Seguridad digital:
resiliencia, innovación y confianza

Políticas Públicas Digitales, Regulación y Competencia

2025

Telefónica

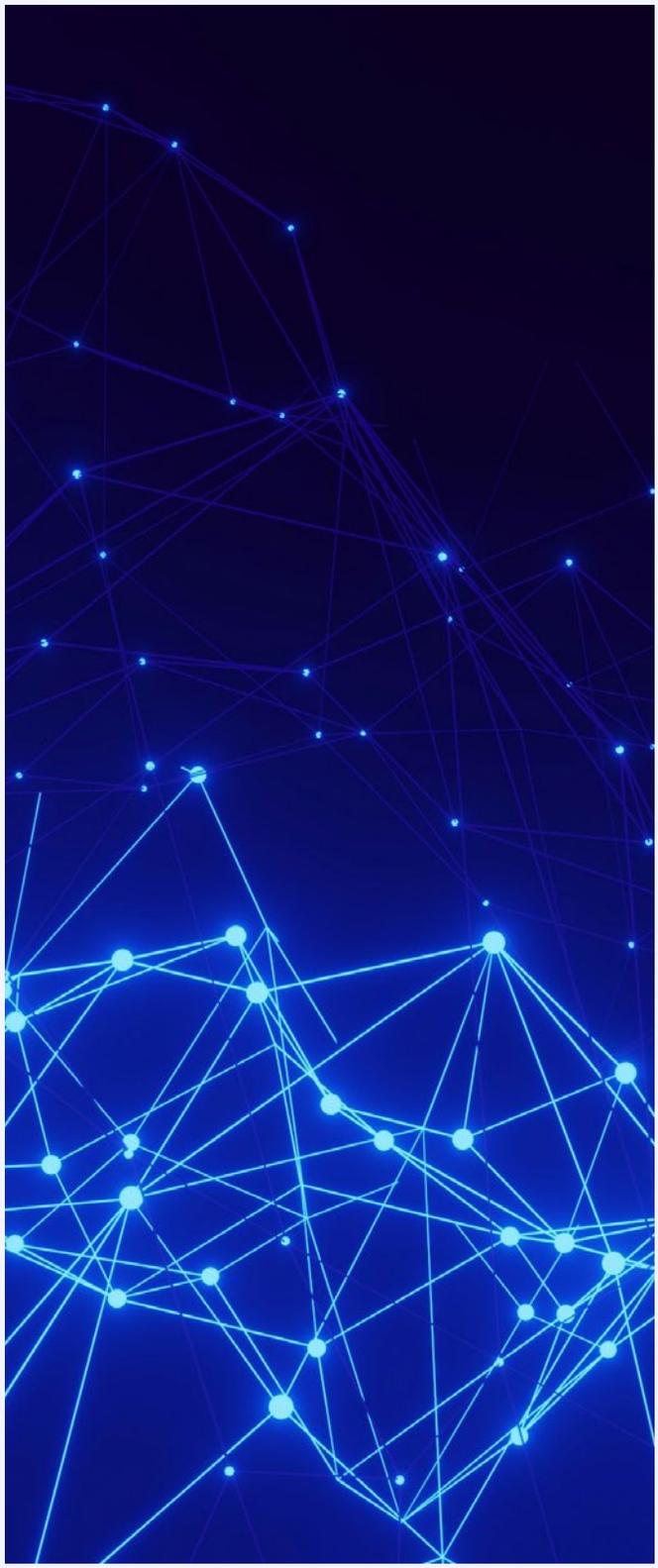
Prólogo

En un contexto de ciberamenazas sin precedentes y ante un panorama regulatorio complejo, resulta más crucial que nunca contar con un socio estratégico tecnológico. En Telefónica, creemos que la seguridad digital no solo es una exigencia empresarial, sino también un pilar fundamental para construir una sociedad resiliente y próspera.

La revolución digital ha transformado todos los aspectos de nuestras vidas, pero este avance trae consigo nuevos retos. Hemos sido testigos del crecimiento exponencial de los ciberataques, de la creciente brecha de habilidades, de la escasez de financiación y de los retos que plantea un entorno regulatorio fragmentado y complejo. Estas cuestiones ponen de manifiesto una realidad: garantizar nuestro futuro digital requiere un nuevo modelo de colaboración. Exige una alianza entre los sectores público y privado, en la que se aproveche la experiencia tecnológica del sector de telecomunicaciones para reforzar las políticas públicas.

Como líder global del sector de telecomunicaciones, nuestro papel va más allá de proporcionar conectividad. Nuestra red segura y nuestras capacidades de vanguardia nos sitúan en el centro de este desafío. Estamos en una posición única para servir de aliado de confianza de los gobiernos, las administraciones públicas y las empresas de todos los tamaños en la construcción de la resiliencia y la seguridad necesarias para prosperar en un mundo cada vez más conectado.

Este documento es nuestra contribución a este debate fundamental. Ofrece un análisis exhaustivo del panorama actual en materia de seguridad y presenta recomendaciones claras y viables para los responsables de políticas públicas. Esperamos que sirva de catalizador para construir un mundo más seguro, innovador y confiable, basado en la responsabilidad compartida y la colaboración.



Índice

1. Resumen ejecutivo

La ambición estratégica en materia de seguridad debe estar respaldada por un entorno propicio

La complejidad regulatoria y las obligaciones sin financiación amenazan con socavar la resiliencia que pretendemos construir. Un sector de telecomunicaciones sostenible y un marco proporcionado y bien financiado son esenciales para lograr seguridad, resiliencia y soberanía. Telefónica, con décadas de experiencia en la gestión y protección de una amplia infraestructura y servicios digitales, está en una posición única para ayudar a gobiernos, empresas y sociedad a desarrollar su resiliencia.

La seguridad es un pilar fundamental de la sociedad: una responsabilidad compartida y un motor clave de innovación

La seguridad digital y la soberanía tecnológica se han convertido en elementos centrales de la agenda política. La industria de seguridad digital es una piedra angular clave, que proporciona capacidades esenciales y genera importantes efectos indirectos. Esto refuerza la necesidad de una mayor coordinación, un compromiso político a largo plazo y una inversión sostenida.

En un contexto de urgencia, mejorar la resiliencia implica superar retos políticos, técnicos y económicos

Los riesgos e incertidumbre crecientes, el continuo aumento de los ciberataques, filtraciones de datos, fraude y ciberespionaje ponen de relieve la necesidad crítica de contar con marcos de seguridad y políticas industriales eficaces.

La protección de infraestructuras estratégicas tiene un valor fundamental

Las redes resilientes son esenciales, al sustentar servicios críticos de la sociedad. El sector de telecomunicaciones lleva tiempo implementando medidas de seguridad robustas para proteger sus activos, clientes y servicios, pero sus contribuciones positivas y sus inversiones sostenidas a menudo pasan desapercibidas. Y las obligaciones regulatorias que van más allá de consideraciones de mercado corren el riesgo de socavar la sostenibilidad de los operadores, si no se acompañan de una financiación adecuada, como se ve en otros sectores.

El sector de las telecomunicaciones, con Telefónica como socio estratégico y de confianza, desempeña un papel crucial en el fortalecimiento de la seguridad

Telefónica cuenta con una amplia experiencia, personal altamente cualificado, sólidas capacidades operativas y una red de alianzas que le permiten no solo proteger su propia infraestructura, sino también reforzar la resiliencia del conjunto de la sociedad, incluyendo empresas y administraciones públicas, al tiempo que promueve activamente la sensibilización y combate el fraude.

El sector actúa además como motor clave de innovación en materia de seguridad

Acelera el desarrollo e implementación de tecnologías de vanguardia, como la inteligencia artificial y la computación cuántica; aplica mejores prácticas para reforzar eficiencia, resiliencia y desarrollo de servicios innovadores; y, al mismo tiempo, impulsa la transformación digital de las industrias y servicios de las administraciones públicas.

Es el momento de actuar, con políticas que apoyen de manera eficaz un entorno digital seguro, innovador y confiable

Recomendaciones

Para mejorar la seguridad y las capacidades digitales, aumentar la resiliencia de la sociedad y reducir las dependencias:

1. **Garantizar un sector de telecomunicaciones sólido y sostenible**, apoyado en operadores de confianza que actúen como socios tecnológicos estratégicos a nivel regional.

2. **Impulsar la inversión en seguridad, resiliencia y tecnologías de doble uso** mediante la combinación de financiación pública, incentivos fiscales específicos y la utilización estratégica de la contratación pública.

3. **Implementar un marco regulatorio y de estándares de seguridad simplificado**, proporcionado, coherente, basado en riesgos, desarrollado en estrecha colaboración con el sector privado.

4. **Fomentar el desarrollo de las competencias en materia de tecnología y ciberseguridad**, al tiempo que se promueve una mayor sensibilización sobre seguridad digital para fomentar una sociedad digital más resiliente.

5. **Mejorar la coordinación en materia de ciberinteligencia, defensa, disuasión y lucha contra la ciberdelincuencia,** asegurando mayores recursos y una cooperación más estrecha.

2. El valor de la *seguridad digital* y la resiliencia

A. La seguridad como pilar de la sociedad: responsabilidad compartida y motor clave de innovación

En una era de creciente complejidad digital y tensiones geopolíticas, la seguridad digital y la soberanía tecnológica han pasado a ocupar un lugar destacado en la agenda política.

Para las organizaciones, el desarrollo de la seguridad digital consiste, fundamentalmente, en adoptar un enfoque integral, garantizar la continuidad del negocio y fomentar la confianza mediante estrategias que trascienden las soluciones puramente técnicas. Para los responsables políticos, se trata de garantizar la estabilidad económica, la soberanía y la confianza pública integrando el concepto de resiliencia[2].

La seguridad digital es una responsabilidad compartida, que requiere esfuerzos coordinados entre gobiernos, administraciones públicas, el sector privado y los organismos internacionales[3]. Por otra parte, el sector de la seguridad digital es también un motor estratégico de innovación, soberanía y modernización regional, con efectos indirectos en toda la sociedad.

Esto exige una mayor coordinación, un compromiso político a largo plazo y una financiación sostenible.

En un contexto de amenazas cibernéticas sin precedentes y de una gran complejidad normativa, la necesidad de un socio estratégico tecnológico nunca ha sido tan crítica.

> **La seguridad es la base sobre la que se construye todo [...] La seguridad es un bien público [...] Es la condición previa para mantener nuestros valores, además de ser una necesidad para nuestro éxito económico y nuestra competitividad**
>
> Informe del asesor Niinistö: *Report on the Preparedness and Readiness of the EU* - Octubre 2024[1]

B. La creciente preocupación por la seguridad digital define el panorama digital actual

El Foro Económico Mundial[4] identifica la inseguridad cibernética (desinformación, ciberespionaje y ciberguerra) como uno de los diez principales riesgos mundiales. El panorama es cada vez más complejo.

Las filtraciones de datos, los ataques de *ransomware*[5], y el ciberespionaje siguen aumentando. El mundo se enfrenta a una nueva realidad de riesgos e incertidumbre crecientes, lo que hace que la preparación sea más urgente que nunca.

