isms forum

CSC
CYBER SECURITY CENTRE

III edición / 2026

Libro Blanco del CISO

PARTICIPANTES

COORDINADOR

Francisco Lázaro

GESTIÓN DE PROYECTO Y EDICIÓN:

Beatriz García

REVISORA

Concepción Cordón

DISEÑO Y MAQUETACIÓN:

Susana Marín

COAUTORES

Carlos Luque

Carlos A. Sáiz

César Ramos

Daniel Largacha

David Esteban

David de la Rosa

Gemma Deler

Gustavo Lozano

Iván Sánchez

Jesús Mérida

Mariano J. Benito

Nuria Lizarbe - Zamora

Rafael Hernández

Ramón Fernández

Ramón Ortiz

CONTENIDO

Objetivos y alcance de la 3ª edición

En ediciones anteriores de este Libro Blanco[1], ya se comentó cómo el rol del Chief Information Security Officer (CISO) está evolucionando rápidamente debido a un entorno digital cada vez más complejo, interconectado y arriesgado. Es una realidad que la Ciberseguridad ha dejado de ser una función puramente técnica para convertirse en un imperativo estratégico del negocio, directamente ligado a la resiliencia, la confianza y la creación de valor a largo plazo.

De este modo el CISO ya no es solo un responsable de la seguridad técnica, debe actuar no sólo como estratega del negocio, alineando la Ciberseguridad con los objetivos corporativos, sino como líder de riesgos operativos, capaz de anticipar y gestionar impactos financieros, reputacionales y regulatorios, y con capacidad de asesorar al comité ejecutivo y al consejo de administración, traduciendo riesgos técnicos en implicaciones de negocio comprensibles.

Así, la tercera edición del Libro Blanco del CISO tiene como objetivo consolidar una visión integral, actualizada y estructurada del rol del CISO en el contexto tecnológico, organizativo y regulatorio actual.

El documento persigue tres objetivos principales:

1. Clarificar el alcance real del rol del CISO: definir su función no solo desde la práctica profesional, sino desde su encaje en el sistema de gobierno corporativo, diferenciando con precisión entre actividades operativas de Ciberseguridad y responsabilidad directiva sobre el riesgo digital.

2. Alinear el rol con la evolución normativa y regulatoria: analizar cómo marcos como el ENS, la normativa de seguridad de redes y sistemas de información y la Directiva NIS2 han consolidado materialmente las funciones del responsable de la seguridad de la información, reforzando exigencias de gobierno, supervisión, independencia y rendición de cuentas.

3. Proporcionar una referencia estructurada para profesionales y organizaciones: ofrecer una guía que permita a quienes ejercen o aspiran a ejercer la función del CISO comprender sus bloques funcionales, su posicionamiento organizativo, sus relaciones internas y externas, sus responsabilidades jurídicas y los retos actuales y emergentes del entorno digital.

En cuanto a su alcance, esta edición no pretende ser un manual técnico de Ciberseguridad ni un compendio exhaustivo de herramientas o controles. Tampoco sustituye los marcos normativos o estándares de referencia. Su propósito es explicar cómo se articula el sistema de ciberseguridad desde una perspectiva directiva, cómo se gobierna el riesgo digital y cuál es la contribución específica del CISO en esa arquitectura.

El documento aborda:

- Las actividades estructurales de la Ciberseguridad como sistema integrado.
- Los perfiles profesionales asociados según el marco europeo ECSF.
- Las funciones directivas del CISO y su mapeo con actividades.
- La evolución normativa que consolida el rol.
- La relación con otros directivos y funciones corporativas.
- Los modelos organizativos habituales.
- Los retos tecnológicos, regulatorios y de talento.
- Su formación.
- Su responsabilidad jurídica.
- Gestión del talento, capacidades y liderazgo, entre otras cuestiones.

Quedan fuera de su alcance el desarrollo técnico detallado de arquitecturas específicas, la descripción operativa de herramientas concretas o la resolución casuística de incidentes individuales. Estas materias pertenecen al ámbito de ejecución técnica y no al gobierno del riesgo digital que centra esta obra.

Esta tercera edición refuerza así una idea central: la Ciberseguridad ya no puede entenderse como una función exclusivamente técnica, sino como una disciplina de gobierno corporativo. El CISO, con sus funciones y nivel organizativo es la figura que permite que esa disciplina se ejerza con coherencia, independencia y alineación estratégica.

Definición del rol del CISO

Con carácter previo al desarrollo de la presente función directiva, se hace constar que, a los efectos de este documento, las denominaciones “CISO”, Responsable de Seguridad de la Información (RSI), o “Responsable de Ciberseguridad”, deberán entenderse como equivalentes y utilizadas indistintamente, sin que dicha elección terminológica implique diferenciación competencial alguna.

El CISO, también denominado RSI o Responsable de Ciberseguridad, es la función directiva encargada de gobernar el riesgo digital en la organización y de estructurar el sistema de gestión de la Ciberseguridad.

Aunque cada organización define y ajusta el rol según sus obligaciones legales, estrategia y capacidades, en esencia podemos describirlo como el profesional que define y propone las políticas de seguridad y la estrategia de Ciberseguridad; establece el marco de gestión del riesgo; supervisa la implantación y eficacia de las medidas técnicas y organizativas; y asegura la capacidad de prevención, detección, respuesta y recuperación ante incidentes. Asimismo, actúa como punto de contacto con las autoridades competentes y los equipos de respuesta, coordinando la gestión y notificación de incidentes cuando procede.

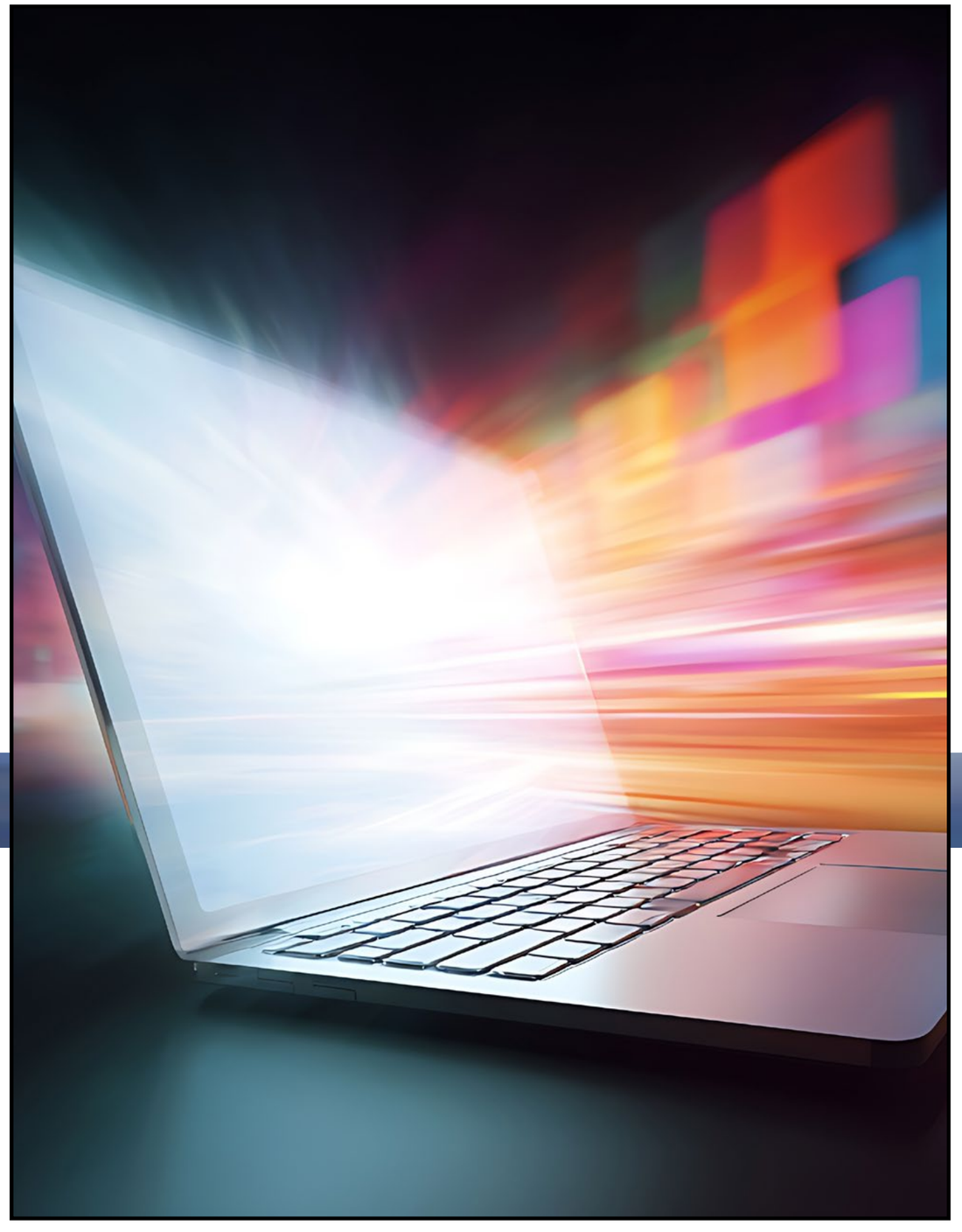
El CISO, debe disponer de una posición organizativa que garantice acceso efectivo a la alta dirección, recursos adecuados y la necesaria independencia respecto de la operación técnica de los sistemas, permitiendo una visión transversal y objetiva del riesgo digital, tanto de la organización, como de la cadena de suministro involucrada en las actividades de Ciberseguridad.

Su función no sustituye la responsabilidad última, en materia de Ciberseguridad, de la alta dirección, pero resulta esencial para que esta pueda ejercerla de forma informada, coherente y trazable conforme al marco normativo aplicable.

[1] ISMS Forum. Libro Blanco del CISO (2ª ed.). ***https://www.ismsforum.es/ficheros/descargas/segunda-edicion-del-libro-blanco-del-ciso-de-isms.pdf***

1.

Ciberseguridad: fundamentos y funciones



1.3. La Ciberseguridad como sistema de actividades coordinadas

La Ciberseguridad, desde una perspectiva directiva, se articula a través de un conjunto de actividades que permiten proteger los activos de información, reducir la exposición al riesgo y mantener la capacidad operativa de la organización. Estas actividades son interdependientes: ninguna resulta eficaz de forma aislada y todas requieren coordinación, priorización y alineación con los objetivos estratégicos.

Cada organización distribuye estas actividades de manera diferente en función de su estructura, tamaño, obligaciones normativas y nivel de madurez. Lo relevante es que la Ciberseguridad se gestione como un sistema integrado y no como un conjunto de acciones aisladas o meramente técnicas.

1.2. Fundamentos de la Ciberseguridad

Este libro no pretende ser una guía técnica exhaustiva, sino ofrecer el contexto necesario para comprender el entorno en el que el CISO desarrolla sus funciones. Por ello, se introducen brevemente conceptos esenciales que ayudan a entender la naturaleza de la Ciberseguridad.

1. Doble perspectiva técnica y directiva

La Ciberseguridad combina dos dimensiones complementarias:

- **Perspectiva técnica:** conjunto de tecnologías, procesos y controles, organizativos, procedimentales y técnicos, orientados a prevenir o mitigar incidentes que afecten a sistemas, redes o datos.
- **Perspectiva directiva:** gestión del riesgo derivado del uso intensivo de entornos digitales, con el objetivo de garantizar continuidad operativa, confianza y cumplimiento regulatorio.

Esta dualidad influye en todas las actividades de Ciberseguridad. La ejecución depende de capacidades especializadas, pero el objetivo final es permitir decisiones informadas sobre prioridades, inversiones y riesgo asumido.

2. Panorama actual del cibercrimen

El cibercrimen es una de las actividades ilícitas más lucrativas y escalables. Su impacto económico global se estima en magnitudes de cientos de miles de millones hasta billones de dólares anuales, impulsado por factores como:

- Deslocalización del delito y dificultad de persecución.
- Industrialización del ecosistema delictivo, con modelos *"as-a-service"*, mercados clandestinos y especialización de funciones.
- Automatización y repetición, que permiten escalar ataques como ransomware.
- Uso de criptoactivos para facilitar monetización y movimiento de fondos.

Los actores criminales presentan motivaciones diversas: lucro económico, ideología *(hacktivismo)*, intereses estatales (espionaje, sabotaje) y amenazas internas *(insider threats)*. Por ello, el CISO debe tratar el cibercrimen como un riesgo estructural más que como una amenaza puntual.

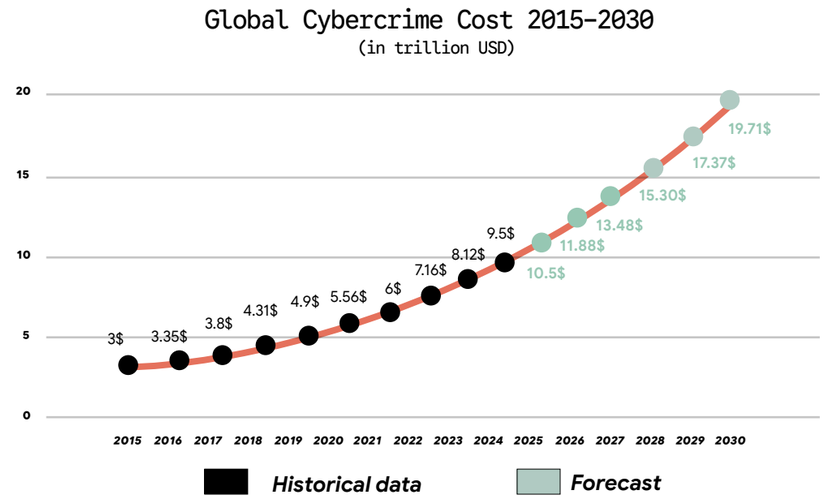


Figura 1. *Impacto económico global del cibercrimen. Elaborado a partir del Global Cybercrime Report 2025.*

3. Tríada CID y quinteto CITAD de la Ciberseguridad

La Tríada C-I-D es el modelo fundamental sobre el que se asienta toda la Ciberseguridad. Se utiliza para diseñar políticas de seguridad y evaluar los riesgos de cualquier sistema. Según este modelo, el objetivo final de la Ciberseguridad es que nuestras casas, negocios, organizaciones, instituciones, gobiernos y el mundo funcionen. Para ello, hay que garantizar tres pilares:

- Confidencialidad: garantizar que la información solo sea accesible por quienes están autorizados.
- Integridad: asegurar que los datos son exactos y no han sido alterados de manera indebida.
- Disponibilidad: asegurar que la información y los sistemas están accesibles cuando se necesitan.

Figura 2. *Modelo CID de la seguridad de la información*

A esas tres dimensiones, en otros marcos de referencia, como es el ENS, se le unen otras dos dimensiones, conformando así el acrónimo CITAD del quinteto dimensiones de seguridad:

- Autenticidad: garantiza la identidad o la fuente de los datos.
- Trazabilidad: permite reconstruir el historial de acciones sobre la información.

4. Panorama actual de amenazas: de los ataques comunes al Ransomware-as-aService

Existen muchos tipos diferentes de ciberataques, que afectan a esas dimensiones de la seguridad. Unos y otros han ido evolucionando, incorporando mecanismos empresariales (como la automatización, especialización, facilidades) o bien, añadiendo capacidades tecnológicas, Inteligencia Artificial (IA), entre otras. A título de ejemplo citaremos una serie de ataques básicos:

Categoría o amenaza	Tipo de ataque	Descripción	Pilar C-I-D afectado
Ataques que infligen daño	DoS/DDoS	Inundación de sistemas con solicitudes para colapsar su capacidad de respuesta	Disponibilidad
Suplantación de identidad	Phishing / Fraude al CEO	Técnicas de ingeniería social para engañar a víctimas y obtener activos o acceso	Confidencialidad
Intercepción	Man-in-the-Middle	Captura y posible alteración de información en tránsito entre interlocutores	Confidencialidad / Integridad
Software malicioso	Malware / Ransomware	Infiltración para dañar sistemas o cifrar datos exigiendo un rescate económico	Integridad / Disponibilidad

Figura 3. *Tipología de ciberataques y pilares de seguridad*

A estas amenazas, se han venido a incorporar nuevas formas, como la oferta de profesionales hackers para trabajos concretos, la irrupción de grandes colectivos asociados a los intereses geopolíticos de estados o la industrialización de las infecciones y la extorsión.

5. El modelo de Ransomware-as-a-Service (RaaS)

El modelo RaaS ejemplifica la industrialización del cibercrimen: el desarrollo, mantenimiento y distribución del ransomware se separan de su ejecución, permitiendo que actores con distintos niveles de capacidad técnica participen en campañas de gran escala.

Esta especialización ha incrementado el volumen y la frecuencia de los ataques, reduciendo las barreras de entrada y ampliando el número de organizaciones potencialmente afectadas. El resultado es un entorno de amenaza persistente, adaptable y menos predecible.

Desde la perspectiva de la organización, este modelo refuerza una idea clave: la Ciberseguridad no puede basarse en respuestas puntuales ni en la protección frente a escenarios aislados. La existencia de estructuras delictivas organizadas y sostenidas en el tiempo exige que las actividades de Ciberseguridad se conciban como un sistema permanente, coordinado y gobernado, capaz de prevenir, detectar y responder de forma consistente ante amenazas en continua evolución.

1.3. Macroactividades de la Ciberseguridad

Hay diversos marcos de Ciberseguridad que pueden ser tomados como referencia, que sea uno u otro depende en muchos casos del entorno geopolítico, cultura del sector y/o marco regulatorio, en el que se desenvuelve la entidad/empresa.

En este punto de lectura del libro, disponer de una visión por bloques de actividad facilita entender cómo se articula el núcleo de la Ciberseguridad y qué papel desempeña el CISO en su dirección, ejecución y supervisión. Estas macro actividades se retroalimentan entre sí y requieren de gobierno, priorización y alineación, con la estrategia corporativa.

En esta primera aproximación nos referiremos a las macro actividades que se derivan del Framework NIST. El modelo NIST es un ecosistema coherente de marcos y guías desarrollado por el National Institute of Standards and Technology para gestionar la ciberseguridad desde una perspectiva basada en riesgo, medible y gobernable.

El modelo se articula en tres capas principales:

- **Marco estratégico, NIST Cybersecurity Framework (CSF).** Define qué hay que hacer (visión de negocio, riesgo, gobierno)
- **Marco operativo y de control, NIST SP 800-53** el cual define qué controles concretos aplicar (catálogo de controles)
- **Guías especializadas;** como, por ejemplo: NIST SP 800-61 (incidentes) o NIST SP 800-30 (riesgos)

El NIST Cybersecurity Framework estructura la ciberseguridad en seis funciones: **Govern**, que establece el gobierno, la estrategia y la supervisión del riesgo por parte de la dirección; **Identify**, que permite comprender los activos, el contexto y los riesgos; **Protect**, que define e implanta controles preventivos para salvaguardar la información; **Detect**, que habilita la monitorización continua y la identificación de anomalías; **Respond**, que articula la gestión coordinada de incidentes de seguridad; y **Recover**, que asegura la restauración de capacidades y la mejora tras incidentes, cerrando el ciclo de resiliencia.

En el siguiente gráfico se representan las seis funciones del CSF. Además, se ha incorporado la función de medición y mejora que, si bien no constituye estrictamente una función independiente del CSF, sí forma parte del ciclo de madurez y se considera de especial relevancia.

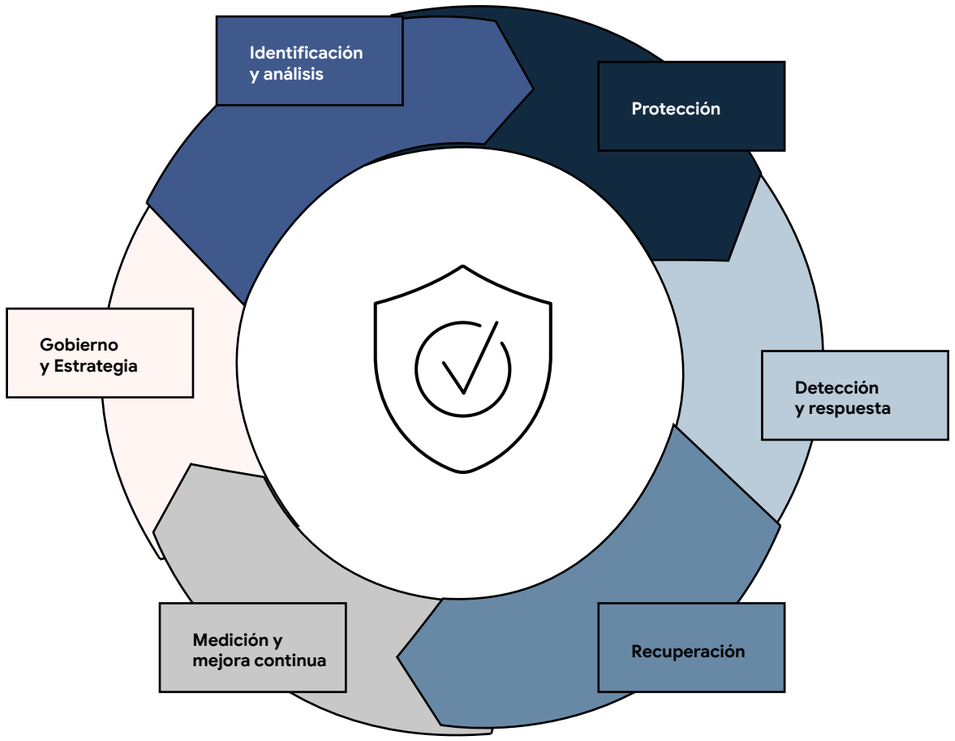


Figura 4. *Ciclo de actividades de la Ciberseguridad*

Gobierno de la Ciberseguridad

Las actividades de gobierno constituyen el marco estructural que permite que la Ciberseguridad funcione como una disciplina coherente, alineada con la estrategia corporativa y capaz de generar valor más allá del mero cumplimiento normativo. Sin un gobierno sólido, las iniciativas de seguridad tienden a fragmentarse, respondiendo a urgencias tácticas en lugar de a una visión de riesgo y resiliencia a medio y largo plazo.

Desde el punto de vista operativo, el gobierno de la Ciberseguridad se materializa en actividades orientadas a traducir los objetivos estratégicos de la organización en directrices claras para la gestión del riesgo digital. Esto incluye la definición de principios rectores, la priorización de dominios críticos y la determinación explícita del nivel de riesgo que la organización está dispuesta a asumir en función de su apetito de riesgo.

Un elemento central de estas actividades es la asignación clara de roles y responsabilidades. La existencia de ambigüedad en la toma de decisiones, en la aceptación del riesgo o en la ejecución de controles genera ineficiencias y expone a la organización a fallos sistémicos.

El gobierno de la Ciberseguridad también abarca las actividades relacionadas con la definición, aprobación, comunicación y revisión periódica del marco normativo interno. Este marco ayuda a las personas de la organización a conocer qué hay que hacer y cómo hay que hacerlo. Así mismo, protege a la organización desde el punto de vista legal y financiero. También protege a las personas ya que permite a las personas tomar las acciones necesarias sin miedo a las consecuencias. La revisión periódica de este marco permite adaptarlo a cambios en el entorno tecnológico, regulatorio y de negocio. Otra de las actividades que incorpora el gobierno de la Ciberseguridad es la definición del marco de gestión del riesgo, incluyendo los criterios de evaluación, los niveles de aceptación y los mecanismos de escalado y decisión. En el panorama actual, donde las inversiones y alternativas en materia de Ciberseguridad parecen ilimitadas, una buena gestión de riesgos permite priorizar las inversiones de modo que protejamos a la organización de los riesgos más probables y con más impacto. Se define *risk appetite* como la cantidad y tipos de riesgo que la organización está dispuesta a asumir. En función de este *risk appetite* se definen los planes estratégicos y el presupuesto, se optimiza la asignación de recursos y se traslada la estrategia de alto nivel en objetivos más específicos.

Además, en el contexto actual, donde se integra el uso de la IA, la automatización de procesos críticos o la dependencia de ecosistemas digitales complejos, el gobierno de la Ciberseguridad debe integrar consideraciones éticas, reputacionales y estratégicas junto a las puramente técnicas.

El gobierno de la Ciberseguridad, entendido como actividad, establece el marco necesario para que el conjunto del sistema funcione de forma coherente y alineada con los objetivos de la organización.

Un marco de gobierno eficaz se caracteriza por pocas decisiones claras y bien comunicadas, no por un gran volumen de normas difíciles de aplicar.

Identificar: conocimiento del entorno y del riesgo

Las actividades de identificación constituyen el punto de partida de toda estrategia de Ciberseguridad eficaz. Su objetivo es proporcionar a la organización una comprensión clara y compartida de qué se debe proteger, por qué es relevante y qué riesgos amenazan su capacidad de cumplir sus objetivos.

Este ámbito incluye, en primer lugar, la identificación y clasificación de activos, entendidos no solo como sistemas o infraestructuras tecnológicas (hardware y software), sino también como información, procesos críticos, servicios digitales y dependencias externas. Esta visión ampliada resulta esencial para evitar enfoques excesivamente centrados en la tecnología que ignoran impactos reales sobre el negocio. Identificar no es solo hacer inventario; es entender qué activos son el corazón del negocio para no protegerlo todo por igual, optimizando así el presupuesto.

A partir de este conocimiento, las actividades de identificación se orientan a evaluar la postura de seguridad de la organización y a analizar los riesgos asociados. Se deben identificar escenarios plausibles y su impacto, de forma que podamos priorizar aquellos que requieran atención preferente. Estas actividades generan información estructurada y objetiva para que las decisiones sobre los riesgos puedan ser tomadas en los niveles de gobierno correspondientes.

La identificación del riesgo asociado a terceros y a la cadena de suministro adquiere un peso creciente en entornos altamente externalizados. La cadena de suministro se ha convertido en uno de los vectores más críticos y complejos de la Ciberseguridad moderna. Estos riesgos se originan fuera del perímetro directo de control de la organización, pero tienen un impacto directo y significativo sobre su operación, reputación y continuidad del negocio. A lo largo del documento iremos tratando la cadena de suministro en aquellos apartados en los que deba ser contemplada; por ejemplo, cuando hablemos de la legislación nacional en materia de Ciberseguridad.

Otros riesgos que considerar son los provenientes de proveedores de servicios en la nube, socios tecnológicos o plataformas compartidas, que amplían la superficie de exposición y exigen actividades específicas de análisis y evaluación que permitan comprender dependencias críticas y puntos de fallo.

Estas actividades de identificación generan información clave para la toma de decisiones posteriores sobre protección, detección y respuesta.

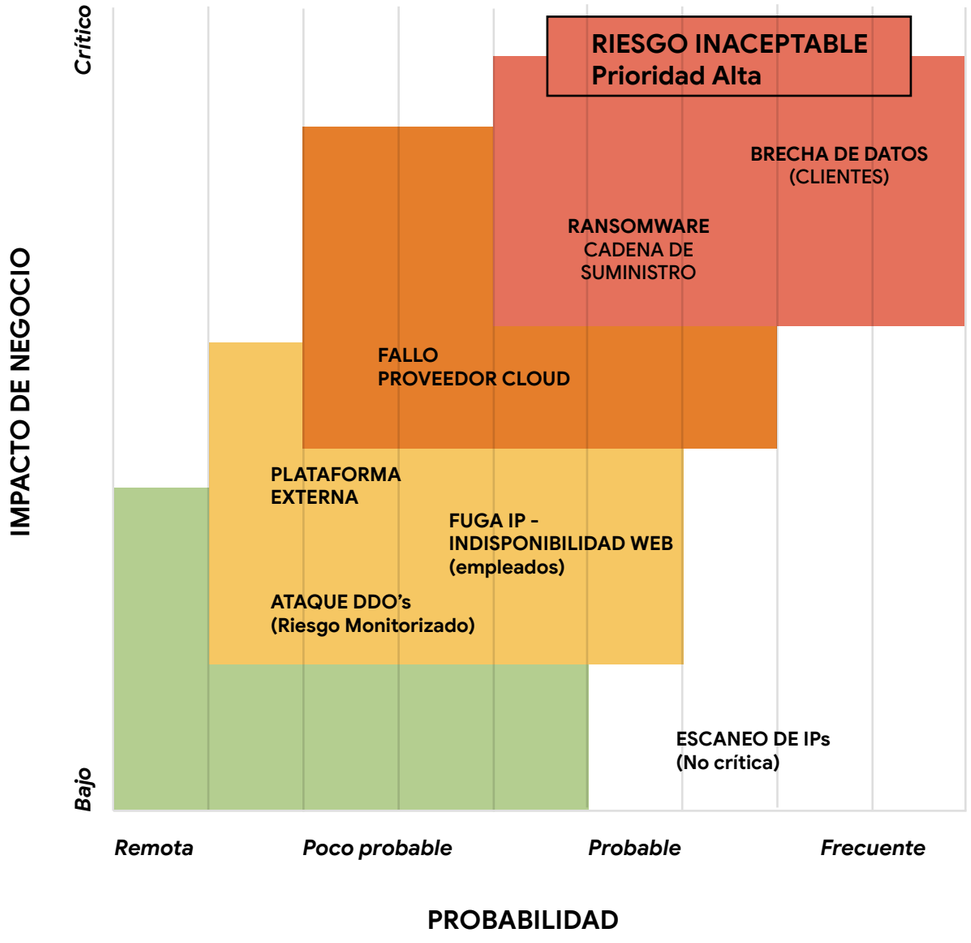


Figura 5. *Mapa de riesgos – Priorización y dependencias.*

Proteger: diseño y despliegue de medidas de seguridad

Las actividades de identificación constituyen el punto de partida de toda estrategia de Ciberseguridad eficaz. Las actividades de protección agrupan el conjunto de decisiones y controles destinados a reducir la probabilidad de que un riesgo identificado se materialice o, en su defecto, a limitar su impacto inicial. Estas actividades no deben entenderse como un catálogo de soluciones técnicas, sino como un proceso continuo de diseño, implantación y ajuste de medidas coherentes con el contexto de riesgo de la organización.

