los impactos producidos.
CE79	Aplicar niveles (es decir, la taxonomía de aprendizaje de Bloom), modos y estilos de aprendizaje.
CE80	Aplicar técnicas y métodos de producción, comunicación y difusión de los medios de comunicación, incluidas maneras alternativas de informar a través de medios escritos, orales y visuales.
CE81	Diseñar y aplicar técnicas de prueba y evaluación del aprendizaje (rúbricas, planes de evaluación, exámenes, pruebas cortas).
CE82	Incorporar el uso del ordenador en la formación, incluyendo servicios de aprendizaje en línea, técnicas de virtualización, etc.
CE83	Realizar o supervisar competiciones de ciberseguridad como una forma para desarrollar habilidades por medio de experiencias prácticas en situaciones simuladas del mundo real.

5.3. Listado de pre-requisitos

El marco de competencias propuesto en la sección anterior recoge competencias específicas relacionadas con las diez áreas que se han tenido en cuenta en la fase de recogida de información inicial realizada mediante el envío del formulario (anexo I). Durante el diseño de un plan de estudios será necesario traducir estas competencias a materias, asignaturas y contenidos o unidades temáticas.

En este proceso, se identificarán pre-requisitos o conocimientos previos necesarios, es decir, condiciones que los estudiantes deben cumplir para poder cursar estas materias o asignaturas y ser evaluados. Dependiendo del tipo de plan de estudios que se esté diseñando, grado o post-grado, estos pre-requisitos llevarán a la definición de nuevas competencias específicas (asociadas a asignaturas de los primeros cursos de un grado, por ejemplo) o permitirán identificar los requisitos de acceso a la titulación (materias que habrá sido necesario cursar antes de ser admitido en un post-grado, por ejemplo).

Se proporciona a continuación un listado de conocimientos específicos que pueden traducirse en el proceso de diseño de un plan de estudios en ciberseguridad a nuevas competencias específicas (grado) o a requisitos de acceso (post-grado). Se expresan de momento con el concepto genérico de "conocimiento" para que en cada plan de estudios se redacten de la manera más adecuada en función de su papel, competencia específica o requisito que determina perfil de acceso.

PR1	Conocimiento de matemática.
PR2	Conocimiento de estadística.
PR3	Conocimiento de teoría, técnicas y algoritmos de machine learning.
PR4	Conocimiento de estrategias de investigación y gestión del conocimiento.
PR5	Conocimiento de los objetivos y las principales misiones empresariales.
PR6	Conocimiento de los roles, de las responsabilidades y de la organización.
PR7	Conocimiento de las tecnologías de la información empresariales.
PR8	Conocimiento de herramientas y entornos de colaboración.
PR9	Conocimiento del funcionamiento básico de los ordenadores.
PR10	Conocimiento de sistemas cliente y servidor.
PR11	Conocimiento de procesado de datos.
PR12	Conocimiento de implementación, gestión y tipos de sistemas de archivos.
PR13	Conocimiento de sistemas operativos.
PR14	Conocimiento de arquitectura de ordenadores.
PR15	Conocimiento de sistemas embebidos.
PR16	Conocimiento de métodos para la evaluación y la prueba de sistemas.
PR17	Conocimiento de tipos, administración y funciones de los sitios web y los gestores de contenidos.
PR18	Conocimiento de las capacidades y la funcionalidad asociadas con las tecnologías de creación de contenido.

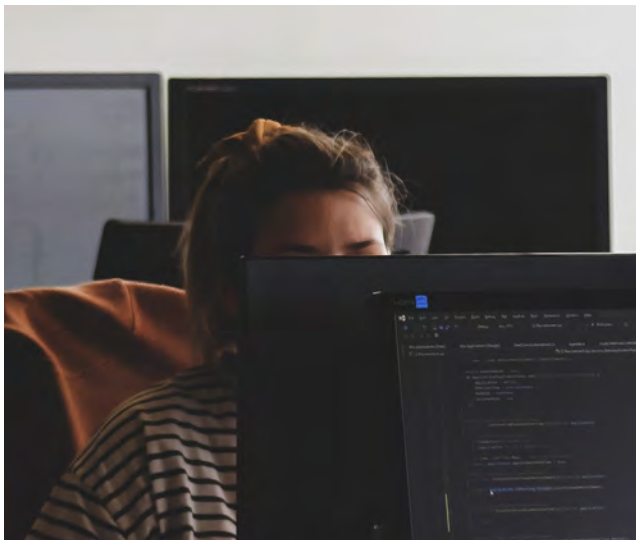
PR19	Conocimiento de los principales métodos, procedimientos y técnicas para la recogida de información y la producción, reporte o compartición de la misma.
PR20	Conocimiento de principios de interacción persona-ordenador.
PR21	Conocimiento de tecnologías de acceso remoto.
PR22	Conocimiento de sistemas de bases de datos, incluyendo su gestión, administración y mantenimiento.
PR23	Conocimiento de tecnologías de virtualización.
PR24	Conocimiento de modelos, administración, gestión y mantenimiento de sistemas y servicios en la nube.
PR25	Conocimiento de conceptos y marcos arquitectónicos de tecnología de la información.
PR26	Conocimiento de administración y mantenimiento de sistemas.
PR27	Conocimiento de técnicas y herramientas de depuración, diagnosis e identificación de fallos de sistemas.
PR28	Conocimiento de metodologías de tolerancia a fallos del sistema.
PR29	Conocimiento de procedimientos de auditoría y registro.
PR30	Conocimiento de principios y conceptos de programación como son lenguajes, depuradores o compiladores.
PR31	Conocimiento de programación en lenguajes de alto y bajo nivel.
PR32	Conocimiento de lenguajes de programación de bases de datos.
PR33	Conocimientos de programación en lenguajes de scripting.
PR34	Conocimiento de las implicaciones de seguridad en el diseño y la configuración de software.
PR35	Conocimiento de los principios de la ingeniería del software.
PR36	Conocimiento de procesos de control de calidad del software.
PR37	Conocimiento de los métodos para diseñar y analizar algoritmos.
PR38	Conocimiento de la estructura, arquitectura y diseño de sistemas de comunicación.
PR39	Conocimiento de sistemas de comunicación móvil.
PR40	Conocimiento de tipos de comunicación y protocolos de red.
PR41	Conocimiento de topologías de redes.
PR42	Conocimiento de mecanismos de control de acceso a nivel de host y red.
PR43	Conocimiento de administración de redes.
PR44	Conocimiento de dispositivos de red y sus configuraciones.
PR45	Conocimiento de aplicación de cortafuegos y sus funciones.
PR46	Conocimiento de métodos y herramientas de análisis de red.
PR47	Conocimiento básico de seguridad de red.
PR48	Conocimiento de funciones de seguridad actuales y emergentes del cifrado de datos en tránsito por redes de comunicaciones.

PR49	Conocimiento de registros de transmisión y técnicas de interferencia que permiten la transmisión de información no deseada o impiden que los sistemas instalados funcionen correctamente.
PR50	Conocimiento de algoritmos de cifrado y descifrado.
PR51	Conocimiento de gestión del ciclo de vida de las claves y secretos criptográficos.
PR52	Conocimiento de técnicas y conceptos de infraestructuras de clave pública y sistemas de certificados.
PR53	Conocimiento de funciones de seguridad actuales y emergentes del cifrado de datos en bases de datos.
PR54	Conocimiento de conceptos de cifrado en la nube.
PR55	Conocimiento de ciberamenazas y vulnerabilidades.
PR56	Conocimiento de técnicas y métodos de ciberataque.
PR57	Conocimiento de los modelos y las tecnologías de ciberseguridad.
PR58	Conocimiento de los principios y requisitos de confidencialidad, integridad y disponibilidad.
PR59	Conocimiento de técnicas básicas de fortificación ("hardening") de sistemas, redes y sistemas operativos.
PR60	Conocimiento de controles de seguridad y privacidad.
PR61	Conocimiento de gestión de la ciberseguridad.
PR62	Conocimiento del concepto de riesgo.
PR63	Conocimiento de regulaciones, políticas y leyes relevantes.
PR64	Conocimiento de los modelos de seguridad estándar industriales.