Figura 1. Panorama global de la segurida digital[6]

Fuentes: Telefónica basado en: Checkpoint (Abril 2025)- Q1 2025 Global Cyber Attack Report. Checkpoint - The state of Cybersecurity | World Economic Forum (WEF) (Enero 2025) - Global Cybersecurity Outlook 2025 | GSMA (Febrero 2025) - Fraud and Scams: Staying Safe in the Mobile World | International Monetary Fund (IMF) (Abril 2024) - Chapter 3 Global Financial Stability Report, Cyber Risk: A Growing Concern for Macro financial Stability

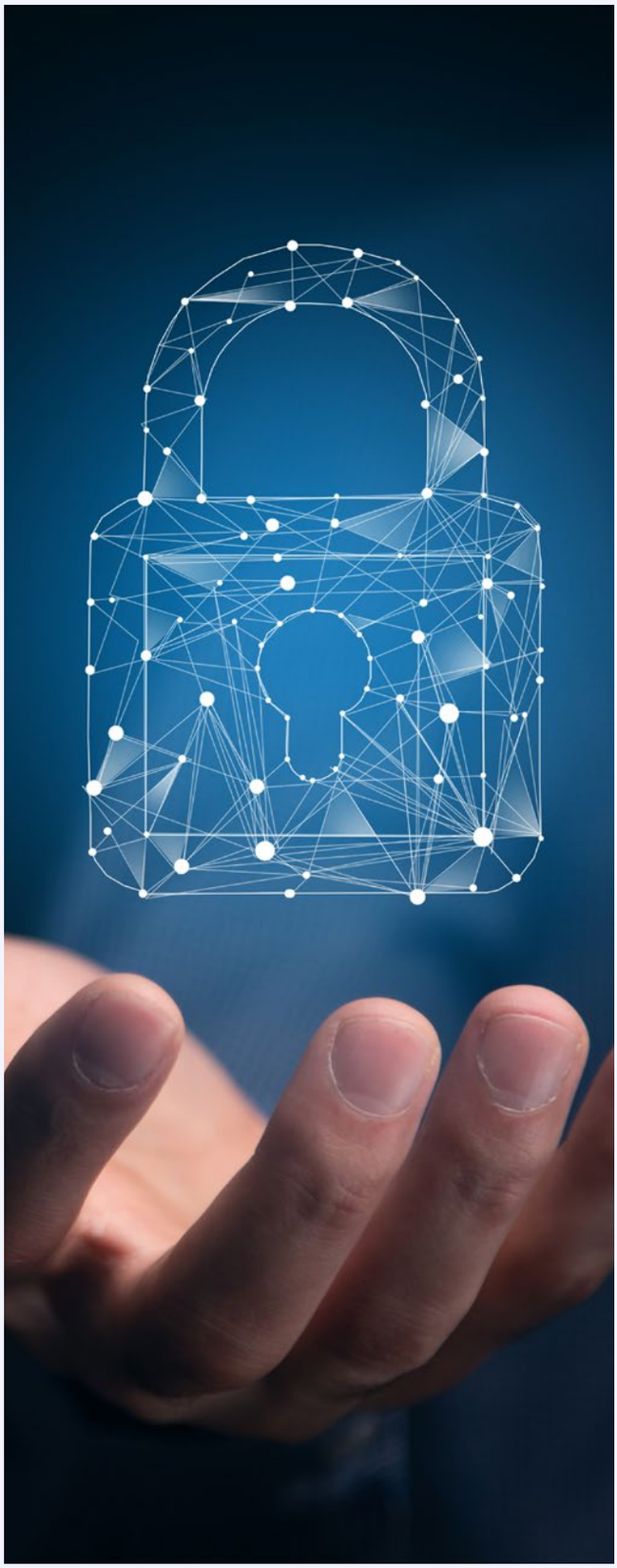
El número de ciberataques se ha disparado un 50% durante el último año, alcanzando una media de 1.925 ataques semanales por organización en el primer trimestre de 2025[7]. En 2024, alrededor del 42% de las organizaciones sufrieron un ataque con éxito basado ingeniería social, una cifra que solo puede aumentar con la adopción maliciosa de la IA[8]. La cadena de suministro es especialmente sensible, ya que el 54% de los incidentes cibernéticos se originaron en terceros.

Se prevé que el coste económico global de la ciberdelincuencia, incluido el fraude[9], aumente de los 9.220 miles de millones de 2024 a 15.630 miles de millones de dólares en 2029. El coste de los ciberataques o las filtraciones de datos son cada vez más elevadas: el coste total medio por incidente supera los 4 millones de euros[10].

Según el Informe sobre riesgos cibernéticos del FMI[11], las organizaciones que corren mayor riesgo son las de sectores altamente conectados, las que tienen activos atractivos pero una protección más débil (como las pymes) y las que operan en países con un alto riesgo geoestratégico o una legislación de ciberseguridad inadecuada. Los atacantes tienen diversos motivos, el más común es el lucro, como se observa en grupos delictivos organizados, pero también la búsqueda de reconocimiento o el avance de causas políticas y sociales.

Existe una brecha cada vez mayor entre las organizaciones que son ciberresilientes y las que no lo son. Las pequeñas organizaciones ya no pueden protegerse adecuadamente contra la creciente complejidad de los riesgos, según el 71% de los líderes en temas de ciberseguridad. Menos de una cuarta parte de las pymes cuentan con un seguro de ciberseguridad, en comparación con el 75% de las organizaciones más grandes, y más del doble de pymes que de grandes organizaciones afirman que carecen de la resiliencia cibernética necesaria para cumplir con sus requisitos operativos críticos, lo que retrasa su evolución en el mundo digital. En el sector de las telecomunicaciones, las causas fundamentales de las interrupciones del servicio, medidas en términos de horas de comunicación perdidas, son principalmente fallos del sistema (60%), seguidos de errores humanos (19%), fenómenos naturales (13%) y acciones maliciosas (8%).

Reforzar la preparación y combatir las ciberamenazas es más urgente que nunca. Las consecuencias de las filtraciones de información, amenazas a la seguridad digital y el fraude pueden ocasionar pérdidas financieras significativas, poner en peligro la viabilidad de las empresas y provocar la pérdida de confianza en los servicios digitales, lo que, en última instancia, dificulta la adopción de tecnologías que, de otro modo, serían beneficiosas. Por otra parte, contrarrestar la manipulación y la injerencia extranjeras se ha vuelto esencial para salvaguardar la estabilidad, así como la protección soberana de los derechos individuales, las empresas, los procesos democráticos y los valores fundamentales.



C. Mejorar la resiliencia implica superar retos geopolíticos, técnicos, políticos y económicos

En el contexto actual, el desarrollo de la resiliencia requiere afrontar una serie de **retos críticos**[13].

Figura 2. Principales retos que configuran el panorama de la seguridad digital

Habilidades - Alta prioridad en **71%** de empresas en UE[4]

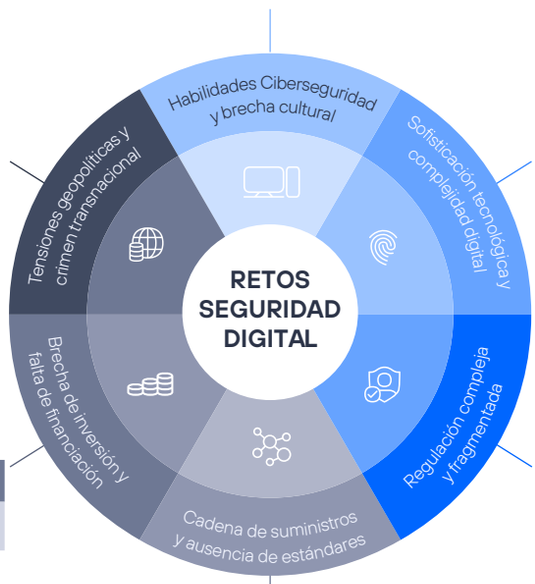
Solo **14%** de empresas confía en sus competencias[1]

Escasez de profesionales: gap de **500.000** expertos en la UE y entre **2,8 to 4,8 millones** a nivel mundial[1]

60% de organizaciones señalan que las tensiones geopolíticas afectan a su estrategia de ciberseguridad[1]

Más de **$1 Billón** (millones de mill.) de fraude en 2023[2]

Dificultad **aplicación de ley** en internacional



Tecnología usada en defensa y ataque (IA, cuántica)

Paradoja[1]**: 66%** preve impacto de IA en 2026, solo **37%** tiene procesos de seguridad

Complejidad: fallos configuración & IT vs OT

Complejidad regulatoria: 76% de empresas señala que la fragmentación dificulta el cumplimiento y eficacia en ciberseguridad

Riesgo de ***de-coupling*** o ***de-risking*** más allá del mercado, requiriendo financiación pública

Brecha de inversión en seguridad digital[3]

	Gasto en seguridad digital	
	Por empleado / año	% de gasto en IT
Media	$ 709	5,6%
Admin. Pública		
Local & Regional	$ 520	4,6%
Nac. & Internac.	$ 1.346	5,7%
Telecoms	$ 1.851	7,3%

Ausencia de **análisis económico**, y estrategias de financiación

Fuentes: Telefónica, basado en: (1) World Economic Forum (WEF) (Enero 2025) - Global Cybersecurity Outlook 2025 | (2) GSMA (Febrero 2025) - Fraud and Scams: Staying Safe in the Mobile World. | (3) Gartner (Diciembre 2024) – IT Key Metrics Data 2025: IT Security Measures Analysis; ENISA (Noviembre 2024) - NIS Investments | (4) Eurobarometer (Mayo 2024) - Survey on cyber-skills | EU Mind the Cyber Skills Gap (Agosto 2023): a deep-dive

Las tensiones geopolíticas y la delincuencia transnacional siguen complicando los esfuerzos para hacer frente a la inseguridad y el fraude. La escasez de profesionales de ciberseguridad y la ausencia de una cultura sólida en esta materia agravan aún más estos retos. Si bien las tecnologías emergentes ofrecen nuevas oportunidades para la defensa y la resiliencia, la creciente complejidad de los sistemas digitales dificulta la seguridad extremo-a-extremo. Además, las interdependencias de la cadena de suministro y la falta de estándares comunes o abiertos siguen siendo obstáculos importantes para la creación de infraestructuras resilientes a largo plazo.

La resiliencia sigue sin recibir los fondos necesarios, tanto en el sector público como en el privado, debido a los limitados incentivos, al igual que se observa en la I+D con los efectos indirectos. A menudo, los objetivos públicos superan un enfoque basado en riesgo, en la proporcionalidad o en las dinámicas de mercado, y carece del análisis económico y de estrategias de financiación necesarios para garantizar su implementación. Mejorar la resiliencia es costoso: por ejemplo, el coste de proporcionar una hora de respaldo en la red de acceso radio (RAN) del Reino Unido en las cuatro redes móviles sería de entre 900 y 1.800 millones de libras esterlinas, más el mantenimiento[14].