Como bien describe la guía NIST 800-39 (Managing Information Security Risk)[2], la arquitectura de seguridad debe verse como: **"...una parte integrada y esencial de la arquitectura empresarial que describe la estructura y el comportamiento de los procesos de seguridad, los sistemas, el personal y las subunidades organizativas, mostrando su alineación con la misión y los planes estratégicos. Proporciona la hoja de ruta para asegurar que las necesidades de protección de los procesos de negocio se asignen adecuadamente a los sistemas y entornos donde estos operan."**

Desde una perspectiva estructural, la protección comienza en el diseño de arquitecturas de seguridad.

Para comprender el alcance de este concepto, debemos entender que la arquitectura de seguridad no es una tarea puntual donde el arquitecto de seguridad define y coordina los principios y procesos que sostienen la protección de la organización.

Cuando hablamos de arquitectura de seguridad, tenemos que pensar en la arquitectura de todos los elementos que conforman nuestro sistema de activos de información: activos TI con su arquitectura de la red (network), seguridad del host (hardware, sistema operativo, aplicaciones y dispositivos individuales) y de los entornos nube y la información en sí misma, como principal activo de información.

En cuanto a la protección de redes y de hosts, hay que crear un diseño estructurado que se materializa en tres planos fundamentales:

Modelo	Enfoque de Red (Network)	Enfoque de Host
Lógico	Segmentación, firewalls y VPNs para controlar el flujo entre activos	Gestión de identidades (IAM), políticas de grupo (GPO) para privilegios internos
Físico	Seguridad del centro de datos, cámaras y control de acceso biométrico	Bloqueo de puertos USB, candados físicos
Técnico	Sistema de prevención de intrusiones (IPS) y cifrado en tránsito (TLS)	Antivirus / EDR, parches del sistema operativo y cifrado de disco (BitLocker)

Figura 6. *Tabla con ejemplos, para los tres planos, de elementos a ser contemplados en los enfoques de Red y de Host.*

[2] Managing Information Security Risk: Organization, Mission, and Information System View (NIST Special Publication 800-39). National Institute of Standards and Technology. ***https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=908030***

Los servicios en nube se basan en un modelo de responsabilidad compartida. El proveedor de los servicios es responsable de la seguridad “de” la nube y el cliente es responsable de la seguridad “dentro” de la nube. Esto incluye la responsabilidad final sobre la seguridad de los datos y accesos adecuados y dependiendo del modelo contratado (IaaS, PaaS, SaaS,), incluirá o no la seguridad de las aplicaciones y plataformas, además de los ajustes de configuración del sistema operativo, la red y el firewall.

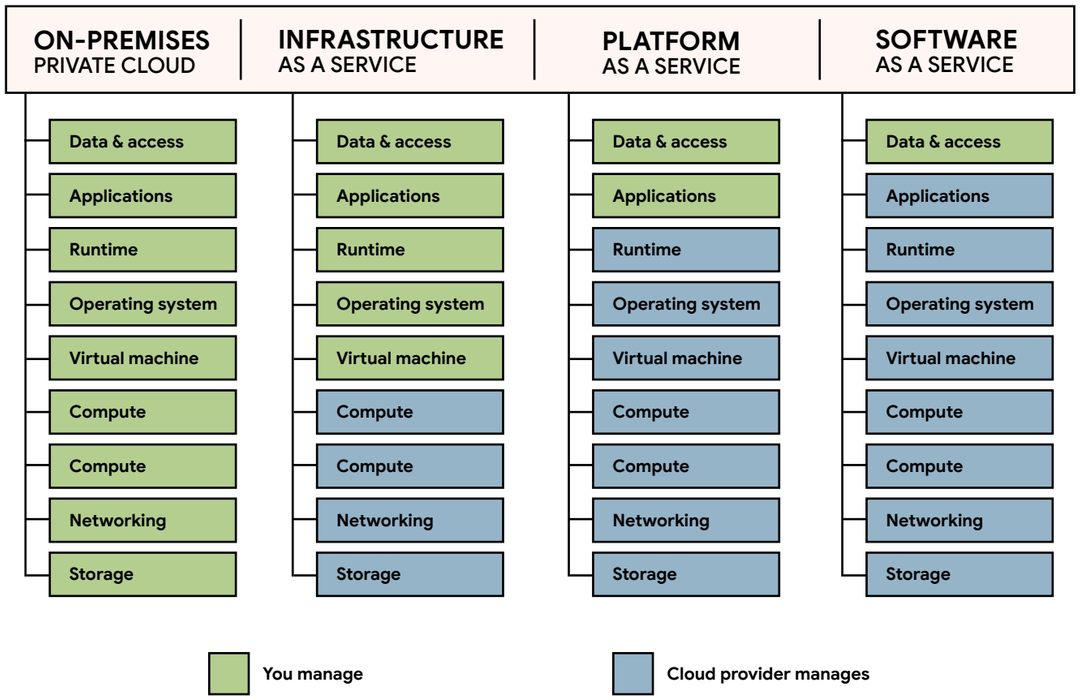


Figura 7. *Modelo tradicional de responsabilidad compartida. Fuente: varonis.com*

A veces estamos tan centrados en la tecnología y en los riesgos de estas, que nos olvidamos de que el verdadero elemento a proteger es la información; es decir, el dato y que el resto de los elementos son contingentes y que su valor estriba en el procesamiento que hacen de la información. Así, mientras que los firewalls y el cifrado protegen los perímetros y los activos, los sistemas de Prevención de Pérdida de Datos (DLP) se centran exclusivamente en el activo más valioso: la información. El objetivo del DLP es garantizar que los datos sensibles (propiedad intelectual, datos financieros, información de clientes) no abandonen la organización de manera no autorizada.

En estas breves consideraciones nos permitimos recordar que la protección de la información debe abordarse conforme a los principios de Ciberseguridad y privacidad desde el diseño y por defecto. Esto implica que, desde la fase inicial de concepción de un producto, sistema o servicio, la seguridad y la protección de datos formen parte de las decisiones estructurales: desde la definición de la arquitectura hasta su puesta en producción.

Este enfoque obliga a tener en cuenta la finalidad del activo o servicio, el marco normativo aplicable y las exigencias concretas que de él se derivan, entre ellas la limitación de la conservación y la reducción de la exposición de la información tratada. La seguridad no se añade al final; se incorpora como criterio de diseño.

En relación con la reducción de la exposición de datos personales y, en general, de información sensible existen dos mecanismos fundamentales, complementarios a la gestión de identidades y a las soluciones de prevención de fuga de información:

- → **La seudonimización:** sustituye identificadores directos por tokens. Es reversible bajo controles estrictos; adecuada cuando se necesita trazabilidad sin exponer identidad.
- → **La anonimización:** transformación irreversible que impide reidentificación; los datos dejan de estar sujetos al RGPD cuando la anonimización es efectiva.

La arquitectura moderna evoluciona hacia **Zero Trust:** la confianza no es implícita; se gana y verifica continuamente. El acceso se concede de forma condicional y dinámica, en función de la identidad, el contexto y el estado del activo.

Junto con la Ciberseguridad desde el diseño y por defecto, el principio de la seguridad por capas es otro de los pilares sobre los que se asienta la Ciberseguridad. De hecho, aunque sin nombrar a este último principio no hemos estado refiriendo a sus componentes cuando hemos mencionado elementos de forma individual.

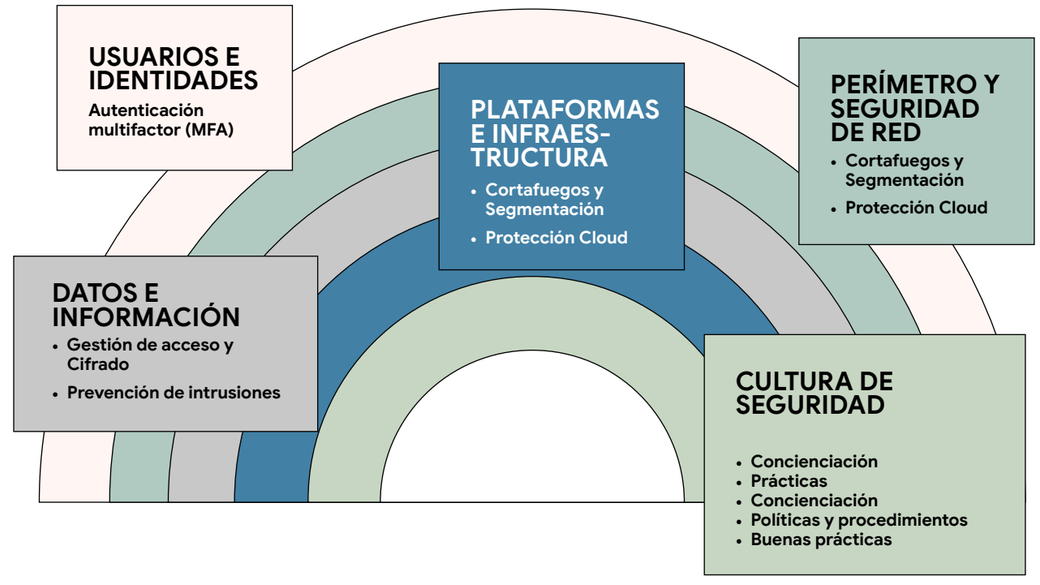


Figura 8. *Arquitectura de Protección en capas. La protección es un sistema integrado de decisiones de diseño y comportamiento.*

La concienciación es un control transversal, no es una formación puntual, sino la creación de una cultura en la que cada persona entiende su rol y actúa como primera línea de defensa.

Actividad	Objetivo	Ejemplo de implementación
Formación Continua	Proveer conocimientos básicos y actualizados.	Píldoras formativas mensuales sobre nuevas estafas.
Simulacros de Ataque	Evaluar la reacción real ante amenazas.	Campañas controladas de Phishing o Smishing.
Gamificación	Fomentar el compromiso a través del juego.	Rankings de departamentos que reportan más correos sospechosos.
Comunicación Interna	Mantener la seguridad en el "top of mind".	Alertas inmediatas ante una amenaza global detectada.

Figura 9. *Actividades de concienciación y formación en Ciberseguridad orientadas a reforzar el comportamiento seguro en la organización.*

Detectar: visibilidad y anticipación

Las actividades de detección parten de una premisa realista: ningún entorno digital es completamente inmune a incidentes de seguridad. Su objetivo principal no es impedir que el ataque se produzca, sino reducir al mínimo el tiempo durante el cual un adversario puede operar sin ser detectado, limitando así su capacidad de causar daño y facilitando una respuesta eficaz.

Para diseñar detección temprana se emplean marcos de amenazas:

- **Cyber Kill Chain (Lockheed Martin):** fases del atacante, de reconocimiento a acciones sobre el objetivo. Interrumpir cualquier fase impide el éxito, incluso tras un compromiso inicial.
- **MITRE ATT&CK®:** catálogo operativo de tácticas, técnicas y procedimientos (TTPs) utilizados por adversarios reales; permite diseñar casos de uso, identificar lagunas de cobertura y priorizar esfuerzos.

Figura 10. *Cyber Kill Chain*

Esta función incluye monitorización continua de eventos de seguridad (sistemas, redes, aplicaciones, nube), su correlación y análisis contextual, y la gestión de vulnerabilidades. La inteligencia de amenazas permite anticipar campañas y técnicas relevantes, ajustando dinámicamente la detección a escenarios plausibles y actuales.

La detección suele apoyarse en estructuras especializadas: SOC (centro de operaciones de seguridad) y, en mayor madurez, CSIRT. Para validar la efectividad real de las medidas de protección y detección, la organización debe entrenar y verificar sus capacidades mediante ejercicios de simulación técnicos y directivos.

Tipo de Ejercicio	Enfoque	Lo que realmente estamos validando
Red Team	Técnico y Adversario. Un equipo simula ser un atacante real con objetivos específicos.	¿Se han parcheado las vulnerabilidades críticas? ¿Funciona la segmentación de red? ¿El EDR bloquea la ejecución de código malicioso?
Blue Team	Defensivo. Es el equipo interno que debe identificar y bloquear al Red Team.	¿Son efectivas nuestras reglas de detección? ¿El equipo sabe interpretar las alertas antes de que el daño sea masivo?
Purple Team	Colaborativo. Red y Blue Team trabajan juntos en tiempo real.	Optimización de controles: el atacante muestra por dónde pasó y el defensor cierra esa brecha (parche o regla) al instante.
Simulacros de Crisis	Estratégico / Directivo. Ejercicios de mesa (Tabletop).	¿Funcionan los protocolos de comunicación? ¿Sabe la dirección cuándo debe notificar a la autoridad de protección de datos?

Figura 11. *Ejercicios clave para validar la eficacia operativa y la preparación ante incidentes.*

Responder y recuperar: gestión del impacto

Las actividades de respuesta y recuperación son la prueba de fuego de la Ciberseguridad. Ante un incidente, la capacidad para reaccionar coordinadamente, contener el daño y restablecer la operación determina no solo el impacto técnico, sino también las consecuencias económicas, legales y reputacionales.

Para asegurar una ejecución sistemática, la industria se apoya en PICERL, que estructura la gestión de incidentes en seis fases:

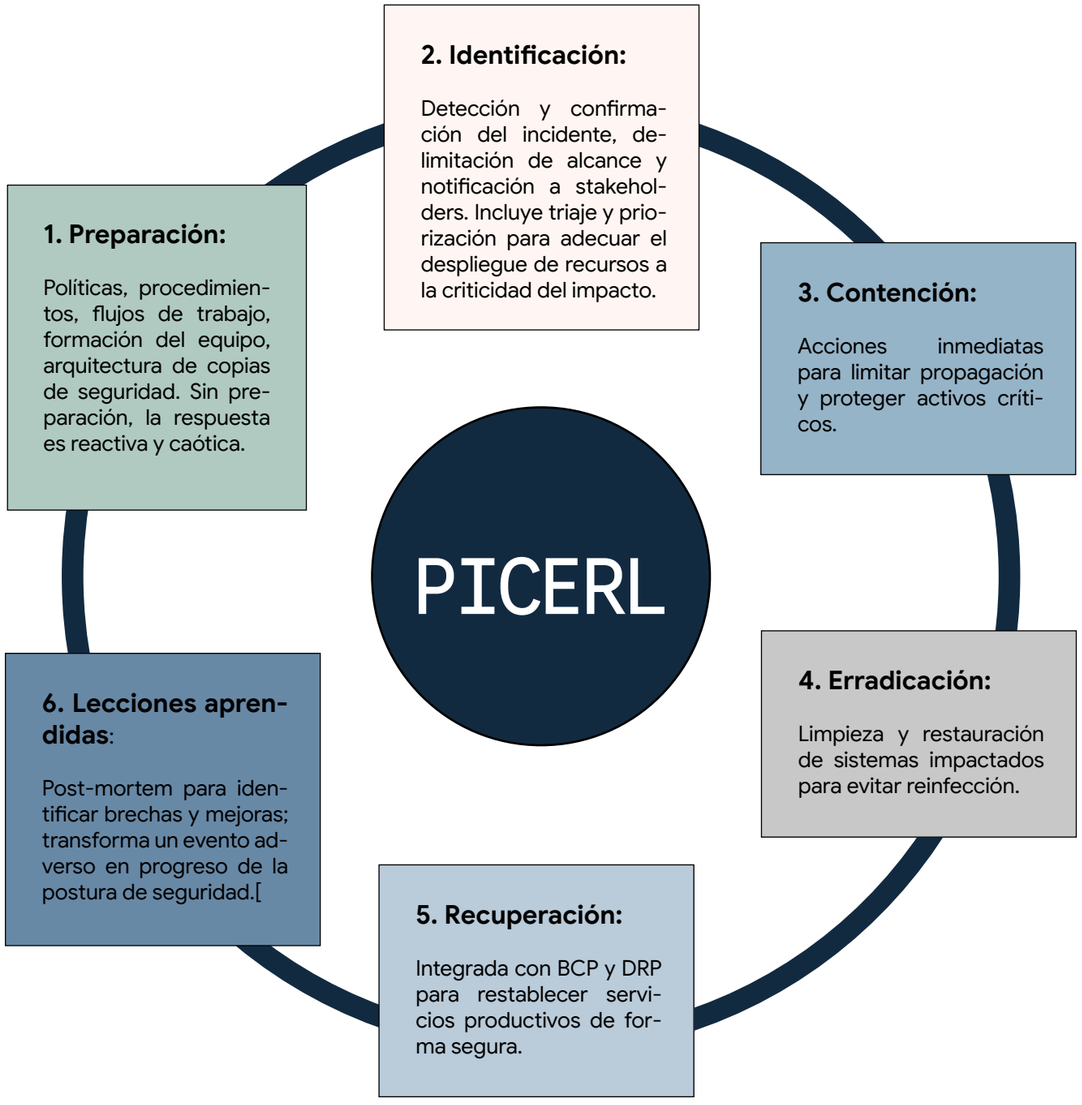


Figura 12. *El ciclo PICERL para la gestión de incidentes*

La diferencia entre un incidente gestionable y una crisis suele residir en la preparación previa, no en la gravedad técnica del ataque. Precisamente la gestión de crisis es otro de los pilares fundamentales en los que el CISO desempeña sus funciones con una visión integral y holística de la misma.

Medición y reporte orientado a la toma de decisiones

La medición y el reporte constituyen actividades transversales del sistema de Ciberseguridad, cuyo objetivo es proporcionar información fiable y comprensible sobre el estado del riesgo digital y la eficacia de las medidas implantadas.

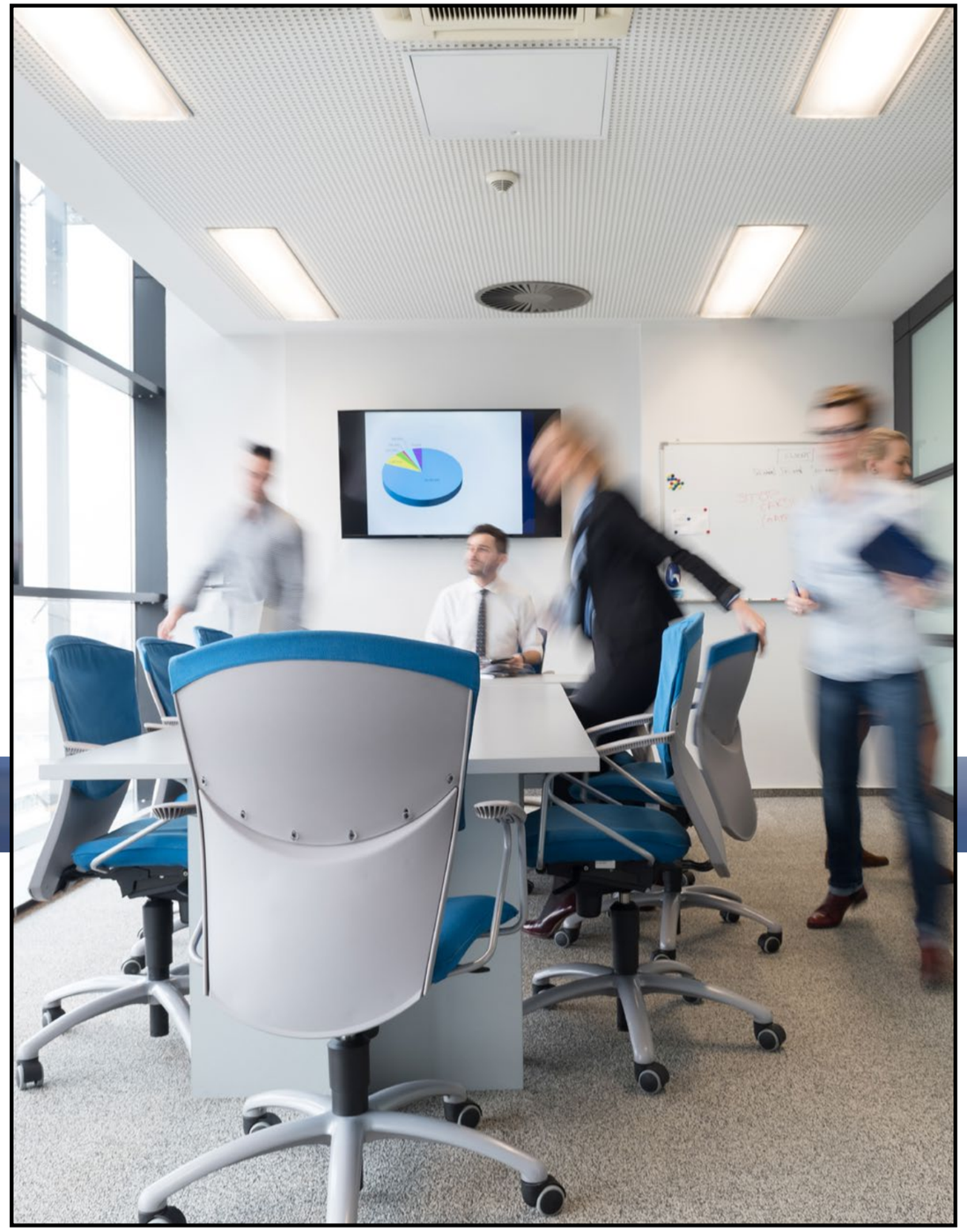
Estas actividades permiten transformar datos técnicos en información relevante para la organización, facilitando la toma de decisiones mediante la priorización de iniciativas, la asignación de recursos y la evaluación del impacto de las decisiones adoptadas. Para ello, resulta esencial que los indicadores utilizados estén alineados con los objetivos de la organización y reflejen tanto el nivel de exposición al riesgo como la capacidad de prevención, detección y respuesta.

Un sistema de medición eficaz contribuye a la mejora continua de la Ciberseguridad, al permitir identificar tendencias, anticipar desviaciones y valorar la evolución del riesgo en el tiempo. El reporte periódico, por su parte, refuerza la coherencia del conjunto de actividades y favorece una toma de decisiones informada en los distintos niveles de la organización.

Consideradas de forma conjunta, estas actividades configuran el sistema operativo de la Ciberseguridad en la organización. Su eficacia depende de que se encuentren coordinadas, priorizadas y alineadas con los objetivos estratégicos, lo que exige un ejercicio continuado de dirección y supervisión. El apartado siguiente profundiza en las funciones que permiten articular este sistema desde una perspectiva directiva y de gobierno, y en el papel que desempeña el CISO en dicho contexto.

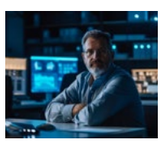
2.

Funciones



2.1. Perfiles profesionales de la Ciberseguridad conforme al Marco de referencia European Cybersecurity Skills Framework (ECSF)

El ECSF establece 12 perfiles profesionales estándar que estructuran las competencias necesarias para una función de Ciberseguridad completa. A continuación, se presentan los perfiles definidos por el marco:

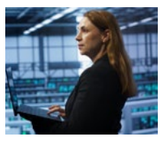


1. Chief Information Security Officer (CISO)

Responsable estratégico de la Ciberseguridad organizativa. Define la política, el apetito de riesgo, el roadmap de seguridad y reporta a alta dirección. Supervisa cumplimiento, riesgos e incidentes críticos.

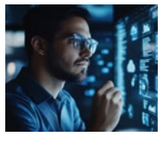
2. Cybersecurity Architect

Diseña la arquitectura de seguridad de sistemas y redes. Define controles técnicos, principios de segmentación, identidad y protección en entornos IT/OT/cloud. Traduce requisitos de riesgo en diseño técnico.



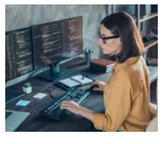
3. Cybersecurity Engineer

Implementa y mantiene controles de seguridad (EDR, firewalls, IAM, cifrado, etc.). Opera técnicamente las soluciones definidas por la arquitectura y asegura su correcto funcionamiento.



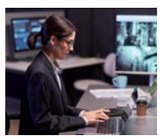
4. Cybersecurity Risk Manager

Identifica, analiza y evalúa riesgos de Ciberseguridad. Mantiene el registro de riesgos, propone mitigaciones y coordina revisiones periódicas conforme al marco de gestión adoptado.



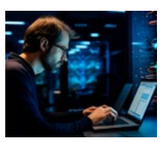
5. Cyber Incident Responder

Gestiona incidentes de seguridad: análisis, contención, erradicación y recuperación. Documenta lecciones aprendidas y coopera con SOCs y CSIRTs en la respuesta operativa.



6. Cyber Threat Intelligence Specialist

Analiza amenazas, actores y campañas. Produce inteligencia accionable para anticipar riesgos y ajustar controles defensivos y priorización de vulnerabilidades.



7. Digital Forensics Investigator

Realiza análisis forense de sistemas comprometidos. Preserva evidencias, reconstruye vectores de ataque y apoya procesos disciplinarios, regulatorios o judiciales.

8. Penetration Tester (Ethical Hacker)

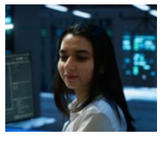
Evalúa la seguridad mediante pruebas controladas de intrusión. Identifica vulnerabilidades explotables y proporciona recomendaciones técnicas de remediación.

9. Cybersecurity Auditor

Evalúa la conformidad con políticas, estándares y regulación. Verifica la efectividad de controles y emite informes independientes de cumplimiento.

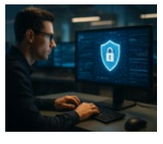
10. Cybersecurity Trainer / Awareness Specialist

Diseña y ejecuta programas de formación y concienciación. Reduce el riesgo humano mediante campañas, simulaciones y métricas de comportamiento seguro.



11. Cyber Legal, Policy and Compliance Officer

Interpreta requisitos regulatorios y contractuales en materia de Ciberseguridad. Asegura alineación normativa (NIS2, ENS, ISO, etc.) y coordina obligaciones de reporte.



12. Identity and Access Management (IAM) Specialist

Gestiona identidades, autenticación y control de accesos. Implementa modelos de mínimo privilegio, federación, MFA y gobierno de identidades.

2.2. Funciones del Responsable de la práctica de Ciberseguridad

El alcance efectivo de la función del CISO varía en función del tamaño organizativo, la madurez en gobierno corporativo, el sector regulatorio y el nivel de recursos disponibles. Estas variables condicionan qué funciones ejerce directamente, cuáles delega en perfiles especializados y cómo se articula la segregación de responsabilidades dentro del modelo operativo. Así, por ejemplo, un responsable de Ciberseguridad en:

- Empresa A, sus funciones pueden coincidir totalmente y de forma estricta con las funciones que el ECSF asigna al CISO.
- Empresa B, de menor tamaño que la anterior, puede tener y ejercer personalmente el conjunto de funciones de todos los perfiles y/o dirigir mediante un contrato externo algunas de ellas y además con cobertura ocasional de la prestación.
- Empresa C, puede dirigir desde su área todas las funciones relacionadas con la estrategia, el asesoramiento y la supervisión, incluido la detección y gestión de incidentes, pero no las de ingeniería de Ciberseguridad, pues por separación/segregación de funciones no sea responsable de la operación de la Ciberseguridad.
- Una empresa D, sea entidad esencial española y por tanto deba cumplir con la transposición de la NIS2 y consecuentemente tenga su RSI con las funciones que le asigna dicha transposición nacional.

En cualquier modelo, el objetivo central es que la Ciberseguridad se gestione como un riesgo empresarial, integrando prioridades de negocio, cumplimiento normativo y resiliencia operativa. La función del CISO puede materializarse a través de un rol plenamente integrado en la estructura ejecutiva o mediante soluciones híbridas (por ejemplo, un CISO interno reforzado por servicios especializados externos), especialmente en organizaciones con menor capacidad presupuestaria.

Para comprender el rol del CISO resulta necesario diferenciar entre el marco operativo, que articula cómo se gestiona la seguridad, y la naturaleza funcional del puesto, que define qué tipo de responsabilidad ejerce dentro de la organización.

