Universidad de Deusto

Ingeniería para la Sociedad de la Información y Desarrollo Sostenible

Tesis doctoral

Propuesta de un mapa de competencias en seguridad de la información para el personal no TIC de las universidades españolas

Josué Mendívil Caldentey

Dirigida por

Dra. Miren Gutiérrez Almazor
Dr. Borja Sanz Urquijo

JOSUE MENDIVIL CALDENTEY
Firmado digitalmente por JOSUE MENDIVIL CALDENTEY
Fecha: 2022.09.01 09:18:59 +02'00'

Firmado digitalmente por SANZ URQUIJO BORJA - 78908494W
Nombre de reconocimiento (DN): c=ES, serialNumber=IDCES-78908494W, givenName=BORJA, sn=SANZ URQUIJO, cn=SANZ URQUIJO BORJA - 78908494W
Fecha: 2022.09.01 14:11:46 +02'00'

San Sebastián, 1 de septiembre de 2022

Dedicatoria

A Pilar y Jon.

Como diría Fito,
con vosotros pude aprender
lo que se puede llegar a querer.

Agradecimientos

Resulta difícil transmitir en unas pocas frases mi sincero agradecimiento y gratitud a todas las personas que durante la realización de esta tesis me habéis guiado, asesorado y apoyado.

Quisiera agradecer en primer lugar a mis codirectores de tesis, Miren Gutiérrez y Borja Sanz, vuestra imprescindible ayuda, colaboración y dedicación.

También quisiera dar las gracias a mis compañeros "korrikalaris" Alazne Mújika y Juanjo Gibaja. Vuestros consejos, orientaciones y apoyo han sido fundamentales en esta tesis.

Mi gratitud a la vicerrectora Elena Auzmendi y a mi gran compañero y adjunto a vicerrector Iñaki Fuertes, por vuestra confianza y permanente apoyo durante todos estos años.

Deseo expresar mi especial reconocimiento y enorme deuda con mis colegas, los expertos y expertas de las universidades de Burgos, Comillas, Politécnica de Cartagena, Sevilla y Valencia, que han contribuido con su excepcional conocimiento y experiencia a esta tesis. Fonse, Julia, Luís, Paco, Zulema, sin vuestra generosidad, esta tesis no hubiera sido posible. Os pertenece.

En el ámbito personal tengo que dar las gracias a Pilar, mi ángel de la guarda. Sin tus traducciones exprés, orientaciones y constante amparo, este trabajo hubiera sido aún más complicado.

Jon, aunque no lo supieras, también has tenido un papel muy relevante en esta tesis. La estabilidad emocional y la alegría de verte crecer sano y feliz durante estos tres años de tesis y pandemia han sido muy importantes para mí.

No quiero cerrar este capítulo sin dar las gracias a mis padres y hermanos, siempre pendientes de cómo se iba desarrollando la tesis. Especialmente a mi padre, la persona que más se alegró cuando le dije que la había terminado... y la que en ocasiones me reñía si consideraba que no estaba trabajando lo suficiente.

Abstract

This dissertation argues that training and awareness activities in the field of information security are a vital element in the security strategy of any organization. Competency management models are shown to be one of the most effective tools to achieve the objectives to develop such awareness. However, the analysis of the situation, both in companies and organizations as well as in Spanish universities, together with the corresponding review of the literature carried out, confirms that the use of competency-based management for training activities and security awareness of information is practically non-existent.

This dissertation opens a new line of research to fill this gap and presents the development of a map of competencies in information security for personnel in Spanish universities who do not belong to the domain of Information and Communication Technologies, ICT.

As a second substantial contribution to the body of knowledge, the use of industry standards for the design and construction of competence maps is explored. Due to its relevance for Spanish public universities, Royal Decree 3/2010 of January 8, which regulates the National Security Scheme, ENS, is used in this dissertation.

To carry out this task, the methodology of the Functional Analysis of Competencies is implemented, firstly by obtaining the functional map of labor competencies from the security measures of Annex II of the NSS. Next, the existing non-ICT job profiles in the universities are identified from a security approach and the performance levels are detailed, to finally obtain, as a compendium of all the above, the competency map.

This work has been carried out with the participation of a group of experts in the field of information security belonging to different Spanish universities, with whose collaboration the different phases of the methodology used have been reviewed and resolved. Once the work is finished, it is possible to answer the research question that gives meaning to this doctoral thesis: What are the skills and level of performance in the field of information security that each university non-ICT personnel profile must achieve? By answering this question, it is possible to promote and improve the much-needed information security training and awareness activities in our universities.

Resumen

A lo largo de esta tesis se describe y argumenta que las actividades de formación y concienciación en el ámbito de la seguridad de la información son un elemento vital en la estrategia de seguridad de cualquier organización. Y para ello, los modelos de gestión por competencias se demuestran como una de las herramientas más eficaces para llevarlas a cabo. Sin embargo, el análisis de la situación, tanto en las empresas y organizaciones como en las universidades españolas, junto con la correspondiente revisión de la literatura llevada a cabo, confirman que el empleo de la gestión por competencias en labores de formación y concienciación en seguridad de la información es prácticamente inexistente.

Esta tesis abre una nueva línea de investigación para cubrir esta carencia y propone la elaboración de un mapa de competencias en seguridad de la información para el personal no perteneciente al dominio de las Tecnologías de la Información y la Comunicación, TIC, de las universidades españolas.

Como segundo aporte sustancial al cuerpo de conocimiento, se explora el uso de estándares de la industria para el diseño y la construcción de mapas de competencias. Se emplea en esta tesis, por su relevancia para las universidades públicas españolas, el Real Decreto 3/2010, de 8 de enero, que regula el Esquema Nacional de Seguridad, ENS.

Para llevar a cabo esta tarea, se utiliza la metodología del Análisis Funcional, obteniendo en primer lugar el mapa funcional de competencias laborales a partir de las medidas de seguridad del Anexo II del ENS. A continuación se identifican los perfiles laborales no TIC existentes en las universidades desde un enfoque de seguridad, y se detallan los niveles de desempeño, para finalmente obtener, como compendio de todo lo anterior, el mapa de competencias.

Este trabajo se ha llevado a cabo con la participación de un grupo de expertos y expertas en el ámbito de la seguridad de la información pertenecientes a distintas universidades españolas, con cuya colaboración se han ido recorriendo y resolviendo las diferentes fases de la metodología empleada. Una vez finalizado el trabajo, se está en disposición de contestar a la pregunta de investigación que da sentido a la presente tesis doctoral: ¿cuáles son las competencias y nivel de desempeño en el ámbito de la seguridad de la información que debe alcanzar cada perfil laboral universitario no TIC? Mediante la respuesta a esta pregunta, se pretende fomentar y mejorar las tan necesarias actividades de formación y concienciación de la seguridad de la información en nuestras universidades.

Índice general

Índice de tablas

Índice de figuras

Glosario y Acrónimos

AEPD Agencia Española de Protección de Datos

AMOD A Model

Benchmarking: Proceso de mediante el cual se recopila información de las organizaciones líderes o destacadas, para utilizar esa información en beneficio y mejora de la propia empresa.

BSI British Standards Institution

CISA Certified Information Systems Auditor

CMM Capability Maturity Model

CMMC Cybersecurity Maturity Model Certification

COBIT Control Objectives for Information and related Technology

CSF NIST Cybersecurity Framework

CUI Controlled Unclassified Information

DACUM Developing a Curriculum

DDoS Destributed Denial of Service

ENS Esquema Nacional de Seguridad

GFDL GNU Free Documentation License

GRC Gobernanza, riesgo y cumplimiento

Hacktivismo: Activismo político, social o económico que se manifiesta mediante ataques informáticos a corporaciones y gobiernos.

IEC International Electrotechnical Commission

INCIBE Instituto Nacional de Ciberseguridad

INES Informe Nacional del Estado de la Seguridad

IoT Internet of Things

ISACA: Information Systems Audit and Control Association. Asociación global independiente y sin fines de lucro dedicada al desarrollo, adopción y divulgación de conocimientos y buenas prácticas de sistemas de gestión de la información.

ISO International Organization for Standardization

ISO 27000: Conjunto de estándares internacionales sobre Seguridad de la Información.

ISSAF Information Systems Security Assessment Framework

ITIL Information Technology Infrastructure Library

LMS Learning Management Systems

LOPDGDD Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales

Malware: Abreviatura de *Malicious software*, término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.

N.A. No Aplica

NIS Network and Information Systems

OIT Organización Internacional del Trabajo

OSA Open Security Architecture

OSSTMM Open Source Security Testing Methodology Manual

PAS Personal de Administración y servicios

PDI Personal Docente e Investigador

Pentest: Abreviatura de Penetration Testing o Test de Intrusión, una metodología para evaluar la seguridad de un sistema informático mediante la simulación de un ataque.

RAE Real Academia Española de la Lengua

Ransomware: Programa malicioso que restringe el acceso a determinadas partes o archivos del sistema operativo infectado, y pide un rescate a cambio de retirar esa restricción.

RedIRIS: Red académica y de investigación española que proporciona servicios avanzados de comunicaciones a la comunidad científica y universitaria nacional. Está financiada por el Ministerio de Ciencia, Innovación y Universidades.

RGPD Reglamento General de Protección de Datos

RSL Revisión Sistemática de Literatura

SCID Systematic Curriculum and Instructional Development

SGSI Sistema de Gestión de Seguridad de la Información

SGSTI Sistema de Gestión de Servicios TI

Stakeholders: Las partes interesadas son personas, organizaciones o empresas que tienen participación interna o externa en una empresa u organización, y que pueden afectar, verse afectadas o percibirse como afectadas por las decisiones o actividades que realiza dicha empresa u organización.

TI Tecnologías de la Información

TIC Tecnologías de la Información y de la Comunicación

UNE Asociación Española de Normalización

Capítulo 1

Introducción

"He mirado con sus ojos, he escuchado con sus oídos, y te digo que es el indicado: o por lo menos, lo más adecuado que vamos a encontrar".

El juego de Ender

1.1. Presentación

Las economías, las organizaciones, las empresas, los puestos de trabajo, las relaciones personales e incluso el mundo físico son cada vez más digitales. Toda actividad humana y no humana, como el internet de las cosas, IoT, se transforma en datos en un proceso que Viktor Mayer-Schoenberger y Kenneth Cukier han denominado datificación (Mayer-Schönberger y Cukier, 2013). Las actuales tecnologías de la información y comunicación, TIC, se han introducido en todos los ámbitos de las sociedades occidentales, modificando nuestra forma de producir, trabajar, estudiar, consumir o socializar.

En el ámbito empresarial, la aparición de plataformas tecnológicas globales como Google, Amazon o Meta, basadas en las TIC, en la conversión de procesos o en la creación de modelos de negocio disruptivos, están provocando una profunda transformación en las organizaciones. Incluso el precio de los productos y servicios ha dejado de ser el factor más relevante en las relaciones con los consumidores (Downes y Nunes, 2013).

La industria, a través de la digitalización e interconexión de los procesos productivos y la aplicación de inteligencia no solo a los procesos, sino también a los productos, está inmersa desde comienzos de este siglo en lo que se conoce como la cuarta revolución industrial

(Schwab, 2016). Aunque sometido a restricciones en países como Arabia Saudita o China, Internet se ha convertido en un recurso universal y de uso masivo (Desjardins, 2019).

El mundo físico también está siendo transformado por las TIC a través de la interconexión a la red de dispositivos y objetos cotidianos. En el año 2018, siete mil millones de dispositivos estaban conectados a la red, interactuando con otros dispositivos o personas, y se espera alcanzar los veintiún mil millones en el año 2025 (Lasse, 2018).

Esta actividad está generando un crecimiento exponencial de los datos almacenados en internet. En el año 2010 internet tenía un tamaño de doce zettabytes, el equivalente a unos doce billones de gigabytes, 10^{21} bytes. En el año 2018 alcanzó los treinta y tres zettabytes, y se espera sobrepasar los dos mil en el año 2035 (Schwandt, 2018).

El crecimiento de la industria digital es constante desde 1991, cuando los primeros servidores se conectaron a la *world wide web*, con expectativas de que este crecimiento continúe (IDC, 2020). En el caso de España, la cifra de negocio de la industria TIC no ha dejado de aumentar desde el año 2014, situándose en el año 2019 en los 95.473 millones de euros de facturación, presentando un crecimiento respecto al año 2018 de un 3,9 % (ONTSI, 2021).

Estas transformaciones también han provocado el nacimiento de una nueva disciplina desde las ciencias sociales, los estudios críticos de datos, que se preocupa de los retos éticos y sociales que plantean a las personas y las sociedades la explotación y procesamiento de los datos masivos o *big data* generados por las TIC. Dentro de esta disciplina, Tom Boellstorff (2013) y Lisa Gitelman (2013) ya establecieron que los datos no son un recurso natural, sino un recurso cultural, resultado de procesos humanos. En la actualidad estos procesos son la base que cada vez más organizaciones utilizan para establecer sus estrategias y tomar decisiones. Este cambio de paradigma basado en el dato ha convertido en los últimos años a las compañías tecnológicas, tal y como se aprecia en la tabla 1.1, en las mayores empresas del mundo por capitalización bursátil, desplazando a las industrias manufactureras y petroleras (marketcap.com, 2022).

	Compañía	País	Industria
1	Aramco	Arabia Saudí	Energía
2	Apple	Estados Unidos	Tecnológica
3	Microsoft	Estados Unidos	Tecnológica
4	Google	Estados Unidos	Tecnológica
5	Amazon	Estados Unidos	Tecnológica
6	Tesla	Estados Unidos	Industrial
7	Berkshire Hataway	Estados Unidos	Financiera
8	Meta	Estados Unidos	Tecnológica
9	TSMC	Taiwan	Industrial
10	Johnson & Johnson	Estados Unidos	Farmacéutica

Tabla 1.1: Mayores empresas por capitalización bursátil. Marzo 2021

Nos encontramos, por tanto, en una era digital caracterizada por su complejidad y por una permanente y acelerada evolución tecnológica, desarrollada apenas en los últimos treinta años, y en la que las fronteras entre los aspectos económicos, tecnológicos, sociales y culturales no cesan de desdibujarse.

1.2. Ámbito del problema

El auge y desarrollo tecnológico descritos en las páginas precedentes presenta sin embargo puntos débiles. El primero es la disparidad de las tecnologías empleadas, formadas por sistemas, arquitecturas y protocolos heterogéneos, muchas de ellas no diseñadas inicialmente para trabajar en los actuales entornos. Ejemplos de esta realidad pueden ser los protocolos de correo electrónico o el protocolo HTTP, diseñados en los años 80. El segundo punto débil es la complejidad de gestionar el enorme número y variedad de dispositivos y equipos interconectados. En tercer lugar, el actual grado de conexión y automatización, si bien ofrece evidentes aspectos positivos, implica una completa dependencia por parte de las economías, las empresas y los particulares del correcto funcionamiento de la tecnología. Finalmente, y este será el punto de partida de esta tesis, el avance tecnológico no ha venido acompañado de un progreso similar en el ámbito de la seguridad y privacidad de los datos ni de la información generada y gestionada por las TIC. En una sociedad que

proclama que su recurso más valioso ya no es el petróleo sino los datos (The Economist, 2017), estos se encuentran expuestos a cada vez mayores riesgos (Haqaf y Koyuncu, 2018). Esta exposición al riesgo no solo se produce a nivel tecnológico. Como se explica más adelante, la ausencia de una adecuada concienciación del impacto que pueden suponer los riesgos de seguridad, y en consecuencia la escasa formación, suponen un grave peligro en las sociedades desarrolladas.

Estas carencias en la seguridad provocan como resultado en organizaciones y empresas vulnerabilidades, es decir, debilidades en sus activos de información que pueden ser explotadas por amenazas, entendidas estas como causas potenciales de un incidente no deseado que puede ocasionar daño a un sistema (López y Ruiz, 2012). El reto que subyace tras estas amenazas y vulnerabilidades no es solo económico o tecnológico; se trata de un problema de confianza, definida como "la esperanza firme que se tiene de que algo responderá a lo previsto" (Mañas, 2012, p. 6). La necesaria confianza en los sistemas informáticos se ha convertido en un valor crítico (BOE, 2022b), y con él la necesidad de minimizar los riesgos que sufren.

Mientras que las debilidades por su naturaleza son siempre internas, las amenazas a las que están expuestos los sistemas pueden ser de carácter externo o interno. En el primer grupo se encuentran los ataques deliberados desde el exterior de la organización con el objetivo de acceder de manera no autorizada, modificar, degradar o destruir los sistemas de información, las telecomunicaciones o las infraestructuras que los soportan (CCN-CERT, 2010). Como amenazas internas se catalogan todas las actividades comprometidas realizadas de manera voluntaria o involuntaria por los propios usuarios de las organizaciones.

Para una mejor comprensión, a continuación se presentan y explican brevemente estas amenazas, aportando ejemplos de cada una de ellas.

1.2.1. Amenazas externas

El número y variedad de amenazas externas son muy amplios, derivados de los numerosos agentes que desarrollan estas actividades. Los propios estados, la ciberdelincuencia común, el ciberterrorismo o el *hacktivismo* son unos cuantos ejemplos, cada uno de ellos con distintos objetivos y propósitos, pero con un punto de partida común: llevar a cabo acciones

dirigidas contra equipos informáticos y sistemas de información para lograr el acceso no autorizado a un dispositivo o negar el acceso a un usuario legítimo (Interpol, 2020). Se trata de un fenómeno de plena actualidad, tanto por el constante incremento en el número y notoriedad de los casos como por la negativa repercusión económica y reputacional que ocasionan.

Como amenazas externas más habituales pueden identificarse las siguientes (CCN-CERT, 2019):

- La propagación de código dañino o *malware* a través del correo electrónico. Existen muchos tipos de malware, como el *adware* o publicidad no deseada, el *spyware* que recopila información del equipo para enviarlo a un tercero, el *riskware* o software que permite la administración remota de un equipo o la apertura de puertos, o el *ransomware*, software que encripta archivos del equipo afectado para solicitar un pago para su recuperación.

- El *cryptomining*, es decir, la utilización ilegal de los recursos de una máquina para realizar operaciones de encriptación de datos y registro de transacciones en *blockchain*.

- El *phishing* o suplantación de personalidad con el objetivo de obtener información de manera ilegal mediante el uso de ingeniería social.

- Los *DDoS* o ataques de denegación de servicio, que persiguen bloquear los equipos y los servicios que prestan a través de la saturación de sus recursos.

Todavía está en el recuerdo de muchas personas el primer ataque a gran escala ocurrido en España. En mayo de 2017 los ordenadores de cientos de empleados de la compañía Telefónica sufrieron el ataque de un ransomware conocido como *WannaCry*, literalmente, "quieres llorar", que bloqueaba el acceso a los archivos de los equipos infectados y que obligó a la paralización temporal de la actividad de la compañía. Este incidente fue parte de un ataque global masivo que afectó a empresas de todo el mundo. Apenas un mes más tarde se informó de un nuevo ataque global de ransomware, en esta ocasión una variante denominada *Petya*, más sofisticada y dañina (Lozano, 2017).

Desde entonces, los ataques contra empresas e instituciones, tanto en España como en el resto del mundo se han sucedido de manera regular y sin interrupción, como los sufridos por el sistema de salud de Castilla y León, la Cadena SER y otras emisoras de Prisa Radio, la empresa Prosegur (20 Minutos, 2019), la consultora multinacional Everis (Muñoz, 2021), el Servicio Público Estatal de Empleo (INCIBE, 2021a), el Instituto Nacional de Estadística (INCIBE, 2021b), o el oleoducto de la empresa Colonial en Estados Unidos (Sánchez-Vallejo, 2021) por citar algunos. El hecho de que algunas de las víctimas de estos ataques sean medios informativos y organismos públicos no ha hecho sino incrementar su notoriedad.

El Foro Económico Mundial en su informe anual *The Global Risks Report 2021* sitúa, un año más, a los ciberataques entre los principales riesgos globales, situándolos como uno de los riesgos con mayor probabilidad e impacto. Un riesgo que no se prevé que disminuya en los próximos diez años(WEF, 2021). El CCN-CERT señalaba en su informe *Ciberamenazas y Tendencias 2018* que tan solo el malware *Cobalt*, activo durante el período comprendido entre los años 2016 a 2018 generó unas pérdidas a nivel mundial de unos mil millones de euros (CCN-CERT, 2018). También se han incrementado el número de ataques. En el año 2018 hubo un 350 % más de ataques ransomware que en el año anterior (The Cocktail Analysis, 2019).

En el caso de España, el Instituto Nacional de Ciberseguridad, INCIBE, gestionó durante el año 2020 más de 133.000 incidentes de seguridad. De ellos, más de 25.000, casi un 19 %, correspondieron al ámbito académico de RedIRIS (INCIBE, 2020a). Si a este número se añade la consideración de que muchos incidentes de seguridad no son reportados por las empresas y organizaciones por temor a que su imagen se vea perjudicada, se puede asumir que la gravedad del problema es todavía mayor.

Los incidentes de seguridad suponen por tanto un elevado riesgo, cuyos efectos se traducen para los gobiernos, organizaciones y particulares en perjuicios considerables, como pérdidas económicas, amenazas a infraestructuras críticas, afecciones a las cadenas de suministro o robos de datos personales.

1.2.2. Amenazas internas

A las amenazas externas se deben añadir las amenazas internas, consideradas como uno de los mayores problemas no resueltos de seguridad de la información (Bailey et al., 2018). De acuerdo con el *Informe de investigación sobre incidentes de seguridad* publicado en el año 2020, elaborado por la compañía de telecomunicaciones americana Verizon, el robo de credenciales basado en ingeniería social, habitualmente phishing, y los errores de los empleados y empleadas causaron cerca del 67 % de los incidentes de seguridad reportados (Bassett et al., 2021).

El IBM X-Force Research, uno de los equipos de investigación en seguridad de la información más prestigiosos del mundo, señala que los incidentes de seguridad debidos a errores no intencionados representaron más del 20 % de los incidentes de seguridad reportados públicamente. Y lo que resulta más grave, en el mismo informe se indica que más de un tercio de la actividad involuntaria llevada a cabo por los clientes monitorizados por este equipo fue debido a ataques cuyo objetivo era engañar a los usuarios y usuarias para que pincharan sobre un enlace o abrieran un archivo adjunto (IBM, 2018).

La compañía aseguradora Hiscox, en su *Informe Siniestros 2020*, presenta datos más preocupantes. De acuerdo con este informe, El 55 % de las reclamaciones de ciberseguridad cursadas por esta compañía en el año 2020 se debieron a accidentes o errores humanos, mientras que el 39 % de los siniestros gestionados fueron debidos a ataques basados en ingeniería social (Hiscox, 2020).

Sin embargo, la percepción del impacto que provocan los incidentes de seguridad entre los usuarios y usuarias es bajo, siendo su nivel de confianza en los mecanismos tecnológicos elevado. En el *Estudio sobre la ciberseguridad y confianza en los hogares españoles*, el 42 % de las personas encuestadas dicen tener mucha o bastante confianza en Internet, y el 71 % considera que su ordenador personal y/o dispositivo móvil se encuentran razonablemente protegidos contra las amenazas de la Red (ONTSI, 2019). Respecto al uso de protocolos de seguridad, solo el 14 % afirma en la misma encuesta actualizar sus contraseñas con regularidad, y apenas el 21 % realiza de manera regular copias de seguridad de sus archivos (The Cocktail Analysis, 2019).

Respecto a su percepción sobre la responsabilidad que debe asumir cada persona ante los riesgos de ciberseguridad, el 45 % considera necesario asumir ciertos riesgos para disfrutar de Internet, el 67 % que las herramientas de seguridad son demasiado costosas, y el 80 %, cuatro de cada cinco personas, piensan que el uso de herramientas y procedimientos de seguridad requieren demasiado esfuerzo por su parte. Esta actitud de relegar sistemáticamente la seguridad ante la comodidad, el coste o cualquier otro aspecto se identifica en la literatura sobre seguridad de la información como *el factor humano* (Ani, 2019; Fielding, 2020).

1.2.3. Las universidades

En el caso de las universidades, su actividad, objetivos y funciones, unidos a su relevancia social, las sitúan en un entorno diferenciado y complejo, encontrándose sujetas a condiciones cambiantes y siempre exigentes (Tomás y Castro, 2010). Por ello, tal y como se explicará con mayor detalle cuando se analice la cultura organizacional, las universidades presentan elementos únicos y característicos, como son los claustros docentes, la libertad de cátedra o los propios estudiantes. A estas singularidades se debe añadir la actividad investigadora de las universidades, en ocasiones con proyectos de alto valor estratégico o económico, o incluso relacionados directamente con ciberdelitos o infraestructuras críticas, y sin embargo desarrollada en un escenario en el que la seguridad de la información está supeditada a otros aspectos, como son la colaboración y la compartición de recursos, el acceso libre a los servicios o el uso de operativas abiertas (Sampalo et al., 2018).

Estas características hacen que las universidades, además de ser objetivos atractivos para sufrir amenazas, presenten un elevado número de vulnerabilidades y por tanto un alto riesgo. Debido a ello, son uno de los sectores más afectados por las ciberamenazas, tal y como expone el *Estudio sobre ciberseguridad en el sector universitario español* llevado a cabo por la compañía Deloitte, según el cual el 80 % de las universidades participantes en el estudio afirmaron haber sufrido algún incidente de seguridad durante el año 2018 (Deloitte, 2018). Ejemplos de esta realidad son los ataques sufridos por la Universidad de Burgos (INCIBE, 2020b), la Universidad de Valladolid (INCIBE, 2019a), la Universidad de Cádiz (INCIBE, 2020c), la Universidad de Castilla La Mancha (INCIBE, 2021c), la

Universidad Autónoma de Barcelona (EFE, 2021), la Universidad de Oviedo (Rodríguez, 2022) o la Universitat Oberta de Catalunya (INCIBE, 2022).

1.2.4. Tecnología, políticas y personas

A la vista de lo expuesto, parece necesario seguir trabajando en la mejora de la seguridad de la información de las empresas y organizaciones en general, y de las universidades en particular. Pero esta necesaria mejora no puede ser solo tecnológica. La seguridad de una organización está conformada por la tecnología, pero también por sus políticas y procedimientos y por el nivel de formación y concienciación de las personas que trabajan o se relacionan con ellas (Calder, 2016; Eloff y Eloff, 2005). Estos tres componentes, tecnología, políticas y personas, tal y como puede apreciarse en la figura 1.1, mantienen una estrecha relación e influencia entre sí, siendo por tanto necesaria su participación coordinada para asegurar una adecuada gestión de la seguridad de la información.

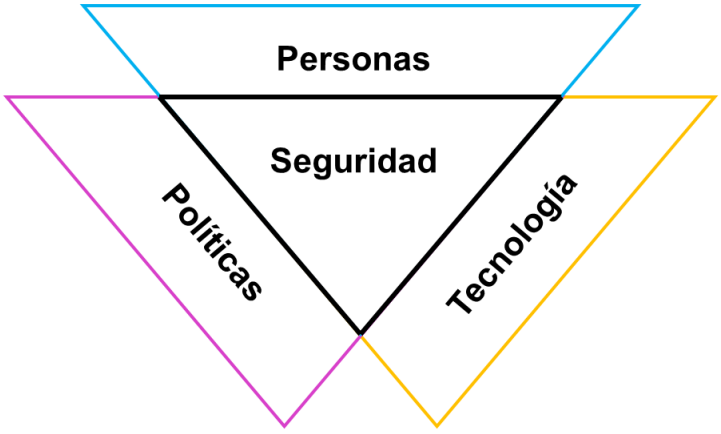

Figura 1.1: Personas, políticas y tecnología
Fuente: Elaboración propia

Pero si los avances tecnológicos en materia de seguridad han sido constantes, y el establecimiento de políticas y procedimientos de seguridad ha tenido un importante desarrollo en los últimos años, con un notable auge e incremento en la implantación de buenas prácticas y estándares en muchas empresas y organizaciones, en las siguientes páginas se explica que no ocurre lo mismo con las actividades de formación y concienciación. Sin embargo, es necesario que los avances citados estén acompañados por una mejora en la formación y

concienciación de las personas, tal y como señala el *Informe sobre la cultura de la ciberseguridad en España*, donde se afirma que "los usuarios deben conocer y tomar conciencia de los riesgos (de seguridad) a los que se enfrentan" (Foro Nacional de Ciberseguridad, 2021).

En uno de los documentos considerados fundacionales sobre seguridad TIC, *The Protection of Information in Computer Systems*, Jerome Saltzer (1975) y Michael Schroeder (1975) ya incluían entre los principios de diseño que deben aplicarse para establecer mecanismos de protección, que estos debían ser "psicológicamente aceptables" para el usuario o usuaria, de manera que puedan ser aplicados de forma rutinaria y automática, y por ello correcta. Afirmaban que "en la medida en que la imagen mental que tiene el usuario sobre las medidas de protección coincida con los mecanismos que debe utilizar, se minimizarán los errores" (Saltzer y Schroeder, 1975).

En el año 2001, Victor Maconachy (Maconachy et al., 2001) ya definía a las personas como "el corazón y el alma de los sistemas seguros", afirmando que las personas "requieren concienciación, alfabetización, capacitación y educación en prácticas sólidas de seguridad para que los sistemas estén protegidos".

Este enfoque centrado en las personas está recibiendo en los últimos años un creciente reconocimiento. Las medidas técnicas o procedimentales por sí solas no van a resolver los actuales problemas de seguridad, siendo necesario que operen de manera coordinada con los usuarios y usuarias de las empresas y organizaciones (ENISA, 2018; Aldawood y Skinner, 2018; Zhang-Kennedy, 2021). Abundando en esta idea, el CCN-CERT en su informe *Ciberamenazas y Tendencias 2019* alerta sobre la necesidad de llevar a cabo actividades de formación y concienciación, afirmando que "los seres humanos siguen siendo el eslabón débil en todos los sistemas de seguridad, por lo que, a medida que aumente la eficacia de las protecciones contra código dañino, los agentes de las amenazas modificarán su objetivo, atacando a las personas".

> Una empresa puede gastar cientos de miles de dólares en *firewalls*, sistemas de detección de intrusos, cifrado y otras tecnologías de seguridad, pero si un atacante puede contactar con una persona de la empresa, esa persona le res-

> ponde y el atacante accede, entonces todo ese dinero gastado en tecnología no habrá servido para nada (Mitnick, 2005).

Estas palabras, pronunciadas en el año 2005 por Kevin Mitnick, el primer *hacker* que utilizó técnicas de ingeniería social para acceder a algunos de los ordenadores más seguros de su época, siguen plenamente vigentes, y sirven para ilustrar la idea de que la formación y concienciación en seguridad de la información deben desempeñar un papel fundamental en la minimización de los riesgos de seguridad de las empresas y organizaciones en general, y de las universidades en particular.

Presentada una primera aproximación de las amenazas y dificultades que conforman el problema que esta tesis aborda, a continuación se presentan y exponen las razones que justifican su realización.

1.3. Justificación

El nivel de conocimiento y concienciación en materia de seguridad "afecta de manera significativa el comportamiento hacia la seguridad de la información y debe considerarse por ello como un factor crítico en la efectividad de la seguridad" (Mahfuth et al., 2017). Esta criticidad se produce tanto en los perfiles técnicos y profesionales como en las personas que interrelacionan con los sistemas como usuarias.

Para afrontar esta situación, una de las estrategias consideradas más eficaces son las actividades de formación destinadas tanto a explicar la importancia y necesidad de la seguridad de la información como a instruir en el modo en que se interrelaciona con las distintas funciones laborales que conforman los puestos de trabajo de una organización (Infante-Moro et al., 2022; Chowdhury et al., 2022).

En la actualidad, existen multitud de iniciativas formativas enfocadas a mejorar la cultura de la seguridad. A nivel internacional, caben destacar dos marcos de referencia (Estepa et al., 2021): el ACM *Cybersecurity Curricula Guideline* (ACM y IEEE, 2020) y la *National Initiative for Cybersecurity Education*, NICE (NICE, 2021). El primero está orientado al diseño de grados universitarios en seguridad de la información, mientras que el segundo define las competencias y conocimientos que deben alcanzar los trabajadores y trabaja-

doras TIC en el ámbito de la ciberseguridad. También el *Marco europeo de competencias digitales*, DIGCOMP (Comisión Europea, 2020), identifica competencias en el ámbito de la seguridad de la información dirigidas a los ciudadanos y ciudadanas de Europa.

Para los perfiles técnicos, en España existe una creciente oferta académica que proporciona formación de calidad. En el momento de redactar este trabajo, las universidades españolas ofertan sesenta y ocho programas de Máster y cuatro estudios de grado sobre ciberseguridad o seguridad de la información (INCIBE, 2019b).

Pero si las universidades aseguran un currículo contrastable y coherente para los perfiles profesionales, no ocurre lo mismo con la formación destinada a los usuarios y usuarias que no poseen un perfil técnico. Debido a la naturaleza compleja del dominio de la seguridad de la información, las empresas y organizaciones se enfrentan a considerables dificultades para implantar y gestionar un sistema de formación y concienciación en seguridad eficaz y sostenible.

Para dar respuesta a esta situación, las organizaciones o bien llevan a cabo una formación de carácter generalista, con contenidos limitados y sin criterios contrastados que permitan asegurar su idoneidad, o construyen desarrollos internos, desde cero y a medida de sus necesidades, lo que lleva aparejado un alto coste y esfuerzo (Lebek et al., 2013; Beuran et al., 2019; Hatzivasilis et al., 2020).

Los planes de formación generalistas, más allá de una primera aproximación e introducción a la materia, no pueden constituir el núcleo de una formación y concienciación de garantía. Los distintos perfiles profesionales que existen en una organización en general, y en una universidad en particular, requieren formación, atención y recursos adecuados a su desempeño y grado de responsabilidad. Respecto al uso de soluciones a medida, no cabe duda que resultan de gran utilidad al adaptarse a las necesidades y objetivos de la organización que las implanta, pero también presentan dificultades y limitaciones. Su complejidad de diseño y puesta en marcha, unida a los elevados costes, tanto económicos como en dedicación de personal, son un importante freno para acometer estos proyectos. Solo escasas corporaciones tienen los recursos y la voluntad de abordarlos. Y cuando se llevan a cabo, sus resultados no pueden extrapolarse o ser utilizados en otros entornos al

ser desarrollados para dar respuesta específica al alcance y entorno definidos.

En el ámbito competencial, las empresas que tienen implantado un sistema de gestión por competencias de manera mayoritaria llevan a cabo sus propios análisis y desarrollos. Un estudio de la Chartered Institute of Personel and Development realizado en el Reino Unido, muestra que el 85 % de los mapas de competencia son desarrollos internos, bien en solitario o apoyados en una consultora externa (Taylor, 2007). Sin embargo, este enfoque, al igual que en el caso de los planes de formación y concienciación a medida, limita la posibilidad de disponer de mapas comunes y compartidos y aprovechar las ventajas que esto supondría, a lo que hay que añadir su elevado coste.

Otra opción consiste en utilizar alguno de los numerosos modelos de gestión por competencias existentes en el mercado. A modo de ejemplo, en el entorno educativo destaca el proyecto universitario europeo *Tuning* (EEES, 2020). Este proyecto, puesto en marcha el año 2000, tiene como objetivo concretar la aplicación del Proceso de Bolonia en las instituciones de educación superior europeas. Se trata de un proyecto especialmente relevante y de validez reconocida a nivel mundial (González y Wagenaar, 2003). En él se expresa de forma nítida la relevancia y necesidad de expresar los procesos y resultados del aprendizaje en términos de competencias. En el ámbito empresarial se pueden citar el Catálogo Nacional de Cualificaciones Profesionales (INC, 2020), la clasificación europea ESCO (ESCO, 2020) de capacidades, competencias, cualificaciones y ocupaciones, o las recogidas por la Organización Internacional del Trabajo, OIT (OIT, 2020). En el ámbito de la seguridad de la información cabe señalar el Programa de capacitación y concienciación sobre seguridad de la información del National Institute of Standards and Technology, NIST (Wilson y Hash, 2003), o el ya citado NICE.

En las universidades españolas, las labores de formación y concienciación en seguridad que se llevan a cabo no cuentan a día de hoy con un modelo o estándar de referencia basado en competencias que apoye y facilite la configuración o validación de planes de formación y concienciación destinadas al personal. La única iniciativa existente es el convenio marco de colaboración entre la Asociación de Universidades Españolas, Crue, e INCIBE, firmado en el año 2016. Pero este proyecto, de indudable relevancia y significación, tiene como único objetivo desarrollar actividades básicas y generalistas de concienciación sobre ciber-

seguridad en las universidades. (CRUE-TIC, 2021). Así mismo, una gestión de seguridad eficaz requiere que las organizaciones puedan evaluar la efectividad y nivel de impacto de sus actividades de formación y concienciación en el comportamiento de los empleados y empleadas (Beautement et al., 2016).

Para superar los problemas y limitaciones descritas, algunos autores (Ruth, 2006; Urquiza, 2009), proponen explorar innovaciones metodológicas que simplifiquen la generación de marcos de competencia, de tal manera que los recursos destinados a la generación de mapas de competencia puedan ser asumidos por un mayor número de organizaciones, y que el retorno de la inversión y los beneficios obtenidos sean mejor comprendidos y valorados por la dirección de las empresas.

En línea con esta propuesta, esta tesis contribuye a mejorar las limitaciones expuestas. En primer lugar define, a partir del correspondiente análisis, el mapa funcional de competencias en seguridad de la información para el personal no TIC de las universidades españolas, es decir, aquel que utiliza las TIC a nivel de usuario. A continuación identifica los roles laborales no TIC existentes en las universidades, los niveles de desempeño y finalmente construye el mapa de competencias específico para cada perfil laboral universitario identificado. El resultado proporciona por tanto un conjunto de competencias técnicas y niveles de concienciación y formación para cada perfil de usuario o usuaria no técnico, todo ello organizado en un marco común medible, reproducible y consistente.

Como segunda contribución significativa al cuerpo de conocimiento, se explora y propone el uso de estándares de la industria en la elaboración de mapas funcionales. Esta línea de investigación se lleva a cabo mediante la incorporación al modelado del mapa funcional de las medidas de seguridad recogidas en el Anexo II del Esquema Nacional de Seguridad, ENS (BOE, 2010), norma de obligado cumplimiento para todas las universidades públicas y un referente para el resto de universidades. Este enfoque tiene como objetivo agilizar y facilitar la construcción de mapas de competencias, así como dotarles de un mayor nivel de estandarización.

Desde un punto de vista competencial, los resultados de este trabajo permiten incorporar al mapa general de competencias laborales de las universidades las competencias en

seguridad de la información, concediéndoles una necesaria visibilidad y consideración. La metodología desarrollada posibilita disponer de un criterio estándar para diseñar planes de formación, dotando a los responsables de formación en seguridad de las universidades españolas de una herramienta con la que pueden configurar o validar sus propios planes, así como diseñar de manera conjunta planes de formación compartidos, al contar con un corpus de competencias normalizado. Se entiende por normalización de competencia "la formalización de una competencia a través del establecimiento de estándares que la convierten en un referente válido para un determinado colectivo" (Irigoin y Vargas, 2002, p. 66).

1.4. Objetivos de la investigación

De acuerdo con las propuestas y argumentos presentados, y con el propósito de dar respuesta a las carencias señaladas, esta tesis propone la construcción de un mapa de competencias laborales en el ámbito de la seguridad de la información orientado a la mejora y promoción de las actividades de formación y concienciación del personal no TIC de las universidades españolas.

Para ello, este trabajo plantea un modelo que responde a la pregunta de investigación principal: ¿cuáles son las competencias laborales y nivel de desempeño en el ámbito de la seguridad de la información que debe alcanzar cada perfil laboral universitario no TIC?

Las preguntas de investigación específicas (PI) a las que esta tesis dará respuesta son:

- PI1. ¿Cuál es el estado de la formación y concienciación en seguridad de la información en las universidades españolas?
- PI2. ¿Qué medidas de seguridad del ENS aplican en un mapa funcional de competencias de usuarios y usuarias no TIC de las universidades españolas?
- PI3. ¿Cuáles son las actitudes y conocimientos asociadas a las medidas de seguridad identificadas?
- PI4. ¿Qué perfiles de usuarios y usuarias no TIC pueden establecerse atendiendo a sus necesidades en el ámbito de la seguridad de la información para su puesto de

trabajo y responsabilidad?

- PI5. ¿Cuál es el mapa de competencias derivado del mapa funcional construido y en qué grado aplican los conocimientos y actitudes para cada uno de los roles definidos?

Vinculado con la pregunta principal y con las específicas, se plantea como objetivo general construir el mapa de competencias en seguridad de la información para cada rol laboral no TIC identificado, basado en el diseño y creación de un mapa funcional de competencias utilizando para ello las medidas de seguridad del Anexo II del ENS.

Como objetivos específicos:

- OE1. Conocer el estado de la formación y concienciación en seguridad de la información en las universidades españolas.
- OE2. Identificar las medidas de seguridad del ENS que aplican en un mapa funcional dirigido a usuarios y usuarias no TIC de las universidades españolas.
- OE3. Establecer las actitudes y conocimientos asociadas a las medidas de seguridad identificadas.
- OE4. Construir el mapa funcional en el ámbito de la seguridad de la información para el personal no TIC de las universidades españolas, basado en las medidas del Anexo II del ENS.
- O5. Identificar los perfiles de usuarios y usuarias no TIC de acuerdo con el nivel de conocimiento y concienciación en materia de seguridad de la información necesario para el adecuado desarrollo de sus actividades.
- OE6. Construir el mapa de competencias en seguridad de la información para cada perfil identificado, incluyendo los niveles de conocimiento y concienciación que deben alcanzarse.

Estos objetivos específicos ayudan a resolver y completar el objetivo principal. El modelo propuesto facilitará el posterior diseño, elaboración, seguimiento y control de planes de formación y concienciación. Las personas responsables de los procesos de formación podrán contar con indicadores de desempeño y evaluación contra los que validar los planes anuales de formación de su organización y controlar su evolución. También ofrecerá datos compara-

bles con otras universidades, lo que puede ayudar a elaborar estudios y análisis agregados, facilitar estrategias de *benchmarking* o compartir estrategias y esfuerzos de formación.

1.5. Alcance y limitaciones del trabajo

Llegados a este punto, y conocidos tanto el ámbito del problema como la justificación y objetivos de este trabajo, es conveniente delimitar su alcance y señalar las limitaciones y restricciones del mismo. Como ya se ha explicado, esta tesis circunscribe sus aportaciones al mapa de competencias laborales del personal no TIC de las universidades españolas, respondiendo a la pregunta de investigación principal. El aporte metodológico empleado, consistente en utilizar un estándar de la industria para la identificación de competencias, se limita al alcance citado.

Como ya se ha explicado, el trabajo de investigación identifica los diferentes perfiles labores desde el punto de vista de la seguridad de la información en las universidades españolas, diseña el mapa funcional, determina los niveles de desempeño y construye el mapa de competencias. Para ello emplea la metodología del Análisis Funcional que se presenta y explica en el capítulo 2, obteniendo como resultado la formulación de las competencias laborales en el ámbito definido que los trabajadores y trabajadoras no TIC de las universidades españolas deben conocer y comprender. Sin embargo, se sale del propósito y marco de este trabajo la elaboración completa de la norma de competencia. De acuerdo con ello, en esta tesis se definen las unidades y los elementos de competencia que conforman el mapa de competencias, pero no los criterios de desempeño ni los procesos de obtención de evidencias de conocimiento.

Por otro lado, el mapa de competencias propuesto identifica los conocimientos, comportamientos y capacidades necesarias en el ámbito de la seguridad de la información. Pero su uso no se restringe a las actividades de formación y concienciación. También permite mejorar y satisfacer las necesidades actuales y futuras en el ámbito de la gestión de recursos humanos, como pueden ser el establecimiento de remuneraciones, la gestión de planes de carrera, las mejoras en la organización del trabajo o los procesos de selección de personal. Pero estos aspectos no se desarrollan en esta tesis, que se orienta a remarcar el aporte que un mapa de competencias basado en el ENS supone para las necesarias tareas

de formación y concienciación en materia de seguridad.

También resulta conveniente anotar que esta tesis no plantea una validación del mapa de competencias obtenido. Dos son los motivos. El primero de ellos es el elevado coste temporal que supone la realización de un proceso de evaluación basado en el mapa resultante, muy superior a las posibilidades de este trabajo, ya que para ello sería necesario, como se ha explicado, completar la norma de competencia. El segundo motivo son las dudas sobre el valor que aportaría un proceso de validación, teniendo en cuenta que el punto de partida son las medidas del Anexo II del ENS, un estándar de facto de seguridad en España.

1.6. Estructura de la tesis

En esta sección se presenta la estructura de la presente tesis doctoral. Esta consta de seis capítulos y un apartado dedicado a los anexos. En el primer capítulo se realiza una breve introducción al tema de la tesis, presentando el problema a resolver, la justificación y contribuciones de este trabajo al ámbito investigado, así como los objetivos y alcance de la investigación.

En el segundo capítulo se muestra el estado del arte de los diferentes ámbitos de conocimiento tratados en este trabajo: se presentan los conceptos más relevantes sobre seguridad de la información, se repasan los principales estándares de la industria referidos a la seguridad de la información, y se lleva a cabo una aproximación a la gestión por competencias y a la cultura de la seguridad de la información.

El tercer capítulo analiza con detalle el problema que busca resolver esta tesis a través de un estudio detallado tanto de la seguridad en el contexto empresarial español como en las universidades españolas. Para comprender con mayor profundidad el problema así como para identificar otras posibles propuestas previas, se cierra el capítulo con un análisis sistemático de la literatura.

El cuarto capítulo describe de manera pormenorizada la metodología de investigación que se ha llevado a cabo. Se trata de un capítulo relevante, ya que la propia metodología utilizada en este trabajo es una de las aportaciones de esta tesis.

En el capítulo quinto se detalla el proceso que se lleva a cabo para dar respuesta tanto

a la pregunta de investigación principal como a las preguntas y objetivos específicos. En este capítulo se presentan los resultados de esta tesis, consistentes en el mapa funcional de competencias laborales en el ámbito de la seguridad de la información, los perfiles laborales no TIC en las universidades españolas, y el correspondiente mapa de competencias.

Finalmente, en el sexto capítulo se exponen las conclusiones, se repasan y confirman las aportaciones de la tesis y se plantean nuevas líneas de trabajo que completen y amplíen los pasos iniciados en este estudio.

Capítulo 2

Estado de la cuestión

"Un año allí y aún soñaba con el ciberespacio... aún veía
la matriz durante el sueño: brillantes reticulados
de lógica desplegándose sobre aquel incoloro vacío".

Neuromante

2.1. Conceptos y consideraciones sobre la seguridad de la información

Para contar con un marco de información común sobre el que se organicen y expliquen las propuestas y aportaciones de este trabajo, es conveniente conocer en primer lugar aquellos conceptos más relevantes en varios dominios del conocimiento. La seguridad de la información y los distintos elementos que la conforman constituyen el punto de partida. Se continúa, por su relevancia para esta tesis, con un repaso a los marcos de seguridad y estándares de la industria más significativos, para analizar a continuación la trascendencia de la cultura organizacional en general y de la cultura de la seguridad en particular. El capítulo finaliza con un análisis del significado e importancia de la gestión por competencias y con una revisión de los principales modelos de competencia laborales existentes.

2.1.1. Securitización

A finales del siglo XX, los estudios de seguridad estratégica comenzaron a trabajar con lo que se denominó una *visión ampliada*. Frente a los enfoques que restringían las amenazas a peligros de carácter militar, emerge una corriente que considera necesaria la ampliación de la agenda de seguridad, incluyendo otros ámbitos, como el ecológico, el social o

el tecnológico, que, bajo esta nueva concepción, pasan a convertirse en posibles amenazas (Treviño, 2016). Estas amenazas potenciales, en muchas ocasiones injustificadas, permiten respaldar la aprobación de mayores recursos económicos, policiales o militares, la restricción de derechos o el incremento de la vigilancia y el control. En esta interpretación de la realidad, cualquier tema puede ser *securitizado*, es decir, convertido en una amenaza para la seguridad (Lipschutz, 1995, pp. 46-86).

Hablar de interpretación de la realidad no es casual, ya que la securitización es ante todo la construcción de un discurso, es decir, la elaboración de mensajes y significados mediante diferentes recursos expresivos y estrategias. Un discurso que persigue, como ya se ha indicado, transformar un problema en una amenaza. Las estrategias de securitización no son monopolio del Estado. Pueden ser promovidas por políticos, medios de comunicación o grupos de presión (Buzan et al., 1998). O como afirma Ole Waever en *Securitization and Desecuritization*, "por definición, algo es un problema de seguridad cuando las élites declaran que lo es" (Lipschutz, 1995, p. 52).

Es conveniente por tanto analizar si la seguridad de la información en general está sujeta a un proceso de securitización. El Real Decreto-ley 14/2019, más conocido como *decretazo digital*, que permite al Gobierno intervenir las telecomunicaciones sin orden judicial, puede ser buen punto de partida para abordar este tema. Esta ley hace referencia a "las actividades de desinformación, las interferencias en los procesos de participación política de la ciudadanía y el espionaje" como "actividades ilícitas que impactan en la seguridad pública" lo que pone de relieve "la necesidad de modificar el marco legislativo vigente para hacer frente a la situación" (BOE, 2019). Otra forma de abordar este análisis es comparar el impacto de los riesgos de la seguridad de la información con otros riesgos. Como ya se ha citado, frente a los riesgos derivados de ciberataques y robos masivos de datos, los principales riesgos globales son los desastres climáticos y naturales. A modo de ejemplo, tan solo la inundación de los monzones de 2018 en India causó la muerte de 1.424 personas durante el período de verano de junio a agosto, con un coste de cinco mil millones de dólares (Martín, 2019). Y aunque hay informes que indican que las muertes por ciberataques podrían llegar a ser numerosas (Straub, 2019), afortunadamente se está muy lejos de las cifras causadas por otro tipo de catástrofes.

Aunque esta breve reflexión sobre el nivel de securitización de la seguridad de la información resulta pertinente en el contexto de esta tesis, conviene señalar que sobrepasa el alcance de la misma. Aunque no se produzcan muertes ni daños billonarios, no cabe duda de que las amenazas a los datos y a la información pueden ser muy disruptivos y tener un elevado coste económico. Por ello, conviene señalar que este estudio se centra en la identificación de las competencias laborales en el ámbito de la seguridad de la información que faciliten y favorezcan actividades de formación y concienciación, y no en una necesidad derivada de una supuesta amenaza o emergencia social.

2.1.2. Ciberespacio

Ciberespacio, ciberseguridad, cibernauta, cibercafé, ciberataque, cibersexo o ciberarte hacen alusión a nuevas realidades creadas a partir del entorno informático y de las redes de comunicaciones (RAE, 2019). El origen del prefijo *ciber* fue utilizado por primera vez por el matemático norteamericano Norbert Wiener en su libro *Cybernetics, or Control and Communication in the Animal and the Machine*, publicado en 1948. En él proponía una teoría sobre las relaciones de control y comunicación entre máquinas y animales, a la que denominó Cibernética, con la que ilustraba y adelantaba el contenido de su teoría (Enciclopedia Británica, 2019).

El término ciberespacio apareció por primera vez en la famosa novela de ciencia ficción *Neuromante*, de William Gibson, publicada en 1984. En ella, el ciberespacio se mostraba como una representación metafórica que representaba los datos y conexiones del mundo real, denominada *matriz*, a la que se accedía a través de interfaces de realidad virtual (Gibson, 1997). El posterior desarrollo de la tecnología convirtió esta imaginativa visión en la forma de identificar la nueva realidad que estaba surgiendo. Sin embargo, en la actualidad no existe un consenso sobre este término, de modo que hay una amplia gama de definiciones de acuerdo con el punto de vista que se adopte (Ottis y Lorents, 2010). Esta disparidad de definiciones ha llevado a algunos investigadores, como Lance Strate (1999), a construir una taxonomía que ayude a organizar y explicar este polisémico término. Lance lo divide en tres niveles. El nivel inicial, o nivel cero, agrupa los enfoques centrados en el ciberespacio como espacio imaginario, simulado o irreal. En el siguiente nivel, el nivel

uno, se encuentran las definiciones asociadas a aspectos físicos (equipamientos informáticos, infraestructura de telecomunicaciones, conexiones o usuarios), conceptuales (aspectos metáforicos, lógicos o retóricos del término) y perceptivos (espacio virtual). Finalmente, el último nivel, el nivel dos, engloba a los enfoques centrados en la transmisión y recepción de información. (interrelaciones sociales, interacciones personales) (Strate, 1999).

Para los objetivos de esta tesis, se adopta la propuesta del Departamento de Defensa de Estados Unidos, que define ciberespacio como "un dominio global dentro del entorno de la información que consiste en una infraestructura tecnológica y de datos que incluyen Internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores" (DOD, 2019). O la definición muy semejante del CCN-CERT, que define ciberespacio como el "dominio global y dinámico compuesto por infraestructuras de tecnología de la información, incluyendo internet, redes de telecomunicaciones y sistemas de información" (CCN-CERT, 2010).

2.1.3. Ciberseguridad vs. Seguridad de la información

Como se expone a continuación, el término ciberseguridad está de plena actualidad. La frecuencia y gravedad de los ataques informáticos que han sufrido y siguen sufriendo relevantes empresas y organizaciones en todo el mundo han convertido esta palabra en habitual y recurrente en los medios de comunicación y en las conversaciones comunes. Esto ha provocado que cualquier aspecto relacionado con la seguridad de la información se considere ciberseguridad. Sin embargo son conceptos diferentes. Resulta por tanto necesario aclarar el significado y alcance de ambos términos, así como la relación entre ellos.

Ciberseguridad

Bajo el término ciberseguridad se agrupan e intervienen diferentes disciplinas, como la informática, las telecomunicaciones, la criptología, aspectos legales o de privacidad, así como intereses muy dispares: económicos, técnicos, políticos o industriales. También se trata de un término cada vez más utilizado, tal y como puede apreciarse en la figura 2.1 donde se muestra la evolución entre enero de 2015 y mayo de 2022 de las búsquedas realizadas en Google del término ciberseguridad en España, incluyendo una línea de tendencia que

permite apreciar con mayor claridad dicha progresión, desde valores iniciales en el índice próximos a 10, hasta alcanzar un valor cercano a 100 a mediados del año 2022. En el gráfico también se pueden observar con claridad los picos de mayo de 2017, en los días posteriores al ataque global de ransomware a Telefónica y a otras grandes compañías, y de enero de 2022, coincidente con la publicación del primer ciberataque Ruso contra Ucrania.

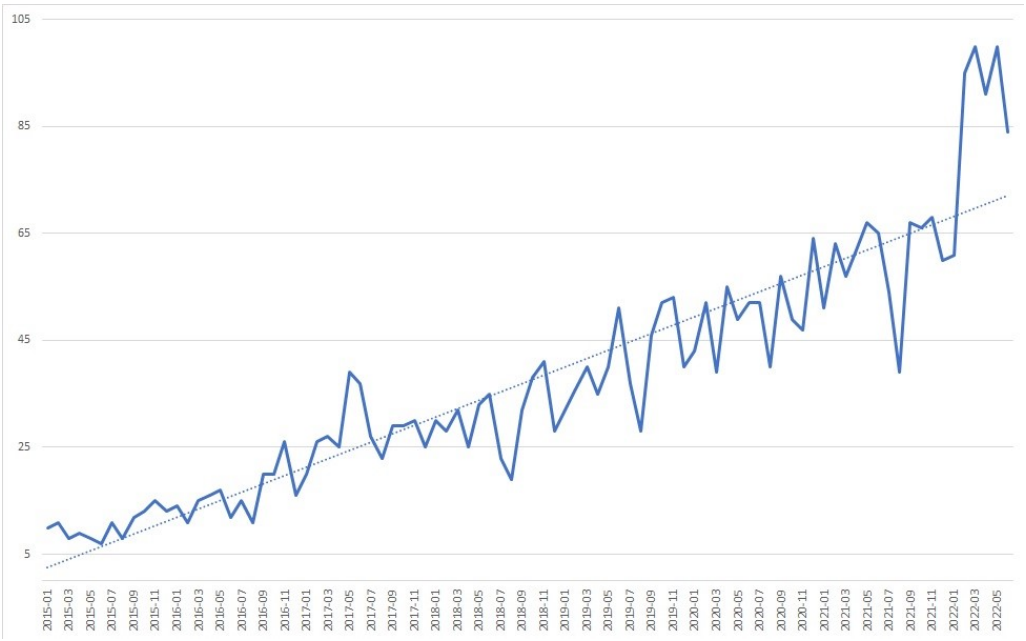

Figura 2.1: Evolución del término ciberseguridad en Google
Fuente: Elaboración propia

Dada la amplia utilización del término y los distintos conceptos y significados que agrupa, el concepto de ciberseguridad conlleva un elevado número de definiciones, que en ocasiones pueden llegar a producir confusión. El propio avance de la tecnología y los procedimientos que la acompañan también obligan a su permanente revisión y actualización. Resulta por tanto necesario aclarar el significado del término que se utiliza en este trabajo, y de manera especial diferenciarlo del relativo a la seguridad de la información.

El término ciberseguridad no está recogido en el *Diccionario de la Real Academia Española de la Lengua*, RAE. Sin embargo, existe una amplia literatura científica que aborda este tema. Los investigadores Dan Craigen (2014), Nadia Diakun-Thibault (2014) y Randy Purse (2014), en su artículo "Defining Cybersecurity", repasan las definiciones existentes hasta ese momento, seleccionando nueve de ellas, para finalmente proponer su propia definición del término. "La ciberseguridad es la organización y conjunto de recursos, procesos

y estructuras utilizadas para proteger el ciberespacio y sus sistemas de los sucesos que desalinean de jure los derechos de propiedad de facto" (Craigen et al., 2014).

Esta definición resulta especialmente interesante por plantear la ciberseguridad como "una organización y conjunto de procesos". En efecto, la ciberseguridad no se limita a los aspectos técnicos, ya que los procedimientos y procesos son connaturales y relevantes en todo sistema de gestión. Respecto al ámbito que se debe proteger, el ciberespacio y sus sistemas, permite diferenciarlo del concepto seguridad de la información, más amplio y que engloba al primero. Sin embargo, resulta muy restrictiva la asociación de los problemas de seguridad con la pérdida, de hecho o de iure, de derechos de propiedad. Esta interpretación deja fuera del alcance incidentes que no suponiendo merma de derechos de propiedad son considerados incidentes de seguridad, como por ejemplo la caída temporal de un servidor.

Una definición que especifica con detalle el ámbito de actuación la ofrece Kaspersky, la conocida multinacional dedicada a la seguridad informática. No obstante, solo habla de ataques maliciosos. "La ciberseguridad es la práctica de proteger computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes y datos de ataques maliciosos" (Kaspersky, 2019).

ISACA, organización referente en el desarrollo de metodologías y certificaciones en actividades de auditoría y control de sistemas de información, evita las anteriores restricciones, refiriéndose a activos de información y amenazas. "La protección de los activos de información abordando las amenazas a la información procesada, almacenada y transportada por sistemas de información interconectados" (ISACA, 2020).

Una definición muy conocida es la propuesta por la Cybersecurity and Infrastructure Security Agency de Estados Unidos, que define ciberseguridad como "el arte de proteger redes, dispositivos y datos contra el acceso no autorizado o el uso delictivo para garantizar la confidencialidad, integridad y disponibilidad de la información" (CISA, 2009). Al igual que las definiciones precedentes, presenta algunas lagunas, como considerar incidentes de seguridad únicamente a los producidos por accesos no autorizados o comportamiento criminal, obviando los problemas técnicos o los errores no intencionados de los usuarios y usuarias.

La definición del NIST da respuesta a estas limitaciones. “Prevención de daños, protección y restauración de computadoras, sistemas de comunicaciones electrónicas, infraestructuras de red y servicios, incluida la información contenida en ellas, para garantizar su disponibilidad, integridad, autenticación, confidencialidad y no repudio” (Paulsen y Byers, 2019).

Daniel Schatz (2017), Rabih Bashroush (2017) y Julie Wall (2017) en su artículo “Towards a More Representative Definition of Cyber Security” también llevan a cabo un pormenorizado repaso de las definiciones existentes, para después de un elaborado análisis proponer una nueva definición (Schatz et al., 2017).

> El enfoque y las acciones asociadas con los procesos de gestión de riesgos de seguridad seguidos por organizaciones y estados para proteger la confidencialidad, integridad y disponibilidad de datos y activos utilizados en el ciberespacio. El concepto incluye pautas, políticas y colecciones de salvaguardas, tecnologías, herramientas y capacitación para proporcionar la mejor protección para el estado del entorno cibernético y sus usuarios.

Esta definición, aunque presenta algunos de los problemas ya anotados en anteriores definiciones, como la referencia al ciberespacio, incluye un aspecto de sumo interés: la referencia a la ciberseguridad como actividades asociadas a un sistema de gestión de riesgos. Esta definición cambia el enfoque basado en la protección por un enfoque basado en el análisis de riesgos. Amplía por tanto las actividades de la seguridad de la información no solo a tareas reactivas, y se centra en actividades de carácter proactivo derivadas de dicho análisis.

Un enfoque de sumo interés es el que presentan Rossouw von Solms (2013) y Johan van Niekerk (2013) en su artículo “From information security to cyber security”. Proponen que la ciberseguridad supere los límites de la seguridad de la información tradicional para incluir no solo la protección de los recursos de información, sino también la de otros activos, incluidas las personas. En el ámbito de la ciberseguridad, afirman, este factor tiene una dimensión más amplia, en la que las personas se convierten en objetivos potenciales o en participantes inconscientes de ataques, y por tanto deben ser protegidas. Resulta interesante este punto de vista, ya que implica aspectos éticos al incluir la protección

de grupos sociales vulnerables ante actividades como el ciberacoso o los ataques a la privacidad.

En cualquier caso, en esta tesis la ciberseguridad presenta un alcance limitado al sistema de gestión de la seguridad de la información de una organización. Por ello, se utiliza la definición recogida por el CCN-CERT, que define ciberseguridad como el "conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan".

Seguridad de la información

El NIST define seguridad de la información como "la protección de la información y los sistemas de información contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados para proporcionar confidencialidad, integridad y disponibilidad" (Paulsen y Byers, 2019). Una definición muy semejante a la del CCN-CERT, que emplea la del estándar ISO 27001: "la preservación de la confidencialidad, la integridad y la disponibilidad de la información" (CCN-CERT, 2010).

Ambas definiciones presentan aspectos de interés que conviene señalar. En primer lugar, la forma de garantizar la confidencialidad, integridad y disponibilidad de la información es mediante un proceso sistemático, documentado y conocido, es decir, mediante la existencia de un Sistema de Gestión de la Seguridad de la Información, SGSI. El ENS en su Artículo 5 subraya esta idea, señalando que "la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del SGSI estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural" (BOE, 2010).

En segundo lugar, tal y como señalan ambas definiciones, para garantizar una correcta gestión de la seguridad de la información se deben garantizar los aspectos básicos de confidencialidad, integridad y disponibilidad, representadas de manera habitual como un triángulo, tal y como se muestra en la figura 2.2.

La propia definición del estándar ISO/IEC 27001 hace referencia a estas tres dimensiones básicas de la seguridad de la información:

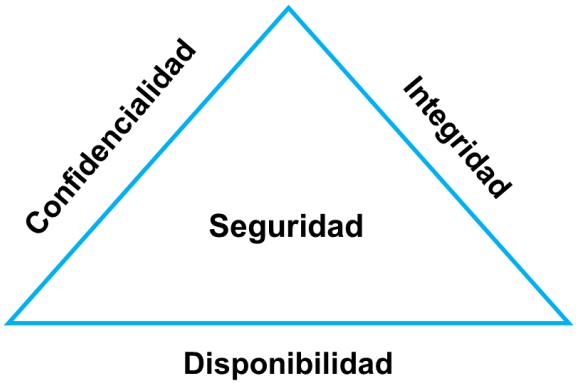

Figura 2.2: Triángulo de la seguridad
Fuente: Elaboración propia basada en Pfleeger, 1989

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

El aseguramiento de la confidencialidad, integridad y disponibilidad de la información en una organización ha sido el primer requisito de seguridad de la información, establecido desde los inicios de la informática. Charles P. Pfleeger, en su libro *Security in Computing*, ya en su primera edición de 1989, afirmaba que "para que un Sistema de Información pueda permanecer seguro es necesario que éste presente sus tres propiedades esenciales" (Pfleeger, 1989).

Este primer y sencillo modelo de representación de la seguridad de la información ha evolucionado con el paso del tiempo. Señalando algunos de los modelos posteriores, en 1991 John McCumber presenta el conocido "Cubo de McCumber" (McCumber, 1991). McCumber considera la seguridad como un cubo de tres dimensiones en las que se definen los estados de información, las dimensiones de seguridad ya mencionadas y las medidas de seguridad, tal y como se muestra en la figura 2.3.