El panorama regulatorio, fragmentado y complejo, dificulta la aplicación de estrategias eficaces. Aunque cada vez existe un mayor consenso en que la normativa es clave para reforzar los niveles básicos de ciberseguridad, su proliferación y la falta de armonización plantean retos significativos. La existencia de regulaciones duplicadas, contradictorias o innecesarias obliga a las empresas a destinar más recursos al cumplimiento técnico, sin que ello se traduzca en una mejora real de los resultados en materia de ciberseguridad[15].

CUADRO 1

POLÍTICAS DE CIBERSEGURIDAD EN EUROPA: COMPLEJIDAD Y FRAGMENTACIÓN

En la Unión Europea, la Directiva NIS2 (Redes y Sistemas de Información) eleva significativamente los estándares de ciberseguridad en 18 sectores, exigiendo gestión de riesgos, respuesta y notificación de incidentes, planificación de la continuidad del negocio, una supervisión más estricta de la cadena de suministro y una mayor responsabilidad a nivel directivo.

Sin embargo, opera en un **contexto regulatorio complejo**[16], en el que se superponen marcos nacionales o europeos como DORA (Ley de Resiliencia Operativa Digital), CRA (Ley de Ciberresiliencia), CSA (Ley de Ciberseguridad-marco de certificación), CER (Resiliencia de Entidades Críticas), la regulación del sector de las telecomunicaciones, el RGPD (Reglamento General de Protección de Datos), la Ley de IA o la Caja de Herramientas 5G de la UE, junto con un número cada vez mayor de estándares de seguridad que las organizaciones deben cumplir.

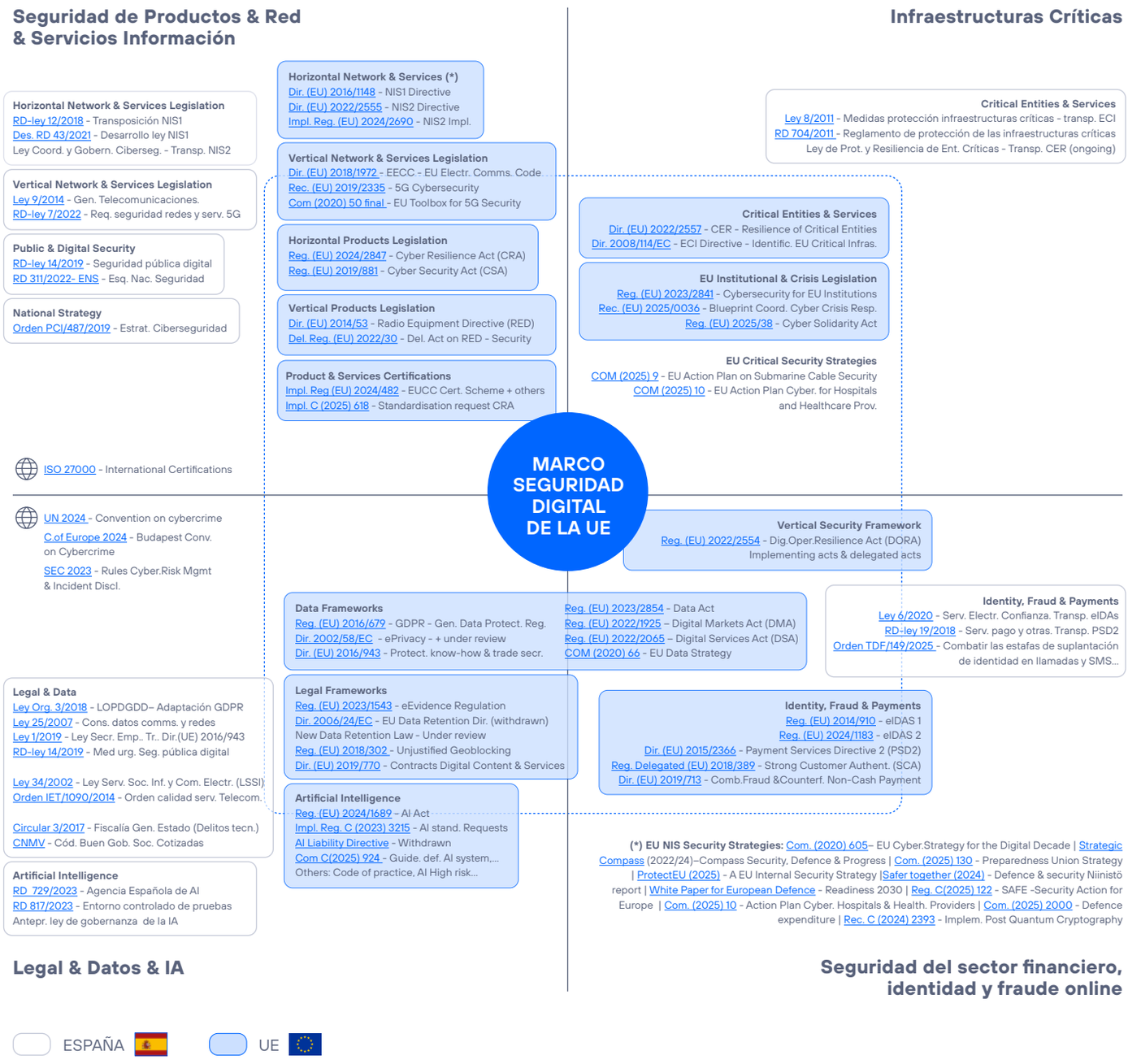
Estos marcos se complementan con **estrategias de seguridad nacionales y europeas**[17], entre las que se incluyen el reciente plan de acción en materia de defensa[18], la propuesta de ciberseguridad para hospitales, la iniciativa para proteger los cables submarinos, la iniciativa *Protect EU* o la Ley de Ciber-solidaridad[19]. Así, la política de ciberdefensa de la UE tiene por objeto mejorar la cooperación y las inversiones para detectar, disuadir, proteger y defender mejor contra un número cada vez mayor de ciberataques.

Otra novedad es la puesta en marcha de la **base de datos de vulnerabilidades de la ENISA (EUVD)**[20] en mayo de 2025. Aunque no es tan amplia como la base de datos CVE-MITRE[21] financiada con fondos públicos de los Estados Unidos, la EUVD busca un alto nivel de interconexión mediante la agregación de información disponible públicamente de diversas fuentes, incluidos los CSIRT, los proveedores y las bases de datos de vulnerabilidades existentes.

Este panorama normativo complejo y fragmentado pone de relieve la necesidad de adoptar un enfoque simplificado y proporcionado para abordar de manera eficaz las ciberamenazas en la UE.

Telefónica

Figura 3. Marco normativo complejo y fragmentado de la UE en seguridad de infraestructuras digitales



Fuentes: Telefónica (Enero 2025) - DORA, NIS2 y CRA: Descifrando la normativa de ciberseguridad en Europa | Telefónica (Abril 2025) - Defensa, seguridad y preparación: Un plan de acción de la UE

CUADRO 2

POLÍTICAS DE CIBERSEGURIDAD EN OTRAS REGIONES: BRASIL Y CHILE

Internacionalmente, el enfoque regulatorio en materia de ciberseguridad varía considerablemente[22]. En América Latina se están llevando a cabo varias iniciativas legislativas; sin embargo, la madurez varía considerablemente entre países y el desarrollo de medidas de protección suele estar correlacionado con haber sufrido anteriormente incidentes graves, como es el caso de Costa Rica.

BRASIL

Brasil ha sentado las bases para un marco sólido de ciberseguridad, en particular a través de la Ley General de Protección de Datos (LGPD) y la Estrategia Nacional de Ciberseguridad (E-Ciber), que actualmente está siendo revisada por el Comité Nacional de Ciberseguridad (CNCiber) de acuerdo con las directrices del Decreto N.º 11.856/2023, que estableció la Política Nacional de Ciberseguridad (PNCiber).

En cuanto a la regulación sectorial, Anatel aprobó en 2020 y actualizó en 2024 el Reglamento de Ciberseguridad aplicado al Sector de las Telecomunicaciones (R-Ciber), que establece normas para las redes y servicios de telecomunicaciones, centrándose en la protección de las infraestructuras críticas, exigiendo medidas preventivas, respuesta a incidentes y gestión de riesgos, bajo la coordinación del GT-Ciber, un grupo técnico responsable de definir plazos, procedimientos y equipos cubiertos.

CHILE

En un contexto tan diverso, Chile destaca por la adopción en marzo de 2024 de la Ley N.º 21.663 sobre Ciberseguridad e Infraestructura Crítica de Información[23], que representa un importante avance en la región. Se trata de la primera respuesta normativa integral de Chile en ciberseguridad. Complementa la Política Nacional de Ciberseguridad 2023-2028, creando un marco fundamental para una estrategia nacional de ciberseguridad cohesionada. Los principios fundamentales son:

- Creación de la Agencia Nacional de Ciberseguridad (ANCI), un CSIRT nacional (incidentes civiles) y un CSIRT de Defensa, cada uno con mandatos claramente definidos, funciones específicas de ciberseguridad y recursos financieros dedicados, todos ellos regidos por el principio de racionalidad. La agencia comenzó a funcionar el 2 de enero de 2025.

- Obligación de cooperar con las autoridades en la gestión de incidentes.

- Protocolos de control de daños y respuesta rápida para mitigar los impactos.

- Compromiso con la seguridad y la privacidad desde el diseño y por defecto.

- Énfasis en la seguridad de la información de conformidad con los estándares internacionales.

Del 28 al 30 de mayo de 2025, representantes gubernamentales y expertos de 10 países de la región se reunieron en Puerto Varas para poner en marcha el proyecto *"Fortalecimiento de las capacidades de ciberseguridad en América Latina y el Caribe"*[24]. Esta iniciativa financiada por la UE, que forma parte de la **Alianza Digital UE-ALC**, apoyará a Chile en el avance de sus políticas de ciberseguridad, al tiempo que compartirá experiencias para ayudar a mejorar la preparación regional en materia de seguridad digital.

La evolución de la política de ciberseguridad en Brasil y Chile muestra el reconocimiento de la seguridad digital como prioridad y motor clave del crecimiento económico.

Fuentes: Cyber Policy Portal https://cyberpolicyportal.org/ | Telefónica (Junio 2024) - Chile: país vanguardista en materia de ciberseguridad en Latinoamérica| EU-Chile (Junio 2025) ANCI lanza en la Patagonia Chilena proyecto de fortalecimiento de la ciberseguridad de América Latina y el Caribe | Brasil - Decreto nº 11.856, de 26 de Dezembro de 2023

3. El sector de las telecomunicaciones —y Telefónica como *socio estratégico*— en la protección de la infraestructura y el fortalecimiento de la seguridad y la confianza digital

Un sector de las telecomunicaciones confiable y sostenible es un socio esencial para garantizar la seguridad y la resiliencia de la sociedad. La industria de telecomunicaciones lleva mucho tiempo comprometida con el desarrollo y la implementación de medidas de seguridad robustas para proteger sus activos, clientes y servicios[25].

Más allá de esta responsabilidad fundamental, utiliza su amplia experiencia y sus capacidades técnicas para desempeñar un papel clave en el fortalecimiento de la seguridad de todos los sectores y de la administración pública. Al mismo tiempo, actúa como motor de innovación, fomentando la adopción de tecnologías digitales de vanguardia y mejores prácticas operativas, incluyendo la computación en la nube, la inteligencia artificial o las tecnologías cuánticas.