Tradicionalmente, las funciones atribuidas al CISO se estructuran en cuatro bloques principales:

Bloques	Naturaleza	Enfoque principal
Estrategia	Definición	Marco y gobierno
Asesoramiento	Decisión	Evaluación y recomendación
Ejecución	Dirección operativa	Implantación de controles
Supervisión	Control y validación	Eficacia y resiliencia

Figura 14. *Relación entre los bloques funcionales del CISO, su naturaleza y su enfoque principal.*

Mapeo de los cuatro bloques funcionales con roles ECSF

Este apartado traduce los cuatro bloques funcionales de la Ciberseguridad en roles concretos del ECSF, detallando cómo se distribuyen las responsabilidades del CISO y qué perfiles apoyan cada ámbito. El propósito es proporcionar una visión precisa del alcance del rol y de su interacción con las capacidades profesionales especializadas.

Estrategia, Gobierno y directrices

Define el marco estratégico y normativo que rige la Ciberseguridad y eleva sus elementos clave a los órganos de dirección cuando proceda.

Actividades:

- Definir el alineamiento de la Ciberseguridad con negocio, legislación y regulación.
- Establecer modelo de gobierno (comités, escalado, RACI).
- Establecer el modelo organizativo de la Ciberseguridad.
- Determinar apetito y tolerancia al riesgo.
- Aprobar políticas, estándares y directrices técnicos.
- Establecer el marco y metodología de la evaluación y gestión de riesgos.
- Integrar la Ciberseguridad en las compras, proyectos y gestión de proveedores.
- Definir cuadro de mando, métricas estratégicas.
- Elaborar el reporte a la alta Dirección, entre otras.

Perfiles ECSF relacionados:

- CISO (liderazgo estratégico).
- Cybersecurity Risk Manager (marco metodológico).
- Cyber Legal, Policy & Compliance Officer (alineamiento normativo).
- Cybersecurity Architect (implementación técnica de las directrices y controles en elementos de la arquitectura de seguridad).
- Cybersecurity Auditor (validación del marco de control).

Asesoramiento

Emitir criterio experto e independiente ante decisiones con impacto en la exposición al riesgo.

Actividades:

- → Evaluar riesgos asociados a nuevos proyectos, tecnologías o cambios organizativos.
- → Emitir opinión técnica en adquisiciones estratégicas.
- → Analizar impacto de amenazas emergentes.
- → Valorar escenarios de cibercrisis.
- → Asesorar sobre cumplimiento regulatorio.
- → Interpretar el nivel de riesgo residual tras implantación de controles.

Perfiles ECSF relacionados:

- → Cybersecurity Risk Manager (análisis formal y valoración del riesgo).
- → Cyber Threat Intelligence Specialist (contexto de amenaza).
- → Cyber Legal & Compliance Officer (implicaciones regulatorias).
- → Cybersecurity Architect (viabilidad técnica de mitigaciones.
- → Digital Forensics Investigator (análisis técnico en incidentes complejos; en la medida que ayuda a evaluar riesgos.

Ejecución de la seguridad (Operación)

Garantizar que el modelo operativo de seguridad funciona eficazmente.

Actividades:

- → Operar el SOC (Caso de existir un CSIRT el SOC operaría y el CSIRT, como gestión de incidentes se consideraría parte de la supervisión).
- → Asegurar cobertura de monitorización adecuada al riesgo.
- → Garantizar implantación de controles técnicos.
- → Priorizar remediación de vulnerabilidades críticas.
- → Supervisar planes de continuidad tecnológica.
- → Validar ejercicios de simulación y cibercrisis.

Perfiles ECSF relacionados:

- → Cybersecurity Engineer (implementación de controles).
- → Identity & Access Management Specialist (gobierno de identidades).
- → Cybersecurity Architect (diseño seguro).
- → Cyber Incident Responder (respuesta técnica al incidente).
- → Digital Forensics Investigator (análisis avanzado).

Supervisión

Este bloque concentra la función de control, validación y mejora continua. Supervisa la eficacia del sistema de seguridad y dirige la respuesta estratégica ante incidentes graves.

Actividades:

- → Revisar KPIs operativos y métricas de riesgo,
- → Supervisar evolución del registro de riesgos,
- → Validar auditorías internas y externas,
- → Activar comité de crisis ante incidentes graves,
- → Asegurar notificación regulatoria en plazo,
- → Supervisar remediación post-incidente,
- → Validar resultados de pruebas técnicas independientes, entre otras.

Perfiles ECSF implicados

- → Cybersecurity Auditor (evaluación independiente del sistema).
- → Penetration Tester / Ethical Hacker (explotación de vulnerabilidades y pruebas de resiliencia).
- → Cyber Incident Responder (ejecución técnica de respuesta).
- → Cyber Legal & Compliance Officer (cumplimiento).
- → Cybersecurity Risk Manager (re-evaluación del riesgo tras incidentes).

Función directiva del CISO y responsabilidades asociadas

Independientemente de las actividades desempeñadas, la función directiva del CISO es la que articula y gobierna el conjunto. Su rol se caracteriza más por la orientación y supervisión de decisiones que por la ejecución técnica de controles.

En este ámbito le corresponde definir y dirigir la estrategia de Ciberseguridad, establecer prioridades y criterios de proporcionalidad, y diseñar el modelo de gobierno del riesgo digital. Supervisa su identificación, evaluación, tratamiento y escalado cuando proceda, garantizando trazabilidad y soporte adecuado a la alta dirección.

Asimismo, evalúa la madurez del marco de control, impulsa la mejora continua de las capacidades de prevención, detección, respuesta y recuperación, y contribuye a la preparación y gestión de crisis aportando criterio experto.

El CISO también impulsa la integración de la Ciberseguridad en la cultura organizativa, coordina funciones corporativas y supervisa el riesgo de terceros y de la cadena de suministro, identificando dependencias críticas.

Finalmente, actúa como interlocutor ante reguladores y organismos externos, incorporando la evolución normativa y el contexto de amenazas a la estrategia corporativa. Esta consolidación normativa refuerza la necesidad de una función especializada capaz de garantizar un gobierno del riesgo digital efectivo y defendible.

2.3. Funciones del CISO reconocidas por la legislación

La evolución del rol del CISO no es consecuencia únicamente de una mayor sofisticación tecnológica ni del incremento sostenido del nivel de amenaza. Responde, sobre todo, a un cambio profundo en la forma en que la legislación y los marcos regulatorios entienden hoy la gestión del riesgo digital y la responsabilidad asociada a las decisiones que lo afectan.

Aunque la normativa europea vigente no menciona de forma expresa la figura del CISO, sí exige un conjunto de responsabilidades que difícilmente pueden gestionarse de manera informal o distribuida. La identificación y evaluación del riesgo de Ciberseguridad, la adopción de medidas razonables, la preparación para la gestión de incidentes y la rendición de cuentas ante autoridades y terceros requieren una función con visión transversal, criterio técnico y capacidad de interlocución con la dirección.

Su función no sustituye la responsabilidad última de la alta dirección, pues esta no se delega, pero resulta esencial para que esta pueda ejercerse de forma informada, defendible, con criterio y con trazabilidad suficientes para sostener las decisiones adoptadas y dirigir la práctica técnica conforme a esas decisiones. El CISO se sitúa aquí como el elemento que permite traducir el riesgo técnico en términos comprensibles para la toma de decisiones, especialmente en situaciones de incidente, supervisión regulatoria o evaluación posterior de responsabilidades.

La legislación nacional en materia de Ciberseguridad, lo que incluye tanto al ENS como a las transposiciones de la NIS y, aunque en borrador, también la de la NIS2, sí define específicamente la figura y lo hace como RSI.

La legislación no exige una denominación concreta, pero presupone la existencia de una función con capacidad técnica, visión transversal y suficiente posicionamiento para articular la gestión del riesgo de Ciberseguridad, supervisar su evolución y proporcionar información fiable a los órganos de gobierno. Sin esta función, resulta difícil sostener que la organización actúa con la diligencia exigible en un entorno digital complejo y altamente interdependiente. De este modo, el reconocimiento del CISO no debe entenderse como la creación de una nueva figura jurídica, sino como la consolidación de un rol imprescindible para dar respuesta a un marco normativo que exige gobierno efectivo del riesgo digital, capacidad de anticipación y resiliencia operativa.

La legislación nacional y la europea avanzan así hacia un modelo en el que la Ciberseguridad deja de tratarse como un ámbito especializado y se integra en el gobierno corporativo y en la gestión ordinaria del riesgo.

Evolución del reconocimiento normativo del rol del CISO

En el RD 12/2018, transposición española de la NIS, se exige a los operadores esenciales la designación de un RSI. En el reglamento que desarrolla la transposición, RD 43/2021, se definen sus funciones y, como hecho de especial relevancia su independencia de los responsables de sistemas.

El RD 311/2022, que actualiza el ENS, incorpora en el alcance subjetivo a las empresas del sector privado, tanto en cuanto prestan servicios a las entidades del sector público. Asimismo, incorpora la figura del Punto de Contacto de Seguridad (POC).

Se espera que, en la futura transposición de la NIS2, sobre las funciones del borrador a información pública que eran un replica literal de las del reglamento de desarrollo de la transposición de la NIS, se incorporen una ampliación de funciones que destacan el papel directivo y de interlocución con los órganos de Gobierno.

ENS
Directivas NIS
RGPD y LOPDyGDD
LPIC y DORA

Esquema Nacional de Seguridad (ENS)

Real Decreto 311/2022

El ENS se aplica a las Administraciones Públicas españolas -Administración General del Estado, Comunidades Autónomas, Entidades Locales y sector público institucional- y a las entidades privadas que presten servicios o gestionen sistemas de información para aquellas, cuando traten información o soporten servicios públicos electrónicos. Su alcance objetivo es establecer los principios básicos y requisitos mínimos de seguridad que deben cumplir los sistemas de información del sector público, garantizando la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad y conservación de la información y de los servicios electrónicos.

El ENS constituye uno de los marcos normativos de mayor relevancia en el ámbito español en lo que respecta al gobierno de la seguridad de la información, especialmente en el sector público y en aquellas organizaciones que les prestan servicios. Su aportación va más allá de la enumeración de medidas técnicas y organizativas, al establecer un modelo explícito de responsabilidades, supervisión y rendición de cuentas.

Aunque el ENS no utiliza de forma expresa las siglas de CISO, sino que define la figura del RSI y le asigna funciones que, en organizaciones con un cierto grado de complejidad, no pueden ejercerse de manera eficaz sin una función especializada, con visión transversal y con capacidad real de interlocución. La definición de la política de seguridad, la supervisión de su implantación y la coordinación con los responsables de sistemas, información y servicios requieren algo más que una gestión distribuida o puramente operativa.

En este marco, el RSI actúa como garante del sistema de seguridad definido por el ENS, asegurando que las decisiones en materia de protección de la información y de los servicios digitales se adoptan con criterio y de forma proporcional al riesgo. Su papel resulta especialmente relevante para evitar enfoques centrados exclusivamente en el cumplimiento formal, donde la existencia documental de controles sustituye a la evaluación de su eficacia real y de su capacidad para sostener la operación en escenarios adversos.

El ENS refuerza asimismo la necesidad de revisar de manera periódica el sistema de seguridad y de adaptarlo a la evolución del contexto tecnológico, organizativo y de amenazas. Para esto último, es interesante destacar el voluminoso corpus de documentación que bajo la denominación de guías STIC sirven de apoyo al RSI.

ENS 2010. Se establece por primera vez el rol

La primera cristalización normativa del rol que hoy identificamos como CISO se encuentra en el Real Decreto 3/2010, por el que se regula el ENS. En este texto se introduce formalmente la figura del RSI, junto al Responsable de la Información y el Responsable del Servicio.

Características relevantes de este primer texto:

- Se reconoce por primera vez la necesidad de una función diferenciada encargada de coordinar la seguridad.
- El enfoque es administrativo y organizativo, no directivo-estratégico.
- El rol se concibe como garante del cumplimiento de principios básicos y requisitos mínimos.
- Su ubicación natural es la Administración Pública y el sector público institucional.

En esta etapa, el Responsable de Seguridad es esencialmente un órgano técnico-organizativo de cumplimiento, no un directivo corporativo con visión estratégica transversal.

Dónde se menciona y/o regula:

→ **Artículo 10. "La seguridad como función diferenciada":** introduce la diferenciación entre responsable de la información, responsable del servicio y responsable de la seguridad, y asigna al responsable de seguridad "determinar las decisiones" para satisfacer requisitos de seguridad.

→ **Artículo 12. "Organización e implantación del proceso de seguridad":** exige que la política de seguridad identifique "claros responsables" de velar por su cumplimiento.

→ **Artículo 27. "Cumplimiento de requisitos mínimos":** reconoce que las medidas mínimas "podrán ser ampliadas" por el "prudente arbitrio del responsable de la seguridad del sistema" y que la Declaración de Aplicabilidad la firma el responsable de seguridad.

Es importante destacar que si bien el responsable de seguridad queda definido como función diferenciada respecto a información/servicio (y se indica separación respecto a la prestación del servicio), no fija: independencia jerárquica frente a operación/explotación, obligación explícita de "reporting", un rol adicional de "responsable del sistema" separado, ni un esquema formal de certificación del responsable.

Nota sobre "nueva versión" 2015: el RD 951/2015 modifica varios preceptos del RD 3/2010 (p. ej., art. 11.1, art. 15.3, art. 18...), pero no altera el núcleo del artículo 10 donde se configura el responsable de seguridad.

ENS 2022 (Real Decreto 311/2022). Diferencias relevantes respecto a 2010

1) Se amplía el modelo de responsabilidades: aparece el "responsable del sistema"

- **Artículo 11.** "Diferenciación de responsabilidades": ya no son 3, sino 4: responsable de la información, del servicio, de la seguridad y del sistema.

  Diferencia con el Real Decreto Ley del 2010: en 2010 la diferenciación explícita era entre información/servicio/seguridad (art. 10); en 2022 se incorpora responsable del sistema como figura propia.

2) Se explicita el contenido funcional del responsable de seguridad (y el "reporting")

- **Artículo 13.2.c):** el responsable de seguridad "determinará las decisiones...", "supervisará la implantación" y "reportará" sobre estas cuestiones.

  Diferencia con el RD 2010: en la versión inicial del 2010, en ella se queda en "determinar decisiones" (art. 10), sin fijar expresamente "supervisar implantación" ni "reportar".

3) Se exige separación real con operación/ explotación: independencia y medidas compensatorias

- **Artículo 13.3:** establece que el responsable de seguridad será distinto del responsable del sistema y que no debe existir dependencia jerárquica; si excepcionalmente no es posible, obliga a medidas compensatorias.

  Diferencia con la versión del 2010: en 2010 se habla de separar la responsabilidad de seguridad de la prestación del servicio (art. 10), pero no fija esa prohibición de dependencia jerárquica ni el régimen de excepción/compensación.

4) El responsable de seguridad puede ejercerlo una persona o "cosa" (permítannos la ironía).

- **El artículo 13.1:** establece literalmente: «El responsable de la seguridad será una persona física u órgano colegiado, que dependerá directamente del órgano superior o directivo competente».

Esta formulación, que permite atribuir el rol del Responsable de la Seguridad de la Información (RSI) a un órgano colegiado o directivo, parece orientada a dar cobertura organizativa, especialmente en el ámbito de pequeñas entidades locales o estructuras administrativas de reducida dimensión.

Sin embargo, desde la práctica profesional, dicha previsión se aparta en buena medida de la realidad operativa de la Ciberseguridad actual. La función exige especialización técnica, capacidad de adaptación continua, conocimiento actualizado de amenazas y de los marcos normativos, así como toma de decisiones ágil en el día a día. Estas exigencias difícilmente pueden satisfacerse de forma eficaz mediante un órgano colegiado no especializado.

La experiencia demuestra que el desempeño adecuado del rol requiere un profesional específicamente formado y capacitado, dedicado de manera explícita a esta responsabilidad, ya sea a tiempo completo o parcial, y con independencia de que su vínculo sea interno o externo, con autoridad funcional y evolución permanente acorde al dinamismo del riesgo tecnológico.

5) Se introduce un esquema específico de certificación del responsable de seguridad

- **Artículo 13.4:** prevé una Instrucción Técnica de Seguridad que regule el Esquema de Certificación de Responsables de la Seguridad.

  Diferencia con la versión del 2010: no existe previsión equivalente en el articulado de 2010. Si bien a efectos prácticos es nula; pues a la hora de publicar esta versión del libro blanco (cuatro años después) ni tan siquiera se ha publicado el esquema de certificación.

6) Se regula explícitamente el rol en servicios externalizados (POC) conectado con el responsable de seguridad

- **Artículo 13 (continuación):** en externalización de servicios, se exige designar un POC de seguridad con apoyo de dirección y se indica que ese POC será el propio Responsable de Seguridad del proveedor o estará en su área con comunicación directa.

  Diferencia con la versión del 2010: no hay una previsión tan directa en el articulado sobre POC del proveedor vinculado al responsable de seguridad.

En resumen, las principales diferencias, en relación con el rol del RSI, entre la primera y la, hasta el momento, última versión del ENS es:

- → Se pasa de 3 roles a 4 roles (se añade "responsable del sistema"): 2010 art. 10 vs 2022 art. 11. Lo que de forma indirecta añade mayor independencia al RSI por la obligación de ser funciones diferenciadas.
- → Se añade "supervisará" y "reportará" como mandato expreso: 2022 art. 13.2.c (no explícito en 2010 art. 10).
- → Se prohíbe dependencia jerárquica seguridad vs sistema, con régimen de excepción y compensatorias: 2022 art. 13.3 (no en 2010).
- → Se prevé certificación del responsable de seguridad: 2022 art. 13.4 (no en 2010).
- → Se aterriza el rol en outsourcing mediante POC ligado al responsable de seguridad del proveedor: 2022 art. 13 (POC).

POC de Seguridad

POC significa Point of Contact en inglés, traducido al español como Punto de Contacto. Se refiere a una persona o departamento designado como el enlace principal para gestionar la comunicación, resolver dudas o coordinar actividades específicas en un proyecto, cliente o asunto técnico.

En el ENS, el POC se trata de una figura que debe existir en cualquier servicio o proyecto prestado por un tercero a una entidad del sector público cuando dicho servicio implique interacción con sus sistemas o información.

La designación del POC debe ser exigida por la entidad pública y formalmente identificada por el proveedor siempre que concurra alguna de las siguientes circunstancias: tratamiento de información digital de la entidad, provisión o implantación de sistemas TIC, o conexión -directa o indirecta- a las redes o infraestructuras tecnológicas de la organización.

Esta exigencia no depende de que el objeto principal del contrato sea tecnológico. Resulta aplicable también cuando la prestación tenga otra finalidad principal, siempre que en su ejecución se acceda, procese o almacene información de la entidad pública, con independencia de que dicha información tenga o no carácter personal.

El POC de Seguridad constituye un elemento estructural de gobernanza y coordinación técnica en la relación Proveedor-Administración cuando exista cualquier impacto, directo o indirecto, sobre la seguridad de la información o de los sistemas.

La mención expresa de esta figura en el Real Decreto responde a una experiencia práctica que de forma reiterada en el tiempo se ha venido produciendo y que los RSI han venido padeciendo y que con esta fórmula se pretende remediar. En muchísimos procedimientos de contratación, no pocos adjudicatarios asumían en fase de licitación los requisitos de seguridad exigidos, para posteriormente, una vez formalizado el contrato, intentar reinterpretarlos, acotarlos o ignorarlos artificialmente o cuestionar su alcance.

La obligación de que el proveedor designe como POC a su CISO o, en su caso, a un profesional con competencias acreditadas en esta materia, introduce un mecanismo de responsabilidad técnica directa. Esta exigencia constituye una garantía recíproca: para la entidad pública, porque asegura interlocución especializada y capacidad real de respuesta; y para el proveedor, porque dota al contrato de un marco claro de responsabilidades y evita conflictos interpretativos posteriores.

El POC de Seguridad actúa, además, como garante de la adecuada gestión de incidentes que se originen en el ámbito del proveedor y puedan afectar a la entidad contratante. En tales supuestos, debe asegurar que la información relevante fluya de forma transparente, íntegra y oportuna, permitiendo que la entidad gestione adecuadamente el incidente repercutido y cumpla en plazo con las obligaciones de notificación y respuesta derivadas de la normativa que le resulte aplicable.

Cabe diferenciar la figura del POC de la figura de "Responsable de Proyecto, o Director Técnico del Contrato (DTC), que es habitual en los proyectos con terceros.

El POC de seguridad por lo tanto tiene una doble función: garantizar que los requisitos de seguridad se han entendido y se van a aplicar y por otro lado, que en caso de incidente la interlocución profesional de seguridad es rápida y tiene la calidad necesaria, para una eficaz coordinación.

Otras consideraciones

Aunque excede el alcance y la extensión de este libro blanco, resulta pertinente dejar apuntada una cuestión de interés: el ENS dio un paso trascendental al reconocer formalmente la figura del Responsable de la Seguridad de la Información (RSI), pero su formulación normativa no alcanza, ni en su última versión, el grado de precisión funcional ni de garantía de independencia que posteriormente se observará en la transposición de la NIS y, en particular, en el desarrollo reglamentario asociado a su artículo 7.

Esta diferencia resulta llamativa si se tiene en cuenta el papel desempeñado por el Centro Criptológico Nacional (CCN) tanto como órgano impulsor y custodio del ENS como en su apoyo a la figura de un RSI directivo e independiente, en los trabajos técnicos que condujeron a una redacción más definida del rol en el ámbito de la transposición de la NIS.

Por un lado, la formalización plena del reconocimiento profesional del RSI -en términos de dedicación específica, perfil competencial e independencia funcional- tendría implicaciones organizativas y presupuestarias relevantes para el conjunto del sector público, lo que necesariamente requiere el correspondiente respaldo del Ministerio competente en materia de función pública y gasto; es decir, del Ministerio de Hacienda.

Por otro lado, debe considerarse la propia concepción del modelo organizativo del ENS para entidades de menor tamaño. En administraciones locales pequeñas, muy numerosas y, paradójicamente, especialmente expuestas, el Comité de Seguridad TIC está llamado a estar presidido por el alcalde o formado por un conjunto de personas con responsabilidad en la entidad y quien, como comité, asumir directamente el liderazgo y la validación de decisiones en materia de seguridad. En ese contexto, la existencia de un RSI con dedicación principal y diferenciada resulta, en la práctica, difícilmente sostenible por razones estructurales y de dimensión organizativa.

Estas circunstancias pueden ayudar a comprender por qué el ENS hasta el presente opta por una formulación más flexible del rol, mientras que el marco de la transposición de la NIS, con operadores (entidades en la nueva jerga del NIS2) esenciales (y ahora en la NIS2 también los importantes) principalmente del sector privado, ha evolucionado hacia una definición más explícita y exigente en términos de gobernanza y responsabilidad.

Directivas NIS
y funciones del RSI

Directiva (UE) 2016/1148 – NIS

La primera Directiva NIS se aplicaba a Operadores de Servicios Esenciales (OSE) en los sectores de energía (electricidad, petróleo, gas), transporte (aéreo, ferroviario, marítimo, carretera), banca, infraestructuras de mercados financieros, salud, suministro y distribución de agua potable e infraestructuras digitales (IXP, DNS, TLD), así como a Proveedores de Servicios Digitales (PSD): mercados en línea, motores de búsqueda y servicios de computación en la nube. Su alcance objetivo fue establecer el primer marco común europeo de seguridad de redes y sistemas de información, imponiendo medidas de gestión de riesgos y obligaciones de notificación de incidentes con impacto significativo.

El Real Decreto-ley 12/2018 se aplica, por un lado, a la prestación de servicios esenciales dependientes de redes y sistemas de información comprendidos en los sectores estratégicos definidos en el anexo de la Ley 8/2011, y, por otro, a determinados servicios digitales (mercados en línea, motores de búsqueda en línea y servicios de computación en nube). Están sujetos al RD-ley los operadores de servicios esenciales establecidos en España y los proveedores de servicios digitales en los términos de establecimiento/representación que fija la norma. Su alcance objetivo es regular la seguridad de las redes y sistemas de información usados para proveer esos servicios esenciales y digitales, estableciendo obligaciones de gestión de riesgos y notificación de incidentes.

La transposición de la Directiva NIS tiene como alcance subjetivo doce sectores al remitir. esta (RD-ley 12/2018) al alcance de la Ley 8/2011 (Infraestructuras críticas) e igualarlos. Los sectores estratégicos del anexo de la Ley 8/2011 son: Administración, Espacio, Industria nuclear, Industria química, Instalaciones de investigación, Agua, Energía, Salud, Tecnologías de la Información y las Comunicaciones (TIC), Transporte, Alimentación, y Sistema financiero y tributario.

El **artículo 7**, en relación con el RSI, establece que:

- **Los operadores de servicios esenciales designarán una persona, unidad u órgano colegiado, responsable de la seguridad de la información** que ejercerá las funciones de punto de contacto y coordinación técnica con la autoridad competente y con el CSIRT de referencia que le corresponda de conformidad con lo previsto en el apartado tercero. En el supuesto de que el RSI sea una unidad u órgano colegiado, se deberá designar una persona física representante, así como un sustituto de este que asumirá sus funciones en casos de ausencia, vacante o enfermedad. El plazo para llevar a cabo dicha designación será de tres meses desde su designación como operador de servicios esenciales.

- **Los operadores de servicios esenciales comunicarán a la autoridad competente respectiva la designación del RSI dentro del plazo establecido** en el apartado anterior, así como los nombramientos y ceses que afecten a dicha designación en el plazo de un mes desde que se produzcan.

- **El RSI actuará como punto de contacto con la autoridad competente en materia de supervisión de los requisitos de seguridad de las redes y sistemas de información**, y como punto de contacto especializado para la coordinación de la gestión de los incidentes con el CSIRT de referencia. Se desarrollarán bajo su responsabilidad, entre otras, las siguientes funciones:

  → Elaborar y proponer para aprobación por la organización, de conformidad con lo establecido en el artículo 6.2 de este real decreto, las políticas de seguridad, que incluirán las medidas técnicas y organizativas adecuadas y proporcionadas para gestionar los riesgos que afecten a la seguridad de las redes y sistemas de información utilizados, y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios.

  → Supervisar y desarrollar la aplicación de las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo controles periódicos de seguridad.

  → Elaborar el documento de Declaración de Aplicabilidad de medidas de seguridad considerado en el artículo 6.3 de este real decreto.

  → Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.

  → e) Remitir a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, las notificaciones de incidentes que tengan efectos perturbadores en la prestación de los servicios.

  → Recibir, interpretar y supervisar la aplicación de las instrucciones y guías emanadas de la autoridad competente, tanto para la operativa habitual como para la subsanación de deficiencias observadas.

  → Recopilar, preparar y suministrar información o documentación a la autoridad competente o al CSIRT de referencia, a su solicitud o por propia iniciativa.

  → El RSI, para desarrollar estas funciones, se podrá apoyar en servicios prestados por terceros.

- **Los operadores de servicios esenciales garantizarán que el responsable de la seguridad de la información cumpla con los siguientes requisitos:**

  → Contar con personal con conocimientos especializados y experiencia en materia de Ciberseguridad, desde los puntos de vista organizativo, técnico y jurídico, adecuados al desempeño de las funciones indicadas en el apartado anterior.

  → Contar con los recursos necesarios para el desarrollo de dichas funciones.

- ⟶ Ostentar una posición en la organización que facilite el desarrollo de sus funciones, participando de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la seguridad, y manteniendo una comunicación real y efectiva con la alta dirección.
- ⟶ Mantener la debida independencia respecto de los responsables de las redes y los sistemas de información.

- Siempre que concurran los requisitos de conocimiento, experiencia, independencia y, en su caso, titulación, l**as funciones y responsabilidades encomendadas al RSI podrán compatibilizarse con las señaladas para el Responsable de Seguridad y Enlace y el Responsable de Seguridad del Esquema Nacional de Seguridad**, de conformidad con lo dispuesto en la normativa aplicable a estas figuras.

  Es importante que destaquemos el **apartado 4** de este artículo. En su redacción leemos que:

  - ⟶ No solo debe contar con personal técnico, sino también jurídico, lo que viene a reforzar el carácter directivo y de garante legal de su rol.
  - ⟶ Debe tener una posición que le garantice el reporte y asesoramiento a los órganos de dirección. Lo que de forma preclara se adelanta al papel que debe jugar el RSI respecto de las obligaciones que la NIS2 establece en materia de Ciberseguridad a los Órganos de Dirección y que por otra parte los debería elevar en el modelo organizativo de la Organización.
  - ⟶ La independencia de los responsables de Sistemas. Lo que acerca de forma inexorable al RSI a una postura de independencia y alejado de la mayor fuente de conflicto con su independencia en sus funciones de asesoramiento y sobre todo de supervisión. En este ámbito, NUNCA será posible que figura del RSI esté situado organizativamente debajo del CIO; es decir, si trabaja para un operador esencial (operador conforme a la nomenclatura de la NIS) o a una entidad esencial o importante (terminología NIS2) el CISO debe estar en un área organizativa diferente a CIO. Las implicaciones de esto, sobre todo en lo relacionado a la operación de la Ciberseguridad, se tratarán más adelante.

Directiva NIS2

La Directiva NIS2 (UE 2022/2555)[3] es la norma europea que redefine cómo las organizaciones deben gestionar la Ciberseguridad. Su objetivo es elevar la resiliencia digital en toda la Unión Europea, demandando que las organizaciones hagan de la Ciberseguridad un asunto estratégico y no solo técnico.