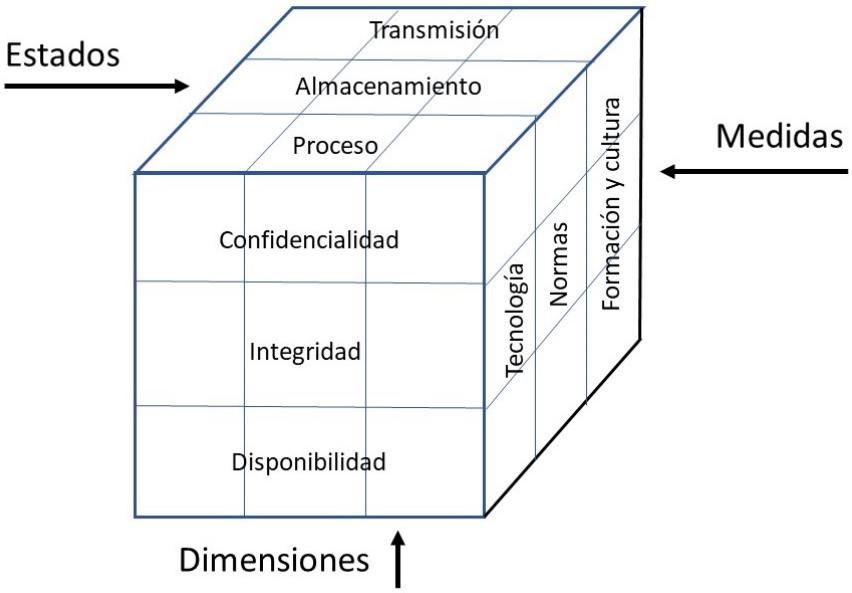

Figura 2.3: Cubo de McCumber
Fuente: Elaboración propia basada en McCumber, 1991

Donn B. Parker, en 1998, propone un nuevo modelo incluyendo tres nuevas categorías a las tres iniciales: posesión, autenticidad y utilidad (Pender-Bey, 2019). W. Victor Maconachy amplía el cubo de McCumber en 2001 introduciendo la dimensión temporal, así como la autenticación y el no repudio (Maconachy et al., 2001). En 2011, The Open Group publica su estándar de gestión de seguridad de la información O-ISM3 (TheOpenGroup, 2021). Posteriormente han aparecido nuevas propuestas, pero el cumplimiento de las tres dimensiones básicas de la seguridad sigue siendo un referente.

Diferencias entre ciberseguridad y seguridad de la información

A la vista de lo dicho en las páginas anteriores, puede deducirse que:

- La seguridad de la información, independientemente del soporte, protege la información y los sistemas que la gestionan. Estos sistemas, denominados *activos de información*, incluyen no solo a los dispositivos informáticos. También engloban a la información soportada en papel o el conocimiento de las personas, así como todos los activos de información asociados, como archivadores, fotocopiadoras o armarios (López y Ruiz, 2012).

- La ciberseguridad se centra en la protección de la información digital, asociada exclusivamente a sistemas informáticos y de comunicaciones digitales.

De acuerdo con estas consideraciones, la seguridad de la información tiene un alcance más amplio, incluyendo dentro del mismo a la ciberseguridad. La seguridad de la información, por tanto, se relaciona con la adecuada protección de los activos de información, digitales o no, y la prestación continuada de los servicios de TI que proporcionan empresas y organizaciones. Para ello, deben contar con las medidas de seguridad necesarias para mantener un nivel de riesgo aceptable, así como realizar un seguimiento continuo de los niveles de prestación de servicios, analizar las vulnerabilidades reportadas y preparar una respuesta efectiva a los incidentes.

Como aclaración metodológica, a lo largo de esta tesis, con el objeto de facilitar la lectura, se utiliza el término seguridad como sinónimo de seguridad de la información.

2.1.4. Gobernanza, riesgo y cumplimiento

En las primeras páginas de esta tesis se ha presentado una perspectiva sobre el impacto de las TIC en la sociedad en general y en las empresas y organizaciones en particular, constatando la cada vez mayor dependencia en los sistemas de información y las amenazas y vulnerabilidades que esta realidad presenta. Se ha explicado que a medida que la inversión en TIC aumenta, y con ello la dependencia de la misma, se hace más necesario crear procedimientos y marcos que permitan minimizar y paliar las dificultades que genera dicha dependencia. La manera más adecuada de organizar y dar respuesta a esta necesidad es mediante un Marco de Gobierno, Riesgo y Cumplimiento, GRC. Este marco, en el ámbito de la TIC, tiene como objetivo establecer una estrategia que garantice la gobernanza, la gestión de los riesgos y el cumplimiento de las obligaciones regulatorias para de este modo garantizar los objetivos estratégicos de una organización (Grama y Petersen, 2013).

Gobernanza y sistemas de gestión

El gobierno TIC es el área de una organización que permite "asegurar que las políticas y estrategias TIC se implementan, y que los procesos requeridos se siguen correctamente. El Gobierno TIC incluye definir roles y responsabilidades, medir y reportar, así como tomar

acciones para resolver cualquier asunto identificado" (CCN-CERT, 2010).

Entre los principales objetivos de un gobierno TIC pueden señalarse:

- Asegurar la alineación de los objetivos estratégicos de la organización con los objetivos TIC.
- Cumplir con las obligaciones legales, las normas de la organización y los propios requerimientos del departamento TIC.
- Mantener la confianza en los servicios de TIC de la organización.
- Garantizar el retorno de la inversión en TIC.

Para lograr estos objetivos existen marcos de gobierno TIC, como el estándar UNE-ISO/IEC 38500:2013, *Gobernanza corporativa de la Tecnología de la Información*, o el *Marco de buenas prácticas para el gobierno y gestión TI*, COBIT. Aunque se encuentran muy relacionados, estos marcos de gobierno no deben ser confundidos con los Sistemas de Gestión de Servicios TI, SGSTI, como ITIL o ISO 20000. Los primeros se encargan de fijar las estrategias TI junto con las políticas y controles, mientras que los segundos tienen como principal objetivo gestionar todas las actividades dirigidas a la prestación de los servicios TIC que se entregan a las partes interesadas.

La gestión de la seguridad de la información forma parte de estas actividades. Las organizaciones se encuentran amenazadas por riesgos que pueden poner en peligro la integridad de su información y con ello la propia viabilidad de sus metas y objetivos. Como se explicará más adelante, en este contexto es crítico conocer el riesgo al que están sometidos los sistemas para poder gestionarlos. Para evitar o minimizar estos riesgos, las organizaciones deben establecer, operar, monitorear, mantener y mejorar la seguridad de su información. Estos objetivos deben estar organizados y sistematizados en políticas, procedimientos, recursos y actividades, que se organizan dentro de un SGSI (López y Ruiz, 2012). De esta manera, un SGSI forma parte de un SGSTI, y éste a su vez está dirigido y controlado por un marco de gobernanza TI. Aunque los distintos marcos y buenas prácticas más relevantes intentan abarcar y dar respuesta a todo el marco de GRC, y por ello presentan ámbitos comunes, la relación entre el gobierno TI, el SGSTI y el SGSI puede ilustrarse de

manera esquemática en el gráfico 2.4 (Fernández y Piattini, 2012).

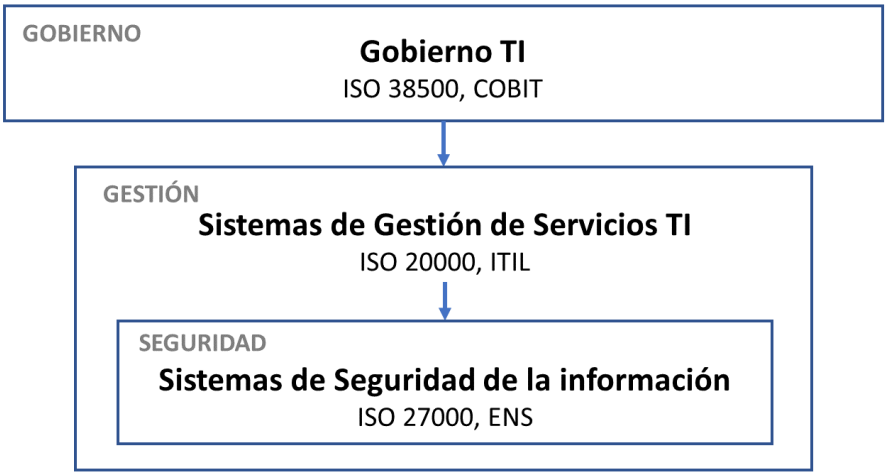

Figura 2.4: Marcos de gobierno, gestión TI y seguridad
Fuente: Elaboración propia

En líneas generales, un SGSI establece tres fases recurrentes: en primer lugar identifica, analiza y ordena la estructura de los activos de información de una organización, en segundo lugar facilita la definición de procedimientos de trabajo que permiten gestionar la seguridad, y finalmente dispone de controles que posibilitan medir la eficacia de las medidas adoptadas (INTECO, 2009). Con el resultado del análisis de dichos controles realimentará la información sobre la estructura de activos y modificará los procedimientos de trabajo, en un proceso de mejora continua.

Este modelo de funcionamiento es el que se describe en la definición de un SGSI que establece el ENS (BOE, 2010):

> Un sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

Gestión de riesgos

La gestión estratégica moderna "considera un principio fundamental que las decisiones de gobierno se fundamenten en el conocimiento de los riesgos que implican" (Mañas,

2012). De ahí resulta la relevancia que en los últimos años ha adquirido la gestión de riesgos, entendida como la actividad dirigida a la identificación y la gestión de las posibles amenazas de una organización, con el objetivo de analizarlos y establecer estrategias para su control. En este contexto, se considera amenaza cualquier factor que potencialmente pueda ocasionar daño a una organización. (CCN-CERT, 2010)

Bajo este enfoque, los sistemas de información se encuentran sujetos a amenazas y debilidades, y en consecuencia a riesgos. Para mantenerlos bajo control, deben ser gestionados. En primer lugar, identificando, analizando y cuantificando los riesgos, y en segundo lugar, tratándolos para que sean asumibles (Mañas, 2012). El ENS en su artículo 6 señala la necesidad de esa gestión y sus objetivos: "La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables" (BOE, 2010).

A continuación, para una mejor comprensión de la gestión de riesgos, se repasan brevemente los principales conceptos.

Activos de información Una primera aproximación al concepto de activo puede encontrarse en el Plan General de Contabilidad, que define activo como todo recurso beneficioso para una organización. "Bienes, derechos y otros recursos controlados económicamente por la empresa, resultantes de sucesos pasados, de los que se espera que la empresa obtenga beneficios o rendimientos económicos en el futuro" (BOE, 2007b).

Una segunda definición más ajustada al ámbito de estudio de esta tesis es la que propone el NIST, que define activo como "un elemento de valor para el logro de la misión organizacional y los objetivos comerciales" (Paulsen y Byers, 2019). En esta definición, el valor del activo deriva de la aportación del bien a la consecución de las metas de la organización, y no de su valor o rendimiento económico.

El NIST define activo de información como "una aplicación, sistema, programa, espacio físico, personal o equipamiento lógicamente relacionado" (Paulsen y Byers, 2019). Se trata de una definición semejante a la que propone el estándar ISO 27001, que define activo de información como "cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización" (López y Ruiz, 2012). El ENS, en su definición pone el foco en los riesgos a los que están

expuestos los activos. “Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización” (BOE, 2010).

Amenazas El estándar ISO 27001 define amenaza como “cualquier circunstancia o evento que puede explotar, intencionadamente o no una vulnerabilidad y provocar un incidente” (López y Ruiz, 2012). Es una definición semejante a la que propone la Asociación Española de Normalización (UNE) en su norma UNE 71504:2008. “Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización” (UNE, 2008).

Salvaguardas Se entiende por salvaguarda el procedimiento o mecanismo tecnológico que reduce el riesgo de un activo de información (Mañas, 2012). Este concepto está muy unido al de vulnerabilidad, que es la ausencia o la mayor o menor ineficacia de una salvaguarda. También puede definirse como “la debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas” (López y Ruiz, 2012).

De acuerdo con estas definiciones, entre las amenazas y las salvaguardas existe una relación inversamente proporcional. Una mayor eficacia de la salvaguarda supone un menor nivel de amenaza y al contrario, una salvaguarda poco eficaz o inexistente se traduce en una amenaza mayor. En consecuencia, la probabilidad de materialización de una amenaza es función tanto de la propia naturaleza de la amenaza como del nivel de salvaguardas del activo amenazado.

Impacto Se denomina impacto a “la consecuencia que sobre un activo tiene la materialización de una amenaza” (Mañas, 2012). El nivel de impacto dependerá del valor del activo, siendo mayor cuanto mayor sea el valor del activo. No se debe confundir valor con coste. El valor de un activo está asociado a la cantidad y criticidad de la información que maneja, a los servicios que presta y al valor acumulado, es decir, a la suma del valor de los activos que dependen de él.

En el gráfico 2.5 se muestra la relación entre estos conceptos.

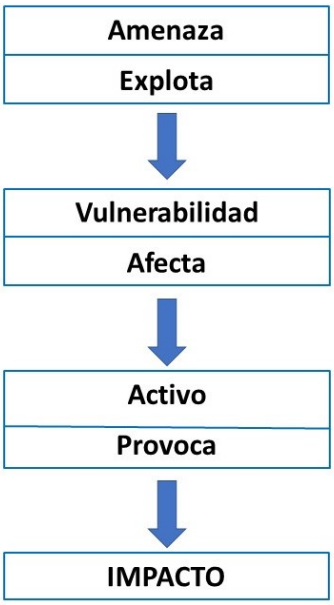

Figura 2.5: Activo, amenaza, vulnerabilidad e impacto
Fuente: INCIBE

Riesgo

Explicados los anteriores conceptos, ya se puede definir el riesgo como la probabilidad de que las amenazas exploten vulnerabilidades de un activo o grupo de activos de información y causen daño a una organización (López y Ruiz, 2012). Se trata de un valor cuantitativo que se expresa como el producto del valor del impacto debido a la materialización de una amenaza por la probabilidad de que esta ocurra.

Una vez identificados, analizados y cuantificados los riesgos mediante el análisis de riesgos, se debe llevar a cabo un plan de tratamiento de los mismos. El análisis de riesgos y su posterior tratamiento configuran la gestión de riesgos de una organización.

En un plan de tratamiento de riesgos, los riesgos deben (INCIBE, 2015, p. 7):

- Evitarse o eliminarse.
- Reducirse o mitigarse.
- Transferirse.
- Asumirse.

Las medidas a adoptar dependen de muchos factores que la organización debe valorar, pero fundamentalmente del nivel de impacto y probabilidad, tal y como se muestra en el gráfico 2.6.

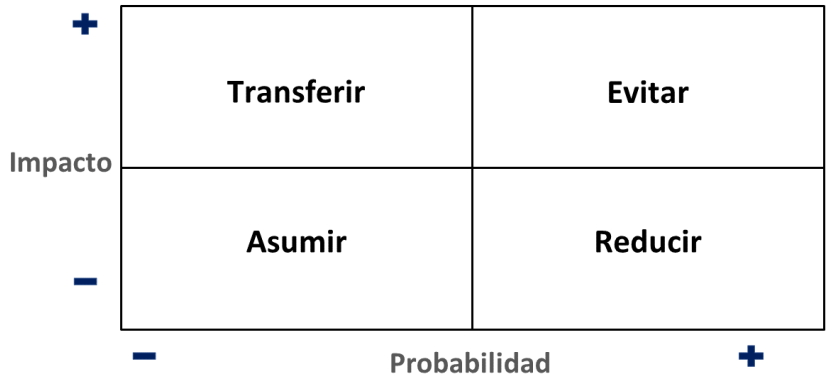

Figura 2.6: Gestión de riesgos
Fuente: Propia

MAGERIT Acrónimo de *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*, MAGERIT es, como su nombre indica, una metodología de análisis de riesgos perteneciente al Ministerio de Asuntos Económicos y Transformación Digital. Es una herramienta libre, utilizada por las organizaciones certificadas en el ENS para llevar a cabo su gestión de riesgos, siguiendo para ello los pasos que se señalan a continuación (Mañas, 2012).

- Definir los activos relevantes en una organización, sus relaciones y su valor, entendido como el coste que supondría su degradación.
- Identificar a qué amenazas están expuestos los activos.
- Determinar qué salvaguardas existen y su nivel de eficacia para mitigar el riesgo.
- Evaluar el impacto, entendido como el daño sobre el activo derivado de la materialización de la amenaza.
- Estimar el riesgo, definido como el impacto ponderado por la probabilidad de que se materialice la amenaza.

Cumplimiento, marco legal y jurídico

Además de las propias necesidades de las organizaciones, existe un amplio marco legal y jurídico que busca preservar la confianza en la confidencialidad, disponibilidad e integridad de los sistemas de información de los organismos de las Administraciones Públicas españolas y de las organizaciones que se relacionen con ellas, así como proteger los datos y la privacidad de los usuarios y usuarias, aspectos que también forman parte del ámbito de la seguridad de la información. Presentar todas las leyes y normas que de manera directa o indirecta abordan la seguridad de la información sobrepasa, por su amplitud, el alcance de esta tesis. Sin embargo, resulta necesario repasar, al menos de forma resumida, las normativa más relevante, así como su evolución y desarrollo. Para un mayor detalle se puede consultar el *Código de Derecho de la Ciberseguridad* (BOE, 2022a), un extenso y completo compendio del marco normativo español en la materia, publicado por el INCIBE y el Boletín Oficial del Estado.

La Constitución Española de 1978, en su artículo 18.4, ya establece la primera referencia a la necesidad de garantizar la intimidad de las personas. "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos" (BOE, 1978). No será sin embargo hasta el año 1992 cuando se publique la primera ley que busca dar respuesta y contenido a este artículo. Será la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, más conocida como LORTAD. En su artículo 1 establece que el objeto de esta ley, será "limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos" (BOE, 1992).

Ese mismo año la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en su artículo 45 señala: "Las Administraciones Públicas impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y el ejercicio de sus competencias, con las limitaciones que a la utilización de estos medios establecen la Constitución y las Leyes" (BOE, 1992).

Dos eran por tanto las preocupaciones en ese momento: mejorar el funcionamiento interno de la administración pública mediante el uso de la informática y garantizar, de acuerdo con la constitución, el derecho a la intimidad de las personas.

La mencionada ley 5/1992 es derogada por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. En su artículo 1 establece el objeto de esta ley, con la primera referencia explícita a la protección de los datos personales: "La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar" (BOE, 1999).

En el año 2007 se promulga la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Se trata de la primera ley que aborda íntegramente la administración electrónica, bajo la necesidad, expresada en su artículo 1, de asegurar "la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias", y de reconocer, en su artículo 6, el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos (BOE, 2007a):

> Se reconoce a los ciudadanos el derecho a relacionarse con las Administraciones Públicas utilizando medios electrónicos para el ejercicio de los derechos previstos en el artículo 35 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, así como para obtener informaciones, realizar consultas y alegaciones, formular solicitudes, manifestar consentimiento, entablar pretensiones, efectuar pagos, realizar transacciones y oponerse a las resoluciones y actos administrativos.

Finalmente, en su artículo 42 establece el objeto del Esquema Nacional de Seguridad, ENS, y se anuncia su futura creación.

El ENS se desarrolla en el Real Decreto 3/2010, de 8 de enero. En su Preámbulo se señala el objetivo del ENS: "Fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones

funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas". En el artículo 1 se establece la obligación de su cumplimiento para las Administraciones Públicas: "Será aplicado por las Administraciones Públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias". También señala la obligatoriedad de aplicar las instrucciones técnicas de seguridad, publicadas por el CCN-CERT: "El Ministerio de Hacienda y Administraciones Públicas... a iniciativa del Centro Criptológico Nacional, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento" (BOE, 2010).

El Real Decreto 951/2015 actualiza el ENS. En su introducción se señala el objetivo de esta actualización (BOE, 2015b):

> Las ciberamenazas, que constituyen riesgos que afectan singularmente a la Seguridad Nacional, se han convertido en un potente instrumento de agresión contra las entidades públicas y los ciudadanos en sus relaciones con las mismas... Por todo ello, y en particular dada la rápida evolución de las tecnologías de aplicación y la experiencia derivada de la implantación del Esquema Nacional de Seguridad, aconsejan la actualización de esta norma.

La Ley 11/2007 es derogada por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, avanzando en el objetivo de que los ciudadanos y ciudadanas puedan relacionarse con la administración por medios electrónicos. En su artículo 12 establece la obligación de las Administraciones Públicas de "garantizar que los interesados pueden relacionarse con la Administración a través de medios electrónicos, para lo que pondrán a su disposición los canales de acceso que sean necesarios así como los sistemas y aplicaciones que en cada caso se determinen". Y en su artículo 13, respecto a las relaciones de las personas con las Administraciones Públicas, se establecen los derechos "a la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas" (BOE, 2015).

Esta referencia a la necesidad de proteger los datos también aparece en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. En su artículo 3.2 señala que "las Administraciones Públicas se relacionarán... a través de medios electrónicos, que... garantizarán la protección de los datos de carácter personal" (BOE, 2015a).

En el año 2016 se publica el Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 donde se establecen las normas relativas a la protección de las personas físicas respecto al tratamiento de sus datos personales y a la libre circulación de tales datos (BOE, 2016a).

La preocupación por la privacidad de los datos surge por la confluencia de varios factores. En primer lugar, el desarrollo de nuevas tecnologías y herramientas informáticas que capturan, gestionan, procesan y analizan ingentes volúmenes de datos. El análisis de estos datos supone para los estados y organizaciones la posibilidad, hasta hace poco inalcanzable, de poder anticipar tendencias y conocer con extremado detalle los comportamientos y motivaciones de sus clientes o ciudadanos. En segundo lugar, el elevado volumen de datos que se generan, de manera voluntaria o involuntaria, a través del empleo de las tecnologías. Y en tercer lugar el ya explicado factor humano, es decir, el desconocimiento o despreocupación por las consecuencias de los dos primeros factores.

Esta situación es descrita en el Reglamento General de Protección de Datos, RGPD, en su Sexto Considerando (BOE, 2016a):

> La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades.

En el Decimoprimer Considerando, el legislador expresa la necesidad de proteger los datos personales. "La protección efectiva de los datos personales en la Unión exige que se refuercen y especifiquen los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal" (BOE, 2016a).

Así pues, los datos que ya aparecían protegidos tanto en el ámbito general de la seguridad de la información como en el más específico de la ciberseguridad, suman una nueva dimensión de protección que las organizaciones deben gestionar, y sobre la que deben concienciar y formar.

Finalmente, la Ley 15/1999 es derogada por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Esta ley adapta la legislación española al Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

La Comisión Europea, como parte de su estrategia de seguridad de la información, aprueba la Directiva conocida como NIS, *Network and Information Systems* (ENISA, 2016) el 9 de julio de 2016, en un contexto de constante preocupación por los cada vez más frecuentes incidentes de seguridad que afectan a agencias gubernamentales, infraestructuras críticas, universidades y a numerosas empresas y organizaciones de Europa. A partir de esta fecha, los estados miembros han ido adoptando sus legislaciones nacionales a esta directiva, transposición que se completa en el año 2018. En el caso español, el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (BOE, 2018) transpone al ordenamiento jurídico español la Directiva NIS, estableciendo, de acuerdo con el CCN-CERT (2021) "el marco estratégico e institucional de seguridad de las redes y sistemas de información, la supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales, así como la gestión de incidentes de seguridad".

A finales de 2020, la Comisión Europea decide revisar su normativa sobre la seguridad de las redes y sistemas de información (CE, 2020) con el triple objetivo de evaluar si en efecto la legislación existente había ayudado a la mejora de la seguridad, identificar áreas y tareas pendientes de abordar o resolver, y definir y cuantificar los costes y beneficios obtenidos hasta la fecha. Esta evaluación permitió conocer la desigual trasposición de la Directiva entre los distintos países, la necesidad de asegurar una mayor armonización, la conveniencia de simplificar los procedimientos existentes, así como la importancia de contar con la industria para mejorar la eficacia de la Directiva. El resultado de todo ello ha sido

la elaboración y presentación de una propuesta para la futura aprobación de una nueva Directiva NIS (CE, 2021), conocida como Directiva NIS 2.0, que corrige las limitaciones de la primera Directiva.

En el Anexo A se presenta de manera esquemática y resumida el marco legal y jurídico explicado en esta sección. Para una mejor comprensión, se ha incluido una columna, identificada como "Tipo", que indica si se trata de una norma aplicada al régimen y procedimiento administrativo, al ámbito de la privacidad o a la seguridad de la información.

Para finalizar este recorrido por la legislación más significativa referida a protección de datos y seguridad de la información, en el gráfico 2.7 se presenta la evolución a lo largo del tiempo de la relación existente entre las distintas normas, tipificadas de acuerdo con sus objetivos. También aparece sombreada la legislación vigente en la actualidad, a la que se hará referencia en este trabajo.

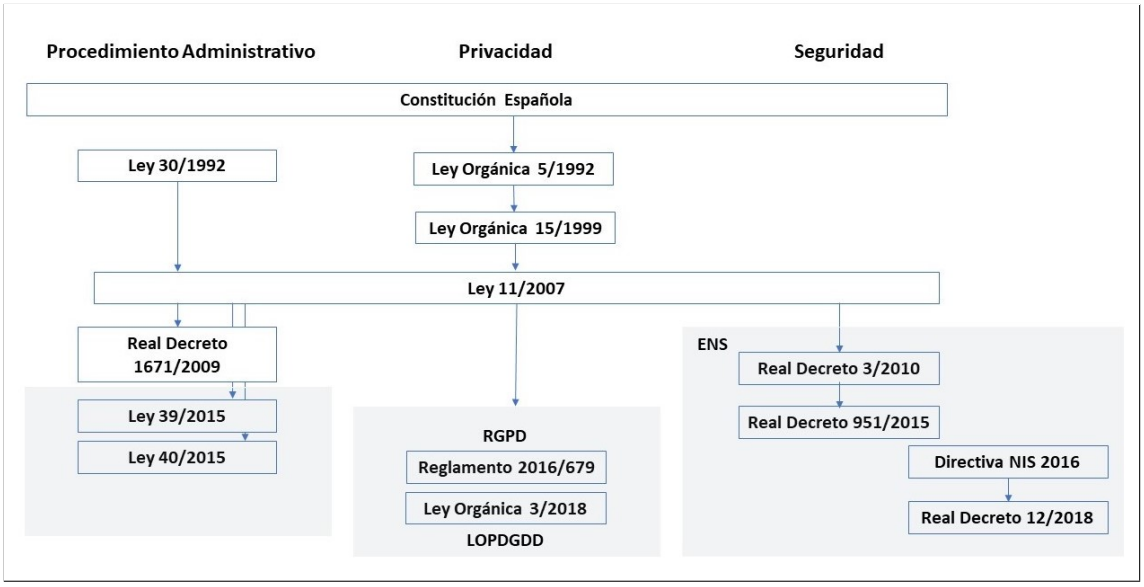

Figura 2.7: Evolución de la legislación
Fuente: Elaboración propia

Cumplimiento corporativo La World Compliance Association define el cumplimiento corporativo, más comúnmente conocido como *corporate compliance* o simplemente *compliance*, como "un conjunto de procedimientos y buenas prácticas adoptados por las organizaciones para identificar y clasificar los riesgos operativos y legales a los que se enfrentan y establecer mecanismos internos de prevención, gestión, control y reacción frente a los

mismos" (WCS, 2019).

Referido a la seguridad, el cumplimiento corporativo se define como el conjunto de procedimientos establecidos en las organizaciones para verificar que se cumple y respeta:

- La legislación relacionada con la seguridad de la información y la privacidad.
- Las regulaciones de la industria de obligado cumplimiento en el ámbito de la seguridad.
- Los estándares, buenas prácticas o certificaciones de seguridad exigidas por un tercero, como clientes, socios o colaboradores.

Incluso a la vista de la definición y características del cumplimiento corporativo referido a la seguridad de la información, es fácil confundirlo con la gestión de la seguridad de la información. Ambos conceptos presentan en efecto objetivos y características comunes que provocan esta confusión. En efecto, un mismo cometido o procedimiento puede considerarse parte de un SGSI cuando el fin perseguido es la seguridad, y también parte del cumplimiento corporativo cuando es requerido por obligación legal o es necesario para establecer relaciones con los *stakeholders*.

Sin embargo, aunque los objetivos pueden coincidir en muchas ocasiones, el alcance es diferente. El cumplimiento se centra específicamente en los requisitos de terceras partes. Bajo este enfoque, la seguridad es relevante en tanto en cuanto forma parte de los requerimientos exigidos por un tercero, mientras que un SGSI debe atender a la seguridad integral de la organización. Por tanto, un SGSI enfocado únicamente al cumplimiento puede resultar peligroso, ya que el mero cumplimiento no garantiza una adecuada seguridad.

Estándares y Normas Para garantizar la seguridad de la información de una organización es necesario implantar un SGSI que, basado en el análisis de los riesgos, implemente, gestione y mejore la seguridad de la información. Por su relevancia en el entorno español e internacional, en la siguiente sección se analizan tanto el Esquema Nacional de Seguridad como el estándar internacional en seguridad de la información ISO 27000.

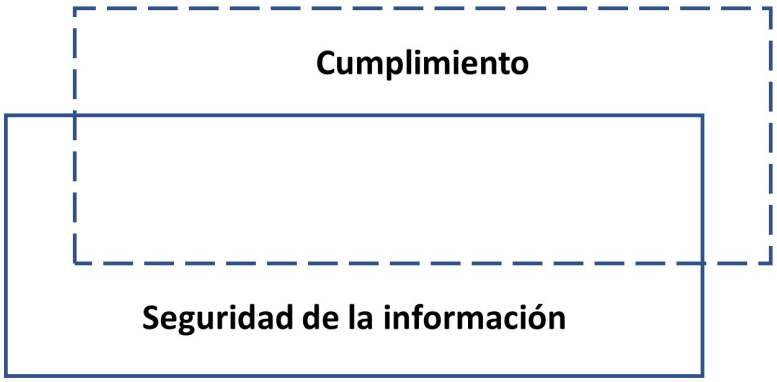

Figura 2.8: Seguridad de la información vs. cumplimiento
Fuente: Elaboración propia

Arquitectura de seguridad de la información La Open Security Architecture, OSA, define una arquitectura de seguridad de la información como "los artefactos de diseño que describen cómo se posicionan los controles de seguridad y cómo se relacionan con la arquitectura general de TI. Estos controles sirven para mantener los atributos de calidad del sistema, entre ellos la confidencialidad, la integridad, la disponibilidad, la responsabilidad y la garantía" (OSA, 2020).

Una arquitectura efectiva de seguridad debe reunir cinco principios (Tang, 2014):

- Orientada al negocio. Todas las metas y objetivos de seguridad de la información deben provenir de las necesidades del negocio, lo que garantiza que la seguridad de la información siempre haga lo correcto en el momento correcto.
- Alineada con otros modelos. La arquitectura de seguridad debe ser coherente y ajustarse bien con los marcos, arquitecturas y procesos existentes dentro de cada organización.
- Marco integrador. Existe un elevado número de regulaciones, leyes, estándares y mejores prácticas relacionadas con la seguridad de la información. Por ello es muy conveniente utilizar una arquitectura de seguridad que englobe todos los requisitos de auditoría y, por otro lado, reduzca las duplicidades entre esas regulaciones y estándares.
- Pensamiento sistémico. Entender la seguridad de la información como un elemento

del sistema general de una organización en general permite integrar la realidad de la organización, proporcionando mejores soluciones a sus requerimientos.

- Sencillo de utilizar. Una arquitectura de seguridad compleja resulta difícil de gestionar y mantener, y por ello corre el peligro de que no se utilice correctamente o que incluso se deje de usar.

2.1.5. Ecosistema de seguridad

Repasados los conceptos más relevantes referentes a la seguridad de la información, el gráfico 2.9 muestra de forma visual lo expuesto hasta el momento en este capítulo, incluyendo los conceptos abordados y la relación existente entre los mismos, y que se resume a continuación.

Un SGSI agrupa al conjunto de actividades, informatizadas o no, relacionadas con la seguridad de la información de una organización. Sus principales referencias son la familia de estándares de seguridad ISO 27000, un conjunto de guías y buenas prácticas para la implantación y uso de un SGSI. La preocupación del legislador español por asegurar el derecho de los ciudadanos a relacionarse con la administración de manera informática o telemática obliga a un adecuado nivel de seguridad y protección, lo que deriva en la existencia de un SGSI específico y de obligado complimiento para toda la administración, el ENS.

La ciberseguridad se centra en la protección tanto de los activos informatizados como en otros riesgos asociados al uso del ciberespacio. Los datos personales y protegidos forman parte de los activos de información, informatizados o no, pero sus características provocan que tengan un tratamiento más riguroso, recogido tanto en el RGPD como en el LOPDGDD.

En todos los casos se han de cumplir las leyes y regulaciones existentes en el ámbito de la seguridad como parte del cumplimiento corporativo.

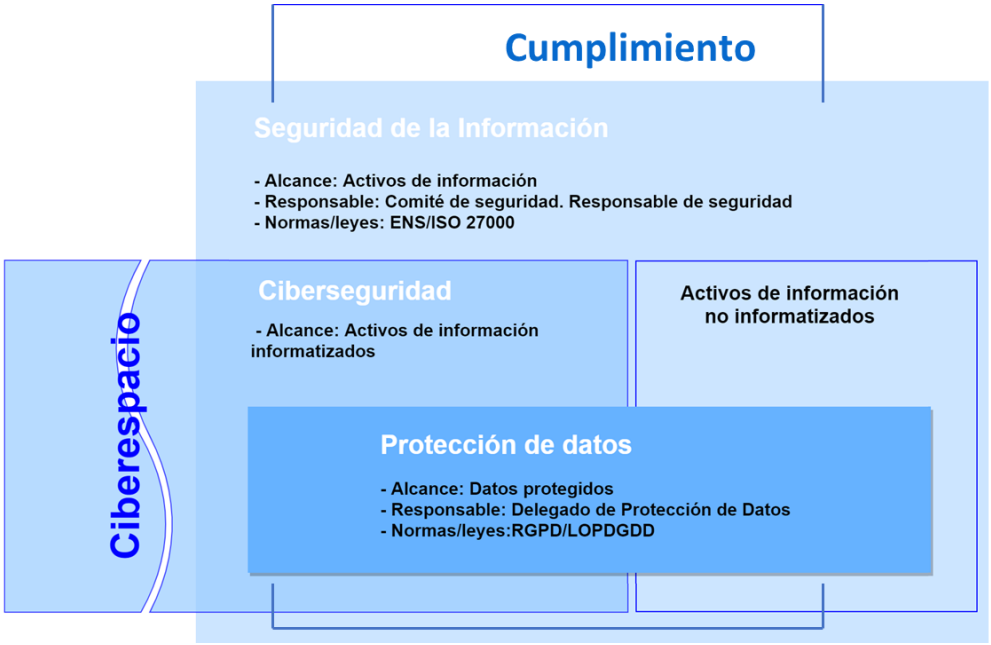

Figura 2.9: Ecosistema de seguridad de la información
Fuente: Elaboración propia

2.2. Estándares y marcos de seguridad

Una vez revisados los conceptos más relevantes en el ámbito de la seguridad de la información así como la interrelación entre los mismos, a continuación se presentan y repasan, por su relevancia en esta investigación, los estándares de la industria, así como los marcos de seguridad que son referentes internacionales para todo tipo de empresas y organizaciones.

2.2.1. Esquema Nacional de Seguridad

La aprobación del ENS en el año 2010 supuso el establecimiento de una política de seguridad que persigue la adecuada protección de la información en las Administraciones Públicas que llevan a cabo actividades de administración electrónica e interoperabilidad de servicios (BOE, 2010), entre las que se encuentran la mayor parte de las universidades españolas (CRUE-TIC, 2020). Se trata de una ley que recoge, organiza y normaliza un amplio, estructurado y específico conocimiento sobre seguridad de la información, de obligado cumplimiento para todas las empresas y organismos públicos, así como para las empresas del sector privado que prestan servicios a entidades públicas. También es una referencia en materia de seguridad de la información para muchas empresas españolas del sector privado.

El ENS es el resultado de un largo trabajo coordinado por el Ministerio de la Presidencia, por el Ministerio de Política Territorial y Administración Pública, con el apoyo del Centro Criptológico Nacional (CCN) y la participación de todas las Administraciones Públicas, incluyendo las universidades, a través de los órganos colegiados con competencias en materia de administración electrónica, como el Consejo Superior de Administración Electrónica, el Comité Sectorial de Administración Electrónica y la Comisión Nacional de Administración Local. También se han considerado en su elaboración los informes preceptivos del Ministerio de Política Territorial, del Ministerio de la Presidencia, de la Agencia Española de Protección de Datos y del Consejo de Estado, así como con la opinión de las asociaciones de la Industria del sector TIC (CCN-CERT, 2021a).

El contenido de la ley se articula de la siguiente manera: (PAE, 2020)

- Los principios básicos a considerar en las decisiones en materia de seguridad de la información, presentados en el capítulo II.
- Los requisitos mínimos que permiten una adecuada protección de la información, recogidos en los artículos 11 a 26.
- La adquisición de productos de seguridad y la contratación de servicios de seguridad, desarrolladas en el artículo 18 y el anexo V.
- El cumplimiento de los requisitos mínimos, recogido en los artículos 27, 43, 44, y en los anexos I y II.
- El criterio de utilización de infraestructuras y servicios comunes mencionado en el artículo 28.
- La necesidad de cumplir y atender las instrucciones técnicas de seguridad y guías de seguridad, señalada en el artículo 29 y en la disposición adicional cuarta.
- Las condiciones y requerimientos técnicos en las comunicaciones electrónicas y los mecanismos de firma electrónica descritos en el capítulo IV.
- El establecimiento de las auditorías de seguridad, desarrollado en el artículo 34 y el anexo III.
- La respuesta a incidentes de seguridad, explicada en los artículos 36 y 37.

- El establecimiento de las normas de conformidad, recogido en los artículos 38 a 41.
- La necesidad de actualización permanente, declarada en el artículo 42.
- la obligación de categorizar los sistemas, desarrollado en el capítulo X.

Anexo I

Las categorías de los sistemas de información se presentan en el Anexo I de la ley, donde se definen las categorías y se explica la forma en que se determina la categoría de un sistema.

La determinación de la categoría de un sistema se basa en la valoración del impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información, repercutiendo en la capacidad del sistema para cumplir sus objetivos, proteger los activos de información, respetar la legalidad y proteger los derechos de las personas (CCN-CERT, 2015).

Para poder conocer el nivel de impacto de un incidente de seguridad sobre una empresa u organización, se consideran las denominadas *dimensiones de la seguridad*:

- Disponibilidad. Las entidades o procesos autorizados tienen acceso a los activos cuando lo requieren.
- Autenticidad. Una entidad es lo que dice ser.
- Integridad. Un activo no ha sido alterado de manera no autorizada.
- Confidencialidad. La información se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados.
- Trazabilidad. Las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

De acuerdo con el nivel de impacto observado, derivado del grado de afección a una o varias dimensiones de seguridad sobre el sistema de información, se determina el nivel o categoría del sistema:

- BAJA. Cuando las consecuencias de un incidente de seguridad supongan un perjuicio limitado sobre las funciones, activos o personas de una organización.

- MEDIA. Cuando las consecuencias de un incidente de seguridad supongan un perjuicio grave.
- ALTA. Cuando las consecuencias de un incidente de seguridad supongan un perjuicio muy grave.

Anexo II

Para los objetivos de esta tesis destaca el artículo 27, donde se recoge el cumplimiento de los requisitos mínimos (BOE, 2010):

> Para dar cumplimiento a los requisitos mínimos establecidos en el presente real decreto, las Administraciones Públicas aplicarán las medidas de seguridad indicadas en el Anexo II, teniendo en cuenta:
>
> - Los activos que constituyen el sistema de información.
> - La categoría del sistema, según lo previsto en el artículo 43.
> - Las decisiones que se adopten para gestionar los riesgos identificados.

Estos requisitos se distribuyen en setenta y cinco indicadores distribuidos en tres marcos, cada uno de ellos, exceptuando el primero, dividido a su vez en varios apartados:

- Marco organizativo. Cuatro indicadores. Constituido por medidas relacionadas con la organización general de la seguridad.
- Marco operacional. Treinta y un indicadores. Formado por las medidas encaminadas a proteger la operación del sistema de información.
- Medidas de protección. Cuarenta indicadores. Orientadas a proteger los activos según su naturaleza y el nivel de seguridad requerido.

Las medidas recogidas en el Anexo II se utilizan en esta tesis para diseñar y construir el mapa de competencias. Su origen, diseño, rigor y alcance las convierten en un excelente alternativa para alcanzar los objetivos propuestos (Mendívil et al., 2021):

- Tal y como ya se ha explicado, son medidas de obligado cumplimiento para todas las Administraciones Públicas, incluidas las universidades, así como un referente y

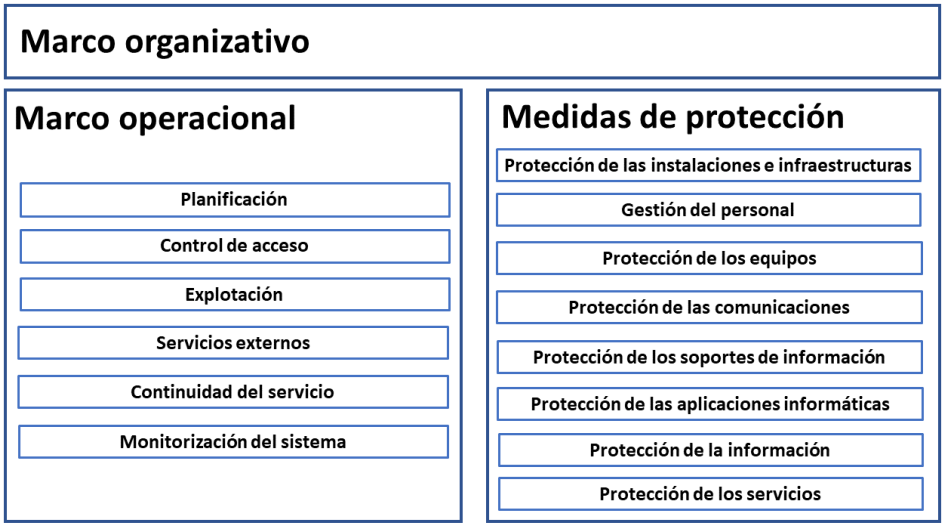

Figura 2.10: Organización de las medidas de seguridad del ENS
Fuente: Elaboración propia

estándar de cumplimiento en el ámbito de la seguridad de la información para muchas otras organizaciones y empresas españolas.

- Son el resultado de un largo y minucioso proceso de análisis y estudio realizado desde el más alto nivel y con una visión integral, por lo que su utilidad y pertinencia están fuera de duda.

- Su uso permite establecer la necesaria relación entre la necesidad de cumplimiento y el modo en cómo hacerlo efectivo en el ámbito de la formación y concienciación, dando de este modo cumplida respuesta a las medidas "5.2.3 Concienciación" y "5.2.4 Formación" del propio Anexo II, en los que se explicita la necesidad de llevar a cabo de manera regular todas las acciones que sean necesarias para formar y concienciar al personal sobre su responsabilidad en la seguridad de los sistemas de información.

2.2.2. ISO 27000

ISO e IEC mantienen desde el año 2005 un conjunto de estándares que, agrupados bajo la denominación ISO 27000, proporcionan un sistema de gestión de la seguridad de la información para las organizaciones. En la actualidad es un referente mundial sobre todos los aspectos concernientes a la seguridad de la información, y como puede apreciarse en la figura 2.11, un estándar con un nivel de implantación muy elevado y en constante

crecimiento. (ISO, 2018)

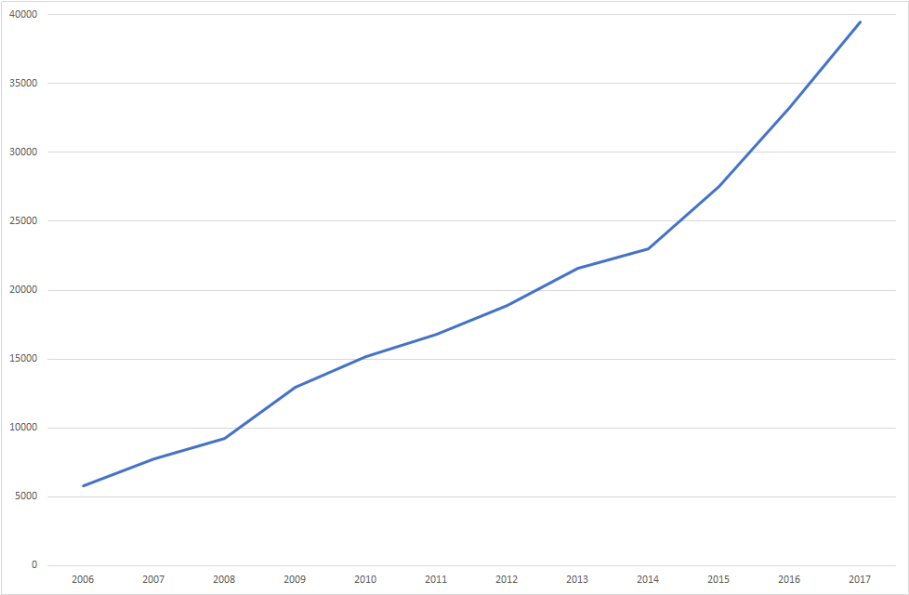

Figura 2.11: Certificaciones en ISO 27001 en el mundo
Fuente: Elaboración propia

El origen de esta familia de normas fue la norma BS 7799 publicada en 1995 por la British Standards Institution, BSI, con el objetivo de establecer un conjunto de buenas prácticas para la gestión de la seguridad de la información en las empresas. Al tratarse de una guía de buenas prácticas, no se establecía un esquema de certificación, entendiendo por tal el conjunto de reglas, procedimientos y gestiones que deben acreditar las organizaciones que deseen obtener la certificación del cumplimiento de una norma por parte de una entidad certificadora. En el año 1998 se publica una segunda parte de la norma, en la que se establecen los requisitos para certificar un SGSI.

En el año 2000 la norma es adoptada por ISO, con el nombre de ISO 17799. En el año 2005, se actualizó y publicó con el nombre de ISO 27001. En paralelo, la norma BS 7799-2 seguía vigente hasta el año 2007, en que se renombró como ISO 27001:2005 con el objetivo de mantener el año inicial de publicación del estándar. La ISO 27001 es la norma principal, certificable, donde se definen los requisitos que debe cumplir el sistema de gestión. La ISO 27002 complementa a la ISO 27001, describiendo pormenorizadamente los controles enunciados en el Anexo A de la ISO 27001.

La primera edición de la norma ISO 27000 fue publicada el 1 de Mayo de 2009. Esta norma

proporciona una visión general de la serie 27000, indicando para cada una de las normas que la componen su alcance y propósito. Incluye las definiciones de todas las normas de la serie y explica la importancia de implantar un SGSI. La serie consta de más de treinta estándares interrelacionados. La figura 2.12 muestra los estándares agrupados de acuerdo a sus objetivos y alcance:

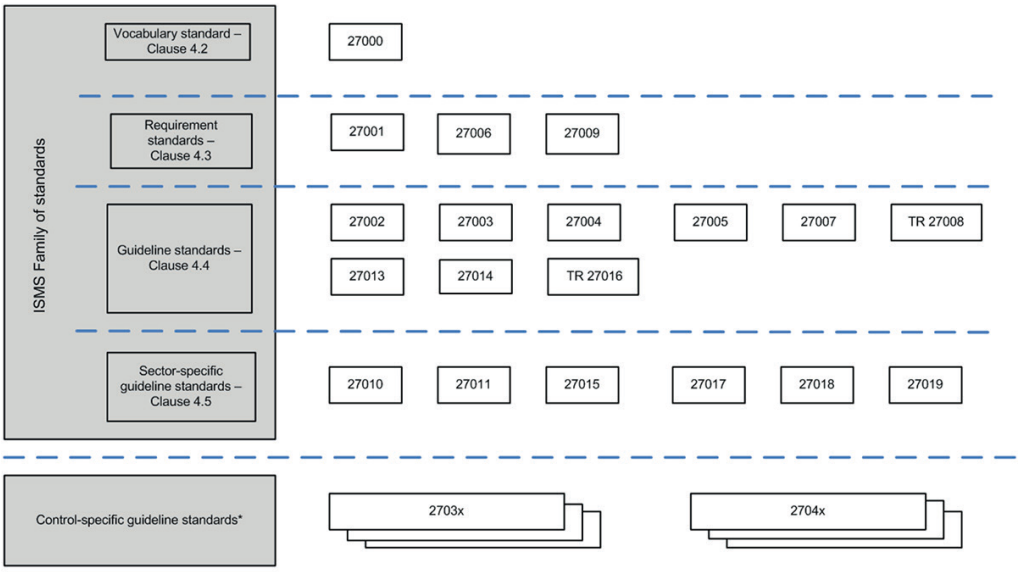

Figura 2.12: Estándares de la familia 27000 y su relación
Fuente: ISO 27000:2018

Pese a la importancia de esta familia de estándares, su número y extensión desaconsejan realizar una explicación pormenorizada. En cualquier caso, para tener una composición general se puede consultar el Anexo B, donde se presentan los principales estándares de la serie y una breve descripción de los mismos.

Diferencias y similitudes entre ENS e ISO 27001

El ENS establece en su artículo 2 la necesidad de tratar la seguridad de la información como un proceso integral, es decir, como un sistema de gestión. Este concepto aparece en el Anexo II, cuando indica la necesidad de contar con un sistema de gestión en las categorías alta y media para proteger la operación del sistema de información.

En el artículo 11 se recogen los requisitos mínimos de seguridad que deberán plasmarse formalmente en una política de seguridad aprobada por la dirección. Entre ellos cabe destacar el análisis de riesgos, para el que, de acuerdo con el artículo 13, "se empleará

alguna metodología reconocida internacionalmente", y la mejora continua, aplicando para ello, según el artículo 14, "los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información". El artículo 34 señala la necesidad de establecer una auditoría "regular ordinaria al menos cada dos años que verifique el cumplimiento de los requerimientos" señalados en el propio ENS.

De acuerdo con estos requisitos, el ENS puede considerarse, al igual que la ISO 27001, un sistema de gestión de la seguridad de la información plasmado en una política de seguridad, gestionado en un ciclo de mejora continua, basado en el análisis de riesgos, y con la obligatoriedad de llevar a cabo auditorías periódicas y certificables. También muchas de sus medidas son complementarias.

Sin embargo, entre ambos modelos existen algunas diferencias significativas. La primera es la naturaleza y alcance: el ENS es una norma jurídica española de carácter obligatorio para las Administraciones Publicas, mientras que ISO 27001 es un estándar internacional de carácter voluntario para empresas y organizaciones. Respecto a las medidas y controles de seguridad, el ENS tiene un mayor nivel de concreción. A modo de ejemplo, el ENS incluye controles que garantizan la continuidad del servicio, aspecto que la ISO 27001 no contempla, dado que la continuidad de servicio se trata de manera específica en la ISO 22301. La protección de los servicios tampoco aparece en la ISO 27001, algo similar a lo que ocurre con el apartado referido al entorno de explotación, sobre el que el ENS articula varios controles que no se contemplan en la ISO 27001.

De acuerdo con estas diferencias, sus certificaciones no son homologables. Estar certificado en ISO 27001 no implica cumplir todos los requisitos del ENS. Ni el caso contrario, aunque no cabe duda que poseer una de las dos certificaciones facilita el poder obtener la segunda.

2.2.3. La serie NIST SP 800

Como ya se ha explicado, ISO/IEC 27001 puede considerarse el marco estándar internacional de gestión de la seguridad de la información, y el ENS el referente, obligado en muchos casos, para empresas y organizaciones españolas. Pero en ambos casos, de acuerdo con sus necesidades, una empresa u organización puede incorporar sus propios controles o agregar controles de otros marcos (López y Ruiz, 2012). A continuación se presentan, de

forma resumida, los más relevantes.

Una referencia para explorar nuevos controles o para apoyar la implantación de los controles de la ISO/IEC 27002 o del Anexo II del ENS es la serie SP 800 (NIST, 2021b). Se trata de un amplio conjunto de documentos publicados por el NIST que describe de manera detallada las políticas de seguridad informática, así como directrices y procedimientos basados en una metodología de gestión de riesgos. Esta metodología, que se detalla en la publicación 800-39 (NIST, 2011), consta de cuatro fases:

- **Identificar los riesgos**. Identificar los condicionantes que afectan a la forma en que se evalúa, responde y monitoriza el riesgo de la organización, así como sus limitaciones y dificultades, determinar el *apetito de riesgo de la organización*, es decir, el nivel de riesgo que considera asumible aceptar, y establecer las prioridades de la organización en la gestión de los riesgos.
- **Evaluar los riesgos**. Señalar las amenazas y vulnerabilidades de los sistemas y establecer el nivel de riesgo aceptable.
- **Responder a los riesgos**. Disponer de cursos de acción alternativos para dar respuesta a los riesgos identificados en la evaluación de riesgos, evaluarlos, decidir la alternativa más apropiada e implantarla.
- **Monitorizar**. Implantar un sistema de seguimiento de los riesgos, así como monitorizar los sistemas para verificar el cumplimiento y la efectividad de las medidas de respuesta al riesgo implantadas.

Algunos de estos documentos son estándares en la industria de la seguridad de la información, pero se sale del alcance de esta tesis realizar un análisis detallado los mismos. Sin embargo, para los objetivos de este trabajo es necesario mencionar algunos de ellos.

NIST SP 800-50

La Publicación Especial 800-50, *Creación de un programa de capacitación y concienciación sobre seguridad de la tecnología de la información* (NIST, 2003), se trata de una guía para la creación de un programa de seguridad de la información. Este documento, tal y como muestra la imagen 2.13, establece el ciclo de vida de un programa de formación y

concienciación basado en cuatro fases:

- Diseño del programa de formación y concienciación.
- Preparación y desarrollo del material necesario.
- Implementación del programa.
- Mantenimiento.

Figura 2.13: Creación de un plan de formación y concienciación
Fuente: NIST SP 800-50

En este documento se señala la necesidad de realizar una evaluación para determinar las necesidades de formación y concienciación de una organización. Conviene anotar que para ello se pueden utilizar una amplia variedad de fuentes de información, como entrevistas al personal, análisis de métricas, revisión de la documentación de seguridad, o la revisión de políticas de acceso a los activos de información. Pero en cualquier caso son recomendaciones, dejando en manos de la propia empresa u organización la manera de llevar a cabo dicho análisis (NIST, 2003, pp. 27-28).

NIST SP 800-16

La publicación 800-50 complementa a la Publicación Especial 800-16, *Requisitos de capacitación en seguridad de tecnología de la información: un modelo basado en roles y desempeño* (NIST, 1998). La publicación 800-50 opera en un nivel estratégico superior, proporcionando orientaciones sobre cómo construir un programa de formación y concienciación sobre seguridad a nivel estratégico, mientras que la publicación 800-16 trabaja a un nivel más táctico. Este último documento resulta especialmente relevante, ya que por vez primera introduce, de manera específica, el concepto de formación y concienciación basada en roles laborales.

NIST SP 800-53

La Publicación Especial 800-53, titulada *Controles de seguridad y privacidad para organizaciones y sistemas de información*, proporciona un catálogo de controles de seguridad y privacidad para los sistemas de información que tienen como objetivo proteger las operaciones y los activos de la organización (NIST, 2020).

Dado su elevado número, los controles se organizan en familias, que agrupan los controles relacionados con un tema específico. Cada familia se identifica con un código unívoco de dos caracteres. Un control puede tener varias *mejoras del control* que aumentan la funcionalidad del control básico. Estas mejoras pueden ser utilizadas por las empresas y organizaciones cuando necesitan, de acuerdo con sus análisis de riesgos, un mayor nivel de protección. Tal y como puede apreciarse en la tabla 2.1 de la página 57, entre controles y mejoras, esta publicación, en su versión 5, alcanza más de 1000 posibles controles.

Id	Familia	Controles	Mejoras
AC	Control de acceso	25	122
AT	Formación y concienciación	6	11
AU	Auditoría y reporting	16	53
CA	Evaluación, autorización y seguimiento	9	32
CM	Gestión de la configuración	14	52
CP	Planificación de contingencias	13	43
IA	Identificación y autenticación	12	58
IR	Respuesta a incidentes	10	32
MA	Mantenimiento	7	23
MP	Protección de los medios	8	22
PE	Protección física y ambiental	23	36
PL	Planificación	11	6
PM	Gestión de programas	32	5
PS	Seguridad ligada al personal	9	9
PT	Transparencia y procesamiento de información personal	8	13
RA	Análisis de riesgos	10	16
SA	Adquisición de sistemas y servicios	23	122
SC	Protección de los sistemas y las comunicaciones	51	111
SI	Integridad de la información y de los sistemas	23	95
SR	Gestión de riesgos de la cadena de suministro	12	15

Tabla 2.1: SP 800-53
Fuente: Elaboración propia

2.2.4. NIST Cybersecurity Framework

Ante el preocupante incremento de ataques que estaban sufriendo los sistemas de información de las empresas y organizaciones norteamericanas, en el año 2013 el presidente Barack Obama encarga al NIST el desarrollo de un marco de ciberseguridad para la protección de las infraestructuras críticas. Este marco se conoce como *Cybersecurity Framework*, CSF.

En el desarrollo de este marco no se plantearon nuevos controles ni procesos, sino que se emplean los controles de los principales marcos y estándares de seguridad de la industria, como el ya mencionado NIST SP 800-53 o la ISO/IEC 27001, pero diferenciándose de estos por un enfoque orientado a la simplicidad y fácil comprensión para el negocio, y a la sencillez de adaptación a cualquier tipo y tamaño de empresa u organización. Estas características han convertido a este modelo en una importante referencia, siendo uno de los más utilizados, incluso por organismos como ISACA o la Organización Internacional de Normalización, ISO (OEA, 2019). Tal es su repercusión, que en el mundo anglosajón de la seguridad de la información este marco de seguridad es conocido como *The Framework*.

El Marco consta de tres partes: el Núcleo del Marco, los Niveles de Implementación y los Perfiles del Marco.

Núcleo del Marco

El Núcleo proporciona una estructura organizativa a través de la disposición y ordenamiento de directrices, prácticas y controles de reconocida utilidad y eficacia, que permiten la comunicación de las actividades y los resultados de seguridad a toda la organización. Asimismo, debido a que utiliza estándares de seguridad reconocidos, el Núcleo puede servir como modelo para relacionar, compartir y compaginar dichos estándares, ayudando de este modo a una mayor homogeneizacion y transversalidad de las normas existentes.

En el gráfico 2.14 se muestran las cinco funciones del Núcleo del Marco: Identificar, Proteger, Detectar, Responder y Recuperar. En su conjunto, representan la visión estratégica del ciclo de vida del SGSI de una organización.

Estas funciones se subdividen en veintitrés categorías, mostradas en la tabla 2.2 de la página 60, que abarcan los objetivos generales de seguridad de cualquier organización,

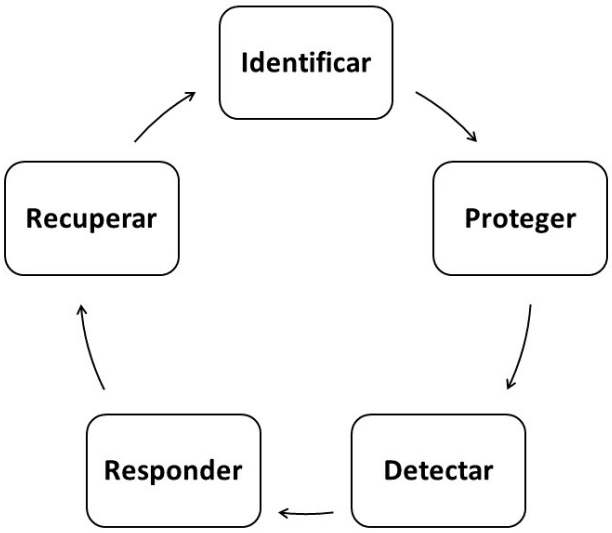

Figura 2.14: Funciones del CSF
Fuente: Elaboración propia

incluyendo la tecnología, las personas y los procesos.

Estas categorías se dividen a su vez en 108 subcategorías, en las que se alcanza un mayor nivel de detalle y concreción. En el siguiente nivel de desglose se mapea cada subcategoría con otros marcos de seguridad relevantes, lo que permite a las empresas y organizaciones adaptar y configurar sus controles y políticas de acuerdo con sus recursos y necesidades. A modo de ejemplo, en la tabla 2.3 de la página 61, se muestra la relación existente entre algunas de las subcategorías de la categoría "Entorno Empresarial" y los controles de ISO 27002, COBIT 5, NIST SP 800-53 y otros (NIST, 2021a).

Niveles de Implementación

Los niveles de implementación organizan y gradúan el nivel de madurez de las actividades de seguridad de una empresa u organización, desde un nivel inicial y parcial hasta un nivel proactivo e interactivo. Estos niveles reflejan una progresión desde respuestas informales y reactivas a enfoques medibles, adaptativos y sujetos a mejora continua, describiendo un grado cada vez mayor de rigor en las gestión de la seguridad. El objetivo de los niveles, presentados en la figura 2.15 es conocer el grado en el que el SGSI de una empresa u organización cumple las características definidas en el Marco.

Función	Categoría
Identificar	Gestión de activos
	Entorno empresarial
	Gobernanza
	Evaluación de riesgos
	Estrategia de gestión de riesgos
	Gestión del riesgo de la cadena de suministro
Proteger	Gestión de identidad y control de acceso
	Conciencia y capacitación
	Seguridad de datos
	Procesos y procedimientos de protección de la información
	Mantenimiento
	Tecnología protectora
Detectar	Anomalías y eventos
	Vigilancia continua de seguridad
	Procesos de detección
Responder	Planificación de respuesta
	Comunicaciones
	Análisis
	Mitigación
	Mejoras
Recuperar	Planificación de recuperación
	Mejoras
	Comunicaciones

Tabla 2.2: Funciones y categorías del CSF

Perfiles del Marco

Para establecer un marco de seguridad o mejorar uno ya existente, toda organización debe en primer lugar, establecer, de acuerdo con su estrategia corporativa, los objetivos, las prioridades y el alcance de su SGSI. A continuación debe identificar los sistemas y activos de información relacionados con el alcance definido, determinar los requisitos normativos, establecer el apetito de riesgo de la organización y realizar un análisis de riesgos (NIST, 2018).

El perfil de una organización se obtiene identificando qué categorías y subcategorías del Marco se están cumpliendo considerando las anteriores actividades. Esta identificación del perfil se asemeja a un análisis de brecha, en el que se compara el perfil real con un

Subcategoría	Controles
ID.BE-1. Se identifica y se comunica la función de la organización en la cadena de suministro.	**COBIT 5:** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53:** CP-2, SA-12
ID.BE-2. Se identifica y se comunica el lugar de la organización en la infraestructura crítica y su sector industrial.	**COBIT 5:** APO02.06, APO03.01 **ISO/IEC 27001:** Cláusula 4.1 **NIST SP 800-53:** PM-8
ID.BE-3. Se establecen y se comunican las prioridades para la misión, los objetivos y las actividades de la organización.	**COBIT 5:** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:** 4.2.2.1, 4.2.3.6 **NIST SP 800-53:** PM-11, SA-14
ID.BE-4. Se establecen las dependencias y funciones fundamentales para la entrega de servicios críticos.	**COBIT 5:** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53:** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5. Los requisitos de resiliencia para respaldar la entrega de servicios críticos se establecen para todos los estados operativos (p. ej. bajo coacción o ataque, durante la recuperación y operaciones normales).	**COBIT 5:** BAI03.02, DSS04.02 **ISO/IEC 27001:** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53:** CP-2, CP-11, SA-13, SA-14

Tabla 2.3: Subcategorías y controles en el CSF

perfil objetivo, lo que permite establecer, planificar y presupuestar planes de mejora que permitan alcanzar el perfil objetivo.

2.2.5. Cybersecurity Maturity Model Certification

Tal vez uno de los marcos conceptuales más significativos sea el *Cybersecurity Maturity Model Certification*, CMMC, un modelo de madurez en el contexto de la ciberseguridad desarrollado por el Departamento de Defensa de Estados Unidos con el objetivo de auditar el cumplimiento de requisitos de seguridad por parte de las empresas e instituciones que trabajan con contratos de defensa o que manejan *Información Controlada no Clasificada*, CUI, del gobierno estadounidense (DOD, 2020).

Se trata de un modelo muy reciente, publicado en el año 2020, basado en regulaciones, marcos y estándares de seguridad ya existentes. La relación existente entre los niveles de madurez del CMMC y las distintas regulaciones se resume en la figura 2.16.