Con décadas de experiencia, Telefónica está en una posición privilegiada para ayudar a gobiernos, empresas y a la sociedad en su conjunto a fortalecer su resiliencia.

A. El valor de proteger las infraestructuras estratégicas

Las redes de telecomunicaciones resilientes son cruciales para los consumidores, las empresas y los gobiernos, ya que las comunicaciones digitales sustentan servicios esenciales como la respuesta a emergencias, los pagos digitales, la asistencia sanitaria, el funcionamiento de sectores críticos, la conectividad de la red energética o la protección de datos sensibles.

El sector de las telecomunicaciones desempeña un papel fundamental en este esfuerzo, realizando importantes inversiones para reforzar la seguridad y la resiliencia de sus infraestructuras[27]. Esto incluye la aplicación de estrictos requisitos de seguridad, de mejores prácticas en la cadena de suministro[28], la minimización de los puntos únicos de fallo y el establecimiento de procesos, herramientas y formación sólidos para apoyar la resiliencia operativa.

A pesar de su papel fundamental en securizar las redes, las contribuciones positivas del sector a menudo pasan desapercibidas, especialmente en un momento en el que se enfrenta a importantes retos de inversión para cumplir los objetivos de conectividad. Una inversión inadecuada en seguridad y resiliencia dejaría las redes más vulnerables a las amenazas, lo que debilitaría tanto las capacidades operativas del sector, como los servicios que dependen de ellas.

La imposición de nuevas obligaciones regulatorias que trascienden las consideraciones de mercado, sin un análisis exhaustivo de la relación coste-beneficio, ni una financiación adecuada —como se observa en el enfoque del sector energético respecto a la resiliencia—, podría incrementar de forma significativa los costes y comprometer aún más la sostenibilidad a largo plazo de los operadores de telecomunicaciones.

> **Las infraestructuras críticas, como las redes de telecomunicaciones y los servicios digitales, son de suma importancia para muchas funciones esenciales de nuestras sociedades y, por lo tanto, son objetivo de los ciberataques**
>
> *Reunión informal de ministros de Telecomunicaciones Nevers, 9 de marzo de 2022*[26]

CUADRO 3

GOBERNANZA DE LA SEGURIDAD DIGITAL EN TELEFÓNICA

Telefónica entiende **la seguridad**[29] como un concepto integral cuyo objetivo es preservar los activos, los intereses y los objetivos estratégicos, garantizando su integridad y protegiéndolos de posibles amenazas. Todos los mercados en los que opera Telefónica cuentan con una organización de seguridad local, coordinada por el área global de seguridad e inteligencia.

La seguridad integral abarca:

- Seguridad física y operativa (de personas y bienes)
- Seguridad digital
- Continuidad del negocio
- Prevención del fraude
- Seguridad de la cadena de suministro
- Cualquier otra área o función relevante cuyo objetivo sea la protección corporativa frente a posibles daños o pérdidas.

A su vez, **la seguridad digital** abarca la seguridad de la información y la ciberseguridad, y se aplica a los medios, sistemas, tecnologías y elementos que conforman la red y los sistemas de información. Para satisfacer las necesidades de información de las partes interesadas, de forma clara, concisa y accesible, Telefónica ofrece una sección dedicada a la «Seguridad» dentro de su Centro de Transparencia Global, disponible en el sitio web[30]. Esta sección también permite informar sobre vulnerabilidades o amenazas que podrían afectar a la infraestructura tecnológica de Telefónica.

La protección temprana de los activos de Telefónica se logra mediante la definición de políticas de seguridad basadas en estándares internacionales y la implementación de arquitecturas de seguridad robustas adaptadas al entorno empresarial. Además, el enfoque de Telefónica en **materia de ciberdefensa** se basa en un modelo integral y proactivo que aprovecha las capacidades avanzadas de la empresa en áreas clave:

- **Anticipación**. Telefónica adopta una estrategia basada en la ciberinteligencia y centrada en la proactividad y la previsión. Mediante la identificación continua de tendencias emergentes, amenazas y patrones de actividad sospechosos, la empresa mejora la detección temprana de brechas. La integración de tecnología avanzada y conocimientos especializados garantiza la identificación oportuna de los riesgos.

- **Prevención**. Equipos internos de expertos dedicados, como Red Team, buscan activamente vulnerabilidades digitales para identificar y mitigar los riesgos antes de que puedan ser explotados.

- **Detección y respuesta**. Telefónica mantiene una capacidad de respuesta rápida y eficaz ante incidentes a través de una red de equipos de respuesta a incidentes de seguridad informática (CSIRT). Estos equipos se coordinan para gestionar los incidentes de seguridad de manera eficiente, minimizando su impacto. También colaboran con CSIRT y CERT nacionales e internacionales, tanto del sector público como del privado, reforzando la resiliencia global en materia de ciberseguridad.

El fortalecimiento progresivo de las capacidades y recursos de seguridad de Telefónica se ha complementado con la decisión de desarrollar internamente capacidades específicas en los campos de la criptografía, la ciberinteligencia y la ciberdefensa.

El sólido modelo de gobernanza de Telefónica, que combina un enfoque *top-down* y *bottom-up*, garantiza que la ciberseguridad sea abordada como un componente fundamental de su estrategia empresarial y sus operaciones.

Fuentes: Telefónica – Centro de Transparencia de Seguridad Global - www.telefonica.com/es/centro-global-de-transparencia/seguridad/ | Telefónica - Ciberseguridad www.telefonica.com/es/nosotros/politicas-publicas-y-regulacion/posicionamiento/ciberseguridad/

CUADRO 4

CONSTRUYENDO UNA CULTURA DE CIBERSEGURIDAD: TELEFÓNICA ALEMANIA

La ciberseguridad se considera a menudo el dominio de especialistas que trabajan de forma aislada, pero la verdadera resiliencia depende de todos los empleados[31]. El concepto del «*eslabón más débil*» ilustra que incluso las mejores defensas pueden fallar si las prácticas cotidianas de toda la organización no se ajustan a las normas básicas de seguridad digital.

En Telefónica, estamos fomentando una cultura que prioriza la seguridad en toda la empresa. Nuestro enfoque combina la concienciación continua, la formación personalizada y formatos de participación modernos para ayudar a todo el personal a adoptar comportamientos seguros. Desde el aprendizaje autónomo en la intranet y en *hubs* de conocimiento, hasta las presentaciones interactivas impartidas por nuestros expertos en seguridad, nuestro objetivo es hacer que la ciberseguridad sea relevante, práctica y accesible para todos.

Para involucrar aún más a los empleados, Telefónica ha introducido formatos como el ***Security Arena***, un evento presencial que combina minijuegos y debates, así como un juego basado en navegador que explora las tácticas de ingeniería social. Para la dirección, los ejercicios de simulación ayudan a poner a prueba y perfeccionar los procesos y las responsabilidades. Las personas siguen siendo uno de nuestros recursos más importantes. Al ofrecer diversos formatos de aprendizaje, fomentar la comunicación abierta y reforzar la responsabilidad compartida, Telefónica está creando una cultura de ciberseguridad que apoya la innovación y la resiliencia a largo plazo.

Como refuerzo de esta base cultural, a principios de 2024 Telefónica Alemania constituyó un equipo virtual e interdisciplinario de inteligencia sobre amenazas. Este equipo analiza los principales riesgos geopolíticos y de ciberseguridad, y elabora el *Radar de Inteligencia sobre Amenazas* (edición más reciente 2024-2025), que ofrece un panorama actualizado.

Al priorizar la concienciación, la formación y la comunicación interna, Telefónica Alemania impulsa una cultura positiva de ciberseguridad que capacita a los empleados para actuar como la primera línea de defensa.

Fuentes: UK National Cybersecurity Centre - Cyber Security Toolkit for Boards | Telefónica Germany - Threat Intelligence Radar 2024–2025

CUADRO 5

PROTECCIÓN DE CABLES SUBMARINOS: TELXIUS

A la luz del creciente número de amenazas híbridas, incluidos los recientes incidentes en el mar Báltico y mar del Norte, los cables submarinos[32] se perfilan como un activo esencial.

Telxius[33] aplica un modelo de seguridad integral que garantiza una gestión eficaz mediante políticas actualizadas, una combinación de sólidas medidas físicas y de ciberseguridad, auditorías periódicas y una evaluación continua de las prácticas de seguridad. Las normas internas se ajustan a los marcos legales y los estándares internacionales, y se complementan con programas de formación y sensibilización de los empleados.

En este sentido, Telxius garantiza la resiliencia de sus estaciones de amarre de cables submarinos mediante la aplicación de un Sistema de Gestión de la Continuidad del Negocio de acuerdo con las normas y directrices del Grupo Telefónica basadas en ISO 22301. También mantiene un sistema de gestión integrado activo para sus principales estaciones de amarre, lo que garantiza la aplicación de las mejores prácticas en línea con la norma ISO 27001 para la gestión de la seguridad de la información, la norma ISO 14001 para la gestión medioambiental y la norma ISO 50001 para la eficiencia energética.

La continuidad de negocio se refuerza mediante la diversificación de rutas, la mejora de la seguridad física, planes de continuidad sólidos, pruebas periódicas y procedimientos de recuperación ante desastres. La gestión de crisis incluye planes de respuesta estructurados, personal capacitado, canales de comunicación definidos y evaluaciones posteriores a la crisis. La seguridad física y del personal se aborda mediante controles de acceso, vigilancia, protección de activos, protocolos de emergencia y la promoción de un entorno de trabajo seguro.

En materia de ciberseguridad, Telxius adopta un enfoque multicapa —que abarca datos, aplicaciones, dispositivos, redes y perímetros— y aprovecha la inteligencia artificial y el aprendizaje automático para la detección de amenazas en tiempo real. Las medidas incluyen cifrado extremo-a-extremo, segmentación de red, protección de dispositivos corporativos y salvaguardias contra el robo de credenciales, lo que garantiza la seguridad de las comunicaciones, la protección de los datos y la mitigación de riesgos.

Aumentar la resiliencia mediante una mejor coordinación

Existe una necesidad urgente de actuar de forma coordinada y mantener un diálogo transfronterizo eficaz para proteger esta infraestructura crítica. El Plan de Acción de la UE sobre la seguridad de los cables submarinos esboza un marco destinado a reforzar la resiliencia y la seguridad de los cables submarinos[34]. La participación de representantes del sector será fundamental para garantizar una respuesta práctica integral.

Un enfoque armonizado del ecosistema de cables submarinos debe alinear los objetivos de seguridad con la viabilidad operativa, los modelos de negocio sostenible y el uso estratégico de la financiación pública. Este enfoque debe basarse en las mejores prácticas basadas en el riesgo, desarrolladas en estrecha colaboración con los socios del sector.

El estudio de caso muestra cómo la colaboración público-privadas son esenciales para proteger infraestructuras estratégicas globales, como los cables submarinos, frente a una amplia gama de amenazas físicas y digitales.