La NIS2 se aplica a entidades públicas y privadas de sectores altamente críticos (Anexo I) y de otros sectores críticos (Anexo II), clasificadas como entidades esenciales o entidades importantes en función de su tamaño y criticidad. Entre los sectores altamente críticos se incluyen: energía (electricidad, gas, petróleo, hidrógeno), transporte (aéreo, ferroviario, marítimo y carretera), banca, infraestructuras de mercados financieros, salud, agua potable, aguas residuales, infraestructura digital (IXP, DNS, TLD, centros de datos, redes públicas), administración pública central y espacio. Entre los otros sectores críticos figuran: servicios postales y mensajería, gestión de residuos, fabricación de productos críticos (farmacéuticos, productos sanitarios, productos químicos, alimentación), proveedores digitales (mercados en línea, motores de búsqueda, redes sociales) e investigación. Su alcance objetivo es establecer obligaciones de gestión de riesgos de Ciberseguridad, notificación de incidentes, gobernanza y supervisión para garantizar la seguridad de las redes y sistemas que soportan servicios esenciales para la economía y la sociedad.

Marca un punto de inflexión en la forma en que la Ciberseguridad se integra en las obligaciones legales de las organizaciones. Incluso antes de su transposición al ordenamiento jurídico español, la directiva establece un estándar claro sobre cómo debe entenderse la gestión del riesgo digital, y, sobre todo, sobre quién debe responder por ella.

El nombre NIS2 se debe a la existencia de una directiva anterior NIS (UE 2016/1148)[4], que establecía la necesidad de seguridad para las redes y los sistemas de información en la Unión Europea, definiendo la necesidad de que los Estados Miembros definan una estrategia de seguridad, designen operadores esenciales y digitales, y estableciendo obligaciones mínimas de controles de seguridad y, sobre todo, estableciendo una estructura europea de reporte de incidentes. Esta directiva fue transpuesta en España como Real Decreto-Ley 12/2018, con pocas novedades relevantes, en particular porque con la publicación de NIS2 se supera NIS y sus previsiones.

NIS2 abandona definitivamente una aproximación centrada en requisitos técnicos aislados y consolida un modelo de gestión del riesgo plenamente integrado en el gobierno de la organización. La exigencia ya no es únicamente disponer de determinadas medidas, sino ser capaz de identificar riesgos relevantes, priorizarlos, adoptar respuestas proporcionadas y mantener capacidades reales de prevención, detección, respuesta y recuperación frente a incidentes que puedan afectar a servicios esenciales o relevantes.

Este planteamiento refuerza de forma directa las funciones que, en la práctica, desempeña el CISO. Aunque la directiva no impone una denominación concreta ni una estructura organizativa específica, sí presupone la existencia de una función con capacidad técnica, visión transversal y suficiente posicionamiento para articular la gestión del riesgo de Ciberseguridad y supervisar la eficacia de las medidas adoptadas. Sin una función de este tipo, resulta difícil sostener que la organización cumple materialmente con las obligaciones que NIS2 establece.

Uno de los elementos más relevantes de la directiva es el refuerzo explícito de la responsabilidad de los órganos de dirección. La aprobación de las medidas de gestión del riesgo, la supervisión de su aplicación y la obligación de recibir formación adecuada sitúan la Ciberseguridad en el núcleo de la toma de decisiones. En este contexto, el CISO no sustituye la responsabilidad de la dirección, pero se convierte en un apoyo imprescindible para su ejercicio, aportando análisis, escenarios y criterio en un ámbito donde la improvisación tiene consecuencias inmediatas.

En el **Artículo 20** se establece la gobernanza de la Ciberseguridad, obligando a los órganos de dirección (consejos, directivos) a aprobar, supervisar y ser responsables de las medidas de gestión de riesgos, y a recibir formación periódica en Ciberseguridad, lo que introduce una responsabilidad legal personal y un enfoque directo en la alta dirección para asegurar la ciberresiliencia de las entidades esenciales e importantes.

El **Artículo 21** de la Directiva NIS2 exige a las entidades medidas técnicas y organizativas para gestionar los riesgos de Ciberseguridad, incluyendo análisis de riesgos, gestión de incidentes y continuidad del negocio, seguridad en la cadena de suministro, seguridad en la adquisición y mantenimiento de sistemas, políticas de ciberhigiene, uso de criptografía y MFA, y seguridad de recursos humanos y física, todo bajo un enfoque integral para proteger sistemas, redes e información.

Como hemos comentado en el apartado en el que introducíamos la evolución de la evolución, si bien, a la hora de publicar el presente libro blanco, la obligada transposición al ordenamiento nacional de la Directiva Europea NIS2, no ha sido aprobada, el borrador que fue presentado a comentarios públicos, el rol del RSI tenía la misma redacción que la transposición a la anterior directiva NIS.

Es por lo que, en la sección siguiente, del presente apartado, para que los responsables de seguridad de la información. o de aquellos que aspiren a serlo. de entidades esenciales e importantes, se detalla en el artículo 7 del RD 43/2021 que desarrolla la transposición del RD 12/2018 en lo relativo al rol del RSI.

NIS2 pone también un énfasis particular en la gestión de incidentes significativos y en la necesidad de actuar con rapidez, coordinación y proporcionalidad. La obligación de notificación y la interacción con las autoridades competentes requieren una preparación previa y una capacidad de decisión que no se construyen en el momento de la crisis. El Artículo 23 establece las

[3] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022. ***https://www.boe.es/buscar/doc.php?id=-DOUE-L-2022-81963***

[4] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016. ***https://www.boe.es/doue/2016/194/L00001-00030.pdf***

obligaciones de notificación de incidentes de Ciberseguridad significativos para las entidades afectadas, tanto a los destinatarios de sus servicios como a la autoridad competente, exigiendo una respuesta rápida y escalonada: una alerta temprana en 24h, una evaluación inicial en 72h y un informe final, a más tardar en un mes, detallando el impacto y las medidas tomadas, para garantizar una respuesta coordinada y eficaz a nivel europeo ante amenazas cibernéticas graves.

Mapeo de obligaciones NIS2 a roles ECSF

Como vemos, la traslación a la legislación nacional de la Directiva NIS tiene definida la función del RSI/ CISO, mientras que la NIS2 fija obligaciones de seguridad, pero no define la figura del CISO o equivalente. Dado que cada estado miembro de la Unión Europea podrá concretar o no el rol; es decir, mantener la no mención del CISO, o designar, como ha sucedido en Grecia, un RSI y comunicaciones, o como la medida adoptada en Italia de identificar la necesidad de que se designe un punto de contacto, o simplemente dejarlo de mencionar como ha ocurrido en otros países.

El informe ***Cybersecurity roles and skills for NIS2 Essential and Important Entities***[5] es una guía práctica para ayudar a las entidades que están dentro del ámbito de la Directiva NIS2 a traducir las obligaciones normativas en roles y competencias concretas de personal de Ciberseguridad. El informe se elabora basado el ECSF como marco de referencia para describir perfiles profesionales y habilidades necesarias.

Perfil ECSF	Obligaciones NIS2 – tareas clave	Entregables/outputs
Chief Information Security Officer (CISO)	Lidera estrategia y cumplimiento NIS2 a nivel organizacional; supervisa gestión de riesgos, respuesta a incidentes, reporte y documentación; coordinación con alta dirección y supervisores.	Informes de vulnerabilidades, pruebas de penetración, reportes ejecutivos, plan estratégico de Ciberseguridad.
Cybersecurity Risk Manager	Identificación y análisis de riesgos, evaluación de controles, priorización de mitigaciones, revisión periódica de riesgos.	Registro de riesgos, análisis de impacto, métricas de riesgo, plan de mitigación.
Cyber Incident Responder / SOC Analyst	Detección y manejo operativo de incidentes; análisis forense inicial; revisión de logs, coordinación técnica de respuesta.	Reporte operativo de incidentes, timeline de respuesta, evidencia técnica.
Cyber Legal, Policy & Compliance Officer	Alineación con requisitos regulatorios, revisión de obligaciones NIS2, soporte en notificación de incidentes, evaluación de impacto legal y contractual.	Reportes de cumplimiento legal, guías internas, checklist normativo.
Security Architect / System Admin	Diseño de medidas y controles seguros, aseguramiento de configuraciones, soporte en pruebas y revisiones técnicas.	Arquitectura segura, evidencias de configuración, hardening checklist.
Awareness / Training Specialist	Formación interna de personal, campañas de concienciación de riesgos, simulacros de incidentes.	Materiales de formación, registros de asistencia, métricas de awareness.

Figura 15. *Mapeo de obligaciones NIS2 con los perfiles profesionales del ECSF*

5 Cybersecurity roles and skills for NIS2 essential and important entities: Mapping NIS2 obligations to ECSF role profiles. European Union Agency for Cybersecurity (ENISA). ***https://www.enisa.europa.eu/sites/default/files/2025-06/Mapping%20NIS%202%20obligations%20with%20ECSF%20role%20profiles.pdf***

Este mapeo cubre referencias a los artículos 21 y 23 de NIS2 (gestión de riesgos y reporte de incidentes), entre otras obligaciones específicas.

Cada obligación se descompone en “tareas” y se asocia con uno o varios perfiles ECSF según competencias y actividades descritas en los perfiles.

Los entregables definidos brindan evidencia concreta para auditorías internas o revisiones por autoridades.

Protección de datos de carácter personal
RGPD y LOPDyGDD

El RGPD se aplica a responsables y encargados que traten datos personales de personas físicas en el contexto de un establecimiento en la Unión Europea, así como a aquellos fuera de la Unión que ofrezcan bienes o servicios o monitoricen el comportamiento de interesados en la UE. No se estructura por sectores, sino por actividad de tratamiento. Su alcance objetivo es regular el tratamiento de datos personales para garantizar la protección de los derechos y libertades fundamentales de las personas físicas, estableciendo obligaciones de licitud, responsabilidad proactiva, seguridad (artículo 32), derechos de los interesados y régimen sancionador.

Un dato personal es aquel que, por sí mismo o combinado con otros, permite identificar a una persona física. La generación, recolección y tratamiento de datos personas es una actividad que puede atentar contra derechos fundamentales de las personas, lo que genera la necesidad de estas regulaciones. Para ello, establece que las personas pueden permitir el tratamiento de sus datos, desde su recogida a su inspección, custodia, utilización, borrado o cualquier otra actividad, otorgando un consentimiento informado a una entidad para ciertos tratamientos y finalidades. Las entidades que recogen estos datos (con estos compromisos) se denominan Responsables de Tratamiento y asumen la responsabilidad del tratamiento correcto de los datos. Cuando un Responsable pide a otra entidad que realice ciertos tratamientos de datos, esta segunda entidad pasa a ser un Encargado de Tratamiento, La relación entre Responsable y Encargado queda regulado a

La normativa de protección de datos de carácter personal, en particular el Reglamento (UE) 2016/679 (RGPD) y su desarrollo en el ordenamiento jurídico español, especialmente mediante la Ley Orgánica 3/2018, refuerza el enfoque de responsabilidad proactiva y gestión del riesgo, aunque no mencionan expresamente la figura del CISO, en contraposición a la definición explicita del rol de DPD, sí introduce obligaciones que refuerzan de manera clara la necesidad de una función especializada en seguridad de la información y Ciberseguridad.

El RGPD incorpora el principio de responsabilidad proactiva, que desplaza el foco desde el cumplimiento formal hacia la capacidad de demostrar que se han adoptado medidas técnicas y organizativas adecuadas al riesgo. En la práctica, esto implica que la seguridad deja de ser un elemento accesorio del cumplimiento y pasa a formar parte de su núcleo.

En este contexto, resulta fundamental delimitar con claridad las funciones del CISO y del Delegado de Protección de Datos. El DPD ejerce una función de supervisión independiente del cumplimiento de la normativa de protección de datos evalúa las implicaciones jurídicas y de derechos fundamentales, permitiendo que las decisiones se adopten con una visión completa y coherente y actúa como punto de contacto con las autoridades de control y con los interesados.

El CISO, por su parte, es responsable de definir, evaluar y supervisar las medidas de seguridad que protegen los datos personales y el resto de la información frente a riesgos de confidencialidad, integridad y disponibilidad. Son roles diferentes si bien comparten un enfoque dónde el cumplimiento legal es su primer objetivo y lo hacen asesorando y supervisando.

Comparten también la necesidad de disponer y sustentarse en una metodología de análisis de riesgos, orientada cada uno de ellos a su ámbito (aunque apoyándose) y un papel, de nuevo cada uno desde su especifica responsabilidad, en las brechas de seguridad y evaluaciones de impacto. Su conocimiento es complementario y su colaboración es esclarecedora y enriquecedora para la empresa.

Como muestra del trabajo coordinado que se espera, aunque con funciones diferenciadas, se recoge a continuación una pregunta tipo que la Agencia Española de Protección de Datos suele dirigir al responsable del tratamiento tras la recepción de una reclamación vinculada a un tratamiento específico: La aportación de los informes técnicos o recomendaciones elaborados por el DPO y por el responsable de seguridad, cualquiera que fuera su formato, respecto de los tratamientos sobre los que se solicita información, incluyendo el análisis de riesgos y, si corresponde, la evaluación de impacto relativa a la protección de datos.

En definitiva, el RGPD consolida un modelo en el que protección de datos y Ciberseguridad se refuerzan mutuamente sin confundirse. El rol de CISO no asume las funciones del rol del DPD ni este sustituye las responsabilidades del CISO, pero ambos resultan esenciales para que la organización gestione adecuadamente el riesgo, cumpla con sus obligaciones legales y preserve la confianza de ciudadanos, clientes y usuarios en un entorno digital cada vez más exigente.

Más adelante volveremos a la relación entre esas figuras, si bien aquí adelantamos que esta diferenciación de funciones no excluye que, dándose las adecuadas condiciones y garantías en el desempeño que eviten conflicto de intereses, una misma persona física puede desempeñar ambos roles o estar en una misma organización (que tenga por funciones principales: asesorar y supervisar).

Marcos regulatorios sectoriales y resiliencia operativa digital
LPIC y DORA

La evolución normativa muestra una tendencia clara hacia la regulación sectorial de la Ciberseguridad y de la resiliencia operativa digital, para infraestructuras críticas; es decir en aquellos ámbitos cuya interrupción puede generar impactos significativos sobre la economía, los servicios esenciales o la confianza de la ciudadanía. Esta evolución no es teórica ni futura, ya está en marcha y está condicionando de forma directa la manera en que las organizaciones, que se encuentren en el ámbito subjetivo (que sean sujetos obligados) de esos marcos regulatorios deben gestionar su riesgo digital. La resiliencia operativa digital deja de ser un objetivo aspiracional para convertirse en un criterio regulatorio verificable.

En cualquier caso, debemos señalar que, tanto en infraestructuras críticas como en la Directiva DORA, no se define un rol de RSI.

A la hora de escribir este libro blanco la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo, aún no ha sido traspuesta por lo que debemos remitirnos a la transposición de la anterior Directiva de Infraestructuras Críticas; es decir Ley8/2011.

Ley 8/2011 y Real Decreto 704/2011. Protección de Infraestructuras Críticas (España)

Esta ley de transposición de la anterior Directiva de Infraestructura Críticas.

Esta normativa se aplica a operadores designados como críticos en sectores estratégicos tales como energía, transporte, agua, tecnologías de la información y comunicaciones, sistema financiero y tributario, salud, alimentación, administración pública e industria química y nuclear. Su alcance objetivo es establecer el sistema nacional de protección de infraestructuras críticas frente a amenazas deliberadas, obligando a la elaboración de Planes de Seguridad del Operador y Planes de Protección Específicos, y articulando la coordinación público-privada.

La ley establece que los operadores críticos nombrarán y comunicarán al Ministerio del Interior un Responsable de Seguridad y Enlace con la Administración en el plazo que reglamentariamente se establezca".

Y es en el artículo 34 del RD 704/2011 donde reglamentariamente se desarrolla mínimamente el artículo precedente estableciendo en su punto 2 que "el Responsable de Seguridad y Enlace representará al operador crítico ante la Secretaría de Estado de Seguridad en todas las materias relativas a la seguridad de sus infraestructuras y los diferentes planes especificados en este reglamento, canalizando, en su caso, las necesidades operativas e informativas que surjan al respecto".

Asimismo, el artículo 35 regula la figura del Delegado de Seguridad, que será identificado y notificado a las Autoridades pertinentes y "constituirá el enlace operativo y el canal de información con las autoridades competentes en todo lo referente a la seguridad concreta de la infraestructura crítica o infraestructura crítica europea de que se trate, encauzando las necesidades operativas e informativas que se refieran a aquélla".

La Ley española, no fija la obligación de nombrar un RSI. No obstante, en una circular posterior de la Secretaría de Estado dirigida a los operadores esenciales se exigía la identificación de los datos del RSI.

DORA: Reglamento (UE) 2022/2554 – DORA (Digital Operational Resilience Act)

DORA, fue aprobado en enero de 2023 entró en vigor en enero de 2025 se aplica a entidades del sector financiero, incluyendo entidades de crédito, entidades de pago y dinero electrónico, empresas de inversión, entidades aseguradoras y reaseguradoras, gestores de fondos, infraestructuras de mercados financieros, proveedores de servicios de criptoactivos y otras entidades financieras reguladas. También afecta a proveedores terceros de servicios TIC que presten servicios a dichas entidades, pudiendo algunos ser designados como proveedores TIC críticos. Su alcance objetivo es establecer un marco integral de resiliencia operativa digital, regulando la gestión del riesgo TIC, la notificación de incidentes graves, la realización de pruebas de resiliencia digital, la gestión del riesgo de terceros TIC y un régimen específico de supervisión de proveedores tecnológicos críticos.

En esta Directiva, ni en dicho reglamento ni en los documentos que extienden DORA (Estándares Técnicos de Implementación [ICT] y Estándares Técnicos Reguladores [RTS]) se hace mención alguna sobre el rol del CISO, ni sobre su papel dentro de DORA; es decir, no se establece una figura similar al CISO, lo que no significa, como es lógico que no sea necesario o que no tenga funciones en relación a DORA.

La responsabilidad directa e implícita del CISO en relación a DORA vendrá marcada por el modo de aproximación al cumplimiento de DORA que la organización defina, que dependerá en gran medida de las funciones que tenga asignado el CISO (tema que ya hemos tratado), no obstante, a continuación, se expone el grado de involucración que debería tener asignado el CISO con respecto a los cinco pilares de DORA:

- **Gestión de Riesgos TIC:** el CISO gestiona de forma directa posiblemente uno de los riesgos más relevantes que afectan a las TIC, los ciberriesgos.
- **Gestión de terceros TIC:** en los que nuevamente el CISO debe gestionar directamente la evaluación de los ciberriresgos de esos terceros.
- **Pruebas de resiliencia operativa:** el CISO nuevamente es protagonista directo en las pruebas avanzadas de intrusión (TLPT) pues son las capacidades reales de protección, detección y respuesta las que se evalúan en estas pruebas. En el resto de las pruebas, el CISO tendrá participación siempre que la Continuidad de Negocio esté incluido dentro de las funciones de éste.
- **Gestión y Comunicación de incidentes TIC:** a pesar de que DORA tiene en su alcance todos los incidentes TIC, tengan o no un origen relacionado con la seguridad, son los de seguridad aquellos que tienen un papel especialmente relevante en DORA. Aunque no es necesario que sea el CISO quien coordine este proceso sí que es recomendable que sea éste, por sinergias con otras normativas que ya establecen y definen la comunicación de incidentes cercana a la función del CISO.
- **Compartición de información:** la compartición de información es una actividad innata en los equipos de seguridad, existiendo en la actualidad sistemas desarrollados para el intercambio de información relevante. Es por ello que lo más aconsejable que el gobierno de esta función recaiga en el CISO.

Cadena de suministro desde la perspectiva de obligación legal

En este apartado desde una visión de las exigencias legales, introduciremos la necesidad[CCF14.1] de gestionar la cadena de suministro, los proveedores y en extensión, los proveedores de estos últimos. También enunciaremos las obligaciones en relación a esa gestión establecen las legislaciones en materia de Ciberseguridad y protección de datos.

Legislaciones como el ENS, NIS2, RGPD o DORA, exigen un control de la cadena de suministro. En las subsecciones siguientes conforme a cada una de ellas, haremos un repaso rápido de sus exigencias para esta.

Contratación pública y ENS
Integración del riesgo de proveedores

En el ámbito español, las entidades del sector público deben regirse por la normativa de contratación pública y, adicionalmente, por los marcos sectoriales que les resulten aplicables -entre ellos el ENS y, en su caso, la normativa de operador esencial, protección de datos o regulación financiera-. Esta convergencia normativa implica que las obligaciones en materia de Ciberseguridad deben proyectarse necesariamente sobre la cadena de suministro.

La legislación de contratación pública no regula la Ciberseguridad como disciplina autónoma, pero sí impone deberes de diligencia, definición precisa del objeto contractual, evaluación de riesgos y supervisión de la correcta ejecución. Cuando el contrato afecta a sistemas de información, tratamiento de datos o prestación de servicios digitales, estos deberes adquieren una dimensión técnica específica: la seguridad pasa a ser una condición esencial del contrato. La omisión de requisitos adecuados o la ausencia de seguimiento efectivo no elimina el riesgo, sino que lo desplaza fuera del perímetro directo de control de la organización.

Desde la perspectiva del ENS, el Real Decreto 311/2022 establece en su artículo 2 la aplicabilidad del Esquema a proveedores que presten servicios o gestionen sistemas para entidades públicas. Esta previsión implica que los sistemas utilizados en la prestación deben cumplir las exigencias del ENS conforme a su categoría y que, cuando proceda, deberán emplearse productos certificados incluidos en el catálogo correspondiente. No se trata únicamente de una cláusula contractual opcional, sino de una exigencia normativa vinculada al propio ámbito subjetivo del Esquema.

En este contexto, la función del CISO no es sustituir a los órganos de contratación ni asumir la gestión contractual, sino integrar el análisis del riesgo digital en el proceso de contratación. Ello supone definir los criterios y requisitos de seguridad que deben incorporarse a los pliegos, en función de la criticidad del servicio y del impacto potencial de un incidente, y posteriormente verificar su cumplimiento. Sin esta intervención especializada, el proceso tiende a priorizar variables económicas o funcionales, relegando el riesgo tecnológico a un plano secundario.

La responsabilidad no concluye con la adjudicación. La supervisión de la ejecución contractual, exigida por la normativa de contratación, debe incorporar una dimensión técnica continua cuando el objeto del contrato es digital. Cambios en el servicio, subcontrataciones o alteraciones en el entorno tecnológico pueden modificar sustancialmente el perfil de riesgo inicial. Mantener visibilidad sobre estas variaciones es esencial para evitar que el contrato se convierta en un punto ciego en materia de seguridad.

Finalmente, la contratación pública pone de relieve la necesidad de identificar dependencias críticas y concentraciones de riesgo. La dependencia de un único proveedor, de una tecnología sin alternativa viable o de un modelo de prestación poco transparente puede generar puntos únicos de fallo con impacto directo en la continuidad del servicio. La aportación del CISO consiste en introducir esta visión preventiva y estratégica dentro de un marco jurídico condicionado por los principios de concurrencia, transparencia y eficiencia, equilibrando la seguridad con las exigencias propias del sector público.

Felizmente para la competitividad, pero lamentablemente para alcanzar el grado más optimo de la seguridad, el CISO, el RSI en este caso, no es libre, como pudiera serlo en el sector privado, para elegir el mejor producto o el mejor servicio basándose sólo en cuestiones técnicas y conforme a su criterio, pues las económicas y los principios de libre competencia, concurrencia, proporcionalidad, eficiencia y transparencia, pues estas limitan el carácter discrecional que en ocasiones sería lo más eficaz (aunque también lo más opaco).

NIS2
Seguridad de la cadena de suministro

La NIS2 incorpora la seguridad de la cadena de suministro como uno de los componentes obligatorios del marco de gestión de riesgos que deben aplicar las entidades esenciales e importantes.

El artículo 21 exige adoptar medidas técnicas, operativas y organizativas apropiadas y proporcionadas, incluyendo expresamente la consideración de los riesgos derivados de proveedores directos y proveedores de servicios. La evaluación debe contemplar la exposición a terceros y la calidad y resiliencia de los productos y servicios utilizados.

A diferencia de DORA, la Directiva no detalla un catálogo contractual cerrado ni establece un régimen autónomo de supervisión de proveedores críticos, sino que integra la dimensión de la cadena de suministro dentro del deber general de gestión del riesgo. Corresponde a cada entidad determinar, en función de su exposición y criticidad, las medidas concretas que aseguren un nivel adecuado de seguridad.

La responsabilidad de aprobar y supervisar estas medidas recae en el órgano de dirección, y su incumplimiento puede dar lugar a sanciones en el marco del régimen de supervisión reforzada previsto para entidades esenciales e importantes. Además, la Directiva prevé mecanismos de cooperación y posibles evaluaciones coordinadas a nivel de la Unión cuando determinados productos, servicios o dependencias generen riesgos significativos.

RGPD
Encargados del tratamiento y garantías en la cadena de suministro

El Reglamento General de Protección de Datos (RGPD) regula de forma expresa la relación entre el responsable del tratamiento y los terceros que tratan datos personales por cuenta de aquel. A diferencia de otros marcos que abordan la cadena de suministro desde la resiliencia operativa o la continuidad del servicio, el RGPD centra su exigencia en la protección de los datos personales y en la atribución clara de responsabilidades.

El artículo 28 establece que cuando un tratamiento sea realizado por cuenta del responsable deberá elegirse únicamente a encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con el Reglamento y garantice la protección de los derechos de las personas interesadas. Esta exigencia implica una evaluación previa del proveedor y la formalización de un contrato u otro acto jurídico que vincule al encargado con el responsable, detallando el objeto, duración, naturaleza y finalidad del tratamiento, así como las obligaciones y derechos de ambas partes.

El contrato debe incluir, entre otros extremos, instrucciones documentadas del responsable, deber de confidencialidad, adopción de medidas de seguridad conforme al artículo 32, régimen de subcontratación, asistencia en el ejercicio de derechos, colaboración en la gestión de brechas de seguridad y destino de los datos al finalizar la prestación. La subcontratación ulterior requiere autorización previa, específica o general, manteniéndose la responsabilidad del encargado inicial frente al responsable.

El RGPD refuerza además la posición del responsable al establecer que este debe ser capaz de demostrar el cumplimiento del Reglamento (principio de responsabilidad proactiva). En el contexto de la cadena de suministro, ello implica no solo incorporar cláusulas contractuales adecuadas, sino también verificar que el encargado aplica efectivamente las medidas acordadas, especialmente cuando el tratamiento pueda entrañar un alto riesgo para los derechos y libertades de las personas físicas.

Desde la perspectiva del RSI o del CISO, el RGPD introduce una dimensión específica del riesgo en la cadena de suministro: el riesgo sobre datos personales. Su función consiste en integrar los requisitos de seguridad técnica exigidos por el artículo 32 dentro del proceso de selección y supervisión de proveedores, asegurando coherencia entre el marco general de Ciberseguridad de la organización y las obligaciones específicas en materia de protección de datos.

DORA
Gestión del riesgo de terceros TIC

DORA establece un régimen normativo específico y detallado sobre la gestión del riesgo derivado de terceros proveedores TIC en el sector financiero. Parte de un principio claro: la externalización no exime de responsabilidad. La entidad financiera mantiene íntegramente su responsabilidad respecto del cumplimiento normativo y de la resiliencia operativa, aun cuando el servicio esté completamente delegado.

El Reglamento exige integrar el riesgo de terceros dentro del marco general de gestión del riesgo TIC, mediante una estrategia formal aprobada por el órgano de dirección y el mantenimiento de un registro actualizado de todos los contratos TIC. Además, obliga a identificar los servicios que soportan funciones críticas o importantes y a aplicarles un régimen reforzado.

DORA impone requisitos contractuales mínimos obligatorios, entre ellos cláusulas sobre niveles de servicio, confidencialidad, integridad, disponibilidad, notificación de incidentes, derechos de auditoría, condiciones de subcontratación y mecanismos de terminación y salida. Estos requisitos son particularmente exigentes cuando el proveedor presta servicios que afectan a funciones críticas.

La norma también establece la obligación de supervisión continua del proveedor durante todo el ciclo de vida contractual, incluyendo la evaluación de concentraciones de riesgo, dependencias tecnológicas y cambios en la subcontratación. Asimismo, exige estrategias de salida viables para evitar dependencias estructurales que comprometan la continuidad operativa.

Como elemento singular, DORA introduce un sistema europeo de supervisión para proveedores TIC designados como críticos, sometiéndolos a control directo por las Autoridades Europeas de Supervisión.

3.

Desarrollo del perfil del CISO

3.1. Perfil híbrido: Técnico, estratégico y comunicador

A lo largo del libro se han descrito la misión, funciones y responsabilidades del CISO. También se ha delimitado el tipo de retos que afronta: proteger la continuidad del negocio, gestionar entornos tecnológicos complejos y responder a amenazas cada vez más sofisticadas.