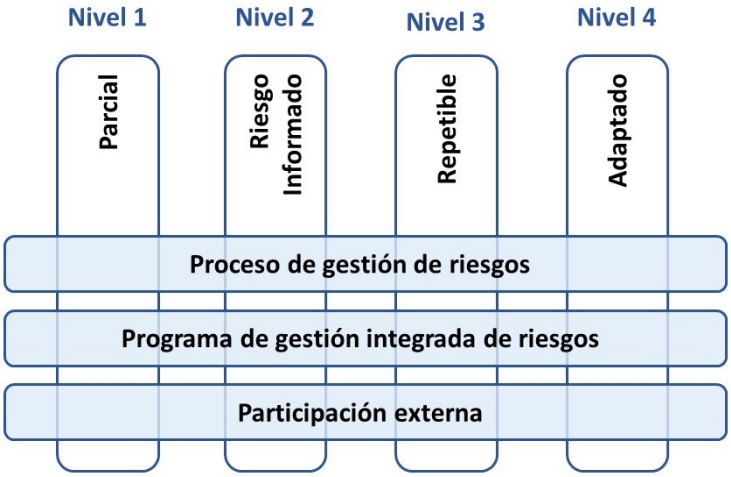

Figura 2.15: Niveles de implementación del CSF
Fuente: Adaptado de NIST (2021)

Es un modelo auditable por terceras partes, compuesto por cinco niveles de madurez, cinco niveles de certificación, diecisiete dominios, cuarenta y tres capacidades y 171 controles, denominados prácticas. El primer nivel o nivel básico de este modelo consta de diecisiete controles básicos de seguridad provenientes de la normativa *Federal Acquisition Regulation*, FAR 52.204-21. El segundo nivel, documentado, presenta setenta y dos controles, que incluyen los controles del primer nivel. Estos controles representan el 75 % de los controles de la norma NIST SP 800-171, denominada *Compliance Program*, NCP. El tercer nivel, gestionado, está compuesto por 130 controles. Este nivel cubre la totalidad de los controles del NCP. Esta normativa está orientada a pequeñas y medianas empresas y organizaciones que no necesitan la complejidad de la norma NIST 800-53. En grandes organizaciones se alcanza el cuarto nivel, proactivo, formado por 156 controles, mediante el cumplimiento del la norma NIST 800-53. El quinto nivel, optimizado, formado por 171 controles, también se basa en la norma NIST 800-53, junto con controles provenientes de otros marcos de cumplimiento, como ISO 27002 o el *CERT Resilience Management Model*, CERT-RMM.

Las asociaciones y dependencias entre las regulaciones y estándares examinados se pueden apreciar en la figura 2.17.

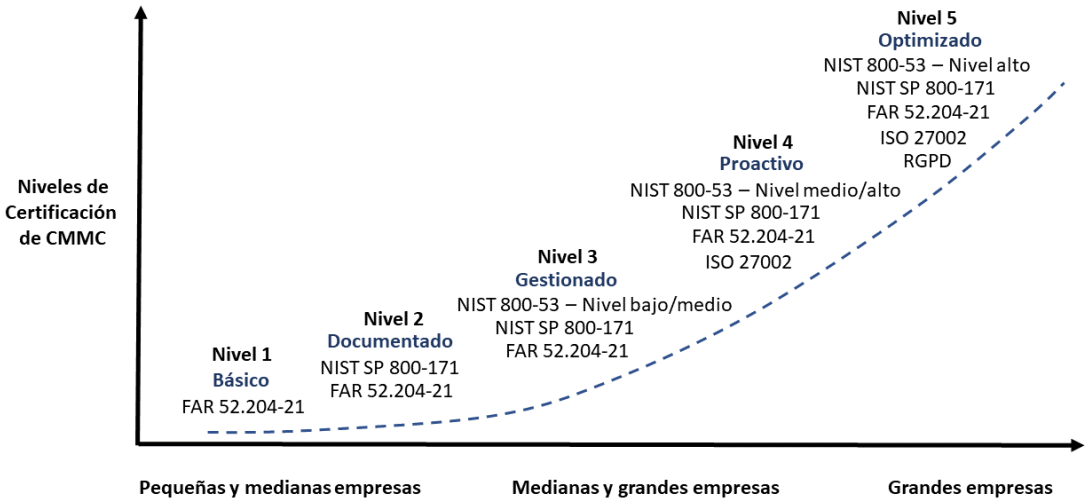

Figura 2.16: Requisitos de las certificaciones CMMC
Fuente: Elaboración propia

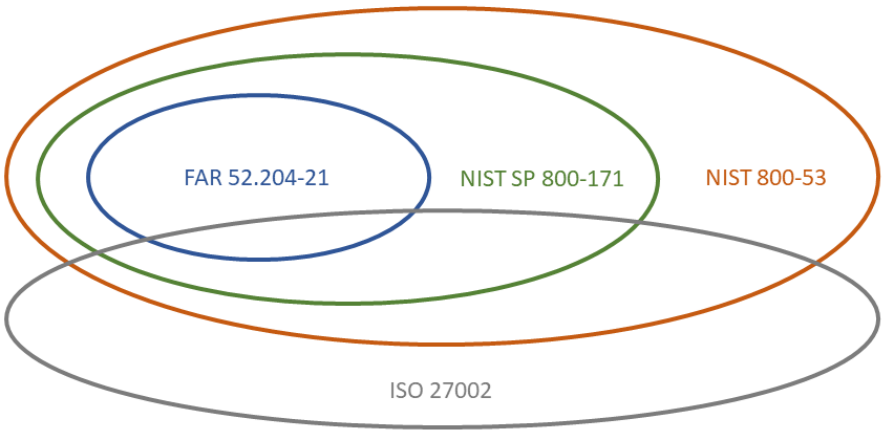

Figura 2.17: Relación con regulaciones y estándares
Fuente: Elaboración propia

2.2.6. Otros marcos de referencia

Las referencias anteriores no agotan los marcos y estándares existentes. Muchos de ellos, como COBIT, orientado a la gestión y gobierno de TI (ISACA, 2021), cuentan con apartados específicos dedicados a la seguridad de la información.

Dentro de esta amplia variedad, resulta conveniente mencionar brevemente las metodologías para la realización de auditorías técnicas de seguridad. La más conocida recibe el nombre de *Pentest*, abreviatura de *Penetration Testing* o Test de Intrusión, que es, muy resumidamente, una metodología para evaluar la seguridad de un sistema informático mediante la simulación de un ataque (CCN-CERT, 2010). Algunas de estas metodologías permiten poner a prueba no solo la seguridad técnica, sino también la confidencialidad, integridad y disponibilidad de los sistemas. Seguidamente se repasan algunos de estos marcos y metodologías.

The Open Source Security Testing Methodology Manual

El *Open Source Security Testing Methodology Manual*, más conocido por sus siglas OSSTMM, es una reconocida metodología para la realización de auditorías de seguridad basadas en la realización de test de intrusión (Herzog, 2010).

Esta actividad de auditoría se lleva a cabo a nivel operativo en toda la organización. Centrada en aspectos técnicos, se focaliza en identificar las posibles brechas entre lo que la organización espera de las operaciones y procesos de TI y lo que realmente está sucediendo. Esta actividad se lleva a cabo mediante la realización de tests y comprobaciones organizadas de acuerdo con la estructura representada en la tabla 2.4 de la página 65.

Information Systems Security Assessment Framework

Esta metodología, más conocida por sus siglas ISSAF, desarrollada por el Open Information Systems Security Group, OISSG, implementa controles de otros estándares, como IEC/ISO 27001 o COBIT. Se trata de un marco muy empleado, fundamentado en un exhaustivo y detallado análisis de las actividades de una organización relacionadas con la seguridad de la información.

Clase	Canal	Descripción
Seguridad física	Humano	Comprende el elemento humano de la comunicación donde la interacción es física o psicológica.
	Físico	Comprende elementos físicos (no electrónicos) de seguridad donde la interacción requiere un esfuerzo físico o una fuente de energía.
Seguridad del espectro electromagnético	Comunicaciones inalámbricas	Comprende todas las comunicaciones, señales y emisiones electrónicas que tienen lugar en el espectro electromagnético.
Seguridad de las comunicaciones	Telecomunicaciones	Comprende todas las redes de telecomunicaciones, digitales o analógicas, en las que la interacción tiene lugar a través de líneas telefónicas o similares.
	Redes de datos	Comprende todos los sistemas electrónicos y redes de datos donde la interacción tiene lugar a través de red cableada

Tabla 2.4: OSSTMM 3. Clases y canales

El modelo se divide en cuatro fases que organizan la gestión de las actividades. Estas fases son: Planificación, Evaluación, Tratamiento y Acreditación. Cada una de estas fases consta de tareas específicas, comunes a todas las organizaciones, independientemente de su actividad, tamaño o ubicación geográfica. A través de la secuenciación de sus actividades, estas fases persiguen entregar resultados específicos y mantener el estado alcanzado (OISSG, 2006, pp. 26-27).

Open Web Application Security Project

El Open Web Application Security Project, OWASP, es una fundación sin ánimo de lucro dedicada a la promoción de software seguro, con una especial atención a la seguridad en aplicaciones web (OWASP, 2021a). Para ello proporciona una amplia y detallada documentación, guías de desarrollo, guías de testeo y software. Uno de sus proyectos más conocidos es el *OWASP Testing Project*, que tiene como objetivo crear un marco de trabajo dirigido a responsables de seguridad para el desarrollo de pruebas de seguridad en aplicaciones web. Tiene la particularidad de no limitarse a la realización de pruebas de intrusión, sino que abarca todo el ciclo de vida de desarrollo de software (OWASP, 2021b).

En el gráfico 2.18 se muestra la secuencia de pruebas de seguridad que esta metodología

propone.

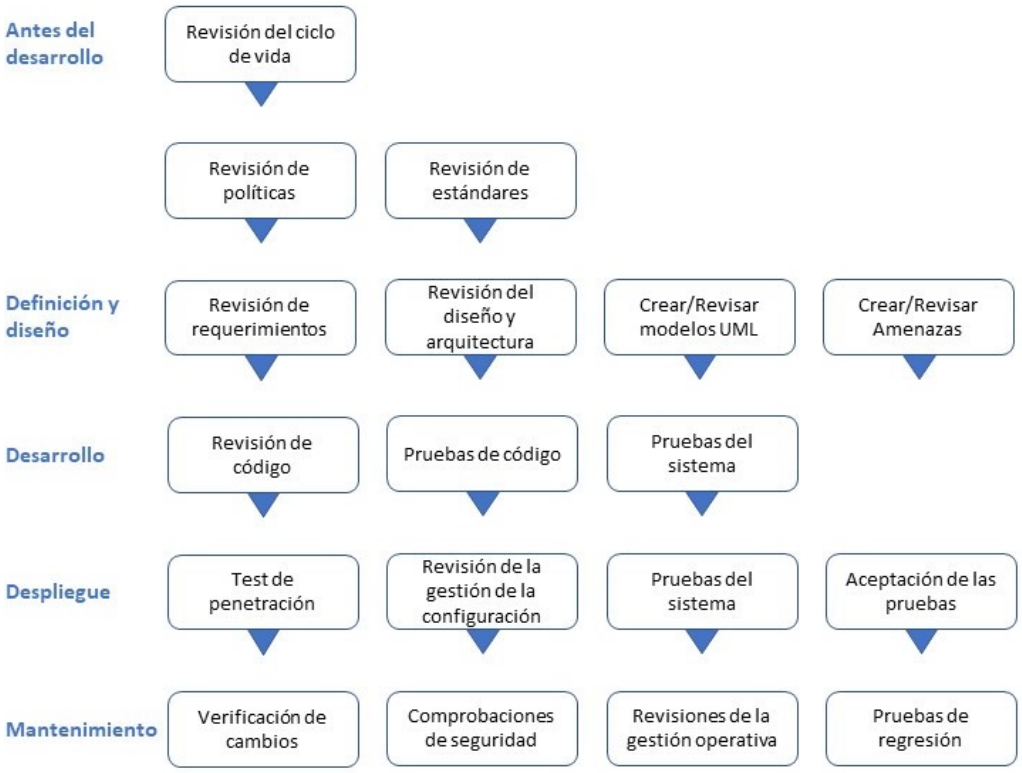

Figura 2.18: Flujo de pruebas
Fuente: OWAPS. (Licencia GFDL)

2.3. Cultura de la seguridad

Para cerrar este repaso y presentación de los elementos conceptuales básicos empleados en esta tesis, es necesario referirse a la cultura organizacional, en la que debe enmarcarse la cultura de la seguridad de la información. Como se explica a continuación, la gestión por competencias laborales en el ámbito de la seguridad no puede ser un elemento aislado en las empresas y organizaciones, sino que debe formar parte indisoluble y connatural de la cultura de la empresa. Ése es el objetivo, y no otro, que debe orientar todas las actividades y esfuerzos en el ámbito de la formación y concienciación en seguridad.

2.3.1. Concienciación y formación

En páginas anteriores se ha presentado la seguridad de la información como un sistema de gestión que involucra a personas, procesos y tecnología. Estos tres elementos, considerados

pilares de la seguridad de la información (Calder, 2016), mantienen una estrecha relación e influencia entre sí. Como ya se ha explicado, la tecnología no puede proteger a las organizaciones si no se utiliza correctamente, si las personas no conocen los procesos o no desean utilizarlos. También se ha argumentado en la página 9 de esta tesis que la seguridad de la información no es únicamente un problema tecnológico: sin la colaboración e implicación de las personas de la organización, sin tener resuelto el factor humano, no es posible mantener un adecuado nivel de seguridad.

Para alcanzar este deseado nivel de colaboración e implicación, es necesario llevar a cabo un continuado y coordinado esfuerzo en formación y concienciación. Estas dos actividades, por su complementariedad y estrecha relación, pueden llegar a confundirse. Es conveniente, por tanto, en primer lugar, aclarar sus características y diferencias.

La RAE define "formar" como "preparar intelectual, moral o profesionalmente a una persona o a un grupo de personas" (RAE, 2019). La definición del NIST ayuda a aproximar la definición de la RAE al ámbito de la seguridad de la información: "crear los necesarios conocimientos, habilidades y competencias de seguridad para el personal" (Paulsen y Byers, 2019). En esta definición conviene señalar, por su relevancia para esta tesis, la mención explicita que se realiza al concepto de competencia.

Respecto al término concienciación, se entenderá como "un proceso de aprendizaje que prepara el escenario para la capacitación, al cambiar las actitudes individuales y organizacionales para darse cuenta de la importancia de la seguridad y las consecuencias adversas de su fracaso" (Paulsen y Byers, 2019). Esta definición señala un importante elemento: el orden en que deben coordinarse ambas actividades, y derivado de ello, la relevancia y necesidad de la concienciación. Las tareas de concienciación preceden a las actividades de formación. En caso de no hacerse así, o limitarse a formar sin concienciar, se obtendrá como resultado personas con escasa motivación para recibir formación, y que una vez recibida no la aplicarán, por considerarla innecesaria, irrelevante y consumidora de tiempo. Un segundo aspecto relevante en esta definición es la referencia al cambio en las actitudes individuales y organizacionales, que permite confirmar que las tareas de concienciación deben estar encaminadas a promover la cultura de la seguridad como parte indispensable de la cultura organizacional.

La definición de concienciación del CCN-CERT también remarca el factor humano: "actividad continuada y recurrente en la que todas las personas relacionadas con el sistema de información se familiarizan con los aspectos de seguridad del mismo a fin de que no provoquen fallos gratuitos por ignorancia, descuido o negligencia" (CCN-CERT, 2010).

El NIST describe con claridad la diferencia entre formación y concienciación: "Concienciación no es formación. El propósito de la concienciación es enfocar la atención en la seguridad, y tienen como objetivo permitir a las personas reconocer la problemática de la seguridad de la información y responder en consecuencia" (Wilson y Hash, 2003).

Estas definiciones permiten apreciar la complementariedad y necesidad de ambas tareas, al mismo tiempo que establecen sus diferencias, presentadas de manera resumida en la tabla 2.5 de la página 68.

	Concienciación	Formación
Objetivos	Llamar la atención sobre los problemas de seguridad	Desarrollar conocimientos y habilidades específicas para dar respuesta a necesidades concretas.
Usuario	Amplio. Receptor. Pasivo	Específicos. Participativo. Activo
Contenidos	Mensajes. Escasos. Atractivos. Repetidos	Información y datos. Específicos. Amplios

Tabla 2.5: Concienciación vs. formación
Fuente: Elaboración propia

2.3.2. Cultura organizacional

Las anteriores definiciones ya adelantaban la necesidad de prestar atención a la cultura organizacional para abordar con garantías de éxito actividades de formación y concienciación en el ámbito de la seguridad de la información. Desarrollar y promover una cultura de seguridad son tareas primordiales que ayudan a abordar los problemas de comportamiento que subyacen en muchos incidentes de seguridad (Bada y Nurse, 2019).

La Real Academia Española define cultura como el "conjunto de modos de vida y costumbres, conocimientos y grado de desarrollo artístico, científico, industrial, en una época, grupo social, etc." (RAE, 2021) Se trata en consecuencia de un concepto amplio, que no solo abarca distintos ámbitos y colectivos, sino que puede presentar diferentes enfoques y respuestas a realidades semejantes.

Las organizaciones, como entorno social, también poseen sus propios modos de vida, costumbres y conocimientos, que reciben el nombre de cultura corporativa u organizacional. Es un concepto ampliamente aceptado (Watkins, 2013; Flamholtz, 2011), que presenta diferentes enfoques y perspectivas. Una definición comúnmente aceptada es la de Michael Armstrong (2006), que define cultura organizacional como "el conjunto de valores, normas, creencias, actitudes y suposiciones que conforman las maneras de hacer y pensar de las personas en una organización" (Armstrong, 2014, p. 120).

Se trata en consecuencia de reconocer y considerar los aspectos subjetivos e informales que existen en toda organización, y que sin duda inciden en el comportamiento de las personas y de los grupos que la conforman. Se trata de un enfoque iniciado por Elton Mayo en 1925, a raíz de sus conocidos experimentos en la Western Electric Company (Álvarez y María, 2006). A raíz de estos experimentos, quedó demostrado que los valores del grupo al que pertenecen las personas de una organización inciden de manera significativa en la percepción que éstas tienen sobre la realidad.

Como ya se adelantó en el capítulo I, la cultura organizacional universitaria presenta claros elementos diferenciadores respecto a otras organizaciones. Ian Mcnay (1995) contempla hasta cuatro culturas coexistiendo, en mayor o menor grado, dentro de una universidad: el claustro, la burocracia, la dirección y la empresa. Todas ellas con sus propias características y necesidades, no siempre coincidentes.

En este escenario, la cultura organizacional se presenta como uno de los factores principales que promueve y facilita el cumplimiento de las políticas y procedimientos de seguridad de la información (Onumo et al., 2021). Por ello, la formación y concienciación en seguridad de la información solo puede ser efectiva si se aborda desde la perspectiva de la cultura organizacional, convirtiendo el conjunto de conocimientos, actividades y acciones que conforman la seguridad de la información en hábitos y costumbres que formen parte de los valores culturales de los diferentes colectivos universitarios.

La seguridad de la información no puede ser, por tanto, una burbuja tecnológica separada del resto de metas de la organización (van't Wout, 2019). Parafraseando a Julie Nosworthy (2000) que hace dos décadas ya afirmaba que la seguridad de la información forma parte

del negocio y no solo de los departamentos de TI, se puede afirmar que la seguridad de la información debe formar parte de la cultura organizacional de las universidades, y no solo de su departamento de TI.

Para alcanzar este objetivo, los esfuerzos en concienciación y formación en seguridad, basados o no en competencias, tienen que ir encaminados a construir una cultura de la seguridad que se integre en la propia cultura organizacional, a través tanto de la construcción de nuevos procesos formales e informales que con el tiempo se interioricen y formen parte de la cultura organizacional, como de la reorientación y modificación de los procesos ya existentes.

2.4. Gestión por competencias

En las páginas precedentes se han identificado y repasado los principales conceptos de seguridad de la información, así como los estándares y marcos de seguridad más relevantes. Con ello se ha presentado un panorama global y coherente, aunque resumido, del significado de la seguridad de la información, de qué modo se organizan los distintos elementos y actores que la conforman, y en qué forma puede ser empleada.

Sin embargo, el alcance de esta tesis no se circunscribe únicamente a la seguridad de la información, sino que ésta debe ser utilizada desde un enfoque competencial, compartiendo de este modo el punto de vista de diversos autores que coinciden en señalar que la formación basada en competencias favorece los procesos de aprendizaje, facilita la implantación de programas de capacitación y permite una adaptación mas rápida a los cambios tecnológicos y productivos (Arancibia y Díaz, 2002). Por tanto es necesario repasar los conceptos más relevantes de la gestión basada en competencias, para de esta manera entender mejor los propósitos de este trabajo.

2.4.1. Gestión basada en competencias

Para toda organización, contar con personas que posean no solo los conocimientos sino también las actitudes y motivaciones adecuadas para el cumplimiento de los objetivos corporativos se ha convertido en un elemento competitivo de primer orden, y en un im-

portante objetivo en el área de la gestión de los recursos humanos (da Silva et al., 2014). Para alcanzar este objetivo, las organizaciones establecen procedimientos que, agrupados bajo el nombre de gestión por competencias, se han convertido en una herramienta de gran validez para desplegar los procesos de la gestión de personas.

Algunas de las premisas que estructuran y organizan todo modelo de gestión por competencias son las siguientes:

- Cada organización y tipo de puesto de trabajo presentan unas características propias que requieren personas con perfiles competenciales específicos a esos puestos.
- Las tareas desempeñadas en los puestos de trabajo están sujetas a permanente evolución y cambio, lo que implica el desarrollo de nuevas competencias o la modificación de las existentes.
- La organización tiene el deber de identificar las competencias necesarias para el adecuado desempeño de sus puestos de trabajo, así como ofrecer a las personas de la organización la posibilidad de adquirir y desarrollar las competencias necesarias para el buen desempeño de sus funciones.

De acuerdo con lo anterior, todo modelo de gestión por competencias se traduce en un proceso continuo y sistemático que permite:

- Identificar las actitudes, habilidades y conocimientos necesarios que se requieren en cada puesto para traducirlos en descriptores objetivos que puedan ser explicados y cuantificados.
- Conocer para cada puesto de trabajo la brecha existente entre el desempeño actual y el requerido.
- Establecer los mecanismos de formación necesarios para corregir las brechas detectadas.

Competencias

El concepto de competencia ha sufrido a lo largo del tiempo una notable evolución y desarrollo en su significado. En la actualidad engloba diferentes enfoques y conceptos, ge-

nerando en ocasiones cierta confusión a la hora de definir qué se entiende por competencia (Mohammad Salman, 2020; Levy-Leboyer, 1997). Esta situación se complica cuando se habla de competencia laboral, término sobre el que también existe confusión en su significado y uso (Alles, 2015; Irigoin y Vargas, 2002).

El término de competencia como aspecto motivacional, más allá de la mera capacidad de interactuar de manera efectiva con el entorno, fue tratado por primera vez por Robert White (White, 1959), que lo identificó como el rasgo o componente humano responsable del buen desempeño.

A partir de ese momento, y a medida que se desarrollan diferentes aproximaciones a una realidad tan compleja y ambigua como son las competencias, se diversifican las definiciones y enfoques que intentan categorizarla. Esta situación se complica con la utilización de manera indistinta de los términos aptitud (*ability, aptitude*) y habilidad (*skill*), que aunque próximos al de competencia, representan realidades diferentes (Agut, 2001; Carlton, 2016).

Una buena aproximación a esta diversidad puede ser el artículo "From task-based to competency-based" (Soderquist et al., 2010), en el que después de llevar a cabo una amplia revisión de la literatura sobre los distintos enfoques en gestión de competencias, se presenta una tipología de competencias que integra los enfoques previos.

Competencias laborales

El concepto de competencia laboral también ha seguido un proceso de redefinición constante, como adaptación natural a la evolución del desempeño laboral en las organizaciones. El concepto de competencia laboral no fue utilizado hasta 1973 por David McClelland en su conocido artículo "Testing for competence rather than for intelligence", en el que plantea la insuficiencia de los tradicionales test basados en la inteligencia para predecir el éxito en el desempeño laboral (McClelland, 1973).

Normalizar las actividades en el área de la seguridad de la información como competencias laborales presenta varias ventajas, tanto para el trabajador como para la organización, entre las que podemos destacar:

- Para la organización

- Le permite disponer de un marco de referencia o patrón de medición de competencias contra el que contrastar el nivel de formación y concienciación del personal, tanto a nivel individual como agregado.
- El marco de referencia utiliza un conjunto de competencias normalizadas, compartidas y conocidas.
- Posibilita planificar actividades individualizadas de capacitación de las personas en el ámbito de la seguridad de la información.
- Permite disponer de un perfil de contratación o promoción en el alcance definido.
- Acrecienta la seguridad de la organización.
- Mejora el desempeño de la organización.
- En aquellos casos en los que el marco o modelo de referencia sea compartido por un sector o industria, se puede hablar de un marco estandarizado, lo que supone nuevas ventajas:
  - Permite integrar y compartir esfuerzos de formación y concienciación con otras empresas u organizaciones del sector.
  - El lenguaje sobre los contenidos y niveles de competencia es común.
  - Los niveles de competencia de las personas son homogéneos y comparables.

- Para las personas:
  - Les permite conocer su nivel competencial respecto a los requerimientos y necesidades de su organización en el ámbito de la seguridad de la información.
  - Tienen la posibilidad de que sus competencias sean objetivables y reconocidas.

2.4.2. Modelos de competencias laborales

La utilización de modelos en el ámbito de las competencias ha demostrado a lo largo del tiempo su importancia y utilidad: permite construir mapas con los conocimientos, habilidades y capacidades necesarios en empresas y organizaciones, y proporciona indicadores

cuantitativos y cualitativos para el desempeño de un puesto de trabajo, de un grupo de trabajadores o de un área o actividad. Con ello, se objetivan actividades como la selección, la evaluación, la remuneración o la capacitación del personal.

Andrew Gronzci y James Athanasou (1996) señalan que las competencias laborales pueden tipificarse en tres grupos: como lista de tareas, como conjunto de atributos personales y como relación holística.

Modelo de competencias como lista de tareas

Basado en el modelo Taylorista, este enfoque se basa en la definición funcional del puesto de trabajo. Explica las competencias laborales como una relación de tareas y conocimientos asociados a un puesto de trabajo. Esta relación ordena y define las tareas y conocimientos que debe desarrollar y conocer una persona en su actividad laboral. Se trata un enfoque muy reduccionista, pero sin embargo ampliamente utilizado por su facilidad de elaboración y seguimiento.

En este modelo, las competencias, entendidas como tareas y conocimientos observados en los puestos de trabajo, permiten establecer un perfil estándar de requisitos para cada competencia. Esto posibilita que se pueda evaluar al trabajador o trabajadora respecto al perfil estándar, y de acuerdo con los resultados obtenidos establecer el aprendizaje necesario en función de las necesidades de cada puesto. Este proceso se representa en la figura 2.19.

Modelo de competencias como conjunto de atributos personales

El enfoque anterior fue completado por los trabajos de David McClelland (1973), con la inclusión de los comportamientos y actitudes, que ayudaban a explicar de una manera más completa el desempeño laboral. La competencia laboral, desde esta perspectiva, se entiende no solo por lo que la persona sabe y puede hacer; también por lo que quiere hacer. Un ejemplo de este enfoque es la definición de Anne Marelli (1999), que define la competencia como "una capacidad laboral, medible, necesaria para realizar un trabajo eficazmente, es decir, para producir los resultados deseados por la organización. Está conformada por conocimientos, habilidades, destrezas y comportamientos que los trabajadores deben demostrar".

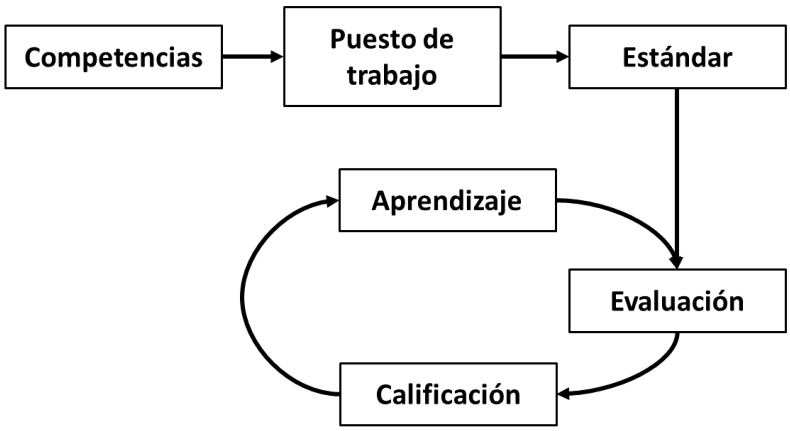

Figura 2.19: Competencias
Fuente: Adaptado de Thompson, J. E. y Harrison, J. (2000)

Esta definición presenta dos aspectos destacados. En primer lugar, la competencia laboral debe ser medible. Esta es una condición que debe satisfacer cualquier competencia laboral y constituye un aspecto común en todos los modelos. Tal y como ya figuraba en el modelo de lista de tareas, el poder medir una competencia significa que puede ser evaluada, y en consecuencia formar parte de programas de formación (Vargas et al., 2001). El segundo aspecto es la inclusión del comportamiento del trabajador. La competencia viene definida no solo por lo que la persona sabe hacer, también por lo que quiere hacer. En el ámbito de la seguridad de la información este es un aspecto muy relevante cuando consideramos el ya conocido factor humano.

Modelo de competencias como relación holística

Los dos modelos anteriores, complementarios, derivan en un planteamiento holístico, en el que, a los conocimientos y actitudes se añade el contexto en el que se desarrolla la actividad. Se trata de un enfoque relevante desde el punto de vista de la seguridad de la información, donde los peligros y amenazas son difusos y están en permanente cambio. En este modelo las competencias son entendidas como relaciones complejas de habilidades, conocimientos, actitudes y valores que varían de acuerdo con las necesidades específicas del entorno (Guerrero y de los Ríos, 2013).

2.4.3. Perfil de competencias

Los anteriores modelos comparten una serie de puntos comunes que podemos considerar como características que debe satisfacer toda competencia (Escobar, 2005).

- Cada competencia se identifica con un nombre y cuenta con una definición precisa.
- Cada competencia tiene un determinado número de niveles que reflejan conductas observables, no juicios de valor.
- Las competencias se pueden desarrollar.
- Los puestos de trabajo están asociados con un perfil de competencias, entendido como un inventario de las mismas, incluyendo el nivel requerido para cada una de ellas.
- Todo modelo de gestión por competencias llega hasta la definición de niveles y de indicadores de conductas esperadas.

En la actualidad existen varias metodologías para identificar perfiles de competencias, entre las que se pueden destacar las siguientes (Sistema Nacional de Certificación de Competencias Laborales, 2010):

- DACUM (Developing a Curriculum) es un método desarrollado en el Centro de Educación y Formación para el Empleo de la Ohio State University de Estados Unidos, en 1995. Es un método globalmente aceptado, dada su fiabilidad y eficacia en el análisis y descripción de puestos de trabajo estándar. Se trata de un procedimiento estructurado que tiene como objetivo identificar, de la manera más clara y precisa posible, lo que el trabajador debe conocer y poder hacer para desempeñar adecuadamente su desempeño.
- SCID (Systematic Curriculum and Instructional Development) es un modelo complementario a DACUM, orientado a la producción de materiales de instrucción relevantes y de calidad, a partir del análisis del puesto de trabajo desarrollado usando el método DACUM.
- AMOD (A Model) es una variante de la metodología DACUM, orientada a identificar las competencias de una familia de ocupaciones.

- El Análisis funcional es un método utilizado para identificar las competencias laborales, desagregando las funciones de una empresa u organización en subfunciones más específicas, que a su vez son divididas en actividades cada vez más concretas, hasta alcanzar la identificación de las acciones elementales que pueden ser asignadas a un trabajador.

2.4.4. Análisis funcional

A diferencia de DACUM, SCID y AMOD, que trabajan con el enfoque de las competencias como lista de tareas, el Análisis funcional analiza las relaciones existentes entre la función productiva de un determinado sector, organización o puesto, y las habilidades, conocimientos y actitudes necesarias para desempeñarlas con éxito (Martínez, 2011). Se trata de una visión diferente que entiende el trabajo en relación con los objetivos de la organización.

El Análisis funcional es "una técnica que se utiliza para la identificación de las competencias laborales requeridas por una función productiva. Considera el trabajo de cada uno en una relación sistémica con el logro del propósito de la organización o sector en el que se realiza" (Vargas et al., 2001).

Es importante señalar que esta metodología no describe procesos, sino resultados. No importa en consecuencia conocer cómo se obtiene un resultado, sino que este se logre. Se trata de un aspecto relevante, ya que dota al trabajador o trabajadora de la posibilidad de utilizar diferentes métodos o estrategias para conseguir las metas esperadas. Por este motivo, en el mapa funcional no se deben describir tareas, sino identificar resultados (Vargas et al., 2001).

En esta tesis se utiliza la metodología del Análisis Funcional para dar respuesta a los objetivos de investigación planteados. Dos son los motivos de esta decisión. En primer lugar, sus características se consideran más adecuadas a los propósitos de este trabajo, y en segundo lugar, se trata de una metodología que valora y subraya la certificación en competencias (Irigoin y Vargas, 2002). Este aspecto, aunque se sale del alcance de esta tesis, se considera un aspecto relevante para futuros trabajos de investigación.

2.4.5. Procesos competenciales

De acuerdo con lo presentado hasta el momento, se pueden establecer una serie de procesos básicos que conforman la gestión basada en competencias. Estos procesos son la identificación, la normalización, la evaluación y la certificación de competencias (Irigoin y Vargas, 2002).

El primer paso es la identificación de las competencias en el alcance definido. Este proceso se lleva a cabo a través de metodologías como las presentadas en las páginas precedentes, organizadas a través de equipos de trabajo formados por consultores, expertos y trabajadores. En este proceso se establece cuáles son la competencias y cómo deben evaluarse para confirmar que han sido alcanzadas.

Identificadas la competencias y los criterios de evaluación, el siguiente paso es determinar si las competencias sirven solo para la organización estudiada, o también podrían ser adecuadas para organizaciones similares o incluso para todas las organizaciones de un sector o país. Este proceso, denominado normalización de las competencias, como ya se ha explicado, transforma cada competencia en un referente consensuado estándar.

Una vez identificada y normalizada una competencia, debe ser objeto de formación en los conocimientos, aptitudes y actitudes necesarias para su adecuado desempeño. Este desempeño se puede obtener mediante la práctica y la experiencia, o bien mediante un proceso de aprendizaje, conocido como "Formación Basada en Competencias", de reconocida relevancia y validez, y de amplio uso en múltiples ámbitos, como por ejemplo el proyecto universitario europeo Tuning, ya mencionado en el capítulo I.

La formación basada en competencias debe ir acompañada de procesos de evaluación con el fin de verificar que las personas poseen las competencias. Así mismo, el resultado de un proceso de evaluación permite conocer las necesidades de formación específicas de las personas evaluadas y establecer con ello los correspondientes procesos de formación.

El último paso es el proceso de certificación, consistente en el reconocimiento formal de las competencias demostradas en el proceso de evaluación.

El proceso competencial descrito se presenta de manera resumida en la figura 2.20.

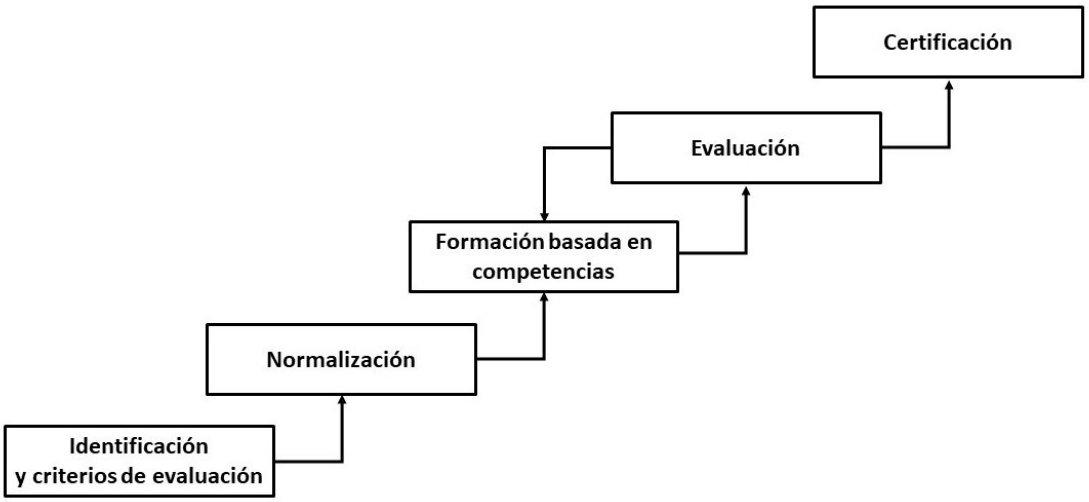

Figura 2.20: Procesos competenciales
Fuente: Adaptado de Vargas, 2004

Si este proceso de aprendizaje se lleva a cabo dentro de una empresa u organización, vinculado con procesos de selección y desarrollo de personal, se puede hablar de una "Gestión de recursos humanos basada en competencias".

Introducido el ámbito del problema, justificada la pertinencia de esta tesis, y repasadas las nociones más destacadas sobre seguridad de la información, estándares de seguridad, cultura de la seguridad y gestión por competencias, se está en disposición de abordar en el próximo capítulo la metodología empleada y el análisis detallado del problema, como pasos previos al desarrollo de la solución.

Capítulo 3

Metodología de investigación

"Me gustaría mirar, -dijo Rachel sentándose-.
Nunca he visto realizar un test Voigt-Kampff".

Blade Runner

3.1. Proceso metodológico

En este capítulo se presenta tanto el proceso metodológico desarrollado a lo largo de la elaboración de la tesis como los principales instrumentos y herramientas de análisis y recopilación de datos que se emplean en la misma.

De acuerdo con el modelo de discrepancia de Witkin y Altschuld (1995), todo análisis y detección de necesidades de formación presenta tres fases: "lo que debería ser", "lo que es" y "cómo alcanzarlo". Esta tesis se centra y tiene como objetivo definir y avanzar en el conocimiento de "lo que debería ser" en el ámbito de las competencias laborales en seguridad de la información. Conocer "lo que debería ser", es decir, identificar, acotar y medir cuáles son los objetivos que se desean alcanzar es, sin duda, el primer y fundamental paso de todo proceso de mejora.

Para definir "lo que debería ser", este trabajo, como ya se ha explicado, explora una nueva línea de investigación, proponiendo la construcción de un mapa de competencias en seguridad de la información para el personal no TIC de las universidades españolas, basado en un estándar de seguridad como es, de facto, el ENS. Se trata por tanto de un estudio exploratorio y descriptivo, de carácter no experimental y donde, dado el objetivo de la investigación, la conjunción de metodología cuantitativa y cualitativa se presenta

como la mejor alternativa. No será por tanto, y este es un aspecto a destacar, un proceso lineal ni estrictamente definido como ocurre en los procesos puramente cuantitativos, sino iterativo y recurrente (Hernández et al., 2014).

Conviene también señalar que aún utilizándose métodos cuantitativos, el enfoque primario será de tipo cualitativo, lo que presenta algunas características muy apropiadas para alcanzar los objetivos planteados en este estudio (Vasilachis, 2009; Mohajan, 2018):

- El investigador tiene la oportunidad de recopilar datos directamente de los participantes en la investigación.
- Se pueden utilizar diversos métodos para obtener datos, de acuerdo a las características y objetivos del estudio.
- La investigación se lleva a cabo en un ámbito real y vinculado al contexto, no en entornos controlados o de laboratorio.
- Permite flexibilidad en el diseño de la investigación, de acuerdo con los datos que se estén obteniendo.
- El investigador es una parte integral del propio proceso de investigación, teniendo la capacidad de utilizar su motivación e interés personal para impulsar el estudio.
- Se persigue establecer una perspectiva holística de la realidad investigada.
- No se plantean hipótesis, sino que, a partir de la investigación, se construyen conclusiones y artefactos sobre los fenómenos estudiados.

Y todo ello con la responsabilidad de obtener y reflejar información fidedigna y de garantizar el tratamiento ético de los participantes y de los datos obtenidos.

Para alcanzar los objetivos planteados en este trabajo, a continuación se presenta el proceso metodológico seguido durante la investigación y elaboración de la tesis, desarrollado de acuerdo con las siguientes fases:

- Fase I. Inicio del trabajo. Planteamiento del problema y análisis del estado de la cuestión sobre los aspectos relevantes de esta investigación.
    - La seguridad de la información en empresas y organizaciones.

    - Los estándares y marcos de seguridad de la industria.
    - La cultura de la seguridad.
    - La gestión por competencias.
- Fase II. Construcción del Mapa Funcional basado en el ENS.
- Fase III. Identificación de los roles laborales aplicables al alcance y entorno definidos, y descripción de los niveles de desempeño.
- Fase IV. Definición del mapa de competencias como conjunción de las competencias que aplican a cada rol laboral, asociado a su correspondiente nivel de desempeño.

A continuación se repasan y detallan cada una de estas fases, indicando las actividades que se llevan a cabo y los resultados que se obtienen, y que se presentan de manera resumida en la figura 3.1.

3.2. Fase I. Análisis del estado del problema

En esta fase preparatoria se realizan lecturas reflexivas enfocadas a la elaboración de las consideraciones iniciales, así como un análisis riguroso de las fuentes primarias más relevantes que ayuden a entender el estado del problema. Este análisis comienza con una aproximación a la realidad de la formación y concienciación en seguridad de la información en las empresas y organizaciones en España, para posteriormente estudiar en particular la situación de la seguridad de las universidades españolas.

A continuación se realiza una exhaustiva revisión sistemática de la literatura científica relacionada con la formación y concienciación en seguridad de la información basada en competencias y dirigidas al personal no TIC de empresas y organizaciones desde el año 2016 hasta la actualidad.

Este análisis permite conocer y contextualizar el ámbito del problema planteado, entender la necesidad y aporte de este trabajo, así como proveer de un marco de referencia para interpretar los resultados obtenidos (Hernández et al., 2014).

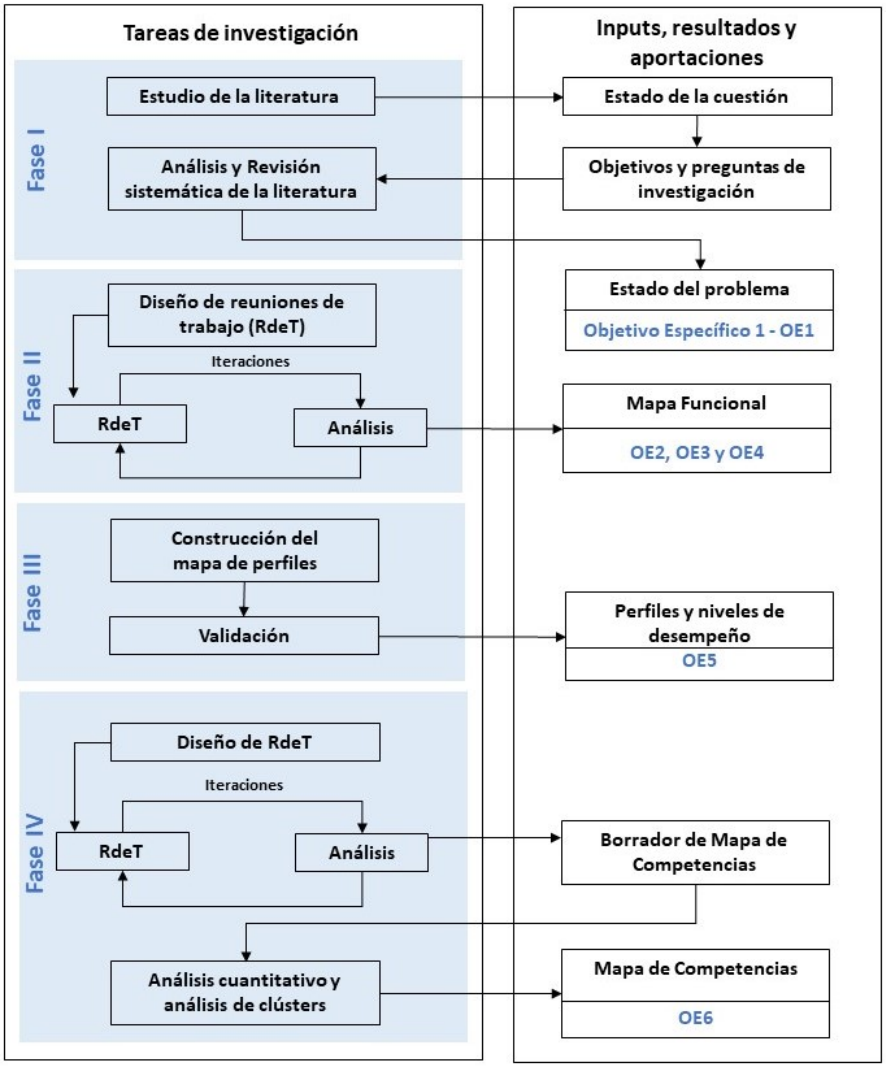

Figura 3.1: Descripción general del proceso de investigación
Fuente: Elaboración propia

3.3. Fase II. Construcción del Mapa Funcional

Para llevar a cabo la elaboración del mapa de competencias se utiliza la metodología del Análisis Funcional, un procedimiento que permite la identificación de las competencias laborales requeridas en una función productiva.

Los principios metodológicos en los que se basa el Análisis Funcional son los siguientes (CONOCER, 2000):

Se aplica de lo general a lo particular

La metodología se inicia identificando un propósito principal que defina la finalidad de la

actividad productiva. A partir del propósito se realiza una desagregación por funciones, de acuerdo con los siguientes niveles (Vargas et al., 2001)):

- Funciones clave
- Funciones principales
- Funciones básicas o unidades de competencia
- Elementos de competencia

Concluye cuando se alcanzan las funciones productivas mínimas que puede desarrollar un trabajador o trabajadora.

Debe identificar funciones delimitadas e independientes de un contexto concreto

Las funciones deben tener un comienzo y un fin claramente delimitado, y no estar asociadas a un puesto de trabajo concreto. Esto permite que las funciones identificadas sean válidas en diferentes entornos laborales. Para facilitar este principio, está generalmente aceptada la utilización de la siguiente estructura gramatical para expresar las funciones:

$$\text{Verbo} + \text{objeto} + \text{condición}$$

En esta estructura, el verbo indica la acción que debe ser ejecutada por la persona, el objeto describe el elemento sobre el que recae la acción, y la condición señala la forma, el criterio o el contexto que debe ser considerado en la realización de la acción (FOIL, 2009).

El desglose se realiza siguiendo la lógica de causa-efecto

Tal y como se ha comentado en el primer principio, la metodología trabaja de lo general a lo particular. Para ello, la lógica que se lleva a cabo se basa en la pregunta: para cumplir con este propósito (o función) *¿qué funciones son necesarias realizar?*.

Procedimiento

Antes de entrar en detalle en describir el procedimiento para la obtención del mapa de competencias, es conveniente señalar que el Análisis Funcional no intenta ser un método exacto o un conjunto de fórmulas que den un resultado exacto (SENA, 2012). Se trata de

una metodología que permite obtener un perfil de competencias laborales de una manera coherente y sistemática.

Como ya se ha dicho, el método de trabajo comienza estableciendo el propósito principal de la función productiva y a continuación se pregunta sucesivamente qué funciones hay que llevar a cabo para conseguir la función precedente. De manera más específica, una vez establecido el propósito principal, se inicia el proceso de desagregación respondiendo a la pregunta ya mencionada de qué hay que hacer para lograr dicho propósito. La respuesta será un primer nivel de desagregación, formado por las actividades, conocimientos o actitudes que se identifican como las funciones clave. A continuación, se repite la pregunta para obtener un segundo nivel de desagregación, las funciones principales. Se repite el proceso para un tercer nivel de desagregación, cuyas actividades se registran como unidades de competencia. El siguiente nivel, constituido por los elementos de competencia, ya debe señalar lo que tiene que ser capaz de conocer, entender o hacer el trabajador o trabajadora respecto a las actividades de seguridad de la información en su entorno laboral.

De acuerdo con el alcance del análisis, la profundidad en la desagregación puede variar. En general, se considera que el mapa funcional de una empresa u organización consta de tres o cuatro niveles. El proceso finaliza cuando la función puede ser desempeñada por una persona (SENA, 2012). Dicho de otro modo, cuando es posible utilizar la expresión "la persona debe ser capaz de..." con la descripción del elemento de competencia (Irigoin y Vargas, 2002). En esta tesis se alcanzan cuatro niveles de desagregación.

El resultado de este proceso es la obtención del mapa funcional, que puede ser representado gráficamente tal y como se muestra en la figura 3.2. Leído de izquierda a derecha responde a qué es necesario hacer, mientras que leído de derecha a izquierda, responde a para qué es necesario hacerlo.

En esta metodología, tradicionalmente el proceso se lleva a cabo por un grupo de expertos y expertas junto con trabajadores y trabajadoras de la función productiva estudiada, que identifican el propósito principal y llevan a cabo el proceso recurrente de desagregación (Martínez, 2011). No cabe dudar de la validez de este enfoque, especialmente si se considera que en las funciones productivas que son objeto de estudio no existe ningún tipo

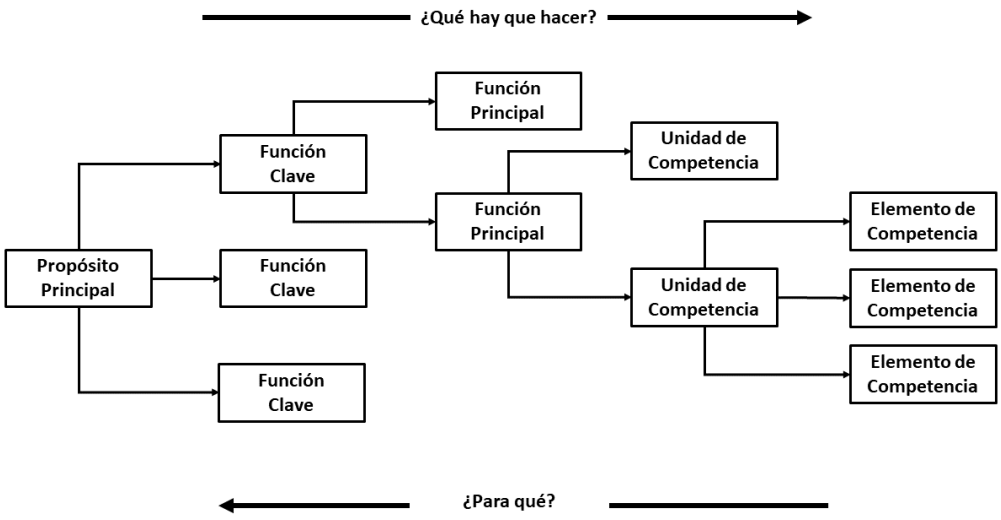

Figura 3.2: Esquema de un mapa funcional
Fuente: Adaptado de Vargas et al., 2001

de conocimiento estandarizado previo. Sin embargo, en esta tesis se propone un nuevo modelo, en el que las funciones de análisis del grupo de trabajo son reemplazadas por las medidas del Anexo II del ENS. De este modo, el grupo de expertos y expertas ya cuentan con los distintos niveles de desagregación, correspondientes a la propia organización del Anexo II. Los expertos y expertas en este nuevo enfoque, por tanto, cambian su papel. No deben llevar a cabo un trabajo de campo que les permita identificar las competencias. Su función es, en primer lugar, seleccionar las medidas de seguridad que aplican de acuerdo con el objetivo perseguido, y en segundo lugar, transformarlas en los diferentes ítems del mapa funcional.

Bajo esta propuesta, el empleo de un estándar de seguridad versus el uso del conocimiento experto permite conjeturar razonablemente varias ventajas:

- Facilita el proceso de definición del mapa funcional. Las medidas de seguridad se transforman en competencias laborales en un proceso menos costoso en recursos económicos y tiempo que la elaboración de un mapa de competencias basado en expertos y expertas que parten de cero.

- Posibilita un mapa de competencias estándar. El empleo de un estándar de seguridad permite plantear el mapa de competencias resultante como un estándar en el ámbito

definido.

- Proporciona un alcance global. Un estándar de seguridad abarca todo el ámbito de la seguridad de una organización, lo que asegura que el mapa de competencias resultante recoge íntegramente todas las necesidades competenciales.

El empleo de un estándar de seguridad también puede eliminar algunos de los inconvenientes del tradicional empleo de expertos y expertas (Yousuf, 2007):

- Los juicios de un grupo limitado de personas pueden no ser representativos.
- El sesgo cultural de los expertos y expertas puede llevarles a respuestas similares.
- Es posible que los expertos y expertas no conozcan la respuestas que se les piden.

3.4. Fase III. Identificación de los perfiles laborales

En esta fase la metodología de trabajo empleada ha sido la realización por parte del equipo de investigación de un primer borrador de perfiles laborales, tomando como punto de partida la legislación vigente. A continuación se lleva a cabo un proceso iterativo de corrección y ajuste, hasta obtener la validación por parte del panel de expertos y expertas.

3.5. Fase IV. Definición del mapa de competencias

Identificados los perfiles laborales existentes en las universidades españolas, la tarea que a continuación debe realizar el equipo de trabajo consiste en determinar para cada perfil laboral, qué elementos de competencia aplican, y de hacerlo, establecer el correspondiente nivel de desempeño.

Para llevar a cabo esta labor, al igual que en el proceso de análisis del mapa funcional, se desarrolla una investigación de tipo cualitativo a través de la realización de reuniones iterativas de trabajo con el objetivo de obtener como resultado final el mapa de competencias laborales del personal no TIC de las universidades españolas en el ámbito de la seguridad de la información.

El proceso comienza con una reunión con cada uno de los expertos y expertas. En ella

se explica y contextualiza con detalle el trabajo que se va a realizar y se resuelven las posibles dudas. Cuando, tras estas sesiones iniciales, los expertos y expertas confirman entender el objetivo perseguido y la dinámica de trabajo, comienza una primera fase de reuniones de trabajo. En estas reuniones, tal y como ya se ha señalado, los expertos y expertas determinan para cada perfil laboral qué elementos de competencia le aplican así como el nivel de desempeño. En una segunda fase, se comparten los resultados individuales obtenidos y se establecen propuestas de ajuste en sucesivas iteraciones hasta consensuar un mapa común.

Obtenida una primera versión del mapa de competencias, se aplican técnicas cuantitativas, como el análisis de clústeres, para ajustar los resultados, obteniendo como resultado la versión definitiva del mapa de competencias.

3.6. Herramientas

Para llevar a cabo las actividades descritas, a continuación se presentan las herramientas e instrumentos metodológicos utilizados en esta tesis, orientados tanto a la consecución de datos e información fiables como a la elaboración y obtención de los resultados de la investigación.

3.6.1. Panel de expertos y expertas

El Análisis Funcional presenta dos características relevantes en su método (Irigoin y Vargas, 2002). En primer lugar, se trata de un proceso experimental; no existe una manera específica de llevarlo a cabo. En segundo lugar, debe ser desarrollado por expertos y expertas de la actividad laboral que se está analizando. De acuerdo con esta segunda exigencia, las personas que intervienen en este estudio poseen una experiencia contrastada en materia de seguridad de la información en universidades españolas como Responsables de Seguridad o sus equivalentes, durante un periodo mínimo de siete años.

También se busca la mayor dispersión posible respecto al tamaño, la situación geográfica y la titularidad de la universidad. Por último, se tiene presente la paridad de género.

En base a estas características, se construye el siguiente equipo:

- Investigadores: formado por dos investigadores y una investigadora, su labor consiste en realizar las labores de diseño y coordinación de las reuniones de trabajo, así como la elaboración de los materiales de trabajo y recopilación de resultados.
- Panel de expertos y expertas: formado por dos expertos y tres expertas en seguridad de la información de universidades españolas.

En total, serán ocho personas las que llevan a cabo esta tarea, siguiendo las recomendaciones de que el grupo de expertos y expertas no sea numeroso, no excediendo de diez personas (Irigoin y Vargas, 2002).

3.6.2. Observación participante

La observación participante es una técnica de investigación cualitativa, utilizada inicialmente en la antropología y sociología, que en la actualidad es utilizada con éxito en diversos campos de investigación. Esta técnica consiste en la observación del contexto con la participación del investigador o investigadora como parte del mismo, de una forma no encubierta ni estructurada, y que permite no sólo la recogida de información, sino también aportar las experiencias y las sensaciones de la persona que observa (Vitorelli et al., 2014).

En esta tesis, el doctorando es director del Servicio Informático de la Universidad de Deusto, Responsable de seguridad de la universidad, miembro de su Comité de Seguridad de la Información, auditor de sistemas de información, CISA, y formador en materia de seguridad de la información. Esta experiencia le permite contribuir y facilitar el estudio con una mejor comprensión e interpretación del funcionamiento de los procesos que en él se producen (Balsiger y Alexandre, 2014, p. 146).

Es conveniente señalar que esta técnica puede presentar algunos inconvenientes que es necesario anotar, como puede ser el influir sobre los datos recogidos, sesgando en consecuencia los resultados (Kawulich, 2005). Sin embargo, presenta ventajas relevantes, como el entender con claridad y sin error las actividades o procesos analizados a medida que éstos se producen, y conocer las posibles formas de expresión, o de ausencia de ella, de los participantes. En cualquier caso, para evitar estos peligros, esta técnica se utiliza en combinación con otras.

3.6.3. Reuniones de trabajo

Las reuniones de trabajo son un procedimiento esencial para la recopilación de datos e información, de manera especial en las fases iniciales de exploración, así como un instrumento muy empleado en procesos de recolección de datos (Díaz-Bravo et al., 2013) y de evaluación y selección de alternativas (Bedingfield y Clarkson, 2020). Esta herramienta es ampliamente utilizada en esta tesis, ya que permite extraer la información necesaria con un alto grado de precisión y rigor para la elaboración y construcción de los distintos artefactos que componen el mapa de competencias.

En necesario anotar que gran parte de esta investigación se lleva a cabo durante el periodo de pandemia causada por el COVID-19. Debido a este motivo, las reuniones de trabajo llevadas a cabo con los expertos y expertas se realizan a través de la herramienta de videoconferencia Google Meet. Este sistema permite reunirse virtualmente con cada uno de los expertos y expertas, trabajando de manera síncrona sobre los documentos de trabajo. También se utiliza de manera generalizada el correo electrónico para coordinar las actividades del panel y compartir información y resultados. En el Anexo C se recogen, a modo de ejemplo, algunos de los correos utilizados en la investigación.

3.6.4. Teoría Fundamentada

La metodología que va a orientar la recolección de la información es la Teoría Fundamentada. La Teoría Fundamentada se utiliza ampliamente en investigaciones en el campo del *management*, de los sistemas de información o de los procesos de cambio organizacional (Cuñat, 2007).

Esta técnica fue presentada por Glaser y Strauss en 1967 (Glaser y Strauss, 2000), y desde entonces se han desarrollado y surgido múltiples enfoques. Todo estos enfoques coinciden sobre unos elementos básicos y distintivos, que servirán de orientación en este trabajo: la generación de teoría con un enfoque inductivo, el muestreo teórico y la saturación teórica.

La Teoría Fundamentada parte de un enfoque inductivo, orientada a construir teoría a partir de los datos recogidos. Para ello se establece un proceso, denominado muestreo teórico, mediante el cual el investigador o investigadora recopila, codifica y analiza los

datos, y a partir de ello decide qué datos recopila a continuación, con el objetivo de desarrollar su teoría. A medida que la investigación avanza, se identifican nuevos escenarios o enfoques para obtener un mayor y más ajustado conocimiento. Este muestreo es un proceso iterativo que se realiza hasta alcanzar la saturación teórica, es decir, el momento en el que la recogida de nuevos datos ya no añade información adicional o relevante para la investigación (Glaser y Strauss, 2000).

Este proceso se presenta, de forma resumida en la Figura 3.3. Señalar que aunque en la figura las actividades se muestran formando parte de una secuencia, en la realidad son procesos iterativos y entrecruzados.

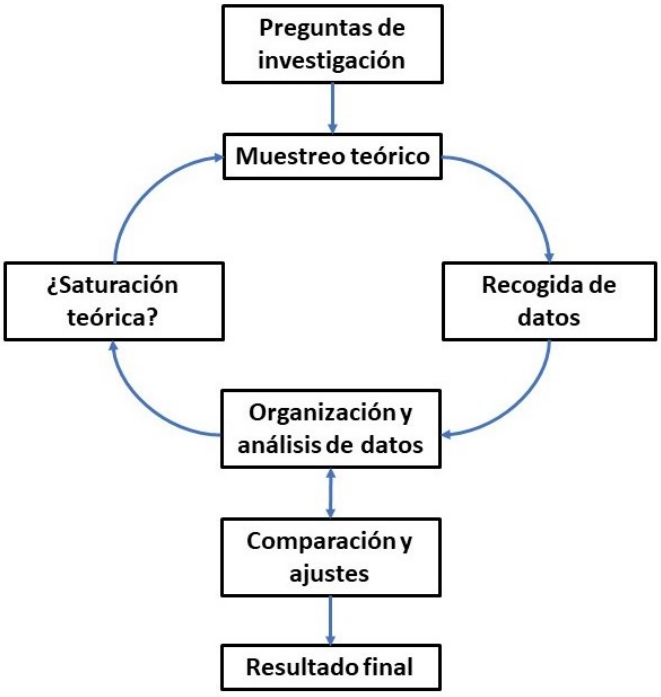

Figura 3.3: Principales fases de la Teoría Fundamentada
Fuente: Adaptado de Spinks, 2014

El procedimiento que se aplicará en este trabajo está descrito por Roberto Hernández, Carlos Fernández y Pilar Baptista (2014), quienes presentan la secuencia de la Teoría Fundamentada ejemplificada con el uso de entrevistas que se muestra en la figura 3.4.

La técnica de realizar de manera iterativa reuniones de trabajo individuales que completen y/o corrijan los resultados de reuniones previas se considera un método adecuado al objetivo perseguido. Este proceso permite alcanzar un alto nivel de consenso con relati-

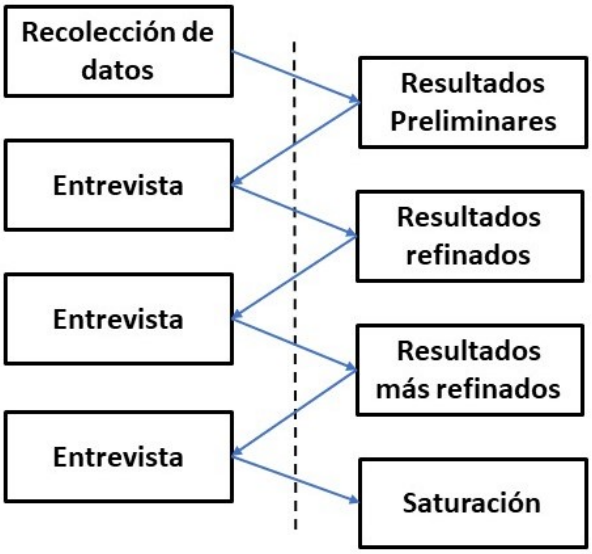

Figura 3.4: Secuencia en la Teoría Fundamentada
Fuente: Adaptado de Hernández et al., 2014

va rapidez y total fiabilidad, y con una escasa posibilidad de influencia entre expertos y expertas, ya que el ámbito de trabajo, circunscrito a las medidas del Anexo II del ENS, facilita la tarea, al limitar la posible dispersión de las respuestas.

Capítulo 4

Planteamiento y análisis del problema

"Aquel que es impuro y ha visto un crys no puede abandonar Arrakis. Ahora las cosas deben seguir su curso. No se puede apresurar nada".

Dune

4.1. La seguridad en el contexto empresarial español

Presentada la metodología de investigación, en este capítulo se analiza en primer lugar el nivel de desarrollo y madurez en el que se encuentran las actividades de formación y concienciación en seguridad de la información en las empresas y organizaciones en España, para posteriormente examinar la situación de las universidades. A este análisis se suma una revisión sistemática de la literatura relacionada con la formación y concienciación en seguridad de la información basada en competencias laborales, todo ello con el objetivo de conocer la realidad analizada y extraer una serie conclusiones que ayuden a establecer y fundamentar las propuestas de esta tesis.

Siendo necesarios procesos de formación y concienciación basados en competencias que establezcan y modulen una cultura de seguridad como parte de la cultura organizacional de cualquier empresa e institución, ¿cuál es la situación en España?, ¿qué grado de madurez tienen las empresas y organizaciones españolas en cultura de la seguridad? Para responder a estas preguntas se analizan algunos de los informes más relevantes sobre la materia realizados por instituciones y organismos de reconocida solvencia.