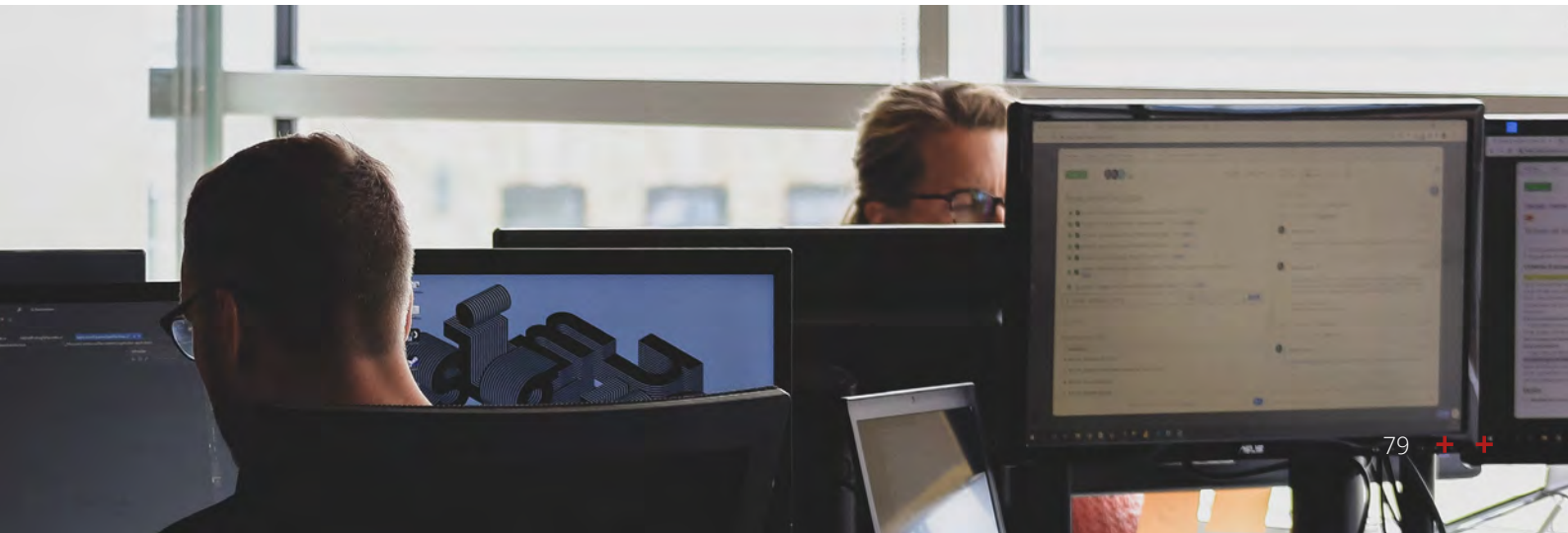
5.4. Listado de competencias básicas

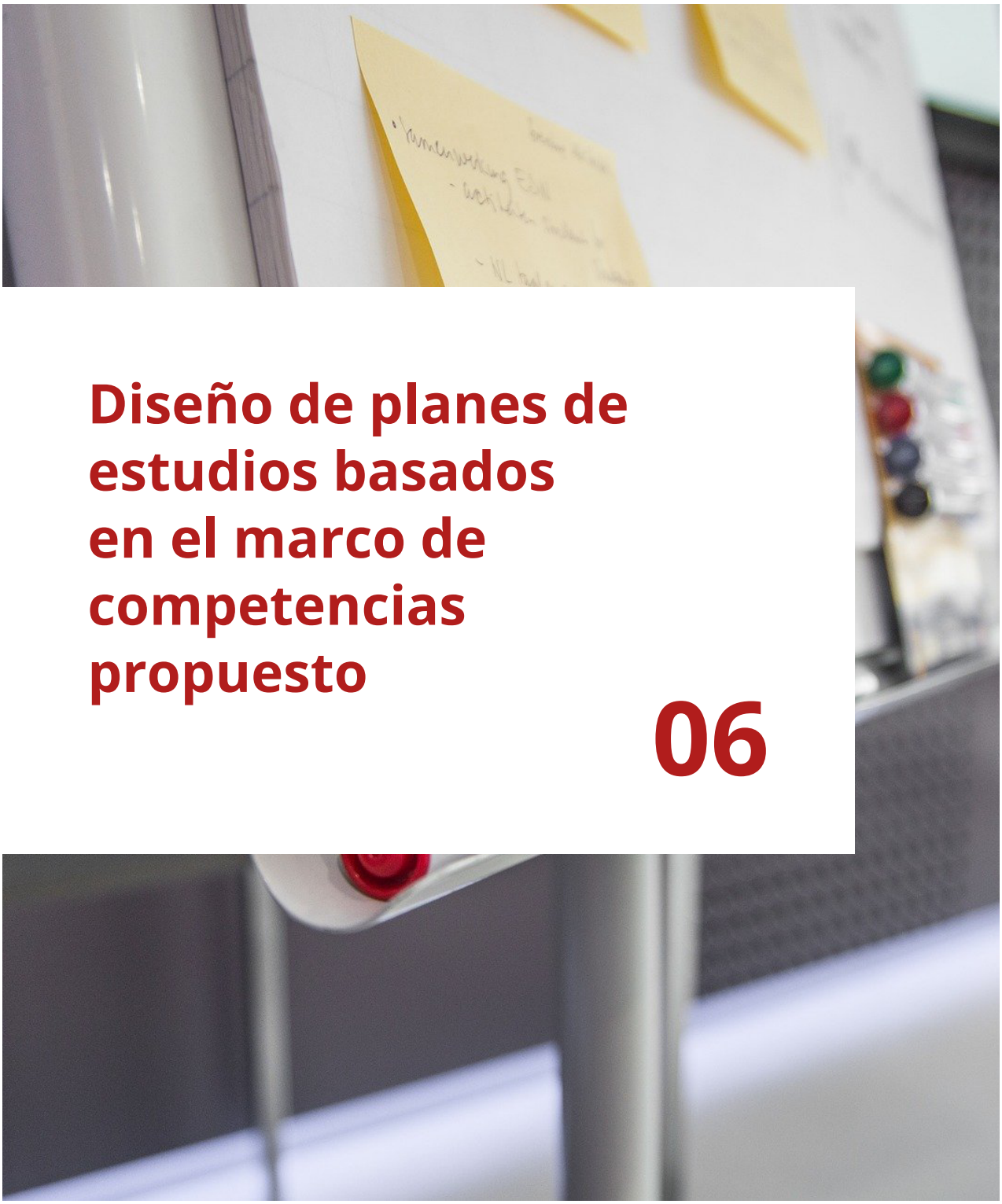
Por último, para completar la propuesta de marco de competencias realizada en este documento, es necesario identificar conocimientos, destrezas y actitudes que todos los egresados de las titulaciones necesitan para su realización y desarrollo profesional, y su inclusión en el mercado laboral.

Estas competencias, también esenciales, relacionadas con lo que se suele denominar soft skills o competencias blandas, son necesarias en la mayoría de los puestos sin importar el sector o industria. Se enumeran a continuación las identificadas como esenciales en el sector de la ciberseguridad gracias al proceso de recogida de información realizado, ya que es necesario incluirlas en el diseño de cualquier plan de estudios.