Aunque cada CISO desarrolla su propio estilo, como ocurre con otros roles ejecutivos como CIO, CTO, CEO o CFO, es necesario partir de una definición base del perfil, sustentada en capacidades que garanticen un ejercicio adecuado de la función.

Para evitar redundancias con capítulos anteriores, en este apartado se resumen tres características esenciales que cualquier CISO debería cultivar. Los perfiles rígidos o aislados pierden valor rápidamente en organizaciones dinámicas.

/ Un CISO Ágil y Adaptativo

El CISO opera en un contexto global marcado por marcos como:

- VUCA (Volatility, Uncertainty, Complexity, Ambiguity): un entorno volátil, incierto, complejo y ambiguo.
- BANI (Brittle, Anxious, Nonlinear, Incomprehensible): sistemas frágiles, organizaciones ansiosas, comportamientos no lineales y situaciones difíciles de interpretar.

En este escenario, la capacidad de adaptarse rápidamente, replantear estrategias y mantener la estabilidad en contextos cambiantes se convierte en una competencia crítica.

Ejemplo: Para responder a un ataque sectorial emergente incluir en su alcance de responsabilidades el ámbito OT (que hasta ahora le era ajeno) y definir en semanas una estrategia concreta de protección para los activos OT.

/ Un CISO en desarrollo permanente

La Ciberseguridad es, por definición, un campo dinámico. Un CISO debe mantener un interés constante por la formación y la actualización: nuevas normativas, nuevas técnicas de ataque (IA generativa, ataques a la cadena de suministro), nuevos modelos de arquitectura (Zero Trust, SASE, entornos híbridos IT/OT).

Cultivar esta mentalidad de aprendizaje no solo permite anticiparse a amenazas futuras, sino también liderar con credibilidad a los equipos técnicos.

/ Un CISO dentro de un Ecosistema

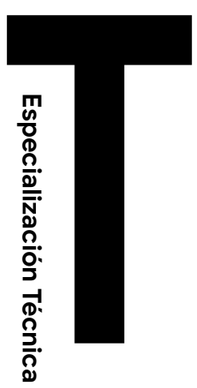
La seguridad no se construye de forma aislada. El CISO debe colaborar con múltiples actores:

- Áreas internas (Operaciones, IT, Jurídico, RR. HH., Comunicación).
- Organismos reguladores.
- Proveedores y socios tecnológicos.
- Comunidades profesionales y ecosistemas sectoriales.

Un CISO aislado pierde influencia y limita la implantación de cualquier estrategia. Participar activamente en la comunidad profesional, intercambiando prácticas y conocimientos, es esencial para evolucionar al ritmo del entorno.

Además de su rol en marcos formales de gobierno, el CISO debe saber relacionarse en ámbitos informales dentro y fuera de la organización, construyendo una red de influencia personal.

3.2. El CISO como *Profesional "T-Shape"*



El CISO moderno encaja plenamente con el concepto de profesional en forma de T (T Shape): una combinación entre amplitud directiva (barra horizontal) y profundidad técnica (barra vertical). Este modelo permite comprender cómo el CISO integra liderazgo, estrategia, conocimiento del negocio y dominio técnico en un solo rol.

Transversalidad Directiva

La barra horizontal engloba las capacidades que diferencian al CISO de un mero especialista técnico. Incluye competencias orientadas a comunicar, gestionar, influir y conectar seguridad con negocio.

1. Comunicación ejecutiva

El CISO debe ser capaz de:

- Elevar a los órganos de dirección todos los elementos que forman parte de sus responsabilidades.
- Explicar riesgos complejos de forma formal, clara y entendible.
- Traducir amenazas técnicas en impactos reales para el negocio.
- Aportar asesoramiento documentado y trazable para la toma de decisiones.

La comunicación ejecutiva es clave para que la seguridad esté integrada en la gobernanza corporativa.

2. Gestión y liderazgo

La transversalidad exige capacidad para:

- Dirigir equipos multiculturales y multidisciplinares.
- Atraer, desarrollar y retener talento técnico escaso y altamente demandado.

El CISO lidera, influye y conecta, no solo gestiona.

3. Visión estratégica de negocio

Una parte esencial de su función directiva implica:

- Alinear la Ciberseguridad con los objetivos corporativos.
- Proponer inversiones con retornos claros, cuantificables y defendibles.
- Comprender procesos de negocio para identificar dependencias críticas y puntos de fallo.
- Trabajar de forma coordinada con áreas como Jurídico, Compras, RRHH, Sistemas, Operaciones, etc.
- Como participar formalmente en procesos de compra para garantizar la seguridad desde el diseño.

4. Gestión de crisis

El CISO debe:

- Liderar incidentes críticos con serenidad y criterio.
- Coordinarse con reguladores, clientes, proveedores y comunicación corporativa.
- Contribuir a los comités de crisis y continuidad.
- Tomar decisiones bajo presión, priorizando técnicamente el riesgo con visión analítica.

5. Capacidades financieras

El rol exige comprender el impacto económico del riesgo:

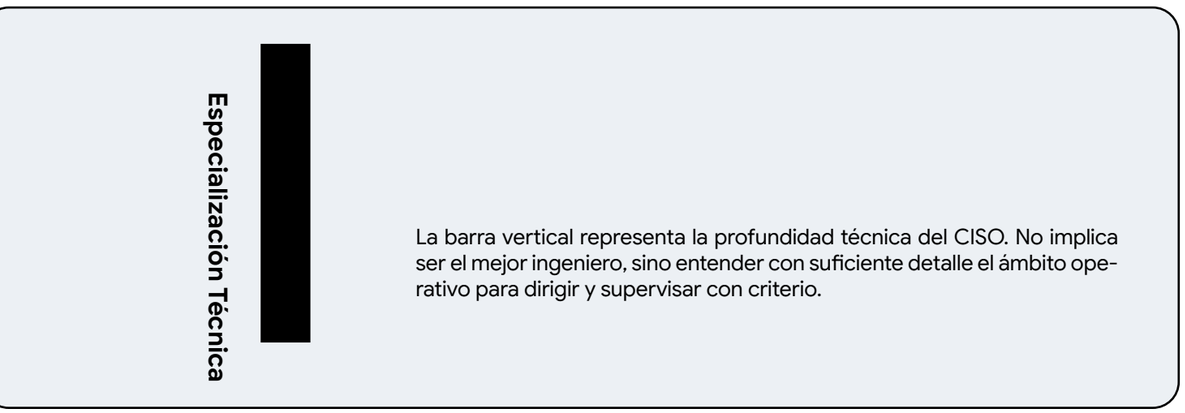
- Elaboración y defensa de presupuestos.
- Evaluación del riesgo en términos de impacto económico y coste de oportunidad.

6. Gobierno Compliance y Regulación:

El CISO debe dominar los marcos normativos relevantes:

- ENS, NIS2, RGPD, DORA, normativa sectorial.
- Frameworks como ISO 27001, NIST CSF, IEC 62443, COBIT, ITIL.
- Capacidad para traducir requisitos regulatorios en acciones operativas.
- Relación fluida con auditores y reguladores.

Incluye también ***habilidades soft:*** rigor, atención al detalle, capacidad de coordinación y visión de empresa, especialmente en organizaciones con fuerte presión regulatoria o contractual.



1. Conocimiento técnico avanzado

Debe comprender:

- Arquitecturas IT/OT.
- Operaciones (SOC), gestión de incidentes (CSIRT).
- Entornos cloud y redes.
- IAM, Zero Trust, SASE.
- IA, cifrado y amenazas post cuánticas.
- Inteligencia de amenazas.
- Tecnologías defensivas y ofensivas.

2. Gobierno y normativas

Incluye:

- ENS, NIS2, DORA, RGPD, ISO 27001, IEC 62443, NIST CSF, entre otras.
- Capacidad para convertir requisitos normativos en controles y acciones prácticas.
- Gestión y gobierno de marcos como COBIT o ITIL.

3. Gestión de riesgos

Un CISO debe dominar:

- Identificación, valoración y tratamiento del riesgo digital.
- Reporting orientado a negocio.
- Metodologías formales.
- Gestión de terceros y ciberseguros.

4. Capacidad para dialogar al nivel técnico adecuado:

Debe poder:

- Entender incidentes, arquitecturas y soluciones con profundidad suficiente.
- Establecer un lenguaje técnico común con ingenieros, arquitectos, desarrolladores y equipos especializados.

No se trata de “saberlo todo”, sino de tener la profundidad necesaria para evaluar, desafiar y decidir con criterio técnico-directivo.

3.3. Dilemas reales del CISO

El ejercicio del rol de CISO se desarrolla, de forma habitual, en un entorno de tensión estructural entre la necesidad de proteger a la organización frente a riesgos digitales crecientes y la presión por alcanzar objetivos de negocio, innovación y eficiencia. Estos dilemas no responden a fallos individuales ni a carencias técnicas. Son inherentes a la naturaleza transversal de la función y a su impacto directo en la operación y la estrategia. Reconocerlos es un indicador de madurez profesional y organizativa.

El conflicto con el negocio y la presión por avanzar

Uno de los dilemas más frecuentes a los que se enfrenta el CISO surge cuando las necesidades de seguridad entran en tensión con los objetivos de negocio, especialmente en contextos de transformación digital, reducción de plazos o presión competitiva. Esa tensión, en demasiadas ocasiones deriva en conflictos.

En estos escenarios, la Ciberseguridad puede percibirse como un factor que introduce fricción, retrasos o costes adicionales. El CISO se ve entonces obligado a equilibrar la protección del riesgo digital con la viabilidad del negocio, evitando tanto el bloqueo sistemático como la aceptación acrítica de decisiones que incrementan de forma desproporcionada la exposición al riesgo.

El ejercicio responsable del rol exige que el CISO:

- Asegurar que el negocio comprende que no existe negocio sin Ciberseguridad.
- Evitar conflictos de intereses derivados de dependencias jerárquicas inadecuadas.
- Traducir riesgos técnicos en impactos de negocio.
- Proponer alternativas proporcionales.
- Asegurar que la gestión del riesgo recae en el negocio (aceptar, rechazar, tratar, transferir).
- Elevar formalmente los riesgos que superan los niveles aceptables.

Aceptar el conflicto y gestionarlo con transparencia suele ser más eficaz que intentar diluirlo.

Riesgos que la Dirección decide asumir

Otro dilema recurrente se produce cuando, tras haber sido correctamente identificado y analizado, un riesgo digital es asumido conscientemente por la Dirección por razones estratégicas, presupuestarias o de oportunidad.

En estas situaciones, la responsabilidad del CISO no consiste en impedir la decisión ni en asumirla de forma implícita, sino en:

- Asegurar que el riesgo se ha explicado con claridad.
- Documentar las implicaciones y escenarios posibles.
- Y supervisar que las medidas de Ciberseguridad se adoptan conforme a la gestión del riesgo tomada.

La madurez del gobierno del riesgo se refleja en la capacidad de la organización para asumir riesgos de forma consciente, no en la pretensión de eliminarlos por completo. No obstante, el CISO debe velar porque esta asunción no se convierta en una normalización de exposiciones inaceptables ni en una transferencia silenciosa de responsabilidad hacia el nivel técnico.

El equilibrio entre independencia y pertenencia a la organización

El CISO debe mantener suficiente independencia para evaluar y elevar riesgos con objetividad, pero a la vez formar parte de la organización y contribuir a sus objetivos.

Una independencia excesiva puede aislar. Una integración excesiva puede diluir la función de control.

La clave es un modelo de gobierno claro, responsabilidades bien definidas y una relación de confianza con la Alta Dirección.

Protección institucional del CISO y diligencia debida

El desempeño del rol del CISO implica una exposición personal y profesional significativa, especialmente en organizaciones sujetas a marcos regulatorios exigentes, escrutinio público o en el ámbito público a rotaciones frecuentes en la alta dirección como consecuencia del devenir político. Por ello, resulta esencial que el ejercicio de la función esté respaldado por mecanismos de protección institucional, que garanticen la trazabilidad de las decisiones y la diligencia debida.

Esta protección no se articula en términos individuales, sino mediante:

- la existencia de procesos formales de elevación de riesgos,
- la documentación de decisiones relevantes y de riesgos asumidos,
- la participación del CISO en los órganos y foros adecuados,
- y el respaldo explícito del órgano de gobierno al modelo de gestión del riesgo.

Sin estos mecanismos, el CISO queda expuesto a responsabilidades que no le corresponden, y la organización pierde capacidad de demostrar diligencia.

Dilemas como señal de madurez organizativa

La existencia de dilemas en torno a la Ciberseguridad no debe interpretarse como una disfunción, sino como un indicador de madurez organizativa. Las organizaciones que reconocen y gestionan estos dilemas de forma explícita están mejor preparadas para integrar el riesgo digital en su toma de decisiones.

El CISO desempeña un papel clave en este proceso, no como garante absoluto de la seguridad, sino como facilitador de decisiones informadas, equilibradas y defendibles en un entorno de riesgo creciente.

3.4. El CISO como función directiva y de gobierno

Todas las actividades descritas que al final estén en su función deben interpretarse, con independencia de que el CISO las ejerza directamente o dirija su ejecución, desde una premisa esencial: su naturaleza es eminentemente directiva.

La función del CISO se integra en el sistema de gobierno de la organización como una responsabilidad de carácter estratégico y transversal. No se define por la administración de tecnologías concretas ni por la supervisión operativa de herramientas específicas, sino por la capacidad de mantener una visión global, independiente y objetiva del riesgo digital.

Su cometido principal es asegurar que dicho riesgo se identifica, evalúa y gestiona de forma coherente con la estrategia corporativa, el apetito de riesgo definido por la alta dirección y las obligaciones normativas y contractuales que resulten de aplicación.

Para que esta función aporte valor real, el CISO debe contar con una jerarquía y un posicionamiento organizativo que garantice la independencia necesaria para evaluar la exposición al riesgo sin condicionantes operativos ni intereses cruzados. Cuando quien identifica el riesgo depende directamente de quien lo ejecuta o lo asume, la Organización pierde visibilidad y sustituye el análisis por una narrativa tranquilizadora que rara vez resiste un incidente real.

En este sentido, el CISO no debe ser percibido como un rol operativo ni como una extensión del área tecnológica, sino como una figura de gobernanza especializada, responsable de velar por que la organización disponga de un marco sólido y sostenible para gestionar el riesgo digital en el tiempo. Su eficacia depende, en gran medida, de su capacidad de influencia, de su acceso a los niveles adecuados de decisión y del reconocimiento explícito de su función como parte integrante del gobierno de la organización.

Definido este carácter directivo, es necesario analizar cómo se traduce en la práctica a través de la estrategia, el gobierno del riesgo, el marco de control, la gestión de crisis y la creación de cultura.

Definición y dirección de la estrategia de Ciberseguridad

Hasta ahora se han descrito las actividades operativas y directivas vinculadas al rol del CISO. Es necesario detenerse en esta última, porque es la que da sentido y dirección al conjunto.

La función directiva no ejecuta controles ni gestiona incidentes en primera línea. Establece el marco en el que esas actividades deben desarrollarse, transformando tareas operativas en decisiones de gobierno articuladas en torno a prioridades, criterios de riesgo y objetivos estratégicos.

Es en este plano donde el riesgo digital deja de ser una cuestión técnica y se integra en la arquitectura de decisiones de la organización.

La estrategia de Ciberseguridad es el mecanismo que permite alinear la seguridad con la estrategia corporativa, formular prioridades de medio y largo plazo y evitar respuestas tácticas dictadas por urgencias puntuales.

Un CISO eficaz traduce el riesgo técnico en impactos comprensibles: continuidad, recuperación, exposición regulatoria, reputación y coste de operar la seguridad.

La implantación de la estrategia debe supervisarse de forma continua para garantizar que los principios estratégicos se reflejan en la arquitectura y los procesos y que las prioridades se ajustan cuando cambia el contexto tecnológico, regulatorio o de amenazas.

Finalmente, la estrategia solo es efectiva cuando se apoya en un modelo de gobierno del riesgo que permita priorizar, decidir y revisar de forma continua las exposiciones relevantes.

Gobierno del riesgo digital

El gobierno del riesgo digital es el núcleo de la función directiva del CISO. No consiste en listar amenazas o inventariar vulnerabilidades, sino en comprender la exposición real de la organización y orientar decisiones coherentes.

Esto exige una visión amplia que incluya operación y prestación de servicios, confianza de clientes y ciudadanos, cumplimiento normativo y sostenibilidad económica.

El CISO actúa como garante de la coherencia entre el apetito de riesgo definido por la alta dirección y las decisiones adoptadas en la práctica.

Cuando el riesgo supera los umbrales aceptables, debe elevarse con claridad.

Si se decide asumirlo, la asunción debe ser consciente, explícita y documentada.

Este gobierno exige comunicación continua, comprensible y orientada a la decisión, con indicadores que permitan comparar, priorizar y actuar.

El riesgo digital debe integrarse en los procesos ordinarios de la organización. La gestión puntual reactiva pierde eficacia: solo un gobierno continuo y transversal permite anticipar, priorizar y construir resiliencia.

Supervisión del marco de control y de la madurez en Ciberseguridad

La estrategia y el gobierno del riesgo digital solo se materializan cuando se traducen en un marco de control que pueda operarse de forma consistente en el día a día. En este ámbito, la función del CISO no es ejecutar controles, sino asegurar que la organización dispone de un conjunto coherente de principios, políticas y mecanismos que protegen lo esencial sin introducir una complejidad innecesaria.

Supervisar el marco de control implica verificar que las medidas técnicas, organizativas y procedimentales responden al nivel de riesgo identificado y que evolucionan al ritmo del negocio, de la tecnología y del contexto regulatorio. Un control que no se puede mantener, que no se entiende o que no se integra en los procesos reales de trabajo deja de ser una medida de protección y se convierte en fricción operativa.

La evaluación de la madurez en Ciberseguridad es una parte esencial de esta función. El CISO debe promover una visión honesta del estado de la organización, identificando avances y carencias sin caer ni en el exceso de confianza ni en la sobrerreacción. La madurez no se mide por el número de controles implantados, sino por su integración, su sostenibilidad y su capacidad para responder eficazmente cuando se produce un incidente.

La dirección necesita indicadores reducidos y relevantes: evolución del riesgo, eficacia de controles clave, exposición a terceros, capacidad de respuesta y recuperación.

El objetivo último es promover una mejora continua, ajustando medidas que aumenten la resiliencia y eviten modelos puramente reactivos.

Gestión de crisis y contribución a la resiliencia organizativa

La continuidad de negocio y la resiliencia organizativa son responsabilidades propias de la organización y de sus órganos de dirección, que se articulan a través de las funciones específicamente designadas para ello. En este marco, el CISO no es responsable de la continuidad de negocio, pero desempeña un papel determinante en la preparación y gestión de las crisis derivadas de incidentes de Ciberseguridad, desde la perspectiva del riesgo digital.

La gestión de crisis en Ciberseguridad no admite improvisación. Corresponde al CISO asegurar que la organización dispone de capacidades adecuadas de prevención, detección y respuesta, y que estas se encuentran alineadas y coordinadas con los planes de continuidad de negocio y de recuperación ante desastres definidos por las funciones competentes. Esta contribución debe contemplar no solo los aspectos técnicos del incidente, sino también sus implicaciones operativas, legales, regulatorias, reputacionales y de comunicación.

Durante un incidente relevante, el CISO actúa como referente en materia de riesgo digital, aportando una visión global de la situación y ayudando a priorizar decisiones en un contexto de información incompleta y presión temporal. Su función no es dirigir la operación técnica ni la continuidad del negocio, sino proporcionar criterio experto sobre impactos, dependencias críticas y escenarios de evolución, contribuyendo a que la respuesta sea proporcionada, coordinada y coherente con las prioridades estratégicas de la organización.

Cultura, concienciación y liderazgo transversal

La Ciberseguridad no se sostiene únicamente sobre controles y procedimientos, sino sobre decisiones cotidianas y comportamientos reales. La forma en que las personas priorizan actúa bajo presión y entienden su responsabilidad frente al riesgo digital condiciona de manera directa la capacidad de la organización para resistir y recuperarse ante incidentes. En este ámbito, el CISO ejerce un liderazgo clave como impulsor de una cultura de seguridad coherente con la realidad del negocio y con los valores de la organización.

La concienciación en Ciberseguridad no debe abordarse como un ejercicio informativo ni como una sucesión de campañas genéricas, sino como un proceso continuo orientado a mejorar el criterio con el que se toman decisiones en contextos reales. Corresponde al CISO definir los objetivos y los mensajes esenciales, alineados con el contexto de amenazas y con las prioridades de la organización, evitando enfoques normativos que no conectan con la operativa diaria.

Para que esta concienciación sea efectiva, el CISO debe ser capaz de comprender y utilizar el lenguaje propio de cada colectivo. Hablar de riesgo, coste y sostenibilidad con las áreas financieras, de confianza y reputación con marketing y comunicación, de disponibilidad, degradación aceptable y tiempos de recuperación con operaciones, y de arquitectura, deuda técnica y operabilidad con tecnología. Esta capacidad de adaptación no es accesoria, es una condición necesaria para que la Ciberseguridad se integre en la toma de decisiones real.

En este contexto, resulta crítico que el CISO se apoye en las áreas de comunicación. Son estas áreas quienes conocen cómo se construye cultura en cada colectivo, qué formatos generan impacto, qué narrativas son creíbles y qué canales funcionan.

La colaboración entre comunicación y seguridad permite trasladar mensajes coherentes, adaptados y sostenibles en el tiempo, evitando campañas uniformes que rara vez cambian comportamientos.

Gestión del riesgo de terceros y de la cadena de suministro

En apartados anteriores se abordó este tema desde la perspectiva normativa. Aquí se analiza desde una visión empresarial más amplia, que aplica incluso cuando las obligaciones legales no afectan por igual a todas las organizaciones.

La dependencia de terceros y la externalización de procesos críticos es hoy uno de los principales factores de exposición al riesgo digital. Aunque la ejecución de determinados servicios se delegue, el impacto de un incidente no se externaliza. La interrupción del servicio, la exposición regulatoria o el daño reputacional recaen siempre sobre la organización.

En este contexto, el CISO desempeña un papel esencial en la definición y supervisión del marco de gestión del riesgo de terceros. Su responsabilidad no es gestionar contratos, sino establecer criterios claros que permitan evaluar el riesgo asociado a cada proveedor en función de la criticidad del servicio, el acceso a información sensible y la dependencia operativa generada.

Este enfoque exige diferenciar entre proveedores de impacto limitado y terceros críticos, evitando modelos uniformes difíciles de sostener. El CISO debe definir los niveles de exigencia adecuados y garantizar que la Ciberseguridad se integre en los procesos de selección, contratación y seguimiento, en coordinación con compras, legal, contratación y gestión de proveedores.

Desde la perspectiva de resiliencia, el CISO debe asegurar que los riesgos de la cadena de suministro digital se integran en el **modelo global de gestión del riesgo**[6]. Esto implica identificar dependencias críticas, evaluar concentraciones de riesgo y contemplar escenarios de fallo que puedan comprometer la continuidad del servicio.

Una cadena de suministro sin alternativas viables es, en la práctica, una fuente de indisponibilidad futura.

El riesgo de terceros cambia con la evolución de los servicios, los modelos de prestación, el contexto de amenazas o el marco regulatorio. El CISO debe promover una vigilancia continua para ajustar criterios y prioridades antes de que un incidente externo se convierta en una crisis interna. La anticipación es una de las palancas más eficaces para reforzar la resiliencia en entornos interconectados.

[6] Modelo de cuestionario unificado para el control de la cadena de suministro: ***https://www.ismsforum.es/ficheros/descargas/cartacadenasuministrosfinal1739549325.pdf***
Guía para la gestión de ciberincidentes originados en la cadena de suministro: ***https://www.ismsforum.es/ficheros/descargas/guia-para-la-gestion-de-crisis-por-ciberincidente.pdf***
Cláusulas contractuales para sistemas/servicios de IA: ***https://master.ismsforum.es/wp-content/uploads/2025/03/informe-isms-v41742972337.pdf***
Guía de Ciberseguridad en entornos industriales para PYMEs: ***https://www.ismsforum.es/ficheros/descargas/guia-entornos-industriales-20231686772410.pdf***

3.5. Responsabilidad de la Alta dirección en materia de Ciberseguridad y posicionamiento en el organigrama del CISO

El rol del CISO ha evolucionado hacia un perfil híbrido, que combina conocimiento técnico, capacidad de comunicación y funciones directivas con visión estratégica. Sin embargo, esta evolución es insuficiente si el modelo organizativo y el grado de implicación de la Alta Dirección no acompañan.

La falta de coherencia entre estructura y funciones continúa siendo uno de los principales obstáculos para alcanzar niveles elevados de madurez en Ciberseguridad, incluso cuando se dispone de profesionales altamente cualificados.

Modelos organizativos y su evolución

Las organizaciones presentan hoy varios modelos posibles para situar la función de Ciberseguridad. Uno de los más habituales es integrar al CISO dentro del área de TI, normalmente bajo la dependencia del Chief Information Officer (CIO).

En este modelo, la función adopta un enfoque predominantemente técnico, centrado en sistemas e incidentes. Esta ubicación condiciona prioridades, visibilidad y capacidad de supervisión, reforzando una visión limitada a la infraestructura tecnológica.

Por ello, resulta necesario definir una interdependencia clara entre la función de Ciberseguridad y las áreas responsables de los sistemas, de modo que el CISO tenga una visión completa y transversal para proteger los intereses del negocio.

Existe otro modelo donde CISO y CIO reportan independientemente a la Alta Dirección. Este enfoque aporta independencia, pero genera preguntas sobre dónde debe situarse la operativa diaria.

- Si la operativa recae íntegramente en Ciberseguridad, las áreas de sistemas pueden perder autonomía, aumentando el riesgo operativo.
- Si recae en TI, la función de Ciberseguridad puede perder visibilidad e influencia, dificultando la identificación temprana de riesgos y la corrección adecuada.

La resolución de esta tensión depende del nivel de colaboración, la claridad de funciones y el respaldo de la Alta Dirección.

La transformación del modelo tradicional responde a la necesidad de ampliar el alcance real de la función. Sin acceso directo a la Alta Dirección, los riesgos relevantes se diluyen en niveles intermedios, los asesoramientos quedan “encajonados” por miedo a escalar realidades incómodas y la conversación se reduce a cuestiones técnicas.

En este contexto, el rol del CISO deja de ser “propietario” del riesgo para convertirse en el principal asesor en materia de Ciberseguridad para la Alta Dirección y las áreas de negocio. Su misión es identificar, contextualizar y trasladar riesgos de manera comprensible, facilitando la toma de decisiones, la priorización y el tratamiento.

Este enfoque requiere un CISO con un perfil híbrido: capaz de comprender la complejidad técnica del riesgo, pero también de comunicarla con claridad directiva.

Posicionamiento del CISO en el organigrama

El posicionamiento del CISO dentro del organigrama es una consecuencia directa de esta evolución del rol. La Ciberseguridad implica decisiones transversales que afectan a áreas como operaciones, legal, compras, comunicación o desarrollo de producto.

Por este motivo, resulta imprescindible (y en ocasiones por cumplimiento legal como hemos visto) que el CISO disponga de una línea de reporte directa a la Alta Dirección. En modelos organizativos alternativos, la efectividad de la función se ve reducida y las decisiones pueden quedar condicionadas por intereses parciales y evite conflicto de interés que repercutan en el nivel de seguridad de la empresa.

Comparar modelos organizativos evidencia el impacto: en estructuras tradicionales, un riesgo relevante puede permanecer semanas circulando entre áreas sin elevarse. Y en modelos maduros, el riesgo se escala con prontitud, se contextualiza en términos de impacto y se decide de manera informada.

La diferencia fundamental reside en el poder de decisión que otorga el encaje organizativo del CISO.

Rol compartido: CISO y Alta Dirección

Un posicionamiento adecuado permite que el CISO actúe con el respaldo de la Alta Dirección a la hora de asumir riesgos, evitando decisiones individuales sin apoyo institucional. La responsabilidad del CISO se centra en garantizar que dichas decisiones se tomen con información suficiente y alineadas con el apetito de riesgo definido por la organización. En ausencia de esta dinámica, el resultado es un CISO con responsabilidad formal, pero sin respaldo real, expuesto a asumir riesgos que no le corresponden.

Las organizaciones que alcanzan un mayor nivel de madurez integran de forma explícita a la Alta Dirección en este proceso. En estos contextos, se establecen prioridades claras, se respaldan decisiones complejas y se comprende la Ciberseguridad como un elemento habilitador del negocio en lugar de un freno. La conversación evoluciona desde controles y auditorías hacia resiliencia, continuidad y toma de decisiones informadas.

3.6. Relación con el ecosistema externo

La función del CISO no se ejerce en un entorno cerrado. El riesgo digital es sistémico por naturaleza: se propaga entre organizaciones y sectores, depende de la interconexión tecnológica y evoluciona conforme lo hace el marco regulatorio. Por ello, la relación con el ecosistema externo no es un complemento, sino un componente esencial de la resiliencia organizativa.