4.1.1. Informe del estado de la cultura de la seguridad en el entorno empresarial

El *Informe del estado de la cultura de la seguridad en el entorno empresarial español* (PwC, 2020) del año 2020 ha sido elaborado por la compañía consultora y auditora PwC sobre una muestra de cincuenta empresas de diferentes sectores, ubicación y tamaño. Para realizar el informe se han combinado varias metodologías cualitativas, como entrevistas a expertos en la materia pertenecientes tanto a las administraciones públicas como a grandes corporaciones, encuestas a responsables de seguridad y análisis de fuentes secundarias.

El informe identifica cinco niveles de cultura, asociados a los diferentes grados de madurez observados. En el nivel 1 o nivel de "Cultura Inexistente", tal y como su propio nombre indica, se sitúan aquellas empresas u organizaciones en las que no existe una cultura de seguridad. Las organizaciones que se encuentran en el nivel 2 o de "Cultura Inicial", llevan a cabo acciones no planificadas de formación y concienciación, orientadas al cumplimiento de obligaciones legales o formales. En el nivel 3 o de "Cultura en desarrollo", ya existe un plan organizado de formación y concienciación, y como consecuencia de ello, las personas conocen la política de seguridad de la organización y reconocen y reportan incidentes de seguridad. En el nivel 4 o de "Cultura avanzada", el plan contiene objetivos a largo con revisiones y actualizaciones anuales, y se trabaja en actividades enfocadas a suscitar un cambio en las creencias, actitudes y percepciones sobre la seguridad. Finalmente, en el nivel 5 o de "Forma de vida", se sitúan las empresas donde la planificación se basa en el empleo de métricas que les permiten realizar un seguimiento de las actividades llevadas a cabo y de los resultados obtenidos, realizando en base a ello acciones de mejora continua.

De acuerdo con esta escala, resumida en la tabla 4.1, el estudio sitúa el nivel medio de la cultura de seguridad alcanzado por las empresas y organizaciones españolas en un 2,8. Esta cifra resume una realidad en la que las actividades de formación y concienciación en seguridad no ocupan un lugar destacado en la estrategia de la organización, y se realizan en líneas generales, de forma aislada y sin objetivos claros ni evaluables (PwC, 2020, p. 17). Se trata de un nivel ciertamente inmaduro y con un amplio margen de mejora.

Detallando esta realidad, y por su interés para este trabajo, se reproduce el siguiente texto

Nivel	Descripción del nivel
1	Cultura Inexistente
2	Cultura Inicial
3	Cultura en desarrollo
4	Cultura avanzada
5	Forma de vida

Tabla 4.1: Niveles de madurez en cultura de la seguridad
Fuente: Elaboración propia

del estudio:

> Por otro lado, se ha podido observar que no existe de forma generalizada una estrategia o políticas de formación y capacitación formalizadas que permitan aumentar las competencias de las personas con responsabilidad en seguridad.
>
> Sin embargo, el punto que queremos resaltar como un hecho preocupante es que la medición del estado y del nivel tanto de formación técnica como de concienciación en ciberseguridad de la compañía se contempla de forma muy limitada o casi inexistente.
>
> Las métricas desempeñan un papel crucial en el cambio de cultura y la seguridad de la información, ya que ayudan a evaluar el estado actual de la compañía y el nivel objetivo deseado de forma realista y progresiva. Nos ayudan a gestionar el proceso y el progreso. Ofrecen retroalimentación útil a la compañía y a la gerencia, y pueden afirmar la efectividad de las medidas de seguridad implementadas y de las iniciativas de cultura de ciberseguridad que se lleven a cabo.
>
> Las buenas métricas deben ser cuantificables, repetibles y comparables para permitir información precisa. También deben poder obtenerse fácilmente, ser relevantes y ofrecer información útil.

Varios aspectos son significativos en este texto. En primer lugar, la trascendencia de utilizar un modelo de competencias que orienten las actividades de formación y concienciación, idea nuclear de esta tesis, y en segundo lugar, la necesidad y la importancia de establecer métricas que permitan establecer objetivos, evaluar la situación inicial y realizar una ade-

cuada gestión del proceso de mejora. Sin embargo, la realidad es bien distinta. El informe señala que el 48 % de las organizaciones estudiadas disponen de planes de formación en seguridad, pero que tan sólo el 28 % consideran dentro de dichos planes las competencias actuales y futuras de sus empleados y empleadas.

4.1.2. Informe de Madurez de Ciberseguridad

El *Informe de Madurez de Ciberseguridad 2021* (Minsait, 2021) ha sido elaborado por la empresa Minsait, perteneciente al grupo Indra, mediante un estudio cualitativo basado en entrevistas individuales basadas en un cuestionario y realizadas a noventa y ocho expertos y expertas de diversas empresas y organizaciones. El perfil predominante de las personas entrevistadas ha sido el de responsable de seguridad, complementado con otros perfiles de dirección.

Los resultados más relevantes de este informe señalan que el 68 % de las organizaciones no cuentan con un responsable de seguridad, y que sólo el 36 % de las empresas destinan recursos económicos específicos a la seguridad. Estos datos generales se complementan con datos más detallados: "únicamente el 28 % de las empresas han desarrollado métricas que midan el impacto de las acciones de ciberseguridad en la organización, evaluando si se cumplen las expectativas fijadas a través de un proceso de reporting formalizado".

Respecto a la formación, "tan sólo el 37 % de las empresas entrevistadas cuentan con mecanismos formales necesarios para formar, concienciar e incentivar a los empleados y empleadas en materia de ciberseguridad".

Las cifras y análisis de estos informes dibujan un panorama preocupante, en el que no existe una cultura de la seguridad, con menos de un tercio de las empresas en las que las actividades de formación y concienciación están planificadas y cuentan con métricas, y donde el empleo de modelos basados en competencias laborales es escaso.

4.2. La seguridad en las universidades españolas

Repasada la situación en el ámbito empresarial, a continuación se lleva a cabo un examen de la situación de las universidades españolas. Para ello se analizarán el *Informe Nacional*

del Estado de la Seguridad, INES, y el documento UNIVERSITIC.

4.2.1. Informe Nacional del Estado de la Seguridad

INES es un procedimiento desarrollado por el CCN para la gobernanza de la seguridad de la información, con el objetivo de evaluar de manera regular el nivel de la seguridad de los sistemas TIC de empresas y organizaciones y su adecuación al ENS.

La recopilación y comunicación de datos que permite confeccionar este informe es de obligado cumplimiento para los organismos a los que se aplica el ENS de acuerdo con el artículo 2 de la Ley 40/2015 (BOE, 2015a), siendo sus objetivos "conocer las principales variables de la seguridad de la información de los sistemas comprendidos en el ámbito de aplicación del Esquema Nacional de Seguridad, y confeccionar un perfil general del estado de la seguridad" (BOE, 2016b).

Las empresas y organizaciones que deben aportar los datos cuentan con una instrucción técnica, la Guía de Seguridad CCN-STIC 824 (CCN, 2020a). En ella se definen y explicitan los procedimientos necesarios para la elaboración del perfil del estado de la seguridad.

Para conocer el nivel de cumplimiento de las medidas de seguridad del ENS, y en consecuencia el nivel de desarrollo de los procedimientos de seguridad, INES utiliza como métrica básica el conocido modelo C*apability Maturity Model*, CMM de la Carnegie Mellon University. De acuerdo con este modelo, se establecen diferentes perfiles, identificados como niveles de madurez, que señalan el grado de cumplimiento de las medidas de seguridad del ENS expresado en porcentaje, tal y como se detalla en la tabla 4.2.

Nivel	Porcentaje	Descripción del nivel
L0	0	Inexistente
L1	10	Inicial/ad hoc
L2	50	Reproducible, pero intuitivo
L3	80	Proceso definido
L4	90	Gestionado y medible
L5	100	Optimizado

Tabla 4.2: Nivel de cumplimiento de las medidas del ENS
Fuente: Ley 40/2015 de 1 de octubre

Hay que tener en cuenta que el nivel mínimo de madurez requerido por el ENS está definido

en función de la categoría del sistema, tal y como se explicó en la página 49 de esta tesis. De acuerdo con ello, los niveles mínimos requeridos según la categoría son los que figuran en la tabla 4.3.

Categoría del sistema	Nivel mínimo de madurez
Básica	L2 – Reproducible, pero intuitivo (50 %)
Media	L3 – Proceso definido (80 %)
Alta	L4 – Gestionado y medible (90 %)

Tabla 4.3: Nivel de madurez según categoría
Fuente: Guía de Seguridad CCN-STIC 824

Realizada esta breve explicación, se analizan los datos relevantes del informe referidos a las universidades españolas para el año 2020 (CCN, 2020b).

Recursos

El primer dominio analizado son los recursos humanos y económicos empleados por las universidades en el ámbito de la seguridad. Dentro del mismo se realizan varias preguntas, siendo una de ellas especialmente significativa para el propósito de este trabajo: ¿qué parte del presupuesto de seguridad TIC se dedica a actividades de concienciación y formación? Nótese que esta pregunta no limita la respuesta a un determinado nivel de madurez en la propia actividad de formación. Por ello, cualquier tipo de actividad es válida, independientemente de su nivel de madurez.

De las cuarenta y nueve respuestas válidas, veintidós han respondido con un cero. Es decir, el 45 % de las universidades españolas no recogen en su presupuesto de seguridad de la información ninguna partida económica destinada a formación y concienciación en seguridad. Un dato a todas luces muy significativo que ilustra la situación de la cultura de la seguridad en nuestras universidades.

Detallando más las cifras, el 29 % de las universidades dedican entre un 1 % y un 4 % de su presupuesto a formación y concienciación, porcentaje que desciende al 22 % cuando la partida económica para formación y concienciación se encuentra entre el 5 % y el 10 %. Por encima del 10 % se sitúan tan sólo un 4 % de las universidades, tal y como se muestra en la tabla 4.4.

Porcentaje del presupuesto	Número de universidades	Porcentaje de universidades
0	22	44,90 %
1-4	14	28,57 %
5-10	11	22,45 %
11-20	2	4,08 %
21-100	0	0,00 %

Tabla 4.4: Esfuerzo en actividades de concienciación y formación
Fuente: elaboración propia

Estos datos resultan muy significativos para comprender la realidad de las universidades españolas en el ámbito de la formación y concienciación en seguridad de la información, y ponen de relieve la pertinencia de la propuesta de esta tesis.

El dominio de los recursos humanos y económicos empleados por las universidades en el ámbito de la seguridad muestra el porcentaje del presupuesto dedicado a la seguridad sobre el total de recursos dedicados a TI. Este dato, cruzado con el porcentaje del presupuesto destinado a actividades de formación y concienciación en aquellas universidades que lo tienen, permite conocer el esfuerzo real que representa ese porcentaje sobre el conjunto de las actividades TI, expresadas a través del presupuesto destinado a formación respecto al presupuesto total, y no sólo al de seguridad. Los datos para cada una de las universidades pueden consultarse en el Anexo D de este trabajo, donde puede apreciarse que tan sólo dos universidades dedican a actividades de formación y concienciación más del 1 % de su presupuesto de TI, en ambos casos el 1,20 %, estando por debajo del 0,5 % cuarenta y tres universidades, es decir, el 87,75 %.

Esta situación se presenta de manera gráfica en la figura 4.1, donde sobre un índice 100 que marca el total del presupuesto en TI de las cuarenta y nueve universidades, se pueden ver los escasos recursos, apenas visibles, destinados a actividades de formación y concienciación en seguridad.

Empleando la mediana como estadístico en lugar de la media con el objetivo de conocer la tendencia central, el porcentaje del presupuesto de TI en las universidades españolas destinado a seguridad representa el 6 %, y el destinado a labores de formación y concienciación en seguridad, sean éstas del tipo que sean, es del 0,2 %.

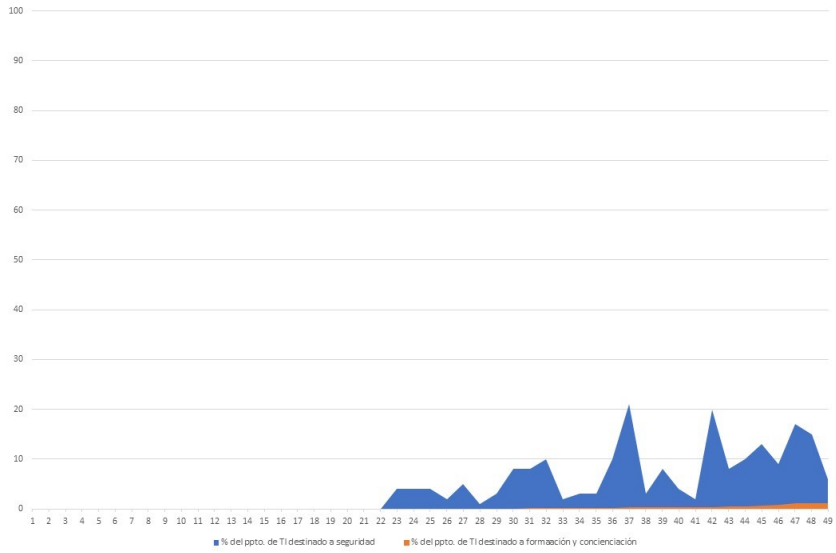

Figura 4.1: Esfuerzo en formación y concienciación
Fuente: Elaboración propia

Estos datos permiten conocer la complicada realidad de la seguridad de la información en general, y de las actividades de formación y concienciación en particular, de la universidades españolas. Una realidad que refleja el escaso nivel de madurez existente y el amplio camino de mejora. A este respecto, el propio informe explicita la necesidad de "desarrollar soluciones horizontales para facilitar actividades de concienciación del personal".

Medidas del Anexo II del ENS

Analizados los recursos económicos y humanos, el informe también analiza el nivel de cumplimiento de las medidas de seguridad del Anexo II del ENS.

Tal y como ya se explicó en la página 50 de esta tesis, las medidas de seguridad se dividen en tres grupos:

- 3. Marco organizativo
- 4. Marco operacional
- 5. Medidas de protección

Dentro de las medidas de protección se encuentra el apartado 5.2 referente a la Gestión del personal, que recoge la caracterización de los puestos de trabajo, los deberes y obligaciones de las personas que trabajan con el sistema y las actividades de concienciación y formación,

recogidas en los puntos 5.2.3 y 5.2.4.

Los valores obtenidos por las universidades respecto al nivel de cumplimiento de las medidas de protección adoptadas en la Gestión del personal se muestran en la tabla 4.5. Para interpretar adecuadamente estos datos, también se presentan los valores objetivo que deben alcanzarse en cada categoría.

Categoría	Gestión del personal	Valor objetivo
Básica	40 %	L2 - 50 %
Media	45 %	L3 - 80 %
Alta	49 %	L4 - 90 %

Tabla 4.5: Nivel de cumplimiento en Gestión del Personal
Fuente: elaboración propia

Los datos específicos para las medidas de seguridad del apartado Formación y Concienciación para cada categoría y el valor objetivo se muestran en la tabla 4.6.

Categoría	Concienciación	Formación	Valor objetivo
Básica	31 %	28 %	50 %
Media	48 %	40 %	80 %
Alta	30 %	25 %	90 %

Tabla 4.6: Nivel de cumplimiento en Formación y Concienciación
Fuente: elaboración propia

Estos datos se presentan de manera gráfica en la figura 4.2, donde se aprecia con claridad el amplio margen de mejora existente para alcanzar los valores objetivo, en especial en la categoría alta.

Formación y concienciación

INES aporta información sobre el esfuerzo realizado tanto en cursos de formación al personal de TI como en cursos de formación y sesiones de concienciación de seguridad dirigidos a toda la organización. Este esfuerzo se mide en horas/persona, considerándose "cualquier tipo de curso, incluida la formación a distancia y los cursos online" (CCN, 2020b, p. 153).

De las cuarenta y una universidades que han aportado datos en este epígrafe, diecinueve reconocen no dedicar ninguna hora a labores de formación y concienciación, prácticamente la mitad de las universidades. Seis dicen dedicar una hora/persona, y sólo siete dicen

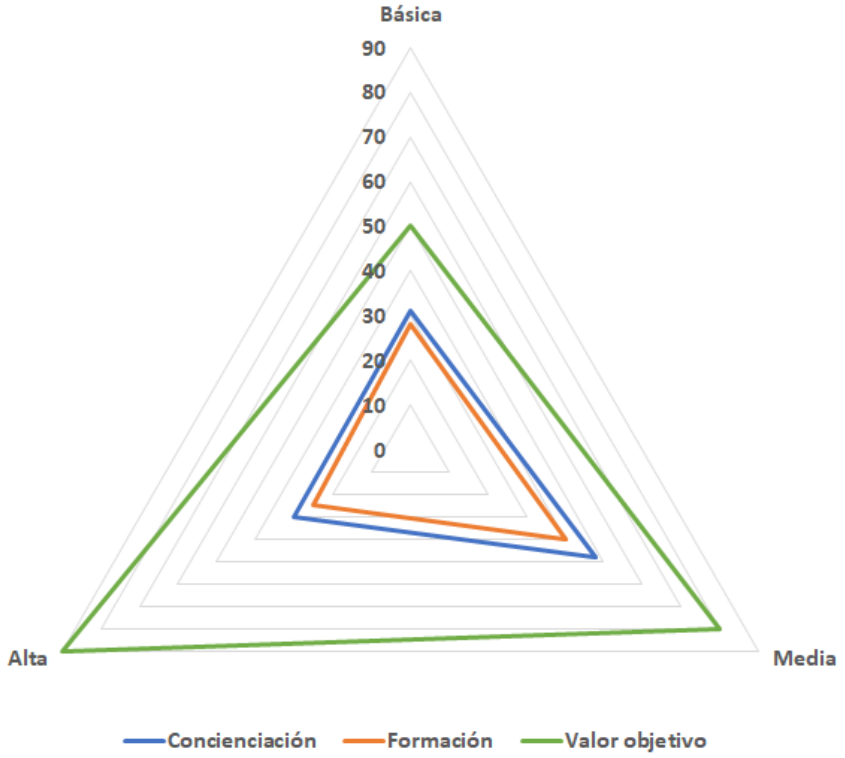

Figura 4.2: Perfil de cumplimiento en Formación y Concienciación
Fuente: elaboración propia

dedicar diez o más horas/persona. La mediana para este epígrafe muestra un valor de una hora/persona dedicada a formación y concienciación a lo largo del año 2020. Es sin duda, un dato definitivo para avalar el escaso nivel dedicado a cualquier tipo de formación y concienciación en seguridad de la información en las universidades españolas.

A la vista de estos datos, no cabe duda de la necesidad de trabajar sin demora en el desarrollo de la cultura de la seguridad en las universidades españolas a través de actividades de formación y concienciación que ayuden a corregir esta situación.

4.2.2. UNIVERSITIC

La Sectorial de Tecnologías de la Información y las Comunicaciones de la Asociación de Universidades Españolas, Crue, publica periódicamente el documento UNIVERSITIC, que recoge el análisis detallado de la situación global de las TI en las universidades españolas a través de indicadores de gestión y de buenas prácticas, utilizando para ello los datos aportados de forma voluntaria por las propias universidades. El último documento disponible,

UNIVERSITIC 2017, está realizado con las respuestas de cuarenta y nueve universidades, sobre un total de setenta y cuatro, lo que representa dos tercios del total de universidades españolas, y que engloban al 84 % de los estudiantes universitarios (Crue, 2017). La recogida de datos se organiza en dos apartados, identificados como "Descripción de las TI" y "Gestión de las TI". Estos apartados están organizados en once ejes, cinco en la capa de descripción y seis en la de gestión, que recogen 214 indicadores.

De estos indicadores, tan sólo uno de ellos hace referencia a actividades de formación para el personal no TI, aunque no se ciñe a actividades de formación y concienciación en seguridad. El indicador recoge el porcentaje del Personal de Administración y Servicios, PAS, y del Personal Docente e Investigador, PDI, que ha recibido formación en competencias TI, siendo el 36,52 % y el 21,52 %.

Más allá de estas cifras, lo que resulta significativo es que en un documento elaborado por las propias universidades españolas no existan datos específicos sobre los recursos destinados a formación y concienciación en seguridad para el personal universitario.

4.3. Revisión sistemática de la literatura

En este apartado se presenta y recoge el análisis pormenorizado de la literatura científica relevante relacionada con la formación y concienciación en seguridad de la información basadas en competencias dirigidas al personal no TIC de empresas y organizaciones. Se pretende conocer si existen experiencias anteriores en el ámbito definido y corroborar los objetivos de investigación de esta tesis, reivindicando de este modo su necesidad y contribución al cuerpo de conocimiento existente. Este estudio ha sido publicado en el artículo "Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura" (Mendivil et al., 2021).

Existen múltiples estudios secundarios que abordan diversos aspectos relacionados con la seguridad de la información, (e.g. Ulven y Wagen, 2021; Ali et al., 2021; Rahim et al., 2015), pero no se han encontrado estudios recientes que analicen desde la perspectiva de las competencias las actividades de formación y concienciación en seguridad para empleados y empleadas no TIC.

Para confirmar esta carencia se analiza la producción científica mediante la Revisión Sistemática de Literatura RSL, propuesta por Kitchenham (Kitchenham, 2004).

De acuerdo con esta metodología, las actividades que se van a desarrollar son los siguientes:

- Definir los aspectos que se desean conocer.
- Determinar las fuentes de datos.
- Definir la estrategia de búsqueda.
- Establecer los criterios de inclusión y exclusión.
- Realizar el proceso de selección.
- Presentar los resultados.

4.3.1. Cuestiones a resolver

La RSL es una metodología que recopila y analiza trabajos de investigación a través de un proceso sistemático en el campo de interés elegido con el objetivo de dar respuesta a determinadas preguntas de investigación (García-Peñalvo, 2020). En este estudio se busca dar respuesta a las siguientes cuestiones:

- ¿Cuál es la evolución en el número de publicaciones relacionadas con el uso de competencias en la formación y concienciación en materia de seguridad de la información para personal no TIC desde el año 2016 hasta la actualidad?
- ¿Cuáles son las metodologías que se utilizan para identificar las competencias en seguridad?
- ¿Se identifican diferentes roles de acuerdo a las distintas necesidades en el ámbito de la seguridad de los puestos de trabajo y responsabilidades de una organización?
- ¿Cuáles son los objetivos que se persiguen?

4.3.2. Selección de las bases de datos

El análisis de las bases de datos se lleva a cabo entre los meses de julio y agosto del año 2021. Después de un examen de las bases de datos existentes, se seleccionan como fuentes

de búsqueda de datos primarios IEEE Xplore, ACM Digital Library y SCOPUS.

IEEE Xplore es una base de datos de investigación académica que cuenta con una amplia literatura en el ámbito de las TIC. ACM Digital Library es la mayor base de datos existente especializada en informática y tecnologías de la información, y SCOPUS es una de las bases de datos con mayor número de resúmenes y citas de artículos de revistas científicas revisadas por pares. La selección de estas bases de datos, de gran prestigio y uso, ayuda a garantizar la calidad y fiabilidad de los estudios y artículos seleccionados.

4.3.3. Estrategia de búsqueda

Para las búsquedas se utilizan los términos "formación", "concienciación", "seguridad" y "competencias", algunos términos equivalentes, así como los conectores lógicos "Y" y "O", tanto en español como en inglés. La cadena de búsqueda inicial diseñada es, para las fuentes primarias en inglés:

("cybersecurity" OR "cyber security" OR "computer security" OR "IT Security") AND "awareness" AND "training" AND ("skills" OR "competences" OR "competencies")

4.3.4. Criterios de inclusión y exclusión

Acotadas las bases de datos y definida la cadena general de búsqueda, se seleccionan los estudios primarios de acuerdo con los siguientes criterios.

Criterios de inclusión:

- Estudios primarios que reporten iniciativas de investigación en el ámbito de formación y concienciación en seguridad en empresas y organizaciones que utilicen marcos de competencias.
- Las búsquedas se realizan en todo el texto del artículo, incluyendo el título, palabras clave y resumen.
- Estudios primarios reportados tanto en idioma inglés como en español.
- Estudios primarios reportados entre enero de 2016 y agosto de 2021.
- Artículos de revistas o conferencias.

Criterios de exclusión:

- Artículos duplicados.
- Artículos cuyo contenido completo no sea accesible.
- Artículos que hagan referencia a formación en seguridad, pero no relacionada con el uso de competencias.
- Artículos sobre formación y concienciación en seguridad pero que no están orientados al personal no TIC de empresas y organizaciones.

4.3.5. Proceso de selección

En esta fase se ejecuta la cadena de búsqueda en las bases de datos seleccionadas, ajustando la cadena a la sintaxis de cada base de datos, considerando los criterios de inclusión.

A continuación se señalan las cadenas utilizadas para las búsquedas en inglés:

IEEE: (((“Full Text Only”:“cybersecurity” OR “cyber security” OR “computer security” OR ´´IT Security”) AND “Full Text Only”:“awareness” AND “Full Text Only”:“training” AND (“Full Text Only”:“skills” OR “Full Text Only”:“competences” OR “competencies”))) Filters Applied: Conferences. Journals. 2016 - 2021.

ACM: [[All: “cybersecurity”] OR [All: “cyber security”] OR [All: “computer security”] OR [All: “it security”]] AND [All: awareness] AND [All: training] AND [All: skills OR competences OR competencies] AND [Publication Date: (01/01/2016 TO 08/31/2021)]

SCOPUS: TITLE-ABS-KEY (“cybersecurity” OR “cyber security” OR “computer security” OR “IT Security”) AND “awareness” AND “training” AND (“skills” OR “competencies” OR “competences”) AND (LIMIT-TO (DOCTYPE,“cp”) OR LIMIT-TO (DOCTYPE,“ar”)) AND (LIMIT-TO (PUBYEAR,2021) OR LIMIT-TO (PUBYEAR,2020) OR LIMIT-TO (PUBYEAR,2019) OR LIMIT-TO (PUBYEAR,2018) OR LIMIT-TO (PUBYEAR,2017) OR LIMIT-TO (PUBYEAR,2016)) AND (LIMIT-TO (LANGUAGE, “English”) OR LIMIT-TO (LANGUAGE,“Spanish”))

Las búsquedas llevadas a cabo dan como resultado 1300 artículos, sobre los que se lleva a cabo una primera selección, revisando los títulos, resúmenes y, en caso necesario leyendo los

artículos completos, con el objetivo tanto de comprobar si la información está relacionada con el objeto de estudio como de evaluar si se cumplen los criterios de exclusión. En este primer proceso de selección se recopilan cuarenta y nueve artículos.

Los artículos seleccionados se someten a un segundo examen más detallado, de acuerdo con los siguientes criterios de selección:

- Las actividades de formación y concienciación en seguridad deben tener un alcance global, y no estar limitadas a un área específica, como por ejemplo el ransomware, el phising, la telefonía móvil o la *gamificación*.
- Las actividades de formación y concienciación en seguridad deben estar diseñadas para los trabajadores y trabajadoras no TIC de las empresas y organizaciones.
- La identificación de las competencias tiene que ser un elemento central en la definición de las actividades de formación y concienciación.
- La investigación debe centrarse en la selección y diseño de los contenidos, y no en las metodologías de impartición, modelos de medición o aspectos pedagógicos.

Son leídos, analizados y evaluados, cumpliendo todos los criterios de selección únicamente diez de ellos. La figura 4.3 muestra de forma gráfica el proceso de selección llevado a cabo y los resultados obtenidos, compuestos por un artículo de IEEE Explore, tres artículos de ACM Digital Library y seis artículos de SCOPUS.

En la Tabla 4.7 se recoge el detalle de los estudios seleccionados.

4.3.6. Interpretación de los datos obtenidos

Con la información recogida puede darse respuesta a las cuestiones inicialmente planteadas.

¿Cuál es la evolución en el número de publicaciones relacionadas con el uso de competencias en la formación y concienciación en materia de seguridad para personal no TIC desde el año 2016 hasta la actualidad?

El aspecto tal vez más destacado, y una aportación relevante de esta investigación es la constatación del escaso número de artículos que contemplan el uso de marcos de competencias a la hora de abordar la formación y concienciación del personal no TIC de empresas

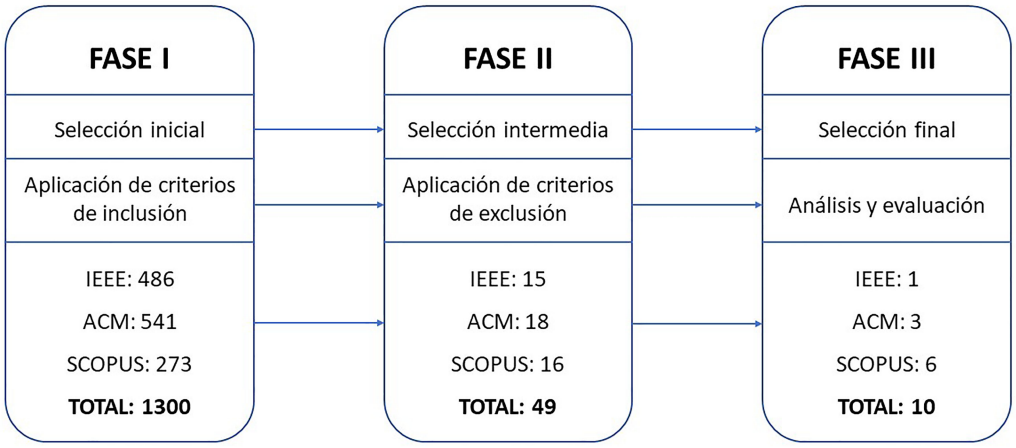

Figura 4.3: Proceso de selección de estudios primarios
Fuente: Elaboración propia

y organizaciones. Pese a este limitado número de publicaciones y estudios que cumplen los criterios de selección, la evolución en su número muestra una clara linea ascendente, tal y como refleja la figura 4.4, lo que permite apuntar un interés creciente.

¿Cuáles son las metodologías que se utilizan para identificar las competencias en seguridad?

En los artículos analizados se constata el empleo de tres diferentes metodologías para identificar las competencias en seguridad de la información que deben alcanzar los trabajadores y trabajadoras no TIC.

En primer lugar se encuentran las investigaciones que emplean estándares de seguridad. Es la metodología más empleada, con cinco estudios. Respecto a los estándares utilizados, la tabla 4.8 muestra cuáles fueron tomados como referencia. Se utilizan el *Programa sobre formación y concienciación en ciberseguridad* de la London Digital Security Centre, LDSC, la serie de publicaciones NIST 800 sobre seguridad y privacidad para organizaciones y sistemas de información del NIST, el ya mencionado NICE, recogido en la publicación NIST 800-181, y finalmente el programa GEIGER de *Aprendizaje estándar en ciberseguridad*, desarrollado por un consorcio de empresas y organizaciones del ámbito de la ciberseguridad

Código	Referencia	Título	Base de datos
C01	(Bada y Nurse, 2019)	Developing cybersecurity education and awareness programmes for small and medium-sized enterprises.	SCOPUS
C02	(Ani et al., 2019)	Human factor security: evaluating the cybersecurity capacity of the industrial workforce.	SCOPUS
C03	(Carlton et al., 2019)	Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills.	SCOPUS
C04	(Hatzivasilis et al., 2020)	Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees.	SCOPUS
C05	(Sithole et al., 2020)	A framework for a foundational cyber counter-intelligence awareness and skills training programme.	SCOPUS
C06	(Trim y Lee, 2021)	The Global Cyber Security Model: Counteracting Cyber Attacks through a Resilient Partnership Arrangement.	SCOPUS
C07	(Wang et al., 2018)	Framework of Raising Cyber Security Awareness.	IEEE
C08	(Khan et al., 2019)	viCyber: An Intelligent Curriculum Design Tool for Cybersecurity Education.	ACM
C09	(Remmele y Peichl, 2021)	Structuring a Cybersecurity Curriculum for Non-IT Employees of Micro- and Small Enterprises.	ACM
C10	(de Vicente et al., 2021)	GEIGER: Solution for small businesses to protect themselves against cyber-threats.	ACM

Tabla 4.7: Estudios seleccionados

con fondos del programa Horizonte 2020 de la Unión Europea.

Estándar	Organismo	Estudio primario
Programa sobre formación y concienciación en ciberseguridad.	LDSC	[C01]
Serie NIST 800	NIST	[C07]
NIST 800 - 181 - NICE	NIST	[C08]
GEIGER	Consorcio	[C09][C10]

Tabla 4.8: Estándares empleados

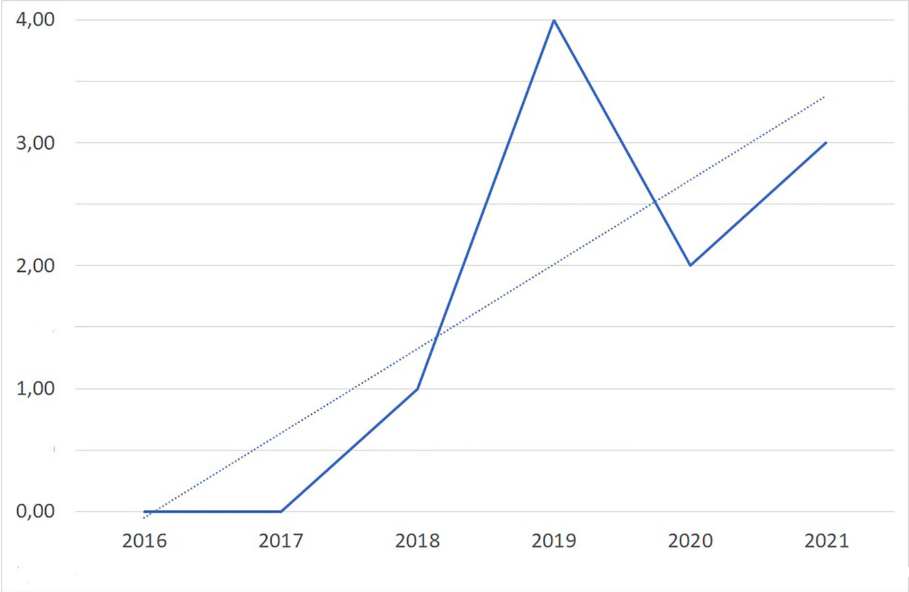

Figura 4.4: Número de publicaciones por año y tendencia
Fuente: Elaboración propia

La segunda metodología, empleada en tres de los artículos seleccionados, es la conocida como *juicio de expertos*. Se lleva a cabo mediante la realización de entrevistas o empleando el método Delphi, para, a partir de los resultados, definir y establecer un modelo de formación y concienciación en seguridad de la información.

Finalmente, como tercera metodología se utiliza el análisis interno de las necesidades en materia de seguridad de una empresa u organización específica, y el posterior diseño y configuración de un programa de formación y concienciación a medida.

¿Se identifican diferentes roles de acuerdo a las distintas necesidades en el ámbito de la seguridad de los puestos de trabajo y responsabilidades de una organización?

Tan sólo uno de los estudios analizados plantea la necesidad de establecer diferentes contenidos y niveles de formación y concienciación de acuerdo con el sector industrial, el perfil laboral y el puesto de trabajo específico del personal. En otros dos artículos se utiliza el concepto de "nivel" para establecer diferentes grados de formación para el personal no TIC, aunque estos niveles no se encuentran relacionados directamente a perfiles laborales. En el resto de publicaciones no se hace referencia a estos perfiles, considerando por ello que las necesidades de formación y concienciación en seguridad son iguales para todo el

personal usuario de las TIC en una organización.

¿Cuáles son los objetivos que se persiguen?

Todos los estudios analizados tienen como objetivo principal el proponer un programa de formación y concienciación en materia de seguridad dirigido al personal laboral no TIC. Aunque en todos ellos se consideran las competencias, los planteamientos varían. En la tabla 4.9 se presentan los diferentes enfoques de los estudios analizados. La mitad de las investigaciones se orientan a los aspectos educativos, pedagógicos o de diseño de los modelos propuestos; tres artículos hacen énfasis en la medición de las capacidades y conocimientos de los empleados sobre aspectos de seguridad, y finalmente el resto de estudios se centran en la contrainteligencia o en el incremento de la resiliencia.

Objetivos	Estudios primario
Aspectos educativos, pedagógicos o de diseño del marco propuesto	[C01], [C04], [C08], [C09], [C10]
Medición de capacidades y conocimientos	[C02], [C03], [C07]
Enfoque de contrainteligencia	[C05]
Incremento de la resiliencia	[C06]

Tabla 4.9: Objetivos

4.4. Algunas consideraciones

Del análisis de las fuentes primarias y de la literatura llevados a cabo pueden extraerse varias conclusiones. La primera de ellas es la existencia de un elevado número de artículos y estudios que abordan de maneras muy diversas la formación y concienciación en seguridad desde un punto de vista competencial, lo que demuestra el interés que suscita la materia. Sin embargo, los estudios enfocados de manera específica a los trabajadores y trabajadoras no TIC son significativamente escasos. Esta falta de estudios evidencia una carencia que debe ser corregida. Se necesitan nuevas investigaciones que amplíen y mejoren el actual estado del arte en la materia con nuevas propuestas metodológicas que faciliten la creación de marcos de competencias ajustados a las necesidades de las organizaciones y

que permitan identificar los contenidos y niveles de formación y concienciación necesarios para cada perfil laboral y puesto de trabajo.

La segunda conclusión que se obtiene es la constatación de la práctica inexistencia de estudios que contemplen de manera explícita el uso de perfiles laborales a la hora de diseñar planes de formación y concienciación en seguridad. Sin embargo, los distintos roles profesionales que existen en las empresas y organizaciones requieren actividades de formación y concienciación específicas y adecuadas a sus diversos desempeños y niveles de responsabilidad. No atender estas diferencias impide al personal de empresas y organizaciones alcanzar el nivel adecuado de formación y concienciación en seguridad.

En tercer lugar, se observa que las metodologías que se emplean en la confección de programas de formación y concienciación se siguen basando en enfoques clásicos: estándares de seguridad, análisis internos ad hoc y juicios de expertos. Estos enfoques sin duda han demostrado su validez, pero también presentan limitaciones. Como ya se ha explicado, la aplicación de estándares sin una adaptación y adecuación a las distintas necesidades de cada perfil laboral puede dar como resultado un modelo de carácter excesivamente generalista, y que en consecuencia no satisfaga las exigencias reales en el ámbito de la seguridad de muchos puestos de trabajo. El uso de programas de formación y concienciación basados en la definición de contenidos determinados por juicios de expertos adolece de la misma limitación. Por otro lado, los análisis y desarrollos internos construidos a medida se ajustan sin duda a las necesidades de la empresa u organización analizada, pero llevan aparejados un nivel de esfuerzo y coste en tiempo, recursos humanos y económicos sólo al alcance de un limitado número de organizaciones. Y sin embargo, sus resultados no pueden extrapolarse o ser utilizados por otras organizaciones al ser desarrollados para dar respuesta específica al alcance y entorno definidos. Pese a estas limitaciones, tal y como se comprueba en este estudio, no existen propuestas alternativas que planteen nuevos enfoques o mejoras a estos modelos.

Estas consideraciones permiten confirmar la existencia de un ámbito de mejora en el estado del arte de la formación y concienciación en seguridad de la información. Aún siendo en línea generales un importante campo de desarrollo e investigación, sin embargo el uso de marcos de competencias asociados a roles laborales para personal no TIC no

presenta el mismo grado de avance. Los escasos estudios que abordan la materia se siguen basando en metodologías que no parecen haber sido revisadas ni actualizadas. También se ha podido constatar el escaso nivel de cultura de seguridad existente en las organizaciones, que conlleva una escasa atención a la formación en seguridad.

Ante esta realidad, explorar nuevas propuestas que investiguen y propongan modelos de referencia estándar basados en competencias para la formación y concienciación del personal no TIC en particular parece conveniente y recomendable, avanzando de este modo en la mejora tanto de la resiliencia de las organizaciones en particular como de la cultura de la seguridad en general.

Capítulo 5

Desarrollo de la solución

"Levanto la cabeza. Tal vez volveré a casa
algún día. Pero ahora mismo no.
Ahora mismo tengo cosas que hacer".

Proyecto Hail Mary

5.1. Plan de trabajo

Analizado en profundidad el problema que se busca resolver, a continuación se construye la propuesta objeto de esta tesis. Para llevar a cabo esta tarea, el capítulo se organiza en las siguientes secciones: en primer lugar se construye el mapa funcional de competencias laborales asociadas a la seguridad de la información para el personal no TIC de las universidades españolas, utilizando para ello el Análisis Funcional y las medidas de seguridad del Anexo II del ENS. A continuación se especifican los perfiles laborales atendiendo a un enfoque orientado a la seguridad de la información, así como los niveles de desempeño para cada perfil identificado. Finalmente se elabora el mapa de competencias, como relación entre los perfiles laborales y las competencias que aplican a cada uno de ellos junto a su nivel necesario de cumplimiento.

5.2. Mapa funcional

Para identificar las competencias de una organización, empresa o sector, habitualmente se desarrollan análisis ocupacionales mediante grupos de trabajo constituidos por personal de dirección, trabajadores, trabajadoras y especialistas en competencias. Estos análisis

ocupacionales se basan en algunas de las metodologías explicadas en el capítulo 2, donde se presentaban los modelos de competencia laborales más relevantes. En esta tesis, tal y como ya se ha expuesto, se utiliza la metodología del Análisis Funcional, sustituyendo el papel del grupo de trabajo por las medidas de seguridad del Anexo II del ENS. Se mantiene un equipo de trabajo, pero con una composición y propósito distintos, y como se explica a continuación, con tareas diferentes a las habituales.

El mapa funcional que se desarrolla en esta sección fue presentado en las Jornadas Nacionales de Investigación en Ciberseguridad organizadas por la Universidad de Castilla-La Mancha, en el año 2021, bajo el título "Mapa Funcional de competencias en seguridad para el personal no TI de las universidades españolas" (Mendívil et al., 2021).

Para llevar a cabo su construcción, las tareas que debe efectuar el panel de expertos y expertas son las siguientes:

- Transformar los textos de las medidas de seguridad del Anexo II del ENS a la estructura gramatical propuesta por la metodología del Análisis Funcional.
- Identificar las medidas de seguridad que no aplican al ámbito de estudio abordado.
- Señalar los elementos de competencia que permitan dar respuesta a las unidades de competencia identificadas.

En primer lugar, se adaptarán los textos del ENS adoptando la estructura gramatical propuesta en la metodología del Análisis Funcional explicada en el capítulo 3, comprobando que se cumple no sólo dicha estructura, sino que el resultado es el proceso de reflexión propuesto por la misma, esto es, que responde a la pregunta: *¿qué hay que hacer para lograr ese propósito?*.

Para realizar esta tarea, los investigadores se reúnen sucesivamente con cada uno de los expertos y expertas. La dinámica de trabajo es similar: comienza con una explicación de los motivos y objetivos del estudio. A continuación se les orienta en la metodología del Análisis Funcional y lo que se espera conseguir con su empleo. Confirmada su comprensión, se comienza definiendo el propósito principal del mapa funcional a partir de los objetivos del ENS. A continuación, se repite la misma mecánica con las funciones claves, identificadas

en la primera clasificación de las medidas de seguridad. El siguiente paso es repasar los diferentes aspectos que conforman las medidas de seguridad, ajustándolas a la sintaxis propia del Análisis Funcional, y de esta manera ir obteniendo las funciones principales, las unidades de competencia y los elementos de competencia. Este proceso se lleva a cabo en sucesivas reuniones de una hora de duración.

Realizado este proceso con el primer experto, y de acuerdo con la Teoría Fundamentada descrita en el capítulo 3, se repite la parte inicial de explicación y orientación con el segundo experto. En este caso se le muestran el propósito principal, las funciones clave, las funciones principales, las unidades de competencia y los elementos de competencia realizados por el primer entrevistado, para que corrija, elimine o añada lo que considere oportuno, incluyendo comentarios o aclaraciones. Para realizar esta tarea también se emplean varias reuniones. El resultado obtenido con esta segunda persona experta se presenta al primer experto para que corrobore o modifique sus propios resultados.

El equipo investigador, de forma iterativa, después de cada reunión analiza, clasifica y ordena los resultados obtenidos, agrupa coincidencias o señala errores, compartiendo todo ello con los expertos y expertas que hasta ese momento participan en la investigación.

La tercera persona recibe los resultados y aportaciones de los dos primeros expertos, incluyendo los cambios realizados y las correcciones. Ésta aporta su conocimiento para modificar o ratificar lo realizado hasta el momento, añadiendo a su vez las consideraciones que estima convenientes.

Con los siguientes expertos y expertas se sigue la misma dinámica de trabajo. En este caso, el cuarto entrevistado valida casi en su totalidad el mapa funcional obtenido y el quinto lo ratifica con pequeños ajustes, lo que indica que se ha alcanzado el estado de saturación teórica, concepto explicado en la página 92 de la esta tesis. El resultado final es enviado a todos los expertos y expertas para que aprueben los resultados obtenidos.

Detallando más la mecánica del proceso llevado a cabo, este comienza con la identificación del propósito principal. Este propósito define la meta, objetivo o finalidad de la actividad realizada. Para ello se utiliza como referencia la Disposición General I, que recoge la finalidad del ENS BOE (2010):

> La finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.
>
> El Esquema Nacional de Seguridad persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas.

El texto se adaptada a la estructura propuesta por el Análisis Funcional, de acuerdo con la idea de reflejar el propósito principal identificado por el equipo de expertos y expertas: la salvaguarda de los sistemas de información de las universidades españolas.

> **Propósito principal:**
>
> Garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, para permitir a los usuarios de la universidad el desarrollo de sus actividades a través de estos medios y fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas.

A continuación se organizan las medidas de seguridad recogidas en el ENS con la estructura de árbol característica de un mapa funcional, asociando cada nivel de agrupación del ENS con el correspondiente nivel de desagregación del mapa funcional. De esta manera se consiguen explicitar los primeros niveles del mapa funcional, correspondientes a las funciones clave, funciones principales y unidades de competencia.

Para llegar a este conocimiento, las cuestiones concretas que deberá resolver el panel de expertos y expertas para cada una de las medidas serán las siguientes:

- ¿Aplica esta medida para la mejora de la formación y concienciación en materia de seguridad de la información para el personal no TIC de las universidades españolas?
- Si aplica, ¿cuáles son las acciones concretas en formación y concienciación que deben llevarse a cabo para asegurar que el personal no TIC cumple en el ámbito de su responsabilidad con la medida de seguridad analizada?

El último paso es identificar los elementos de competencia, donde ya se establece lo que el trabajador o trabajadora debe conocer o ser capaz de hacer.

El resultado final de este proceso es el Mapa Funcional sobre la seguridad de la información del personal no TIC de las universidades españolas que se presenta a continuación. Este mapa se compone, sin considerar los items que no aplican, del propósito principal ya presentado, tres funciones clave, dieciocho funciones principales, cuarenta y nueve unidades de competencia y 110 elementos de competencia.

Algunas explicaciones y aclaraciones

Con el objeto de ayudar a la interpretación del mapa funcional se anotan algunas indicaciones de interés:

- Para conseguir una mejor compresión de la relación entre las medidas de seguridad del Anexo II y el mapa funcional, se mantiene una organización similar: las funciones clave derivan de la agrupación de las medidas de seguridad en sus tres apartados de marco organizativo, marco operacional y medidas de protección, y las funciones principales y unidades de competencias se corresponden con los correspondientes niveles de desglose en los que se organizan las medidas de seguridad.
- Relacionado con el punto anterior, y para facilitar la conexión entre los ítems del mapa funcional y las medidas de seguridad, se utilizan en el mapa funcional los identificadores del Anexo II.
- Las unidades de competencia de la primera función clave presentan la particularidad de coincidir con las funciones principales. Esto se debe a que esta unidad de competencia, que atiende a la organización global de la seguridad, no muestra un mayor nivel de desglose en el Anexo II.

- Se incluyen las unidades de competencia cuyos elementos de competencia “No Aplican”, es decir, con elementos de competencia que los expertos y expertas entienden que no forman parte de lo que los trabajadores y trabajadoras no TIC de las universidades españolas deben conocer o entender, anotando esta circunstancia como N.A..

Función clave: 3. Conocer el conjunto de medidas relacionadas con la organización global de la seguridad en la universidad		
Funciones principales	Unidades de competencia	Elementos de competencia
3.1. Documentar los objetivos de la organización, el marco legal y regulatorio en el que se desarrollarán las actividades, definir los roles de seguridad, la estructura del comité de seguridad, y la documentación de seguridad.	3.1.0. Documentar los objetivos de la organización, el marco legal y regulatorio en el que se desarrollarán las actividades, definir los roles de seguridad, la estructura del comité de seguridad, y la documentación de seguridad.	3.1.0.1. Conocer la política de seguridad de la universidad. 3.1.0.2. Conocer dónde puede consultarse la Política de seguridad de la universidad. 3.1.0.3. Entender la importancia, significado y objetivos de la política de seguridad. 3.1.0.4. Entender la necesidad de conocer las actualizaciones de la política de seguridad.
3.2. Disponer de documentación que describe el uso de equipos, servicios e instalaciones, lo que se considerará uso indebido y su responsabilidad con respecto al cumplimiento de las normas.	3.2.0. Disponer de documentación que describe el uso de equipos, servicios e instalaciones, lo que se considerará uso indebido y su responsabilidad con respecto al cumplimiento de las normas.	3.2.0.1. Conocer el uso correcto de los equipos, servicios e instalaciones que utilice en el desempeño de su labor. 3.2.0.2. Conocer qué se considera uso indebido de los equipos, servicios e instalaciones que utilice en el desempeño de su labor. 3.2.0.3. Conocer su responsabilidad con respecto al cumplimiento o violación de la política de seguridad: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente. 3.2.0.4. Entender la importancia y necesidad del conocimiento y cumplimiento de la normativa de seguridad de la universidad.

Función clave: 3. Conocer el conjunto de medidas relacionadas con la organización global de la seguridad en la universidad		
Funciones principales	Unidades de competencia	Elementos de competencia
3.3. Disponer de una serie de documentos que detallen cómo llevar a cabo las tareas habituales, quién debe hacer cada tarea y cómo identificar y reportar comportamientos anómalos.	3.3.0. Disponer de una serie de documentos que detallen cómo llevar a cabo las tareas habituales, quién debe hacer cada tarea y cómo identificar y reportar comportamientos anómalos.	3.3.0.1. Saber qué tareas en el ámbito de la seguridad debe realizar y cómo llevarlas a cabo en el desempeño de su labor.
		3.3.0.2. Conocer los procedimientos de seguridad relacionados con el desempeño de su actividad.
		3.3.0.3. Saber identificar y reportar comportamientos anómalos en el ámbito de la seguridad.
		3.3.0.4. Entender la importancia de conocer los procedimientos de seguridad en el desempeño de su actividad.
3.4. Establecer un proceso formal de autorizaciones que cubra todos los elementos del sistema de información.	3.4.0. Establecer un proceso formal de autorizaciones que cubra todos los elementos del sistema de información.	3.4.0.1. Conocer el funcionamiento de los procesos de autorización para el uso de los sistemas de información.
Función clave: 4. Proteger la operación del sistema como conjunto integral de componentes.		
4.1. Establecer una política de análisis de riesgos y arquitectura de seguridad.	4.1.1. Analizar los riesgos de la organización para identificar los activos más valiosos, las amenazas más probables, las salvaguardas que protegen de dichas amenazas, e identificar el riesgo residual.	4.1.1.1. Identificar y valorar cualitativamente los activos de información más valiosos de su entorno de trabajo.
		4.1.1.2. Conocer la valoración de los sistemas derivados del análisis de riesgos, y el nivel de riesgo asumido.

Función clave: 4. Proteger la operación del sistema como conjunto integral de componentes.		
Funciones principales	Unidades de competencia	Elementos de competencia
4.1. Establecer una política de análisis de riesgos y arquitectura de seguridad.	4.1.2. Identificar y detallar, para la categoría del sistema de información a proteger, la planificación, organización y control de los recursos relativos a la seguridad de la información	4.1.2.1. N.A. Medida de seguridad de TI
	4.1.3. Establecer un proceso formal para planificar la adquisición de nuevos componentes del sistema, para atender las conclusiones del análisis de riesgos, ser acorde a la arquitectura de seguridad escogida y contemplar las necesidades técnicas, de formación y de financiación de forma conjunta.	4.1.3.1. N.A. Medida de seguridad de TI
	4.1.4. Realizar un análisis previo que identifique las necesidades de procesamiento, de almacenamiento de información, de comunicación, de personal y de instalaciones y medios auxiliares.	4.1.4.1. N.A. Medida de seguridad de TI
	4.1.5. Utilizar sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.	4.1.5.1. N.A. Medida de seguridad de TI

Función clave: 4. Proteger la operación del sistema como conjunto integral de componentes.		
Funciones principales	Unidades de competencia	Elementos de competencia
4.2. Identificar el conjunto de actividades preparatorias y ejecutivas para que una determinada entidad, usuario o proceso, pueda, o no, acceder a un recurso del sistema para realizar una determinada acción.	4.2.1. Identificar a los usuarios y roles que acceden al sistema de información con un identificador singular para cada rol que pudieran tener, de forma que siempre queden delimitados y conocidos sus privilegios y sus registros de actividad.	4.2.1.1. Utilizar el identificador adecuado para acceder al sistema en el caso de disponer de diferentes roles de forma que siempre queden delimitados privilegios y registros de actividad.
		4.2.1.2. Entender que se guardará la información de cuándo accede y qué actividad realiza.
		4.2.1.3. Entender la importancia de utilizar el identificador adecuado.
	4.2.2. Establecer requisitos de acceso que permitan proteger los recursos del sistema impidiendo su utilización, salvo a las personas o procesos que disfruten de derechos de acceso suficientes.	4.2.2.1. Conocer las políticas de establecimiento de derechos de acceso a los recursos de su responsabilidad, ateniéndose a la normativa de seguridad.
		4.2.2.2. Entender la importancia de gestionar los derechos de acceso a los recursos de su responsabilidad, especialmente en los casos de actualización o bajas.
	4.2.3. Organizar el sistema de control de acceso de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas.	4.2.3.1. N.A. Medida de seguridad de TI y/o dirección

Función clave: 4. Proteger la operación del sistema como conjunto integral de componentes.		
Funciones principales	Unidades de competencia	Elementos de competencia
4.2. Identificar el conjunto de actividades preparatorias y ejecutivas para que una determinada entidad, usuario o proceso, pueda, o no, acceder a un recurso del sistema para realizar una determinada acción.	4.2.4. Limitar los derechos de acceso de cada usuario atendiendo a los principios de mínimo privilegio, necesidad de conocer y capacidad de autorizar.	4.2.4.1. Comprender que los derechos de acceso se limitan atendiendo a los principios de mínimo privilegio y necesidad de conocer.
		4.2.4.2. Conocer las políticas y procedimientos para conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable.
	4.2.5. Utilizar mecanismos de autenticación que se adecúen al nivel del sistema, empleando para ello contraseñas o claves concertadas, componentes lógicos, dispositivos físicos o elementos biométricos.	4.2.5.1. Entender que sus credenciales de acceso a los sistemas estarán bajo su responsabilidad y control exclusivo.
		4.2.5.2. Conocer las obligaciones que implica la tenencia de credenciales de acceso, en particular, el deber de custodia diligente, protección de su confidencialidad y notificación inmediata en caso de pérdida.
		4.2.5.3. Conocer la política de credenciales y el procedimiento de cambio de credenciales.
	4.2.6. Acceder de manera controlada a los puestos de trabajo dentro de las propias instalaciones de la organización de acuerdo con el nivel de las dimensiones de seguridad.	4.2.6.1. Entender la necesidad de cumplir la información que suministre el sistema respecto a sus obligaciones una vez que se ha obtenido el acceso.
		4.2.6.2. Entender la necesidad de comprobar la información que suministre el sistema respecto a su último acceso efectuado con su identidad.
		4.2.6.3. Entender la necesidad de no compartir sus credenciales de acceso.

Función clave: 4. Proteger la operación del sistema como conjunto integral de componentes.		
Funciones principales	Unidades de competencia	Elementos de competencia
4.2. Identificar el conjunto de actividades preparatorias y ejecutivas para que una determinada entidad, usuario o proceso, pueda, o no, acceder a un recurso del sistema para realizar una determinada acción.	4.2.6. Acceder de manera controlada a los puestos de trabajo dentro de las propias instalaciones de la organización de acuerdo con el nivel de las dimensiones de seguridad.	4.2.6.4. No guardar en formato legible las credenciales de acceso.
		4.2.6.5. Entender la importancia de no guardar en formato legible las credenciales de acceso.
	4.2.7. Acceder de manera controlada a los puestos de trabajo desde fuera de las propias instalaciones de la organización, a través de redes de terceros.	4.2.7.1. Conocer las políticas y procedimientos de acceso remoto a los sistemas.
		4.2.7.2. No guardar en los equipos las credenciales de acceso remoto.
		4.2.7.3. Conocer y aplicar las buenas prácticas de acceso remoto.
		4.2.7.4. Entender que es necesario aplicar los mismos principios de seguridad que rigen para un acceso local.
4.3. Identificar en las tareas de explotación los requisitos de seguridad a aplicar.	4.3.1. Mantener un inventario de los elementos del sistema, detallando su naturaleza e identificando a la persona que es responsable de las decisiones relativas al mismo.	4.3.1.1. Entender la necesidad de conocer y proteger los activos de información de los que es responsable.
		4.3.1.2. Comprender la importancia de comunicar la existencia de un equipo no inventariado.
	4.3.2. Configurar los equipos previamente a su entrada en operación, de forma que se retiren cuentas y contraseñas estándar, se aplique la regla de "mínima funcionalidad" y la regla de "seguridad por defecto".	4.3.2.1. Entender la necesidad de configurar los equipos bajo las reglas de "mínima funcionalidad" y "seguridad por defecto".
	4.3.3. Gestionar de manera continua la configuración de los componentes del sistema de manera que se mantenga en todo momento las reglas de "funcionalidad mínima" y "seguridad por defecto", el sistema se adapte a nuevas necesidades previamente autorizadas, y reaccione a vulnerabilidades reportadas e incidentes.	4.3.3.1. Entender la necesidad de gestionar la configuración de componentes bajo las reglas de "mínima funcionalidad" y "seguridad por defecto".

Función clave: 4. Proteger la operación del sistema como conjunto integral de componentes.		
Funciones principales	Unidades de competencia	Elementos de competencia
4.3. Identificar en las tareas de explotación los requisitos de seguridad a aplicar.	4.3.4. Mantener el equipamiento físico y lógico que constituye el sistema	4.3.4.1. Atender las especificaciones de los fabricantes en lo relativo al buen uso y mantenimiento de los equipos que utilice en el desempeño de sus tareas.
		4.3.4.2. Aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones en los equipos que proceda hacerlo.
	4.3.5. Mantener un control continuo de cambios realizados en el sistema.	4.3.5.1. N.A. Medida de seguridad de TI
	4.3.6. Disponer de mecanismos de prevención y reacción frente a código dañino.	4.3.6.1. Evitar el malware mediante un uso cuidadoso y atento de los sistemas.
		4.3.6.2. Comprender la necesidad de utilizar el antivirus y herramientas de protección
	4.3.7. Disponer de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema.	4.3.7.1. Conocer el procedimiento de reporte de incidentes reales o sospechosos.
		4.3.7.2. Comprender la importancia y necesidad de utilizar el procedimiento de gestión de incidentes.
	4.3.8. Registrar las actividades de los usuarios en el sistema, de forma que se recoja quién realiza la actividad, cuándo la realiza y sobre qué información.	4.3.8.1. Entender que se registrará su actividad, cuándo la realiza, sobre qué información, y los motivos de hacerlo.
	4.3.9. Registrar todas las actuaciones relacionadas con la gestión de incidentes, de forma que se anoten el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.	4.3.9.1. N.A. Medida de seguridad de TI.
	4.3.10. Proteger los registros del sistema, de forma que se determine su periodo de retención, se asegure su fecha y hora y que no puedan ser modificados ni eliminados por personal no autorizado.	4.3.10.1. N.A. Medida de seguridad de TI

Función clave: 4. Proteger la operación del sistema como conjunto integral de componentes.		
Funciones principales	Unidades de competencia	Elementos de competencia
4.3. Identificar en las tareas de explotación los requisitos de seguridad a aplicar.	4.3.11. Proteger las claves criptográficas durante todo su ciclo de vida: generación, transporte al punto de explotación, custodia durante la explotación, archivo a su retirada de explotación y destrucción final.	4.3.11.1. Conocer cómo proteger los certificados de los equipos vinculados a su uso.
		4.3.11.2. Entender la importancia de proteger los certificados y los equipos asociados a su uso.
4.4. Establecer las limitaciones y requerimientos de seguridad de los servicios externos.	4.4.1. Establecer contractualmente las características de los servicios prestados y las responsabilidades de las partes, detallando lo que se considera calidad mínima del servicio prestado y las consecuencias de su incumplimiento.	4.4.1.1. Conocer los SLA que le afectan, las características del servicio prestado y las responsabilidades de las partes.
		4.4.1.2. Entender la necesidad de participar activamente en el ciclo de vida de los SLA y en el seguimiento de su cumplimiento.
	4.4.2. Establecer un sistema para medir el cumplimiento y la neutralización de cualquier desviación, el mecanismo de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas, y procedimientos de coordinación en caso de incidentes y desastres.	4.4.2.1. Conocer el sistema rutinario para medir el cumplimiento de las obligaciones de servicio.
		4.4.2.2. Conocer los procedimientos de coordinación en caso de incidentes y desastres en los servicios.

Función clave: 4. Proteger la operación del sistema como conjunto integral de componentes.		
Funciones principales	Unidades de competencia	Elementos de competencia
4.4. Establecer las limitaciones y requerimientos de seguridad de los servicios externos.	4.4.3. Prever la provisión del servicio por medios alternativos en caso de indisponibilidad del servicio contratado.	4.4.3.1. N.A. Medida destinada a proveedores.
4.5. Analizar el impacto de las interrupciones en los servicios, establecer un plan de continuidad, así como pruebas periódicas para asegurar la continuidad de los servicios.	4.5.1. Realizar análisis de impacto que permita determinar los requisitos de disponibilidad de cada servicio y los elementos que son críticos para la prestación de cada servicio.	4.5.1.1. Conocer los requisitos de disponibilidad de los servicios que sea responsable.
		4.5.1.2. Conocer los elementos que son críticos para la prestación de los servicios que sea responsable.
		4.5.1.3. Comprender la importancia de colaborar en la realización de un correcto análisis de impacto.
	4.5.2. Desarrollar un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales.	4.5.2.1. Conocer las funciones, responsabilidades y actividades a realizar en un plan de continuidad.
		4.5.2.2. Conocer los medios alternativos que se utilizarán para mantener el servicio.
	4.5.3. Realizar pruebas periódicas para localizar y, corregir en su caso, los errores o deficiencias que puedan existir en el plan de continuidad.	4.5.3.1. Entender la necesidad de hacer pruebas periódicas del plan de continuidad y colaborar activamente.
4.6. Identificar las medidas de monitorización a las que estará sujeta la actividad de los sistemas.	4.6.1. Disponer de herramientas de detección o de prevención de intrusión.	4.6.1.1. N.A. Medida de seguridad de TI
	4.6.2. Recopilar los datos necesarios atendiendo a la categoría del sistema para conocer el grado de implantación de las medidas de seguridad que apliquen de las detalladas en el Anexo II del ENS	4.6.2.1. N.A. Medida de seguridad de TI

Función clave: 5. Proteger los activos de la universidad, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.		
Funciones principales	Unidades de competencia	Elementos de competencia
5.1. Proteger las instalaciones e infraestructuras que soporten o alojen activos de información.	5.1.1. Controlar los accesos a las áreas indicadas de forma que sólo se pueda acceder por las entradas previstas y vigiladas.	5.1.1.1. Entender que no puede acceder a locales a los que no está autorizado, ni solicitar credenciales de acceso de manera no autorizada.
	5.1.2. Identificar y registrar las entradas y salidas de todas las personas que accedan a los locales donde hay equipamiento que forme parte del sistema de información.	5.1.2.1. Entender la necesidad de identificarse cuando se acceda a los locales donde hay equipamiento que forme parte del sistema de información.
		5.1.2.2. Saber que las entradas y salidas de locales donde hay equipamiento que forme parte del sistema de información quedarán registradas.
	5.1.3. Disponer de elementos adecuados para el eficaz funcionamiento del equipamiento en los locales donde se ubiquen los sistemas de información y sus componentes.	5.1.3.1. N.A. Medida de seguridad de TI.
	5.1.4. Disponer de energía eléctrica y sus tomas correspondientes, necesaria para el eficaz funcionamiento del equipamiento en los locales donde se ubiquen los sistemas de información y sus componentes, así como garantizar el suministro eléctrico a los sistemas en caso de fallo del suministro general.	5.1.4.1. N.A. Medida de seguridad de TI
	5.1.5. Proteger frente a incendios fortuitos o deliberados los locales donde se ubiquen los sistemas de información y sus componentes.	5.1.5.1. N.A. Medida de seguridad de TI.
	5.1.6. Proteger frente a incidentes fortuitos o deliberados causados por el agua los locales donde se ubiquen los sistemas de información y sus componentes.	5.1.6.1. N.A. Medida de seguridad de TI.