CB1	Capacidad de comunicación oral y escrita.
CB2	Capacidad de comunicación en otros idiomas.
CB3	Capacidad de argumentación.
CB4	Capacidad de investigación.
CB5	Capacidad de razonamiento lógico.
CB6	Capacidad para demostrar y poner ejemplos.
CB7	Capacidad para identificar, plantear y resolver problemas con diferentes enfoques.
CB8	Capacidad para usar las tecnologías de la información y de la comunicación.
CB9	Capacidad para para buscar, procesar y analizar información procedente de fuentes diversas.
CB10	Capacidad para trabajar en forma autónoma.
CB11	Capacidad de abstracción, análisis y síntesis.
CB12	Capacidad de aprender y actualizarse permanentemente mediante diferentes formas y en diferentes foros de aprendizaje.
CB13	Capacidad de aplicar los conocimientos en la práctica.
CB14	Capacidad crítica y autocrítica.
CB15	Capacidad para organizar y planificar el tiempo.
CB16	Capacidad para adaptarse a situaciones de cambio constante.
CB17	Capacidad creativa.
CB18	Capacidad para formular, acometer y gestionar proyectos.
CB19	Capacidad para tomar decisiones y saber justificarlas, así como para establecer prioridades.
CB20	Capacidad para trabajar en equipo asumiendo diferentes roles.
CB21	Capacidad de motivar y conducir hacia metas comunes.
CB22	Capacidad de adquirir un compromiso con la calidad.
CB23	Capacidad de adquirir un compromiso con la preservación del medio ambiente.
CB24	Capacidad de asumir responsabilidad social y ética.
CB25	Capacidad para valorar y respetar la diversidad y la multiculturalidad.





Diseño de planes de estudios basados en el marco de competencias propuesto

06

El proceso de diseño de un plan de estudios en el marco de educación superior actual se podría resumir en las siguientes fases o etapas:

1. Decidir el perfil de los egresados de la titulación.

2. Identificar las competencias básicas/generales necesarias para el perfil.

3. Identificar las competencias específicas que permiten desarrollar este perfil.

4. Agrupar las competencias relacionadas en materias.

5. Definir asignaturas dentro de estas materias que permitan adquirir subconjuntos de estas competencias que estén relacionados.

6. Desarrollar los contenidos de estas asignaturas.

7. Establecer los pre-requisitos de estas asignaturas y comprobar si es necesario añadir competencias específicas nuevas (algunos se adquirirán en titulaciones previas, otros tendrán que abordarse en el propio plan de estudios).

8. Comprobar que todas las asignaturas se justifican en las competencias identificadas y que todas las competencias se cubren en, al menos, una asignatura.

9. Analizar las dependencias entre asignaturas y establecer una secuencia lógica para cursarlas.

El presente documento puede dar soporte a estas fases o etapas de las siguientes maneras:

- La primera fase o etapa suele depender de la estrategia de títulos de cada centro, de los recursos disponibles (humanos y en cuanto a infraestructuras) y también de la información disponible acerca de la necesidad de un título en la sociedad o en el mercado laboral. En este sentido, esta primera fase podría apoyarse, en mayor o menor medida, en los resultados obtenidos con la consulta realizada a los potenciales empleadores.

Aunque los resultados de dicha consulta se completarán y analizarán con mayor profundidad en el futuro, de momento han permitido seleccionar las competencias más representativas para cada función/área (sabiendo las actividades y tareas que es más probable que los egresados tengan que acometer en su labor profesional). Además, las prioridades de las funciones/áreas por las que se ha preguntado se muestran en la tabla 6.1. Estas valoraciones pueden tenerse en cuenta a la hora de decidir los perfiles más interesantes para los egresados, aunque de momento hay que recordar que provienen de una muestra pequeña. Hay que señalar que las áreas que han obtenido más puntuación son las transversales, la que se consideran con importancia media o alta en la mayor parte de organizaciones. Mientras que las que han obtenido menos puntuación, pueden resultar de importancia alta para algún tipo de organización, pero no para todas. Lo que puede hacer interesante, por ejemplo, un post-grado específico en ciertos contextos.

En el anexo I de este documento se proporciona el cuestionario que se ha empleado para la recogida de información, de manera que se pueda ampliar la recogida en el futuro para tener en cuenta una muestra mayor, actualizarla (ya que las necesidades del mercado evolucionan con el tiempo) o realizar iniciativas de recogida de información

propias basadas en ese cuestionario o en otro similar que lo utilice como punto de partida. Por ejemplo, una universidad podría realizar una consulta antes de diseñar un plan de estudios incidiendo en los empleadores de un sector o de una zona geográfica concretas.

1	Responsabilidad y dirección (331 puntos)
2	Detección y respuesta (300 puntos)
3	Formación, concienciación y sensibilización (273 puntos)
4	Arquitectura (267 puntos)
5	Auditoría (254 puntos)
6	Análisis (238 puntos)
7	Ingeniería y administración (237 puntos)
8	Desarrollo y producto (203 puntos)
9	Ingeniería de la confiabilidad (173 puntos)
10	Investigación (144 puntos)

Tabla 6.1. Funciones/áreas consideradas para la definición del marco de competencias ordenadas por prioridad según las respuestas obtenidas para el formulario

- La segunda fase o etapa, puede apoyarse en la discusión realizada en la sección 5.4 (listado de competencias básicas).

- La tercera fase o etapa puede apoyarse en el marco de competencias específicas proporcionado en la sección 5.2 (listado de competencias específicas).

- Las fases o etapas cuarta, quinta y sexta pueden usar como referencia el marco curricular ACM/IEEE en ciberseguridad y la sección 4 de este documento en la que se han analizado planes de estudios implantados en la actualidad que pueden servir como ejemplo.

- La séptima fase puede apoyarse en los pre-requisitos listados en la sección 5.3.

Se proporcionan a continuación algunos ejemplos ilustrativos acerca de cómo utilizar este documento en el proceso de diseño de planes de estudios. Estos ejemplos no son más que eso, muestras de cómo el presente marco puede ser útil a lo largo de las diferentes etapas identificadas para el diseño de un plan de estudios. No pretenden ser, en ningún caso, una recomendación acerca de títulos concretos que deberían implantarse en el futuro.

Ejemplo de uso 1: Diseño de títulos de grado en ciberseguridad

Si, por ejemplo, una universidad decide diseñar un plan de estudios de ciclo largo, un grado, con perfil de ingeniería que abarque las competencias técnicas de las áreas consideradas más importantes por los futuros empleadores consultados de momento, podría centrarse en las competencias específicas de las áreas Detección y respuesta, Arquitectura, Análisis e Ingeniería y administración. Con esto ya se tendría decidido el perfil de los egresados de la titulación.

A continuación, se deberían identificar las competencias básicas/generales necesarias para el perfil, escogiendo para ello el subconjunto más adecuado de las listadas en la sección 5.4 de este documento. Tras esta etapa, se deberían identificar las competencias específicas que permiten desarrollar este perfil. Para ello se debería escoger un subconjunto concreto de competencias de entre las listadas para las áreas de interés (Detección y respuesta, Arquitectura, Análisis e Ingeniería y administración) en la sección 5.2 de este documento. Y se agruparían las competencias relacionadas entre sí en materias. Para ello se podría emplear como punto de partida el Marco Curricular ACM/IEEE en Ciberseguridad, que ayudaría a definir asignaturas dentro de estas materias y a desarrollar sus programas y contenidos.

Ya que el acceso a este título de grado se realizaría desde bachillerato, ciclos formativos y formación profesional o acceso para mayores de 25 años, los pre-requisitos que se identifiquen como esenciales para poder cursar estas asignaturas y materias no pueden serlo directamente. Sino que tendrían que ser competencias específicas de asignaturas de los primeros años del grado que se cursen con la secuenciación adecuada respecto a las asignaturas más específicas del área de la ciberseguridad.