El CISO actúa como interlocutor técnico y de gobierno frente a reguladores y autoridades competentes, organismos de respuesta a incidentes, entidades sectoriales, y mecanismos de coordinación público privada.

Esta interlocución es clave tanto en situaciones ordinarias, para alinear expectativas y criterios, como durante incidentes relevantes, donde la calidad del mensaje y la capacidad de coordinación condicionan la evolución y el impacto final.

Asimismo, corresponde al CISO mantener una relación activa con las comunidades profesionales, foros sectoriales y redes de intercambio de información. Este contacto no debe limitarse a seguir tendencias o modas tecnológicas, sino a mejorar la calidad de las decisiones estratégicas mediante: aprendizaje comparado, análisis de incidentes sectoriales, identificación temprana de amenazas emergentes, y contraste de prácticas de gestión del riesgo.

Cuando el contexto lo requiere, el CISO debe impulsar la participación de la organización en esquemas de cooperación sectorial y en iniciativas público privadas. En escenarios de alto impacto, la resiliencia rara vez es individual: depende de la coordinación entre múltiples actores, de la transparencia informativa y de la capacidad conjunta de respuesta.

Finalmente, la relación con el ecosistema externo exige una actitud de actualización permanente y una lectura crítica del entorno tecnológico, normativo y de amenazas. Integrar esta visión externa en la estrategia y en el modelo de gobierno evita enfoques endogámicos y fortalece la capacidad de anticipación, adaptación y recuperación ante un contexto digital cada vez más interdependiente.

3.7. Relación con el ecosistema interno directivo: CXO, DPD y RSE

El posicionamiento del CISO y su relación con la Alta Dirección se materializan en la interacción diaria con otras funciones ejecutivas. Este apartado adopta un enfoque práctico, centrado en las dinámicas de colaboración, coordinación y tensión que se producen entre el CISO y el resto del equipo directivo.

Figura 15. *Relación entre los bloques funcionales del CISO, su naturaleza y su enfoque principal.*

La Relación Crucial entre el CISO y los CXO

La relación entre el CISO y los ejecutivos de alto nivel, CXO (CEO, CFO, COO, CIO, CMO, CHRO, etc.), debe ser colaborativa, estratégica y transparente. Esta relación influye directamente en la capacidad de la organización para alinear seguridad y negocio.

Una relación sólida permite que:

- La **seguridad esté alineada con los objetivos corporativos:** el CISO comprende el negocio y adapta la estrategia de seguridad para respaldar crecimiento, innovación y continuidad.
- Los **riesgos se comprendan y gestionen adecuadamente**: el CISO comunica riesgos en términos ejecutivos, y los CXO participan activamente en su gestión.
- La seguridad sea una **responsabilidad compartida**, no un asunto exclusivo de TI.
- El CISO disponga del **respaldo necesario** (presupuesto, personal, tecnología) para implantar una estrategia efectiva.
- La organización esté **preparada para responder a incidentes**, con roles claros y coordinación inmediata.

Una relación exitosa se caracteriza por:

- **Comunicación abierta y frecuente.**
- **Confianza mutua** entre el criterio técnico del CISO y el criterio estratégico de los CXO.
- **Respeto profesional:** cada parte comprende las presiones y responsabilidades de la otra.
- **Responsabilidad compartida:** la seguridad recae en toda la organización, no en un departamento.
- **Enfoque estratégico:** la seguridad entendida como inversión y habilitador, no como fricción.

Cómo construir una relación CISO–CXO fuerte. Para consolidar esta relación, la organización debe:

- Fomentar que el CISO **hable en el lenguaje del negocio**: impacto financiero, reputacional, operacional y regulatorio.
- Reforzar el rol **proactivo** del CISO, anticipando riesgos y tendencias, sin esperar a que le consulten.
- Integrar al CISO como **socio estratégico** del Comité de Dirección.
- Implicar activamente a los CXO en decisiones de riesgo y asignación de recursos.
- Promover liderazgo por parte de los CXO en cultura de seguridad.
- Establecer **reuniones periódicas** entre CISO y CXO.
- Utilizar **métricas y KPIs**[7] comprensibles que permitan tomar decisiones informadas.

Una relación madura permite que la organización prospere en un entorno digital complejo, con una visión holística del riesgo.

[7] ISMS Forum 2025. The CISO and Senior Management. ***https://www.ismsforum.es/ficheros/descargas/the-ciso-and-senior-management1765382437.pdf***

La Relación Crucial entre el CISO y el DPD

La relación entre el CISO y el Delegado de Protección de Datos (DPD) es esencial para garantizar tanto la seguridad de la información como el cumplimiento del marco legal en materia de protección de datos. Aunque sus competencias son distintas, ambos roles son complementarios y mantienen áreas de colaboración estructural.

Existen ámbitos de solapamiento que requieren coordinación continua:

- **Seguridad de los datos personales:** el CISO define e implanta los controles técnicos y organizativos que protegen los datos personales, mientras que el DPD verifica su adecuación a los requisitos del RGPD y de la normativa nacional.
- **Gestión de incidentes:** cuando un incidente afecta a la confidencialidad, integridad o disponibilidad de datos personales, se convierte en una brecha de seguridad. En estos casos, CISO y DPD deben coordinarse para minimizar el impacto y cumplir los plazos de notificación.

  No todo incidente de seguridad es una brecha, pero toda brecha que afecte datos personales es un incidente relevante para el RGPD.
- **Evaluaciones de Impacto (EIPD):** el CISO aporta análisis técnicos y medidas de mitigación; el DPD garantiza que el tratamiento y las medidas propuestas cumplen la normativa.
- **Concienciación y formación:** ambos roles participan en programas formativos integrados que abarcan seguridad de la información, privacidad y buenas prácticas del tratamiento de datos.
- **Cumplimiento normativo:** CISO y DPD deben mantenerse alineados en relación con el RGPD, la LOPDyGDD, el ENS, la NIS2 y el resto de marcos aplicables, asegurando coherencia entre seguridad, privacidad y obligaciones legales.

Para que la colaboración sea eficaz, resulta necesario definir roles y responsabilidades de forma clara, establecer canales formales de comunicación entre ambas funciones, celebrar reuniones conjuntas de seguimiento, compartir información sobre incidentes, riesgos y cambios normativos e impulsar una cultura de cooperación y respeto mutuo entre equipos.

Una relación fluida entre CISO y DPD incrementa la capacidad de la organización para proteger datos personales, gestionar riesgos de forma informada y generar confianza entre clientes, empleados y terceros.

¿Puede una misma persona desempeñar como CISO y DPD simultáneamente? Legalmente, no existe una prohibición legal explícita ni un régimen de incompatibilidad en este sentido. Y se trata de funciones cercanas, con áreas de conocimiento y estrategias muy alineadas. La mayor dificultad es esta persona debe desempeñar ambas funciones correctamente, entendiendo cuando debe actuar como CISO, y cuando como DPD. Se requiere que esta persona tenga madurez, ética y gran conocimiento de los requisitos de cada función para que tenga éxito.

En el entorno de las entidades del sector público, frente a las dudas de independencia frente al responsable de sistemas (que es quién determina los medios) y el responsable de la información (normalmente que es quién estipula la finalidad del tratamiento de datos de carácter personal), que puede plantear la nefasta redacción del apartado c del artículo 13 del ENS, en el que se indica que “El responsable de la seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.”, debemos indicar que el RSI será independiente siempre que: su rol se preste sin dependencia del área de sistemas, y sin dependencia de las áreas de negocio y de aquellas otras que toman decisiones de finalidades. Esto es obvio, pero no por ello hay que dejar de citarlo.

En relación con esto último, si la entidad bajo el RD 40/2015 (entidad pública) es además operador esencial, por cumplimiento del artículo 7 del RD 43/2021 (y casi con toda seguridad de este u otro artículo equivalente en la futura transposición de la NIS2) es obligatorio que sea independiente de los responsables de sistemas. En este caso, no debería depender de un área operativo o de “negocio”, para poder evidenciar, si se requiere, ante la AEPD su independencia. Independencia, que se puede reforzar con medidas organizativas, procedimentales y de recursos que demuestren es independencia.

La Relación Estratégica entre el CISO y el Responsable de Responsabilidad Social Corporativa (RSC)

La Ciberseguridad ha dejado de ser únicamente una disciplina técnica orientada a proteger activos. En el contexto actual, su impacto tiene también dimensiones sociales, éticas y reputacionales, que conectan directamente con la Responsabilidad Social Empresarial Corporativa (RSERSC). Por ello, la relación entre el CISO y la RSC se ha vuelto estratégica.

La convergencia entre la seguridad de la información y la RSC se manifiesta en varios aspectos:

- **Privacidad y protección de datos personales:** se han convertido en un valor social y corporativo. Garantizar un tratamiento responsable de los datos forma parte tanto de la estrategia de seguridad como del compromiso de sostenibilidad y ética empresarial.
- **Ética en el uso de tecnologías, especialmente IA:** la adopción de IA introduce riesgos de discriminación, opacidad o uso indebido. La colaboración entre CISO y RSC garantiza políticas responsables en su diseño, entrenamiento y despliegue.
- **Ciberseguridad como contribución al bien social:** la protección de infraestructuras críticas, la lucha contra la desinformación o la promoción de la alfabetización digital son actividades de impacto social donde ambas funciones deben cooperar.
- **Transparencia y rendición de cuentas:** las expectativas de clientes, ciudadanía y reguladores requieren que la organización informe sobre sus prácticas de seguridad y responda adecuadamente ante incidentes.
- **Cadena de suministro responsible:** la seguridad debe extenderse a proveedores y terceros. La RSC y el CISO comparten la necesidad de garantizar prácticas responsables, éticas y sostenibles en toda la cadena.

Una colaboración efectiva entre el CISO y los responsables de la RSC puede generar una serie de beneficios para la organización:

- Mejora reputacional y refuerzo de la confianza del mercado.
- Reducción de riesgos legales, operativos y regulatorios.
- Ventaja competitiva, especialmente en sectores sensibles a ESG.
- Cumplimiento reforzado de normativas de privacidad y seguridad.
- Mayor capacidad de innovación responsable.
- Confianza de stakeholders internos y externos (clientes, empleados, socios, inversores).

Estas sinergias permiten que la organización aborde la seguridad no solo como protección interna, sino como compromiso ético y de responsabilidad social.

Para integrar de forma efectiva seguridad y sostenibilidad, se recomienda:

- Establecer objetivos comunes que conecten seguridad de la información y estrategia ESG.
- Mantener una comunicación fluida y continua entre ambas funciones.
- Promover capacitación cruzada sobre riesgos cibernéticos y responsabilidad social.
- Participar conjuntamente en comités y grupos de trabajo internos.
- Definir políticas y procedimientos que integren tanto criterios de seguridad como principios de RSC.
- Garantizar el apoyo explícito de la Alta Dirección, imprescindible para una visión unificada.

La colaboración entre el CISO y la RSC refuerza la capacidad de la organización para operar de manera ética, segura y sostenible. Comprender que la seguridad de la información es también una responsabilidad social habilita un modelo corporativo más resiliente, confiable y alineado con las expectativas actuales de mercado y sociedad.

La Relación Estratégica entre el CISO y el Responsable de Seguridad y Enlace (RSE)

Como ya hemos indicado la Directiva (UE) 2022/2557 de Resiliencia de Entidades Críticas (CER) establece un marco obligatorio para proteger infraestructuras físicas esenciales y también como hemos indicado a la hora de escribir este libro blanco aún no se ha aprobada la transposición de dicha directiva, por lo que para tratar la relación entre el RSE y el RSI deberemos ir a la actual transposición de la anterior directiva.

También como hemos dicho, el rol de RSE del operador crítico está en la transposición, mientras que la designación por el operador de su RSI es consecuencia de una circular de la secretaria de estado de interior.

El Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) que es la autoridad de control para la L 8/2011 (la transposición de la que estamos tratando), la figura del RSI es una figura que estando especializado en Ciberseguridad debe coordinarse obligatoriamente con el RSE, siendo este último el enlace con el CNPIC y figura recogida en la Ley.

Por lo tanto, cuando se produce un ciberincidente en un sistema de una infraestructura que ha sido designado como tal por el Ministerio del Interior (a través de la secretaria de estado del interior) es el RSI el que informa al CNPIC, pero debe “poner en copia” al RSE en todas las comunicaciones.

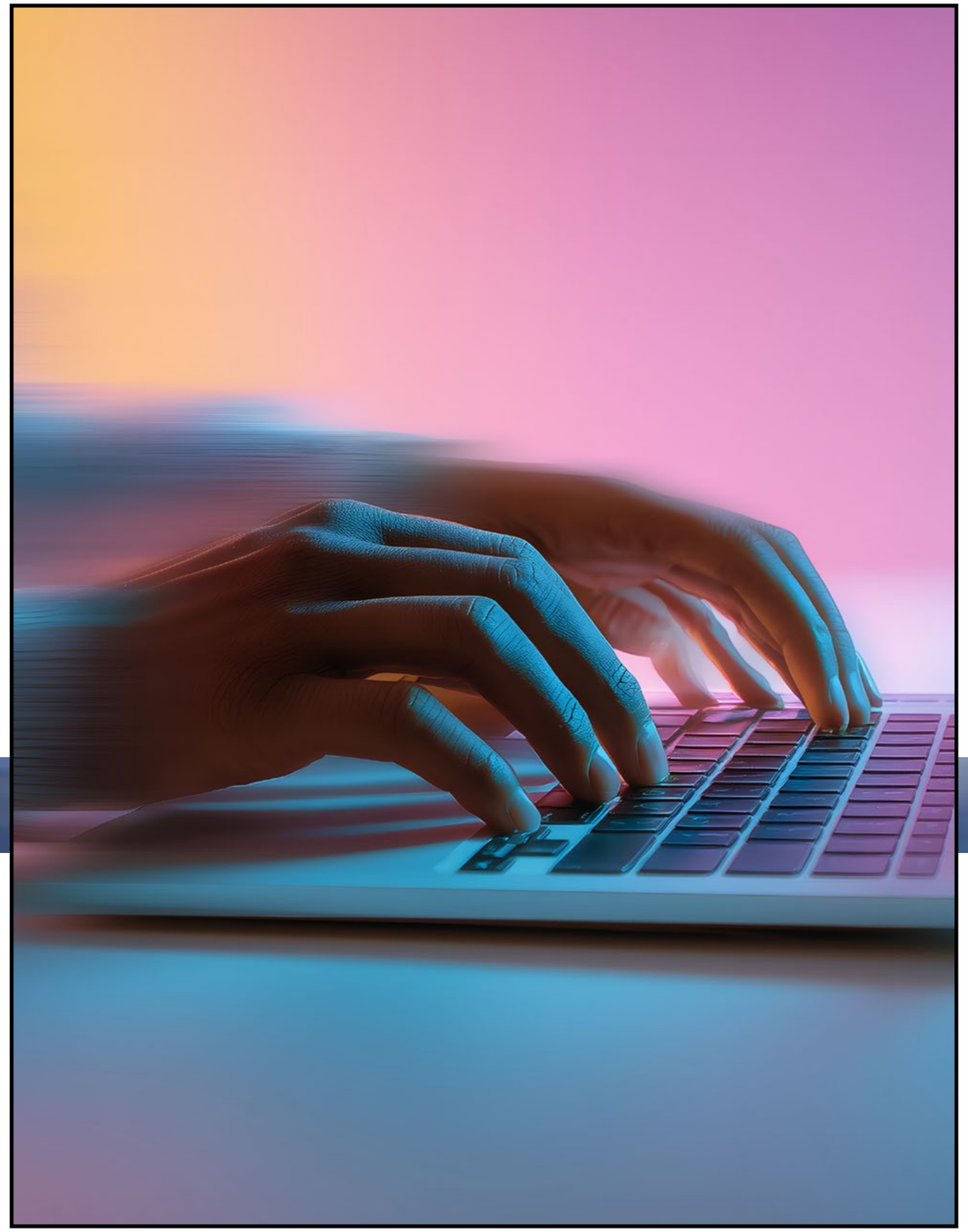
Por su parte el CNPIC trasladará sus mensajes e instrucciones a través del RSE.

De facto, para el CNPIC la figura del RSI es una figura subordinada al RSE en lo que a este centro respecta. Dicho lo cual, el CNPIC no manifiesta una dependencia jerárquica del RSI del RSE, sí que estén en un área orgánica común; es decir, como no puede ser de otra forma, da libertad a las empresas operadoras para que se organicen como mejor evalúe para sus fines.

A la pregunta ¿puede ser un RSI también RSE? La respuesta es que sí, siempre que esté habilitado por el Ministerio del interior como Director de Seguridad (privada).

4.

Modelos



4.1. Organización de la práctica. Modelos habituales de organización

/ Principios Fundamentales de la Gobernanza de la Seguridad

La gobernanza de la seguridad tiene como principal objetivo la composición del modelo de gestión más adecuado de los ciberriesgos, de acuerdo con los requisitos y apetito al riesgo establecidos por los principales Grupos de Interés de la organización y de acuerdo tanto al marco normativo vigente como alineado con los principales estándares de seguridad.

En el Capítulo 3 se ha explicado cómo el posicionamiento organizativo influye en la función del CISO. En este capítulo, se profundiza en modelos concretos de organización y se analizan sus ventajas, inconvenientes y condiciones de gobernanza.

Estos principios constituyen la base para un desempeño sólido de la función:

Autonomía e Independencia

El CISO debe disponer de independencia funcional respecto a áreas operativas y tecnológicas, minimizando conflictos de interés. Su autoridad debe implicar capacidad de decisión, acceso a la Alta Dirección y recursos suficientes.

Responsabilidad

La ejecución de la estrategia de Seguridad debe estar asignada formalmente al CISO, quien podrá delegar ámbitos específicos en otros actores. La asignación de funciones debe ser clara y conocida por todas las partes involucradas.

Transparencia y reporte

Deben existir mecanismos de reporte claros y periódicos que permitan conocer el estado real de los ciberriesgos y comunicar cualquier variación relevante en la exposición de la organización.

Resiliencia

La gestión de los ciberriesgos debe ir más allá de la prevención. Debe contemplar la continuidad de funciones críticas y la recuperación frente a eventos adversos, asegurando la resiliencia operativa del negocio.

La dependencia organizativa del CISO influye directamente en su capacidad, alcance y relevancia, así como en la calidad de sus relaciones con otros ejecutivos. Su ubicación depende del marco regulatorio, sector, tamaño y cultura de la organización.

A continuación, se presentan los modelos organizativos más habituales.

Modelo 1

CISO Dependiente del CEO (u órgano ejecutivo de primer nivel)

Descripción: el CISO depende jerárquicamente del órgano ejecutivo de primer nivel o del CEO de la organización.

Ventajas:

- → Máxima visibilidad en la organización.
- → Mejora la relación con la alta dirección.
- → Facilita el alineamiento con los objetivos mejorando la agilidad en la toma de decisiones estratégicas.
- → Maximiza sus funciones de asesoría y supervisión.
- → Desarrolla al máximo su dimensión directiva.

Inconvenientes:

- → Dificultades de la visibilidad y coordinación con actividades de primera línea de defensa (de seguridad).
- → Mayor necesidad de dimensionamiento en recursos para un adecuado desarrollo de funciones de forma transversal a la organización.
- → Requiere de órganos o mecanismos de coordinación específicos con áreas de riesgo y auditoría.

Modelo 2

CISO Autónomo Reportando al Consejo

Descripción: el CISO tiene dependencia funcional directa del Consejo de Administración o de una Comisión especializada (Auditoría, Riesgos). Generalmente la dependencia jerárquica del CISO suele estar bajo una figura de alta dirección sin capacidades ejecutivas directas (Consejero Delegado o Presidente)

Ventajas:

- → Independencia y autonomía completa respecto al resto de áreas.
- → Refuerza la gobernanza y la transparencia.

Inconvenientes:

- → Requiere alta madurez organizativa para garantizar el correcto desempeño de funciones.
- → Mayor riesgo de conflicto con áreas de riesgo y auditoría.
- → Dificultades de la visibilidad y coordinación con actividades de primera línea de defensa (de seguridad) y con las áreas de seguridad.
- → Mayor necesidad de dimensionamiento en recursos para un adecuado desarrollo de funciones de forma transversal a la organización.

Modelo 3

CISO dependiente del CRO (Chief Risk Officer)

Descripción: El CISO depende del CRO y participa en el Comité de Riesgos.

Ventajas:

- → Aseguramiento de la gestión de los ciberriesgos dentro de la organización.
- → Alineación con la gestión global de riesgos corporativos, facilitando la integración de la Ciberseguridad en el mapa de riesgos global de la organización.

Inconvenientes:

- → Excesivo encasillamiento en funciones de segunda línea de defensa con pérdida de control y de dependencia de la primera línea.
- → Posible subordinación excesiva a principales riesgos a los que se encuentre expuesta la organización (financieros, operativosetc.).
- → Perdida de visibilidad con el despliegue de las iniciativas de negocio y con los procesos tecnológicos.

Modelo 4

CISO Dependiente del CIO

Descripción: El CISO se ubica bajo la Dirección de Tecnología (CIO), formando parte del área de TI.

Ventajas:

- → Mejora de la integración con los equipos técnicos y operativos de tecnología.
- → Facilita la implementación de medidas de seguridad en aplicaciones, sistemas y redes.
- → Un modelo de relación bien definido garantiza el desarrollo de funciones completas y alineadas de actividades de primera línea de defensa en el ámbito tecnológico.

Inconvenientes:

- → Riesgo de conflictos de interés y de pérdida de independencia, respecto de la seguridad frente a la disponibilidad y funcionalidad de sistemas.
- → Limita el adecuado reporte de la función de seguridad ante los órganos de dirección y del Consejo.
- → Favorece un encapsulamiento de la seguridad en tecnología que dificulta la visibilidad de otros procesos de negoción y de gestión interna (gestión de personas, financiero, etc.).
- → Posibles conflictos con regulaciones.

4.2. Beneficios y dificultades en la segregación de funciones dentro de la práctica

La segregación de funciones (Segregation of Duties, SoD) es un control estructural esencial para prevenir fraude, errores y abuso de privilegios. Consiste en dividir tareas sensibles para evitar que una sola persona controle un proceso completo. Para el CISO representa una herramienta clave de seguridad y resiliencia, pero también un reto operativo.

Esta práctica aporta una serie de beneficios y dificultades, entre los que caben destacar los siguientes:

Beneficios

- Reducción del riesgo operativo y de fraude: evita concentraciones de funciones críticas.
- Mayor trazabilidad y control: roles delimitados facilitan auditoría y supervisión.
- Aumento de la resiliencia: errores o incidentes se detectan antes de propagarse.
- Cumplimiento normativo: la segregación es un requisito transversal en marcos regulatorios y estándares de madurez.

Dificultades

- Equipos reducidos: falta de capacidad obliga a concentrar funciones o externalizar.
- Resistencia cultural: puede percibirse como burocracia o fricción operativa.
- Ambigüedad de roles: sin procedimientos claros, las fronteras se difuminan.
- Falta de documentación: dificulta la aplicación real y consistente.
- Dependencia de proveedores externos: obliga a verificar su propia segregación interna.

4.3. SOC y CSIRT: dos funciones complementarias con distinta naturaleza

En la evolución de la Ciberseguridad organizativa, la aparición del SOC y, posteriormente, del CSIRT, no responde a una cuestión nominal, sino a un proceso de maduración en la forma de entender la operación y la gestión del incidente. No todas las organizaciones cuentan con ambas capacidades diferenciadas, y la forma en que distribuyen responsabilidades es un indicador claro de su modelo de gobierno y de su nivel de especialización.

En el enfoque que aquí se defiende, el SOC y el CSIRT no se solapan: desempeñan funciones distintas, con responsabilidades diferenciadas y con una lógica de segregación funcional que refuerza la trazabilidad y la calidad de la respuesta.

Cuando estas funciones se externalizan, es posible encontrar que ambos servicios se ofrecen de manera conjunta por el proveedor.

Security Operations Center (SOC)

El SOC constituye la función encargada de la operación técnica continua de la arquitectura de seguridad. Su misión es garantizar que los mecanismos de protección, detección y respuesta técnica estén desplegados, correctamente configurados y operativos en todo momento.

El SOC administra y mantiene las herramientas de seguridad, ejecuta medidas de contención técnica, aplica cambios en configuraciones, participa en tareas de endurecimiento y recuperación de sistemas, y asegura la disponibilidad de la infraestructura defensiva.

Muchas organizaciones no cuentan con un SOC formal 24/7, pero sí con equipos que realizan funciones equivalentes. El SOC puede abarcar tareas heterogéneas cuando no existe CSIRT diferenciado, mezclando operación y dirección del incidente.

En modelos más maduros, el SOC no dirige incidentes: ejecuta acciones técnicas siguiendo la estrategia definida por otro nivel de responsabilidad.

Computer Security Incident Response Team (CSIRT)

El CSIRT representa un estadio superior de especialización. Su creación implica reconocer que la detección y la operación técnica no son equivalentes a la gestión estructurada de un incidente.

En este modelo, el CSIRT asume la responsabilidad del SIEM y de la correlación de eventos, lo que sitúa la capacidad analítica bajo el equipo que dirige el ciclo del incidente. La interpretación de eventos, el triage, la confirmación formal de incidente y la definición de la estrategia de contención y erradicación son competencias propias del CSIRT.

El CSIRT:

- Analiza y correlaciona eventos.
- Determina si un evento constituye un incidente.
- Evalúa impacto y criticidad.
- Define la estrategia de respuesta.
- Coordina a las áreas implicadas.
- Supervisa que el SOC ejecute las medidas técnicas.
- Lidera el análisis posterior y la extracción de lecciones aprendidas.

Mientras el SOC actúa sobre la infraestructura, el CSIRT actúa sobre el incidente como evento de riesgo corporativo.

La existencia de un CSIRT diferenciado es un indicador de madurez y de una clara separación entre operación y supervisión. Evita conflictos de interés y fortalece la resiliencia organizativa, permitiendo que la respuesta sea técnica, estructurada y orientada a la no repetición, no solo a la recuperación rápida.

5.

Retos actuales y emergentes

El rol del CISO evoluciona en un entorno marcado por la aceleración tecnológica, la sofisticación de los adversarios y una creciente presión regulatoria. Estos factores configuran un panorama de riesgo dinámico y transversal. Para gestionarlo con eficacia, el CISO debe anticiparse, priorizar y orientar decisiones basadas en impacto y resiliencia.

Este capítulo sintetiza los principales retos actuales y emergentes que condicionan el gobierno del riesgo digital, con un enfoque pragmático y orientado a la toma de decisiones directivas.

5.1. Gestión del riesgo en entornos complejos

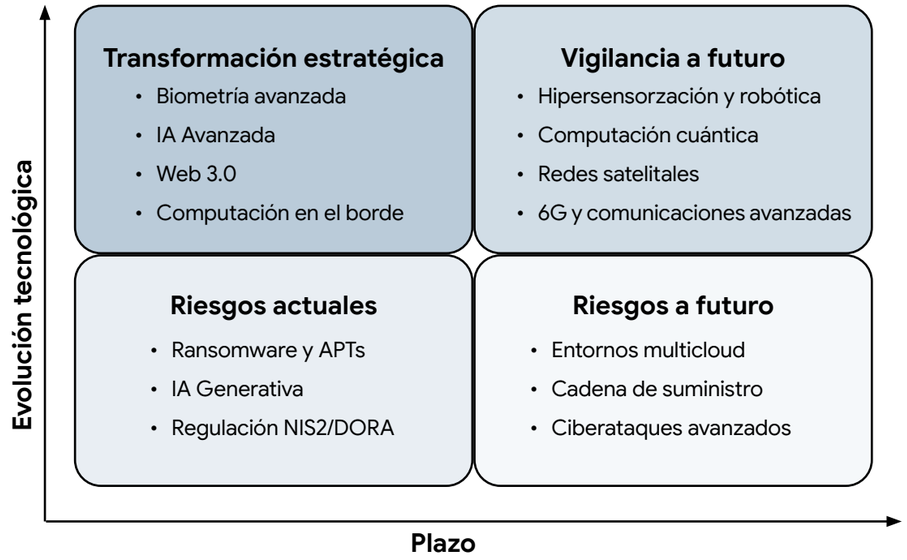
El panorama tecnológico ha cambiado de forma significativa desde la edición anterior de este Libro Blanco. Los entornos actuales son más complejos, tanto por los avances derivados de la innovación -que han dado lugar a nuevos productos y paradigmas en la última década- como por la evolución en las capacidades y tácticas de los adversarios.

Este cambio no ha pasado desapercibido para los reguladores. Si antes el CISO se enfrentaba a un escenario con pocas palancas de acción, hoy la regulación ofrece mecanismos que fortalecen la gestión del riesgo desde el inicio del proceso. Esto permite al CISO responder preguntas clave: ¿qué debe proteger? o ¿qué motiva a los adversarios?

El CISO debe contrastar los controles y salvaguardas existentes, así como con la disponibilidad y el talento interno y externo (el de la cadena de suministro) para garantizar la protección y resiliencia de los activos digitales a través de la adecuada gestión del riesgo.