Función clave: 5. Proteger los activos de la universidad, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.		
Funciones principales	Unidades de competencia	Elementos de competencia
5.1. Proteger las instalaciones e infraestructuras que soporten o alojen activos de información.	5.1.7. Llevar un registro pormenorizado de toda entrada y salida de equipamiento, incluyendo la identificación de la persona que autoriza el movimiento.	5.1.7.1. N.A. Medida de seguridad de TI
	5.1.8. Garantizar la existencia y disponibilidad de instalaciones alternativas para poder trabajar en caso de que las instalaciones habituales no estén disponibles.	5.1.8.1. Conocer la ubicación y la forma de acceso a las instalaciones alternativas para poder trabajar en caso de que las instalaciones habituales no estén disponibles, así como el procedimiento y condiciones de cambio de ubicación.
5.2. Caracterizar los puestos de trabajo en base a responsabilidades y requisitos en materia de seguridad.	5.2.1. Definir las responsabilidades relacionadas en cada puesto de trabajo en materia de seguridad.	5.2.1.1. Conocer las responsabilidades relacionadas con su puesto de trabajo en materia de seguridad.
	5.2.2. Conocer los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.	5.2.2.1. Conocer las medidas disciplinarias en caso de incumplimiento de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.
		5.2.2.2. Conocer las obligaciones tanto durante el periodo de desempeño del puesto como en caso de término de la asignación o traslado a otro puesto de trabajo.
		5.2.2.3. Entender el deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que esté adscrito al puesto de trabajo, como posteriormente a su terminación.

Función clave: 5. Proteger los activos de la universidad, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.		
Funciones principales	Unidades de competencia	Elementos de competencia
5.2. Caracterizar los puestos de trabajo en base a responsabilidades y requisitos en materia de seguridad.	5.2.3. Concienciación	5.2.3.1. N.A.
	5.2.4. Formación	5.2.4.1. N.A.
	5.2.5. Garantizar la existencia y disponibilidad de otras personas que se puedan hacer cargo de las funciones en caso de indisponibilidad del personal habitual.	5.2.5.1. Entender la importancia de conocer la existencia y disponibilidad de personas que se puedan hacer cargo de las funciones en caso de indisponibilidad del personal habitual.
5.3. Proteger los equipos	5.3.1. Asegurar que el puesto de trabajo permanece despejado, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.	5.3.1.1. Entender la necesidad de que su puesto de trabajo permanezca despejado, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.
		5.3.1.2. Entender que el material deberá guardarse en lugar cerrado cuando no se esté utilizando.
	5.3.2. Bloquear al cabo de un tiempo prudencial de inactividad el puesto de trabajo, requiriendo una nueva autenticación para reanudar la actividad en curso.	5.3.2.1. Entender la necesidad de que el puesto de trabajo se bloquee al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación para reanudar la actividad en curso.
		5.3.2.2. Entender la necesidad de que, pasado un cierto tiempo sin utilizar, se cancelen las sesiones abiertas desde su puesto de trabajo.
	5.3.3. Proteger adecuadamente los equipos que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente.	5.3.3.1. Conocer el procedimiento para informar de la pérdida o sustracción de un portátil.

Función clave: 5. Proteger los activos de la universidad, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.		
Funciones principales	Unidades de competencia	Elementos de competencia
5.3. Proteger los equipos	5.3.3. Proteger adecuadamente los equipos que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente.	5.3.3.2. Entender la necesidad de proteger el portátil y la información que contiene, así como tenerlo en todo momento controlado y custodiado.
		5.3.3.3. Entender que cuando el equipo portátil se conecte remotamente a través de redes que no están bajo el estricto control de la universidad, no debe enviarse información confidencial o protegida.
		5.3.3.4. Entender que en el equipo portátil no deben almacenarse información o datos de carácter confidencial o protegido.
		5.3.3.5. Entender que en el equipo portátil no deben almacenarse claves de acceso de la universidad.
		5.3.3.6. En caso de almacenar información sensible en el equipo, conocer herramientas y técnicas de protección.
	5.3.4. Garantizar la existencia y disponibilidad de medios alternativos de tratamiento de la información para el caso de que fallen los medios habituales.	5.3.4.1. Conocer el procedimiento de acceso a medios alternativos de tratamiento de la información para el caso de que fallen los medios habituales.
5.4. Proteger las comunicaciones	5.4.1. Disponer de un sistema cortafuegos que separe la red interna del exterior.	5.4.1.1. N.A. Medida de seguridad de TI.
	5.4.2. Establecer mecanismos para proteger la confidencialidad de la información.	5.4.2.1. Conocer técnicas de navegación seguras aplicables.
		5.4.2.2. Entender la necesidad de utilizar técnicas de navegación seguras.

Función clave: 5. Proteger los activos de la universidad, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.		
Funciones principales	Unidades de competencia	Elementos de competencia
5.4. Proteger las comunicaciones	5.4.3. Asegurar la autenticidad del otro extremo de un canal de comunicación antes de intercambiar información alguna.	5.4.3.1. Conocer técnicas de navegación seguras aplicables.
		5.4.3.2. Entender la necesidad de utilizar técnicas de navegación seguras.
	5.4.4. Segmentar las redes para acotar el acceso a la información y, consiguientemente, la propagación de los incidentes de seguridad.	5.4.4.1. N.A. Medida de seguridad de TI
	5.4.5. Garantizar la existencia y disponibilidad de medios alternativos de comunicación para el caso de que fallen los medios habituales.	5.4.5.1. N.A. Medida de seguridad de TI
5.5. Proteger los soportes de información.	5.5.1. Entender el significado de las etiquetas de los soportes de información, bien mediante simple inspección, bien mediante el recurso a un repositorio que lo explique.	5.5.1.1. Conocer el significado de las etiquetas que indiquen el nivel de seguridad de la información, bien mediante simple inspección, bien mediante el recurso a un repositorio que lo explique.
		5.5.1.2. Conocer el tratamiento y gestión de la información en base a su nivel de seguridad.
		5.5.1.3. Entender la necesidad de clasificar y etiquetar la información respecto a su nivel de seguridad.
	5.5.2. Aplicar mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida.	5.5.2.1. Entender la necesidad de aplicar mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida en dispositivos removibles.
		5.5.2.2. Saber utilizar mecanismos criptográficos sobre dispositivos de almacenamiento móvil.

Función clave: 5. Proteger los activos de la universidad, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.		
Funciones principales	Unidades de competencia	Elementos de competencia
5.5. Proteger los soportes de información	5.5.3. Emplear el control de acceso y las exigencias de mantenimiento del fabricante de los soportes de información que permanecen bajo la responsabilidad de la organización.	5.5.3.1. Saber aplicar medidas físicas o lógicas para garantizar el control de acceso a los soportes de información bajo su responsabilidad.
		5.5.3.2. Entender la necesidad de respetar las exigencias de mantenimiento del fabricante de los soportes de información, en especial, en lo referente a temperatura, humedad y otros agresores medioambientales.
	5.5.4. Garantizar que los dispositivos permanecen bajo control y que satisfacen sus requisitos de seguridad mientras están siendo desplazados de un lugar a otro.	5.5.4.1. N.A. Medida de seguridad de TI
	5.5.5. Garantizar el borrado y destrucción de soportes de información susceptibles de almacenar información.	5.5.5.1. Saber borrar de manera segura los soportes de información que vayan a ser reutilizados para otra información o liberados.
		5.5.5.2. Entender la necesidad de realizar borrados seguros de soportes cuando vayan a ser reutilizados o liberados.
		5.5.5.3. Conocer el procedimiento de solicitud de destrucción de soportes de información.
5.6. Proteger las aplicaciones informáticas utilizadas por la organización.	5.6.1. Garantizar que el desarrollo de aplicaciones se realiza sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción.	5.6.1.1. N.A. Medida de seguridad de TI
	5.6.2. Comprobar el correcto funcionamiento de la aplicación antes de su puesta en producción.	5.6.2.1. Conocer los criterios de aceptación en materia de seguridad en caso de contratación externa.

Función clave: 5. Proteger los activos de la universidad, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.		
Funciones principales	Unidades de competencia	Elementos de competencia
5.7. Proteger la información de la organización.	5.7.1. Cumplir, cuando el sistema trate datos de carácter personal, lo dispuesto en las leyes vigentes	5.7.1.1. Saber cómo garantizar y proteger, en lo que concierne al tratamiento de los datos personales, los derechos de las personas físicas, y especialmente de su honor e intimidad personal y familiar.
		5.7.1.2. Entender la importancia de la protección de los datos personales y derechos digitales.
	5.7.2. Calificar, etiquetar y tratar la información en consideración al nivel de seguridad que requiere.	5.7.2.1. Conocer los criterios para asignar a cada información el nivel de seguridad requerido, y ser responsable de su documentación y aprobación formal.
		5.7.2.2. Conocer las políticas y procedimientos que describan en detalle la forma en la que se ha de etiquetar y tratar la información en consideración al nivel de seguridad que requiere; y precisando cómo se ha de realizar
		5.7.2.3. Entender que como responsable de información, en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad.
	5.7.3. Cifrar la información con un nivel alto en confidencialidad tanto durante su almacenamiento como durante su transmisión.	5.7.3.1. Entender que la información con un nivel alto de confidencialidad se cifrará tanto durante su almacenamiento como durante su transmisión. Sólo estará en claro mientras se está haciendo uso de ella.
	5.7.4. Emplear la firma electrónica para comprobar la autenticidad de la procedencia y la integridad de la información ofreciendo las bases para evitar el repudio.	5.7.4.1. Conocer las políticas, procedimientos y circunstancias de uso de la firma electrónica.

Función clave: 5. Proteger los activos de la universidad, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.		
Funciones principales	Unidades de competencia	Elementos de competencia
5.7. Proteger la información de la organización.	5.7.4. Emplear la firma electrónica para comprobar la autenticidad de la procedencia y la integridad de la información ofreciendo las bases para evitar el repudio.	5.7.4.2. Entender la importancia del buen uso y resguardo de la firma electrónica.
	5.7.5. Utilizar sellos de tiempo para prevenir la posibilidad de repudio.	5.7.5.1. N.A. Medida de seguridad de TI
	5.7.6. Retirar de los documentos toda la información adicional contenida en campos ocultos, metadatos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.	5.7.6.1. Conocer el uso de los metadatos en la documentación utilizada en su puesto de trabajo.
		5.7.6.2. Entender la necesidad de gestionar los metadatos de la documentación que se utilice o genere.
	5.7.7. Realizar copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente con una antigüedad determinada.	5.7.7.1. Conocer las políticas y procedimientos de realización de copias de seguridad en su entorno de trabajo.
		5.7.7.2. Entender la necesidad de realizar copias de seguridad de manera periódica, así como comprobar que han sido bien realizadas.
5.8. Proteger los servicios que se prestan a los usuarios de los sistemas.	5.8.1. Proteger frente a las amenazas que le son propias la información distribuida por medio de correo electrónico.	5.8.1.1. Proteger la información de los correos electrónicos, tanto en el cuerpo de los mensajes, como en los anexos.
		5.8.1.2. Proteger a la universidad frente a problemas que se materializan por medio del correo electrónico: spam...
		5.8.1.3. Conocer las normas de uso del correo electrónico.
		5.8.1.4. Entender la importancia de un uso cuidadoso del correo electrónico.

Función clave: 5. Proteger los activos de la universidad, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.		
Funciones principales	Unidades de competencia	Elementos de competencia
5.8. Proteger los servicios que se prestan a los usuarios de los sistemas.	5.8.2. Proteger frente a las amenazas que les son propias a los subsistemas dedicados a la publicación de información.	5.8.2.1. N.A. Medida de seguridad de TI
	5.8.3. Establecer medidas preventivas y reactivas frente a ataques de denegación de servicio.	5.8.3.1. N.A. Medida de seguridad de TI
	5.8.4. Garantizar la existencia y disponibilidad de medios alternativos para prestar los servicios en el caso de que fallen los medios habituales.	5.8.4.1. Conocer la existencia, circunstancias y procedimiento de uso medios alternativos para prestar los servicios en el caso de que fallen los medios habituales.
		5.8.4.2. Entender la importancia de conocer los procedimientos de uso de los medios alternativos.

5.3. Perfiles laborales

Obtenido el mapa funcional, la siguiente tarea es elaborar la relación de perfiles laborales existentes en las universidades españolas. Para ello, el equipo investigador parte en primer lugar de la Ley del Estatuto Básico del Empleado Público (BOE, 2015c), donde se fijan los grupos profesionales del personal funcionario de carrera de acuerdo con la siguiente clasificación, basada en la titulación exigida para el acceso a los mismos:

- Grupo A. Dividido en dos subgrupos, A1 y A2. Para acceder a este grupo se exige estar en posesión del título universitario de Grado. El acceso a cada subgrupo estará en función del nivel de responsabilidad de las funciones a desempeñar y de las características de las pruebas de acceso.
- Grupo B. Para el acceso al Grupo B se debe acreditar el título de Técnico Superior.
- Grupo C. Dividido en dos Subgrupos, C1 y C2, según la titulación exigida para el ingreso.
    - C1. Título de Bachiller o Técnico.
    - C2. Título de Graduado en Educación Secundaria. Obligatoria.

También se emplea la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades (BOE, 2001). En su Capítulo I del Título III desglosa los órganos de gobierno y representación colegiados y unipersonales de las universidades públicas españolas.

- Colegiados:
    - Consejo Social
    - Consejo de Gobierno
    - Claustro Universitario
    - Juntas de Escuela y Facultad
    - Consejos de Departamento
- Unipersonales:
    - Rector o Rectora

    - Vicerrector o Vicerrectora
    - Secretario o Secretaria General
    - Gerente
    - Decano o Decana de Facultad
    - Director o Directora de Escuela
    - Director o Directora de Departamento o de Instituto Universitario de Investigación.

Respecto al personal docente e investigador, el Capítulo I del Título IX señala los siguientes perfiles:

- Ayudante
- Profesora o profesor Ayudante Doctor
- Profesora o profesor Contratado Doctor
- Profesora o profesor Asociado
- Profesora o profesor Visitante
- Profesora o profesor Emérito

Finalmente, también se consideran en este análisis el baremo aplicable al personal funcionario de las universidades. Este baremo se divide en treinta niveles, de acuerdo con la siguiente distribución.

- Grupo A.
    - Subgrupo A1. Rango de niveles entre el 20 y 30.
    - Subgrupo A2. Rango de niveles entre el 16 y 26.
- Grupo B. No procede.
- Grupo C.
    - Subgrupo C1. Rango de niveles entre el 11 y 22.

- Subgrupo C2. Rango de niveles entre el 9 y 18.

Como se puede observar, los niveles presentan un grado de yuxtaposición respecto a los rangos, lo que permite ajustar, de acuerdo con las características y necesidades de cada universidad, los perfiles resultantes.

Perfiles iniciales

De acuerdo con todo lo anterior, el equipo de trabajo comienza el proceso identificando los siguientes perfiles iniciales:

- Miembro del Consejo Social
- Miembro del Consejo de Gobierno
- Miembro del Claustro Universitario
- Miembro de las Juntas de Escuela y Facultad
- Miembro del Consejo de Departamento
- Rector o Rectora
- Vicerrector o Vicerrectora
- Secretario o Secretaria General
- Gerente
- Decano o Decana de Facultad
- Director o Directora de Escuela
- Director o Directora de Departamento o de Instituto Universitario de Investigación.
- Ayudante
- Profesora o profesor Ayudante Doctor
- Profesora o profesor Contratado Doctor
- Profesora o profesor Asociado
- Profesora o profesor Visitante

- Profesora o profesor Emérito
- Subgrupo A1. Rango de niveles entre el 20 y 30. Asociados a jefaturas.
- Resto de grupos y subgrupos. Hasta el nivel 22 aproximadamente.

A continuación se eliminan aquellos cargos colegiados para los que necesariamente también se ha de tener un perfil unipersonal, considerándose que los perfiles que deben aplicarse son los perfiles unipersonales. Los cargos colegiados a los que aplica este criterio son:

- Miembro del Consejo de Gobierno.
- Miembro del Claustro universitario.
- Miembro de las Juntas de Escuela y Facultad.
- Miembro del Consejo de Departamento.

Esta misma pauta se aplica a los cargos de Director o Directora de Departamento y de Institutos Universitarios de Investigación.

Finalizado el proceso de identificación y depuración, los perfiles resultantes finales son los siguientes:

- Miembro del Consejo Social
- Rector o Rectora
- Vicerrector o Vicerrectora
- Secretario o Secretaria General
- Gerente
- Decano o Decana de Facultad
- Director o Directora de Escuela
- Ayudante
- Profesora o profesor Ayudante Doctor
- Profesora o profesor Contratado Doctor

- Profesora o profesor Asociado
- Profesora o profesor Visitante
- Profesora o profesor Emérito
- Subgrupo A1. Rango de niveles entre el 20 y 30. Asociados a jefaturas.
- Resto de grupos y subgrupos. Hasta el nivel 22 aproximadamente.

Grupos y perfiles asociados

A continuación los expertos y expertas deciden agrupar perfiles cuyos requisitos de seguridad consideran semejantes y en consecuencia sus necesidades de formación y concienciación también lo sean. Dos son los motivos de llevar a cabo esta agrupación de perfiles. El primero de ellos es la conveniencia de contener dentro de un rango manejable los resultados que deben obtener los expertos y expertas en las siguientes etapas del trabajo. Hay que tener presente que se debe identificar para cada perfil laboral el nivel de formación o concienciación en cada competencia registrada, y asignarle un nivel de desempeño en el cumplimiento de dicha competencia. Si se quisiera dar respuesta a los quince perfiles identificados, teniendo presente que se han identificado 110 elementos de competencia, habría que analizar 1.650 ítems, lo que sobrepasa las posibilidades de este trabajo. El segundo motivo es la consideración de los expertos y expertas de que entre los perfiles que agrupan no existen diferencias apreciables ni significativas en su actividad y exposición al riesgo que justifique abordar su nivel de formación y concienciación de manera diferenciada.

Finalmente, también es conveniente señalar la flexibilidad del modelo, que no impide que en su empleo por una universidad concreta, esta no pueda, de acuerdo con sus características y necesidades específicas, incluir nuevos perfiles o grupos de perfiles o modificar los establecidos en esta tesis.

Los perfiles finalmente definidos son los siguientes:

1. Personal Docente e Investigador, PDI
2. Jefatura de Personal de Administración y Servicios, PAS
3. Puesto Base PAS

4. Consejeras y consejeros externos
5. Dirección

Cada uno de estos grupos incluyen los siguientes perfiles:

1. Personal Docente e Investigador - PDI
    - Ayudante
    - Profesor o profesora Ayudante Doctor
    - Profesor o profesora Contratado Doctor
    - Profesor o profesora Asociado
    - Profesor o profesora Visitante
    - Profesor o profesora Emérito
2. Jefatura PAS
    - Subgrupo A1. Rango de niveles entre el 20 y 30. Asociados a jefaturas.
3. Puesto Base PAS
    - Resto de grupos y subgrupos. Hasta el nivel 22. No asociados a jefaturas.
4. Consejeras y Consejeros externos
    - Miembro del Consejo Social
5. Dirección
    - Rector o Rectora
    - Vicerrector o Vicerrectora
    - Secretario o Secretaria General
    - Gerente
    - Decano o Decana de Facultad
    - Director o Directora de Escuela

Una mención especial merece el grupo "Personal Docente e Investigador - PDI". El grupo de expertos y expertas barajó la opción de separar el perfil de profesor o profesora del perfil investigador. Sin embargo, finalmente optó por mantenerlos unidos. Dos fueron los motivos de esta decisión. En primer lugar, en general son dos perfiles muy relacionados, ya que prácticamente todo el profesorado realiza labores de investigación. En segundo lugar, el nivel de exposición al riesgo del profesorado, que trabaja de manera habitual con recursos TIC, se considera, desde el punto de vista de la seguridad, semejante al nivel de riesgo de un investigador o investigadora.

5.4. Niveles de desempeño

En el capítulo 4 se explicó la importancia de las métricas como componentes necesarios para conocer y evaluar el proceso de adquisición de competencias por parte del personal, comprobar la efectividad de las actividades de formación y concienciación llevadas a cabo y explicitar el nivel objetivo deseado de desarrollo de cada competencia.

Identificados los perfiles laborales que emplea el mapa de competencias, y de acuerdo con la conveniencia de establecer métricas que ayuden a la gestión de las competencias definidas, la siguiente fase aborda la elaboración de una escala que defina los niveles de desempeño que deben alcanzar las competencias atendiendo a las necesidades de cada perfil laboral. Hay que tener presente que no todos los perfiles desarrollan las competencias a un mismo nivel, y por ello es necesario estimar ese valor.

Existen varias escalas para evaluar el desempeño laboral, como la escala de Likert, que mide el nivel de acuerdo o desacuerdo con una afirmación, o la escala semántica diferencial, en la que se utilizan dos alternativas y el evaluador debe seleccionar un punto entre ambas (Taherdoost, 2019). En este caso, atendiendo a los criterios ya mencionados de que una métrica debe ser sencilla de obtener, cuantificable, repetible y comparable, se establece una escala numérica que identifica los distintos niveles de desempeño que cada perfil laboral debe alcanzar en cada competencia, de acuerdo con la información que se recoge en la tabla 5.1:

Id	Nivel	Descripción
0	No aplica	No es necesario ningún conocimiento. Son temas propios del departamento de TI o de gerencia.
1	Bajo	Conocimiento muy general del contenido y de la necesidad de su aplicación.
2	Medio	Conocimiento general, sin necesidad de conocer su aplicación concreta o funcionamiento. Debe conocer en qué circunstancias podría aplicarse y cómo y dónde conseguir más información si fuera necesario.
3	Alto	Conocimiento completo, adecuada y correcta aplicación y comprensión plena de su necesidad.

Tabla 5.1: Niveles de conocimiento y concienciación

5.5. Mapa de competencias

Desarrollado el mapa funcional que recoge las competencias asociadas a las funciones laborales obtenidas de las medidas de seguridad del Anexo II del ENS, establecidos los perfiles laborales y identificados los niveles de desempeño, la última fase de este trabajo es determinar para cada perfil los niveles de desempeño específicos que debe alcanzar en las competencias que le son propias, conformando con ello el mapa de competencias.

Concretando la tarea a realizar, dado que el número de elementos de competencia obtenidos en el mapa de competencias que aplican es de 110, y cinco son los perfiles definidos, los expertos y expertas deben dar una respuesta consensuada a 550 ítems. Para alcanzar este objetivo, se lleva a cabo un proceso iterativo que consta de las siguientes fases:

Reuniones iniciales y cuestionario

Se realiza una primera reunión para explicar el plan de trabajo, su propósito, así como para resolver posibles dudas. También se entrega y explica a cada experto y experta una hoja de cálculo en la que deben anotar los niveles de desempeño para cada perfil y competencia.

El resultado de esta primera fase se muestra en el Anexo E, donde se recogen las respuestas de los expertos y expertas para cada uno de los 550 ítems sujetos al análisis. En la tabla se incluye una columna denominada “Nivel” donde se anota en la correspondiente celda el valor con el que se ha alcanzado unanimidad en la respuesta. En caso contrario, la celda permanece en blanco. Los resultados sobre el nivel de coincidencia obtenido se presentan

en la tabla 5.2.

Respuestas	Número	Porcentaje
Coincidentes	273	49,64 %
Distintos	277	50,36 %
Total	550	100 %

Tabla 5.2: Respuestas iniciales coincidentes

La distribución de las respuestas de los expertos y expertas distribuidos por nivel de desempeño se presenta en la tabla 5.3, mientras que la tabla 5.4 refleja los mismos valores expresados en porcentaje.

Nivel	Experto/a 1	Experto/a 2	Experto/a 3	Experto/a 4	Experto/a 5
No Aplica	15	27	21	6	25
Bajo	66	40	69	55	37
Medio	116	125	119	77	60
Alto	353	358	341	412	428

Tabla 5.3: Respuestas iniciales

Nivel	Experto/a 1	Experto/a 2	Experto/a 3	Experto/a 4	Experto/a 5	Promedio
No Aplica	2,73 %	4,91 %	3,82 %	1,09 %	4,55 %	3,42 %
Bajo	12,00 %	7,27 %	12,55 %	10,00 %	6,73 %	9,71 %
Medio	21,09 %	22,73 %	21,64 %	14,00 %	10,91 %	18,07 %
Alto	64,18 %	65,09 %	62,00 %	74,91 %	77,82 %	68,80 %

Tabla 5.4: Respuestas iniciales en porcentaje

Resulta relevante para los objetivos de esta tesis comprobar que en las respuestas iniciales ya se obtiene una coincidencia entre los cinco expertos y expertas de casi el 50 %.

Primera iteración

Con el objetivo de alcanzar de manera progresiva la unanimidad en las respuestas, el equipo de trabajo establece de manera consensuada un primer patrón de ajuste: en todos aquellos ítems que tengan la misma respuesta por parte de cuatro de los cinco expertos y expertas se ajustará la respuesta diferente al valor mayoritario. Para evaluar la conveniencia de este ajuste en cada ítem concreto, cada experto y experta recibe un documento con todos los ítems que le afectan, indicando para cada uno de ellos el valor inicial y el valor final. Analizan los resultados, pudiendo aceptar o rechazar el nuevo valor. De no aceptarlo,

deben justificar en el mismo documento compartido el porqué de su decisión, quedando esa respuesta pendiente para una revisión posterior. También es posible señalar propuestas de cambio sobre otras respuestas, como resultado de los ajustes que se realicen en los ítems analizados.

Los expertos y expertas analizan los resultados obtenidos, confirmando la oportunidad de los ajustes, no produciéndose en consecuencia ningún cambio respecto a los valores resultantes de aplicar el patrón. Las respuestas de los expertos y expertas se presentan en el Anexo F. Los niveles de coincidencia obtenidos tras la primera iteración se muestran en la tabla 5.5, donde se puede comprobar que se han consensuado 138 ítems, prácticamente el 75 % del total.

Respuestas	Número	Porcentaje
Coincidentes	411	74,73 %
Distintos	139	25,27 %
Total	550	100 %

Tabla 5.5: Respuestas coincidentes tras la 1ª iteración

Segunda iteración

A continuación el grupo de trabajo analiza las pautas de respuesta existentes para establecer nuevos patrones de ajuste. El objetivo es mantener criterios homogéneos que permitan alcanzar resultados coherentes. Naturalmente, estos patrones no son más que un punto de partida para facilitar el inicio de la reflexión, siendo los criterios técnicos los que finalmente deciden la respuesta consensuada.

De acuerdo con este análisis, el grupo de trabajo decide establecer como patrón de ajuste para los ítems con tres respuestas iguales la elección del valor con mayor número de respuestas. También se acuerda hacer una excepción: cuando tres personas responden "Alto" y dos personas "Medio" no se aplica el patrón y se repasa el ítem. Respecto a los ítems con dos pares de respuestas iguales, el patrón es seleccionar el valor del par de respuestas iguales más próximo a la respuesta diferente. Si los pares de respuestas iguales no son adyacentes, como orientación se analizan las respuestas de la misma unidad de competencia. En el caso de tres respuestas con valores diferentes, prima como respuesta

el valor repetido.

Al igual que en la iteración anterior, cada experto y experta recibe un documento con todas las respuestas que le afectan, indicando para cada una de ellas el valor inicial y el valor resultante de aplicar los patrones de ajuste. En caso de no aceptar algún valor, se deben argumentar los motivos, quedando la respuesta pendiente para una revisión común posterior. Al igual que en la iteracion anterior, si se considera que la modificación de alguna de las respuestas puede afectar a otra ya consensuada, se puede incluir en las respuestas a revisar. En esta iteración no se alcanza el consenso o se solicita una nueva revisión en diecinueve ítems. El resultado se muestra en el Anexo G.

Tercera iteración

En esta tercera y última iteración se repasan colectivamente sobre un documento compartido los ítems que los expertos y expertas consideran que deben ser nuevamente analizados, o en los que no se ha logrado alcanzar el consenso respecto al valor obtenido con los patrones empleados, valorando los argumentos. En cada caso el grupo debe llegar a un consenso. En el Anexo H se recogen los ítems afectados y los ajustes realizados.

Con estas últimas modificaciones se consigue alcanzar el objetivo inicial, un primer borrador del mapa de competencias laborales para el personal no TIC de las universidades españolas en el ámbito de la seguridad de la información.

5.5.1. Análisis de clústeres

Obtenida una primera versión consensuada de los niveles de formación y concienciación para cada perfil, el siguiente paso es comprobar si los expertos y expertas, a través del análisis de sus valoraciones, perciben la existencia real de los perfiles definidos, o por el contrario, de sus respuestas se puede deducir que no advierten diferencias entre algunos de ellos. Si esta hipótesis se cumple, el siguiente paso sería agrupar los perfiles considerados semejantes. Esto último permitiría obtener un mapa de competencias más ligero y por ello más fácilmente gestionable.

Para llevar a cabo esta labor, se realiza un análisis de clústeres o de conglomerados. Se trata de una técnica cuantitativa, exploratoria, no inferencial y descriptiva que permite obtener

clústeres a partir de los perfiles inicialmente identificados, en función de sus competencias y niveles de desempeño. De este modo se pueden encontrar asociaciones en los datos que no son evidentes a priori, y de este modo confirmar o mejorar la taxonomía obtenida (Gil, 2015).

Las acciones que se llevan a cabo para efectuar este análisis se resumen a continuación:

Seleccionar los perfiles

Deben seleccionarse aquellos perfiles que caractericen con claridad al objeto de estudio. En este caso, son los perfiles laborales utilizados en la investigación y ya presentadas en la página 145 de esta tesis.

- G1: PDI
- G2: Jefatura PAS
- G3: Puesto Base PAS
- G4: Consejeras y Consejeros externos
- G5: Dirección

Las variables a analizar serán los niveles de desempeño otorgados a cada uno de los ciento diez ítems que conforman el mapa de competencias.

Seleccionar la medida de distancia

La distancia expresa el grado de semejanza o disimilitud que existe entre dos perfiles. Para medir este grado de proximidad o distancia existen varios métodos (González y Díaz, 2013). En este trabajo se utiliza como coeficiente la suma de los valores absolutos de las diferencias entre los valores de las ciento diez variables analizadas. Siendo la distancia *d(A,B)* entre dos variables cualesquiera A y B de la población, definidas por los conjuntos de valores $a = (a_1, a_2, ..., a_n)$ y $b = (b_1, b_2, ..., b_n)$, donde se cumple que:

- $d(A, A) = 0$
- $d(A, B) \geq 0$
- $d(A, B) = d(B, A)$

la distancia se define como:

$$d(A, B) = \sum_{i=1}^{n} |a_i - b_i|$$

La ventaja de este método frente a otros es que sus resultados son intuitivos, donde una mayor distancia entre los perfiles laborales significa una mayor diferencia entre éstos. También resulta sencillo de aplicar y al mismo tiempo es un método eficaz y fiable para los objetivos que se persiguen.

Para llevar a cabo esta medida, se obtiene una matriz formada en sus filas por las ciento diez variables que conforman el mapa de competencias, y en sus columnas por la resta en valor absoluto de todos los pares de combinaciones de los cinco grupos de perfiles. Esta matriz se presenta en el Anexo I.

Obtener los clústeres y valorar el resultado

Para identificar los grupos de manera general se utilizan criterios teóricos propios de la investigación, apoyados en representaciones gráficas, denominadas dendrogramas, que facilitan la identificación de los grupos.

Para llevar a cabo esta identificación se ha utilizado R, un lenguaje de programación orientado al análisis estadístico. El Anexo J recoge el proceso llevado a cabo, partiendo de la matriz de coeficientes de distancia del Anexo F, hasta la obteneción del dendrograma que se muestra en la figura 5.1.

Para alcanzar la solución se corta el dendrograma por medio de una línea horizontal, tal y como se aprecia, a modo de ejemplo, en la figura 5.2. En este ejemplo, el corte identificado en la línea A obtiene dos clústeres, el primero formado por los roles “Jefatura PAS” (G2) y “Dirección” (G5), y el segundo por los roles “Consejeras y Consejeros externos” (G4), “ PDI” (G1) y “Puesto base PAS” (G3). La línea B origina tres clústeres: G2-G5, G1-G3 y G4. La línea C generaría cuatro clústeres, G2-G5, G4, G1 y G3. En los extremos inferior y superior del dendrograma, se obtienen tantos clústeres como perfiles, o un único clúster que agrupa a los cinco perfiles laborales.

Dado que el número de clústeres depende del lugar donde se establezca el corte en el dendrograma, la decisión que a continuación se debe tomar depende de las características,

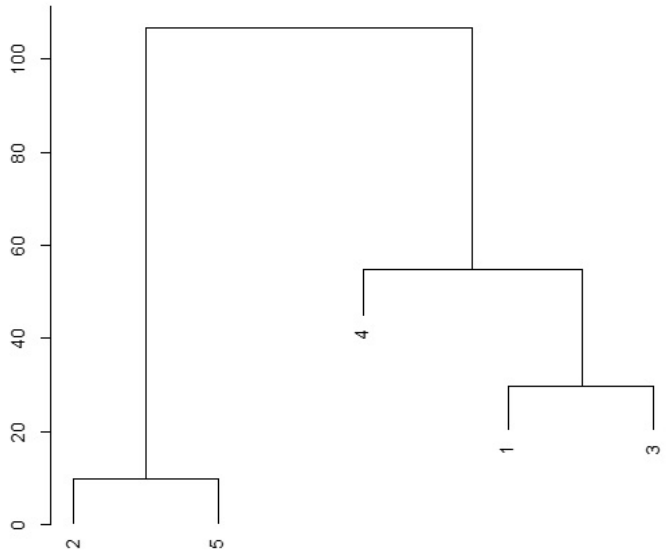

Figura 5.1: Clústeres de perfiles laborales
Fuente: Elaboración propia

criterios y objetivos del análisis que se esté realizando.

En el clúster G2-G5, cien de los 110 ítems presentan los mismos valores, lo que representa una coincidencia del 91 %. Analizando los perfiles que conforman este grupo, se aprecia que en efecto comparten características semejantes, asociadas a la jefatura y dirección en las universidades.

En el caso del clúster G1-G3, el nivel de coincidencia baja al 72,7 %. Treinta ítems presentan valores diferentes. También se considera que las características de ambos grupos presentan las suficientes diferencias como para descartar este clúster.

Finalmente, el grupo G4 presenta respecto a los grupos G1 y G3 cuarenta y seis y treinta seis valores diferentes, lo que supone un nivel de coincidencia del 58 % y del 67 % respectivamente. Además de estas diferencias, las características propias y diferenciadas de las Consejeras y Consejeros externos hacen oportuno mantener este grupo diferenciado del resto.

Como resultado del análisis efectuado, se establecen los siguientes grupos de perfiles laborales:

- Dirección

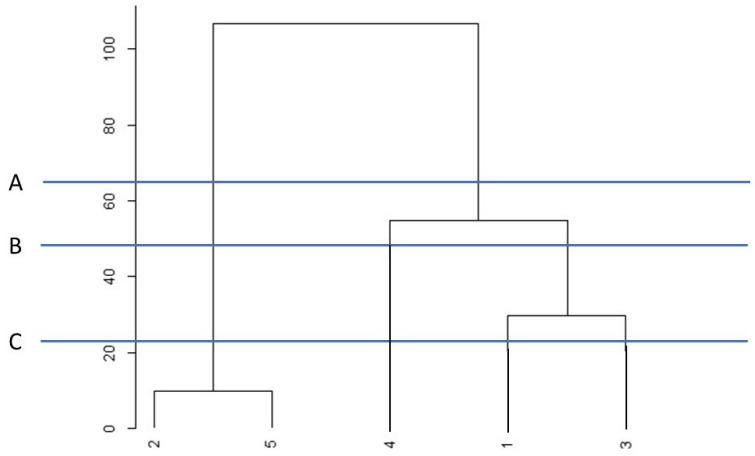

Figura 5.2: Selección de clústeres
Fuente: Elaboración propia

- Jefatura PAS
- Dirección

- Puesto Base PAS
- PDI
- Consejeras y Consejeros externos

Como paso final, es necesario unir los diez valores discordantes de los grupos "Jefatura PAS" (G2) y "Dirección" (G5). Para ello, el grupo de expertos y expertas decide mantener para cada ítem el valor más alto de los dos existentes. El resultado se muestra en el Anexo K.

5.5.2. Generación de un mapa común de competencias

Agrupados los perfiles percibidos como semejantes por los expertos y expertas, es necesario analizar a continuación si existen competencias que presenten el mismo nivel de desempeño para todos los perfiles laborales. Con este análisis se pretende identificar un conjunto común y básico de competencias que conformen el núcleo del mapa de competencias.

Analizando los datos, se constata que en efecto existen treinta y nueve competencias

que presentan el mismo nivel de desempeño. De ellas, treinta y cinco, es decir, el 89,7 % presentan un nivel de desempeño alto.

A la vista de estos datos, se organiza el mapa de competencias en dos grupos. El primero, denominado "Mapa común de competencias", está formado por las treinta y cinco competencias que presentan un nivel de desempeño "Alto" para todos los perfiles laborales. Estas competencias, que podemos identificar como básicas y esenciales, representan el 31,8 % del total de competencias. En el segundo grupo se encuentran tanto las competencias que presentan diferentes niveles de desempeño como las que mostrando un mismo nivel de desempeño, este no es de nivel alto.

Esta división se lleva a cabo con el objetivo de facilitar la elaboración de planes de formación y concienciación, ya que las competencias que conforman el mapa común de competencias pueden ser presentadas, explicadas y evaluadas para todo el personal, sin considerar los perfiles laborales, lo que permite optimizar recursos y esfuerzos.

5.5.3. Mapa común de competencias

En esta sección se presenta el mapa común de competencias para todo el personal no TIC de las universidades.

Antes de presentar el mapa de competencias conviene señalar que las explicaciones y aclaraciones que ayudaban a comprender e interpretar el mapa funcional siguen siendo válidas para el mapa de competencias.

Añadir que para cada perfil laboral se incluyen en cada competencia tanto el nivel de desempeño que se debe alcanzar como si este debe ser desarrollado mediante actividades de formación o de concienciación, un aspecto relevante, tal y como ya quedó explicado en el capítulo 2 al explicar las diferencias entre ambos conceptos.

Función clave: 3. Marco organizativo. Conocer el conjunto de medidas relacionadas con la organización global de la seguridad en la universidad.

Unidad de competencia: Normativa de seguridad		
3.2.0	Conocer el uso correcto de equipos, servicios e instalaciones, lo que se considerará uso indebido y su responsabilidad con respecto al cumplimiento o violación de las normas.	
Competencia profesional		
3.2.0.3	Formación	Conocer su responsabilidad con respecto al cumplimiento o violación de la política de seguridad: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

Función clave: 4. Proteger la operación del sistema como conjunto integral de componentes

Unidad de competencia: Identificación		
4.2.1	Identificar a los usuarios y roles que acceden al sistema de información con un identificador singular para cada rol que pudieran tener, de forma que siempre queden delimitados y conocidos sus privilegios y sus registros de actividad.	
Competencia profesional		
4.2.1.1	Formación	Utilizar el identificador adecuado para acceder al sistema en el caso de disponer de diferentes roles de forma que siempre queden delimitados privilegios y registros de actividad.
4.2.1.2	Concienciación	Entender que se guardará la información de cuándo accede y qué actividad realiza.
4.2.1.3	Concienciación	Entender la importancia de utilizar el identificador adecuado.

Unidad de competencia: Mecanismo de autenticación		
4.2.5	Utilizar mecanismos de autenticación que se adecúen al nivel del sistema, empleando para ello contraseñas o claves concertadas, componentes lógicos, dispositivos físicos o elementos biométricos.	
Competencia profesional		
4.2.5.1	Concienciación	Entender que sus credenciales de acceso a los sistemas estarán bajo su responsabilidad y control exclusivo.
4.2.5.2	Formación	Conocer las obligaciones que implica la tenencia de credenciales de acceso, en particular, el deber de custodia diligente, protección de su confidencialidad ey notificación inmediata en caso de pérdida.
4.2.5.3	Formación	Conocer la política de credenciales y el procedimiento de cambio de credenciales.

Unidad de competencia: Acceso local (local logon)		
4.2.6	Acceder de manera controlada a los puestos de trabajo dentro de las propias instalaciones de la organización de acuerdo con el nivel de las dimensiones de seguridad.	
Competencia profesional		
4.2.6.2	Concienciación	Entender la necesidad de comprobar la información que suministre el sistema respecto a su último acceso efectuado con su identidad.
4.2.6.3	Concienciación	Entender la necesidad de no compartir sus credenciales de acceso.
4.2.6.4	Formación	No guardar en formato legible las credenciales de acceso.
4.2.6.5	Concienciación	Entender la importancia de no guardar en formato legible las credenciales de acceso.

Unidad de competencia: Acceso remoto (remote login)		
4.2.7	Acceder de manera controlada a los puestos de trabajo desde fuera de las propias instalaciones de la organización, a través de redes de terceros.	
Competencia profesional		
4.2.7.2	Formación	No guardar en los equipos las credenciales de acceso remoto.

Unidad de competencia: Mantenimiento		
4.3.04	Mantener el equipamiento físico y lógico que constituye el sistema.	
Competencia profesional		
4.3.04.2	Formación	Aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones en los equipos que proceda hacerlo.

Unidad de competencia: Protección frente a código dañino		
4.3.06	Disponer de mecanismos de prevención y reacción frente a código dañino.	
Competencia profesional		
4.3.06.1	Formación	Evitar el malware mediante un uso cuidadoso y atento de los sistemas.
4.3.06.2	Concienciación	Comprender la necesidad de utilizar el antivirus y herramientas de protección

Unidad de competencia: Gestión de incidentes		
4.3.07	Disponer de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema.	
Competencia profesional		
4.3.07.1	Formación	Conocer el procedimiento de reporte de incidentes reales o sospechosos.

Unidad de competencia: Protección de claves criptográficas		
4.3.11	Proteger las claves criptográficas durante todo su ciclo de vida: generación, transporte al punto de explotación, custodia durante la explotación, archivo posterior a su retirada de explotación activa y destrucción final.	
Competencia profesional		
4.3.11.1	Formación	Conocer cómo proteger los certificados de los equipos vinculados a su uso.
4.3.11.2	Concienciación	Entender la importancia de proteger los certificados y los equipos asociados a su uso.

Función clave: 5. Proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad

Unidad de competencia: Identificación de las personas		
5.1.2	Identificar y registrar las entradas y salidas de todas las personas que accedan a los locales donde hay equipamiento que forme parte del sistema de información.	
Competencia profesional		
5.1.2.2	Formación	Saber que las entradas y salidas de locales donde hay equipamiento que forme parte del sistema de información quedarán registradas.

Unidad de competencia: Puesto de trabajo		
5.2.1	Conocer las responsabilidades de su puesto de trabajo en materia de seguridad.	
Competencia profesional		
5.2.1.1	Formación	Conocer las responsabilidades relacionadas con su puesto de trabajo en materia de seguridad.

Unidad de competencia: Deberes y obligaciones		
5.2.2	Conocer los deberes y obligaciones de su puesto de trabajo en materia de seguridad.	
Competencia profesional		
5.2.2.2	Formación	Conocer las obligaciones tanto durante el periodo de desempeño del puesto como en caso de término de la asignación o traslado a otro puesto de trabajo.
5.2.2.3	Concienciación	Entender el deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que esté adscrito al puesto de trabajo, como posteriormente a su terminación.

Unidad de competencia: Protección de equipos portátiles		
5.3.3	Proteger adecuadamente los equipos que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente.	
Competencia profesional		
5.3.3.2	Concienciación	Entender la necesidad de proteger el portátil y la información que contiene, así como tenerlo en todo momento controlado y custodiado.
5.3.3.5	Concienciación	Entender que en el equipo portátil no deben almacenarse claves de acceso de la universidad.

Unidad de competencia: Protección de la confidencialidad		
5.4.2	Establecer mecanismos para proteger la confidencialidad de la información.	
Competencia profesional		
5.4.2.1	Formación	Conocer técnicas de navegación seguras.
5.4.2.2	Concienciación	Entender la necesidad de utilizar técnicas de navegación seguras.

Unidad de competencia: Protección de la autenticidad y de la integridad		
5.4.3	Asegurar la autenticidad del otro extremo de un canal de comunicación antes de intercambiar información alguna.	
Competencia profesional		
5.4.3.1	Formación	Conocer técnicas de navegación seguras.
5.4.3.2	Concienciación	Entender la necesidad de utilizar técnicas de navegación seguras.

Unidad de competencia: Criptografía		
5.5.2	Aplicar mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida.	
Competencia profesional		
5.5.2.1	Concienciación	Entender la necesidad de aplicar mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida en dispositivos removibles.
5.5.2.2	Formación	Saber utilizar mecanismos criptográficos sobre dispositivos de almacenamiento móvil.

Unidad de competencia: Datos de carácter personal		
5.7.1	Cumplir, cuando el sistema trate datos de carácter personal de lo dispuesto en las leyes Orgánica 15/1999, de 13 de diciembre, normas de desarrollo y medidas establecidas por este real decreto.	
Competencia profesional		
5.7.1.1	Formación	Saber cómo garantizar y proteger, en lo que concierne al tratamiento de los datos personales, los derechos de las personas físicas, y especialmente de su honor e intimidad personal y familiar.
5.7.1.2	Concienciación	Entender la importancia de la protección de los datos personales y derechos digitales.

Unidad de competencia: Protección del correo electrónico		
5.8.1	Proteger frente a las amenazas que le son propias la información distribuida por medio de correo electrónico.	
Competencia profesional		
5.8.1.2	Formación	Proteger a la universidad frente a problemas que se materializan por medio del correo electrónico: spam...
5.8.1.3	Formación	Conocer las normas de uso del correo electrónico.
5.8.1.4	Concienciación	Entender la importancia de un uso cuidadoso del correo electrónico.

5.5.4. Mapa de competencias por perfil laboral

En esta sección se presentan los mapas de competencias específicos para cada perfil laboral.

Perfil laboral: Dirección y jefaturas

Función clave: 3. Marco organizativo. Conocer el conjunto de medidas relacionadas con la organización global de la seguridad en la universidad.

Unidad de Competencia: Política de seguridad			
3.1.0	Conocer los objetivos de la organización, el marco legal y regulatorio en el que se desarrollarán las actividades, conocer los roles de seguridad, la estructura del comité de seguridad, y la documentación de seguridad.		
Competencia profesional			
3.1.0.1	Alto	Formación	Conocer la política de seguridad de la universidad.
3.1.0.2	Alto	Formación	Conocer dónde puede consultarse la política de seguridad de la universidad.
3.1.0.3	Alto	Concienciación	Entender la importancia, significado y objetivos de la política de seguridad.
3.1.0.4	Alto	Concienciación	Entender la necesidad de conocer las actualizaciones de la política de seguridad.

Unidad de Competencia: Normativa de seguridad			
3.2.0	Conocer los documentos que describen el uso correcto de equipos, servicios e instalaciones, lo que se considerará uso indebido y su responsabilidad con respecto al cumplimiento o violación de las normas.		
Competencia profesional			
3.2.0.1	Alto	Formación	Conocer el uso correcto de los equipos, servicios e instalaciones que utilice en el desempeño de su labor.
3.2.0.2	Alto	Formación	Conocer qué se considera uso indebido de los equipos, servicios e instalaciones que utilice en el desempeño de su labor.
3.2.0.4	Alto	Concienciación	Entender la importancia del cumplimiento de la normativa de seguridad de la universidad.

Unidad de Competencia: Procedimientos de seguridad			
3.3.0	Conocer los documentos que detallan cómo llevar a cabo las tareas habituales, quién debe hacer cada tarea y cómo identificar y reportar comportamientos anómalos.		
Competencia profesional			
3.3.0.1	Alto	Formación	Saber qué tareas en el ámbito de la seguridad de la información debe realizar en el desempeño de su labor.
3.3.0.2	Alto	Formación	Saber cómo llevar a cabo las tareas habituales en el ámbito de la seguridad de la información en el desempeño de su labor.
3.3.0.3	Alto	Formación	Saber identificar y reportar comportamientos anómalos en el ámbito de la seguridad.
3.3.0.4	Alto	Concienciación	Entender la importancia de conocer los procedimientos de seguridad en el desempeño de su actividad.

Unidad de Competencia: Proceso de autorización			
3.4.0	Establecer un proceso formal de autorizaciones que cubra todos los elementos del sistema de información.		
Competencia profesional			
3.4.0.1	Alto	Formación	Conocer el funcionamiento de los procesos de autorización para el uso de los sistemas de información.

Función clave: 4. Proteger la operación del sistema como conjunto integral de componentes

Unidad de Competencia: Análisis de riesgos			
4.1.1.	Analizar los riesgos de seguridad de la organización para identificar los activos más valiosos del sistema, las amenazas más probables, las salvaguardas que protegen de dichas amenazas, así como identificar y valorar el riesgo residual.		
Competencia profesional			
4.1.1.1	Alto	Formación	Identificar y valorar cualitativamente los activos de información más valiosos de su entorno de trabajo.
4.1.1.2	Alto	Formación	Conocer la valoración de los sistemas derivados del análisis de riesgos, y el nivel de riesgo asumido.

Unidad de Competencia: Requisitos de acceso			
4.2.2	Utilizar requisitos de acceso que permitan proteger los recursos del sistema impidiendo su utilización, salvo a las personas o procesos que disfruten de derechos de acceso suficientes.		
Competencia profesional			
4.2.2.1	Alto	Formación	Conocer las políticas y procedimiento de establecimiento de derechos de acceso a los recursos de su responsabilidad, ateniéndose a la política y normativa de seguridad del sistema.
4.2.2.2	Alto	Concienciación	Entender la importancia de gestionar los derechos de acceso a los recursos de su responsabilidad, especialmente en los casos de actualización o bajas.

Unidad de Competencia: Proceso de gestión de derechos de acceso			
4.2.4	Limitar los derechos de acceso de cada usuario atendiendo a los principios de mínimo privilegio, necesidad de conocer y capacidad de autorizar.		
Competencia profesional			
4.2.4.1	Alto	Concienciación	Comprender que los derechos de acceso se limitan atendiendo a los principios de mínimo privilegio y necesidad de conocer.
4.2.4.2	Alto	Formación	Conocer las políticas y procedimientos para conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable.

Unidad de Competencia: Acceso local (local logon)			
4.2.6	Acceder de manera controlada a los puestos de trabajo dentro de las propias instalaciones de la organización de acuerdo con el nivel de las dimensiones de seguridad.		
Competencia profesional			
4.2.6.1	Alto	Concienciación	Entender la necesidad de cumplir la información que suministre el sistema respecto a sus obligaciones una vez que se ha obtenido el acceso.

Unidad de Competencia: Acceso remoto (remote login)			
4.2.7	Acceder de manera controlada a los puestos de trabajo desde fuera de las propias instalaciones de la organización, a través de redes de terceros.		
Competencia profesional			
4.2.7.1	Alto	Formación	Conocer las políticas y procedimientos de acceso remoto a los sistemas.
4.2.7.3	Alto	Formación	Conocer y aplicar las buenas prácticas de acceso remoto.
4.2.7.4	Alto	Concienciación	Entender que es necesario aplicar los mismos principios de seguridad que rigen para un acceso local.

Unidad de Competencia: Inventario de activos			
4.3.01	Mantener un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a la persona que es responsable de las decisiones relativas al mismo.		
Competencia profesional			
4.3.01.1	Alto	Concienciación	Entender la necesidad de conocer y proteger los activos de información de los que es responsable.
4.3.01.2	Alto	Concienciación	Comprender la importancia de comunicar la existencia de un equipo no inventariado.

Unidad de Competencia: Configuración de seguridad			
4.3.02	Configurar los equipos previamente a su entrada en operación, de forma que se retiren cuentas y contraseñas estándar, se aplique la regla de "mínima funcionalidad" y la regla de "seguridad por defecto".		
Competencia profesional			
4.3.02.1	Alto	Concienciación	Entender la necesidad de configurar los equipos bajo las reglas de "mínima funcionalidad" y "seguridad por defecto".

Unidad de Competencia: Gestión de la configuración			
4.3.03	Gestionar de manera continua la configuración de los componentes del sistema de manera que se mantenga en todo momento las reglas de "funcionalidad mínima" y "seguridad por defecto", el sistema se adapte a nuevas necesidades previamente autorizadas, y reaccione a vulnerabilidades reportadas e incidentes.		
Competencia profesional			
4.3.03.1	Alto	Concienciación	Entender la necesidad de gestionar la configuración de los sistemas bajo las reglas de "mínima funcionalidad" y "seguridad por defecto"

Unidad de Competencia: Mantenimiento			
4.3.04	Mantener el equipamiento físico y lógico que constituye el sistema.		
Competencia profesional			
4.3.04.1	Medio	Formación	Atender las especificaciones de los fabricantes en lo relativo al buen uso y mantenimiento de los equipos que utilice en el desempeño de sus tareas.

Unidad de Competencia: Gestión de incidentes			
4.3.07	Disponer de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema.		
Competencia profesional			
4.3.07.2	Alto	Concienciación	Comprender la importancia de utilizar el procedimiento de gestión de incidentes

Unidad de Competencia: Registro de la actividad de los usuarios			
4.3.08	Registrar las actividades de los usuarios en el sistema, de forma que se recoja quién realiza la actividad, cuándo la realiza y sobre qué información.		
Competencia profesional			
4.3.08.1	Alto	Concienciación	Entender que se registrará su actividad, cuándo la realiza y sobre qué información.

Unidad de Competencia: Contratación y acuerdos de nivel de servicio			
4.4.1	Establecer contractualmente las características de los servicios prestados y las responsabilidades de las partes, detallando lo que se considera calidad mínima del servicio prestado y las consecuencias de su incumplimiento.		
Competencia profesional			
4.4.1.1	Alto	Formación	Conocer los SLA en los que le afecta, las características del servicio prestado y las responsabilidades de las partes.
4.4.1.2	Alto	Concienciación	Entender la necesidad de participar activamente en el ciclo de vida de los SLA y en el seguimiento de su cumplimiento.

Unidad de Competencia: Gestión diaria			
4.4.2	Establecer un sistema rutinario para medir el cumplimiento de las obligaciones de servicio y el procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado, el mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas afectados por el acuerdo, y el mecanismo y los procedimientos de coordinación en caso de incidentes y desastres.		
Competencia profesional			
4.4.2.1	Alto	Formación	Conocer el sistema rutinario para medir el cumplimiento de las obligaciones de servicio.
4.4.2.2	Alto	Formación	Conocer los procedimientos de coordinación en caso de incidentes y desastres en los servicios.

Unidad de Competencia: Análisis de impacto			
4.5.1	Realizar análisis de impacto que permita determinar los requisitos de disponibilidad de cada servicio y los elementos que son críticos para la prestación de cada servicio.		
Competencia profesional			
4.5.1.1	Alto	Formación	Conocer los requisitos de disponibilidad de los servicios que sea responsable.
4.5.1.2	Alto	Formación	Conocer los elementos que son críticos para la prestación de los servicios que sea responsable.
4.5.1.3	Alto	Concienciación	Comprender la importancia de colaborar en la realización de un correcto análisis de impacto.

Unidad de Competencia: Plan de continuidad			
4.5.2	Desarrollar un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales.		
Competencia profesional			
4.5.2.1	Alto	Formación	Conocer las funciones, responsabilidades y actividades a realizar en un plan de continuidad.
4.5.2.2	Alto	Formación	Conocer los medios alternativos que se utilizarán para mantener el servicio.

Unidad de Competencia: Pruebas periódicas			
4.5.3	Realizar pruebas periódicas para localizar y, corregir en su caso, los errores o deficiencias que puedan existir en el plan de continuidad.		
Competencia profesional			
4.5.3.1	Alto	Concienciación	Entender la necesidad de hacer pruebas periódicas del plan de continuidad y colaborar activamente.

Función clave: 5. Proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad

Unidad de Competencia: Áreas separadas y con control de acceso			
5.1.1	Controlar los accesos a las áreas indicadas de forma que sólo se pueda acceder por las entradas previstas y vigiladas.		
Competencia profesional			
5.1.1.1	Alto	Concienciación	Entender que no puede acceder a locales a los que no está autorizado, ni solicitar credenciales de acceso de manera no autorizada.

Unidad de Competencia: Identificación de las personas			
5.1.2	Identificar y registrar las entradas y salidas de todas las personas que accedan a los locales donde hay equipamiento que forme parte del sistema de información.		
Competencia profesional			
5.1.2.1	Alto	Concienciación	Entender la necesidad de identificarse cuando se acceda a los locales donde hay equipamiento que forme parte del sistema de información.

Unidad de Competencia: Instalaciones alternativas			
5.1.8	Garantizar la existencia y disponibilidad de instalaciones alternativas para poder trabajar en caso de que las instalaciones habituales no estén disponibles.		
Competencia profesional			
5.1.8.1	Medio	Formación	Conocer la ubicación y la forma de acceso a las instalaciones alternativas para poder trabajar en caso de que las instalaciones habituales no estén disponibles, así como el procedimiento y condiciones de cambio de ubicación.

Unidad de Competencia: Deberes y obligaciones			
5.2.2	Conocer los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.		
Competencia profesional			
5.2.2.1	Alto	Formación	Conocer las medidas disciplinarias en caso de incumplimiento de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.

Unidad de Competencia: Personal alternativo			
5.2.5	Garantizar la existencia y disponibilidad de otras personas que se puedan hacer cargo de las funciones en caso de indisponibilidad del personal habitual.		
Competencia profesional			
5.2.5.1	Alto	Concienciación	Entender la importancia de conocer la existencia y disponibilidad de personas que se puedan hacer cargo de las funciones en caso de indisponibilidad del personal habitual.

Unidad de Competencia: Puesto de trabajo despejado			
5.3.1	Asegurar que el puesto de trabajo permanece despejado, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.		
Competencia profesional			
5.3.1.1	Medio	Concienciación	Entender la necesidad de que su puesto de trabajo permanezca despejado, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.
5.3.1.2	Medio	Concienciación	Entender que el material se guardará en lugar cerrado cuando no se esté utilizando.

Unidad de Competencia: Bloqueo de puesto de trabajo			
5.3.2	Bloquear al cabo de un tiempo prudencial de inactividad el puesto de trabajo, requiriendo una nueva autenticación para reanudar la actividad en curso.		
Competencia profesional			
5.3.2.1	Alto	Concienciación	Entender la necesidad de que el puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación para reanudar la actividad en curso.
5.3.2.2	Medio	Concienciación	Entender la necesidad de que pasado un cierto tiempo sin utilizar, se cancelarán las sesiones abiertas desde su puesto de trabajo.

Unidad de Competencia: Protección de equipos portátiles			
5.3.3	Proteger adecuadamente los equipos que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente.		
Competencia profesional			
5.3.3.1	Medio	Formación	Conocer el procedimiento para informar de la pérdida o sustracción de un portátil
5.3.3.3	Alto	Concienciación	Entender que cuando el equipo portátil se conecte remotamente a través de redes que no están bajo el estricto control de la universidad, no debe enviarse información confidencial o protegida.
5.3.3.4	Alto	Concienciación	Entender que en el equipo portátil no deben almacenarse información o datos de carácter confidencial o protegido.
5.3.3.6	Alto	Formación	En caso de almacenar información sensible en el equipo, conocer herramientas y técnicas de protección.

Unidad de Competencia: Medios alternativos			
5.3.4	Garantizar la existencia y disponibilidad de medios alternativos de tratamiento de la información para el caso de que fallen los medios habituales.		
Competencia profesional			
5.3.4.1	Alto	Formación	Conocer el procedimiento de acceso a medios alternativos de tratamiento de la información para el caso de que fallen los medios habituales.

Unidad de Competencia: Etiquetado			
5.5.1	Entender el significado de las etiquetas de los soportes de información, bien mediante simple inspección, bien mediante el recurso a un repositorio que lo explique.		
Competencia profesional			
5.5.1.1	Alto	Formación	Conocer el significado de las etiquetas que indiquen el nivel de seguridad de la información, bien mediante simple inspección, bien mediante el recurso a un repositorio que lo explique.
5.5.1.2	Alto	Formación	Conocer el tratamiento y gestión de la información en base a su nivel de seguridad.
5.5.1.3	Alto	Concienciación	Entender la necesidad de clasificar y etiquetar la información respecto a su nivel de seguridad.

Unidad de Competencia: Custodia			
5.5.3	Emplear el control de acceso y las exigencias de mantenimiento del fabricante de los soportes de información que permanecen bajo la responsabilidad de la organización.		
Competencia profesional			
5.5.3.1	Alto	Formación	Saber aplicar medidas físicas o lógicas para garantizar el control de acceso a los soportes de información bajo su responsabilidad.
5.5.3.2	Medio	Concienciación	Entender las necesidad de respetar las exigencias de mantenimiento del fabricante de los soportes de información, en especial, en lo referente a temperatura, humedad y otros agresores medioambientales

Unidad de Competencia: Borrado y destrucción			
5.5.5	Garantizar el borrado y destrucción de soportes de información susceptibles de almacenar información.		
Competencia profesional			
5.5.5.1	Alto	Formación	Saber borrar de manera segura los soportes de información que vayan a ser reutilizados para otra información o liberados.
5.5.5.2	Alto	Concienciación	Entender la necesidad de realizar borrados seguros de soportes cuando vayan a ser reutilizados o liberados.
5.5.5.3	Alto	Formación	Conocer el procedimiento de solicitud de destrucción de soportes de información.

Unidad de Competencia: Aceptación y puesta en servicio			
5.6.2	Comprobar el correcto funcionamiento de la aplicación antes de su puesta en producción.		
Competencia profesional			
5.6.2.1	Medio	Formación	Conocer los criterios de aceptación en materia de seguridad en caso de contratación externa.

Unidad de Competencia: Calificación de la información			
5.7.2	Calificar, etiquetar y tratar la información en consideración al nivel de seguridad que requiere.		
Competencia profesional			
5.7.2.1	Alto	Formación	Conocer los criterios para asignar a cada información el nivel de seguridad requerido, y ser responsable de su documentación y aprobación formal.
5.7.2.2	Alto	Formación	Conocer las políticas y procedimientos que describan en detalle la forma en la que se ha de etiquetar y tratar la información en consideración al nivel de seguridad que requiere
5.7.2.3	Alto	Concienciación	Entender que como responsable de información, en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad.

Unidad de Competencia: Cifrado			
5.7.3	Cifrar la información con un nivel alto en confidencialidad tanto durante su almacenamiento como durante su transmisión.		
Competencia profesional			
5.7.3.1	Alto	Concienciación	Entender que la información con un nivel alto de confidencialidad se cifrará tanto durante su almacenamiento como durante su transmisión. Sólo estará en claro mientras se está haciendo uso de ella.

Unidad de Competencia: Firma electrónica			
5.7.4	Emplear la firma electrónica como un instrumento capaz de permitir la comprobación de la autenticidad de la procedencia y la integridad de la información ofreciendo las bases para evitar el repudio.		
Competencia profesional			
5.7.4.1	Alto	Formación	Conocer las políticas, procedimientos y circunstancias de uso de la firma electrónica.
5.7.4.2	Alto	Concienciación	Entender la importancia del buen uso y resguardo de la firma electrónica

Unidad de Competencia: Limpieza de documentos			
5.7.6	Retirar de los documentos toda la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.		
Competencia profesional			
5.7.6.1	Alto	Formación	Retirar de la documentación toda la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.
5.7.6.2	Medio	Concienciación	Entender la necesidad de gestionar los metadatos de la documentación que se utilice o genere.

Unidad de Competencia: Copias de seguridad (backup)			
5.7.7	Realizar copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente con una antigüedad determinada.		
Competencia profesional			
5.7.7.1	Alto	Formación	Conocer las políticas y procedimientos de realización de copias de seguridad en su entorno de trabajo.
5.7.7.2	Alto	Concienciación	Entender la necesidad de realizar copias de seguridad de manera periódica, así como comprobar que han sido bien realizadas.

Unidad de Competencia: Protección del correo electrónico			
5.8.1	Proteger frente a las amenazas que le son propias la información distribuida por medio de correo electrónico.		
Competencia profesional			
5.8.1.1	Alto	Formación	Proteger la información de los correos electrónicos, tanto en el cuerpo de los mensajes, como en los anexos.

Unidad de Competencia: Medios alternativos			
5.8.4	Garantizar la existencia y disponibilidad de medios alternativos para prestar los servicios en el caso de que fallen los medios habituales.		
Competencia profesional			
5.8.4.1	Alto	Formación	Conocer la existencia, circunstancias y procedimiento de uso medios alternativos para prestar los servicios en el caso de que fallen los medios habituales
5.8.4.2	Alto	Concienciación	Entender la importancia de conocer los procedimientos de uso de los medios alternativos

Perfil laboral: Personal docente e investigador

Función clave: 3. Marco organizativo. Conocer el conjunto de medidas relacionadas con la organización global de la seguridad en la universidad.