Por ello, para finalizar el diseño de las competencias de este plan de estudios sería necesario proponer un subconjunto de nuevas competencias específicas que garanticen que los conocimientos necesarios de la sección 5.3 se adquieren por parte de los estudiantes antes de cursar las asignaturas que provienen del primer grupo de competencias específicas seleccionadas. Por ejemplo, si una asignatura de Seguridad ofensiva de tercer curso del grado cubre la competencia CE40: “Llevar a cabo tests de penetración aplicando y utilizando los principios, técnicas y herramientas más adecuadas y conociendo las principales tácticas, técnicas y procedimientos (TTP) utilizadas por los adversarios.”, debería haber como mínimo una asignatura de primer o segundo curso del grado que cubriera cada una de las competencias asociadas a los siguientes pre-requisitos PR55, PR56 y PR33 “Conocimiento de ciberamenazas y vulnerabilidades”, “Conocimiento de técnicas y métodos de ciberataque.” y “Conocimientos de programación en lenguajes de scripting.”. Para redactar estos pre-requisitos en forma de competencias específicas en el plan de estudios se recomienda utilizar verbos en los primeros niveles de la taxonomía de Bloom como definir, describir, identificar, reconocer, seleccionar, explicar, incorporar, proporcionar, etc. [P2018].

El mismo proceso se seguiría para diseñar, por ejemplo, un plan de estudios que abarcara las áreas más relacionadas con tareas de responsabilidad, dirección, gestión y control. Para ello se podrían seleccionar competencias específicas de las áreas de Responsabilidad y dirección, Formación, concienciación y sensibilización y Auditoría, por ejemplo. Y se utilizaría este documento de la misma forma que en el ejemplo anterior.

Ejemplo de uso 2: Diseño de títulos de post-grado en ciberseguridad

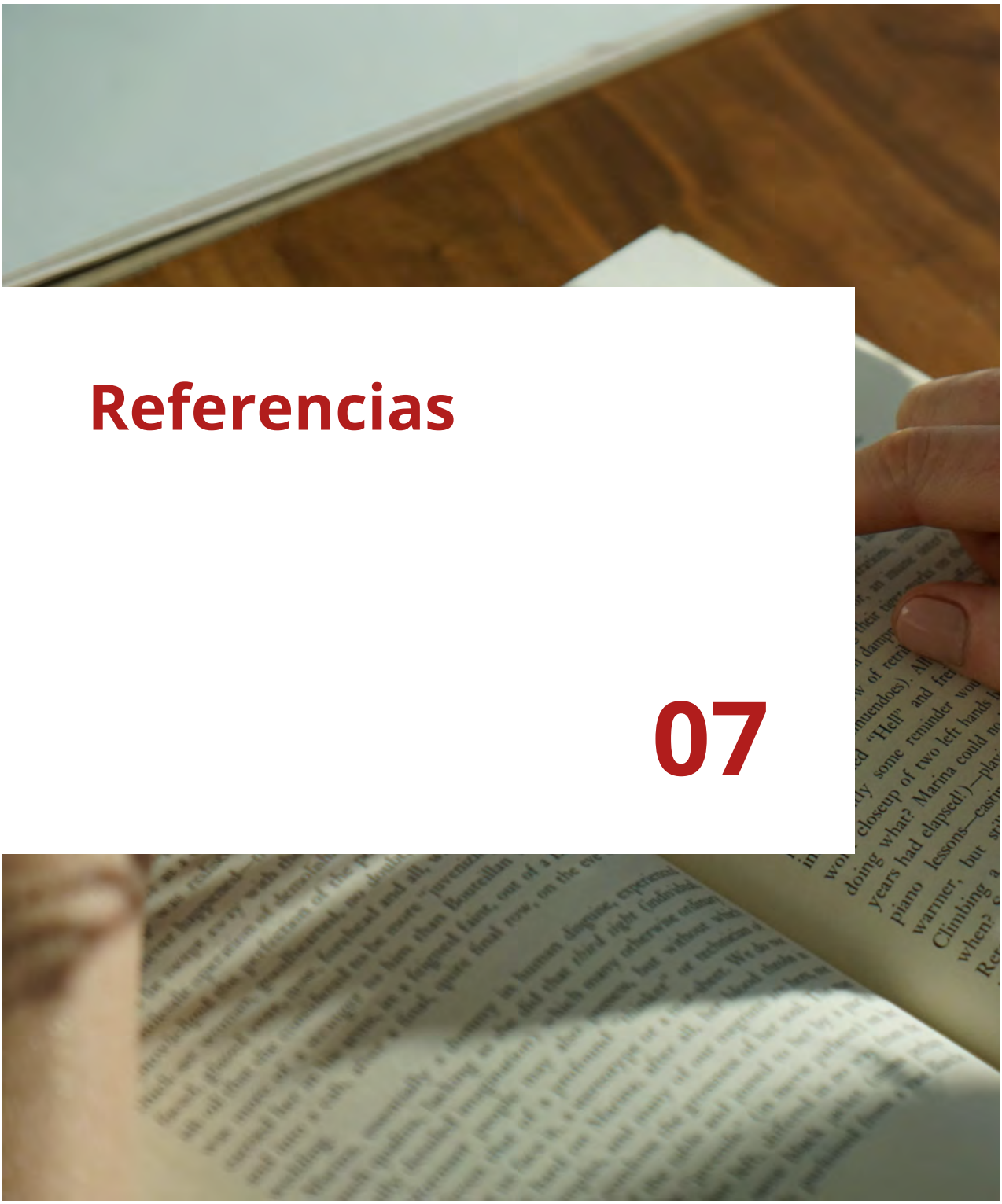
Otro ejemplo sería el de una universidad que desea diseñar un plan de estudios de post-grado (máster) centrado exclusivamente en el área de Responsabilidad y dirección, que parece ser transversal. Por ejemplo, pensando en proporcionar formación para profesionales que deseen certificarse en el futuro como responsables de ciberseguridad según el esquema nacional de certificación de responsables de ciberseguridad [ENCRC2021]. El proceso sería el mismo, pero en este caso sólo se escogerían competencias específicas del área de Responsabilidad y dirección.

Y sí se podrían establecer los conocimientos necesarios del listado proporcionado en la sección 5.3 como pre-requisitos, es decir, como conocimientos que los estudiantes admitidos en el máster deberían haber adquirido en las titulaciones que han cursado con anterioridad. Estos pre-requisitos ayudarían, por tanto, a establecer el perfil de acceso al título de máster. O a diseñar algún tipo de curso cero o curso puente que habilitara el acceso al máster a personas interesadas pero cuyos estudios anteriores no cubran los pre-requisitos identificados.

Lo mismo ocurriría si se deseara diseñar post-grados específicos en cualquiera de las otras áreas para las que se han propuesto competencias específicas en la sección 5.2: Detección y respuesta, Arquitectura, Análisis, etc. El proceso sería similar.

Ejemplo de uso 3: Diseño de títulos de post-grado mixtos o híbridos

También se podría emplear este marco de competencias para diseñar planes de estudios mixtos o híbridos, por ejemplo, un máster en Desarrollo seguro o DevSecOps, un máster en Ciberseguridad industrial y safety (incluida en el área de Ingeniería de la confiabilidad en el presente marco) o un máster en Aspectos legales de la ciberseguridad y privacidad (incluida también en el área de Ingeniería de la confiabilidad en el presente marco). Simplemente habría que buscar la combinación y equilibrio adecuados entre las competencias específicas de las disciplinas o áreas que se pretendiera combinar (desarrollo + ciberseguridad- Desarrollo y producto, industria/OT + ciberseguridad – Ingeniería de la confiabilidad, derecho + ciberseguridad – Ingeniería de la confiabilidad). Y habría que prestar especial cuidado a la identificación de los pre-requisitos para garantizar que los estudiantes pueden aprovechar el programa en su totalidad ya que poseen los conocimientos necesarios cuando acceden a él.