5.2. Innovación y aceleración tecnológica

La velocidad con la que emergen nuevas tecnologías supera la capacidad tradicional de evaluación y despliegue. El CISO debe incorporar criterios de impacto, madurez y riesgo para decidir **cuándo adoptar, cuándo vigilar y cuándo contener.** A continuación, se presenta una visión sintética en forma de cuadrante estratégico que resume el nivel de disrupción y su horizonte temporal.



Ejemplos representativos de esta aceleración tecnológica incluyen:

- **Cloud y multicloud:** su adopción global se ha consolidado tras casi dos décadas de maduración, convirtiéndose en un estándar operativo generalizado que exige al CISO gestionar entornos híbridos, dependencias críticas y configuraciones complejas. El informe The State of Cloud and AI Security 2025[8], revela que el 63 % de las organizaciones utilizan más de un proveedor de nube, lo que confirma que la arquitectura multicloud se ha consolidado como práctica habitual.
- **IA generativa:** en apenas tres años desde su despliegue masivo, ha transformado la producción de contenido, la automatización y el comportamiento de usuarios y atacantes, obligando al CISO a gobernar riesgos de uso indebido, fuga de datos y exposición en “Shadow AI”.
- **Protocolo MCP (Model Context Protocol):** un estándar reciente que permite a modelos de IA conectarse con herramientas y servicios externos, y cuya rápida evolución introduce nuevos riesgos de integración y orquestación que deben evaluarse antes de su adopción en entornos corporativos.
- **Starlink y comunicaciones satelitales masivas:** la transición de un uso corporativo a uno global crea dependencias críticas de un proveedor único, planteando retos en resiliencia, continuidad de servicio y exposición ante fallos o vulnerabilidades en la infraestructura orbital.
- **Computación cuántica:** un paradig ma emergente con potencial disruptivo para la criptografía actual; su avance obliga al CISO a planificar una transición ordenada hacia mecanismos resistentes a ataques cuánticos y a evaluar riesgos sobre la confidencialidad a largo plazo.

En conjunto, la rapidez con la que se introducen estas tecnologías, sumada a la falta de talento especializado y la inmadurez de algunas soluciones, obliga al CISO a **implantar medidas iniciales, monitorizarlas estrechamente y reevaluarlas en ciclos cortos**, manteniendo una capacidad de adaptación continua y basada en criterios de impacto y proporcionalidad.

[8] Cloud Security Alliance. (2025). The State of Cloud and AI Security 2025. ***https://cloudsecurityalliance.org/artifacts/the-state-of-cloud-and-ai-security-2025***

5.3. Evolución de los adversarios

El perfil de los adversarios ha evolucionado hacia una mayor profesionalización, especialización y escala, lo que obliga al CISO a comprender quién tiene capacidad real para comprometer su organización y con qué motivaciones.

Los principales actores son:

- **Amenazas persistentes avanzadas (APT):** grupos vinculados a Estados con financiación estable, capacidades técnicas avanzadas y objetivos estratégicos (espionaje, sabotaje, obtención de información crítica). No actúan solo contra gobiernos: también atacan empresas para obtener ventaja económica, geopolítica o industrial.
- **Crimen organizado:** constituye hoy el vector más rentable y extendido. Opera con estructuras empresariales, especialización de funciones y modelos "as-a-service", facilitando ataques complejos incluso a actores con bajo nivel técnico. Su carácter transnacional dificulta la atribución y la respuesta.
- **Hacktivismo:** actores motivados ideológica o socialmente que buscan impacto reputacional mediante campañas de denegación de servicio, desfiguración web o filtraciones. Su imprevisibilidad obliga a reforzar comunicación, gestión reputacional y continuidad operativa.
- **Ciberterrorismo:** orientado a la interrupción de servicios críticos y a la erosión de la confianza pública, combinando capacidades cibernéticas con potenciales acciones físicas. Requiere coordinación con autoridades y planes específicos de contingencia.
- **Amenaza interna:** empleados, ex empleados o colaboradores con acceso legítimo que pueden actuar por interés personal, negligencia o en coordinación con actores externos. Representan uno de los vectores más críticos por su conocimiento interno y la dificultad de detección.

En conjunto, esta evolución demanda capacidades maduras en inteligencia de amenazas, monitorización, respuesta y resiliencia, así como una visión estratégica que permita anticipar comportamientos, motivaciones y técnicas de ataque.

5.4. Cadena de suministro

La digitalización y la externalización han ampliado el perímetro de riesgo. El CISO debe considerar:

- Dependencias críticas y proveedores estratégicos.
- Riesgos derivados de subprocesos, integradores y terceros.
- Obligaciones regulatorias en NIS2, ENS, DORA y RGPD.
- Evaluaciones continuas ante cambios en servicios y subcontrataciones.

La madurez en la gestión del riesgo de terceros es hoy un factor diferencial de resiliencia; ningún incidente en un proveedor es "externo" si impacta la continuidad operativa de la organización.

6.

Responsabilidad jurídica

Este modelo normativo no exige la inexistencia de incidentes, sino la capacidad de demostrar que el riesgo ha sido identificado, evaluado y gestionado de forma razonable y proporcionada. La ausencia de gobierno efectivo del riesgo digital, la falta de supervisión o la adopción de medidas meramente formales pueden interpretarse como déficits de diligencia, con efectos en los ámbitos administrativo, civil y, en determinados supuestos, penal.

La existencia de un marco de seguridad coherente, la integración del riesgo digital en los procesos de decisión, la supervisión del riesgo de terceros y la preparación para la gestión de incidentes constituyen elementos fundamentales para demostrar que la organización ha actuado con criterio y responsabilidad frente a riesgos conocidos y previsibles.

La gestión de incidentes y crisis adquiere aquí una relevancia particular. La forma en que se evalúan los impactos, se priorizan los servicios, se toman decisiones bajo presión y se documentan las actuaciones influye de manera directa en la valoración jurídica posterior.

En definitiva, el marco regulatorio actual refuerza la necesidad de tratar la Ciberseguridad como una obligación de gestión integrada en el gobierno corporativo y en la operación diaria. El CISO no asume la responsabilidad última, que corresponde a la dirección, pero se configura como una figura imprescindible para que esa responsabilidad pueda ejercerse de manera informada, estructurada y defendible.

6.1. Responsabilidad jurídica y diligencia debida en materia de Ciberseguridad

6.2. Régimen de responsabilidades legales del CISO

La evolución del rol del CISO ha traído consigo un incremento progresivo de la exposición a distintos tipos de responsabilidad legal. Cuando los incidentes digitales generan impactos económicos, operativos o reputacionales relevantes, surge inevitablemente la pregunta sobre quién debía haber previsto, evitado o mitigado ese impacto.

En este contexto, resulta esencial distinguir entre responsabilidad de la organización y responsabilidad personal del CISO. La responsabilidad última frente a terceros, autoridades y personas afectadas corresponde normalmente a la entidad, sin que del CISO se pudiera derivar una responsabilidad penal directa, salvo en casos de fraude o comisión de delitos en el marco de su función.

/ Responsabilidad civil: diligencia profesional y daño

La responsabilidad civil es, en la práctica, el ámbito donde el CISO presenta una mayor exposición potencial.

En el caso del CISO, esta diligencia se evalúa principalmente en tres planos. En primer lugar, en la capacidad de identificar y comunicar riesgos relevantes. En segundo lugar, en la supervisión del marco de control. Y, en tercer lugar, en la diligencia en la gestión del incidente.

Es importante subrayar que la responsabilidad civil del CISO no se basa en el resultado, sino en el proceso. Haber actuado con criterio, haber documentado decisiones y haber elevado los riesgos de forma adecuada constituye la principal protección frente a este tipo de reclamaciones, que, por otra parte, aunque no son frecuentes, sí aumenta su incidencia respecto a años anteriores.

/ Responsabilidad penal: un escenario excepcional

La responsabilidad penal del CISO constituye un escenario excepcional y debe analizarse con cautela. El ordenamiento jurídico no atribuye responsabilidad penal por el mero incumplimiento de obligaciones de seguridad ni por la ocurrencia de incidentes de Ciberseguridad. Para que exista responsabilidad penal es necesario acreditar una conducta dolosa o, en determinados supuestos, una negligencia grave con relevancia penal.

En la práctica, esto implica que el CISO solo podría verse expuesto penalmente en situaciones muy concretas, como la ocultación consciente de información relevante, la manipulación deliberada de evidencias, la colaboración activa en conductas ilícitas o la desatención grave y reiterada de obligaciones esenciales cuando ello genere daños especialmente relevantes.

El riesgo penal no deriva, por tanto, de una mala decisión técnica o de una arquitectura imperfecta, sino de comportamientos que se sitúan fuera del ejercicio razonable de la función, más cercanos al fraude o conductas dolosas.

/ La importancia de la cobertura aseguradora

La creciente exposición del CISO a reclamaciones civiles y a investigaciones posteriores a incidentes ha puesto de relieve la importancia de contar con una cobertura aseguradora adecuada.

Existen pólizas de responsabilidad civil profesional y, especialmente, los seguros de administradores y directivos (D&O), desempeñan un papel fundamental en este contexto. Estas coberturas no protegen frente a conductas dolosas, pero sí frente a reclamaciones derivadas de supuestos errores, omisiones o negligencias en el ejercicio de la función.

Para el CISO, resulta especialmente relevante analizar si se encuentra incluido de forma expresa en la cobertura D&O de la organización o si, su rol, queda en una zona gris entre lo técnico y lo directivo. En muchas organizaciones, el CISO asume responsabilidades estratégicas y de gobernanza de la gestión del riesgo tecnológico, sin que su posición esté claramente reflejada en este tipo de pólizas.

Una cobertura adecuada debe contemplar, entre otros aspectos, los costes de defensa jurídica, las posibles indemnizaciones derivadas de reclamaciones civiles y la protección frente a acciones de terceros. La ausencia de esta cobertura no sólo incrementa el riesgo personal del CISO, sino que puede dificultar la toma de decisiones en situaciones de crisis.

/ Alineación entre responsabilidad y autoridad

Uno de los factores que más incrementa la exposición del CISO a responsabilidades legales es la falta de alineación entre las funciones que se le atribuyen y la autoridad real de la que dispone. Asumir responsabilidades sin capacidad de decisión, sin acceso a la dirección o sin recursos adecuados genera una situación de riesgo estructural.

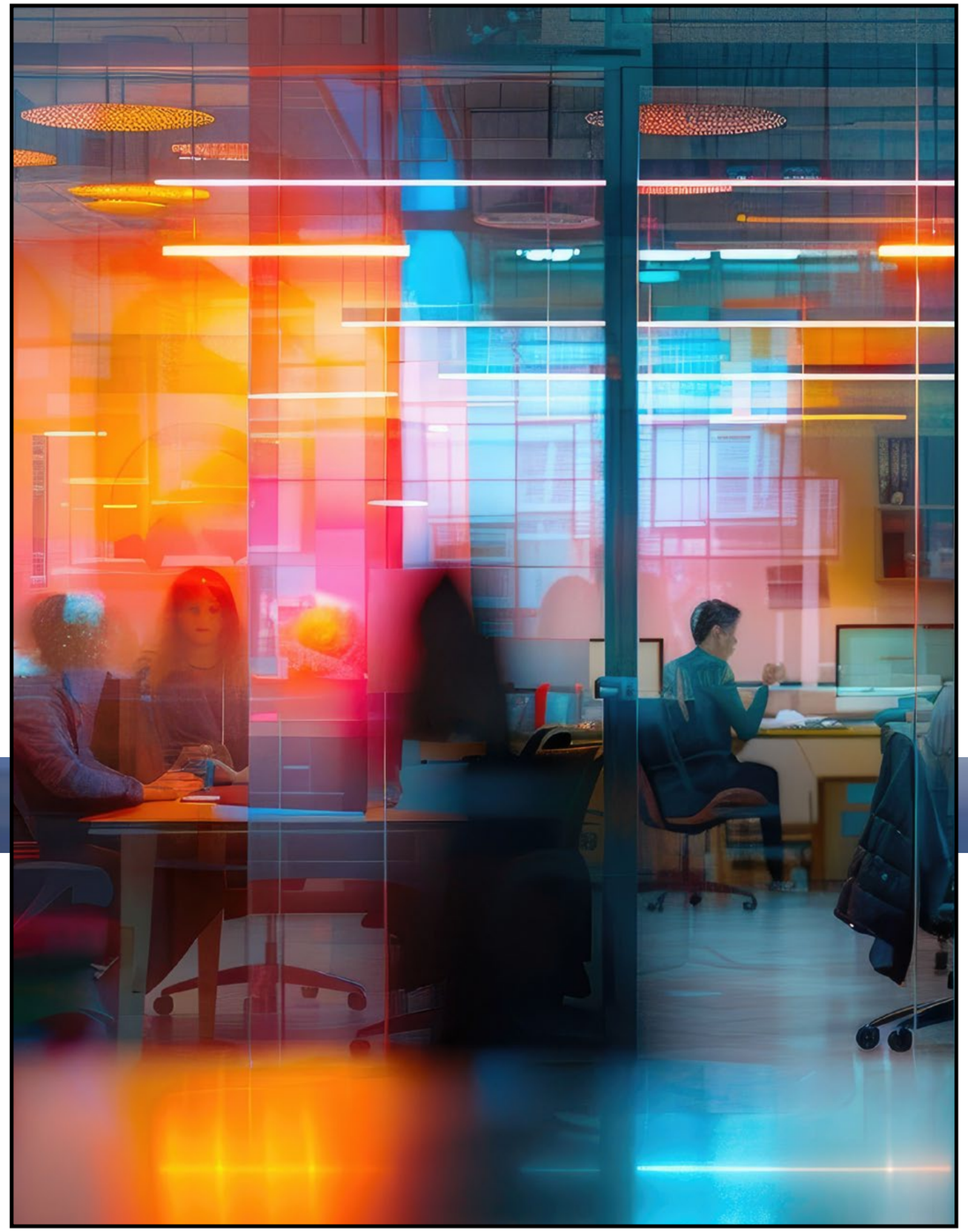
En caso de incidente, la evaluación se centra en quién debía haber actuado, con qué información y con qué capacidad. Cuando el rol no está claramente definido, el riesgo de conflictos de responsabilidad aumenta de forma significativa.

Por ello, resulta esencial que la organización defina de manera explícita el alcance del rol del CISO, su capacidad de escalado y su integración en los mecanismos de decisión. Esta claridad no solo mejora la eficacia de la Ciberseguridad, sino que protege jurídicamente a todas las partes implicadas.

La aparición de normas como NIS2 que explicitan una responsabilidad directa en la alta Dirección animan aún más a definir lo mejor posible el modelo de gobernanza interna, el rol del CISO, sus capacidades de reportar y de tomar decisiones.

7.

Gestión del talento y liderazgo



7.1. Formación

El CISO del siglo XXI debe ser un profesional polivalente, en aprendizaje continuo y con una sólida base tanto técnica como de negocio. La evolución acelerada de las amenazas y la transformación digital exigen que su formación incluya conocimientos especializados en Ciberseguridad, gestión empresarial, riesgos y cumplimiento normativo, sin descuidar el desarrollo de habilidades directivas y soft skills para liderar con eficacia. Se describen a continuación los pilares formativos y competenciales que hoy definen el perfil del CISO.

Formación académica y técnica

Históricamente, muchos CISOs han partido de carreras de Tecnologías de la Información (Informática, Telecomunicaciones, Seguridad de la Información). Sin embargo, el rol ha dejado de ser exclusivamente técnico para centrarse en el negocio y en la gestión del riesgo, por lo que resulta clave complementar esa base técnica con conocimientos de empresa. Una causa frecuente de fracaso en el puesto es no comprender las expectativas del negocio y la priorización que impone la estrategia corporativa. Por ello, cada vez es más frecuente encontrar perfiles híbridos (por ejemplo, ingenieros con MBA, o formación en gobierno corporativo/gestión de riesgos) y valor creciente de la experiencia o estudios en Derecho (privacidad y cumplimiento), dada la expansión regulatoria en Ciberseguridad.

Es recomendable consolidar una base académica en seguridad de la información (másteres en gobierno de la ciberseguridad, gestión de riesgos o seguridad informática). En cuanto a la formación técnica continua, disciplinas como arquitectura de seguridad, respuesta a incidentes, inteligencia de amenazas, seguridad en la nube o DevSecOps resultan críticas; y emergen ámbitos como IA aplicada a la seguridad y computación cuántica (preparación post quantum). El inglés es prácticamente imprescindible por el carácter global del sector (publicaciones, foros, estándares y eventos).

En España, cuando el CISO asume también funciones de Dirección de Seguridad Física, puede resultar pertinente la habilitación de Director de Seguridad conforme a la Ley 5/2014 de Seguridad Privada. Esta cualificación aporta una visión integral (física y lógica) y favorece la coordinación de la protección corporativa cuando ambas dimensiones convergen.

La participación en ejercicios prácticos es un elemento clave del aprendizaje continuo: ciberejercicios, simulaciones de ataques y crisis, red teaming, simulaciones de ransomware o pruebas de respuesta a brechas ayudan a detectar carencias técnicas y organizativas y a acelerar el time to respond real.

Finalmente, la formación no se limita a cursos formales. La asistencia a congresos (INCIBE, CCN, ENISA, RSA Conference, etc.), la participación en comunidades profesionales (ISMS Forum, ISC², ISACA, FIRST, entre otras) y el intercambio entre pares son catalizadores para mantenerse al día en tendencias, mejores prácticas y tecnologías emergentes.

Certificaciones profesionales y aprendizaje continuo

Las certificaciones aportan credenciales y confianza ante la Alta Dirección y terceros, y ayudan a estructurar la evolución competencial del CISO.

Actualmente, las certificaciones de gestión y gobierno de la seguridad son las más demandadas para un CISO, reflejando el carácter cada vez más estratégico del rol. En la siguiente tabla se resumen algunas certificaciones destacadas y su enfoque principal:

Certificación	Organismo emisor	Enfoque principal	Ciberseguridad	Privacidad/ Datos	Cibercompliance /GRC
CISM	ISACA	Gestión de la seguridad de la información y gobierno	✓		✓
CISSP	ISC2	Seguridad de la información integral (técnico + gestión)	✓		✓
CCSP	ISMS Forum	Gobierno de la ciberseguridad (enfoque práctico)	✓		
CISA	ISACA	Auditoría de sistemas de información y control interno			✓
CRISC	ISACA	Gestión de riesgos tecnológicos y controles de SI			✓
CGRC	ISC2	GRC en ciberseguridad			✓
CPCC	ISMS Forum	Adecuación al compliance tecnológico			✓
NIS2PC	ISMS Forum	Cumplimiento NIS2			✓
CGEIT	ISACA	Gobierno corporativo de TI			✓
CC	ISC2	Fundamentos de ciberseguridad (nivel inicial)	✓		
SSCP	ISC2	Seguridad operacional y técnica	✓		
OSCP	Offensive Security	Pentesting (pruebas de penetración)	✓		
CEH	EC-Council	Ethical hacking (hacking ético)	✓		

Figura 17. *Certificaciones relevantes para la función de CISO.*

Existen muchas otras certificaciones especializadas, por ejemplo, las de SANS/GIAC en seguridad ofensiva y forense, OSCP en pentesting, certificaciones de fabricantes en redes y nube, etc., que pueden ser valiosas según las necesidades de la organización).

Certificación	Organismo emisor	Enfoque principal	Ciberseguridad	Privacidad/ Datos	Cibercompliance /GRC	Cloud	IA
CDPP/CDPD	ISMS Forum / AEPD	Privacidad y protección de datos personales		✓	✓		
CCSK	CSA	Conceptos de seguridad en cloud computing				✓	
CCSP	ISC2	Seguridad avanzada en entornos cloud				✓	
CCGP	ISMS Forum	Gobierno y gestión de ciberseguridad en cloud				✓	
AIGP	IAPP	Gobierno y cumplimiento en IA			✓		✓
AAISM	ISACA	Auditoría avanzada en IA			✓		✓
CAIP	ISMS Forum	Ciberseguridad, privacidad y buenas prácticas en IA	✓	✓			✓
TAISE	CSA	Seguridad, gobierno y protección en IA			✓		✓
CAISP	Practical DevSecOps	Exploración de riesgos en la cadena de suministro de IA	✓				✓
CIPM	IAPP	Gestión de programas de privacidad		✓	✓		
CIPP	IAPP	Legislación y cumplimiento en privacidad		✓	✓		
CIPT	IAPP	Tecnologías de privacidad		✓			
PLS	IAPP	Transferencias internacionales y privacidad		✓	✓		
CDPSE	ISACA	Ingeniería de privacidad		✓	✓		

Figura 18. *Certificaciones complementarias y especializadas para el desarrollo avanzado del CISO*

No obstante, el valor de las certificaciones no radica solo en el título, sino en el proceso de aprendizaje continuo que implican. Un buen CISO aprovecha las certificaciones para estructurar su formación a lo largo de la carrera, manteniéndolas actualizadas mediante la obtención de créditos profesionales (CPEs) y, sobre todo, aplicando ese conocimiento en situaciones reales. Además, más allá de las certificaciones formales, los fabricantes ofrecen capacitaciones en tecnologías específicas (por ejemplo, seguridad en la nube, herramientas de monitorización, etc.) que el CISO y su equipo deben seguir de cerca para estar al día en soluciones punteras.

En resumen, la formación de un CISO nunca termina realmente. La Ciberseguridad es un dominio dinámico, en el que surgen constantemente nuevas amenazas, estándares (por ejemplo, nuevas versiones de ISO 27001, marco NIST CSF actualizado) y normativas (NIS2, DORA, etc.). Por ello, el CISO ha de mantener una mentalidad de estudiante permanente, combinando estudios formales, certificaciones y autoaprendizaje. La inversión en conocimiento es, en última instancia, una de las herramientas más poderosas para que el CISO pueda anticipar riesgos emergentes y proteger eficazmente la organización.

Desarrollo de capacidades directivas y soft skills

Además de la formación técnica, un CISO exitoso debe desarrollar un conjunto de habilidades directivas y sociales que resultan críticas para liderar en un entorno complejo. En el pasado, la función de seguridad se concebía de modo más operativo, pero hoy el CISO es un directivo con influencia transversal, cuyo desempeño depende tanto de qué sabe cómo de cómo lo aplica y comunica. De hecho, las llamadas soft skills se señalan a menudo como la mayor carencia en los equipos de Ciberseguridad actuales. A continuación, se describen las competencias clave que un CISO debe cultivar y cómo puede hacerlo.

Visión estratégica del negocio y seniority:

El CISO maneja un grado de responsabilidad muy alto –sus decisiones impactan la estrategia, las inversiones, la continuidad operativa e incluso la reputación de la empresa–, por lo que necesita una profunda comprensión del core business. Debe saber identificar cómo la pérdida de confidencialidad, integridad o disponibilidad de la información puede afectar a cada proceso de negocio, cuantificar riesgos en términos económicos y priorizar controles acordemente. Esta mezcla de experiencia y criterio se adquiere combinando años de trabajo (learning by doing) con formación en gestión empresarial. Muchos CISOs amplían sus conocimientos en áreas como finanzas, gestión de proyectos o análisis de riesgos mediante cursos ejecutivos. También es valioso contar con mentores (por ejemplo, un CFO o COO que guíe al CISO en comprensión de negocio) para acelerar esa madurez directiva. La experiencia profesional variada –no solo en seguridad, sino quizás pasando por roles en TI, riesgo o consultoría– contribuye igualmente a dotar al CISO de perspectiva global.

Liderazgo y gestión de equipos:

Lejos quedó el estereotipo del experto técnico aislado; el CISO moderno lidera equipos humanos multidisciplinares. Para ello, debe desarrollar dotes de liderazgo que inspiren confianza y compromiso en su equipo de seguridad y en otros miembros de la organización. Esto implica capacidades de organización y priorización, para orientar al equipo a las metas correctas, y de delegación, pues un CISO no puede (ni debe) hacerlo todo personalmente. Un buen CISO actúa más como director de orquesta que como solista: no necesita saber tocar cada instrumento, pero sí coordinar a los especialistas para ejecutar la partitura común. Para mejorar estas habilidades, muchos profesionales realizan cursos de liderazgo, coaching ejecutivo o gestión de equipos de alto rendimiento. También la práctica diaria -dirigir reuniones, resolver conflictos, evaluar y coachear a subordinados- va puliendo su estilo de liderazgo. En organizaciones grandes, el CISO puede apoyarse en mandos intermedios (por ejemplo, jefes de área de seguridad) pero aun así debe marcar la pauta y fomentar una cultura de equipo sólida, distribuida incluso más allá de la unidad de seguridad (por ejemplo, formando campeones de seguridad en otras áreas).

Comunicación y habilidades interpersonales:

Un rasgo diferenciador de los CISOs más efectivos es su capacidad para comunicar adecuadamente sobre riesgos y seguridad a audiencias muy diversas. Debe "traducir" el lenguaje técnico de Ciberseguridad a términos de negocio comprensibles para la alta dirección y el Consejo, de modo que apoyen las iniciativas necesarias. También le corresponde sensibilizar a todos los empleados –desde desarrolladores hasta usuarios finales– para crear conciencia y una cultura de seguridad. Para lograrlo, el CISO necesita excelentes habilidades de presentación, persuasión y negociación. Debe saber presentar un informe de estado de seguridad de forma clara, concisa y accionable, y también argumentar para obtener presupuesto o aprobación de proyectos estratégicos.

Asimismo, en situaciones de crisis (por ejemplo, un incidente grave), el CISO a menudo debe ser la voz pública que comunique la postura de la organización, o asesorar en la comunicación externa e interna durante la gestión del incidente. El desarrollo de estas habilidades puede venir de formaciones específicas en comunicación ejecutiva, pero sobre todo de la práctica: participar en comités de dirección, impartir charlas o representar a la empresa en foros sectoriales ayuda al CISO a ganar soltura comunicativa.

Networking y colaboración externa:

Ningún CISO opera en aislamiento. Dado que las amenazas son comunes a muchos y que la información sobre ellas es valiosa, resulta esencial colaborar con la comunidad. El CISO debe dedicar parte de su tiempo a establecer relaciones con otros profesionales del sector –ya sea a través de asociaciones (ISMS Forum, CyberThreat Alliance, etc.), grupos de trabajo público-privados (foros de CERTs nacionales, colaboraciones con organismos como INCIBE o CCN en España) o redes informales de colegas–.

Esta red de contactos de confianza permite intercambiar alertas tempranas, compartir lecciones aprendidas y hasta pedir consejo cuando se enfrenta un problema nuevo. Cultivar activamente esta comunidad (por ejemplo, participando en iniciativas de threat intelligence compartida o en grupos sectoriales de respuesta a incidentes) redunda en un beneficio para la organización del CISO. Además, demuestra actitud de aprendizaje abierto y humildad: reconocer que no lo sabemos todo, pero podemos apoyarnos en otros expertos. Muchos CISOs también devuelven valor a la comunidad publicando guías, dando ponencias o impulsando programas académicos, contribuyendo así a formar a la próxima generación de talento.

Ética e integridad personal:

La naturaleza de la Ciberseguridad implica que, tarde o temprano, el CISO enfrentará situaciones de alta presión (ataques en curso, brechas, crisis reputacionales). En esos momentos, se pone a prueba su templanza, courage y capacidad de decidir con información incompleta. Entrenar simulacros como se mencionó le prepara técnicamente, pero también es necesaria cierta fortaleza mental y emocional. Los mejores CISOs mantienen la cabeza fría en la tormenta, priorizan acciones y lideran con calma a su equipo durante la respuesta. Al mismo tiempo, el CISO debe ejercer de contrapeso equilibrado: no puede ser tan rígido en seguridad que frene la innovación del negocio. Sentido común y flexibilidad son vitales. Debe saber decir "no" cuando un riesgo es inaceptable, pero también encontrar cómo decir sí adaptando controles para habilitar iniciativas.

En la era de la transformación digital, un CISO inflexible que bloquea todos los cambios será visto como un obstáculo; en cambio, un CISO que busca soluciones de seguridad viables agiliza la competitividad de la empresa. Esta mentalidad se desarrolla entendiendo las prioridades de negocio y cultivando empatía con otras áreas: por ejemplo, trabajando codo a codo con Desarrollo para implementar DevSecOps, o con RRHH en políticas de teletrabajo seguro. La experiencia multidisciplinar nuevamente ayuda a tener esa flexibilidad.

Por último, pero no menos importante, un CISO debe ser modelo de integridad. Maneja información sensible, accede a decisiones críticas y sus recomendaciones pueden mover muchos recursos; por tanto, la confianza depositada en él debe corresponderse con los más altos estándares éticos. En palabras de la segunda edición del Libro Blanco, en seguridad no puede existir la "segunda oportunidad" para quienes defraudan la confianza. La honestidad, la transparencia y la defensa de lo correcto aun cuando sea difícil son cualidades imprescindibles.

Un CISO debe atenerse a códigos de conducta estrictos, evitando cualquier conflicto de interés, y fomentando la ética en su equipo (por ejemplo, respecto al uso responsable de herramientas de monitorización interna, o en el tratamiento respetuoso de datos personales). Esta reputación ética es lo que garantiza que la Alta Dirección confíe plenamente en el CISO, un requisito sine qua non para desempeñar su función con eficacia.