Unidad de competencia: Política de seguridad			
3.1.0	Conocer los objetivos de la organización, el marco legal y regulatorio en el que se desarrollarán las actividades, conocer los roles de seguridad, la estructura del comité de seguridad, y la documentación de seguridad.		
Competencia profesional			
3.1.0.1	Alto	Formación	Conocer la política de seguridad de la universidad.
3.1.0.2	Alto	Formación	Conocer dónde puede consultarse la política de seguridad de la universidad.
3.1.0.3	Alto	Concienciación	Entender la importancia, significado y objetivos de la política de seguridad.
3.1.0.4	Medio	Concienciación	Entender la necesidad de conocer las actualizaciones de la política de seguridad.

Unidad de competencia: Normativa de seguridad			
3.2.0	Conocer los documentos que describen el uso correcto de equipos, servicios e instalaciones, lo que se considerará uso indebido y su responsabilidad con respecto al cumplimiento o violación de estas normas.		
Competencia profesional			
3.2.0.1	Alto	Formación	Conocer el uso correcto de los equipos, servicios e instalaciones que utilice en el desempeño de su labor.
3.2.0.2	Alto	Formación	Conocer qué se considera uso indebido de los equipos, servicios e instalaciones que utilice en el desempeño de su labor.
3.2.0.4	Alto	Concienciación	Entender la importancia del cumplimiento de la normativa de seguridad de la universidad.

Unidad de competencia: Procedimientos de seguridad			
3.3.0	Conocer los documentos que detallan cómo llevar a cabo las tareas habituales, quién debe hacer cada tarea y cómo identificar y reportar comportamientos anómalos.		
Competencia profesional			
3.3.0.1	Alto	Formación	Saber qué tareas en el ámbito de la seguridad de la información debe realizar en el desempeño de su labor.
3.3.0.2	Medio	Formación	Saber cómo llevar a cabo las tareas habituales en el ámbito de la seguridad de la información en el desempeño de su labor.
3.3.0.3	Medio	Formación	Saber identificar y reportar comportamientos anómalos en el ámbito de la seguridad.
3.3.0.4	Medio	Concienciación	Entender la importancia de conocer los procedimientos de seguridad en el desempeño de su actividad.

Unidad de competencia: Proceso de autorización			
3.4.0	Establecer un proceso formal de autorizaciones que cubra todos los elementos del sistema de información.		
Competencia profesional			
3.4.0.1	Alto	Formación	Conocer el funcionamiento de los procesos de autorización para el uso de los sistemas de información.

Función clave: 4. Proteger la operación del sistema como conjunto integral de componentes

Unidad de competencia: Análisis de riesgos			
4.1.1	Analizar los riesgos de seguridad de la organización para identificar los activos más valiosos del sistema, las amenazas más probables, las salvaguardas que protegen de dichas amenazas, así como identificar y valorar el riesgo residual.		
Competencia profesional			
4.1.1.1	Medio	Formación	Identificar y valorar cualitativamente los activos de información más valiosos de su entorno de trabajo.
4.1.1.2	Medio	Formación	Conocer la valoración de los sistemas derivados del análisis de riesgos, y el nivel de riesgo asumido.

Unidad de competencia: Requisitos de acceso			
4.2.2	Utilizar requisitos de acceso que permitan proteger los recursos del sistema impidiendo su utilización, salvo a las personas o procesos que disfruten de derechos de acceso suficientes.		
Competencia profesional			
4.2.2.1	Medio	Formación	Conocer las políticas y procedimiento de establecimiento de derechos de acceso a los recursos de su responsabilidad, ateniéndose a la política y normativa de seguridad del sistema.
4.2.2.2	Bajo	Concienciación	Entender la importancia de gestionar los derechos de acceso a los recursos de su responsabilidad, especialmente en los casos de actualización o bajas.

Unidad de competencia: Proceso de gestión de derechos de acceso			
4.2.4	Limitar los derechos de acceso de cada usuario atendiendo a los principios de mínimo privilegio, necesidad de conocer y capacidad de autorizar.		
Competencia profesional			
4.2.4.1	Medio	Concienciación	Comprender que los derechos de acceso se limitan atendiendo a los principios de mínimo privilegio y necesidad de conocer.
4.2.4.2	Medio	Formación	Conocer las políticas y procedimientos para conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable.

Unidad de competencia: Acceso local (local logon)			
4.2.6	Acceder de manera controlada a los puestos de trabajo dentro de las propias instalaciones de la organización de acuerdo con el nivel de las dimensiones de seguridad.		
Competencia profesional			
4.2.6.1	Medio	Concienciación	Entender la necesidad de cumplir la información que suministre el sistema respecto a sus obligaciones una vez que se ha obtenido el acceso.

Unidad de competencia: Acceso remoto (remote login)			
4.2.7	Acceder de manera controlada a los puestos de trabajo desde fuera de las propias instalaciones de la organización, a través de redes de terceros.		
Competencia profesional			
4.2.7.1	Alto	Formación	Conocer las políticas y procedimientos de acceso remoto a los sistemas.
4.2.7.3	Alto	Formación	Conocer y aplicar las buenas prácticas de acceso remoto.
4.2.7.4	Alto	Concienciación	Entender que es necesario aplicar los mismos principios de seguridad que rigen para un acceso local.

Unidad de competencia: Inventario de activos			
4.3.01	Mantener un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a la persona que es responsable de las decisiones relativas al mismo.		
Competencia profesional			
4.3.01.1	Medio	Concienciación	Entender la necesidad de conocer y proteger los activos de información de los que es responsable.
4.3.01.2	Medio	Concienciación	Comprender la importancia de comunicar la existencia de un equipo no inventariado.

Unidad de competencia: Configuración de seguridad			
4.3.02	Configurar los equipos previamente a su entrada en operación, de forma que se retiren cuentas y contraseñas estándar, se aplique la regla de "mínima funcionalidad" y la regla de "seguridad por defecto".		
Competencia profesional			
4.3.02.1	Medio	Concienciación	Entender la necesidad de configurar los equipos bajo las reglas de "mínima funcionalidad" y "seguridad por defecto".

Unidad de competencia: Gestión de la configuración			
4.3.03	Gestionar de manera continua la configuración de los componentes del sistema de manera que se mantenga en todo momento las reglas de "funcionalidad mínima" y "seguridad por defecto", el sistema se adapte a nuevas necesidades previamente autorizadas, y reaccione a vulnerabilidades reportadas e incidentes.		
Competencia profesional			
4.3.03.1	Medio	Concienciación	Entender la necesidad de gestionar la configuración de los sistemas bajo las reglas de "mínima funcionalidad" y "seguridad por defecto"

Unidad de competencia: Mantenimiento			
4.3.04	Mantener el equipamiento físico y lógico que constituye el sistema.		
Competencia profesional			
4.3.04.1	Bajo	Formación	Atender las especificaciones de los fabricantes en lo relativo al buen uso y mantenimiento de los equipos que utilice en el desempeño de sus tareas.

Unidad de competencia: Gestión de incidentes			
4.3.07	Disponer de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema.		
Competencia profesional			
4.3.07.2	Medio	Concienciación	Comprender la importancia de utilizar el procedimiento de gestión de incidentes

Unidad de competencia: Registro de la actividad de los usuarios			
4.3.08	Registrar las actividades de los usuarios en el sistema, de forma que se recoja quién realiza la actividad, cuándo la realiza y sobre qué información.		
Competencia profesional			
4.3.08.1	Medio	Concienciación	Entender que se registrará su actividad, cuándo la realiza y sobre qué información.

Unidad de competencia: Contratación y acuerdos de nivel de servicio			
4.4.1	Establecer contractualmente las características de los servicios prestados y las responsabilidades de las partes, detallando lo que se considera calidad mínima del servicio prestado y las consecuencias de su incumplimiento.		
Competencia profesional			
4.4.1.1	Bajo	Formación	Conocer los SLA en los que le afecta, las características del servicio prestado y las responsabilidades de las partes.
4.4.1.2	N.A.	Concienciación	Entender la necesidad de participar activamente en el ciclo de vida de los SLA y en el seguimiento de su cumplimiento.

Unidad de competencia: Gestión diaria			
4.4.2	Establecer un sistema rutinario para medir el cumplimiento de las obligaciones de servicio y el procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado, el mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas afectados por el acuerdo, y el mecanismo y los procedimientos de coordinación en caso de incidentes y desastres.		
Competencia profesional			
4.4.2.1	N.A.	Formación	Conocer el sistema rutinario para medir el cumplimiento de las obligaciones de servicio.
4.4.2.2	Medio	Formación	Conocer los procedimientos de coordinación en caso de incidentes y desastres en los servicios.

Unidad de competencia: Análisis de impacto			
4.5.1	Realizar análisis de impacto que permita determinar los requisitos de disponibilidad de cada servicio y los elementos que son críticos para la prestación de cada servicio.		
Competencia profesional			
4.5.1.1	Medio	Formación	Conocer los requisitos de disponibilidad de los servicios que sea responsable.
4.5.1.2	Alto	Formación	Conocer los elementos que son críticos para la prestación de los servicios que sea responsable.
4.5.1.3	Medio	Concienciación	Comprender la importancia de colaborar en la realización de un correcto análisis de impacto.

Unidad de competencia: Plan de continuidad			
4.5.2	Desarrollar un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales.		
Competencia profesional			
4.5.2.1	Medio	Formación	Conocer las funciones, responsabilidades y actividades a realizar en un plan de continuidad.
4.5.2.2	Medio	Formación	Conocer los medios alternativos que se utilizarán para mantener el servicio.

Unidad de competencia: Pruebas periódicas			
4.5.3	Realizar pruebas periódicas para localizar y, corregir en su caso, los errores o deficiencias que puedan existir en el plan de continuidad.		
Competencia profesional			
4.5.3.1	Medio	Concienciación	Entender la necesidad de hacer pruebas periódicas del plan de continuidad y colaborar activamente.

Función clave: 5. Proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad

Unidad de competencia: Áreas separadas y con control de acceso			
5.1.1	Controlar los accesos a las áreas indicadas de forma que sólo se pueda acceder por las entradas previstas y vigiladas.		
Competencia profesional			
5.1.1.1	Medio	Concienciación	Entender que no puede acceder a locales a los que no está autorizado, ni solicitar credenciales de acceso de manera no autorizada.

Unidad de competencia: Identificación de las personas			
5.1.2	Identificar y registrar las entradas y salidas de todas las personas que accedan a los locales donde hay equipamiento que forme parte del sistema de información.		
Competencia profesional			
5.1.2.1	Medio	Concienciación	Entender la necesidad de identificarse cuando se acceda a los locales donde hay equipamiento que forme parte del sistema de información.

Unidad de competencia: Instalaciones alternativas			
5.1.8	Garantizar la existencia y disponibilidad de instalaciones alternativas para poder trabajar en caso de que las instalaciones habituales no estén disponibles.		
Competencia profesional			
5.1.8.1	Medio	Formación	Conocer la ubicación y la forma de acceso a las instalaciones alternativas para poder trabajar en caso de que las instalaciones habituales no estén disponibles, así como el procedimiento y condiciones de cambio de ubicación.

Unidad de Competencia: Deberes y obligaciones			
5.2.2	Conocer los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.		
Competencia profesional			
5.2.2.1	Alto	Formación	Conocer las medidas disciplinarias en caso de incumplimiento de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.

Unidad de competencia: Personal alternativo			
5.2.5	Garantizar la existencia y disponibilidad de otras personas que se puedan hacer cargo de las funciones en caso de indisponibilidad del personal habitual.		
Competencia profesional			
5.2.5.1	Bajo	Concienciación	Entender la importancia de conocer la existencia y disponibilidad de personas que se puedan hacer cargo de las funciones en caso de indisponibilidad del personal habitual.

Unidad de competencia: Puesto de trabajo despejado			
5.3.1	Asegurar que el puesto de trabajo permanece despejado, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.		
Competencia profesional			
5.3.1.1	Medio	Concienciación	Entender la necesidad de que su puesto de trabajo permanezca despejado, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.
5.3.1.2	Medio	Concienciación	Entender que el material se guardará en lugar cerrado cuando no se esté utilizando.

Unidad de competencia: Bloqueo de puesto de trabajo			
5.3.2	Bloquear al cabo de un tiempo prudencial de inactividad el puesto de trabajo, requiriendo una nueva autenticación para reanudar la actividad en curso.		
Competencia profesional			
5.3.2.1	Alto	Concienciación	Entender la necesidad de que el puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación para reanudar la actividad en curso.
5.3.2.2	Medio	Concienciación	Entender la necesidad de que pasado un cierto tiempo sin utilizar, se cancelarán las sesiones abiertas desde su puesto de trabajo.

Unidad de competencia: Protección de equipos portátiles			
5.3.3	Proteger adecuadamente los equipos que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente.		
Competencia profesional			
5.3.3.1	Medio	Formación	Conocer el procedimiento para informar de la pérdida o sustracción de un portátil
5.3.3.3	Alto	Concienciación	Entender que cuando el equipo portátil se conecte remotamente a través de redes que no están bajo el estricto control de la universidad, no debe enviarse información confidencial o protegida.
5.3.3.4	Medio	Concienciación	Entender que en el equipo portátil no deben almacenarse información o datos de carácter confidencial o protegido.
5.3.3.6	Medio	Formación	En caso de almacenar información sensible en el equipo, conocer herramientas y técnicas de protección.

Unidad de competencia: Medios alternativos			
5.3.4	Garantizar la existencia y disponibilidad de medios alternativos de tratamiento de la información para el caso de que fallen los medios habituales.		
Competencia profesional			
5.3.4.1	Medio	Formación	Conocer el procedimiento de acceso a medios alternativos de tratamiento de la información para el caso de que fallen los medios habituales.

Unidad de competencia: Etiquetado			
5.5.1	Entender el significado de las etiquetas de los soportes de información, bien mediante simple inspección, bien mediante el recurso a un repositorio que lo explique.		
Competencia profesional			
5.5.1.1	Medio	Formación	Conocer el significado de las etiquetas que indiquen el nivel de seguridad de la información, bien mediante simple inspección, bien mediante el recurso a un repositorio que lo explique.
5.5.1.2	Medio	Formación	Conocer el tratamiento y gestión de la información en base a su nivel de seguridad.
5.5.1.3	Medio	Concienciación	Entender la necesidad de clasificar y etiquetar la información respecto a su nivel de seguridad.

Unidad de competencia: Custodia			
5.5.3	Emplear el control de acceso y las exigencias de mantenimiento del fabricante de los soportes de información que permanecen bajo la responsabilidad de la organización.		
Competencia profesional			
5.5.3.1	Medio	Formación	Saber aplicar medidas físicas o lógicas para garantizar el control de acceso a los soportes de información bajo su responsabilidad.
5.5.3.2	Medio	Concienciación	Entender las necesidad de respetar las exigencias de mantenimiento del fabricante de los soportes de información, en especial, en lo referente a temperatura, humedad y otros agresores medioambientales

Unidad de competencia: Borrado y destrucción			
5.5.5	Garantizar el borrado y destrucción de soportes de información susceptibles de almacenar información.		
Competencia profesional			
5.5.5.1	Medio	Formación	Saber borrar de manera segura los soportes de información que vayan a ser reutilizados para otra información o liberados.
5.5.5.2	Medio	Concienciación	Entender la necesidad de realizar borrados seguros de soportes cuando vayan a ser reutilizados o liberados.
5.5.5.3	Medio	Formación	Conocer el procedimiento de solicitud de destrucción de soportes de información.

Unidad de competencia: Aceptación y puesta en servicio			
5.6.2	Comprobar el correcto funcionamiento de la aplicación antes de su puesta en producción.		
Competencia profesional			
5.6.2.1	Bajo	Formación	Conocer los criterios de aceptación en materia de seguridad en caso de contratación externa.

Unidad de competencia: Calificación de la información			
5.7.2	Calificar, etiquetar y tratar la información en consideración al nivel de seguridad que requiere.		
Competencia profesional			
5.7.2.1	Bajo	Formación	Conocer los criterios para asignar a cada información el nivel de seguridad requerido, y ser responsable de su documentación y aprobación formal.
5.7.2.2	Bajo	Formación	Conocer las políticas y procedimientos que describan en detalle la forma en la que se ha de etiquetar y tratar la información en consideración al nivel de seguridad que requiere
5.7.2.3	Bajo	Concienciación	Entender que como responsable de información, en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad.

Unidad de competencia: Cifrado			
5.7.3	Cifrar la información con un nivel alto en confidencialidad tanto durante su almacenamiento como durante su transmisión.		
Competencia profesional			
5.7.3.1	Medio	Concienciación	Entender que la información con un nivel alto de confidencialidad se cifrará tanto durante su almacenamiento como durante su transmisión. Sólo estará en claro mientras se está haciendo uso de ella.

Unidad de competencia: Firma electrónica			
5.7.4	Emplear la firma electrónica como un instrumento capaz de permitir la comprobación de la autenticidad de la procedencia y la integridad de la información ofreciendo las bases para evitar el repudio.		
Competencia profesional			
5.7.4.1	Alto	Formación	Conocer las políticas, procedimientos y circunstancias de uso de la firma electrónica.
5.7.4.2	Alto	Concienciación	Entender la importancia del buen uso y resguardo de la firma electrónica

Unidad de competencia: Limpieza de documentos			
5.7.6	Retirar de los documentos toda la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.		
Competencia profesional			
5.7.6.1	Medio	Formación	Retirar de la documentación toda la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.
5.7.6.2	Medio	Concienciación	Entender la necesidad de gestionar los metadatos de la documentación que se utilice o genere.

Unidad de competencia: Copias de seguridad (backup)			
5.7.7	Realizar copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente con una antigüedad determinada.		
Competencia profesional			
5.7.7.1	Medio	Formación	Conocer las políticas y procedimientos de realización de copias de seguridad en su entorno de trabajo.
5.7.7.2	Medio	Concienciación	Entender la necesidad de realizar copias de seguridad de manera periódica, así como comprobar que han sido bien realizadas.

Unidad de competencia: Protección del correo electrónico			
5.8.1	Proteger frente a las amenazas que le son propias la información distribuida por medio de correo electrónico.		
Competencia profesional			
5.8.1.1	Medio	Formación	Proteger la información de los correos electrónicos, tanto en el cuerpo de los mensajes, como en los anexos.

Unidad de competencia: Medios alternativos			
5.8.4	Garantizar la existencia y disponibilidad de medios alternativos para prestar los servicios en el caso de que fallen los medios habituales.		
Competencia profesional			
5.8.4.1	Bajo	Formación	Conocer la existencia, circunstancias y procedimiento de uso medios alternativos para prestar los servicios en el caso de que fallen los medios habituales
5.8.4.2	Medio	Concienciación	Entender la importancia de conocer los procedimientos de uso de los medios alternativos

Perfil laboral: Puestos base del personal de Administración y Servicios

Función clave: 3. Marco organizativo. Conocer el conjunto de medidas relacionadas con la organización global de la seguridad en la universidad.

Unidad de competencia: Política de seguridad			
3.1.0	Conocer los objetivos de la organización, el marco legal y regulatorio en el que se desarrollarán las actividades, conocer los roles de seguridad, la estructura del comité de seguridad, y la documentación de seguridad.		
Competencia profesional			
3.1.0.1	Alto	Formación	Conocer la política de seguridad de la universidad.
3.1.0.2	Medio	Formación	Conocer dónde puede consultarse la política de seguridad de la universidad.
3.1.0.3	Medio	Concienciación	Entender la importancia, significado y objetivos de la política de seguridad.
3.1.0.4	Medio	Concienciación	Entender la necesidad de conocer las actualizaciones de la política de seguridad.

Unidad de competencia: Normativa de seguridad			
3.2.0	Conocer los documentos que describen el uso correcto de equipos, servicios e instalaciones, lo que se considerará uso indebido y su responsabilidad con respecto al cumplimiento o violación de las normas.		
Competencia profesional			
3.2.0.1	Medio	Formación	Conocer el uso correcto de los equipos, servicios e instalaciones que utilice en el desempeño de su labor.
3.2.0.2	Medio	Formación	Conocer qué se considera uso indebido de los equipos, servicios e instalaciones que utilice en el desempeño de su labor.
3.2.0.4	Medio	Concienciación	Entender la importancia del cumplimiento de la normativa de seguridad de la universidad.

Unidad de competencia: Procedimientos de seguridad			
3.3.0	Conocer los documentos que detallan cómo llevar a cabo las tareas habituales, quién debe hacer cada tarea y cómo identificar y reportar comportamientos anómalos.		
Competencia profesional			
3.3.0.1	Medio	Formación	Saber qué tareas en el ámbito de la seguridad de la información debe realizar en el desempeño de su labor.
3.3.0.2	Medio	Formación	Saber cómo llevar a cabo las tareas habituales en el ámbito de la seguridad de la información en el desempeño de su labor.
3.3.0.3	Medio	Formación	Saber identificar y reportar comportamientos anómalos en el ámbito de la seguridad.
3.3.0.4	Medio	Concienciación	Entender la importancia de conocer los procedimientos de seguridad en el desempeño de su actividad.

Unidad de competencia: Proceso de autorización			
3.4.0	Establecer un proceso formal de autorizaciones que cubra todos los elementos del sistema de información.		
Competencia profesional			
3.4.0.1	Medio	Formación	Conocer el funcionamiento de los procesos de autorización para el uso de los sistemas de información.

Función clave: 4. Proteger la operación del sistema como conjunto integral de componentes

Unidad de competencia: Análisis de riesgos			
4.1.1.	Analizar los riesgos de seguridad de la organización para identificar los activos más valiosos del sistema, las amenazas más probables, las salvaguardas que protegen de dichas amenazas, así como identificar y valorar el riesgo residual.		
Competencia profesional			
4.1.1.1	Bajo	Formación	Identificar y valorar cualitativamente los activos de información más valiosos de su entorno de trabajo.
4.1.1.2	Bajo	Formación	Conocer la valoración de los sistemas derivados del análisis de riesgos, y el nivel de riesgo asumido.

Unidad de competencia: Requisitos de acceso			
4.2.2	Utilizar requisitos de acceso que permitan proteger los recursos del sistema impidiendo su utilización, salvo a las personas o procesos que disfruten de derechos de acceso suficientes.		
Competencia profesional			
4.2.2.1	Medio	Formación	Conocer las políticas y procedimiento de establecimiento de derechos de acceso a los recursos de su responsabilidad, ateniéndose a la política y normativa de seguridad del sistema.
4.2.2.2	Bajo	Concienciación	Entender la importancia de gestionar los derechos de acceso a los recursos de su responsabilidad, especialmente en los casos de actualización o bajas.

Unidad de competencia: Proceso de gestión de derechos de acceso			
4.2.4	Limitar los derechos de acceso de cada usuario atendiendo a los principios de mínimo privilegio, necesidad de conocer y capacidad de autorizar.		
Competencia profesional			
4.2.4.1	Medio	Concienciación	Comprender que los derechos de acceso se limitan atendiendo a los principios de mínimo privilegio y necesidad de conocer.
4.2.4.2	Bajo	Formación	Conocer las políticas y procedimientos para conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable.

Unidad de competencia: Acceso local (local logon)			
4.2.6	Acceder de manera controlada a los puestos de trabajo dentro de las propias instalaciones de la organización de acuerdo con el nivel de las dimensiones de seguridad.		
Competencia profesional			
4.2.6.1	Medio	Concienciación	Entender la necesidad de cumplir la información que suministre el sistema respecto a sus obligaciones una vez que se ha obtenido el acceso.

Unidad de competencia: Acceso remoto (remote login)			
4.2.7	Acceder de manera controlada a los puestos de trabajo desde fuera de las propias instalaciones de la organización, a través de redes de terceros.		
Competencia profesional			
4.2.7.1	Medio	Formación	Conocer las políticas y procedimientos de acceso remoto a los sistemas.
4.2.7.3	Medio	Formación	Conocer y aplicar las buenas prácticas de acceso remoto.
4.2.7.4	Alto	Concienciación	Entender que es necesario aplicar los mismos principios de seguridad que rigen para un acceso local.

Unidad de competencia: Inventario de activos			
4.3.01	Mantener un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a la persona que es responsable de las decisiones relativas al mismo.		
Competencia profesional			
4.3.01.1	Medio	Concienciación	Entender la necesidad de conocer y proteger los activos de información de los que es responsable.
4.3.01.2	Bajo	Concienciación	Comprender la importancia de comunicar la existencia de un equipo no inventariado.

Unidad de competencia: Configuración de seguridad			
4.3.02	Configurar los equipos previamente a su entrada en operación, de forma que se retiren cuentas y contraseñas estándar, se aplique la regla de "mínima funcionalidad" y la regla de "seguridad por defecto".		
Competencia profesional			
4.3.02.1	Bajo	Concienciación	Entender la necesidad de configurar los equipos bajo las reglas de "mínima funcionalidad" y "seguridad por defecto".

Unidad de competencia: Gestión de la configuración			
4.3.03	Gestionar de manera continua la configuración de los componentes del sistema de manera que se mantenga en todo momento las reglas de "funcionalidad mínima" y "seguridad por defecto", el sistema se adapte a nuevas necesidades previamente autorizadas, y reaccione a vulnerabilidades reportadas e incidentes.		
Competencia profesional			
4.3.03.1	Bajo	Concienciación	Entender la necesidad de gestionar la configuración de los sistemas bajo las reglas de "mínima funcionalidad" y "seguridad por defecto"

Unidad de competencia: Mantenimiento			
4.3.04	Mantener el equipamiento físico y lógico que constituye el sistema.		
Competencia profesional			
4.3.04.1	Bajo	Formación	Atender las especificaciones de los fabricantes en lo relativo al buen uso y mantenimiento de los equipos que utilice en el desempeño de sus tareas.

Unidad de competencia: Gestión de incidentes			
4.3.07	Disponer de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema.		
Competencia profesional			
4.3.07.2	Medio	Concienciación	Comprender la importancia de utilizar el procedimiento de gestión de incidentes

Unidad de competencia: Registro de la actividad de los usuarios			
4.3.08	Registrar las actividades de los usuarios en el sistema, de forma que se recoja quién realiza la actividad, cuándo la realiza y sobre qué información.		
Competencia profesional			
4.3.08.1	Medio	Concienciación	Entender que se registrará su actividad, cuándo la realiza y sobre qué información.

Unidad de competencia: Contratación y acuerdos de nivel de servicio			
4.4.1	Establecer contractualmente las características de los servicios prestados y las responsabilidades de las partes, detallando lo que se considera calidad mínima del servicio prestado y las consecuencias de su incumplimiento.		
Competencia profesional			
4.4.1.1	Bajo	Formación	Conocer los SLA en los que le afecta, las características del servicio prestado y las responsabilidades de las partes.
4.4.1.2	N.A.	Concienciación	Entender la necesidad de participar activamente en el ciclo de vida de los SLA y en el seguimiento de su cumplimiento.

Unidad de competencia: Gestión diaria			
4.4.2	Establecer un sistema rutinario para medir el cumplimiento de las obligaciones de servicio y el procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado, el mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas afectados por el acuerdo, y el mecanismo y los procedimientos de coordinación en caso de incidentes y desastres.		
Competencia profesional			
4.4.2.1	N.A.	Formación	Conocer el sistema rutinario para medir el cumplimiento de las obligaciones de servicio.
4.4.2.2	Bajo	Formación	Conocer los procedimientos de coordinación en caso de incidentes y desastres en los servicios.

Unidad de competencia: Análisis de impacto			
4.5.1	Realizar análisis de impacto que permita determinar los requisitos de disponibilidad de cada servicio y los elementos que son críticos para la prestación de cada servicio.		
Competencia profesional			
4.5.1.1	Bajo	Formación	Conocer los requisitos de disponibilidad de los servicios que sea responsable.
4.5.1.2	Alto	Formación	Conocer los elementos que son críticos para la prestación de los servicios que sea responsable.
4.5.1.3	Bajo	Concienciación	Comprender la importancia de colaborar en la realización de un correcto análisis de impacto.

Unidad de competencia: Plan de continuidad			
4.5.2	Desarrollar un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales.		
Competencia profesional			
4.5.2.1	Medio	Formación	Conocer las funciones, responsabilidades y actividades a realizar en un plan de continuidad.
4.5.2.2	Medio	Formación	Conocer los medios alternativos que se utilizarán para mantener el servicio.

Unidad de competencia: Pruebas periódicas			
4.5.3	Realizar pruebas periódicas para localizar y, corregir en su caso, los errores o deficiencias que puedan existir en el plan de continuidad.		
Competencia profesional			
4.5.3.1	Bajo	Concienciación	Entender la necesidad de hacer pruebas periódicas del plan de continuidad y colaborar activamente.

Función clave: 5. Proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad

Unidad de competencia: Áreas separadas y con control de acceso			
5.1.1	Controlar los accesos a las áreas indicadas de forma que sólo se pueda acceder por las entradas previstas y vigiladas.		
Competencia profesional			
5.1.1.1	Medio	Concienciación	Entender que no puede acceder a locales a los que no está autorizado, ni solicitar credenciales de acceso de manera no autorizada.

Unidad de competencia: Identificación de las personas			
5.1.2	Identificar y registrar las entradas y salidas de todas las personas que accedan a los locales donde hay equipamiento que forme parte del sistema de información.		
Competencia profesional			
5.1.2.1	Medio	Concienciación	Entender la necesidad de identificarse cuando se acceda a los locales donde hay equipamiento que forme parte del sistema de información.

Unidad de competencia: Instalaciones alternativas			
5.1.8	Garantizar la existencia y disponibilidad de instalaciones alternativas para poder trabajar en caso de que las instalaciones habituales no estén disponibles.		
Competencia profesional			
5.1.8.1	Bajo	Formación	Conocer la ubicación y la forma de acceso a las instalaciones alternativas para poder trabajar en caso de que las instalaciones habituales no estén disponibles, así como el procedimiento y condiciones de cambio de ubicación.

Unidad de Competencia: Deberes y obligaciones			
5.2.2	Conocer los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.		
Competencia profesional			
5.2.2.1	Alto	Formación	Conocer las medidas disciplinarias en caso de incumplimiento de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.

Unidad de competencia: Personal alternativo			
5.2.5	Garantizar la existencia y disponibilidad de otras personas que se puedan hacer cargo de las funciones en caso de indisponibilidad del personal habitual.		
Competencia profesional			
5.2.5.1	Bajo	Concienciación	Entender la importancia de conocer la existencia y disponibilidad de personas que se puedan hacer cargo de las funciones en caso de indisponibilidad del personal habitual.

Unidad de competencia: Puesto de trabajo despejado			
5.3.1	Asegurar que el puesto de trabajo permanece despejado, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.		
Competencia profesional			
5.3.1.1	Medio	Concienciación	Entender la necesidad de que su puesto de trabajo permanezca despejado, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.
5.3.1.2	Medio	Concienciación	Entender que el material se guardará en lugar cerrado cuando no se esté utilizando.

Unidad de competencia: Bloqueo de puesto de trabajo			
5.3.2	Bloquear al cabo de un tiempo prudencial de inactividad el puesto de trabajo, requiriendo una nueva autenticación para reanudar la actividad en curso.		
Competencia profesional			
5.3.2.1	Alto	Concienciación	Entender la necesidad de que el puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación para reanudar la actividad en curso.
5.3.2.2	Medio	Concienciación	Entender la necesidad de que pasado un cierto tiempo sin utilizar, se cancelarán las sesiones abiertas desde su puesto de trabajo.

Unidad de competencia: Protección de equipos portátiles			
5.3.3	Proteger adecuadamente los equipos que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente.		
Competencia profesional			
5.3.3.1	Medio	Formación	Conocer el procedimiento para informar de la pérdida o sustracción de un portátil
5.3.3.3	Medio	Concienciación	Entender que cuando el equipo portátil se conecte remotamente a través de redes que no están bajo el estricto control de la universidad, no debe enviarse información confidencial o protegida.
5.3.3.4	Medio	Concienciación	Entender que en el equipo portátil no deben almacenarse información o datos de carácter confidencial o protegido.
5.3.3.6	Medio	Formación	En caso de almacenar información sensible en el equipo, conocer herramientas y técnicas de protección.

Unidad de competencia: Medios alternativos			
5.3.4	Garantizar la existencia y disponibilidad de medios alternativos de tratamiento de la información para el caso de que fallen los medios habituales.		
Competencia profesional			
5.3.4.1	Medio	Formación	Conocer el procedimiento de acceso a medios alternativos de tratamiento de la información para el caso de que fallen los medios habituales.

Unidad de competencia: Etiquetado			
5.5.1	Entender el significado de las etiquetas de los soportes de información, bien mediante simple inspección, bien mediante el recurso a un repositorio que lo explique.		
Competencia profesional			
5.5.1.1	Medio	Formación	Conocer el significado de las etiquetas que indiquen el nivel de seguridad de la información, bien mediante simple inspección, bien mediante el recurso a un repositorio que lo explique.
5.5.1.2	Medio	Formación	Conocer el tratamiento y gestión de la información en base a su nivel de seguridad.
5.5.1.3	Medio	Concienciación	Entender la necesidad de clasificar y etiquetar la información respecto a su nivel de seguridad.

Unidad de competencia: Custodia			
5.5.3	Emplear el control de acceso y las exigencias de mantenimiento del fabricante de los soportes de información que permanecen bajo la responsabilidad de la organización.		
Competencia profesional			
5.5.3.1	Medio	Formación	Saber aplicar medidas físicas o lógicas para garantizar el control de acceso a los soportes de información bajo su responsabilidad.
5.5.3.2	Bajo	Concienciación	Entender las necesidad de respetar las exigencias de mantenimiento del fabricante de los soportes de información, en especial, en lo referente a temperatura, humedad y otros agresores medioambientales

Unidad de competencia: Borrado y destrucción			
5.5.5	Garantizar el borrado y destrucción de soportes de información susceptibles de almacenar información.		
Competencia profesional			
5.5.5.1	Medio	Formación	Saber borrar de manera segura los soportes de información que vayan a ser reutilizados para otra información o liberados.
5.5.5.2	Medio	Concienciación	Entender la necesidad de realizar borrados seguros de soportes cuando vayan a ser reutilizados o liberados.
5.5.5.3	Medio	Formación	Conocer el procedimiento de solicitud de destrucción de soportes de información.

Unidad de competencia: Aceptación y puesta en servicio			
5.6.2	Comprobar el correcto funcionamiento de la aplicación antes de su puesta en producción.		
Competencia profesional			
5.6.2.1	N.A.	Formación	Conocer los criterios de aceptación en materia de seguridad en caso de contratación externa.

Unidad de competencia: Calificación de la información			
5.7.2	Calificar, etiquetar y tratar la información en consideración al nivel de seguridad que requiere.		
Competencia profesional			
5.7.2.1	N.A.	Formación	Conocer los criterios para asignar a cada información el nivel de seguridad requerido, y ser responsable de su documentación y aprobación formal.
5.7.2.2	N.A.	Formación	Conocer las políticas y procedimientos que describan en detalle la forma en la que se ha de etiquetar y tratar la información en consideración al nivel de seguridad que requiere
5.7.2.3	N.A.	Concienciación	Entender que como responsable de información, en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad.

Unidad de competencia: Cifrado			
5.7.3	Cifrar la información con un nivel alto en confidencialidad tanto durante su almacena miento como durante su transmisión.		
Competencia profesional			
5.7.3.1	Medio	Concienciación	Entender que la información con un nivel alto de confidencialidad se cifrará tanto durante su almacenamiento como durante su transmisión. Sólo estará en claro mientras se está haciendo uso de ella.

Unidad de competencia: Firma electrónica			
5.7.4	Emplear la firma electrónica como un instrumento capaz de permitir la comprobación de la autenticidad de la procedencia y la integridad de la información ofreciendo las bases para evitar el repudio.		
Competencia profesional			
5.7.4.1	Medio	Formación	Conocer las políticas, procedimientos y circunstancias de uso de la firma electrónica.
5.7.4.2	Medio	Concienciación	Entender la importancia del buen uso y resguardo de la firma electrónica

Unidad de competencia: Limpieza de documentos			
5.7.6	Retirar de los documentos toda la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.		
Competencia profesional			
5.7.6.1	Medio	Formación	Retirar de la documentación toda la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.
5.7.6.2	Medio	Concienciación	Entender la necesidad de gestionar los metadatos de la documentación que se utilice o genere.

Unidad de competencia: Copias de seguridad (backup)			
5.7.7	Realizar copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente con una antigüedad determinada.		
Competencia profesional			
5.7.7.1	Bajo	Formación	Conocer las políticas y procedimientos de realización de copias de seguridad en su entorno de trabajo.
5.7.7.2	Medio	Concienciación	Entender la necesidad de realizar copias de seguridad de manera periódica, así como comprobar que han sido bien realizadas.

Unidad de competencia: Protección del correo electrónico			
5.8.1	Proteger frente a las amenazas que le son propias la información distribuida por medio de correo electrónico.		
Competencia profesional			
5.8.1.1	Medio	Formación	Proteger la información de los correos electrónicos, tanto en el cuerpo de los mensajes, como en los anexos.

Unidad de competencia: Medios alternativos			
5.8.4	Garantizar la existencia y disponibilidad de medios alternativos para prestar los servicios en el caso de que fallen los medios habituales.		
Competencia profesional			
5.8.4.1	Bajo	Formación	Conocer la existencia, circunstancias y procedimiento de uso medios alternativos para prestar los servicios en el caso de que fallen los medios habituales
5.8.4.2	Bajo	Concienciación	Entender la importancia de conocer los procedimientos de uso de los medios alternativos

Perfil laboral: Consejeras y Consejeros externos

Función clave: 3. Marco organizativo. Conocer el conjunto de medidas relacionadas con la organización global de la seguridad en la universidad.

Unidad de competencia: Política de seguridad			
3.1.0	Documentar los objetivos de la organización, el marco legal y regulatorio en el que se desarrollarán las actividades, definir los roles de seguridad, la estructura del comité de seguridad, y las directrices para la estructuración de la documentación de seguridad.		
Competencia profesional			
3.1.0.1	Medio	Formación	Conocer la política de seguridad de la universidad.
3.1.0.2	Bajo	Formación	Conocer dónde puede consultarse la política de seguridad de la universidad.
3.1.0.3	Alto	Concienciación	Entender la importancia, significado y objetivos de la política de seguridad.
3.1.0.4	Medio	Concienciación	Entender la necesidad de conocer las actualizaciones de la política de seguridad.

Unidad de competencia: Normativa de seguridad			
3.2.0	Conocer los documentos que describen el uso correcto de equipos, servicios e instalaciones, lo que se considerará uso indebido y su responsabilidad con respecto al cumplimiento o violación de las normas.		
Competencia profesional			
3.2.0.1	Bajo	Formación	Conocer el uso correcto de los equipos, servicios e instalaciones que utilice en el desempeño de su labor.
3.2.0.2	Bajo	Formación	Conocer qué se considera uso indebido de los equipos, servicios e instalaciones que utilice en el desempeño de su labor
3.2.0.4	Medio	Concienciación	Entender la importancia del cumplimiento de la normativa de seguridad de la universidad.

Unidad de competencia: Procedimientos de seguridad			
3.3.0	Conocer los documentos que detallan cómo llevar a cabo las tareas habituales, quién debe hacer cada tarea y cómo identificar y reportar comportamientos anómalos.		
Competencia profesional			
3.3.0.1	Medio	Formación	Saber qué tareas en el ámbito de la seguridad de la información debe realizar en el desempeño de su labor.
3.3.0.2	Bajo	Formación	Saber cómo llevar a cabo las tareas habituales en el ámbito de la seguridad de la información en el desempeño de su labor.
3.3.0.3	Bajo	Formación	Saber identificar y reportar comportamientos anómalos en el ámbito de la seguridad.
3.3.0.4	Bajo	Concienciación	Entender la importancia de conocer los procedimientos de seguridad en el desempeño de su actividad.

Unidad de competencia: Proceso de autorización			
3.4.0	Establecer un proceso formal de autorizaciones que cubra todos los elementos del sistema de información.		
Competencia profesional			
3.4.0.1	Bajo	Formación	Conocer el funcionamiento de los procesos de autorización para el uso de los sistemas de información.

Función clave: 4. Proteger la operación del sistema como conjunto integral de componentes

Unidad de competencia: Análisis de riesgos			
4.1.1.	Analizar los riesgos de seguridad de la organización para identificar los activos más valiosos del sistema, las amenazas más probables, las salvaguardas que protegen de dichas amenazas, así como identificar y valorar el riesgo residual.		
Competencia profesional			
4.1.1.1	Bajo	Formación	Identificar y valorar cualitativamente los activos de información más valiosos de su entorno de trabajo.
4.1.1.2	Medio	Formación	Conocer la valoración de los sistemas derivados del análisis de riesgos, y el nivel de riesgo asumido.

Unidad de competencia: Requisitos de acceso			
4.2.2	Utilizar requisitos de acceso que permitan proteger los recursos del sistema impidiendo su utilización, salvo a las personas o procesos que disfruten de derechos de acceso suficientes.		
Competencia profesional			
4.2.2.1	Bajo	Formación	Conocer las políticas y procedimiento de establecimiento de derechos de acceso a los recursos de su responsabilidad, ateniéndose a la política y normativa de seguridad del sistema.
4.2.2.2	Bajo	Concienciación	Entender la importancia de gestionar los derechos de acceso a los recursos de su responsabilidad, especialmente en los casos de actualización o bajas.

Unidad de competencia: Proceso de gestión de derechos de acceso			
4.2.4	Limitar los derechos de acceso de cada usuario atendiendo a los principios de mínimo privilegio, necesidad de conocer y capacidad de autorizar.		
Competencia profesional			
4.2.4.1	Bajo	Concienciación	Comprender que los derechos de acceso se limitan atendiendo a los principios de mínimo privilegio y necesidad de conocer.
4.2.4.2	Bajo	Formación	Conocer las políticas y procedimientos para conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable.

Unidad de competencia: Acceso local (local logon)			
4.2.6	Acceder de manera controlada a los puestos de trabajo dentro de las propias instalaciones de la organización de acuerdo con el nivel de las dimensiones de seguridad.		
Competencia profesional			
4.2.6.1	Medio	Concienciación	Entender la necesidad de cumplir la información que suministre el sistema respecto a sus obligaciones una vez que se ha obtenido el acceso.

Unidad de competencia: Acceso remoto (remote login)			
4.2.7	Acceder de manera controlada a los puestos de trabajo desde fuera de las propias instalaciones de la organización, a través de redes de terceros.		
Competencia profesional			
4.2.7.1	Medio	Formación	Conocer las políticas y procedimientos de acceso remoto a los sistemas.
4.2.7.3	Medio	Formación	Conocer y aplicar las buenas prácticas de acceso remoto.
4.2.7.4	Medio	Concienciación	Entender que es necesario aplicar los mismos principios de seguridad que rigen para un acceso local.

Unidad de competencia: Inventario de activos			
4.3.01	Mantener un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a la persona que es responsable de las decisiones relativas al mismo.		
Competencia profesional			
4.3.01.1	Medio	Concienciación	Entender la necesidad de conocer y proteger los activos de información de los que es responsable.
4.3.01.2	Bajo	Concienciación	Comprender la importancia de comunicar la existencia de un equipo no inventariado.

Unidad de competencia: Configuración de seguridad			
4.3.02	Configurar los equipos previamente a su entrada en operación, de forma que se retiren cuentas y contraseñas estándar, se aplique la regla de "mínima funcionalidad" y la regla de "seguridad por defecto".		
Competencia profesional			
4.3.02.1	Bajo	Concienciación	Entender la necesidad de configurar los equipos bajo las reglas de "mínima funcionalidad" y "seguridad por defecto".

Unidad de competencia: Gestión de la configuración			
4.3.03	Gestionar de manera continua la configuración de los componentes del sistema de manera que se mantenga en todo momento las reglas de "funcionalidad mínima" y "seguridad por defecto", el sistema se adapte a nuevas necesidades previamente autorizadas, y reaccione a vulnerabilidades reportadas e incidentes.		
Competencia profesional			
4.3.03.1	Bajo	Concienciación	Entender la necesidad de gestionar la configuración de los sistemas bajo las reglas de "mínima funcionalidad" y "seguridad por defecto"

Unidad de competencia: Mantenimiento			
4.3.04	Mantener el equipamiento físico y lógico que constituye el sistema.		
Competencia profesional			
4.3.04.1	Bajo	Formación	Atender las especificaciones de los fabricantes en lo relativo al buen uso y mantenimiento de los equipos que utilice en el desempeño de sus tareas.

Unidad de competencia: Gestión de incidentes			
4.3.07	Disponer de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema.		
Competencia profesional			
4.3.07.2	Medio	Concienciación	Comprender la importancia de utilizar el procedimiento de gestión de incidentes

Unidad de competencia: Registro de la actividad de los usuarios			
4.3.08	Registrar las actividades de los usuarios en el sistema, de forma que se recoja quién realiza la actividad, cuándo la realiza y sobre qué información.		
Competencia profesional			
4.3.08.1	Bajo	Concienciación	Entender que se registrará su actividad, cuándo la realiza y sobre qué información.

Unidad de competencia: Contratación y acuerdos de nivel de servicio			
4.4.1	Establecer contractualmente las características de los servicios prestados y las responsabilidades de las partes, detallando lo que se considera calidad mínima del servicio prestado y las consecuencias de su incumplimiento.		
Competencia profesional			
4.4.1.1	Bajo	Formación	Conocer los SLA en los que le afecta, las características del servicio prestado y las responsabilidades de las partes.
4.4.1.2	N.A.	Concienciación	Entender la necesidad de participar activamente en el ciclo de vida de los SLA y en el seguimiento de su cumplimiento.

Unidad de competencia: Gestión diaria			
4.4.2	Establecer un sistema rutinario para medir el cumplimiento de las obligaciones de servicio y el procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado, el mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas afectados por el acuerdo, y el mecanismo y los procedimientos de coordinación en caso de incidentes y desastres.		
Competencia profesional			
4.4.2.1	N.A.	Formación	Conocer el sistema rutinario para medir el cumplimiento de las obligaciones de servicio.
4.4.2.2	Bajo	Formación	Conocer los procedimientos de coordinación en caso de incidentes y desastres en los servicios.

Unidad de competencia: Análisis de impacto			
4.5.1	Realizar análisis de impacto que permita determinar los requisitos de disponibilidad de cada servicio y los elementos que son críticos para la prestación de cada servicio.		
Competencia profesional			
4.5.1.1	Bajo	Formación	Conocer los requisitos de disponibilidad de los servicios que sea responsable.
4.5.1.2	Bajo	Formación	Conocer los elementos que son críticos para la prestación de los servicios que sea responsable.
4.5.1.3	N.A.	Concienciación	Comprender la importancia de colaborar en la realización de un correcto análisis de impacto.

Unidad de competencia: Plan de continuidad			
4.5.2	Desarrollar un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales.		
Competencia profesional			
4.5.2.1	Bajo	Formación	Conocer las funciones, responsabilidades y actividades a realizar en un plan de continuidad.
4.5.2.2	Bajo	Formación	Conocer los medios alternativos que se utilizarán para mantener el servicio.

Unidad de competencia: Pruebas periódicas			
4.5.3	Realizar pruebas periódicas para localizar y, corregir en su caso, los errores o deficiencias que puedan existir en el plan de continuidad.		
Competencia profesional			
4.5.3.1	N.A.	Concienciación	Entender la necesidad de hacer pruebas periódicas del plan de continuidad y colaborar activamente.

Función clave: 5. Proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad

Unidad de competencia: Áreas separadas y con control de acceso			
5.1.1	Controlar los accesos a las áreas indicadas de forma que sólo se pueda acceder por las entradas previstas y vigiladas.		
Competencia profesional			
5.1.1.1	Medio	Concienciación	Entender que no puede acceder a locales a los que no está autorizado, ni solicitar credenciales de acceso de manera no autorizada.

Unidad de competencia: Identificación de las personas			
5.1.2	Identificar y registrar las entradas y salidas de todas las personas que accedan a los locales donde hay equipamiento que forme parte del sistema de información.		
Competencia profesional			
5.1.2.1	Medio	Concienciación	Entender la necesidad de identificarse cuando se acceda a los locales donde hay equipamiento que forme parte del sistema de información.

Unidad de competencia: Instalaciones alternativas			
5.1.8	Garantizar la existencia y disponibilidad de instalaciones alternativas para poder trabajar en caso de que las instalaciones habituales no estén disponibles.		
Competencia profesional			
5.1.8.1	N.A.	Formación	Conocer la ubicación y la forma de acceso a las instalaciones alternativas para poder trabajar en caso de que las instalaciones habituales no estén disponibles, así como el procedimiento y condiciones de cambio de ubicación.

Unidad de Competencia: Deberes y obligaciones			
5.2.2	Conocer los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.		
Competencia profesional			
5.2.2.1	Medio	Formación	Conocer las medidas disciplinarias en caso de incumplimiento de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.

Unidad de competencia: Personal alternativo			
5.2.5	Garantizar la existencia y disponibilidad de otras personas que se puedan hacer cargo de las funciones en caso de indisponibilidad del personal habitual.		
Competencia profesional			
5.2.5.1	N.A.	Concienciación	Entender la importancia de conocer la existencia y disponibilidad de personas que se puedan hacer cargo de las funciones en caso de indisponibilidad del personal habitual.

Unidad de competencia: Puesto de trabajo despejado			
5.3.1	Asegurar que el puesto de trabajo permanece despejado, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.		
Competencia profesional			
5.3.1.1	Bajo	Concienciación	Entender la necesidad de que su puesto de trabajo permanezca despejado, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.
5.3.1.2	Medio	Concienciación	Entender que el material se guardará en lugar cerrado cuando no se esté utilizando.

Unidad de competencia: Bloqueo de puesto de trabajo			
5.3.2	Bloquear al cabo de un tiempo prudencial de inactividad el puesto de trabajo, requiriendo una nueva autenticación para reanudar la actividad en curso.		
Competencia profesional			
5.3.2.1	Medio	Concienciación	Entender la necesidad de que el puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación para reanudar la actividad en curso.
5.3.2.2	Medio	Concienciación	Entender la necesidad de que pasado un cierto tiempo sin utilizar, se cancelarán las sesiones abiertas desde su puesto de trabajo.

Unidad de competencia: Protección de equipos portátiles			
5.3.3	Proteger adecuadamente los equipos que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente.		
Competencia profesional			
5.3.3.1	Medio	Formación	Conocer el procedimiento para informar de la pérdida o sustracción de un portátil
5.3.3.3	Alto	Concienciación	Entender que cuando el equipo portátil se conecte remotamente a través de redes que no están bajo el estricto control de la universidad, no debe enviarse información confidencial o protegida.
5.3.3.4	Medio	Concienciación	Entender que en el equipo portátil no deben almacenarse información o datos de carácter confidencial o protegido.
5.3.3.6	Alto	Formación	En caso de almacenar información sensible en el equipo, conocer herramientas y técnicas de protección.

Unidad de competencia: Medios alternativos			
5.3.4	Garantizar la existencia y disponibilidad de medios alternativos de tratamiento de la información para el caso de que fallen los medios habituales.		
Competencia profesional			
5.3.4.1	Bajo	Formación	Conocer el procedimiento de acceso a medios alternativos de tratamiento de la información para el caso de que fallen los medios habituales.

Unidad de competencia: Etiquetado			
5.5.1	Entender el significado de las etiquetas de los soportes de información, bien mediante simple inspección, bien mediante el recurso a un repositorio que lo explique.		
Competencia profesional			
5.5.1.1	Bajo	Formación	Conocer el significado de las etiquetas que indiquen el nivel de seguridad de la información, bien mediante simple inspección, bien mediante el recurso a un repositorio que lo explique.
5.5.1.2	Alto	Formación	Conocer el tratamiento y gestión de la información en base a su nivel de seguridad.
5.5.1.3	Medio	Concienciación	Entender la necesidad de clasificar y etiquetar la información respecto a su nivel de seguridad.

Unidad de competencia: Custodia			
5.5.3	Emplear el control de acceso y las exigencias de mantenimiento del fabricante de los soportes de información que permanecen bajo la responsabilidad de la organización.		
Competencia profesional			
5.5.3.1	Medio	Formación	Saber aplicar medidas físicas o lógicas para garantizar el control de acceso a los soportes de información bajo su responsabilidad.
5.5.3.2	N.A.	Concienciación	Entender las necesidad de respetar las exigencias de mantenimiento del fabricante de los soportes de información, en especial, en lo referente a temperatura, humedad y otros agresores medioambientales

Unidad de competencia: Borrado y destrucción			
5.5.5	Garantizar el borrado y destrucción de soportes de información susceptibles de almacenar información.		
Competencia profesional			
5.5.5.1	Medio	Formación	Saber borrar de manera segura los soportes de información que vayan a ser reutilizados para otra información o liberados.
5.5.5.2	Medio	Concienciación	Entender la necesidad de realizar borrados seguros de soportes cuando vayan a ser reutilizados o liberados.
5.5.5.3	Medio	Formación	Conocer el procedimiento de solicitud de destrucción de soportes de información.

Unidad de competencia: Aceptación y puesta en servicio			
5.6.2	Comprobar el correcto funcionamiento de la aplicación antes de su puesta en producción.		
Competencia profesional			
5.6.2.1	N.A.	Formación	Conocer los criterios de aceptación en materia de seguridad en caso de contratación externa.

Unidad de competencia: Calificación de la información			
5.7.2	Calificar, etiquetar y tratar la información en consideración al nivel de seguridad que requiere.		
Competencia profesional			
5.7.2.1	N.A.	Formación	Conocer los criterios para asignar a cada información el nivel de seguridad requerido, y ser responsable de su documentación y aprobación formal.
5.7.2.2	N.A.	Formación	Conocer las políticas y procedimientos que describan en detalle la forma en la que se ha de etiquetar y tratar la información en consideración al nivel de seguridad que requiere
5.7.2.3	N.A.	Concienciación	Entender que como responsable de información, en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad.

Unidad de competencia: Cifrado			
5.7.3	Cifrar la información con un nivel alto en confidencialidad tanto durante su almacenamiento como durante su transmisión.		
Competencia profesional			
5.7.3.1	Medio	Concienciación	Entender que la información con un nivel alto de confidencialidad se cifrará tanto durante su almacenamiento como durante su transmisión. Sólo estará en claro mientras se está haciendo uso de ella.

Unidad de competencia: Firma electrónica			
5.7.4	Emplear la firma electrónica como un instrumento capaz de permitir la comprobación de la autenticidad de la procedencia y la integridad de la información ofreciendo las bases para evitar el repudio.		
Competencia profesional			
5.7.4.1	Alto	Formación	Conocer las políticas, procedimientos y circunstancias de uso de la firma electrónica.
5.7.4.2	Alto	Concienciación	Entender la importancia del buen uso y resguardo de la firma electrónica

Unidad de competencia: Limpieza de documentos			
5.7.6	Retirar de los documentos toda la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.		
Competencia profesional			
5.7.6.1	Alto	Formación	Retirar de la documentación toda la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.
5.7.6.2	Medio	Concienciación	Entender la necesidad de gestionar los metadatos de la documentación que se utilice o genere.

Unidad de competencia: Copias de seguridad (backup)			
5.7.7	Realizar copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente con una antigüedad determinada.		
Competencia profesional			
5.7.7.1	Bajo	Formación	Conocer las políticas y procedimientos de realización de copias de seguridad en su entorno de trabajo.
5.7.7.2	Bajo	Concienciación	Entender la necesidad de realizar copias de seguridad de manera periódica, así como comprobar que han sido bien realizadas.

Unidad de competencia: Protección del correo electrónico			
5.8.1	Proteger frente a las amenazas que le son propias la información distribuida por medio de correo electrónico.		
Competencia profesional			
5.8.1.1	Alto	Formación	Proteger la información de los correos electrónicos, tanto en el cuerpo de los mensajes, como en los anexos.

Unidad de competencia: Medios alternativos			
5.8.4	Garantizar la existencia y disponibilidad de medios alternativos para prestar los servicios en el caso de que fallen los medios habituales.		
Competencia profesional			
5.8.4.1	Bajo	Formación	Conocer la existencia, circunstancias y procedimiento de uso medios alternativos para prestar los servicios en el caso de que fallen los medios habituales
5.8.4.2	Medio	Concienciación	Entender la importancia de conocer los procedimientos de uso de los medios alternativos

Capítulo 6

Conclusiones y aportaciones

"Bien, aquí, queridos amigos, a la orilla del mar, termina por fin nuestra comunidad en la Tierra Media. ¡Id en paz!"

El Señor de los Anillos

6.1. Respuesta a las preguntas de investigación

Tras la exposición de los resultados, a continuación se presenta una revisión de las principales cuestiones que se han planteado a lo largo de la misma, se identifican y repasan sus principales contribuciones, y se proponen futuras líneas de trabajo.

La primera pregunta de investigación, ¿cuál es el estado de la formación y concienciación en seguridad de la información en las universidades españolas? se responde de manera expresa en el capítulo 4, donde se analiza en primer lugar el contexto de la seguridad en las empresas y organizaciones españolas, para a continuación estudiar la situación específica de las universidades. Los datos señalan que el nivel medio de la cultura de la seguridad en las empresas y organizaciones españolas alcanza un 2,8 en una escala de 0 a 5. Esta cifra señala un nivel de madurez poco más que "reproducible", e indica que las actividades de formación y concienciación en seguridad son marginales dentro de la estrategia de las organizaciones, llevándose a cabo de manera aislada y sin objetivos claros ni evaluables.

Respecto a la situación de las universidades españolas, cabe señalar como primera evidencia que el 45 % de las mismas, prácticamente la mitad, no recogen en su presupuesto de seguridad de la información ninguna partida económica destinada a formación y concien-

ciación en seguridad, sea ésta del tipo que sea. Y un 28 % dedica cifras inferiores al 5 %. Estos datos resultan aún más concluyentes si se considera que el presupuesto destinado por las universidades a actividades de formación y concienciación representa tan sólo el 0,2 % del total del presupuesto destinado a TI.

Para profundizar más en la realidad que reflejan estas cifras, también se presentan los niveles de madurez de las universidades españolas referidos a los niveles de cumplimiento de las medidas de seguridad "Formación" y "Concienciación" del ENS, donde se aprecian las notables diferencias entre los valores obtenidos por las universidades y los valores objetivo. A modo de ejemplo, para la categoría media, el nivel de cumplimiento es del 30 % para las actividades de concienciación y del 25 % para las referidas a formación. Sin embargo, el valor objetivo, es decir, el porcentaje de cumplimiento que debiera obtenerse, es del 80 %.

Estos datos permiten constatar el escaso nivel de desarrollo de las actividades de formación y concienciación en seguridad de las universidades españolas, y ayudan a comprender y contextualizar tanto el problema que aborda esta tesis como la necesidad de explorar iniciativas que ayuden a mitigarlo.

La segunda y tercera preguntas de investigación, ¿qué medidas de seguridad del ENS aplican en un mapa funcional de competencias de usuarios y usuarias no TIC de las universidades españolas? y ¿cuáles son las actitudes y conocimientos asociadas a las medidas de seguridad identificadas? tienen respuesta en el mapa funcional que se presenta en el capítulo 5. El mapa funcional recoge los elementos de competencia, es decir, lo que el trabajador o trabajadora no TIC debe conocer, entender o saber hacer respecto a la seguridad de la información en su puesto de trabajo de la universidad.

La cuarta pregunta, ¿qué perfiles de usuarios y usuarias no TIC pueden establecerse según sus necesidades en el ámbito de la seguridad de la información para su puesto de trabajo y responsabilidad? también se responde en el capítulo 5. Allí se desarrolla el proceso de identificación y creación de los grupos de perfiles laborales que compilan las diferentes necesidades y requisitos de seguridad. Los perfiles establecidos por el panel de expertos y expertas son los siguientes: Personal Docente e Investigador, Jefatura PAS, Puesto Base

PAS, Consejeras y Consejeros externos y Dirección.

Obtenido un primer borrador del mapa de competencias, se lleva a cabo un análisis clúster para confirmar si los expertos y expertas perciben diferencias significativas entre los perfiles identificados, determinadas por los diferentes niveles de desempeños asociados a las competencias. El análisis clúster descubre que, a la vista de sus respuestas, no advierten diferencias relevantes entre los perfiles de Jefatura PAS y Dirección, de modo que se agrupan en un único perfil, identificado como Dirección. Por tanto, los perfiles finales resultantes son: Personal Docente e Investigador, Puesto Base PAS, Consejeros externos y Dirección.

Finalmente, la quinta pregunta, ¿cuál es el mapa de competencias derivado del mapa funcional construido y en qué grado aplican los conocimientos y actitudes para cada uno de los roles definidos? se responde con la construcción del mapa de competencias, donde para cada perfil laboral identificado se señalan las competencias que le aplican y el correspondiente nivel de desempeño que debe alcanzarse.

Todas estas respuestas permiten responder a la pregunta principal planteada en esta tesis: ¿cuáles son las competencias y su nivel de desempeño en el ámbito de la seguridad de la información para cada perfil laboral universitario no TIC?

Así mismo, y derivado de estas respuestas, se satisfacen y cumplen tanto el objetivo general planteado en esta tesis como los objetivos específicos.

6.2. Contribuciones principales

Un aporte sustancial de esta tesis es la creación del primer mapa de competencias laborales en seguridad de la información para el personal no TIC de las universidades españolas.

Esta mapa de competencias proporciona a las universidades un instrumento común de trabajo de suma utilidad para disponer de un referente respecto a qué competencias en el dominio de la seguridad de la información debe conocer y ser capaz de realizar su personal no TIC, así como contar con un instrumento que les permita conocer y evaluar dichas competencias. Se superan de este modo, tanto los inconvenientes que presentan los modelos de formación generalistas y en consecuencia no adaptados a la realidad de las

universidades, como las barreras que presentan los elevados costes en recursos y tiempo asociados a la creación desde cero de mapas específicos. Así mismo, al organizar el mapa de competencias en dos apartados, uno de ellos formado por las competencias identificadas como comunes y esenciales a todos los perfiles, se facilitan las labores de formación y concienciación básicas y necesarias.

También ofrece a la comunidad universitaria española un mapa de competencias común dentro del alcance definido, que favorece y posibilita compartir esfuerzos y recursos destinados a la elaboración de procesos de formación y concienciación y abre el camino a trabajar en un estándar de competencia, entendido como "un proceso de acuerdo entre empresas, trabajadores e instituciones públicas con el propósito de establecer un estándar sobre las competencias que son representativas de una determinada ocupación o área ocupacional" (Vargas et al., 2001).

Otra importante ventaja que presenta el mapa de competencias propuesto es la posibilidad de adaptarlo a las necesidades específicas de cada universidad. Con el empleo de la metodología planteada en esta tesis, no sólo es posible, sino que también resulta recomendable, que se establezcan ajustes tanto en las competencias definidas como en los roles identificados o en los niveles de desempeño establecidos.

Desde el punto de vista de los trabajadores y trabajadoras, este mapa les proporciona un conocimiento claro de qué es lo que deben conocer y qué se espera de ellos y ellas respecto a la seguridad de la información en el desempeño de sus funciones laborales.

Otro de los aportes de esta tesis al cuerpo de conocimiento es el empleo de las medidas de seguridad recogidas en el Anexo II del ENS en el Análisis Funcional realizado. Esto permite que el papel habitual de los expertos y expertas se sustituya en primera instancia por las setenta y cinco medidas de seguridad señaladas por el ENS. Este enfoque asegura razonablemente que "desde el diseño" se contemplan todos los ámbitos de la seguridad de la información, al establecerse una relación directa e inequívoca entre las medidas de seguridad señaladas en la ley y las competencias que en el dominio de la seguridad de la información debe demostrar el personal universitario no TIC.

6.3. Mejoras propuestas y líneas futuras de trabajo

Este trabajo puede considerarse pionero tanto en la creación del primer mapa de competencias en el alcance definido como en su planteamiento metodológico, proponiendo la sustitución de un conocimiento experto específico, limitado y costoso, por los contenidos y propuestas de lo que puede considerarse un estándar de seguridad en España. Este carácter pionero permite que las mejoras sobre el propio modelo presentado y las posibles líneas de trabajo sean muy amplias.

De acuerdo con los procesos competenciales explicados en la página 78 y siguientes, la primera propuesta de mejora que conviene señalar es la de obtener los criterios de evaluación de las competencias identificadas y completar el proceso de normalización. De este modo, se puede abordar en fases futuras los procesos de formación, evaluación y certificación. En otras palabras, esta tesis identifica y desarrolla lo que la persona debe conocer, entender y ser capaz de hacer. Los siguientes pasos deben ir encaminados a desarrollar la forma en que la persona adquiere ese conocimiento y concienciación, establecer cómo puede juzgarse si lo que conoce, entiende y hace está bien hecho y hasta qué punto, y finalmente certificar ese conocimiento.