Referencias

07

/// **[CC2020]** ACM/IEEE, Computing Curricula 2020, CC2020, Paradigms for Global Computing Education, 31 de diciembre de 2020. URL: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2020.pdf

/// **[CS2017]** ACM/IEEE, Cybersecurity Curricula 2017, Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity, Computing Curricula Series Joint Task Force on Cybersecurity Education, 31 de diciembre de 2017. URL: https://cybered.hosting.acm.org/wp/wp-content/uploads/2018/02/csec2017_web.pdf

/// **[CYBOK2018]** Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M., & Peersman, C. (2018). Scoping the cyber security body of knowledge. IEEE Security & Privacy, 16(3), 96-102.

/// **[DLMS2021]** Dragoni, N., Lluch Lafuente, A., Massacci, F., & Schlichtkrull, A. (2021). Are We Preparing Students to Build Security In? A Survey of European Cybersecurity in Higher Education Programs [Education]. IEEE Security & Privacy, 19(1), 81-88.

/// **[ENCRC2021]** Propuesta de Esquema Nacional de Certificación de Responsables de Ciberseguridad, desarrollada por el Grupo de Trabajo de Formación, Capacitación y Talento, del Foro Nacional de Ciberseguridad, creado por mandato de la Estrategia Nacional de Cibserseguridad de 2019.

/// **[H2008]** Howard, M. (2008). Becoming a security expert. IEEE Security & Privacy, 6(1), 71-73.

/// **[INCIBE2021a]** INCIBE. Másteres y Grados en Ciberseguridad en España. Febrero 2021. https://www.incibe.es/sites/default/files/paginas/talento/catalogos-formacion/catalogo-masteres.pdf

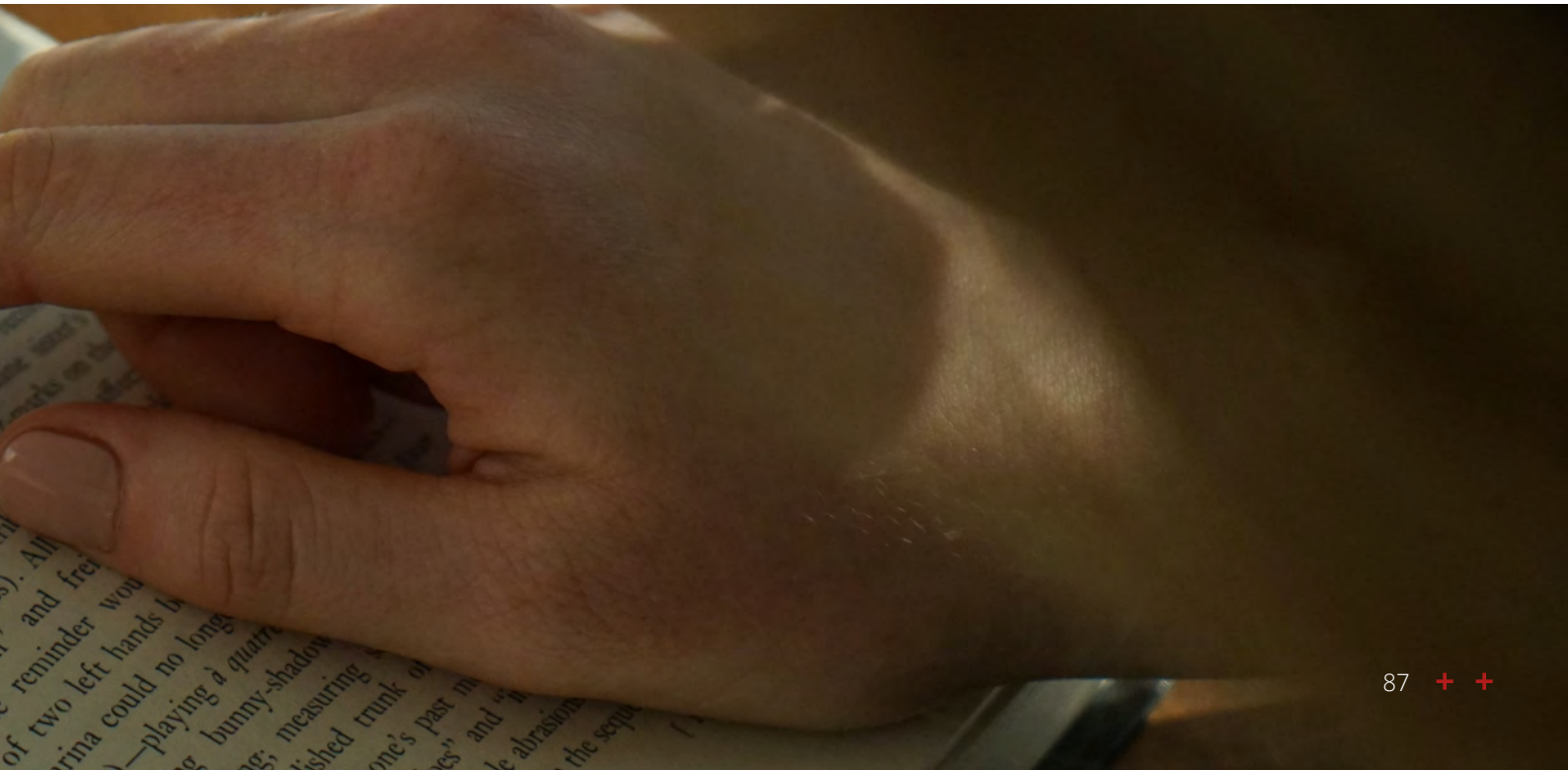
/// **[INCIBE2021b]** INCIBE. Instituciones que imparten formación en ciberseguridad en España. Febrero 2021. https://www.incibe.es/sites/default/files/paginas/talento/catalogos-formacion/catalogo-instituciones.pdf

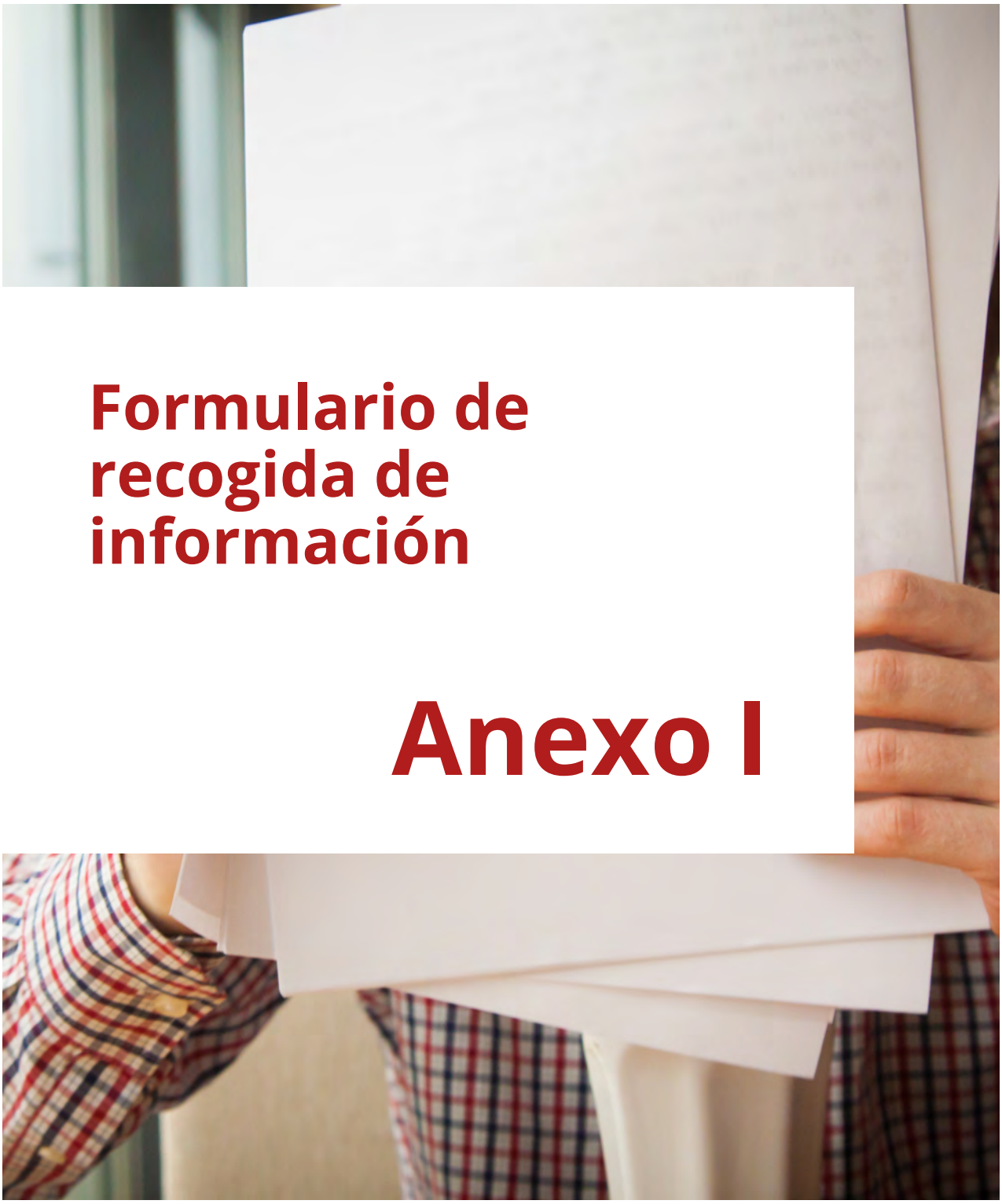
/// **[JRC2019]** Fovino, I. N., Neisse, R., Hernandez Ramos, J. L., Polemi, N., Ruzzante, G. L., Figwer, M., & Lazari, A. (2019). A proposal for a European cybersecurity taxonomy. Luxembourg: Publications Office of the European Union.