En síntesis, la formación del CISO abarca múltiples dimensiones. No se trata solo de acumular títulos o conocimientos, sino de integrar todo ello en la práctica diaria: un CISO altamente cualificado técnicamente, pero sin habilidades de liderazgo difícilmente logrará que la empresa mejore su seguridad, y a la inversa, un gran comunicador sin base técnica suficiente perderá credibilidad ante su equipo y la dirección. Por ello, el CISO debe evolucionar constantemente, formándose tanto en hard skills (tecnología, normativa, técnicas de seguridad) como en soft skills (liderazgo, comunicación, gestión de personas). Las tendencias actuales –como la creciente importancia de la resiliencia organizacional, la rápida adopción de IA o la amenaza omnipresente del ransomware– demandan CISOs versátiles, capaces de aprender y desaprender con agilidad. La buena noticia es que hoy existe más apoyo que nunca para su formación: desde una amplia oferta de certificaciones y estudios especializados, hasta comunidades colaborativas y recursos en línea. Un CISO que aproveche estas herramientas y abrace el aprendizaje continuo estará mejor preparado para enfrentar los retos presentes y futuros de la Ciberseguridad.

La gestión del talento en Ciberseguridad se ha convertido en uno de los retos más críticos para las organizaciones. Nos encontramos en un entorno de escasez de profesionales cualificados, donde la demanda supera con creces a la oferta disponible. Para un CISO, esto supone una doble responsabilidad: por un lado, captar a los mejores especialistas posibles para conformar un equipo competente, y por otro, retener a ese talento en la organización, motivado y comprometido, evitando la fuga de personal clave. En esta sección analizamos la situación actual del mercado laboral en Ciberseguridad, sus implicaciones, y las estrategias que un CISO puede adoptar para atraer y fidelizar talento en medio de esta escasez.

La brecha de talento en Ciberseguridad: una realidad alarmante

Diversos estudios recientes reflejan la magnitud del déficit de talento en Ciberseguridad a nivel global. Según datos de ISC², el organismo internacional de certificación, en 2022 la fuerza laboral mundial en seguridad contaba con unos 4,7 millones de profesionales, cuando se estimaba una necesidad de aproximadamente 9 millones; es decir, había un déficit de más de 4 millones de especialistas. Lejos de cerrarse, esta brecha persiste e incluso se amplía ligeramente: en 2023 el gap global se calculó en alrededor de 4,8 millones de puestos sin cubrir. Dicho de otro modo, haría falta casi duplicar la cantidad de expertos en Ciberseguridad en el mundo para satisfacer la demanda actual. Esta escasez no es teórica: se manifiesta en la dificultad que enfrentan empresas de todos los tamaños para encontrar candidatos cualificados para sus vacantes de seguridad, y en la sobrecarga de trabajo de los equipos existentes.

Concretamente en Europa, la situación refleja similar preocupación. Un informe reciente de ISACA indica que solo 35% de las empresas europeas cree tener el personal de Ciberseguridad adecuado, mientras que un 61% reconoce que su equipo es insuficiente para las necesidades actuales. Esta brecha se agrava por factores demográficos: profesionales veteranos que se jubilan sin que haya reemplazo proporcional de talento joven, y una todavía limitada incorporación de mujeres en Ciberseguridad (que representan alrededor del 24% del campo según ISC², lo que sugiere que hay un enorme potencial de reclutamiento desaprovechado en la mitad de la población).

Paradójicamente, esta escasez coincide con un aumento de la presión sobre los departamentos de seguridad. Hoy 74% de los profesionales afirma que el panorama de amenazas es el más desafiante de los últimos cinco años, con riesgos crecientes por la expansión de la superficie de ataque (nube, IoT, trabajo remoto) y la sofisticación de atacantes (ransomware de doble extorsión, amenazas persistentes avanzadas, etc.). Sin embargo, muchas organizaciones no están pudiendo invertir lo necesario en personal: un porcentaje significativo enfrenta restricciones presupuestarias que les impiden contratar o retener talento (según el estudio de ISC², un 37% de empresas sufrió recortes de presupuesto en seguridad en 2023, y un 38% congeló contrataciones). De hecho, por primera vez la falta de presupuesto fue citada como la principal causa de la escasez de personal de Ciberseguridad, creando una peligrosa paradoja: precisamente cuando más se necesita reforzar las plantillas, algunas empresas recortan recursos, lo que las deja aún más vulnerables.

El impacto de la escasez de talento se refleja en múltiples ámbitos. Desde luego, retrasa proyectos clave de seguridad (por ejemplo, la implantación de nuevas herramientas puede aplazarse por falta de especialistas para administrarlas); aumenta la carga sobre el personal existente, con el consiguiente riesgo de burnout y errores; y en última instancia puede comprometer la seguridad de la organización. No tener suficiente personal o las habilidades adecuadas es percibido ya como un riesgo mayor que las propias amenazas externas: el 90% de las organizaciones identifica brechas de habilidades importantes en sus filas, y un 58% considera que esa falta de habilidades pone a la empresa en riesgo significativo. En otras palabras, la escasez de talento se ha convertido en una amenaza interna adicional, que se suma a la lista de preocupaciones del CISO.

Frente a esta realidad, los CISOs deben desarrollar estrategias proactivas tanto para captar nuevo talento de Ciberseguridad como para desarrollar el talento interno existente, reduciendo la dependencia del volátil mercado externo. A continuación, exploramos tácticas concretas de atracción y retención de profesionales en un entorno de alta competencia por el talento.

Estrategias para la captación de talento

1. Ampliar y diversificar el pool de candidatos: ante la escasez generalizada, ceñirse al perfil "ideal" puede ser poco realista. Es recomendable buscar talento en fuentes no tradicionales. Por ejemplo, muchos roles de Ciberseguridad pueden ser cubiertos formando a internos de otras áreas de TI que tienen conocimiento del negocio; un administrador de sistemas con interés en seguridad podría convertirse en analista SOC con la capacitación adecuada. Asimismo, incorporar graduados de disciplinas diversas (matemáticas, físicas, incluso económicas o psicología) e invertir en su formación en seguridad puede dar buenos resultados – aportan perspectivas distintas y aprenden rápido si hay base técnica. También es crucial fomentar la diversidad de género: promover vocaciones en Ciberseguridad entre mujeres (mediante programas universitarios, mentoring, visibilizando referentes femeninos en el sector) incrementa la cantera de talento disponible. En España, iniciativas como CyberAcademy (INCIBE) o los programas de capacitación del CCN y asociaciones como Women in Cybersecurity buscan nutrir esa futura generación de profesionales.

2. Potenciar la marca empleadora en Ciberseguridad: para atraer a los mejores, la empresa debe mostrarse como un lugar atractivo donde trabajar en seguridad. Esto implica dar visibilidad a los proyectos interesantes que se llevan a cabo, a las tecnologías punteras con las que se trabaja, y a la importancia que la dirección concede a la Ciberseguridad. Un candidato valioso suele buscar entornos donde pueda aprender y tener impacto. El CISO puede colaborar con Recursos Humanos para destacar la propuesta de valor: por ejemplo, participación en conferencias (presentar en eventos forma parte de la cultura de la empresa), apoyo para obtener certificaciones, un laboratorio interno para pruebas de hacking, etc. También ayuda difundir casos de éxito del equipo (p. ej., publicaciones en blogs técnicos o presentaciones en meetups locales). En resumen, "vender" el puesto como algo más que un salario: como una misión apasionante defendiendo a la organización, con acceso a formación continua y posibilidades de crecimiento. Muchas grandes empresas ya realizan hackathons o desafíos abiertos (como bug bounties, competiciones tipo CTF –Capture The Flag–) para identificar talento entusiasta en la comunidad de seguridad e invitarlo a unirse.

3. Agilidad en los procesos de selección: en un mercado tan competido, los candidatos con buenas credenciales suelen tener múltiples ofertas. Por ello, las empresas que dilatan excesivamente sus procesos de selección corren el riesgo de perder a esos profesionales. Es importante que el CISO colabore con RRHH para diseñar procesos ágiles y atractivos: evaluaciones prácticas en lugar de varias rondas de entrevistas genéricas, feedback rápido tras cada etapa, y comunicación transparente sobre expectativas. Incorporar desafíos técnicos razonables (por ejemplo, analizar un caso sencillo de incidente) puede ser útil para evaluar habilidades sin ser demasiado exigente. Además, el CISO debe estar dispuesto a tomar decisiones rápidas y ser competitivo con las condiciones ofrecidas a un candidato deseable, sabiendo que el "tiempo de vida" de una oferta en el mercado es limitado.

4. Colaboración con educación y cantera: una estrategia a medio plazo para paliar la escasez es que el CISO se involucre en iniciativas educativas. Por ejemplo, asociarse con universidades o centros de formación profesional para ofrecer prácticas, participar en la definición de contenidos académicos actualizados o impartir charlas a estudiantes. Programas de becarios en Ciberseguridad permiten incorporar juniors con potencial e ir formándolos en la cultura de la empresa. Si bien requieren inversión de tutoría, a largo plazo muchos becarios pueden convertirse en empleados de planta leales. Del mismo modo, apoyar competiciones estudiantiles de Ciberseguridad (como CyberOlympics, CyberCamp, etc.) o eventos de talento joven da visibilidad a la empresa entre quienes pronto buscarán empleo. En esencia, se trata de sembrar hoy para recoger mañana: contribuir a aumentar el número de profesionales formados e identificar tempranamente a aquellos con más pasión y aptitudes.

Estrategias para la retención de talento

Captar talento es solo la mitad de la batalla; en un entorno donde los profesionales reciben ofertas constantemente, retenerlos es igual o más importante. La rotación frecuente no solo encarece la operación (costes de reclutamiento, tiempo de adaptación), sino que puede debilitar seriamente al departamento de seguridad. Mantener a los empleados satisfechos y comprometidos es, por tanto, una prioridad estratégica. Resulta preocupante saber que solo 3 de cada 10 trabajadores de Ciberseguridad se sienten plenamente conformes en su trabajo, según un estudio de Gartner. ¿Qué factores influyen en esta insatisfacción y cómo puede el CISO mitigarlos? A continuación, presentamos algunas claves de retención, muchas de las cuales están vinculadas a la motivación intrínseca del profesional más que al salario en sí.

Estrategia de retención	Descripción y beneficio
Desarrollo profesional continuo	Ofrecer oportunidades de capacitación (cursos, certificaciones, conferencias). Mantiene alta la motivación y sensación de progreso. El CISO debe planificar rutas de desarrollo, identificar habilidades y facilitar medios.
Reconocimiento y sentido de propósito	Implementar mecanismos de reconocimiento (elogios, recompensas, visibilidad ante la dirección). Comunicar misión del equipo y cómo cada rol protege la organización. Sentir un propósito alimenta la lealtad.
Flexibilidad y conciliación	Adaptarse a necesidades personales y generacionales. Ofrecer teletrabajo, horarios flexibles o modalidades híbridas. Medir resultados y eficacia más que horas presenciales. Entorno comprensivo genera fidelidad.
Plan de carrera y sucesión	Delinear caminos de evolución interna. Establecer perspectivas de crecimiento, abrir espacios para promociones internas y pensar en plan de sucesión. Envía mensaje de futuro y evita estancamiento.
Clima laboral positivo y cultura de equipo	Fomentar compañerismo, colaboración interna, bienestar cotidiano. Equipo diverso e inclusivo retiene mejor. El CISO debe ser accesible, escuchar sugerencias y demostrar empatía. Sentir que importan aumenta lealtad.
Cuidar la carga de trabajo y evitar “burnout”	Ciberseguridad implica sobre exigencia y agotamiento. El CISO debe priorizar proyectos, evitar posponer sin recursos, implementar rotaciones, automatizar tareas y gestionar picos laborales. Ignorar esto hace perder talento.

Figura 19. *Claves para retener talento de Ciberseguridad (fuente: tendencias identificadas por Gartner e ISC², adaptado de Forbes y del Libro Blanco del CISO).*

Como se desprende de las estrategias listadas, la retención gira en torno a motivación, crecimiento y bienestar. Si bien la compensación económica debe ser competitiva (los salarios en Ciberseguridad han subido por la alta demanda, y una política retributiva injusta disparará la rotación rápidamente), muchos estudios revelan que los factores no monetarios son igualmente determinantes para que un profesional decida quedarse. Por ejemplo, (ISC)² señala que la falta de oportunidades de desarrollo profesional en una empresa puede pesar más que un aumento salarial ofrecido por otra. Del lado positivo, cuando una organización invierte en su talento –le forma, le cuida y le traza un horizonte de carrera–, genera compromiso y sentido de pertenencia.

El papel del CISO como líder es fundamental en la retención. Un dicho popular es que “la gente no deja empresas, deja jefes”. Si el CISO logra ser un líder inspirador y cercano, tendrá un equipo más leal. Adaptarse a las diferencias generacionales es parte de ese liderazgo: en un mismo departamento pueden convivir desde baby boomers hasta centennials, cada cohorte con motivaciones y estilos de trabajo distintos. El CISO efectivo sabrá equilibrar, por ejemplo, la autonomía que valoran los más jóvenes con la estabilidad que aprecia el profesional senior, aprovechando lo mejor de cada grupo. Mentorización cruzada (que los veteranos transmitan conocimiento tácito a los noveles, y estos enseñen nuevas tecnologías a los mayores) puede crear un entorno de aprendizaje mutuo muy enriquecedor.

Otro aspecto a considerar es la mentalidad de equipo flexible. Esto significa estar dispuesto a reorganizar funciones según talento disponible o aspiraciones individuales. Por ejemplo, si un analista muestra interés y aptitud en threat hunting, ¿por qué no asignarle más tareas en esa línea para que se desarrolle, en lugar de encasillarlo en monitorear alertas pasivamente? Esa flexibilidad, dentro de lo razonable, hará que el profesional sienta que su puesto se adapta a sus intereses y no tenga que buscar ese rol ideal fuera. Empresas punteras incluso promueven que sus especialistas roten temporalmente por diferentes funciones de Ciberseguridad (pentesting, respuesta a incidentes, gobierno, ect.) para ampliar su visión y evitar la monotonía.

En definitiva, captar y retener talento en Ciberseguridad requiere un enfoque humano tanto como estratégico. El CISO, además de gestor de la seguridad, es gestor de personas: debe saber atraerlas ofreciéndoles un proyecto apasionante y formarlas para el futuro, y debe saber cuidar de su equipo para que crezca profesionalmente y se sienta valorado.

Cabe destacar que la escasez de talento no se resolverá de la noche a la mañana, pero las organizaciones que mejor naveguen este entorno serán aquellas que logren crear su propio vivero de talento. Esto implica combinar la contratación externa con la identificación y formación interna de personal, alimentando continuamente la cantera. Invertir en jóvenes profesionales, aunque requiera tiempo, puede fidelizarlos desde el inicio de su carrera. También conviene estar abiertos a perfiles atípicos: por ejemplo, profesionales de otras áreas (riesgos, auditoría, desarrollo) interesados en pasarse a seguridad, o incluso antiguos atacantes éticos (hackers) reconvertidos a defensores. En Ciberseguridad, la pasión y la capacidad de aprendizaje a menudo son más importantes que la experiencia previa directa.

Por último, es importante mencionar la colaboración sectorial como respuesta macro a la falta de profesionales. Los CISOs, a través de asociaciones y foros, pueden impulsar iniciativas conjuntas de capacitación de talento (como programas de certificación masiva, academias de Ciberseguridad en colaboración con gobiernos, etc.). Un ejemplo es el esfuerzo de entidades públicas y privadas en España para lanzar Másteres en Ciberseguridad industrial o en IA aplicada a la seguridad, alineados con las necesidades reales detectadas en la industria. Estos esfuerzos colaborativos, si bien no dan frutos inmediatos, contribuyen a ensanchar el embudo de entrada de profesionales en el mediano plazo.

En resumen, la guerra por el talento en Ciberseguridad es una realidad de nuestro tiempo, y el CISO se encuentra en primera línea de esta batalla. Su capacidad para reclutar, inspirar y retener a un equipo preparado puede marcar la diferencia entre una organización resiliente y otra vulnerable. A pesar de las dificultades, las empresas que cultivan una cultura de talento –donde se atrae, desarrolla y retiene a los mejores– no solo mitigarán el impacto de la escasez, sino que convertirán su capacidad humana en una ventaja competitiva en el ámbito de la seguridad. El desafío para el CISO es grande, pero también lo es la recompensa: un equipo con talento, estable y motivado es el mayor activo para afrontar cualquier reto de Ciberseguridad que depare el futuro.

[9] Forbes Argentina, *“No todo CISO es líder: cómo motivar, retener y formar talento en Ciberseguridad”*, Pedro Adamovic (CISO Banco Galicia), 10/09/2025.

7.3. Liderar equipos diversos y distribuidos

Este apartado resume prácticas recomendadas para responsables de seguridad que lideran equipos diversos y distribuidos. El objetivo final es mejorar la colaboración, la eficiencia y la resiliencia del área de Ciberseguridad.

1. Fomentar la comunicación clara y estructurada:

- Establecer canales oficiales para comunicación operativa y de emergencia.
- Utilizar métodos asíncronos (Chats, correo) para equipos en múltiples zonas horarias si aplicase.
- Mantener reuniones breves y regulares para asegurar alineamiento tanto en objetivos como en caso de incidente.

2. Priorizar la diversidad de perspectivas en la toma de decisiones:

- Asegurar que las decisiones críticas se revisen con miembros de distintos perfiles (técnicos, gestión, análisis).
- Promover entornos donde todos puedan expresar riesgos y preocupaciones sin barreras jerárquicas.

3. Establecer procesos de trabajo claros y documentados:

- Definir roles y responsabilidades para todas las funciones de Ciberseguridad.
- Documentar flujos de escalado y respuesta a incidentes.
- Facilitar acceso a repositorios comunes (por ejemplo, SharePoint, Confluence).

4. Promover una cultura de confianza y responsabilidad compartida:

- Reconocer públicamente contribuciones del equipo.
- Establecer expectativas claras de responsabilidad individual y colectiva.
- Fomentar la mentoría cruzada entre perfiles junior y senior.

5. Impulsar el desarrollo continuo y la actualización técnica:

- Proveer acceso a formaciones en Ciberseguridad, inteligencia de amenazas y herramientas emergentes.
- Organizar sesiones internas de intercambio de conocimiento.
- Definir objetivos de desarrollo profesional personalizados.

6. Utilizar herramientas colaborativas para equipos distribuidos:

- Emplear plataformas de seguimiento de tareas y proyectos (Azure DevOps, Jira, Planner).
- Centralizar dashboards que faciliten la visibilidad operativa.
- Asegurar que las herramientas cumplen requisitos de seguridad y privacidad desde el diseño y por defecto.

7. Gestionar la carga de trabajo de forma sostenible:

- Vigilar la rotación en guardias y funciones de alta demanda.
- Detectar signos de sobrecarga y equilibrar esfuerzos entre regiones (si aplica) y perfiles.
- Implementar la automatización en tareas repetitivas.

8. Garantizar la cohesión del equipo a pesar de la distancia:

- Organizar encuentros periódicos presenciales o virtuales para que el equipo esté conectado y cercano entre sí.
- Crear espacios informales de conversación que fortalezcan la confianza interpersonal.

Con la implementación de estas recomendaciones, se potenciaría la eficacia y cohesión de los equipos de Ciberseguridad, especialmente en entornos híbridos y globales.

7.4. Salud mental del CISO y sostenibilidad en el cargo

El rol del CISO conlleva alta presión, exposición y responsabilidad continuas. La sostenibilidad del cargo depende de cuidar la salud mental y de mecanismos organizativos que reduzcan la sobrecarga.

La sostenibilidad en el cargo depende en gran medida del cuidado activo de la salud mental y del desarrollo de mecanismos personales y organizativos que reduzcan la sobrecarga. A continuación, recogemos pautas para conseguir los objetivos positivos del capítulo.

1. Establecer límites saludables en un rol de alta disponibilidad:

- → Definir ventanas claras de disponibilidad y comunicar expectativas realistas al equipo y a la organización.
- → Evitar el hábito de responder fuera del horario laboral salvo incidentes críticos.
- → Rotar responsabilidades con otros líderes del área CISO o responsables operativos para preservar el descanso.

2. Reforzar una cultura de delegación y confianza:

- → Evitar centralizar decisiones operativas: delegar en managers de dominios específicos (SOC, IAM, GRC, Arquitectura Seguridad, etc.).
- → Implantar procesos que permitan autonomía y reduzcan la dependencia directa del CISO en actividades diarias.
- → Revisar periódicamente la carga de trabajo y reasignar responsabilidades para evitar cuellos de botella.

3. Crear un sistema de gestión del estrés:

- → Incorporar rutinas de desconexión diaria: ejercicio, mindfulness, o hábitos que reduzcan la tensión acumulada.
- → Reconocer señales tempranas de agotamiento: irritabilidad, falta de concentración, sueño irregular o deterioro de la toma de decisiones.
- → Utilizar recursos de apoyo profesional si fuera necesario (coaching ejecutivo, psicología del trabajo, etc.) o influir en la organización para que exista.

4. Proteger el foco estratégico frente a la “trampa operativa”:

- → Reservar tiempo semanal exclusivamente para análisis, planificación, innovación y reflexión.
- → Filtrar reuniones y priorizar temas que realmente requieran presencia del CISO.
- → Evitar que el día a día operativo absorba la totalidad del tiempo y energía.

5. Gestionar expectativas del negocio y comunicar de forma transparente:

- → Alinear periódicamente prioridades con la alta dirección para evitar conflictos de prioridades y sobrecarga.
- → Comunicar riesgos y limitaciones de manera clara para evitar presiones innecesarias o expectativas irreales.
- → Asegurar soporte ejecutivo para iniciativas de transformación y modernización.

6. Construir una red de apoyo profesional:

- → Mantener contacto regular con otros CISOs (foros, comunidades, benchmarkings).
- → Compartir experiencias y buenas prácticas ayuda a normalizar los desafíos del rol y reduce la sensación de aislamiento.
- → Utilizar mentores o asesores externos para obtener otras perspectivas.

7. Diseñar una estrategia de sostenibilidad a largo plazo:

- → Invertir en automatización, IA y herramientas que reduzcan trabajo manual y fatiga de alertas, información, etc.
- → Crear un plan de sucesión y desarrollo interno para no depender exclusivamente del CISO para la continuidad operativa.
- → Evaluar periódicamente el equilibrio entre expectativas del cargo, recursos disponibles y nivel de riesgo asumido.

8. Priorizar la salud mental como parte de la cultura del área de seguridad:

- → Visibilizar el tema dentro del equipo, fomentando conversaciones abiertas y apoyo mutuo.
- → Establecer políticas de guardias sostenibles, tiempos de descanso y cobertura en incidentes.
- → Predicar con el ejemplo: un CISO que cuida su bienestar permite que el equipo haga lo mismo.

8.

Conclusiones

A lo largo de esta obra hemos analizado la ciberseguridad como un sistema estructurado de actividades, y no como un conjunto aislado de herramientas. Hemos descrito sus fundamentos técnicos, su dimensión directiva, su encaje organizativo y su consolidación normativa. La conclusión es clara: el CISO se ha consolidado como la función que transforma los principios teóricos de la seguridad en decisiones efectivas de gobierno corporativo.

La ciberseguridad descansa sobre pilares conceptuales sólidos. La tríada Confidencialidad, Integridad y Disponibilidad -ampliada en determinados marcos al modelo CITAD, incorporando Autenticidad y Trazabilidad- no constituye una abstracción académica, sino el criterio estructural que orienta la arquitectura de controles, la gestión del riesgo y la respuesta ante incidentes. Proteger la información implica garantizar estas dimensiones de forma proporcional al contexto y al impacto potencial sobre el negocio.

Ahora bien, estos principios no se materializan de forma automática. Requieren decisiones deliberadas de diseño y gobierno. De ahí la relevancia de:

- Seguridad desde el diseño, que integra la protección como criterio estructural desde la concepción de sistemas, servicios y procesos.
- Seguridad por defecto, que prioriza configuraciones restrictivas compatibles con la finalidad perseguida.
- Seguridad por capas, que reconoce que ningún control aislado es suficiente y que la resiliencia surge de la combinación coordinada de medidas organizativas, técnicas y humanas.

El CISO es la figura que articula estos principios dentro del funcionamiento real de la organización. No se limita a validar soluciones técnicas: asegura que las decisiones arquitectónicas, las prioridades presupuestarias, la gestión de terceros y la aceptación del riesgo respondan a una lógica coherente y defendible.

La evolución normativa ha reforzado esta exigencia. El Esquema Nacional de Seguridad (Real Decreto 311/2022) consolida la diferenciación de responsabilidades y la supervisión sistemática. El Real Decreto 43/2021, que desarrolla la normativa de seguridad de redes y sistemas de información, define con claridad la función responsable de la seguridad de la información, estableciendo sus atribuciones, posición organizativa, recursos e independencia, así como su papel como punto de contacto con autoridades y equipos de respuesta. La Directiva (UE) 2022/2555 (NIS2) intensifica, por su parte, la responsabilidad de la alta dirección y exige capacidades formales de gestión del riesgo, notificación de incidentes y seguridad en la cadena de suministro.

Aunque estas normas no siempre emplean expresamente el término “CISO”, sí consolidan de forma material su contenido funcional. La identificación, evaluación y tratamiento del riesgo digital; la definición de políticas; la supervisión de su implantación; la coordinación con autoridades competentes; y la rendición de cuentas requieren una función especializada, transversal e independiente.

El CISO no sustituye la responsabilidad última de la alta dirección: la operacionaliza. Permite que el riesgo digital se eleve, se documente, se priorice y se gestione con criterios objetivos, aportando trazabilidad, proporcionalidad y coherencia.

La madurez organizativa se evidencia en la segregación entre operación y supervisión, en la existencia de capacidades diferenciadas de detección y respuesta, en la medición orientada a la toma de decisiones y en la integración de la ciberseguridad en la estrategia corporativa. En este entorno, el CISO actúa como garante del equilibrio entre protección, innovación y resiliencia.

El entorno digital seguirá incrementando su complejidad: IA, infraestructuras distribuidas, dependencia de terceros y adversarios con capacidades industrializadas convierten el riesgo digital en un riesgo estructural y permanente. Frente a ello, la organización no necesita promesas de invulnerabilidad, sino gobierno efectivo.

En última instancia, el CISO representa la institucionalización del gobierno del riesgo digital. Es la función que convierte los principios de la tríada CID, la seguridad desde el diseño, la configuración segura por defecto y la protección por capas en decisiones estratégicas sostenidas en el tiempo.

Allí donde esta función está claramente definida, adecuadamente posicionada e integrada en el modelo de gobierno corporativo, la organización no solo protege información: protege su continuidad, su reputación y su legitimidad en un entorno digital que ha dejado de ser accesorio para convertirse en esencial.

9.

Referencias

ISMS Forum. Libro Blanco del CISO (2ª ed.). ***https://www.ismsforum.es/ficheros/descargas/segunda-edicion-del-libro-blanco-del-ciso-de-isms.pdf***

Managing Information Security Risk: Organization, Mission, and Information System View (NIST Special Publication 800-39). National Institute of Standards and Technology. ***https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=908030***

Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022. ***https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963***

Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016. ***https://www.boe.es/doue/2016/194/L00001-00030.pdf***

Cybersecurity roles and skills for NIS2 essential and important entities: Mapping NIS2 obligations to ECSF role profiles. European Union Agency for Cybersecurity (ENISA). ***https://www.enisa.europa.eu/sites/default/files/2025-06/Mapping%20NIS%202%20obligations%20with%20ECSF%20role%20profiles.pdf***

Modelo de cuestionario unificado para el control de la cadena de suministro: ***https://www.ismsforum.es/ficheros/descargas/cartacadenasuministrosfinal1739549325.pdf***

Guía para la gestión de ciberincidentes originados en la cadena de suministro: ***https://www.ismsforum.es/ficheros/descargas/guia-para-la-gestion-de-crisis-por-ciberincidente.pdf***

Cláusulas contractuales para sistemas/servicios de IA: ***https://master.ismsforum.es/wp-content/uploads/2025/03/informe-isms-v41742972337.pdf***

Guía de Ciberseguridad en entornos industriales para PYMEs: ***https://www.ismsforum.es/ficheros/descargas/guia-entornos-industriales-20231686772410.pdf***

ISMS Forum 2025. The CISO and Senior Management. ***https://www.ismsforum.es/ficheros/descargas/the-ciso-and-senior-management1765382437.pdf***

Cloud Security Alliance. (2025). The State of Cloud and AI Security 2025. ***https://cloudsecurityalliance.org/artifacts/the-state-of-cloud-and-ai-security-2025***

Forbes Argentina, *"No todo CISO es líder: cómo motivar, retener y formar talento en Ciberseguridad"*, Pedro Adamovic (CISO Banco Galicia), 10/09/2025.

isms forum

CSC
CYBER SECURITY CENTRE

III edición
/ 2026

Libro Blanco del CISO