Fuentes: Telxius, proveedor líder mundial de conectividad | Telefónica (Diciembre 2024) - La infraestructura invisible que mueve el mundo digital: cables submarinos

B. Apalancando la experiencia en protección de infraestructuras digitales para reforzar la protección de todos los sectores

El sector de las telecomunicaciones desempeña un papel transversal clave en la seguridad de una amplia gama de sectores. Gracias a su experiencia, su mano de obra cualificada, sus amplias redes de colaboración y sus sólidas capacidades operativas no solo protege su propia infraestructura, sino también refuerza la resiliencia de empresas, administraciones públicas y la sociedad. Con una profunda experiencia técnica y una alta capacidad operativa, el sector contribuye de manera crítica a la seguridad de los servicios en los ámbitos de la defensa, la banca, la energía, la sanidad, las finanzas, el transporte, la industria manufacturera y otros sectores clave.

El creciente volumen y coste del fraude online ha atraído a grupos delictivos organizados internacionales, cuya identificación y procesamiento resulta cada vez más complejo. En su lucha contra el fraude, los operadores invierten recursos significativos para identificar, filtrar y bloquear el tráfico fraudulento. Sin embargo, estos delitos suelen involucrar cadenas de actuación sofisticadas y organizadas, por lo que las medidas técnicas por sí solas no resultan suficientes. A pesar de los esfuerzos del sector, los delincuentes continúan eludiendo las defensas técnicas y explotando el comportamiento humano mediante la ingeniería social.

CUADRO 6

SERVICIOS DE SEGURIDAD DE TELEFÓNICA PARA EMPRESAS Y AAPP

Telefónica ofrece un portafolio integral de soluciones de ciberseguridad. Como proveedor de servicios de seguridad gestionados (MSSP) de confianza, Telefónica Tech se centra en la prevención, detección y respuesta ágil y eficaz, con el objetivo de mitigar ciberataques, proteger a las empresas y a los servicios digitales públicos, y fortalecer la ciberresiliencia en diversos sectores y geografías. Telefónica también ofrece protección especializada para los sistemas de tecnología operativa (OT), responsables de regular procesos industriales y que requieren enfoques de ciberseguridad personalizados, adaptados a sus arquitecturas y limitaciones específicas. Esta labor está liderada por un equipo multidisciplinar de expertos en ciberseguridad, altamente cualificados y respaldados por una sólida trayectoria en la prestación de servicios a terceros.

Las capacidades 24/7 de Telefónica Tech se basan en un Centro de Operaciones Digitales (DOC) y en Centros de Operaciones de Seguridad (SOC) de última generación, estratégicamente ubicados en Europa y América. Con ello, ofrece una protección global respaldada por experiencia local, acompañando a sus clientes. Su cartera de servicios, flexible y en constante evolución, combina tecnologías propias con las mejores soluciones de terceros para garantizar una defensa integral frente a un panorama de riesgos cada vez más complejo.

Las capacidades de ciberseguridad de Telefónica Tech cuentan con un amplio reconocimiento entre clientes de diversos sectores, fortalecidas por una sólida red de socios estratégicos y avaladas por los principales analistas del mercado. Además de sus servicios de seguridad esenciales, Telefónica ofrece soluciones avanzadas para reforzar la protección y apoyar la gestión de riesgos. Asimismo, publica periódicamente informes y análisis de inteligencia en ciberseguridad que aportan información clave sobre amenazas y tendencias emergentes.

La amplia gama de servicios de seguridad que Telefónica ofrece a empresas y administraciones públicas la consolida como un socio estratégico en la construcción de un ecosistema digital seguro y resiliente.

Fuentes: Telefónica Tech | Telefónica Tech – Servicios de ciberseguridad | Telefónica Tech – Casos prácticos | Telefónica Tech (Julio 2025) – Informe sobre el estado de la seguridad 2025 H1 | Telefónica Tech (2025) - Ciberresiliencia en infraestructuras críticas | Ciberseguro de Telefónica | Telefónica Empresas - Servicios de Ciberseguridad y Seguridad Tecnológica para Empresas | Telefónica Empresas - Servicios de Ciberseguridad y Seguridad Tecnológica para Empresas

Telefónica Tech

Proveedor global de servicios gestionados de seguridad con un portafolio completo de capacidades

~ 5,5M B2B clientes
Sobre el portfolio de servicios de Telefónica Tech

~7.000 profesionales
Trabajan en Telefónica Tech

24x7 servicio de soporte
1 Centro de Operaciones Digitales (DOC) con 2 ubicaciones y una red global de SOCs

+50 tecnologías
de ciberseguridad gestionadas en nuestros SOCs

+6.500 certificaciones
de socios tecnológicos o terceros

Top-tier partner
Máximo nivel de *partnership*

Experiencia, fiabilidad e innovación continua

RECONOCIMIENTO INDUSTRIA

AVASANT · IDC Analyze the Future · GlobalData. · FORRESTER

RECONOCIMIENTO CLIENTES

Telefónica - CASOS DE ÉXITO
Casos de éxito

ESCALA TÉCNICA

+290k Amenazas identificadas

+350k Tickets gestionados por año

+370k EDR agentes desplegados

+50k h. Pentesting y Red Team

+4.150 TB Logs ingresados en SIEM

HIGHEST LEVEL PARTNERSHIP

aws · CHECK POINT · CROWDSTRIKE · FORTINET · Microsoft · paloalto NETWORKS

Fuentes: Telefónica Tech | Telefónica Tech – Servicios de ciberseguridad | Telefónica Tech – Casos prácticos | Telefónica Tech (Julio 2025) – Informe sobre el estado de la seguridad 2025 H1 | Telefónica Tech (2025) - Ciberresiliencia en infraestructuras críticas | Ciberseguro de Telefónica | Telefónica Empresas - Servicios de Ciberseguridad y Seguridad Tecnológica para Empresas | Telefónica Empresas - Servicios de Ciberseguridad y Seguridad Tecnológica para Empresas

CUADRO 7

EL PAPEL DE TELEFÓNICA EN EL FORTALECIMIENTO DE LAS CAPACIDADES TECNOLÓGICAS DEL SECTOR DE LA DEFENSA

Ninguna capacidad de defensa puede operar de forma segura sin una infraestructura digital avanzada y resiliente, ni sin socios tecnológicos de confianza. En la Feria Española de Defensa y Seguridad (FEINDEF 2025)[35], Telefónica presentó su estrategia tecnológica integral para reforzar las capacidades estratégicas, operativas y tácticas, al tiempo que fortalece la seguridad en todo el sector de la defensa. Las operaciones militares modernas exigen comunicaciones y tecnologías de vanguardia.

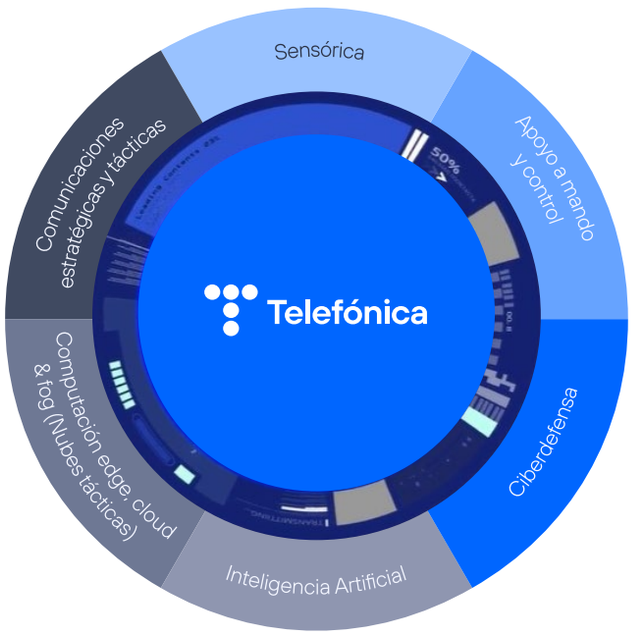
Telefónica aporta su amplia experiencia en la integración de tecnologías de defensa en ámbitos clave como la sensórica avanzada, la conectividad estratégica y táctica —incluidas las burbujas tácticas 5G[36] y el dominio del espectro—, así como en la transmisión segura de datos *quantum-safe*.

Estas capacidades se complementan con arquitecturas avanzadas de computación en la nube, en el borde (*edge*) y *fog*, esta última concebida como una capa descentralizada entre los entornos *edge* y de nube. En conjunto, facilitan la organización y gestión eficiente de la información crítica de misión.

Combinado con el procesamiento de datos potenciado por inteligencia artificial, una seguridad digital robusta, capacidades avanzadas de ciberdefensa y puestos de mando de última generación con realidad extendida, este ecosistema tecnológico integral proporciona una ventaja decisiva tanto en la protección como en la explotación estratégica de la información.

En otro ámbito relacionado, los drones se han convertido en una preocupación creciente citado en los informes de seguridad nacional[37] debido a su posible uso indebido por parte de organizaciones terroristas o criminales. En respuesta, Telefónica ofrece una amplia gama de soluciones, desde sistemas '*drone-in-a-box*' hasta tecnologías avanzadas de contramedidas contra drones, todas diseñadas para fortalecer la seguridad del espacio aéreo y garantizar una mitigación eficaz de las amenazas[38].

Integración de tecnologías para la superioridad de la información



Paralelamente, Telefónica impulsa la innovación tanto internamente como a través de modelos de innovación abierta, mediante Wayra, su vehículo de inversión corporativa. La compañía ha establecido diversos acuerdos, entre ellos con el Acelerador de Innovación en Defensa para el Atlántico Norte (DIANA) de la OTAN, integrando seis de sus laboratorios en la red internacional de centros de pruebas de DIANA. Estos laboratorios se especializan en áreas de vanguardia como tecnologías cuánticas, redes de próxima generación, Internet de las cosas (IoT) y ciberseguridad.

La colaboración de Telefónica con el sector de la defensa pone de relieve el papel fundamental de la innovación y la experiencia tecnológica del sector privado en el fortalecimiento de la seguridad nacional y de las capacidades de defensa.

Fuentes: Telefónica Defensa y Seguridad | Telefónica (Mayo 2025)- Feria de defensa y seguridad FEINDEF: tecnología, talento e innovación

CUADRO 8

LUCHA CONTRA EL FRAUDE: ELEVANDO LOS ESTÁNDARES Y LA CONCIENCIACIÓN

El incremento del fraude es una preocupación creciente, lo que ha llevado a los actores del ecosistema digital a reforzar sus esfuerzos para combatir esta amenaza. Los delincuentes continúan explotando el factor humano mediante técnicas de ingeniería social, mientras que el auge de la delincuencia transnacional facilitada por tecnologías digitales dificulta cada vez más la labor de las fuerzas del orden. Telefónica ha respaldado de manera constante la lucha contra el fraude mediante diversas iniciativas en todas las regiones. A continuación, se presentan algunos ejemplos representativos.