/// **[OECD2001]** Rychen, D.S.,& Salganik, L.H. (2001). Defining and selecting key competencies. DeSeCo Project (Definition and Selection of Competencies: Theoretical and Conceptual Foundations), OECD. https://www.deseco.ch/bfs/deseco/en/index/02.html

/// **[P2018]** Parrish, A., Impagliazzo, J., Raj, R.K., Santos, H., Asghar, M.R., Jøsang, A., Pereira, T., & Stavrou, E., (2018). Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. In Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE 2018 Companion). Association for Computing Machinery, New York, NY, USA, 36–54. https://doi.org/10.1145/3293881.3295778

/// **[SPARTA2020]** D9.1 Cybersecurity skills framework. Deliverable. Available at https://www.sparta.eu/assets/deliverables/SPARTA-D9.1-Cybersecurity-skills-framework-PU-M12.pdf. Accessed April 2021





Formulario de recogida de información

Anexo I

Marco de competencias para programas superiores (universitarios) de formación en ciberseguridad

Instrucciones para responder el formulario

El siguiente formulario forma parte de la iniciativa para la definición de competencias para programas superiores (universitarios) de formación especializada en ciberseguridad del grupo de trabajo en Formación, Capacitación y Talento del Foro Nacional de Ciberseguridad. **Gracias** por colaborar con esta iniciativa.

Rellenar el formulario le llevará entre **30 y 40 minutos**.

Estamos intentando **recoger información sobre las actividades y tareas que necesitarán realizar los profesionales de la ciberseguridad en el medio plazo** para definir el conjunto de competencias más adecuado para los títulos universitarios que se oferten en esta área. Nuestro objetivo no es analizar el mercado laboral ni el organigrama de las organizaciones, sino **definir planes de estudios para títulos universitarios** con las competencias apropiadas.
En las primeras secciones se muestran 10 funciones/áreas de la ciberseguridad. Para cada una de ellas se identifican una serie de tareas o actividades asociadas a la función/área. Por favor, **usando la escala de Likert (1- nunca, 2 -casi nunca, 3 -ocasionalmente, 4 - a menudo, 5 - constantemente), indique si esa tarea o actividad se desarrolla en su organización**, independientemente de la denominación que tiene el puesto o rol de la persona que la desempeña en su organización en concreto. También independientemente del dominio (IT, OT, cloud, etc.). Al indicar su respuesta, no tenga en cuenta sólo lo que ocurre actualmente, sino también la tendencia a medio o largo plazo. Es decir, lo que se espera que ocurra en los próximos años.

Dispone de una caja de **texto libre** por si quiere indicarnos alguna tarea o actividad que cree importante y no ha encontrado.

En la última sección se le pide que, una vez comprendidas las tareas y actividades que se asocian a cada una, **ordene las 10 funciones/áreas por las que se le acaba de preguntar en relación con la importancia que tiene para su organización** contar con ella dentro de su equipo. Siendo el puesto 1 el que corresponde a la primera, la más importante, la que seguro que es necesaria. Y el puesto 10 el que corresponde a la menos importante. Se trata de una puntuación relativa, comparando unas funciones con otras.

Información básica sobre Protección de Datos

• Datos y procedencia: Se tratarán los siguientes datos proporcionados por los interesados: nombre completo, organización, cargo y dirección de correo electrónico.

• Responsable: Foro Nacional de Ciberseguridad, Grupo de Trabajo 3 – Formación, Capacitación y Talento.

• Finalidad: Recogida de información para el Grupo de Trabajo 3 del Foro Nacional de Ciberseguridad, como parte de la iniciativa cuyo objetivo es proponer un marco de competencias para programas superiores (universitarios) de formación en ciberseguridad.

• Legitimación: Consentimiento del interesado.

• Destinatarios: No se cederán datos a terceros, salvo obligación legal.

• Derechos: Los interesados tienen derecho a solicitar el acceso a sus datos personales, a solicitar su rectificación o supresión, a solicitar la limitación de su tratamiento, a oponerse al tratamiento y a la portabilidad de sus datos. Para ello deben dirigirse por email al responsable antes citado.

• Información adicional: Puede consultar la información adicional y detallada sobre Protección de Datos dirigiéndose al responsable antes citado.

1. Nombre completo

2. Organización

3. Cargo

Arquitectura

Tarea o actividad
Identificar las necesidades de seguridad de la organización para diseñar su arquitectura de seguridad en consecuencia.
Determinar los niveles adecuados de confidencialidad, integridad y disponibilidad para los activos críticos que permiten la continuidad de las operaciones de la organización y dar soporte a dicha continuidad.
Determinar las necesidades en seguridad física en relación con la protección de personas, bienes, instalaciones o medio.
Evaluar arquitecturas posibles y tomar decisiones respecto al diseño y localización de las capacidades de seguridad.
Traducir las capacidades de seguridad de alto nivel a especificaciones criptográficas y técnicas relacionadas con mecanismos y servicios de seguridad concretos.
Asegurar que los mecanismos y servicios seleccionados son consistentes con las necesidades de seguridad de la organización y cumplen los requisitos establecidos.
Documentar requisitos de seguridad, especificaciones funcionales, patrones de diseño, etc.
Definir configuraciones base seguras para diferentes tipos de activos tanto físicos como lógicos.
Señalar los gaps entre las arquitecturas diseñadas y las realmente desplegadas y ayudar a gestionar los riesgos.
Comprender cómo los cambios en la infraestructura pueden afectar a los niveles de seguridad disfrutados.
Asesorar durante la realización de los proyectos en aspectos de diseño, patrones, costes y riesgos.
Apoyar en la adquisición y contratación de mecanismos y servicios de seguridad, garantizando una gestión adecuada de la cadena de suministro.
Por favor, en la celda inferior indique si ha echado en falta alguna tarea o actividad que en su organización tendría una puntuación de 5.