Sería también conveniente llevar a cabo procedimientos de validación del mapa propuesto. Un modo de llevarlo a cabo podría ser mediante una validación por expertos y expertas. En esta línea, dentro de la iniciativa UniDigital, proyecto del Ministerio de Universidades que tiene como objetivos la innovación, la transformación y la modernización de las universidades desde el ámbito digital, un grupo formado por más de una docena de universidades españolas ha preparado un pliego para la creación de campañas de formación y concienciación basadas en los requisitos del nuevo ENS y dirigidas tanto al personal como a estudiantes. Una iniciativa en la línea de lo propuesto y desarrollado en esta tesis, y que de alguna manera lo corrobora y avala.

En las tareas iniciales de la investigación, el equipo de trabajo estimó que en esta primera investigación no era oportuno incluir en el análisis las categorías de los sistemas de información presentados en el capítulo 2. Se consideró que el estudio debía abarcar la totalidad de las medidas de seguridad, independientemente de que algunas de ellas sólo estuvieran

dirigidas a sistemas de categoría media o alta. Sin embargo, finalizada esta primera versión del mapa, seria interesante reflexionar cómo puede mejorar el mapa de competencias el empleo de las categorías definidas en el Anexo II del ENS.

Como ya se ha señalado, esta tesis abre una línea de investigación en el ámbito metodológico al proponer el empleo de estándares y marcos de la industria en la confección de mapas de competencia. Probada la validez de este planteamiento, otra interesante iniciativa sería emplear los controles de la ISO 27002. Dado el amplio uso de estas normas internacionales, la aplicación de la misma metodología utilizada en esta tesis posibilitaría la obtención de mapas de competencia en seguridad de la información específicos de cualquier sector, industria o país.

Otra línea de interés es la integración del mapa de competencias obtenido en un LMS o Sistema de Gestión del Aprendizaje. Esta línea de trabajo presenta varias ventajas, entre las que se pueden destacar las siguientes:

- Un LMS proporciona un sistema jerárquico en el que se pueden describir y relacionar los distintos elementos que lo componen, lo que facilita su comprensión y seguimiento dentro de un itinerario formativo.
- El registro de evidencias necesario en todo proceso de formación, normalización y certificación se ve facilitado por la automatización intrínseca de un LMS.
- La integración con otros sistemas de gestión posibilita que la formación y concienciación en la seguridad de la información se integre en los recursos humanos de la organización, lo que favorece la tan necesaria cultura de la seguridad.

Otra tarea que es necesario abordar es la adecuación de los resultados obtenidos al nuevo ENS. Esta tesis se ha basado en el Real Decreto 3/2010, de 8 de enero, que regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Sin embargo, con fecha 3 de mayo de 2022, se ha publicado el Real Decreto 311/2022, que presenta el nuevo ENS (BOE, 2022b).

Las diferencias son escasas. De manera muy resumida, sin considerar algunas correcciones menores en los nombres y el ajuste de la medida “op.ext.9 Medios alternativos” al apartado

"Continuidad del Servicio" con el identificativo "op.cont.4", los cambios se ciñen a la supresión de diez medidas de seguridad y a la implantación de ocho medidas nuevas. En el Anexo L se pueden apreciar las medidas eliminadas, marcadas en color naranja, y las nuevas medidas, en color azul.

En esta misma línea, también se debe también considerar la Guía CCN-STIC-881 de Adecuación al ENS para Universidades, publicada por el CCN en febrero de 2022.

La realización de esta tesis y las líneas de trabajo sugeridas responden al reto de aportar propuestas innovadoras en la definición de marcos de competencias en el dominio de la seguridad de la información, con el objetivo último de ayudar a proteger y salvaguardar los sistemas de información de las universidades españolas a través de las tan necesarias actividades de formación y concienciación dirigidas el personal no TIC de las universidades. Es un campo de escaso y sin embargo necesario desarrollo, al que las propuestas de esta tesis aspiran a contribuir.

Capítulo 7

Anexos

7.1. Anexo A: Marco legal y jurídico

Año	Tipo	Normativa	Comentario	Situación
1978		Constitución Española		Vigente
1992	Procedimiento administrativo	Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las AAPP y del Procedimiento Administrativo Común.	Primera referencia a la necesidad de utilizar por parte de las Administraciones Públicas medios informáticos.	Derogada por la Ley 39/2015.
1992	Privacidad	Ley Orgánica 5/1992, de 29 de octubre.	Primera ley que preserva el derecho a la protección de datos y a la intimidad. Establece la AEPD	Derogada por la Ley Orgánica 15/1999
1999	Privacidad	Ley Orgánica 15/1999, de 13 de diciembre.	Garantiza y protege, en lo que concierne al tratamiento de los datos personales, los derechos fundamentales de las personas físicas.	Derogada por la Ley Orgánica 3/2018
2007	Procedimiento administrativo	Ley 11/2007, de 22 de junio	Se basa en el derecho de los ciudadanos a utilizar los medios de comunicación electrónica para relacionarse con las AAPP y ejercer sus derechos.	Derogada por la Ley 39/2015

Continúa en la página siguiente

Año	Tipo	Normativa	Comentario	Situación
2009	Procedimiento administrativo	Real Decreto 1671/2009, de 6 de noviembre.	Desarrolla ley 11/2007, de 22 de junio.	Derogada parcialmente por las leyes 39/2015 y 40/2015
2010	Seguridad	Real Decreto 3/2010, de 8 de enero	Se regula el Esquema Nacional de Seguridad	Modificada por el Real Decreto 951/2015
2015	Procedimiento administrativo	Ley 39/2015, de 1 de octubre.	Primera referencia a la necesidad de proteger los datos de carácter personal	Vigente
2015	Procedimiento administrativo	Ley 40/2015, de 1 de octubre.	Explicita la obligación de garantizar la protección de los datos de carácter personal	Vigente
2015	Seguridad	Real Decreto 951/2015.	Actualización del ENS	Vigente
2016	Privacidad	Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.	Establece las normas relativas a la protección de las personas físicas respecto al tratamiento de los datos personales y las normas relativas a su libre circulación	Vigente
2018	Privacidad	Ley Orgánica 3/2018, de 5 de diciembre.	Adapta la legislación española al RGPD	Vigente

7.2. Anexo B: Serie ISO 27000

Norma	Descripción
27000	Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge las definiciones de la serie de normas 27000, explica por qué es importante la implantación de un SGSI, y describe los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI.
27001	Es la norma principal de la serie y contiene los requisitos del SGSI. Es la norma con arreglo a la cual se certifican las organizaciones.
27002	Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables. La versión 2022 contiene 93 controles, divididos en cuatro cláusulas.
27003	Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo con la ISO/IEC 27001. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI.
27004	Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.
27005	Proporciona directrices para la gestión de riesgos en la seguridad de la información.
27006	Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.
27007	Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011.
27008	Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.
27009	Define los requisitos para el uso de la norma ISO/IEC 27001 en cualquier sector específico (campo, área de aplicación o sector industrial). El documento explica cómo refinar e incluir requisitos adicionales a los de la norma ISO/IEC 27001.
27010	Guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores.
27032	Proporciona orientación sobre la seguridad cibernética, identificando sus características específicas y de su relación con otros dominios de seguridad.

7.3. Anexo C: Correos enviados durante la investigación

Correo de presentación

Buenos días

¿Qué tal estás? Espero que no hayáis tenido ningún problema de salud, y que estéis llevando lo mejor posible este confinamiento. Y en la universidad imagino que estarás como nosotros, teletrabajando y metiendo más horas que en presencial :-)

Me pongo en contacto contigo para ver si me puedes ayudar. Llevo casi un año haciendo la tesis doctoral. Es algo que siempre quise hacer y ahora había encontrado el momento oportuno. El objetivo de la investigación es definir un mapa de competencias en seguridad de la información basado en los controles del ENS para los perfiles académicos y laborales de las universidades españolas.

Es un proyecto que tengo avanzado, y en consecuencia ha llegado el momento de continuarlo con algunos expertos. Y he pensado que nadie mejor que tú. La idea, si fuera posible, es mantener una videoconferencia en la que te presentase el asunto y lo que he diseñado, y que pudieras darme tu opinión experta.

Entiendo que en la situación actual te resultará complicado dedicar tiempo a todo lo que no sea centrarse en el trabajo, pero si fuera posible me harías un favor enorme. Si no pudieras, no te preocupes, lo entenderé perfectamente.

Un abrazo

Correo con la primera iteración del mapa de competencias

Buenos días

Reunidas ya las respuestas que me habéis dado los cinco expertos y expertas, el siguiente paso es conseguir, mediante el consenso, un modelo común. Lo ideal sería el que nos reuniéramos las personas que estamos realizando este estudio hasta alcanzar ese modelo, pero como eso no es viable, y con la idea de molestaros lo menos posible, mi idea es llevar a cabo propuestas concretas que, sin mucho esfuerzo por vuestra parte, nos permitan avanzar.

Vuestras respuestas iniciales alcanzan un porcentaje de coincidencia del 47 %. Un porcentaje muy elevado teniendo en cuenta que sois cinco personas. Pero tenemos que alcanzar el 100 %.

El primer paso que propongo para ello es muy sencillo, y creo que no representará demasiado problema. En el fichero adjunto, de las más de 500 respuestas, señalo aquellas en las que ha habido unanimidad en las respuestas del resto de compañeros y compañeras, siendo tu respuesta la única diferente. Para que la vuelvas a repasar y veas si es posible y razonable ajustar tu respuesta y de este modo acercarnos al modelo compartido.

Simplemente debes dar el visto bueno a los ajustes, o indicar si hay respuestas que te gustaría mantener. Si así fuera, la dejaremos para una fase posterior fase de discusión. Por supuesto, si alguna respuesta concreta te provoca dudas de interpretación, estoy a tu entera disposición.

Muchas gracias por tu tiempo y tu ayuda.

Correo con la última iteración del mapa de competencias

Buenos días

Antes de nada, agradeceros vuestro tiempo y ayuda. Me supone un alivio muy grande... y sin duda a vosotros y vosotras aún más saber que este sería el último ajuste que tendríais que hacer :-)

Todos habéis enviado comentarios, aportaciones y dudas que he compartido y anotado cuidadosamente, y que me serán de gran utilidad para contextualizar y explicar en la tesis el trabajo que habéis llevado a cabo. Algunos también habéis expresado la conveniencia de hacer una última reflexión sobre unos pocos valores, veinte en concreto, que pensáis que habría que ajustar, y que os comparto en el documento adjunto. Teniendo en cuenta que empezamos con más de 500.

No he incluído, para no alargar el trabajo, alguna propuesta que aceptaba el valor inicial, aunque sugería otro diferente.

Sobre cómo proceder... en el adjunto se recogen las propuestas de cambio, así como vuestras explicaciones al respecto. Así que podríamos empezar bajo el supuesto de aceptación de

esos cambios. A partir de ahí, si alguien tiene otra opinión con alguno de ellos, en este mismo hilo podría compartirla, y el resto podéis dar vuestro parecer. Si vemos que no llegamos aun consenso, procederíamos a hacer una videoconferencia.

Una vez más daros las gracias por vuestra ayuda, y pediros disculpas por robaros vuestro tiempo.

7.4. Anexo D: Esfuerzo en concienciación y formación

Porcentaje del presupuesto de TI dedicado a la seguridad	Porcentaje del presupuesto de seguridad dedicado a formación y concienciación	Porcentaje del presupuesto de TI destinado a formación y concienciación
4	1	0,04
4	1	0,04
4	1	0,04
2	2	0,04
5	1	0,05
1	5	0,05
3	2	0,06
8	1	0,08
8	1	0,08
10	1	0,10
2	5	0,10
3	5	0,15
3	5	0,15
10	2	0,20
21	1	0,21
3	10	0,30
8	4	0,32
4	8	0,32
2	16	0,32
20	2	0,40
8	5	0,40
10	5	0,50
13	4	0,52
9	8	0,72
17	5	0,85
15	8	1,20
6	20	1,20

7.5. Anexo E. Resultados iniciales

Código	Grupo	Experto/a 1	Experto/a 2	Experto/a 3	Experto/a 4	Experto/a 5	Nivel
3.1.0.1	1	3	3	3	3	3	3
3.1.0.1	2	3	3	3	3	3	3
3.1.0.1	3	3	3	3	3	3	3
3.1.0.1	4	3	2	2	3	3	-
3.1.0.1	5	3	3	3	3	3	3
3.1.0.2	1	2	3	3	2	3	-
3.1.0.2	2	3	3	3	3	3	3
3.1.0.2	3	1	3	3	1	3	-
3.1.0.2	4	1	2	2	1	2	-
3.1.0.2	5	3	3	3	3	3	3
3.1.0.3	1	3	3	3	3	3	3
3.1.0.3	2	3	3	3	3	3	3
3.1.0.3	3	2	3	3	2	3	-
3.1.0.3	4	3	3	3	3	3	3
3.1.0.3	5	3	3	3	3	3	3
3.1.0.4	1	1	3	2	1	3	-
3.1.0.4	2	3	3	2	3	3	-
3.1.0.4	3	1	3	2	1	3	-
3.1.0.4	4	1	3	2	1	3	-
3.1.0.4	5	3	3	3	3	3	3
3.2.0.1	1	3	3	3	3	3	3
3.2.0.1	2	3	3	3	3	3	3
3.2.0.1	3	2	3	3	2	3	-
3.2.0.1	4	1	2	3	1	3	-
3.2.0.1	5	3	3	3	3	3	3
3.2.0.2	1	3	3	3	3	3	3
3.2.0.2	2	3	3	3	3	3	3
3.2.0.2	3	2	3	3	2	3	-
3.2.0.2	4	1	2	3	1	3	-
3.2.0.2	5	3	3	3	3	3	3
3.2.0.3	1	3	3	3	3	3	3
3.2.0.3	2	3	3	3	3	3	3
3.2.0.3	3	3	3	3	3	3	3
3.2.0.3	4	3	3	3	3	3	3
3.2.0.3	5	3	3	3	3	3	3
3.2.0.4	1	2	3	3	2	3	-
3.2.0.4	2	3	3	3	3	3	3
3.2.0.4	3	2	3	3	2	3	-
3.2.0.4	4	2	3	3	2	3	-
3.2.0.4	5	3	3	3	3	3	3
3.3.0.1	1	3	3	3	3	3	3
3.3.0.1	2	3	3	3	3	3	3
3.3.0.1	3	2	3	3	2	3	-
3.3.0.1	4	2	2	3	2	2	-

Continúa en la página siguiente

Codigo	Grupo	Exp. 1	Exp. 2	Exp. 3	Exp. 4	Exp. 5	Nivel
3.3.0.1	5	3	3	3	3	3	3
3.3.0.2	1	2	3	3	2	3	-
3.3.0.2	2	3	3	3	3	3	3
3.3.0.2	3	2	3	3	2	3	-
3.3.0.2	4	1	2	3	1	3	-
3.3.0.2	5	3	3	3	3	3	3
3.3.0.3	1	2	3	3	2	3	-
3.3.0.3	2	3	3	3	3	3	3
3.3.0.3	3	2	3	3	2	3	-
3.3.0.3	4	1	3	3	1	3	-
3.3.0.3	5	3	3	3	3	3	3
3.3.0.4	1	2	3	3	2	3	-
3.3.0.4	2	3	3	3	3	3	3
3.3.0.4	3	2	3	3	2	3	-
3.3.0.4	4	1	2	3	1	3	-
3.3.0.4	5	3	3	3	3	3	3
3.4.0.1	1	3	3	1	3	3	-
3.4.0.1	2	3	3	3	3	3	3
3.4.0.1	3	2	1	1	2	1	-
3.4.0.1	4	1	1	1	1	1	1
3.4.0.1	5	3	3	1	3	3	-
4.1.1.1	1	2	2	3	2	2	-
4.1.1.1	2	3	2	3	3	3	-
4.1.1.1	3	1	0	1	1	1	-
4.1.1.1	4	1	0	1	1	1	-
4.1.1.1	5	3	3	3	3	3	3
4.1.1.2	1	1	3	1	1	1	-
4.1.1.2	2	3	3	3	3	3	3
4.1.1.2	3	1	2	1	1	1	-
4.1.1.2	4	2	2	1	2	2	-
4.1.1.2	5	3	3	3	3	3	3
4.2.1.1	1	3	2	3	3	3	-
4.2.1.1	2	3	3	3	3	3	3
4.2.1.1	3	3	2	3	3	3	-
4.2.1.1	4	3	0	3	3	3	-
4.2.1.1	5	3	3	3	3	3	3
4.2.1.2	1	3	3	3	3	3	3
4.2.1.2	2	3	3	3	3	3	3
4.2.1.2	3	3	3	3	3	3	3
4.2.1.2	4	3	3	3	3	0	-
4.2.1.2	5	3	3	3	3	3	3
4.2.1.3	1	3	2	3	3	3	-
4.2.1.3	2	3	3	3	3	3	3
4.2.1.3	3	3	2	3	3	3	-
4.2.1.3	4	3	0	3	3	3	-

Continúa en la página siguiente

Codigo	Grupo	Exp. 1	Exp. 2	Exp. 3	Exp. 4	Exp. 5	Nivel
4.2.1.3	5	3	3	3	3	3	3
4.2.2.1	1	2	2	1	2	2	-
4.2.2.1	2	3	3	3	3	3	3
4.2.2.1	3	2	1	1	2	2	-
4.2.2.1	4	2	1	1	2	1	-
4.2.2.1	5	3	3	3	3	3	3
4.2.2.2	1	1	2	1	1	1	-
4.2.2.2	2	3	3	3	3	3	3
4.2.2.2	3	1	1	1	1	3	-
4.2.2.2	4	1	1	1	1	0	-
4.2.2.2	5	3	3	3	3	3	3
4.2.4.1	1	1	3	2	1	3	-
4.2.4.1	2	3	3	3	3	3	3
4.2.4.1	3	1	2	2	1	2	-
4.2.4.1	4	1	2	2	1	1	-
4.2.4.1	5	3	3	3	3	3	3
4.2.4.2	1	1	2	2	1	2	-
4.2.4.2	2	3	3	3	3	3	3
4.2.4.2	3	1	1	2	1	1	-
4.2.4.2	4	1	1	2	1	1	-
4.2.4.2	5	3	3	3	3	3	3
4.2.5.1	1	3	3	3	3	3	3
4.2.5.1	2	3	3	3	3	3	3
4.2.5.1	3	3	3	3	3	3	3
4.2.5.1	4	3	3	3	3	3	3
4.2.5.1	5	3	3	3	3	3	3
4.2.5.2	1	3	3	3	3	3	3
4.2.5.2	2	3	3	3	3	3	3
4.2.5.2	3	3	3	3	3	3	3
4.2.5.2	4	3	3	3	3	3	3
4.2.5.2	5	3	3	3	3	3	3
4.2.5.3	1	3	3	3	3	3	3
4.2.5.3	2	3	3	3	3	3	3
4.2.5.3	3	3	3	3	3	3	3
4.2.5.3	4	3	2	3	3	3	-
4.2.5.3	5	3	3	3	3	3	3
4.2.6.1	1	2	3	3	2	3	-
4.2.6.1	2	3	3	3	3	3	3
4.2.6.1	3	1	3	3	1	3	-
4.2.6.1	4	1	3	3	1	0	-
4.2.6.1	5	3	3	3	3	3	3
4.2.6.2	1	3	3	3	3	3	3
4.2.6.2	2	3	3	3	3	3	3
4.2.6.2	3	3	3	3	3	3	3
4.2.6.2	4	3	3	3	3	0	-

Continúa en la página siguiente

Codigo	Grupo	Exp. 1	Exp. 2	Exp. 3	Exp. 4	Exp. 5	Nivel
4.2.6.2	5	3	3	3	3	3	3
4.2.6.3	1	3	3	3	3	3	3
4.2.6.3	2	3	3	3	3	3	3
4.2.6.3	3	3	3	3	3	3	3
4.2.6.3	4	3	3	3	3	3	3
4.2.6.3	5	3	3	3	3	3	3
4.2.6.4	1	3	3	3	3	3	3
4.2.6.4	2	3	3	3	3	3	3
4.2.6.4	3	3	3	3	3	3	3
4.2.6.4	4	3	3	3	3	3	3
4.2.6.4	5	3	3	3	3	3	3
4.2.6.5	1	3	3	3	3	3	3
4.2.6.5	2	3	3	3	3	3	3
4.2.6.5	3	3	3	3	3	3	3
4.2.6.5	4	3	3	3	3	3	3
4.2.6.5	5	3	3	3	3	3	3
4.2.7.1	1	3	3	3	3	3	3
4.2.7.1	2	3	3	3	3	3	3
4.2.7.1	3	2	1	3	2	3	-
4.2.7.1	4	2	2	1	2	2	-
4.2.7.1	5	3	3	3	3	3	3
4.2.7.2	1	3	3	3	3	3	3
4.2.7.2	2	3	3	3	3	3	3
4.2.7.2	3	3	3	3	3	3	3
4.2.7.2	4	3	3	3	3	0	-
4.2.7.2	5	3	3	3	3	3	3
4.2.7.3	1	3	3	3	3	3	3
4.2.7.3	2	3	3	3	3	3	3
4.2.7.3	3	2	1	3	2	3	-
4.2.7.3	4	2	2	1	2	2	-
4.2.7.3	5	3	3	3	3	3	3
4.2.7.4	1	3	3	3	3	3	3
4.2.7.4	2	3	3	3	3	3	3
4.2.7.4	3	3	1	3	3	3	-
4.2.7.4	4	3	2	1	3	0	-
4.2.7.4	5	3	3	3	3	3	3
4.3.01.1	1	2	2	3	2	2	-
4.3.01.1	2	3	3	3	3	3	3
4.3.01.1	3	2	1	3	2	3	-
4.3.01.1	4	2	1	3	2	0	-
4.3.01.1	5	3	3	3	3	3	3
4.3.01.2	1	2	2	1	2	2	-
4.3.01.2	2	3	3	1	3	3	-
4.3.01.2	3	1	1	1	1	1	1
4.3.01.2	4	1	1	0	1	1	-

Continúa en la página siguiente

Codigo	Grupo	Exp. 1	Exp. 2	Exp. 3	Exp. 4	Exp. 5	Nivel
4.3.01.2	5	3	3	1	3	3	-
4.3.02.1	1	2	2	3	2	3	-
4.3.02.1	2	3	3	3	3	3	3
4.3.02.1	3	1	1	3	1	1	-
4.3.02.1	4	1	1	3	1	1	-
4.3.02.1	5	3	3	3	3	3	3
4.3.03.1	1	2	2	3	2	2	-
4.3.03.1	2	3	3	3	3	3	3
4.3.03.1	3	1	1	3	1	1	-
4.3.03.1	4	1	1	3	1	1	-
4.3.03.1	5	3	3	3	3	3	3
4.3.04.1	1	1	2	2	1	2	-
4.3.04.1	2	2	2	2	2	3	-
4.3.04.1	3	1	1	2	1	1	-
4.3.04.1	4	1	1	2	1	1	-
4.3.04.1	5	2	1	2	2	2	-
4.3.04.2	1	3	3	3	3	3	3
4.3.04.2	2	3	3	3	3	3	3
4.3.04.2	3	3	3	3	3	3	3
4.3.04.2	4	3	3	3	3	3	3
4.3.04.2	5	3	3	3	3	3	3
4.3.06.1	1	3	3	3	3	3	3
4.3.06.1	2	3	3	3	3	3	3
4.3.06.1	3	3	3	3	3	3	3
4.3.06.1	4	3	3	3	3	3	3
4.3.06.1	5	3	3	3	3	3	3
4.3.06.2	1	3	3	3	3	3	3
4.3.06.2	2	3	3	3	3	3	3
4.3.06.2	3	3	3	3	3	3	3
4.3.06.2	4	3	3	3	3	3	3
4.3.06.2	5	3	3	3	3	3	3
4.3.07.1	1	3	3	3	3	3	3
4.3.07.1	2	3	3	3	3	3	3
4.3.07.1	3	3	3	3	3	3	3
4.3.07.1	4	3	3	3	3	3	3
4.3.07.1	5	3	3	3	3	3	3
4.3.07.2	1	2	3	3	2	3	-
4.3.07.2	2	3	3	3	3	3	3
4.3.07.2	3	2	3	3	2	3	-
4.3.07.2	4	2	3	3	2	3	-
4.3.07.2	5	3	3	3	3	3	3
4.3.08.1	1	2	3	3	2	3	-
4.3.08.1	2	3	3	3	3	3	3
4.3.08.1	3	1	3	3	1	3	-
4.3.08.1	4	1	3	3	1	3	-

Continúa en la página siguiente

Codigo	Grupo	Exp. 1	Exp. 2	Exp. 3	Exp. 4	Exp. 5	Nivel
4.3.08.1	5	3	3	3	3	3	3
4.3.11.1	1	3	3	3	3	3	3
4.3.11.1	2	3	3	3	3	3	3
4.3.11.1	3	3	3	3	3	3	3
4.3.11.1	4	3	3	3	3	3	3
4.3.11.1	5	3	3	3	3	3	3
4.3.11.2	1	3	3	3	3	3	3
4.3.11.2	2	3	3	3	3	3	3
4.3.11.2	3	3	3	3	3	3	3
4.3.11.2	4	3	3	3	3	3	3
4.3.11.2	5	3	3	3	3	3	3
4.4.1.1	1	1	2	1	1	1	-
4.4.1.1	2	3	3	3	3	3	3
4.4.1.1	3	1	1	1	1	1	1
4.4.1.1	4	1	0	0	1	0	-
4.4.1.1	5	3	3	3	3	3	3
4.4.1.2	1	0	2	1	0	3	-
4.4.1.2	2	3	3	3	3	3	3
4.4.1.2	3	0	0	1	0	0	-
4.4.1.2	4	0	0	0	0	0	0
4.4.1.2	5	3	3	3	3	3	3
4.4.2.1	1	0	2	1	0	0	-
4.4.2.1	2	3	3	3	3	3	3
4.4.2.1	3	0	1	1	0	1	-
4.4.2.1	4	0	0	0	0	1	-
4.4.2.1	5	3	3	3	3	3	3
4.4.2.2	1	2	2	1	2	2	-
4.4.2.2	2	3	3	3	3	3	3
4.4.2.2	3	1	2	1	1	1	-
4.4.2.2	4	1	1	0	1	1	-
4.4.2.2	5	3	3	3	3	3	3
4.5.1.1	1	3	2	1	3	1	-
4.5.1.1	2	3	3	3	3	3	3
4.5.1.1	3	3	0	1	3	1	-
4.5.1.1	4	3	0	0	3	0	-
4.5.1.1	5	3	3	3	3	3	3
4.5.1.2	1	3	2	3	3	3	-
4.5.1.2	2	3	3	3	3	3	3
4.5.1.2	3	3	0	3	3	3	-
4.5.1.2	4	3	0	0	3	0	-
4.5.1.2	5	3	3	3	3	3	3
4.5.1.3	1	2	2	0	2	2	-
4.5.1.3	2	3	3	3	3	3	3
4.5.1.3	3	2	0	0	2	2	-
4.5.1.3	4	1	0	0	1	0	-

Continúa en la página siguiente

Codigo	Grupo	Exp. 1	Exp. 2	Exp. 3	Exp. 4	Exp. 5	Nivel
4.5.1.3	5	3	3	3	3	3	3
4.5.2.1	1	3	2	1	3	3	-
4.5.2.1	2	3	3	3	3	3	3
4.5.2.1	3	3	2	1	3	3	-
4.5.2.1	4	3	0	0	3	0	-
4.5.2.1	5	3	3	3	3	3	3
4.5.2.2	1	3	2	2	3	3	-
4.5.2.2	2	3	3	3	3	3	3
4.5.2.2	3	3	2	2	3	3	-
4.5.2.2	4	3	0	0	3	0	-
4.5.2.2	5	3	3	3	3	3	3
4.5.3.1	1	2	2	0	2	2	-
4.5.3.1	2	3	3	3	3	3	3
4.5.3.1	3	1	2	1	1	1	-
4.5.3.1	4	1	0	0	1	0	-
4.5.3.1	5	3	3	3	3	3	3
5.1.1.1	1	3	2	2	3	3	-
5.1.1.1	2	3	2	2	3	3	-
5.1.1.1	3	3	2	2	3	3	-
5.1.1.1	4	3	2	2	3	3	-
5.1.1.1	5	3	2	2	3	3	-
5.1.2.1	1	3	2	2	3	3	-
5.1.2.1	2	3	2	2	3	3	-
5.1.2.1	3	3	2	2	3	3	-
5.1.2.1	4	3	2	2	3	3	-
5.1.2.1	5	3	2	2	3	3	-
5.1.2.2	1	3	3	1	3	3	-
5.1.2.2	2	3	3	1	3	3	-
5.1.2.2	3	3	3	1	3	3	-
5.1.2.2	4	3	3	1	3	3	-
5.1.2.2	5	3	3	1	3	3	-
5.1.8.1	1	2	2	1	2	2	-
5.1.8.1	2	3	2	2	3	3	-
5.1.8.1	3	1	2	1	1	1	-
5.1.8.1	4	1	2	0	1	0	-
5.1.8.1	5	3	2	2	3	3	-
5.2.1.1	1	3	3	3	3	3	3
5.2.1.1	2	3	3	3	3	3	3
5.2.1.1	3	3	3	3	3	3	3
5.2.1.1	4	3	2	3	3	3	-
5.2.1.1	5	3	3	3	3	3	3
5.2.2.1	1	3	3	2	3	3	-
5.2.2.1	2	3	3	2	3	3	-
5.2.2.1	3	3	3	2	3	3	-
5.2.2.1	4	3	3	1	3	3	-

Continúa en la página siguiente

Codigo	Grupo	Exp. 1	Exp. 2	Exp. 3	Exp. 4	Exp. 5	Nivel
5.2.2.1	5	3	3	2	3	3	-
5.2.2.2	1	3	3	3	3	3	3
5.2.2.2	2	3	3	3	3	3	3
5.2.2.2	3	3	3	3	3	3	3
5.2.2.2	4	3	3	2	3	3	-
5.2.2.2	5	3	3	3	3	3	3
5.2.2.3	1	3	3	3	3	3	3
5.2.2.3	2	3	3	3	3	3	3
5.2.2.3	3	3	3	3	3	3	3
5.2.2.3	4	3	3	3	3	3	3
5.2.2.3	5	3	3	3	3	3	3
5.2.5.1	1	1	0	1	1	1	-
5.2.5.1	2	2	3	1	3	3	-
5.2.5.1	3	1	0	1	1	1	-
5.2.5.1	4	0	0	1	2	0	-
5.2.5.1	5	3	3	2	3	3	-
5.3.1.1	1	2	2	2	2	3	-
5.3.1.1	2	2	2	2	3	2	-
5.3.1.1	3	2	2	2	1	2	-
5.3.1.1	4	2	2	1	1	1	-
5.3.1.1	5	2	2	2	3	2	-
5.3.1.2	1	2	2	2	2	3	-
5.3.1.2	2	2	2	2	3	2	-
5.3.1.2	3	2	2	2	2	3	-
5.3.1.2	4	2	2	1	2	2	-
5.3.1.2	5	2	2	2	3	2	-
5.3.2.1	1	3	3	3	3	3	3
5.3.2.1	2	3	3	3	3	3	3
5.3.2.1	3	3	3	3	3	3	3
5.3.2.1	4	2	2	3	3	3	-
5.3.2.1	5	3	3	3	3	3	3
5.3.2.2	1	2	2	2	3	2	-
5.3.2.2	2	2	2	2	3	2	-
5.3.2.2	3	2	2	2	3	2	-
5.3.2.2	4	2	2	2	3	2	-
5.3.2.2	5	2	2	2	3	2	-
5.3.3.1	1	2	3	2	3	3	-
5.3.3.1	2	2	3	2	3	3	-
5.3.3.1	3	2	3	2	3	3	-
5.3.3.1	4	2	3	2	3	3	-
5.3.3.1	5	2	3	2	3	3	-
5.3.3.2	1	3	3	3	3	3	3
5.3.3.2	2	3	3	3	3	3	3
5.3.3.2	3	3	3	3	3	3	3
5.3.3.2	4	3	3	3	3	3	3

Continúa en la página siguiente

Codigo	Grupo	Exp. 1	Exp. 2	Exp. 3	Exp. 4	Exp. 5	Nivel
5.3.3.2	5	3	3	3	3	3	3
5.3.3.3	1	3	3	3	3	3	3
5.3.3.3	2	3	3	3	3	3	3
5.3.3.3	3	2	2	3	3	3	-
5.3.3.3	4	3	3	3	3	3	3
5.3.3.3	5	3	3	3	3	3	3
5.3.3.4	1	2	2	3	3	3	-
5.3.3.4	2	3	3	3	3	3	3
5.3.3.4	3	2	2	3	3	3	-
5.3.3.4	4	2	2	3	3	3	-
5.3.3.4	5	3	3	3	3	3	3
5.3.3.5	1	3	3	3	3	3	3
5.3.3.5	2	3	3	3	3	3	3
5.3.3.5	3	3	3	3	3	3	3
5.3.3.5	4	3	3	3	3	3	3
5.3.3.5	5	3	3	3	3	3	3
5.3.3.6	1	2	2	3	3	3	-
5.3.3.6	2	3	3	3	3	3	3
5.3.3.6	3	2	2	3	3	3	-
5.3.3.6	4	3	2	3	3	3	-
5.3.3.6	5	3	3	3	3	3	3
5.3.4.1	1	2	2	2	2	2	2
5.3.4.1	2	2	3	2	3	3	-
5.3.4.1	3	2	2	2	2	2	2
5.3.4.1	4	1	2	1	2	2	-
5.3.4.1	5	2	3	2	3	3	-
5.4.2.1	1	3	3	3	3	3	3
5.4.2.1	2	3	3	3	3	3	3
5.4.2.1	3	3	3	3	3	3	3
5.4.2.1	4	3	3	3	3	3	3
5.4.2.1	5	3	3	3	3	3	3
5.4.2.2	1	3	3	3	3	3	3
5.4.2.2	2	3	3	3	3	3	3
5.4.2.2	3	3	3	3	3	3	3
5.4.2.2	4	3	3	3	3	3	3
5.4.2.2	5	3	3	3	3	3	3
5.4.3.1	1	3	3	3	3	3	3
5.4.3.1	2	3	3	3	3	3	3
5.4.3.1	3	3	3	3	3	3	3
5.4.3.1	4	3	3	1	3	3	-
5.4.3.1	5	3	3	3	3	3	3
5.4.3.2	1	3	3	3	3	3	3
5.4.3.2	2	3	3	3	3	3	3
5.4.3.2	3	3	3	3	3	3	3
5.4.3.2	4	3	3	1	3	3	-

Continúa en la página siguiente

Codigo	Grupo	Exp. 1	Exp. 2	Exp. 3	Exp. 4	Exp. 5	Nivel
5.4.3.2	5	3	3	3	3	3	3
5.5.1.1	1	1	2	1	2	2	-
5.5.1.1	2	3	3	2	3	3	-
5.5.1.1	3	2	2	1	2	2	-
5.5.1.1	4	1	2	1	1	1	-
5.5.1.1	5	3	3	1	3	3	-
5.5.1.2	1	2	2	3	3	3	-
5.5.1.2	2	3	3	3	3	3	3
5.5.1.2	3	2	2	3	3	3	-
5.5.1.2	4	3	2	3	3	3	-
5.5.1.2	5	3	3	3	3	3	3
5.5.1.3	1	2	2	1	2	2	-
5.5.1.3	2	2	3	2	3	3	-
5.5.1.3	3	2	2	2	2	2	2
5.5.1.3	4	2	2	2	2	2	2
5.5.1.3	5	3	3	2	3	3	-
5.5.2.1	1	3	3	3	2	3	-
5.5.2.1	2	3	3	3	3	3	3
5.5.2.1	3	3	3	3	2	3	-
5.5.2.1	4	3	3	3	2	3	-
5.5.2.1	5	3	3	3	3	3	3
5.5.2.2	1	3	3	3	3	3	3
5.5.2.2	2	3	3	3	3	3	3
5.5.2.2	3	3	3	3	3	3	3
5.5.2.2	4	3	3	3	3	3	3
5.5.2.2	5	3	3	3	3	3	3
5.5.3.1	1	2	3	2	3	3	-
5.5.3.1	2	2	3	2	3	3	-
5.5.3.1	3	2	3	2	3	3	-
5.5.3.1	4	2	3	2	3	3	-
5.5.3.1	5	3	3	2	3	3	-
5.5.3.2	1	2	1	2	2	2	-
5.5.3.2	2	2	1	2	3	3	-
5.5.3.2	3	1	1	2	2	2	-
5.5.3.2	4	0	1	2	2	3	-
5.5.3.2	5	1	1	2	3	3	-
5.5.5.1	1	2	2	2	3	2	-
5.5.5.1	2	3	3	2	3	3	-
5.5.5.1	3	2	2	2	3	2	-
5.5.5.1	4	2	2	1	3	3	-
5.5.5.1	5	2	2	2	3	2	-
5.5.5.2	1	2	2	2	2	2	2
5.5.5.2	2	3	3	3	3	3	3
5.5.5.2	3	2	2	2	2	2	2
5.5.5.2	4	2	2	2	2	2	2

Continúa en la página siguiente

Codigo	Grupo	Exp. 1	Exp. 2	Exp. 3	Exp. 4	Exp. 5	Nivel
5.5.5.2	5	3	3	3	3	3	3
5.5.5.3	1	2	2	2	3	2	-
5.5.5.3	2	3	3	3	3	3	3
5.5.5.3	3	2	2	2	3	2	-
5.5.5.3	4	2	2	2	3	2	-
5.5.5.3	5	3	2	3	3	3	-
5.6.2.1	1	1	2	1	2	1	-
5.6.2.1	2	2	3	2	3	3	-
5.6.2.1	3	0	0	0	3	0	-
5.6.2.1	4	0	0	0	3	0	-
5.6.2.1	5	2	3	2	3	3	-
5.7.1.1	1	3	3	3	3	3	3
5.7.1.1	2	3	3	3	3	3	3
5.7.1.1	3	3	3	3	3	3	3
5.7.1.1	4	3	3	3	3	3	3
5.7.1.1	5	3	3	3	3	3	3
5.7.1.2	1	3	3	3	3	3	3
5.7.1.2	2	3	3	3	3	3	3
5.7.1.2	3	3	3	3	3	3	3
5.7.1.2	4	3	3	3	3	3	3
5.7.1.2	5	3	3	3	3	3	3
5.7.2.1	1	1	1	1	3	1	-
5.7.2.1	2	3	3	3	3	3	3
5.7.2.1	3	1	0	1	3	3	-
5.7.2.1	4	0	1	0	1	0	-
5.7.2.1	5	3	3	3	3	3	3
5.7.2.2	1	1	1	1	3	1	-
5.7.2.2	2	3	3	3	3	3	3
5.7.2.2	3	0	0	1	3	3	-
5.7.2.2	4	0	1	0	3	3	-
5.7.2.2	5	3	3	3	3	3	3
5.7.2.3	1	1	1	1	1	1	1
5.7.2.3	2	3	3	2	3	3	-
5.7.2.3	3	0	0	0	3	0	-
5.7.2.3	4	0	1	0	1	0	-
5.7.2.3	5	3	3	2	3	3	-
5.7.3.1	1	3	3	2	2	2	-
5.7.3.1	2	3	3	2	3	3	-
5.7.3.1	3	3	3	2	2	3	-
5.7.3.1	4	3	3	2	2	3	-
5.7.3.1	5	3	3	2	3	3	-
5.7.4.1	1	3	3	2	3	3	-
5.7.4.1	2	3	3	3	3	3	3
5.7.4.1	3	3	0	3	3	3	-
5.7.4.1	4	3	3	3	3	3	3

Continúa en la página siguiente

Codigo	Grupo	Exp. 1	Exp. 2	Exp. 3	Exp. 4	Exp. 5	Nivel
5.7.4.1	5	3	3	3	3	3	3
5.7.4.2	1	3	3	3	2	3	-
5.7.4.2	2	3	3	3	3	3	3
5.7.4.2	3	3	0	3	2	3	-
5.7.4.2	4	3	3	3	2	3	-
5.7.4.2	5	3	3	3	3	3	3
5.7.6.1	1	2	2	3	3	3	-
5.7.6.1	2	2	2	3	3	3	-
5.7.6.1	3	2	2	3	3	3	-
5.7.6.1	4	3	2	3	3	3	-
5.7.6.1	5	3	2	3	3	3	-
5.7.6.2	1	2	2	2	3	2	-
5.7.6.2	2	2	2	2	3	2	-
5.7.6.2	3	2	2	2	2	2	2
5.7.6.2	4	3	2	2	2	2	-
5.7.6.2	5	3	2	2	3	3	-
5.7.7.1	1	2	2	2	3	2	-
5.7.7.1	2	2	3	2	3	3	-
5.7.7.1	3	1	1	2	3	3	-
5.7.7.1	4	1	1	2	3	0	-
5.7.7.1	5	3	3	2	3	3	-
5.7.7.2	1	2	2	2	3	2	-
5.7.7.2	2	3	3	2	3	3	-
5.7.7.2	3	2	1	2	3	3	-
5.7.7.2	4	1	1	2	3	3	-
5.7.7.2	5	3	3	2	3	3	-
5.8.1.1	1	2	3	2	3	3	-
5.8.1.1	2	2	3	2	3	3	-
5.8.1.1	3	2	3	2	3	3	-
5.8.1.1	4	3	3	2	3	3	-
5.8.1.1	5	3	3	2	3	3	-
5.8.1.2	1	3	3	3	3	3	3
5.8.1.2	2	3	3	3	3	3	3
5.8.1.2	3	3	3	3	3	3	3
5.8.1.2	4	3	3	3	3	3	3
5.8.1.2	5	3	3	3	3	3	3
5.8.1.3	1	3	3	3	3	3	3
5.8.1.3	2	3	3	3	3	3	3
5.8.1.3	3	3	3	3	3	3	3
5.8.1.3	4	3	3	3	3	3	3
5.8.1.3	5	3	3	3	3	3	3
5.8.1.4	1	3	3	3	3	3	3
5.8.1.4	2	3	3	3	3	3	3
5.8.1.4	3	3	3	3	3	3	3
5.8.1.4	4	3	3	3	3	3	3

Continúa en la página siguiente

Codigo	Grupo	Exp. 1	Exp. 2	Exp. 3	Exp. 4	Exp. 5	Nivel
5.8.1.4	5	3	3	3	3	3	3
5.8.4.1	1	1	2	1	2	3	-
5.8.4.1	2	3	3	2	3	3	-
5.8.4.1	3	1	2	1	2	2	-
5.8.4.1	4	1	2	1	2	2	-
5.8.4.1	5	3	3	2	3	3	-
5.8.4.2	1	2	2	1	3	3	-
5.8.4.2	2	2	3	2	3	3	-
5.8.4.2	3	1	2	1	3	3	-
5.8.4.2	4	2	2	2	3	2	-
5.8.4.2	5	3	3	2	3	3	-

7.6. Anexo F. Primera iteración

Código	Id	Descripción	Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
3.1.0.1	org.1.01	Conocer la política de seguridad de la universidad.	Alto	Alto	Alto	-	Alto
3.1.0.2	org.1.02	Conocer dónde puede consultarse la política de seguridad de la universidad.	-	Alto	-	-	Alto
3.1.0.3	org.1.03	Entender la importancia, significado y objetivos de la política de seguridad.	Alto	Alto	-	Alto	Alto
3.1.0.4	org.1.04	Entender la necesidad de conocer las actualizaciones de la política de seguridad.	-	Alto	-	-	Alto
3.2.0.1	org.2.01	Conocer el uso correcto de los equipos, servicios e instalaciones que utilice en el desempeño de su labor.	Alto	Alto	-	-	Alto
3.2.0.2	org.2.02	Conocer qué se considera uso indebido de los equipos, servicios e instalaciones que utilice en el desempeño de su labor.	Alto	Alto	-	-	Alto
3.2.0.3	org.2.03	Conocer su responsabilidad con respecto al cumplimiento o violación de la política de seguridad: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.	Alto	Alto	Alto	Alto	Alto
3.2.0.4	org.2.04	Entender la importancia del cumplimiento de la normativa de seguridad de la universidad.	-	Alto	-	-	Alto
3.3.0.1	org.3.01	Saber qué tareas en el ámbito de la seguridad de la información debe realizar en el desempeño de su labor.	Alto	Alto	-	Medio	Alto
3.3.0.2	org.3.02	Saber cómo llevar a cabo las tareas habituales en el ámbito de la seguridad de la información en el desempeño de su labor.	-	Alto	-	-	Alto
3.3.0.3	org.3.03	Saber identificar y reportar comportamientos anómalos en el ámbito de la seguridad.	-	Alto	-	-	Alto
3.3.0.4	org.3.04	Entender la importancia de conocer los procedimientos de seguridad en el desempeño de su actividad.	-	Alto	-	-	Alto
3.4.0.1	org.4.01	Conocer el funcionamiento de los procesos de autorización para el uso de los sistemas de información.	Alto	Alto	-	Bajo	Alto

Continúa en la página siguiente

Código	Id	Descripción	Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
4.1.1.1	op.pl.1.01	Identificar y valorar cualitativamente los activos de información más valiosos de su entorno de trabajo.	Medio	Alto	Bajo	Bajo	Alto
4.1.1.2	op.pl.1.02	Conocer la valoración de los sistemas derivados del análisis de riesgos, y el nivel de riesgo asumido.	Bajo	Alto	Bajo	Medio	Alto
4.2.1.1	op.acc.1.01	Utilizar el identificador adecuado para acceder al sistema en el caso de disponer de diferentes roles de forma que siempre queden delimitados privilegios y registros de actividad.	Alto	Alto	Alto	Alto	Alto
4.2.1.2	op.acc.1.02	Entender que se guardará la información de cuándo accede y qué actividad realiza.	Alto	Alto	Alto	Alto	Alto
4.2.1.3	op.acc.1.03	Entender la importancia de utilizar el identificador adecuado.	Alto	Alto	Alto	Alto	Alto
4.2.2.1	op.acc.2.01	Conocer las políticas y procedimiento de establecimiento de derechos de acceso a los recursos de su responsabilidad, ateniéndose a la política y normativa de seguridad del sistema.	Medio	Alto	-	-	Alto
4.2.2.2	op.acc.2.02	Entender la importancia de gestionar los derechos de acceso a los recursos de su responsabilidad, especialmente en los casos de actualización o bajas.	Bajo	Alto	Bajo	Bajo	Alto
4.2.4.1	op.acc.4.01	Comprender que los derechos de acceso se limitan atendiendo a los principios de mínimo privilegio y necesidad de conocer.	-	Alto	-	-	Alto
4.2.4.2	op.acc.4.02	Conocer las políticas y procedimientos para conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable.	-	Alto	Bajo	Bajo	Alto
4.2.5.1	op.acc.5.01	Entender que sus credenciales de acceso a los sistemas estarán bajo su responsabilidad y control exclusivo.	Alto	Alto	Alto	Alto	Alto
4.2.5.2	op.acc.5.02	Conocer las obligaciones que implica la tenencia de credenciales de acceso, en particular, el deber de custodia diligente, protección de su confidencialidad ey notificación inmediata en caso de pérdida.	Alto	Alto	Alto	Alto	Alto

Continúa en la página siguiente

Código	Id	Descripción	Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
4.2.5.3	op.acc.5.03	Conocer la política de credenciales y el procedimiento de cambio de credenciales.	Alto	Alto	Alto	Alto	Alto
4.2.6.1	op.acc.6.01	Entender la necesidad de cumplir la información que suministre el sistema respecto a sus obligaciones una vez que se ha obtenido el acceso.	-	Alto	-	-	Alto
4.2.6.2	op.acc.6.02	Entender la necesidad de comprobar la información que suministre el sistema respecto a su último acceso efectuado con su identidad.	Alto	Alto	Alto	Alto	Alto
4.2.6.3	op.acc.6.03	Entender la necesidad de no compartir sus credenciales de acceso.	Alto	Alto	Alto	Alto	Alto
4.2.6.4	op.acc.6.04	No guardar en formato legible las credenciales de acceso.	Alto	Alto	Alto	Alto	Alto
4.2.6.5	op.acc.6.05	Entender la importancia de no guardar en formato legible las credenciales de acceso.	Alto	Alto	Alto	Alto	Alto
4.2.7.1	op.acc.7.01	Conocer las políticas y procedimientos de acceso remoto a los sistemas.	Alto	Alto	-	Medio	Alto
4.2.7.2	op.acc.7.02	No guardar en los equipos las credenciales de acceso remoto.	Alto	Alto	Alto	Alto	Alto
4.2.7.3	op.acc.7.03	Conocer y aplicar las buenas prácticas de acceso remoto.	Alto	Alto	-	Medio	Alto
4.2.7.4	op.acc.7.04	Entender que es necesario aplicar los mismos principios de seguridad que rigen para un acceso local.	Alto	Alto	Alto	-	Alto
4.3.01.1	op.exp.1.01	Entender la necesidad de conocer y proteger los activos de información de los que es responsable.	Medio	Alto	-	-	Alto
4.3.01.2	op.exp.1.02	Comprender la importancia de comunicar la existencia de un equipo no inventariado.	Medio	Alto	Bajo	Bajo	Alto
4.3.02.1	op.exp.2.01	Entender la necesidad y los motivos que llevan a aplicar estas medidas.	-	Alto	Bajo	Bajo	Alto
4.3.03.1	op.exp.3.01	Entender la necesidad y los motivos que llevan a aplicar estas medidas.	Medio	Alto	Bajo	Bajo	Alto
4.3.04.1	op.exp.4.01	Atender las especificaciones de los fabricantes en lo relativo al buen uso y mantenimiento de los equipos que utilice en el desempeño de sus tareas.	-	Medio	Bajo	Bajo	Medio
4.3.04.2	op.exp.4.02	Aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones en los equipos que proceda hacerlo.	Alto	Alto	Alto	Alto	Alto
4.3.06.1	op.exp.6.01	Evitar el malware mediante un uso cuidadoso y atento de los sistemas.	Alto	Alto	Alto	Alto	Alto

Continúa en la página siguiente

Código	Id	Descripción	Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
4.3.06.2	op.exp.6.02	Comprender la necesidad de utilizar el antivirus y herramientas de protección	Alto	Alto	Alto	Alto	Alto
4.3.07.1	op.exp.7.01	Conocer el procedimiento de reporte de incidentes reales o sospechosos.	Alto	Alto	Alto	Alto	Alto
4.3.07.2	op.exp.7.02	Comprender la importancia de utilizar el procedimiento de gestión de incidentes	-	Alto	-	-	Alto
4.3.08.1	op.exp.8.01	Entender que se registrará su actividad, cuándo la realiza y sobre qué información.	-	Alto	-	-	Alto
4.3.11.1	op.exp.11.01	Conocer cómo proteger los certificados de los equipos vinculados a su uso.	Alto	Alto	Alto	Alto	Alto
4.3.11.2	op.exp.11.02	Entender la importancia de proteger los certificados y los equipos asociados a su uso.	Alto	Alto	Alto	Alto	Alto
4.4.1.1	op.ext.1.01	Conocer los SLA en los que le afecta, las características del servicio prestado y las responsabilidades de las partes.	Bajo	Alto	Bajo	-	Alto
4.4.1.2	op.ext.1.02	Entender la necesidad de participar activamente en el ciclo de vida de los SLA y en el seguimiento de su cumplimiento.	-	Alto	N.A.	N.A.	Alto
4.4.2.1	op.ext.2.01	Conocer el sistema rutinario para medir el cumplimiento de las obligaciones de servicio.	-	Alto	-	N.A.	Alto
4.4.2.2	op.ext.2.02	Conocer los procedimientos de coordinación en caso de incidentes y desastres en los servicios.	Medio	Alto	Bajo	Bajo	Alto
4.5.1.1	op.cont.1.01	Conocer los requisitos de disponibilidad de los servicios que sea responsable.	-	Alto	-	-	Alto
4.5.1.2	op.cont.1.02	Conocer los elementos que son críticos para la prestación de los servicios que sea responsable.	Alto	Alto	Alto	-	Alto
4.5.1.3	op.cont.1.03	Comprender la importancia de colaborar en la realización de un correcto análisis de impacto.	Medio	Alto	-	-	Alto

Continúa en la página siguiente

Código	Id	Descripción	Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
4.5.2.1	op.cont.2.01	Conocer las funciones, responsabilidades y actividades a realizar en un plan de continuidad.	-	Alto	-	-	Alto
4.5.2.2	op.cont.2.02	Conocer los medios alternativos que se utilizarán para mantener el servicio.	-	Alto	-	-	Alto
4.5.3.1	op.cont.3.01	Entender la necesidad de hacer pruebas periódicas del plan de continuidad y colaborar activamente.	Medio	Alto	Bajo	-	Alto
5.1.1.1	mp.if.1.01	Entender que no puede acceder a locales a los que no está autorizado, ni solicitar credenciales de acceso de manera no autorizada.	-	-	-	-	-
5.1.2.1	mp.if.2.01	Entender la necesidad de identificarse cuando se acceda a los locales donde hay equipamiento que forme parte del sistema de información.	-	-	-	-	-
5.1.2.2	mp.if.2.02	Saber que las entradas y salidas de locales donde hay equipamiento que forme parte del sistema de información quedarán registradas.	Alto	Alto	Alto	Alto	Alto
5.1.8.1	mp.if.9.01	Conocer la ubicación y la forma de acceso a las instalaciones alternativas para poder trabajar en caso de que las instalaciones habituales no estén disponibles, así como el procedimiento y condiciones de cambio de ubicación.	Medio	-	Bajo	-	-
5.2.1.1	mp.per.1.01	Conocer las responsabilidades relacionadas con su puesto de trabajo en materia de seguridad.	Alto	Alto	Alto	Alto	Alto
5.2.2.1	mp.per.2.01	Conocer las medidas disciplinarias en caso de incumplimiento de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.	Alto	Alto	Alto	Alto	Alto
5.2.2.2	mp.per.2.02	Conocer las obligaciones tanto durante el periodo de desempeño del puesto como en caso de término de la asignación o traslado a otro puesto de trabajo.	Alto	Alto	Alto	Alto	Alto

Continúa en la página siguiente

Código	Id	Descripción	Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
5.2.2.3	mp.per.2.03	Entender el deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que esté adscrito al puesto de trabajo, como posteriormente a su terminación.	Alto	Alto	Alto	Alto	Alto
5.2.5.1	mp.per.9.01	Entender la importancia de conocer la existencia y disponibilidad de personas que se puedan hacer cargo de las funciones en caso de indisponibilidad del personal habitual.	Bajo	-	Bajo	-	Alto
5.3.1.1	mp.eq.1.01	Entender la necesidad de que su puesto de trabajo permanezca despejado, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.	Medio	Medio	Medio	-	Medio
5.3.1.2	mp.eq.1.02	Entender que el material se guardará en lugar cerrado cuando no se esté utilizando.	Medio	Medio	Medio	Medio	Medio
5.3.2.1	mp.eq.2.01	Entender la necesidad de que el puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación para reanudar la actividad en curso.	Alto	Alto	Alto	-	Alto
5.3.2.2	mp.eq.2.02	Entender la necesidad de que pasado un cierto tiempo sin utilizar, se cancelarán las sesiones abiertas desde su puesto de trabajo.	Medio	Medio	Medio	Medio	Medio
5.3.3.1	mp.eq.3.01	Conocer el procedimiento para informar de la pérdida o sustracción de un portátil	-	-	-	-	-
5.3.3.2	mp.eq.3.02	Entender la necesidad de proteger el portátil y la información que contiene, así como tenerlo en todo momento controlado y custodiado.	Alto	Alto	Alto	Alto	Alto
5.3.3.3	mp.eq.3.03	Entender que cuando el equipo portátil se conecte remotamente a través de redes que no están bajo el estricto control de la universidad, no debe enviarse información confidencial o protegida.	Alto	Alto	-	Alto	Alto
5.3.3.4	mp.eq.3.04	Entender que en el equipo portátil no deben almacenarse información o datos de carácter confidencial o protegido.	-	Alto	-	-	Alto

Continúa en la página siguiente

Código	Id	Descripción	Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
5.3.3.5	mp.eq.3.05	Entender que en el equipo portátil no deben almacenarse claves de acceso de la universidad.	Alto	Alto	Alto	Alto	Alto
5.3.3.6	mp.eq.3.06	En caso de almacenar información sensible en el equipo, conocer herramientas y técnicas de protección.	-	Alto	-	Alto	Alto
5.3.4.1	mp.eq.9.01	Conocer el procedimiento de acceso a medios alternativos de tratamiento de la información para el caso de que fallen los medios habituales.	Medio	-	Medio	-	-
5.4.2.1	mp.com.2.01	Conocer técnicas de navegación seguras.	Alto	Alto	Alto	Alto	Alto
5.4.2.2	mp.com.2.02	Entender la necesidad de utilizar técnicas de navegación seguras.	Alto	Alto	Alto	Alto	Alto
5.4.3.1	mp.com.3.01	Conocer técnicas de navegación seguras.	Alto	Alto	Alto	Alto	Alto
5.4.3.2	mp.com.3.02	Entender la necesidad de utilizar técnicas de navegación seguras.	Alto	Alto	Alto	Alto	Alto
5.5.1.1	mp.si.1.01	Conocer el significado de las etiquetas que indiquen el nivel de seguridad de la información, bien mediante simple inspección, bien mediante el recurso a un repositorio que lo explique.	-	Alto	Medio	Bajo	Alto
5.5.1.2	mp.si.1.02	Conocer el tratamiento y gestión de la información en base a su nivel de seguridad.	-	Alto	-	Alto	Alto
5.5.1.3	mp.si.1.03	Entender la necesidad de clasificar y etiquetar la información respecto a su nivel de seguridad.	Medio	-	Medio	Medio	Alto
5.5.2.1	mp.si.2.01	Entender la necesidad de aplicar mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida en dispositivos removibles.	Alto	Alto	Alto	Alto	Alto
5.5.2.2	mp.si.2.02	Saber utilizar mecanismos criptográficos sobre dispositivos de almacenamiento móvil.	Alto	Alto	Alto	Alto	Alto

Continúa en la página siguiente

Código	Id	Descripción	Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
5.5.3.1	mp.si.3.01	Saber aplicar medidas físicas o lógicas para garantizar el control de acceso a los soportes de información bajo su responsabilidad.	-	-	-	-	Alto
5.5.3.2	mp.si.3.02	Entender las necesidad de respetar las exigencias de mantenimiento del fabricante de los soportes de información, en especial, en lo referente a temperatura, humedad y otros agresores medioambientales	Medio	-	-	-	-
5.5.5.1	mp.si.5.01	Saber borrar de manera segura los soportes de información que vayan a ser reutilizados para otra información o liberados.	Medio	Alto	Medio	-	Medio
5.5.5.2	mp.si.5.02	Entender la necesidad de realizar borrados seguros de soportes cuando vayan a ser reutilizados o liberados.	Medio	Alto	Medio	Medio	Alto
5.5.5.3	mp.si.5.03	Conocer el procedimiento de solicitud de destrucción de soportes de información.	Medio	Alto	Medio	Medio	Alto
5.6.2.1	mp.sw.2.01	En caso de contratación externa, se tendrán presentes los criterios de aceptación en materia de seguridad.	-	-	N.A.	N.A.	-
5.7.1.1	mp.info.1.01	Saber cómo garantizar y proteger, en lo que concierne al tratamiento de los datos personales, los derechos de las personas físicas, y especialmente de su honor e intimidad personal y familiar.	Alto	Alto	Alto	Alto	Alto
5.7.1.2	mp.info.1.02	Entender la importancia de la protección de los datos personales y derechos digitales.	Alto	Alto	Alto	Alto	Alto
5.7.2.1	mp.info.2.01	Conocer los criterios para asignar a cada información el nivel de seguridad requerido, y ser responsable de su documentación y aprobación formal.	Bajo	Alto	-	-	Alto
5.7.2.2	mp.info.2.02	Conocer las políticas y procedimientos que describan en detalle la forma en la que se ha de etiquetar y tratar la información en consideración al nivel de seguridad que requiere	Bajo	Alto	-	-	Alto
5.7.2.3	mp.info.2.03	Entender que como responsable de información, en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad.	Bajo	Alto	N.A.	-	Alto

Continúa en la página siguiente

Código	Id	Descripción	Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
5.7.3.1	mp.info.3.01	Entender que la información con un nivel alto de confidencialidad se cifrará tanto durante su almacenamiento como durante su transmisión. Sólo estará en claro mientras se está haciendo uso de ella.	-	Alto	-	-	Alto
5.7.4.1	mp.info.4.01	Conocer las políticas, procedimientos y circunstancias de uso de la firma electrónica.	Alto	Alto	Alto	Alto	Alto
5.7.4.2	mp.info.4.02	Entender la importancia del buen uso y resguardo de la firma electrónica	Alto	Alto	-	Alto	Alto
5.7.6.1	mp.info.6.01	Retirar de la documentación toda la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.	-	-	-	Alto	Alto
5.7.6.2	mp.info.6.02	Entender la necesidad de gestionar los metadatos de la documentación que se utilice o genere.	Medio	Medio	Medio	Medio	-
5.7.7.1	mp.info.9.01	Conocer las políticas y procedimientos de realización de copias de seguridad en su entorno de trabajo.	Medio	-	-	-	Alto
5.7.7.2	mp.info.9.02	Entender la necesidad de realizar copias de seguridad de manera periódica, así como comprobar que han sido bien realizadas.	Medio	Alto	-	-	Alto
5.8.1.1	mp.s.1.01	Proteger la información de los correos electrónicos, tanto en el cuerpo de los mensajes, como en los anexos.	-	-	-	Alto	Alto
5.8.1.2	mp.s.1.02	Proteger a la universidad frente a problemas que se materializan por medio del correo electrónico: spam...	Alto	Alto	Alto	Alto	Alto
5.8.1.3	mp.s.1.03	Conocer las normas de uso del correo electrónico.	Alto	Alto	Alto	Alto	Alto
5.8.1.4	mp.s.1.04	Entender la importancia de un uso cuidadoso del correo electrónico.	Alto	Alto	Alto	Alto	Alto

Continúa en la página siguiente

Código	Id	Descripción	Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
5.8.4.1	mp.s.9.01	Conocer la existencia, circunstancias y procedimiento de uso medios alternativos para prestar los servicios en el caso de que fallen los medios habituales	-	Alto	-	-	Alto
5.8.4.2	mp.s.9.02	Entender la importancia de conocer los procedimientos de uso de los medios alternativos	-	-	-	Medio	Alto

7.7. Anexo G: Segunda iteración

Código	Id	Descripción	Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
3.1.0.1	org.1.01	Conocer la política de seguridad de la universidad.	Alto	Alto	Alto	Medio	Alto
3.1.0.2	org.1.02	Conocer dónde puede consultarse la política de seguridad de la universidad.	Alto	Alto	Medio	Bajo	Alto
3.1.0.3	org.1.03	Entender la importancia, significado y objetivos de la política de seguridad.	Alto	Alto	Medio	Alto	Alto
3.1.0.4	org.1.04	Entender la necesidad de conocer las actualizaciones de la política de seguridad.	Medio	Alto	Medio	Medio	Alto
3.2.0.1	org.2.01	Conocer el uso correcto de los equipos, servicios e instalaciones que utilice en el desempeño de su labor.	Alto	Alto	Medio	Bajo	Alto
3.2.0.2	org.2.02	Conocer qué se considera uso indebido de los equipos, servicios e instalaciones que utilice en el desempeño de su labor.	Alto	Alto	Medio	Bajo	Alto
3.2.0.3	org.2.03	Conocer su responsabilidad con respecto al cumplimiento o violación de la política de seguridad: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.	Alto	Alto	Alto	Alto	Alto
3.2.0.4	org.2.04	Entender la importancia del cumplimiento de la normativa de seguridad de la universidad.	Alto	Alto	Medio	Medio	Alto
3.3.0.1	org.3.01	Saber qué tareas en el ámbito de la seguridad de la información debe realizar en el desempeño de su labor.	Alto	Alto	Medio	Medio	Alto
3.3.0.2	org.3.02	Saber cómo llevar a cabo las tareas habituales en el ámbito de la seguridad de la información en el desempeño de su labor.	Medio	Alto	Medio	Bajo	Alto
3.3.0.3	org.3.03	Saber identificar y reportar comportamientos anómalos en el ámbito de la seguridad.	Medio	Alto	Medio	Bajo	Alto
3.3.0.4	org.3.04	Entender la importancia de conocer los procedimientos de seguridad en el desempeño de su actividad.	Medio	Alto	Medio	Bajo	Alto
3.4.0.1	org.4.01	Conocer el funcionamiento de los procesos de autorización para el uso de los sistemas de información.	Alto	Alto	Bajo	Bajo	Alto