Iniciativa GSMA Open Gateway[39]

Los operadores han desarrollado diversas API (interfaces de programación de aplicaciones) de red, diseñadas para mejorar la seguridad digital y combatir el fraude, incluyendo funcionalidades como estado del dispositivo, ubicación, intercambio de SIM y detección de fraude. Estas API permiten a desarrolladores y socios crear capas inteligentes de autenticación, verificación y protección de clientes dentro de las redes móviles. Gracias a esta innovación, empresas como instituciones financieras pueden reforzar la autenticación de usuarios y prevenir el fraude de manera más eficaz.

ESPAÑA

En febrero de 2025, el Gobierno español, con amplio consenso del sector, aprobó una Orden Ministerial para combatir el fraude en llamadas de voz y SMS[40]. Esta normativa establece medidas para enfrentar las estafas de suplantación de identidad, en las que se modifica el número de origen para que el destinatario vea un número de confianza, un número conocido o el de una institución legítima.

El plan contempla diversas medidas técnicas: bloquear los números no autorizados, como aquellos no asignados a ningún servicio, operador o cliente; impedir la recepción de números españoles falsificados procedentes de llamadas o mensajes internacionales, salvo para usuarios que se encuentren legítimamente en itinerancia en el extranjero; crear un registro nacional de identificadores alfanuméricos de remitentes, gestionado por la Comisión Nacional de los Mercados y la Competencia (CNMC), para evitar la suplantación de entidades legítimas como bancos u organismos públicos; y prohibir el uso de números móviles para servicios de atención al cliente o telemarketing no solicitado, exigiendo que las empresas empleen números geográficos o líneas 800/900, ahora autorizadas para llamadas salientes.

BRASIL

Brasil recurre cada vez más a la identificación biométrica, incluida la biometría conductual, en diversos sectores como seguridad social, banca, telecomunicaciones y servicios gubernamentales, para combatir el fraude. Al verificar identidades con precisión, los sistemas biométricos contribuyen a detectar y prevenir delitos como el robo de identidad, la apropiación de cuentas y las transacciones no autorizadas

Vivo también ofrece una variedad de productos y servicios para combatir las estafas. Por ejemplo, *Vivo Anti-Spam*[41], un servicio gratuito para usuarios móviles, analiza el comportamiento de las llamadas en toda la red y utiliza algoritmos inteligentes para bloquear llamadas no deseadas. Además, la plataforma *Modo Seguro*[42] permite a los usuarios bloquear remotamente su dispositivo y borrar los datos en caso de robo o pérdida.

REINO UNIDO

Virgin Media O2 (VMO2) adopta un enfoque proactivo y multifacético para combatir el fraude, combinando tecnología, colaboración sectorial y concienciación de los clientes. Como miembro de la *Government's Telecoms Fraud Sector Charter* del Reino Unido, VMO2 respalda los esfuerzos conjuntos para mejorar la detección de llamadas y SMS fraudulentos, prevenir el uso indebido de números y facilitar el intercambio de información con las fuerzas del orden. En el ámbito del consumidor, la compañía ha lanzado *DAISY*[43], una innovadora campaña de concienciación que emplea números de clientes simulados para atraer y analizar llamadas fraudulentas, reduciendo así la probabilidad de que los clientes reales sean afectados. Combinadas con herramientas como el filtrado de SMS basado en IA y la mejora de la selección de llamadas, estas iniciativas reflejan el firme compromiso de VMO2 con la protección de los usuarios y la reducción del fraude en todo el ecosistema de telecomunicaciones.

Un enfoque integral para combatir el fraude

La cooperación y un enfoque integral son esenciales en la lucha contra el fraude. Para implementar herramientas avanzadas de manera eficaz, las empresas necesitan flexibilidad y acceso oportuno a los datos relevantes, sin que políticas de protección de datos excesivamente restrictivas obstaculicen este esfuerzo. Es fundamental abordar toda la cadena de valor, priorizar la concienciación[44] de los usuarios y la aplicación de la ley contra los criminales[45]. La cooperación intersectorial resulta clave para alcanzar objetivos colectivos y requiere un enfoque flexible, pragmático y con visión de futuro, que evite medidas excesivamente prescriptivas dada la naturaleza dinámica del fraude.

El enfoque proactivo de Telefónica para combatir el fraude, basado en tecnología avanzada y experiencia, subraya la importancia de un esfuerzo colaborativo, tanto público como sectorial, para fortalecer la confianza digital.

Fuentes: UK VMO2 (Mayo 2025) - New report calls for overhaul of fraud policing as majority of police believe officers lack the resources and skills to investigate the crime | INCIBE. Qué hacer si eres víctima de un fraude | GSMA – GSMA Open Gateway | Gobierno de España (Febrero 2025) - Estafas telefónicas y por SMS: protección contra el fraude | VIVO – Antispam service | Vivo (Mayo 2025) - Vivo Seguro | UK VMO2 (Noviembre 2024) - O2 unveils Daisy, the AI granny wasting scammers' time

C. Un sector innovador clave en tecnologías avanzadas y catalizador de su adopción

El sector de las telecomunicaciones es un motor clave de la innovación, que adopta e integra continuamente tecnologías digitales de vanguardia y las mejores prácticas operativas. Esto abarca desde la computación en la nube y la inteligencia artificial hasta tecnologías cuánticas emergentes, no solo para mejorar su propia eficiencia, resiliencia y calidad de servicio, sino también para impulsar una transformación digital segura en todos los sectores industriales y servicios públicos.

> **La tecnología será la principal característica de la competencia en el nuevo entorno geopolítico. Un conjunto reducido de tecnologías críticas y fundamentales, como la inteligencia artificial, la cuántica, la biotecnología, la robótica y la hipersónica, son elementos clave tanto para el crecimiento económico a largo plazo como para la preeminencia militar**
>
> *Libro blanco sobre la preparación de la defensa europea para 2030 - Marzo 2025*

CUADRO 9

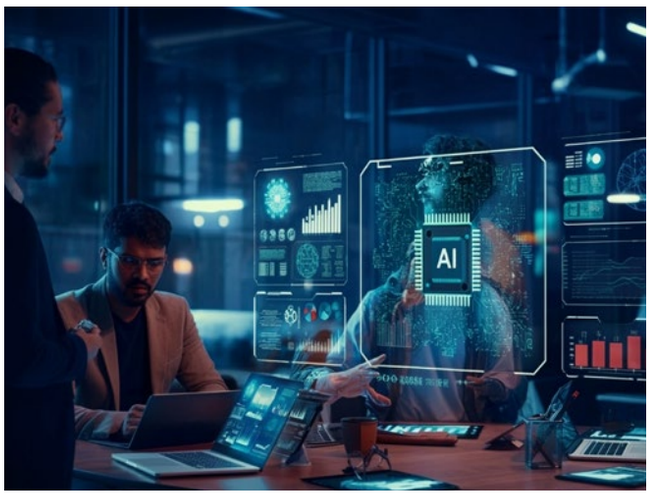
EL FUTURO DE LOS SOCs: POTENCIANDO LA SEGURIDAD DIGITAL CON IA

Telefónica Tech lidera una transformación significativa en la manera en que las organizaciones afrontan los desafíos de la ciberseguridad, impulsando la evolución de los Centros de Operaciones de Seguridad (SOC) mediante el **uso estratégico de inteligencia artificial (IA)** y la automatización.

Frente a un panorama digital cada vez más complejo y hostil y caracterizado por infraestructuras híbridas que combinan sistemas locales y múltiples entornos de nube pública y privada, la proliferación de dispositivos conectados y una escasez crítica de talento especializado, Telefónica Tech promueve una arquitectura SOC moderna, eficiente y anticipativa.

Con su solución *NextDefense*[46], la compañía integra capacidades avanzadas como análisis del comportamiento, gestión automatizada de alertas e inteligencia sobre amenazas, lo que permite reducir significativamente los falsos positivos, priorizar de manera más eficaz los incidentes críticos y acelerar los tiempos de respuesta.

Este enfoque brinda a las organizaciones una visibilidad completa de todo su ecosistema digital, incluidos los entornos multinube y de tecnología operativa (OT), facilitando la detección temprana de riesgos, el análisis contextual de amenazas y la mitigación preventiva. Además, Telefónica Tech complementa sus capacidades tecnológicas con servicios especializados, como búsqueda de amenazas, evaluación de posicionamiento en ciberseguridad y consultoría estratégica, ayudando a las empresas a definir estrategias de seguridad personalizadas que optimizan los recursos y reducen los costes operativos.



Al integrar plenamente la inteligencia artificial (IA) en el SOC[47], se automatizan las tareas repetitivas y de bajo valor, liberando a los especialistas para centrarse en acciones de mayor impacto. La combinación de IA y automatización permite a las organizaciones detectar y neutralizar anticipadamente las amenazas, aumentando la velocidad de detección y los tiempos de respuesta, y transformando un enfoque reactivo en uno preventivo. Los sistemas de IA analizan grandes volúmenes de datos para identificar anomalías y riesgos emergentes en tiempo real. Además, el aprendizaje automático potencia estas capacidades al adaptarse continuamente a nuevas amenazas, haciendo que las defensas sean más eficientes y adaptables.

La integración de la inteligencia artificial (IA) en los Centros de Operaciones de Seguridad (SOC) será fundamental para afrontar el creciente volumen y la complejidad de las ciberamenazas facilitando una detección y respuesta más rápidas y eficaces.

Fuentes: Telefónica Tech – Next Defense | Telefónica Tech - El SOC del futuro: cómo la IA y la automatización están redefiniendo el futuro | Telefónica Tech - Automatización en ciberseguridad con IA para anticipar y neutralizar amenazas

CUADRO 10

OPORTUNIDADES Y AMENAZAS CUÁNTICAS

Las tecnologías cuánticas abrirán oportunidades transformadoras, permitiendo avances en capacidad de cómputo, comunicaciones ultraseguras y una precisión de medición sin precedentes. Sin embargo, el desarrollo de la computación cuántica presenta una seria amenaza, en particular mediante estrategias de «*almacenar ahora*, descifrar después» que buscan explotar **vulnerabilidades criptográficas**. Para mitigar este riesgo, la contramedida más eficaz a corto plazo es la adopción de la criptografía poscuántica (PQC) o de sistemas criptográficos híbridos.

En este contexto, la declaración conjunta[48] firmada en 2024 por 18 Estados miembros de la UE instaba a acelerar la transición hacia la criptografía poscuántica, en línea con la Recomendación de la Comisión Europea[49]. Estas iniciativas se reforzaron con la publicación, en junio de 2025, de la Hoja de Ruta para la Transición a la Criptografía Poscuántica[50].

En 2024 se publicaron las primeras normas. En medio de los esfuerzos de estandarización en diferentes regiones, el **concepto de criptoagilidad**[51] —la capacidad de adaptar dinámicamente las soluciones de seguridad para incorporar nuevos estándares o algoritmos de cifrado— está cobrando una relevancia creciente para la resiliencia.