Desarrollo y producto

Tarea o actividad
Trasladar requisitos de seguridad a aspectos de diseño del software.
Aplicar metodologías de desarrollo seguro para minimizar el número de vulnerabilidades con las que se libera el código desarrollado.
Identificar la superficie de exposición del software desarrollado.
Realizar modelado de amenazas/análisis de riesgos del software desarrollado en diferentes momentos de su ciclo de vida.
Llevar a cabo análisis de código tanto estático como dinámico de código.
Planificar y llevar a cabo las tareas de testing y validación de seguridad.
Identificar las dependencias del software y las implicaciones que tienen para su seguridad.
Gestionar adecuadamente las implicaciones que tiene para la seguridad la interacción del software con el sistema operativo, el hipervisor, el hardware, etc.
Automatizar las tareas repetitivas que tienen que ver con la seguridad del software.
Documentar los aspectos de seguridad del software para otros desarrolladores, usuarios y demás agentes involucrados en el ciclo de vida del software.
Generar parches y actualizaciones que resuelvan las vulnerabilidades encontradas en el software tras ser liberado.
Definir planes de respuesta ante incidentes de productos software y dar soporte a esta respuesta.
Implementar mecanismos, controles y mitigaciones de seguridad mediante software.
Apoyar a otras funciones del área de la ciberseguridad en el desarrollo de herramientas, scripts, etc. que les ayuden a desarrollar sus tareas o actividades.
Por favor, en la celda inferior indique si ha echado en falta alguna tarea o actividad que en su organización tendría una puntuación de 5.

Ingeniería y administración

Tarea o actividad
Instalar, configurar, desplegar, integrar, mantener, actualizar los activos de la organización cumpliendo las especificaciones y políticas de seguridad.
Realizar test y diagnósticos de capacidad, conectividad o rendimiento y optimizar las prestaciones de los activos sin incumplir estas especificaciones y políticas.
Colaborar con la definición de especificaciones y políticas de seguridad en los que se refiere a los procedimientos técnicos.
Gestionar cuentas, permisos, privilegios, etc. en el acceso a los activos según el modelo de control de accesos definido para la organización.

Realizar inventarios de activos y mapas de red a diferentes niveles.
Planificar los cambios en la infraestructura/activos para minimizar los riesgos que producen los proyectos que los implementan.
Realizar la gestión de la configuración de los activos.
Realizar backup y copias de seguridad de diferentes tipos de datos e información.
Automatizar las tareas repetitivas que tienen que ver con la administración segura de los activos de la organización.
Proporcionar recomendaciones de uso seguro a los usuarios finales de los activos.
Proporcionar los medios para que los usuarios finales puedan cumplir las políticas de seguridad (o no puedan incumplirlas).
Monitorizar los activos bajo su responsabilidad y analizar tendencias para ayudar en la detección de anomalías, intrusiones, etc.
Dar soporte a los equipos de respuesta a incidentes.
Recuperar los activos tras incidentes de seguridad, contingencias y catástrofes.
Por favor, en la celda inferior indique si ha echado en falta alguna tarea o actividad que en su organización tendría una puntuación de 5.

Análisis

Tarea o actividad
Asegurar que la configuración, despliegue, integración, etc. de los activos cumplen con las especificaciones y políticas de seguridad.
Asegurar que los controles de seguridad y los productos/servicios de seguridad que se incorporan reducen el riesgo como se esperaba.
Realizar distintos tipos de verificaciones de seguridad, revisiones y test a diferentes tipos de activos para analizar los niveles de seguridad a los que llegan.
Asegurar que las especificaciones y políticas de seguridad se llevan a la práctica de la manera establecida y permiten que se cumplan los requisitos de seguridad.
Analizar los parches y actualizaciones de seguridad antes de que sean aplicados en los activos de la organización.
Realizar diferentes tipos de análisis y escaneo de vulnerabilidades en la infraestructura de la organización.
Realizar test de penetración y ejercicios de simulación de adversarios.
Crear, desplegar y mantener conjuntos de herramientas actualizados de seguridad ofensiva para realizar análisis periódicos de vulnerabilidades, continuos, etc.
Analizar las tendencias de los agentes de amenaza y del mercado para apoyar a otras áreas en su labor (arquitectura, ingeniería y administración, investigación, etc.).
Realizar procesos de ingeniería inversa para comprender cómo funcionan diferentes artefactos y objetos estáticos y dinámicos empleados por los agentes de amenaza.

Colaborar con las funciones de desarrollo y producto para ayudarles a reducir la superficie de exposición y a desarrollar los artefactos de software necesarios.
Asesorar en la toma de decisiones en base a los resultados de los análisis realizados.
Dar soporte a los equipos de respuesta a incidentes, por ejemplo, con capacidades de análisis forense.
Por favor, en la celda inferior indique si ha echado en falta alguna tarea o actividad que en su organización tendría una puntuación de 5.

Detección y respuesta

Tarea o actividad
Definir mecanismos de monitorización necesarios para detectar incidentes de seguridad.
Definir los requisitos de las fuentes de datos y herramientas necesarias para realizar detección.
Desarrollar estándares, especificaciones y políticas en relación con estos datos y herramientas.
Gestionar la captura de datos y su ciclo de vida de manera que sean útiles para la detección de incidentes.
Valorar la validez y valor de los datos y de sus fuentes en relación con la detección.
Plantear hipótesis a partir de grandes volúmenes de datos y validarlas mediante distintos tipos de modelos matemáticos o estadísticos.
Caracterizar las situaciones consideradas normales y detectar las anomalías.
Conocer las TTPs empleadas por los adversarios para proponer métricas, indicadores, etc. que permitan detectarlas en tiempos razonables para el contexto y levantar alertas.
Compartir inteligencia de amenazas e información similar con terceros según los objetivos de la organización con los formatos y mecanismos adecuados.
Automatizar las tareas repetitivas mediante lenguajes de scripting o específicos para manejo de grandes volúmenes de datos.
Realizar triaje y priorizar eventos de seguridad y alertas.
Coordinar personas y equipos internos y externos con diferentes perfiles e intereses durante y después del incidente (comunicación, reporting, denuncia, etc.).
Investigar el incidente y sus causas, realizar atribución y comprender los patrones de ataque empleados.
Realizar análisis forense incluyendo la recogida y custodia de evidencias digitales.
Analizar artefactos y objetos estáticos y dinámicos para extraer de ellos información relevante en cuanto a detección y respuesta.
Contener el incidente con soluciones temporales.
Asesorar a otras funciones para contener el incidente con soluciones permanentes y evitar que se produzca en el futuro.
Documentar los incidentes.
Extraer lecciones aprendidas de los incidentes.

Apoyar a otras funciones en la recuperación de activos tras los incidentes.
Por favor, en la celda inferior indique si ha echado en falta alguna tarea o actividad que en su organización tendría una puntuación de 5.

Investigación

Tarea o actividad
Llevar a cabo revisiones de la literatura y del estado del arte.
Identificar aspectos en los que se puede avanzar el estado del arte, así como tendencias del mercado o de los agentes de amenaza.
Descubrir nuevas vulnerabilidades, malware o amenazas; proponer nuevos mecanismos y capacidades defensivas; romper criptosistemas con técnicas novedosas, etc.
Coordinarse con otras funciones para determinar los objetivos de I+D+i de la organización.
Formular proyectos, coordinarlos y gestionar los recursos y presupuesto asignado.
Desarrollar metodologías, técnicas o herramientas propias apropiadas para conseguir los objetivos planteados.
Apoyar a otras funciones para que incorporen las innovaciones producidas a sus tareas y actividades.
Captar financiación para llevar a cabo los proyectos de I+D+i.
Establecer alianzas estratégicas con posibles socios que contribuyan en actividades de I+D+i.
Proteger la propiedad intelectual producida mediante patentes y licencias adecuadas.
Participar en consorcios, foros, redes, etc. que puedan enriquecer la función de investigación y permitan compartir el conocimiento generado según los objetivos de la organización.
Por favor, en la celda inferior indique si ha echado en falta alguna tarea o actividad que en su organización tendría una puntuación de 5.