Continúa en la página siguiente

Código	Id	Descripción	Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
4.1.1.1	op.pl.1.01	Identificar y valorar cualitativamente los activos de información más valiosos de su entorno de trabajo.	Medio	Alto	Bajo	Bajo	Alto
4.1.1.2	op.pl.1.02	Conocer la valoración de los sistemas derivados del análisis de riesgos, y el nivel de riesgo asumido.	Bajo	Alto	Bajo	Medio	Alto
4.2.1.1	op.acc.1.01	Utilizar el identificador adecuado para acceder al sistema en el caso de disponer de diferentes roles de forma que siempre queden delimitados privilegios y registros de actividad.	Alto	Alto	Alto	Alto	Alto
4.2.1.2	op.acc.1.02	Entender que se guardará la información de cuándo accede y qué actividad realiza.	Alto	Alto	Alto	Alto	Alto
4.2.1.3	op.acc.1.03	Entender la importancia de utilizar el identificador adecuado.	Alto	Alto	Alto	Alto	Alto
4.2.2.1	op.acc.2.01	Conocer las políticas y procedimiento de establecimiento de derechos de acceso a los recursos de su responsabilidad, ateniéndose a la política y normativa de seguridad del sistema.	Medio	Alto	Bajo	Bajo	Alto
4.2.2.2	op.acc.2.02	Entender la importancia de gestionar los derechos de acceso a los recursos de su responsabilidad, especialmente en los casos de actualización o bajas.	Bajo	Alto	Bajo	Bajo	Alto
4.2.4.1	op.acc.4.01	Comprender que los derechos de acceso se limitan atendiendo a los principios de mínimo privilegio y necesidad de conocer.	Bajo	Alto	Bajo	Bajo	Alto
4.2.4.2	op.acc.4.02	Conocer las políticas y procedimientos para conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable.	Bajo	Alto	Bajo	Bajo	Alto
4.2.5.1	op.acc.5.01	Entender que sus credenciales de acceso a los sistemas estarán bajo su responsabilidad y control exclusivo.	Alto	Alto	Alto	Alto	Alto
4.2.5.2	op.acc.5.02	Conocer las obligaciones que implica la tenencia de credenciales de acceso, en particular, el deber de custodia diligente, protección de su confidencialidad ey notificación inmediata en caso de pérdida.	Alto	Alto	Alto	Alto	Alto

Continúa en la página siguiente

Código	Id	Descripción	Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
4.2.5.3	op.acc.5.03	Conocer la política de credenciales y el procedimiento de cambio de credenciales.	Alto	Alto	Alto	Alto	Alto
4.2.6.1	op.acc.6.01	Entender la necesidad de cumplir la información que suministre el sistema respecto a sus obligaciones una vez que se ha obtenido el acceso.	Medio	Alto	Medio	Bajo	Alto
4.2.6.2	op.acc.6.02	Entender la necesidad de comprobar la información que suministre el sistema respecto a su último acceso efectuado con su identidad.	Alto	Alto	Alto	Alto	Alto
4.2.6.3	op.acc.6.03	Entender la necesidad de no compartir sus credenciales de acceso.	Alto	Alto	Alto	Alto	Alto
4.2.6.4	op.acc.6.04	No guardar en formato legible las credenciales de acceso.	Alto	Alto	Alto	Alto	Alto
4.2.6.5	op.acc.6.05	Entender la importancia de no guardar en formato legible las credenciales de acceso.	Alto	Alto	Alto	Alto	Alto
4.2.7.1	op.acc.7.01	Conocer las políticas y procedimientos de acceso remoto a los sistemas.	Alto	Alto	Medio	Medio	Alto
4.2.7.2	op.acc.7.02	No guardar en los equipos las credenciales de acceso remoto.	Alto	Alto	Alto	Alto	Alto
4.2.7.3	op.acc.7.03	Conocer y aplicar las buenas prácticas de acceso remoto.	Alto	Alto	Medio	Medio	Alto
4.2.7.4	op.acc.7.04	Entender que es necesario aplicar los mismos principios de seguridad que rigen para un acceso local.	Alto	Alto	Alto	Medio	Alto
4.3.01.1	op.exp.1.01	Entender la necesidad de conocer y proteger los activos de información de los que es responsable.	Medio	Alto	Medio	Medio	Alto
4.3.01.2	op.exp.1.02	Comprender la importancia de comunicar la existencia de un equipo no inventariado.	Medio	Alto	Bajo	Bajo	Alto
4.3.02.1	op.exp.2.01	Entender la necesidad y los motivos que llevan a aplicar estas medidas.	Medio	Alto	Bajo	Bajo	Alto
4.3.03.1	op.exp.3.01	Entender la necesidad y los motivos que llevan a aplicar estas medidas.	Medio	Alto	Bajo	Bajo	Alto
4.3.04.1	op.exp.4.01	Atender las especificaciones de los fabricantes en lo relativo al buen uso y mantenimiento de los equipos que utilice en el desempeño de sus tareas.	Bajo	Medio	Bajo	Bajo	Medio
4.3.04.2	op.exp.4.02	Aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones en los equipos que proceda hacerlo.	Alto	Alto	Alto	Alto	Alto
4.3.06.1	op.exp.6.01	Evitar el malware mediante un uso cuidadoso y atento de los sistemas.	Alto	Alto	Alto	Alto	Alto

Continúa en la página siguiente

Código	Id	Descripción	Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
4.3.06.2	op.exp.6.02	Comprender la necesidad de utilizar el antivirus y herramientas de protección	Alto	Alto	Alto	Alto	Alto
4.3.07.1	op.exp.7.01	Conocer el procedimiento de reporte de incidentes reales o sospechosos.	Alto	Alto	Alto	Alto	Alto
4.3.07.2	op.exp.7.02	Comprender la importancia de utilizar el procedimiento de gestión de incidentes	Medio	Alto	Medio	Medio	Alto
4.3.08.1	op.exp.8.01	Entender que se registrará su actividad, cuándo la realiza y sobre qué información.	Medio	Alto	Bajo	Bajo	Alto
4.3.11.1	op.exp.11.01	Conocer cómo proteger los certificados de los equipos vinculados a su uso.	Alto	Alto	Alto	Alto	Alto
4.3.11.2	op.exp.11.02	Entender la importancia de proteger los certificados y los equipos asociados a su uso.	Alto	Alto	Alto	Alto	Alto
4.4.1.1	op.ext.1.01	Conocer los SLA en los que le afecta, las características del servicio prestado y las responsabilidades de las partes.	Bajo	Alto	Bajo	N.A.	Alto
4.4.1.2	op.ext.1.02	Entender la necesidad de participar activamente en el ciclo de vida de los SLA y en el seguimiento de su cumplimiento.	N.A.	Alto	N.A.	N.A.	Alto
4.4.2.1	op.ext.2.01	Conocer el sistema rutinario para medir el cumplimiento de las obligaciones de servicio.	N.A.	Alto	N.A.	N.A.	Alto
4.4.2.2	op.ext.2.02	Conocer los procedimientos de coordinación en caso de incidentes y desastres en los servicios.	Medio	Alto	Bajo	Bajo	Alto
4.5.1.1	op.cont.1.01	Conocer los requisitos de disponibilidad de los servicios que sea responsable.	Medio	Alto	Bajo	N.A.	Alto
4.5.1.2	op.cont.1.02	Conocer los elementos que son críticos para la prestación de los servicios que sea responsable.	Alto	Alto	Alto	N.A.	Alto
4.5.1.3	op.cont.1.03	Comprender la importancia de colaborar en la realización de un correcto análisis de impacto.	Medio	Alto	Bajo	N.A.	Alto

Continúa en la página siguiente

Código	Id	Descripción	Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
4.5.2.1	op.cont.2.01	Conocer las funciones, responsabilidades y actividades a realizar en un plan de continuidad.	Medio	Alto	Medio	N.A.	Alto
4.5.2.2	op.cont.2.02	Conocer los medios alternativos que se utilizarán para mantener el servicio.	Medio	Alto	Medio	N.A.	Alto
4.5.3.1	op.cont.3.01	Entender la necesidad de hacer pruebas periódicas del plan de continuidad y colaborar activamente.	Medio	Alto	Bajo	N.A.	Alto
5.1.1.1	mp.if.1.01	Entender que no puede acceder a locales a los que no está autorizado, ni solicitar credenciales de acceso de manera no autorizada.	Medio	Alto	Medio	Medio	Alto
5.1.2.1	mp.if.2.01	Entender la necesidad de identificarse cuando se acceda a los locales donde hay equipamiento que forme parte del sistema de información.	Medio	Alto	Medio	Medio	Alto
5.1.2.2	mp.if.2.02	Saber que las entradas y salidas de locales donde hay equipamiento que forme parte del sistema de información quedarán registradas.	Alto	Alto	Alto	Alto	Alto
5.1.8.1	mp.if.9.01	Conocer la ubicación y la forma de acceso a las instalaciones alternativas para poder trabajar en caso de que las instalaciones habituales no estén disponibles, así como el procedimiento y condiciones de cambio de ubicación.	Medio	Medio	Bajo	N.A.	Medio
5.2.1.1	mp.per.1.01	Conocer las responsabilidades relacionadas con su puesto de trabajo en materia de seguridad.	Alto	Alto	Alto	Alto	Alto
5.2.2.1	mp.per.2.01	Conocer las medidas disciplinarias en caso de incumplimiento de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.	Alto	Alto	Alto	Alto	Alto
5.2.2.2	mp.per.2.02	Conocer las obligaciones tanto durante el periodo de desempeño del puesto como en caso de término de la asignación o traslado a otro puesto de trabajo.	Alto	Alto	Alto	Alto	Alto

Continúa en la página siguiente

Código	Id	Descripción	Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
5.2.2.3	mp.per.2.03	Entender el deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que esté adscrito al puesto de trabajo, como posteriormente a su terminación.	Alto	Alto	Alto	Alto	Alto
5.2.5.1	mp.per.9.01	Entender la importancia de conocer la existencia y disponibilidad de personas que se puedan hacer cargo de las funciones en caso de indisponibilidad del personal habitual.	Bajo	Medio	Bajo	N.A.	Alto
5.3.1.1	mp.eq.1.01	Entender la necesidad de que su puesto de trabajo permanezca despejado, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.	Medio	Medio	Medio	Bajo	Medio
5.3.1.2	mp.eq.1.02	Entender que el material se guardará en lugar cerrado cuando no se esté utilizando.	Medio	Medio	Medio	Medio	Medio
5.3.2.1	mp.eq.2.01	Entender la necesidad de que el puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación para reanudar la actividad en curso.	Alto	Alto	Alto	Medio	Alto
5.3.2.2	mp.eq.2.02	Entender la necesidad de que pasado un cierto tiempo sin utilizar, se cancelarán las sesiones abiertas desde su puesto de trabajo.	Medio	Medio	Medio	Medio	Medio
5.3.3.1	mp.eq.3.01	Conocer el procedimiento para informar de la pérdida o sustracción de un portátil	Medio	Medio	Medio	Medio	Medio
5.3.3.2	mp.eq.3.02	Entender la necesidad de proteger el portátil y la información que contiene, así como tenerlo en todo momento controlado y custodiado.	Alto	Alto	Alto	Alto	Alto
5.3.3.3	mp.eq.3.03	Entender que cuando el equipo portátil se conecte remotamente a través de redes que no están bajo el estricto control de la universidad, no debe enviarse información confidencial o protegida.	Alto	Alto	Medio	Alto	Alto
5.3.3.4	mp.eq.3.04	Entender que en el equipo portátil no deben almacenarse información o datos de carácter confidencial o protegido.	Medio	Alto	Medio	Medio	Alto

Continúa en la página siguiente

Código	Id	Descripción	Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
5.3.3.5	mp.eq.3.05	Entender que en el equipo portátil no deben almacenarse claves de acceso de la universidad.	Alto	Alto	Alto	Alto	Alto
5.3.3.6	mp.eq.3.06	En caso de almacenar información sensible en el equipo, conocer herramientas y técnicas de protección.	Medio	Alto	Medio	Alto	Alto
5.3.4.1	mp.eq.9.01	Conocer el procedimiento de acceso a medios alternativos de tratamiento de la información para el caso de que fallen los medios habituales.	Medio	Medio	Medio	Bajo	Alto
5.4.2.1	mp.com.2.01	Conocer técnicas de navegación seguras.	Alto	Alto	Alto	Alto	Alto
5.4.2.2	mp.com.2.02	Entender la necesidad de utilizar técnicas de navegación seguras.	Alto	Alto	Alto	Alto	Alto
5.4.3.1	mp.com.3.01	Conocer técnicas de navegación seguras.	Alto	Alto	Alto	Alto	Alto
5.4.3.2	mp.com.3.02	Entender la necesidad de utilizar técnicas de navegación seguras.	Alto	Alto	Alto	Alto	Alto
5.5.1.1	mp.si.1.01	Conocer el significado de las etiquetas que indiquen el nivel de seguridad de la información, bien mediante simple inspección, bien mediante el recurso a un repositorio que lo explique.	Medio	Alto	Medio	Bajo	Alto
5.5.1.2	mp.si.1.02	Conocer el tratamiento y gestión de la información en base a su nivel de seguridad.	Medio	Alto	Medio	Alto	Alto
5.5.1.3	mp.si.1.03	Entender la necesidad de clasificar y etiquetar la información respecto a su nivel de seguridad.	Medio	Medio	Medio	Medio	Alto
5.5.2.1	mp.si.2.01	Entender la necesidad de aplicar mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida en dispositivos removibles.	Alto	Alto	Alto	Alto	Alto
5.5.2.2	mp.si.2.02	Saber utilizar mecanismos criptográficos sobre dispositivos de almacenamiento móvil.	Alto	Alto	Alto	Alto	Alto

Continúa en la página siguiente

Código	Id	Descripción	Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
5.5.3.1	mp.si.3.01	Saber aplicar medidas físicas o lógicas para garantizar el control de acceso a los soportes de información bajo su responsabilidad.	Medio	Medio	Medio	Medio	Alto
5.5.3.2	mp.si.3.02	Entender las necesidad de respetar las exigencias de mantenimiento del fabricante de los soportes de información, en especial, en lo referente a temperatura, humedad y otros agresores medioambientales	Medio	Medio	Bajo	Bajo	Medio
5.5.5.1	mp.si.5.01	Saber borrar de manera segura los soportes de información que vayan a ser reutilizados para otra información o liberados.	Medio	Alto	Medio	Medio	Medio
5.5.5.2	mp.si.5.02	Entender la necesidad de realizar borrados seguros de soportes cuando vayan a ser reutilizados o liberados.	Medio	Alto	Medio	Medio	Alto
5.5.5.3	mp.si.5.03	Conocer el procedimiento de solicitud de destrucción de soportes de información.	Medio	Alto	Medio	Medio	Alto
5.6.2.1	mp.sw.2.01	En caso de contratación externa, se tendrán presentes los criterios de aceptación en materia de seguridad.	Bajo	Medio	N.A.	N.A.	Medio
5.7.1.1	mp.info.1.01	Saber cómo garantizar y proteger, en lo que concierne al tratamiento de los datos personales, los derechos de las personas físicas, y especialmente de su honor e intimidad personal y familiar.	Alto	Alto	Alto	Alto	Alto
5.7.1.2	mp.info.1.02	Entender la importancia de la protección de los datos personales y derechos digitales.	Alto	Alto	Alto	Alto	Alto
5.7.2.1	mp.info.2.01	Conocer los criterios para asignar a cada información el nivel de seguridad requerido, y ser responsable de su documentación y aprobación formal.	Bajo	Alto	Bajo	N.A.	Alto
5.7.2.2	mp.info.2.02	Conocer las políticas y procedimientos que describan en detalle la forma en la que se ha de etiquetar y tratar la información en consideración al nivel de seguridad que requiere	Bajo	Alto	N.A.	N.A.	Alto
5.7.2.3	mp.info.2.03	Entender que como responsable de información, en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad.	Bajo	Alto	N.A.	N.A.	Alto

Continúa en la página siguiente

Código	Id	Descripción	Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
5.7.3.1	mp.info.3.01	Entender que la información con un nivel alto de confidencialidad se cifrará tanto durante su almacenamiento como durante su transmisión. Sólo estará en claro mientras se está haciendo uso de ella.	Medio	Alto	Medio	Medio	Alto
5.7.4.1	mp.info.4.01	Conocer las políticas, procedimientos y circunstancias de uso de la firma electrónica.	Alto	Alto	Alto	Alto	Alto
5.7.4.2	mp.info.4.02	Entender la importancia del buen uso y resguardo de la firma electrónica	Alto	Alto	Alto	Alto	Alto
5.7.6.1	mp.info.6.01	Retirar de la documentación toda la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.	Medio	Medio	Medio	Alto	Alto
5.7.6.2	mp.info.6.02	Entender la necesidad de gestionar los metadatos de la documentación que se utilice o genere.	Medio	Medio	Medio	Medio	Medio
5.7.7.1	mp.info.9.01	Conocer las políticas y procedimientos de realización de copias de seguridad en su entorno de trabajo.	Medio	Medio	Bajo	Bajo	Alto
5.7.7.2	mp.info.9.02	Entender la necesidad de realizar copias de seguridad de manera periódica, así como comprobar que han sido bien realizadas.	Medio	Alto	Medio	Bajo	Alto
5.8.1.1	mp.s.1.01	Proteger la información de los correos electrónicos, tanto en el cuerpo de los mensajes, como en los anexos.	Medio	Medio	Medio	Alto	Alto
5.8.1.2	mp.s.1.02	Proteger a la universidad frente a problemas que se materializan por medio del correo electrónico: spam...	Alto	Alto	Alto	Alto	Alto
5.8.1.3	mp.s.1.03	Conocer las normas de uso del correo electrónico.	Alto	Alto	Alto	Alto	Alto
5.8.1.4	mp.s.1.04	Entender la importancia de un uso cuidadoso del correo electrónico.	Alto	Alto	Alto	Alto	Alto

Continúa en la página siguiente

Código	Id	Descripción	Grupo 1	Grupo 2	Grupo 3	Grupo 4	Grupo 5
5.8.4.1	mp.s.9.01	Conocer la existencia, circunstancias y procedimiento de uso medios alternativos para prestar los servicios en el caso de que fallen los medios habituales	Bajo	Alto	Bajo	Bajo	Alto
5.8.4.2	mp.s.9.02	Entender la importancia de conocer los procedimientos de uso de los medios alternativos	Medio	Medio	Bajo	Medio	Alto

7.8. Anexo H: Tercera iteración

Código	Grupo	Respuesta inicial	Respuesta final
3.4.0.1	3	1	2
4.1.1.2	1	1	2
4.2.2.1	3	1	2
4.2.4.1	1	1	2
4.2.4.1	3	1	2
4.2.4.2	1	1	2
4.2.6.1	4	1	2
4.3.08.1	3	1	2
4.4.1.1	4	0	1
4.5.1.1	4	0	1
4.5.1.2	4	0	1
4.5.2.1	4	0	1
4.5.2.2	4	0	1
5.2.2.1	4	3	2
5.5.3.2	4	1	0
5.5.3.2	5	2	1
5.7.2.1	3	1	0
5.7.4.1	3	3	2
5.7.4.2	3	3	2

7.9. Anexo I: Matriz de coeficientes de distancia

G1-G2	G1-G3	G1-G4	G1-G5	G2-G3	G2-G4	G2-G5	G3-G4	G3-G5	G4-G5
0	0	1	0	0	1	0	1	0	1
0	1	2	0	1	2	0	1	1	2
0	1	0	0	1	0	0	1	1	0
1	0	0	1	1	1	0	0	1	1
0	1	2	0	1	2	0	1	1	2
0	1	2	0	1	2	0	1	1	2
0	0	0	0	0	0	0	0	0	0
0	1	1	0	1	1	0	0	1	1
0	1	1	0	1	1	0	0	1	1
1	0	1	1	1	2	0	1	1	2
1	0	1	1	1	2	0	1	1	2
1	0	1	1	1	2	0	1	1	2
0	1	2	0	1	2	0	1	1	2
1	1	1	1	2	2	0	0	2	2
1	1	0	1	2	1	0	1	2	1
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
1	0	1	1	1	2	0	1	1	2
2	0	0	2	2	2	0	0	2	2
1	0	1	1	1	2	0	1	1	2
1	1	1	1	2	2	0	0	2	2
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
1	0	0	1	1	1	0	0	1	1
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	1	1	0	1	1	0	0	1	1
0	0	0	0	0	0	0	0	0	0
0	1	1	0	1	1	0	0	1	1
0	0	1	0	0	1	0	1	0	1
1	0	0	1	1	1	0	0	1	1
1	1	1	1	2	2	0	0	2	2
1	1	1	1	2	2	0	0	2	2
1	1	1	1	2	2	0	0	2	2
1	0	0	1	1	1	0	0	1	1
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
1	0	0	1	1	1	0	0	1	1

G1-G2	G1-G3	G1-G4	G1-G5	G2-G3	G2-G4	G2-G5	G3-G4	G3-G5	G4-G5
1	0	1	1	1	2	0	1	1	2
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
2	0	0	2	2	2	0	0	2	2
3	0	0	3	3	3	0	0	3	3
3	0	0	3	3	3	0	0	3	3
1	1	1	1	2	2	0	0	2	2
1	1	1	1	2	2	0	0	2	2
0	0	2	0	0	2	0	2	0	2
1	1	2	1	2	3	0	1	2	3
1	0	1	1	1	2	0	1	1	2
1	0	1	1	1	2	0	1	1	2
1	1	2	1	2	3	0	1	2	3
1	0	0	1	1	1	0	0	1	1
1	0	0	1	1	1	0	0	1	1
0	0	0	0	0	0	0	0	0	0
0	1	2	0	1	2	0	1	1	2
0	0	1	0	0	1	0	1	0	1
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
1	0	1	2	1	2	1	1	2	3
0	0	1	0	0	1	0	1	0	1
0	0	0	0	0	0	0	0	0	0
0	0	1	0	0	1	0	1	0	1
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	1	0	0	1	0	0	1	1	0
1	0	0	1	1	1	0	0	1	1
0	0	0	0	0	0	0	0	0	0
1	0	1	1	1	0	0	1	1	0
0	0	1	1	0	1	1	1	1	2
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
1	0	1	1	1	2	0	1	1	2
1	0	1	1	1	0	0	1	1	0
0	0	0	1	0	0	1	0	1	1
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	1	0	1	1
0	1	2	1	1	2	1	1	0	1

G1-G2	G1-G3	G1-G4	G1-G5	G2-G3	G2-G4	G2-G5	G3-G4	G3-G5	G4-G5
1	0	0	0	1	1	1	0	0	0
1	0	0	1	1	1	0	0	1	1
1	0	0	1	1	1	0	0	1	1
1	1	1	1	2	2	0	0	2	2
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
2	1	1	2	3	3	0	0	3	3
2	1	1	2	3	3	0	0	3	3
2	1	1	2	3	3	0	0	3	3
1	0	0	1	1	1	0	0	1	1
0	1	0	0	1	0	0	1	1	0
0	1	0	0	1	0	0	1	1	0
0	0	1	1	0	1	1	1	1	0
0	0	0	0	0	0	0	0	0	0
0	1	1	1	1	1	1	0	2	2
1	0	1	1	1	2	0	1	1	2
0	0	1	1	0	1	1	1	1	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
2	0	0	2	2	2	0	0	2	2
0	1	0	1	1	0	1	1	2	1

7.10. Anexo J: Programación con R

```
> sum(abs(Grupo.1-Grupo.2))
[1] 54
> sum(abs(Grupo.1-Grupo.3))
[1] 30
> sum(abs(Grupo.1-Grupo.4))
[1] 55
> sum(abs(Grupo.1-Grupo.5))
[1] 62
> sum(abs(Grupo.2-Grupo.3))
[1] 84
> sum(abs(Grupo.2-Grupo.4))
[1] 105
> sum(abs(Grupo.2-Grupo.5))
[1] 10
> sum(abs(Grupo.3-Grupo.4))
[1] 37
> sum(abs(Grupo.3-Grupo.5))
[1] 90
> sum(abs(Grupo.4-Grupo.5))
[1] 107

> matriz<-c(0,54,30,55,62,54,0,84,105,10,30,84,0,
37,90,55,105,37,0,107,62,10,90,107,0)

> dim(matriz)<-c(5,5)

> matriz
     [,1] [,2] [,3] [,4] [,5]
```

```
[1,]    0   54   30   55   62
[2,]   54    0   84  105   10
[3,]   30   84    0   37   90
[4,]   55  105   37    0  107
[5,]   62   10   90  107    0

> cluster<-hclust(as.dist(matriz),method="complete")
> plot(cluster)
>
```

7.11. Anexo K: Agrupación de valores diferentes en el nuevo clúster

Código	Id	Descripción	Grupo 2	Grupo 5	Clúster
5.2.5.1	mp.per.9.01	Entender la importancia de conocer la existencia y disponibilidad de personas que se puedan hacer cargo de las funciones en caso de indisponibilidad del personal habitual.	Medio	Alto	Alto
5.3.4.1	mp.eq.9.01	Conocer el procedimiento de acceso a medios alternativos de tratamiento de la información para el caso de que fallen los medios habituales.	Medio	Alto	Alto
5.5.1.3	mp.si.1.03	Entender la necesidad de clasificar y etiquetar la información respecto a su nivel de seguridad.	Medio	Alto	Alto
5.5.3.1	mp.si.3.01	Saber aplicar medidas físicas o lógicas para garantizar el control de acceso a los soportes de información bajo su responsabilidad.	Medio	Alto	Alto
5.5.3.2	mp.si.3.02	Entender las necesidad de respetar las exigencias de mantenimiento del fabricante de los soportes de información, en especial, en lo referente a temperatura, humedad y otros agresores medioambientales	Medio	Bajo	Medio
5.5.5.1	mp.si.5.01	Saber borrar de manera segura los soportes de información que vayan a ser reutilizados para otra información o liberados.	Alto	Medio	Alto
5.7.6.1	mp.info.6.01	Retirar de la documentación toda la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.	Medio	Alto	Alto
5.7.7.1	mp.info.9.01	Conocer las políticas y procedimientos de realización de copias de seguridad en su entorno de trabajo.	Medio	Alto	Alto
5.8.1.1	mp.s.1.01	Proteger la información de los correos electrónicos, tanto en el cuerpo de los mensajes, como en los anexos.	Medio	Alto	Alto
5.8.4.2	mp.s.9.02	Entender la importancia de conocer los procedimientos de uso de los medios alternativos	Medio	Alto	Alto

7.12. Anexo L: Diferencias y similitudes en el nuevo ENS

org	Marco organizativo
org.1	Política de seguridad
org.2	Normativa de seguridad
org.3	Procedimientos de seguridad
org.4	Proceso de autorización
op	Marco operacional
op.pl	Planificación
op.pl.1	Análisis de riesgos
op.pl.2	Arquitectura de seguridad
op.pl.3	Adquisición de nuevos componentes
op.pl.4	Dimensionamiento / Gestión de capacidades
op.pl.5	Componentes certificados
op.acc	Control de acceso
op.acc.1	Identificación
op.acc.2	Requisitos de acceso
op.acc.3	Segregación de funciones y tareas
op.acc.4	Proceso de gestión de derechos de acceso
op.acc.5	Mecanismo de autenticación
op.acc.6	Acceso local (local logon)
op.acc.7	Acceso remoto (remote login)
op.acc.5	Mecanismo de autenticación (usuarios externos)
op.acc.6	Mecanismo de autenticación (usuarios de la organización)
op.exp	Explotación
op.exp.1	Inventario de activos
op.exp.2	Configuración de seguridad
op.exp.3	Gestión de la configuración

op.exp.4	Mantenimiento
op.exp.5	Gestión de cambios
op.exp.6	Protección frente a código dañino
op.exp.7	Gestión de incidentes
op.exp.8	Registro de la actividad de los usuarios
op.exp.9	Registro de la gestión de incidentes
op.exp.10	Protección de los registros de actividad
op.exp.11	Protección de claves criptográficas
op.ext	Servicios externos
op.ext.1	Contratación y acuerdos de nivel de servicio
op.ext.2	Gestión diaria
op.ext.9	Medios alternativos
op.ext.3	Protección de la cadena de suministro
op.ext.4	Interconexión de sistemas
op.nub	Servicios en la nube
op.nub.1	Protección de servicios en la nube
op.cont	Continuidad del servicio
op.cont.1	Análisis de impacto
op.cont.2	Plan de continuidad
op.cont.3	Pruebas periódicas
op.cont.4	Medios alternativos. (Anterior op.ext.9)
op.mon	Monitorización del sistema
op.mon.1	Detección de intrusión
op.mon.2	Sistema de métricas
op.mon.3	Vigilancia
mp	Medidas de protección

mp.if	Protección de las instalaciones e infraestructuras
mp.if.1	Áreas separadas y con control de acceso
mp.if.2	Identificación de las personas
mp.if.3	Acondicionamiento de los locales
mp.if.4	Energía eléctrica
mp.if.5	Protección frente a incendios
mp.if.6	Protección frente a inundaciones
mp.if.7	Registro de entrada y salida de equipamiento
mp.if.9	Instalaciones alternativas
mp.per	Gestión del personal
mp.per.1	Caracterización del puesto de trabajo
mp.per.2	Deberes y obligaciones
mp.per.3	Concienciación
mp.per.4	Formación
mp.per.9	Personal alternativo
mp.eq	Protección de los equipos
mp.eq.1	Puesto de trabajo despejado
mp.eq.2	Bloqueo de puesto de trabajo
mp.eq.3	Protección de equipos portátiles
mp.eq.4	Otros dispositivos conectados a la red
mp.eq.9	Medios alternativos
mp.com	Protección de las comunicaciones
mp.com.1	Perímetro seguro
mp.com.2	Protección de la confidencialidad
mp.com.3	Protección de la autenticidad y de la integridad
mp.com.4	Segregación de redes

mp.com.9	Medios alternativos
mp.si	Protección de los soportes de información
mp.si.1	Etiquetado
mp.si.2	Criptografía
mp.si.3	Custodia
mp.si.4	Transporte
mp.si.5	Borrado y destrucción
mp.sw	Protección de las aplicaciones informáticas
mp.sw.1	Desarrollo
mp.sw.2	Aceptación y puesta en servicio
mp.info	Protección de la información
mp.info.1	Datos de carácter personal
mp.info.2	Calificación de la información
mp.info.3	Cifrado
mp.info.4	Firma electrónica
mp.info.5	Sellos de tiempo
mp.info.6	Limpieza de documentos
mp.info.9	Copias de seguridad (backup)
mp.s	Protección de los servicios
mp.s.1	Protección del correo electrónico
mp.s.2	Protección de servicios y aplicaciones web
mp.s.3	Protección de la navegación web
mp.s.8	Protección frente a la denegación de servicio
mp.s.9	Medios alternativos

Bibliografía

20 Minutos (2019). Prosegur, como antes Prisa, Everis y Sacyl, obligada a cerrar sus servicios por un ciberataque con 'ransomware'. Recuperado el 6-12-2019 de https://www.20minutos.es/noticia/4070463/0/prosegur-cierra-servicios-ciberataque/.

ACM y IEEE (2020). Computing Curricula 2020. Recuperado el 27/6/2021 de https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2020.pdf.

Agut, S. y Grau, R. M. (2001). Una aproximación psicosocial al estudio de las competencias. *Revista de relaciones laborales*, 2001(9):13–24.

Aldawood, H. A. y Skinner, G. (2018). A Critical Appraisal of Contemporary Cyber Security Social Engineering Solutions: Measures, Policies, Tools and Applications. In *26th International Conference on Systems Engineering (ICSEng)*, paginas 1–6.

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., y Sohail, A. (2021). Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. *Applied Sciences*, 11(8):3383.

Alles, M. (2015). *Dirección estratégica de RRHH. Gestión por competencias.* Granica, Buenos Aires, tercera edición edition.

Ani, U., He, H., y Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*, 21(1):2–35.

Arancibia, V. H. y Díaz, R. (2002). Enfoque de las Competencias Laborales: Historia,

Definiciones y Generación de un Modelo de Competencias para las Organizaciones y las Personas. *Psykhe*, 11(2).

Armstrong, M. (2014). *A handbook of human resource management practice*. Kogan Page, decimotercera edition.

Bada, M. y Nurse, J. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information and Computer Security*, 27(3):393–410.

Bailey, T., Kolo, B., Rajagopalan, K., y Ware, D. (2018). Insider threat: The human element of cyberrisk. Technical report, McKinsey.

Bassett, G., Hylender, C. D., Langlois, P., Pinto, A., y Widup, S. (2021). 2021 DataBreach Investigations Report. Technical report, Verizon.

Beautement, A., Becker, I., Parkin, S., Krol, K., y Sasse, A. (2016). Productive Security: A Scalable Methodology forAnalysing Employee Security Behaviours. In *Proceedings of theTwelfth Symposium on Usable Privacy and Security (SOUPS 2016)*.

Bedingfield, C. y Clarkson, P. (2020). Design meetings: towards an understanding of the stages and activities that influence success. *Proceedings of the Design Society: DESIGN Conference*, (1):501–510.

Beuran, R., Tang, D., Tan, Z., Hasegawa, S., Tan, Y., y Shinoda, Y. (2019). Supporting cybersecurity education and training via LMS integration: CyLMS. *Education and Information Technologies*, 24(6):3619–3643.

BOE (1978). La Constitución española de 1978. Recuperado el 11/01/2020 de https://www.boe.es/diario_boe/txt.php?id=BOE-A-1978-31229.

BOE (1992). Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Recuperado el 11/01/2020 de https://www.boe.es/buscar/act.php?id=BOE-A-1992-26318.

BOE (1999). Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Recuperado el 11/01/2020 de https://www.boe.es/eli/es/lo/1999/12/13/15.

BOE (2001). Ley Orgánica 6/2001, de 21 de diciembre, de Universidades. Recuperado de https://www.boe.es/buscar/pdf/2001/BOE-A-2001-24515-consolidado.pdf el 26/07/2020.

BOE (2007a). Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Recuperado el 11/01/20220 de https://boe.es/buscar/act.php?id=BOE-A-2007-12352.

BOE (2007b). Real Decreto 1514/2007, de 16 de noviembre, por el que se aprueba el Plan General de Contabilidad. Recuperado el 28/12/2019 en https://www.boe.es/buscar/doc.php?id=BOE-A-2007-19884.

BOE (2010). Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Recuperado el 28/12/2019 en https://www.boe.es/buscar/doc.php?id=BOE-A-2010-1330.

BOE (2015). Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Recuperado el 11/01/20202 de https://www.boe.es/eli/es/l/2015/10/01/39/con.

BOE (2015a). Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. Recuperado el 25/02/2020 de https://www.boe.es/buscar/act.php?id=BOE-A-2015-10566.

BOE (2015b). Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Recuperado el 6/3/2022 de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-11881.

BOE (2015c). Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público. Recuperado el 6/03/2022 de https://www.boe.es/buscar/act.php?id=BOE-A-2015-11719.

BOE (2016a). Reglamento del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Recuperado el 9/01/2020 de https://www.boe.es/doue/2016/119/L00001-00088.pdf.

BOE (2016b). Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad. Recuperado el 19/04/2021 de https://www.boe.es/eli/es/res/2016/10/07/(5).

BOE (2018). Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Recuperado el 10/7/2021 de https://www.boe.es/buscar/doc.php?id=BOE-A-2018-12257.

BOE (2019). Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones. Recuperado el 8/02/2020 de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-15790.

BOE (2022a). Código de Derecho de la Ciberseguridad. Recuperado el 11/08/2022 de https://bit.ly/3ddkq7U.

BOE (2022b). Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Recuperado el 4/06/2022 de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191.

Boellstorff, T. (2013). Making Big Data, in Theory. *First Monday*.

Buzan, B., Waever, O., y Wilde, J. (1998). *Security. A new framework for analysis*. Lynne Rienner.

Calder, A. (2016). *Nueve pasos para el éxito: Una visión de conjunto para la aplicación de la ISO 27001:2013*. IT Governance Publishing.

Carlton, M. (2016). *Development of a Cybersecurity Skills Index: A Scenarios-Based, Hands-On Measure of Non-IT Professionals' Cybersecurity Skills*. PhD thesis, Nova Southeastern University.

Carlton, M., Levy, Y., y Ramim, M. (2019). Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. *Information & Computer Security*, 27(1):101–121.

CCN (2020a). Guía de Seguridad de las TICCCN-STIC 824. Recuperado el

21/04/2021 de https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/542-ccn-stic-824-informacion-del-estado-de-seguridad/file.html.

CCN (2020b). INES - Informe universidades. Technical report, CCN-CERT. INFORME EJECUTIVO CCN-CERT IT 28/20.

CCN-CERT (2010). Glosario de términos. Recuperado el 8-12-2019 en https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html.

CCN-CERT (2015). Anexo II. Medidas de seguridad. Recuperado el 12/10/2020 de https://www.ccn-cert.cni.es/publico/ens/ens/index.html.

CCN-CERT (2018). Informe de Amenazas y Tendencias.

CCN-CERT (2019). Ciberamenazas y Tendencias 2019. Recuperado el 9/5/2020 de https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3767-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-resumen-ejecutivo-2019/file.html.

CCN-CERT (2021a). Esquema Nacional de Seguridad – Preguntas Frecuentes. Recuperado el 3/01/2021 de https://www.ccn-cert.cni.es/publico/dmpublidocuments/ENS-FAQ.pdf.

CCN-CERT (2021b). Publicado en el BOE el Real Decreto de transposición de la Directiva europea NIS. Recuperado el 11/7/2021 de https://www.ccn-cert.cni.es/seguridad-al-dia/noticias-seguridad/10774-publicado-en-el-boe-el-real-decreto-ley-de-transposicion-de-la-directiva-europea-nis.html.

CE (2020). Ciberseguridad: revisión de las normas de la UE sobre la seguridad de las redes y sistemas de información. Recuperado el 11/7/2021 de https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Ciberseguridad-revision-de-las-normas-de-la-UE-sobre-la-seguridad-de-las-redes-y-sistemas-de-informacion_es.

CE (2021). Proposal for directive on measures for high common level of cybersecurity across the Union. Recuperado el 11/7/2021 de https://digital-

strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union.

Chowdhury, N., Katsikas, S., y Gkioulos, V. (2022). Modeling effective cybersecurity training frameworks: A delphi method-based study. *Computers & Security*, 113.

CISA (2009). Security tip (st04-001). Recuperado el 1/1/2020 en https://www.us-cert.gov/ncas/tips/ST04-001.

Comisión Europea (2020). Marco europeo de competencias digitales DIGCOMP. Recuperado el 11/08/2022 de http://www.ikanos.eus/wp-content/uploads/2018/03/DigComp-ikanos.pdf.

CONOCER, C. (2000). *Análisis Ocupacional y Funcional del Trabajo*. OEI.

Craigen, D., Diakun-Thibault, N., y Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*.

Crue (2017). Universitic 2017. Análisis de las TIC en las Universidades Españolas. Technical report, Crue Universidades Españolas.

CRUE-TIC (2020). Universidades españolas. Recuperado el 17/03/2020 de http://www.crue.org/universidades/SitePages/Universidades.aspx.

CRUE-TIC (2021). Adaptación del Kit de Concienciación de INCIBE a universidades. Recuperado el 25/03/2021 de https://tic.crue.org/wp-content/uploads/2017/11/10.30-Seguridad-presentacion_kit_incib_CRUE_20171026_US.pdf.

Cuñat, R. (2007). Aplicación de la teoría fundamentada (grounded theory) al estudio del proceso de creación de empresas. *XX Congreso anual de AEDEM*.

da Silva, A. C., Martins, F., Oliveira, L. B., Roberto, W., da Silva, C., Woehl, S., Catapan, A., y Martins, P. F. (2014). Competencias en gestión para una efectiva organización de búsqueda: Un estudio de caso en la Universidad de Brasil. *Revista de Globalización, Competitividad y Gobernabilidad*, 8(2):102–120.

Díaz-Bravo, L., Torruco-García, U., Martínez-Hernández, M., y Varela-Ruiz, M. (2013). La entrevista, recurso flexible y dinámico. *Investigación en educación médica*, 2(7).

de Vicente, J. J., Mallouli, W., Ruiz, J. F., y van Haastrecht, M. (2021). GEIGER: Solution for small businesses to protect themselves against cyber-threats. In *The 16th International Conference on Availability, Reliability and Security*, volume 2021, paginas 1–4. ACM.

Deloitte (2018). Estudio de ciberseguridad: Principales universidades en españa. Recuperado el 2/02/2020 de https://www2.deloitte.com/content/dam/Deloitte/es/Documents/governance-risk-compliance/Deloitte-ES-GRC-Ciberseguridad-Universidades.pdf.

Desjardins, J. (2019). What Happens in an Internet Minute in 2019? Recuperado el 4/4/2020 de https://www.visualcapitalist.com/what-happens-in-an-internet-minute-in-2019/.

DOD (2019). DOD Dictionary of Military and Associated Terms. Recuperado el 27-12-2019 en https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

DOD (2020). Cybersecurity maturity model certification. Recuperado el 1/7/2021 en https://ndisac.org/dibscc/cyberassist/cybersecurity-maturity-model-certification.

Downes, L. y Nunes, P. (2013). Big-bang disruption. *Harvard Business Review*.

EEES (2020). La respuesta de la universidad mediante el proyecto «Tuning». Recuperado el 1/05/2020 de http://www.eees.es/es/eees-estructuras-educativas-europeas.

EFE (2021). Un ataque informático obliga a desconectar todos los servidores de la Universidad Autónoma de Barcelona. Recuperado el 17/10/2021 de https://elpais.com/espana/catalunya/2021-10-11/un-ataque-informatico-obliga-a-desconectar-todos-los-servidores-de-la-universidad-autonoma-de-barcelona.html.

Eloff, J. y Eloff, M. (2005). Information security architecture. *Computer Fraud & Security*, 2005(11):10–16.

Enciclopedia Británica (2019). Norbert Wiener. Recuperado el 1/1/2020 de https://www.britannica.com/biography/Norbert-Wiener.

ENISA (2016). Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar

un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Recuperado el 11/7/2022 de https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016L1148&from=EN.

ENISA (2018). Cybersecurity CultureGuidelines: Behavioural Aspects of Cybersecurity. Technical report, European Union Agency for Cybersecurity.

ESCO (2020). Clasificación europea de capacidades, competencias, cualificaciones y ocupaciones. Recuperado el 27/06/2021 de https://ec.europa.eu/esco/portal/home.

Escobar, M. (2005). Las competencias laborales: ¿la estrategia laboral para la competitividad de las organizaciones? *Estudios Gerenciales*, 21(96):31–35.

Estepa, R., de Fuentes, J. M., González-Manzano, L., Estepa, A., Domínguez, J., y Segovia-Vargas, D. (2021). Selección de competencias en ciberseguridad para la formación en la industria de defensa. In *Actas de las VI Jornadas Nacionales (JNIC2021)*.

Fernández, C. y Piattini, M. (2012). *Modelo para el gobierno de las TIC basado en las normas ISO*, capitulo 1, paginas 21–27. AENOR.

Fielding, J. (2020). The people problem: how cyber security's weakest link can become a formidable asset. Recuperado el 9/02/2020 de https://reader.elsevier.com/reader/sd/pii/S1 361372320300063?token= D6DAD7D1A90840AC1229008 FA4B80DB398E033FCF4638 AAD1F67 BD6FF63331739320DED8C3C7FA6DA2898C58CC759D4B.

Flamholtz, E. y Randle, Y. (2011). *Corporate culture : The ultimate strategic asset.* Stanford University Press.

FOIL (2009). Metodología para la elaboración de Normas de Competencia Laboral. Recuperado el 18/10/2020 de https://www.ilo.org/wcmsp5/groups/public/—americas/—ro-lima/—sro-san_jose/documents/publication/wcms_207580.pdf.

Foro Nacional de Ciberseguridad (2021). Informe sobre la cultura de la ciberseguridad en España. Technical report, Foro Nacional de Ciberseguridad.

García-Peñalvo, F. (2020). *Método para la revisión sistemática de literatura.* Universidad de Salamanca.

Gibson, W. (1997). *Neuromante (José Arconada y Javier Ferreira trad.).* Minotauro. (Obra original publicada en 1984).

Gil, J. A. (2015). *Metodología cuantitativa en educación.* UNED - Universidad Nacional de Educación a Distancia.

Gitelman, L. (2013). *"Raw Data" Is an Oxymoron.* The MIT Press.

Glaser, B. G. y Strauss, A. L. (2000). *The Discovery of Grounded Theory. Strategies for Qualitative Research.* Aldine Transaction.

Gonczi, A. y Athanasou, J. (1996). *Instrumentación de la educación basada en competencias. Perspectiva de la teoría y la práctica en Australia.* Limusa, Mexico.

González, J. y Wagenaar, R. (2003). *Tuning Educational Structures in Europe.* Comisión Europea.

González, n. y Díaz, M. (2013). *Introducción al análisis estadístico multivariado aplicado*, capitulo 8, paginas 232–253. Universidad del Norte.

Grama, J. y Petersen, R. (2013). Governance, Risk, and Compliance: Why Now? *EDUCAUSE Review.*

Guerrero, D. y de los Ríos, I. (2013). Modelos internacionales de competencias profesionales. *DYNA: Ingeniería e industria*, 88(3):266–270.

Haqaf, H. y Koyuncu, M. (2018). Understanding key skills for information security managers. *International Journal of Information Management*, 43:165–172.

Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., Hildebrandt, T., Tsakirakis, G., Oikonomou, F., Leftheriotis, G., y Koshutanski, H. (2020). Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees. *Applied Sciences*, 10(16):5702.

Hernández, R., Fernández, C., y Baptista, P. (2014). *Metodología de la investigación*, capitulo Capítulo14, paginas 394–467. McGraw-Hill, sexta edition.

Herzog, P. (2010). *The Open Source Security Testing Methodology Manual.* ISECOM, tercera edition.

Hiscox (2020). Hiscox cyberclaims report2020. Recuperado el 11/04/2021 de https://www.hiscox.es/sites/spain/files/2021-04/21444-Claims-cyber-report-2020-final2.pdf?utm_source=Press&utm_medium=ndp.

IBM (2018). IBM X-Force Threat Intelligence Index 2018. *IBM Security*.

IDC (2020). Global ICT Spending. Forecast 2020 - 2023. Recuperado el 6/9/2021 de https://www.idc.com/promo/global-ict-spending/forecast.

INC (2020). Catálogo Nacional de Cualificaciones Profesionales. Recuperado el 1/05/2020 de https://incual.mecd.es/bdc. Instituto Nacional de Cualificaciones.

INCIBE (2015). Gestión de riesgos. Una guía de aproximación para el empresario. Technical report, Instituto Nacional de Ciberseguridad.

INCIBE (2019a). Expuestos datos de alumnos de la Universidad de Valladolid. Recuperado el 23/02/2020 de https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/expuestos-datos-alumnos-universidad-valladolid.

INCIBE (2019b). Másteres y grados en ciberseguridad en españa. Recuperado el 28/12/2019 en https://www.incibe.es/sites/default/files/paginas/talento/catalogos - formacion/catalogo-masteres-ciberseguridad-mayo-2019.pdf.

INCIBE (2020a). Balance de ciberseguridad 2020. Recuperado el 22-05-2021 en https://www.incibe.es/sites/default/files/paginas/que-hacemos/balance_ciberseguridad_2020_incibe.pdf.

INCIBE (2020b). Incidente de seguridad en la Universidad de Burgos. Recuperado el 23/02/20202 de https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/incidente-seguridad-universidad-burgos.

INCIBE (2020c). La Universidad de Cádiz sufre ciberataque de ransomware. Recuperado el 28/07/2020 de https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/universidad-cadiz-sufre-ciberataque-ransomware.

INCIBE (2021a). Campaña de smishing suplanta al SEPE utilizando como gancho los ERTE. Recuperado el 9/5/2021 de https://www.incibe.es/protege-tu-empresa/avisos-seguridad/campana-smishing-suplanta-al-sepe-utilizando-gancho-los-erte.

INCIBE (2021b). Incidente de seguridad afecta a diferentes organismos. Recuperado el 9/5/2021 de https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/incidente-seguridad-afecta-diferentes-organismos.

INCIBE (2021c). La UCLM ha sido víctima del ransomware Ryuk. Recuperado el 8/05/2021 de https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/uclm-ha-sido-victima-del-ransomware-ryuk.

INCIBE (2022). Ransomware contra la Universitat Oberta de Catalunya. Recuperado el 26/07/2022 de https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/ransomware-universitat-oberta-catalunya.

Infante-Moro, A., Infante-Moro, J. C., y Gallardo-Pérez, J. (2022). Factores claves para concienciar la ciberseguridad en los empleados. *Revista de Pensamiento Estratégico y Seguridad CISDE*.

INTECO (2009). Implantación de un SGSI en la empresa . Recuperado el 1/03/2020 de https://bit.ly/3nx4wHD.

Interpol (2020). Ciberdelincuencia. Recuperado el 9/02/2020 de https://www.interpol.int/es/Delitos/Ciberdelincuencia.

Irigoin, M. y Vargas, F. (2002). *Competencia laboral: manual de conceptos, métodos y aplicaciones en el sector salud*. Organización Internacional del Trabajo. CINTERFOR, Montevideo.

ISACA (2020). ISACA Glossary. Recuperado el 28/01/20202 de https://www.isaca.org/Pages/Glossary.aspx?tid=2077&char=C.

ISACA (2021). COBIT. Recuperado el 19/7/2021 de https://www.isaca.org/resources/cobit.

ISO (2018). ISO Standars Development. Recuperado el 18/01/2020 de https://bit.ly/3yFB8E6.

Kaspersky (2019). What is cyber-security? Recuperado el 3/1/2020 de https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security.

Kawulich, B. (2005). La observación participante como método de recolección de datos. *Forum: Qualitative Social Research*, 6(2).

Khan, S., Wang, S., y Hodhod, R. (2019). viCyber: An Intelligent Curriculum Design Tool for Cybersecurity Education. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*, pagina 1252. ACM.

Kitchenham, B. (2004). Procedures for Performing Systematic Reviews. techreport, Keele University.

Lasse, K. (2018). State of the iot 2018: Number of iot devices now at 7b – market accelerating. Recuperado el 08-12-2019 en https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/.

Lebek, B., Uffen, J., Neumann, M., y Hohler, B. (2013). Towards A Needs Assessment Process Model For Security, Education, Training And Awareness Programs: An Action Design Research Study. In *ECIS*.

Levy-Leboyer, C. (1997). *Gestión de las competencias.* Gestión 2000.

Lipschutz, R. (1995). *On security*, capitulo 3, paginas 46–86. Columbia University Press.

Lozano, M. (2017). 2017, el año en que las empresas se concienciaron en ciberseguridad. Recuperado el 6-12-2019 en https://www.incibe.es/protege-tu-empresa/blog/2017-el-ano-las-empresas-se-concienciaron-ciberseguridad.

López, A. y Ruiz, J. (2012). ISO 27000.es. Recuperado el 16/01/2020 de http://www.iso27000.es.

Álvarez, G. y María, C. (2006). Una aproximación al concepto de cultura organizacional. *Universitas Psychologica*, 5(1):163–174.

Mañas, J. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método*, capitulo 1, pagina 6. Ministerio de Hacienda y Administraciones Públicas.

Maconachy, W., Schou, C., Ragsdale, D., y Welch, D. (2001). A Model for Information

Assurance: An Integrated Approach. *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*.

Mahfuth, A., Yussof, S., Abu Baker, A., y Ali, N. (2017). A systematic literature review: Information security culture. In *International Conference on Research and Innovation in Information Systems (ICRIIS)*. Recuperado el 23/01/2020 de https://ieeexplore.ieee.org/abstract/document/8002442.

Marelli, A. (1999). Introducción al análisis y desarrollo de modelos de competencia. documento de trabajo.

marketcap.com (2022). Largest Companies by Market CapLargest Companies by Market Cap. Recuperado el 14/05/2022 de https://companiesmarketcap.com/.

Martín, F. (2019). Muertes y daños materiales por desastres naturales en 2018. Recuperado el 8/02/2020 de https://www.tiempo.com/ram/499691/muertes-y-danos-materiales-por-desastres-naturales-en-2018/.

Martínez, P. M. M. (2011). La tutoría sanitaria: mapa funcional ¿amenaza u oportunidad? *Revista de Investigación Educativa*, 29:111–135.

Mayer-Schönberger, V. y Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work and Think*. John Murray Press.

McClelland, D. (1973). Testing for Competence Rather Than for "Intelligence". *American Psychologist*.

McCumber, J. (1991). Information Systems Security: A Comprehensive Model. In *Proceeding of the 14th National Computer Security Conference*.

Mcnay, I. (1995). From Collegial Academy to the Corporate Enterprise: The Changing Cultures of Universities. Recuperado el 11/06/2022 de https://bit.ly/3OZcpkD.

Mendivil, J., Gutierrez, M., y Sanz, B. (2021). Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura. *Pixel - Bit*.

Mendívil, J., Gutiérrez, M., y Sanz, B. (2021). Mapa Funcional de competencias en seguridad para el personal no TI de las universidades españolas. In *Investigación en*

Ciberseguridad. Jornadas Nacionales de Investigación en Ciberseguridad, number 34, paginas 319–326. Ediciones de la Universidad de Castilla-La Mancha.

Minsait (2021). Informe de Madurez de Ciberseguridad. Technical report, Minsait.

Mitnick, K. (2005). A convicted hacker debunks some myths. *CNN*. Recuperado el 13/12/2019 de http://edition.cnn.com/2005/TECH/internet/10/07/kevin.mitnick.cnna/index.html.

Mohajan, H. (2018). Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Environment and People*, 7(1).

Mohammad Salman, Showkat Ahmad Ganie, I. S. (2020). The concept of competence: a thematic review and discussion. *European Journal of Training and Development*.

Muñoz, R. (2021). Everis revela que el ciberataque de finales de 2019 le costó 15 millones de euros. Recuperado el 10/10/2021 de https://elpais.com/economia/2021-06-09/everis-revela-que-el-ciberataque-de-finales-de-2019-le-costo-15-millones-de-euros.html.

NICE (2021). National Initiative for Cybersecurity Education. Recuperado el 27/6/2021 de https://www.nist.gov/itl/applied-cybersecurity/nice.

NIST (1998). Information Technology Security Training Requirements: a Role- and Performance-Based Model. Recuperado el 28/7/2021 de https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=151633.

NIST (2003). Building an Information Technology Security Awareness and Training Program. Recuperado el 28/7/2021 de https://csrc.nist.gov/publications/detail/sp/800-50/final.

NIST (2011). Managing InformationSecurity Risk. Recuperado el 26/7/2021 de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf.

NIST (2018). Framework for Improving Critical Infrastructure Cybersecurity. Recuperado el 4/7/2021 en https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

NIST (2020). Security and Privacy Controls for Federal Information Sys-

tems and Organizations. Revision 5. Recuperado el 31/7/2021 en https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

NIST (2021a). CSF. An Introduction to the Components of the Framework. Recuperado el 4/7/2021 de https://www.nist.gov/cyberframework/online-learning/components-framework.

NIST (2021b). Sp 800 series. Recuperado el 26/7/2021 de https://csrc.nist.gov/publications/sp800.

Nosworthy, J. D. (2000). Implementing InformationSecurity In The 21st Century. Do You Have the Balancing Factors? *Comput. Secur.*, 19.

OEA (2019). Marco NIST. Un abordaje integral de la Ciberseguridad. Recuperado el 3/7/2021 de https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf.

OISSG (2006). *Information Systems Security Assessment Framework*, capitulo 3, paginas 26–27. Open Information Systems Security Group.

OIT (2020). Banco de Competencias Laborales. Recuperado el 1/05/2020 de https://www.oitcinterfor.org/banco-competencias-laborales/inicio.

ONTSI (2019). Estudio sobre la ciberseguridad y confianza en los hogares españoles. Recuperado el 12/11/2019 en https://www.ontsi.red.es/es/estudios-e-informes/ciberseguridad-y-confianza-en-los-hogares-espanoles-abril-2019.

ONTSI (2021). Informe Anual del sector de las TIC, los medios y los servicios audiovisuales 2020. Technical report, Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información.

Onumo, A., Ullah-Awan, I., y Cullen, A. (2021). Assessing the Moderating Effect of Security Technologies on Employees Compliance with Cybersecurity Control Procedures. *Association for Computing Machinery*, 12(2).

OSA (2020). Open security architecture. Recuperado el 20/03/2020 de http://www.opensecurityarchitecture.org/cms/.

Ottis, R. y Lorents, P. (2010). Cyberspace: Definition and implications. Reading: Academic Conferences International Limited. Recuperado el 27-12-2019 en https://search-proquest-com.proxy-oceano.deusto.es/docview/869617247?accountid=14529.

OWASP (2021a). Open Web Application Security Project. Recuperado el 19/7/2021 de https://owasp.org/.

OWASP (2021b). Web Security Testing Guide. Recuperado el 18/7/2021 de https://owasp.org/www-project-web-security-testing-guide/v42/.

PAE (2020). Esquema Nacional de Seguridad - ENS. Recuperado el 19/03/2020 de https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Seguridad_Inicio /pae_Esquema_Nacional_de_Seguridad.html.

Paulsen, C. y Byers, R. (2019). Glossary of Key Information Security Terms. Recuperado el 8/01/20202 de https://www.nist.gov/publications/glossary-key-information-security-terms-2.

Pender-Bey, G. (2019). The Parkerian Hexad: The CIA Expanded. Master's thesis, Lewis University.

Pfleeger, C. (1989). *Security in Computing*, capitulo 1, paginas 4–6. Prentice Hall Professional Technical Reference.

PwC (2020). Informe del estado de cultura de ciberseguridad en el entorno empresarial. Technical report, PricewaterhouseCoopers.

RAE (2019). Diccionario de la lengua española.

RAE (2021). Cultura. Recuperado el 28/02/2021 de https://dle.rae.es/cultura?m=form.

Rahim, N. H. A., Hamid, S., Kiah, M. L. M., Shamshirband, S., y Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes*, 44(4):606–622.

Remmele, B. y Peichl, J. (2021). Structuring a Cybersecurity Curriculum for Non-IT Employees of Micro- and Small Enterprises. In *The 16th International Conference on Availability, Reliability and Security*, volume 2021, paginas 1–7. ACM.

Rodríguez, M. (2022). La Universidad de Oviedo, afectada por un ciberataque procedente de Rusia. Recuperado el 2705/2022 de https://www.lavozdeasturias.es/noticia/asturias/2022/02/26/universidad-oviedo-afectada-ciberataque-procedente-rusia/00031645877244831842414.htm.

Ruth, D. (2006). Frameworks of managerial competence: limits, problems and suggestions. *Journal of European Industrial Training*.

Saltzer, J. H. y Schroeder, M. D. (1975). The Protection of Information in Computer Systems. *Fourth ACM Symposium on Operating System Principles*, 63(9):1278–1308.

Sampalo, F. J., Cortés, J., Gumbau, J. P., y Mendívil, J. (2018). Marco de recomendaciones de Seguridad y Auditoría en Universidades. *CRUE TIC*.

Schatz, D., Bashroush, R., y Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, 12(2):52–74. Recuperado el 13/12/2019 de https://commons.erau.edu/cgi/viewcontent.cgi?article=1476&context=jdfsl.

Schwab, K. (2016). *La cuarta revolución industrial*. Debate.

Schwandt, F. (2018). Digital economy compass 2019. Recuperado el 08-12-2019 en https://www.statista.com/study/52194/digital-economy-compass/.

SENA (2012). Guía de Apoyo para la Elaboración del Análisis Funcional. Recuperado el 11/10/2020 de https://bit.ly/3ygxkca.

Sistema Nacional de Certificación de Competencias Laborales (2010). Mirada comparativa sobre métodos para identificar competencias laborales. Documento de trabajo Nº 3. Recuperado el 4/10/2020 de https://bit.ly/3AocKtk.

Sithole, T., du Toit, J., Jaquire, V., y von Solms, S. (2020). A framework for a foundational cyber counterintelligence awareness and skills training programme. In *Proceedings of the 19th European Conference on Cyber Warfare*, paginas 510–517. ACPI.

Sánchez-Vallejo, M. A. (2021). Uno de los mayores oleoductos de Estados Unidos suspende sus operaciones tras sufrir un ciberataque. Recuperado el

23/8/2021 de https://elpais.com/economia/2021-05-08/la-mayor-red-de-oleoductos-de-eeuu-suspende-sus-operaciones-tras-sufrir-un-ciberataque.html.

Soderquist, K., Papalexandris, A., Ioannou, G., y Prastacos, G. (2010). From task-based to competency-based. A typology and process supporting a critical HRM transition. *Personnel Review*, 39(3):325–346.

Solms, R. y Niekerk, J. (2013). From information security to cyber security. *Computers & Security. Elsevier*, 2013(38):97–102.

Spinks, N. (2014). Grounded Theory. In *Encyclopedia of Research Design.*

Strate, L. (1999). The varieties of cyberspace: Problems in definition and delimitation. Western Journal of Communication, 63(3), 382-412. Recuperado el 27/12/2019 en https://search-proquest-com.proxy-oceano.deusto.es/docview/202724750?accountid=14529.

Straub, J. (2019). Hackers Could Kill More People Than a Nuclear Weapon. Recuperado el 8/02/2020 de https://www.livescience.com/cyberattacks-could-kill-more-than-nuclear-attacks.html.

Taherdoost, H. (2019). What Is the Best Response Scale for Survey and Questionnaire Design; Review of Different Lengths of Rating Scale / Attitude Scale / Likert Scale. *International Journal of Academic Research inManagement (IJARM)*, 8(1).

Tang, C. (2014). Establish a Dynamic Business Driven Integrative Information Security Architecture. *Applied Mechanics and Materials.*

Taylor, D. (2007). Competency frameworks, learning and developement and the CIPD. Recuperado el 1/05/2020 de https://donaldhtaylor.co.uk/insight/competency-frameworks-learning-and-development-and-the-cipd/.

The Cocktail Analysis (2019). Panorama actual de la Ciberseguridad en España. Recuperado el 6-12-2019 en https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf.

The Economist (2017). The world's most valuable resource is no longer oil, but data. *The Economist.*

TheOpenGroup (2021). Information security management maturity. O-ISM3. Recuperado el 19/8/2021 de https://www.opengroup.org/forum/security/infosecmanagement.

Tomás, M. y Castro, D. (2010). Multidimensional Framework for the Analysis of Innovationsat Universities in Catalonia. *Education Policy Analysis Archives*, 19(27).

Treviño, J. (2016). ¿De qué hablamos cuando hablamos de la "securitización" de la migración internacional en México?: una crítica. *Foro internacional*, 56:253–291.

Trim, P. y Lee, Y. (2021). The Global Cyber Security Model: Counteracting Cyber Attacks through a Resilient Partnership Arrangement . *Big Data and Cognitive Computing*, 5(3):32.

Ulven, J. B. y Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*, 13(2):39.

UNE (2008). Metodología de análisis y gestión de riesgos para los sistemas de información. Recuperado el 9/03/2020 de https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0041430.

Urquiza, A. (2009). *Creación de un Marco de Competencias para la Evaluación del Rendimiento de los Gestores de Sistemasde Información en las Grandes Organizaciones*. PhD thesis, Universidad de Alcalá.

van't Wout, C. (2019). Develop and Maintain a Cybersecurity Organisational Culture. In *ICCWS 2019 14th International Conference on Cyber Warfare and Security*, paginas 457–466.

Vargas, F. (2004). *Competencias clave y aprendizaje permanente*. OIT.

Vargas, F., Casanova, F., y Montanaro, L. (2001). *El enfoque de competencia laboral: manual de formación*. OIT. CINTERFOR.

Vasilachis, I. (2009). *Estrategias de investigación cualitativa*. Gedisa.

Vitorelli, K., Magalhaes, A., Campos, C., y Garcia, C. (2014). Hablando de la Observación Participante en la investigación cualitativa. *Index de enfermerí*.

Wang, Y., Qi, B., Zou, H.-X., y Li, J.-X. (2018). Framework of Raising Cyber Security

Awareness. In *2018 IEEE 18th International Conference on Communication Technology (ICCT)*, paginas 865–869. IEEE.

Watkins, M. D. (2013). What is organizational culture? and why should we care? *Harvard Business Review*.

WCS (2019). ¿Qué es el Corporate Compliance? Recuperado el 9/01/2020 de http://www.worldcomplianceassociation.com/que-es-compliance.php.

WEF (2021). The Global Risks Report 2021. Technical report, World Economic Forum.

White, R. (1959). Motivation reconsidered: The concept of competence. *Psychological Review*, 66(5):297–333.

Wilson, M. y Hash, J. (2003). *Building an Information Technology Security Awareness and Training Program*. NIST.

Witkin, B. R. y Altschuld, J. W. (1995). *Planning and Conducting Needs Assessments: A Practical Guide*, pagina 15. Sage Publications, Thousand Oaks, California.

Yousuf, M. (2007). Using Experts' Opinions Through Delphi Technique. *Practical Assessment, Research, and Evaluation*, 12(4).

Zhang-Kennedy, L. y Chiasson, S. (2021). A Systematic Review of Multimedia Tools for CybersecurityAwareness and Education. *Association for Computing Machinery*, 54(1).