El papel de Telefónica en el ámbito cuántico

Telefónica ha creado un Centro de Excelencia en Tecnologías Cuánticas[52], desde el cual impulsa tanto la investigación como la aplicación práctica. La compañía ya está avanzando hacia la construcción de redes cuánticamente seguras[53], incorporando una capa adicional de protección mediante tecnologías resistentes a la computación cuántica que combinan la criptografía tradicional con la criptografía poscuántica (PQC). Más allá del laboratorio, Telefónica también está avanzando en tecnologías de futuro como la distribución de claves cuánticas (QKD), que ha implementado operativamente en la red EuroQCI[54], contribuyendo a acelerar su madurez. Este esfuerzo se ha llevado a cabo en estrecha colaboración con instituciones académicas y de investigación líderes, así como en asociación con los principales fabricantes de equipos de red.

Telefónica también colabora con terceros. En el MWC25 se presentaron diversos casos de uso[55], que abarcan aplicaciones en ámbitos como la sanidad[56], la defensa o los servicios públicos, junto con iniciativas más amplias para crear un ecosistema cuántico sólido, junto a fabricantes de computación cuántica o con la colaboración con la Diputación Foral de Vizcaya[57].

La importancia de la financiación

La colaboración y los bancos de pruebas son fundamentales para desarrollar servicios seguros e innovadores. La mejora de la resiliencia debe estar impulsada por el mercado y respaldada por un sector de las telecomunicaciones sostenible. Cuando los incentivos privados resultan insuficientes, la financiación pública específica puede cubrir las carencias de inversión, mientras que la contratación pública se convierte en una palanca clave para acelerar la adopción de tecnologías estratégicas a largo plazo.

La temprana implicación de Telefónica en las tecnologías cuánticas la posiciona a la vanguardia, tanto en la preparación frente a los riesgos de seguridad como en el aprovechamiento de las nuevas oportunidades que traerá consigo la computación cuántica.

Fuentes: EU Commission (Abril 2024) - Recommendation on Post-Quantum Cryptography | EU Member States declaration (Nov. 2024) - Securing tomorrow today: transitioning to Post-Quantum Cryptography. | EU Commission (Junio 2025)- A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography |Telefónica Tech (Junio 2025) – Preparación estratégica para la criptografía poscuántica | Telefónica (Marzo 2025) - Telefónica crea un Centro de Excelencia dedicado a las tecnologías cuánticas | Telefónica - Quantum-Safe Networks | Telefónica (Octubre 2024) - QKD, claves criptográficas y redes cuánticas |Telefónica (Marzo 2025) - Telefónica se adelanta a los desafíos cuánticos con una innovadora demo en el MWC |Telefónica (Marzo 2025) - Telefónica y Vithas prueban el blindaje frente a ataques cuánticos en dos hospitales |Telefónica (Marzo 2025) - Socio del Gobierno de Vizcaya para el desarrollo de su estrategia industrial de tecnología cuántica

4. *Recomendaciones* de políticas públicas para un mundo más seguro, innovador y confiable

Las regiones están trabajando para mejorar la seguridad, fortalecer sus capacidades, impulsar la resiliencia social, realizar inversiones significativas y reducir las dependencias estratégicas. En este contexto, resulta fundamental contar con un sector de las telecomunicaciones sólido y sostenible, apoyado en operadores de confianza que actúen como socios tecnológicos clave.

Sin embargo, ni siquiera un sector privado fuerte puede afrontar estos retos por sí solo. Para desbloquear plenamente el potencial de las ambiciones digitales y de seguridad se requiere: un marco regulador racionalizado, proporcionado y coherente; apoyo específico para el desarrollo de un ecosistema competitivo en tecnologías de red estratégicas; financiación pública que considere la seguridad y la resiliencia como bienes públicos; y el uso estratégico de la contratación pública. Igualmente importantes son el desarrollo de habilidades digitales en ciberseguridad, una coordinación y cooperación más estrecha entre autoridades, un compromiso sostenido con el sector privado y un incremento de recursos y cooperación internacional para combatir el fraude y la ciberdelincuencia.

Las ambiciones estratégicas deben estar respaldadas por un entorno propicio. Un marco coordinado, simplificado y adecuadamente financiado no es simplemente una opción: constituye un requisito para lograr los objetivos de resiliencia y seguridad. A continuación, se presentan una serie de recomendaciones clave para promover un mundo digital más seguro y confiable.

> **Una preparación sólida no es gratuita. Las inversiones en preparación implican costes, pero estos se ven compensados por las ganancias a largo plazo en resiliencia, reducción de interrupciones, menores gastos de recuperación y competitividad a largo plazo**
>
> *Estrategia de la Unión Europea para la Preparación – March 2025*

A. Garantizar un sector de telecomunicaciones sólido y sostenible, apoyado en operadores de confianza que actúen como socios tecnológicos estratégicos a nivel regional

Ninguna capacidad puede operar de manera segura sin una infraestructura digital fiable y socios estratégicos con liderazgo tecnológico. En este contexto, el sector de las telecomunicaciones juega un papel fundamental, no solo como facilitador de la conectividad, sino también como garante de la autonomía estratégica. La sostenibilidad económica del sector se convierte, por tanto, en una piedra angular de la resiliencia digital global. Para fortalecer este rol, resultan esenciales las siguientes medidas políticas:

- **Reconocer la importancia estratégica del sector de las telecomunicaciones** como pilar para reforzar la resiliencia de todas las industrias.
- **Reconocer los costes asociados a mantener una infraestructura de telecomunicaciones segura y resiliente**, así como capacidades operativas y respuesta rápida ante incidentes, en el debate más amplio sobre el futuro de la conectividad.
- **Adoptar un marco regulatorio modernizado y una política de competencia con visión de futuro que refuerce los cimientos del sector**, permitiendo la escalabilidad y la inversión a largo plazo necesarias para garantizar la seguridad y la resiliencia frente a las crecientes amenazas.

B. Impulsar la inversión en seguridad, resiliencia y tecnologías de doble uso mediante la combinación de financiación pública, incentivos fiscales específicos y la utilización estratégica de la contratación pública

El sector privado no puede asumir por sí solo la responsabilidad de proporcionar bienes públicos, ni financiar la resiliencia más allá de lo que sea comercialmente razonable. Los gobiernos deben participar mediante políticas industriales eficaces, inversiones públicas y el uso estratégico de la contratación pública:

- **Incrementar la financiación pública y ofrecer incentivos fiscales** para respaldar los esfuerzos en materia de defensa, ciberseguridad y resiliencia, de forma similar a las medidas aplicadas en otros sectores estratégicos como el energético, con el fin de cerrar la brecha de inversión.
- **Apoyar el despliegue de tecnologías esenciales** que impulsen la innovación y la resiliencia a largo plazo, incluyendo la inteligencia artificial y las soluciones cuánticas seguras.
- **Reforzar la contratación pública como palanca estratégica para impulsar la innovación tecnológica y la resiliencia**, priorizando no solo reducción de costes, sino también la seguridad, la adopción de tecnologías europeas y el valor a largo plazo.

.

C. Implementar un marco regulatorio y de estándares de seguridad simplificado, proporcionado, coherente, basado en riesgos, desarrollado en estrecha colaboración con el sector privado

Reducir la complejidad normativa, fomentar las mejores prácticas y asegurar un marco coherente, proporcionado y predecible, acompañado de una mentalidad que confíe en el sector privado y le otorgue autonomía, será fundamental para alcanzar un éxito duradero. Para avanzar en este objetivo, los responsables políticos deberían:

- **Promover las mejores prácticas en materia de ciberseguridad junto con el desarrollo de normas mínimas**, especialmente en las regiones donde no existen, organismos de supervisión independientes y marcos estratégicos con recursos suficientes que apoyen su aplicación y cumplimiento.
- **Racionalizar el panorama fragmentado de la seguridad y las obligaciones de notificación**, asegurando la igualdad de condiciones en todos los ecosistemas, priorizando la armonización con normas internacionales y revisando la interacción entre los marcos normativos y los diferentes puntos de contacto, para facilitar una asignación más eficaz de recursos.
- **Garantizar que todas las obligaciones regulatorias se basen en evidencias y riesgos, sean proporcionadas**, y vayan acompañadas sistemáticamente de análisis exhaustivos coste-beneficio y estrategias de financiación claras.

D. Fomentar el desarrollo de las competencias en materia de tecnología y ciberseguridad, al tiempo que se promueve una mayor sensibilización sobre seguridad digital para fomentar una sociedad digital más resiliente

- **Invertir en educación y formación** en todos los niveles para formar un talento sólido y capacitado en ciberseguridad y tecnología.

- **Fomentar el aprendizaje continuo y la mejora de competencias** mediante iniciativas específicas dirigidas a la población activa, especialmente en sectores críticos.

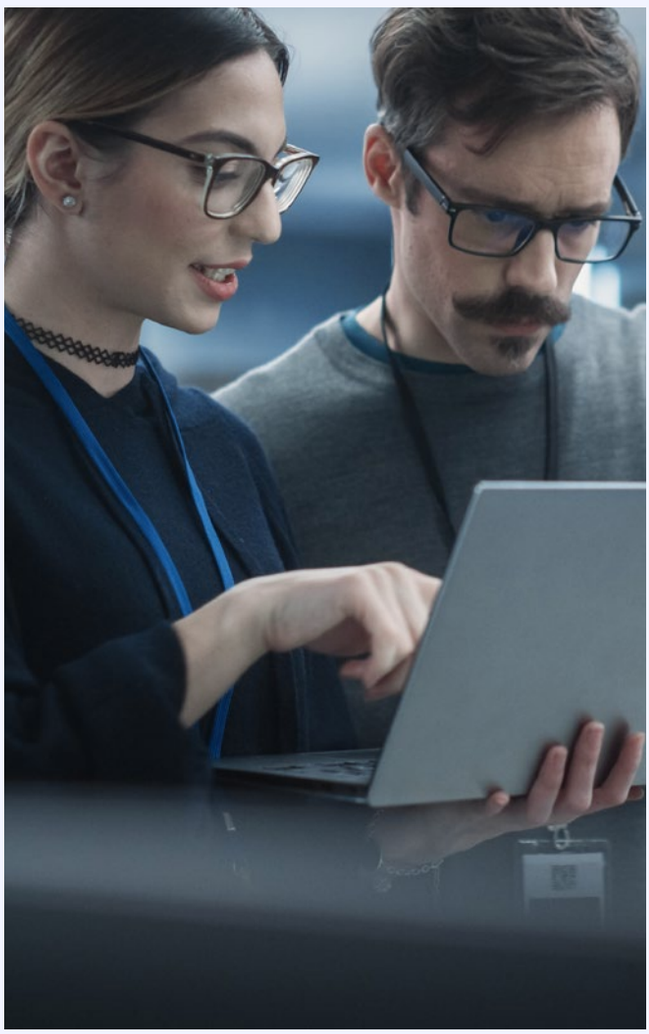
- **Apoyar campañas de sensibilización** para educar a ciudadanos y empresas, en particular pymes, sobre prácticas esenciales de ciberseguridad, riesgos digitales, fraude y buenas prácticas de seguridad online.

E. Mejorar la coordinación en materia de ciberinteligencia, defensa, disuasión y lucha contra la ciberdelincuencia, asegurando mayores recursos y una cooperación más estrecha

La ciberresiliencia es una responsabilidad compartida que demanda una comprensión precisa de los riesgos para la sociedad, así como una cooperación sólida en la lucha contra la ciberdelincuencia y el fraude.