Responsabilidad y dirección

Tarea o actividad
Contribuir al desarrollo de la Política de Seguridad de la organización y a definir su tolerancia al ciberriesgo.
Definir la estrategia de seguridad de la organización y coordinar la creación de normas, políticas, etc.
Informar y reportar a la dirección general y al comité de dirección acerca del estado de la organización en cuanto a la ciberseguridad, KPIs, ROI, etc.
Coordinar los procesos de evaluación. y análisis de riesgos así como las auditorías de seguridad.
Proponer estrategias de mitigación y transferencia del riesgo y alinearlas con los objetivos de negocio.
Planificar el despliegue de las mitigaciones y controles.

Predecir la evolución de los paradigmas tecnológicos y de los agentes de amenaza para intentar anticiparse de manera proactiva.
Definir y coordinar Programas y Planes para garantizar una correcta gobernanza de la seguridad.
Definir y coordinar planes de continuidad de negocio, contingencia, respuesta a incidentes, etc.
Definir KPIs e indicadores de éxito que permitan evaluar el éxito o eficiencia de estos Programas y Planes, también desde el punto de vista de negocio (ROI, etc.), actualizarlos y realizar mejora continua.
Fomentar la cultura de seguridad mediante la definición y comunicación de políticas de seguridad y otros documentos.
Analizar el grado de cumplimiento de estas políticas y garantizar que se cumplen en un grado adecuado.
Identificar las obligaciones de cumplimiento regulatorio.
Analizar qué certificaciones, evaluaciones, etc. es necesario o conveniente obtener (individuales y organizativas).
Identificar las necesidades de recursos humanos y materiales para conseguir los niveles de seguridad adecuados en la organización.
Gestionar las nuevas contrataciones, evaluar sus riesgos y hacer seguimiento durante la relación.
Gestionar presupuesto, adquisiciones, subcontrataciones, cadena de suministro, etc.
Validar que las contrataciones y adquisiciones responden a los objetivos y requisitos establecidos previamente.
Apoyar a la comunicación interna, vertical y horizontal, para transmitir el valor de la seguridad para la organización y coordinar a todas las funciones relacionadas con la seguridad.
Apoyar a la comunicación externa con terceras partes, socios, proveedores, clientes, etc.
Mantener el contacto con autoridades y grupos de interés.
Coordinar la respuesta a incidentes y la recuperación cuando sea necesario ejecutar los planes correspondientes.
Por favor, en la celda inferior indique si ha echado en falta alguna tarea o actividad que en su organización tendría una puntuación de 5.

Ingeniería de confiabilidad

Tarea o actividad
Ayudar a otras funciones a definir la Política de Privacidad de la organización y su tolerancia al riesgo para la protección de datos.
Coordinar los procesos de evaluación de impacto para la protección de datos y la evaluación de riesgos para la privacidad.
Identificar categorías de datos, realizar inventarios y etiquetarlos.
Ayudar a otras funciones a proponer estrategias de mitigación y transferencia del riesgo para la privacidad y la protección de datos y alinearlas con los objetivos de negocio.

Evaluar y probar mecanismos de privacidad desde el diseño.
Incorporar estos mecanismos a los activos, proyectos, etc. en los que sea necesario.
Mantener una actitud proactiva que permita identificar oportunidades para incorporar en la organización nuevas herramientas, prácticas, etc. que mejoren los niveles de privacidad.
Definir y coordinar el Plan de Cumplimiento relacionado con la privacidad y otros programas y planes relacionados.
Ayudar a otras funciones a definir la Política de Safety de la organización y su tolerancia al riesgo para la salud de las personas, para el medio ambiente, etc.
Ayudar a otras funciones a proponer estrategias de mitigación y transferencia del riesgo para la safety y alinearlas con los objetivos de negocio.
Evaluar y probar mecanismos de safety desde el diseño.
Incorporar estos mecanismos a los activos, proyectos, etc. en los que sea necesario.
Mantener una actitud proactiva que permita identificar oportunidades para incorporar en la organización nuevas herramientas, prácticas, etc. que mejoren los niveles de safety.
Definir y coordinar el Plan de Cumplimiento relacionado con la safety y otros programas y planes relacionados.
Identificar las obligaciones de cumplimiento regulatorio en relación con la confiabilidad (privacidad, safety, resiliencia, etc.).
Analizar qué certificaciones, evaluaciones, etc. en relación con la confiabilidad (privacidad, safety, resiliencia, etc.) es necesario o conveniente obtener (individuales y organizativas).
Apoyar a la comunicación interna, vertical y horizontal, para transmitir el valor de la confiabilidad para la organización y coordinar a todas las funciones.
Realizar comunicación externa con terceras partes, socios, proveedores, clientes, etc.
Mantener el contacto con autoridades y grupos de interés.
Coordinar la respuesta a incidentes de privacidad o safety y la recuperación.
Gestionar las acciones legales relacionadas con los incidentes de privacidad o safety.
Por favor, en la celda inferior indique si ha echado en falta alguna tarea o actividad que en su organización tendría una puntuación de 5.

Auditoría

Tarea o actividad
Conocer los procesos de negocio que soportan la organización y sus objetivos y requisitos de seguridad.
Planificar y realizar auditorías de seguridad de activos, proyectos, procesos, programas, etc.
Seleccionar o proponer los estándares y las metodologías más adecuados para realizar estas auditorías en cada caso.
Proponer y validar mecanismos para monitorizar y medir riesgo, nivel de cumplimiento, nivel de seguridad.

Proponer y validar métricas para cuantificar riesgo, nivel de cumplimiento, nivel de seguridad.
Proporcionar recomendaciones para realizar acciones correctoras y mejora continua en la seguridad de la organización tras los resultados de los diferentes procesos de auditoría.
Comunicar los resultados de los procesos de auditoría y documentarlos adecuadamente.
Evaluar el grado de cumplimiento de otras funciones respecto de los objetivos y requisitos fijados en la organización.
Evaluar el grado de segregación de funciones.
Revisar el grado de cumplimiento que proveedores y otras terceras partes hacen de sus obligaciones.
Ayudar a otras funciones a incluir en contratos, consentimientos, etc. la expresión de estas obligaciones en un lenguaje claro y adecuado.
Por favor, en la celda inferior indique si ha echado en falta alguna tarea o actividad que en su organización tendría una puntuación de 5.

Formación, concienciación y sensibilización

Tarea o actividad
Ayudar a otras funciones (gestión y dirección, etc.) a definir las necesidades de formación, concienciación y sensibilización de diferentes funciones dentro de la organización y a preparar programas y planes.
Diseñar iniciativas que permitan cubrir estas necesidades.
Llevar a cabo actividades internas de formación, concienciación y sensibilización.
Definir KPIs e indicadores de éxito que permitan evaluar el éxito o eficiencia de estas actividades, también desde el punto de vista de negocio (ROI, etc.) y realizar mejora continua.
Preparar materiales adecuados para las iniciativas internas de formación, concienciación y sensibilización.
Identificar a agentes adecuados para llevar a cabo actividades de formación, concienciación y sensibilización externas y coordinar su trabajo.
Establecer alianzas estratégicas con posibles socios que contribuyan en actividades de formación, concienciación y sensibilización.
Evaluar la adquisición de competencias por parte de todos los agentes involucrados en las iniciativas de formación, concienciación y sensibilización.
Cuantificar el nivel de madurez de la organización en relación con la formación, concienciación y sensibilización en seguridad de sus recursos humanos.
Sensibilizar a la dirección acerca de la importancia de la ciberseguridad para la consecución de los objetivos de negocio, cumplimiento normativo, etc.
Analizar, desplegar, escoger, configurar, etc. plataformas de entrenamiento, simulación, gemelos digitales o similares para dar soporte a las actividades que se realicen.
Por favor, en la celda inferior indique si ha echado en falta alguna tarea o actividad que en su organización tendría una puntuación de 5.

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): 089-23-019-1
Fecha de edición: junio 2023

FORO
NACIONAL DE
CIBERSEGURIDAD

2023