- **Fortalecer la coordinación entre el sector público y el privado,** involucrando al sector privado desde fases iniciales en el proceso de elaboración de políticas y promoviendo la colaboración en el intercambio de información sobre ciberamenazas, la elaboración de guías y el desarrollo de capacidades, adoptando un enfoque que vaya más allá de medidas basadas en sanciones.

- **Mejorar la cooperación multilateral** para facilitar el intercambio eficaz de información sobre ciberamenazas, así como respaldar la prevención, detección, contención, investigación y enjuiciamiento de la ciberdelincuencia y el fraude, incluyendo la asignación de recursos adicionales.



5. Glosario de conceptos clave

Ciberinteligencia se refiere generalmente al proceso de recopilar, analizar y aplicar información sobre ciberamenazas para fundamentar la toma de decisiones y mejorar la ciberseguridad.

Ciberamenaza o amenaza cibernética es cualquier situación potencial, hecho o acción que pueda dañar, perturbar o afectar desfavorablemente de otra manera las redes y los sistemas de información, a los usuarios de tales sistemas y a otras personas[59].

Ciberseguridad se refiere a todas las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas.

Disuasión (*Deterrence*) es la acción de disuadir una acción o un acontecimiento mediante la generación de dudas o el temor a las consecuencias.

Incidente se refiere a todo hecho que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios ofrecidos por sistemas de redes y de información o accesibles a través de ellos.

Resiliencia es la capacidad para la prevención, la protección, la respuesta, la resistencia, la mitigación, la absorción, la adaptación y la recuperación en caso de un incidente[60]. En el sentido más amplio, es la capacidad de una organización, recurso o estructura para resistir una serie de amenazas internas y externas conocidas y futuras, soportar los efectos de una pérdida o degradación parcial de la plataforma, el sistema o el servicio, recuperarse y reanudar el servicio con la mínima pérdida razonable de rendimiento, y adoptar las lecciones aprendidas de cualquier incidente[61]. **La ciberresiliencia** va más allá de la ciberseguridad tradicional; es la capacidad de una organización para minimizar el impacto de incidentes cibernéticos significativos en sus principales metas y objetivos empresariales[62]. Reconociendo que la seguridad al 100% es inalcanzable, las organizaciones deben adoptar estrategias adaptativas y una mentalidad de «*cuándo, no si*», reconociendo que los incidentes son inevitables.

Seguridad de las redes y los sistemas de información es la capacidad de los sistemas de redes y de información de resistir, con un nivel determinado de fiabilidad, cualquier hecho que pueda comprometer la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o de los servicios ofrecidos por tales sistemas de redes y de información o accesibles a través de ellos[63].

Seguridad digital abarca la seguridad de la información y la ciberseguridad, y se aplica a los medios, sistemas, tecnologías y elementos de la red y los sistemas de información.

Servicio esencial es aquel que resulta crucial para el mantenimiento de funciones sociales vitales, las actividades económicas, la salud pública y la seguridad, o el medio ambiente.

Fuentes: Definiciones establecidas en el Reglamento (UE) 2019/881 sobre la ENISA; Directiva (UE) 2022/2557 sobre la resiliencia de las entidades críticas (CER); Directiva (UE) 2022/2555 - NIS 2 sobre medidas para un alto nivel común de ciberseguridad en toda la Unión. Definición de disuasión, traducción de *deterrence* según Oxford Languages.

6. Referencias

1. EU Commission (Octubre 2024) - Sauli Niinistö report - Safer Together: Strengthening Europe's civil and military preparedness and readiness

2. Gobierno español (2021) - Estrategia de Seguridad Nacional de España

3. Gobierno alemán (2022) - Estrategia de Seguridad Nacional alemana | Gobierno del Reino Unido (2022) - UK Cyber Security Strategy 2022-2030

4. World Economic Forum (WEF) (Enero 2025) – Global Risk report 2025

5. ENISA (Septiembre 2024) - ENISA Threat Landscape 2024

6. Fuentes Figura 1. Telefónica basado en: Checkpoint (Abril 2025)- Q1 2025 Global Cyber Attack Report. Checkpoint - The state of Cybersecurity | World Economic Forum (WEF) (Enero 2025) - Global Cybersecurity Outlook 2025 | GSMA (Febrero 2025) - Fraud and Scams: Staying Safe in the Mobile World | International Monetary Fund (IMF) (Abril 2024) - Chapter 3 Global Financial Stability Report, Cyber Risk: A Growing Concern for Macro financial Stability

7. Checkpoint (Abril 2025) - Q1 2025 Global Cyber Attack Report. Checkpoint: The state of Cybersecurity 2025

8. World Economic Forum (WEF) (Enero 2025) - Global Cybersecurity Outlook 2025

9. GSMA (Febrero 2025) - Fraud and Scams: Staying Safe in the Mobile World

10. ENISA (Noviembre 2024) - NIS Investments

11. International Monetary Fund (IMF) (Abril 2024) - Chapter 3 Global Financial Stability Report, Cyber Risk: A Growing Concern for Macro financial Stability

12. ENISA (Julio 2025) - Telecom Security Incidents 2024

13. Fuentes Figura 2. (1) World Economic Forum (WEF) (Enero 2025) - Global Cybersecurity Outlook 2025 | (2) GSMA (Febrero 2025) - Fraud and Scams: Staying Safe in the Mobile World | (3) Gartner (Diciembre 2024) – IT Key Metrics Data 2025: IT Security Measures Analysis; ENISA (Noviembre 2024) - NIS Investments | (4) Eurobarómetro (Mayo 2024) - Survey on cyber-skills | UE Mind the Cyber Skills Gap (Agosto 2023) - a deep-dive

14. Ofcom (Febrero 2025) - Mobile RAN Power resilience

15. US Office of the National Cyber Director (Junio 2024) - Summary 2023 cybersecurity regulatory harmonization request for information

16. Telefónica (Enero 2025) - DORA, NIS2 y CRA: Descifrando la normativa de ciberseguridad en Europa

17. Telefónica (Abril 2025) - Defensa, seguridad y preparación: Un plan de acción de la UE. Referencias: Informe Niinistö sobre la preparación y la disponibilidad de la UE, octubre 2024; Libro Blanco sobre la preparación de la defensa europea para 2030, marzo 2025; Estrategia del Plan Europeo de Preparación, marzo 2025; Proteger la UE: Estrategia de Seguridad Interior de la UE, abril 2025; Plan Presupuestario para el Rearme de Europa, marzo 2025; programas de trabajo para el marco plurianual.

18. Telefónica (Abril 2025) - Defensa, seguridad y preparación: Un plan de acción de la UE

19. La Ley de Cibersolidaridad de la UE entró en vigor el 4 de febrero de 2025. Su objetivo es reforzar las capacidades de la UE para detectar, prepararse y responder a amenazas y ataques significativos y a gran escala contra la ciberseguridad. La Ley incluye un Sistema Europeo de Alerta de Ciberseguridad y un Mecanismo Integral de Emergencia de Ciberseguridad para mejorar la ciberresiliencia de la UE.

20. ENISA - European Vulnerability Database

21. MITRE CVE Vulnerability data base - https://www.cve.org/

22. Cyber Policy Portal - https://cyberpolicyportal.org/

23. Telefónica (Junio 2024) - Chile: país vanguardista en materia de ciberseguridad en Latinoamérica

24. UE-Chile (Junio 2025) - ANCI lanza en la Patagonia chilena un proyecto de fortalecimiento de la ciberseguridad en América Latina y el Caribe

25. GSMA (Febrero 2025) - Mobile Telecommunications Security Landscape 2025

26. European Commission - Report on the cybersecurity and resiliency of the EU communications infrastructures and networks; Informal meeting of the telecommunications - Joint call. Marzo 2022

27. NIS Cooperation Group (Febrero 2024) - Cybersecurity and resiliency of Europe's communications infrastructures and networks; OECD (Mayo 2025) - Enhancing the resilience of communication networks; World Bank (Deciembre 2024) - Resilient telecommunications infrastructure: A practitioner's guide

28. International Chamber of Commerce (ICC) (Julio 2024) - Protecting the cybersecurity of critical infrastructures and their supply chains; ENISA (Junio 2023) - Good practices for supply chain cybersecurity

29. Telefónica (Febrero 2025) – Informe de gestión consolidado 2024

30. Telefónica - Centro de transparencia de seguridad global

31. UK National Cybersecurity Centre - Cyber Security Toolkit for Boards

32. Telefónica (Diciembre 2024) – La infraestructura invisible que mueve el mundo digital: cables submarinos

33. Telxius, un proveedor líder de conectividad global

34. UE (Febrero 2025) - Joint Communication to strengthen the security and resilience of submarine cables

35. Telefónica (Mayo 2025): Feria de Defensa y Seguridad FEINDEF: tecnología, talento e innovación

36. Telefónica (Febrero 2024) - Burbujas 5G tácticas y Network Slicing en redes públicas

37. España (Mayo 2025) - Informe Anual de Seguridad Nacional 2024

38. Telefónica (Marzo 2025) - Telefónica revoluciona el uso de drones con un servicio integral y seguro

39. GSMA – GSMA Open Gateway

40. Gobierno de España (Febrero 2025) - Plan de España para combatir las estafas por teléfono y mensajes de texto

41. Vivo (Diciembre 2024) – Servicio antispam

42. Vivo (Mayo 2025) - Vivo Seguro

43. UK VMO2 (Noviembre 2024) - O2 unveils Daisy, the AI granny wasting scammers' time

44. INCIBE - Qué hacer si eres víctima de un fraude

45. VMO2 (Mayo 2025) - New report calls for overhaul of fraud policing as majority of police believe officers lack the resources and skills to investigate the crime

46. Telefónica Tech – Next Defense

47. Telefónica Tech - El SOC del futuro: cómo la IA y la automatización están redefiniendo el futuro

48. EU Member States declaration (Noviembre 2024) - Securing tomorrow today: transitioning to Post-Quantum Cryptography

49. European Commission (Abril 2024) - Recommendation on Post-Quantum Cryptography

50. European Commission (Junio 2025) - A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography

51. Telefónica Tech (Junio 2025) - Preparación estratégica para la criptografía poscuántica

52. Telefónica (Marzo 2025) - Telefónica crea un Centro de Excelencia dedicado a las tecnologías cuánticas

53. Telefónica – Quantum-Safe Networks

54. Telefónica (Octubre 2024) - QKD, claves criptográficas y redes cuánticas

55. Telefónica (Marzo 2025) - Telefónica se adelanta a los desafíos cuánticos con una innovadora demo en el MWC

56. Telefónica (Marzo 2025) - Telefónica y Vithas prueban el blindaje frente a ataques cuánticos en dos hospitales

57. Telefónica (Marzo 2025) – Socio del Gobierno de Vizcaya para el desarrollo de su estrategia industrial de tecnología cuántica

58. UE (Marzo 2025) - European Preparedness Union Strategy

59. UE (2019) - Regulation (EU) 2019/881 (CSA) on ENISA and on ICT cybersecurity certification

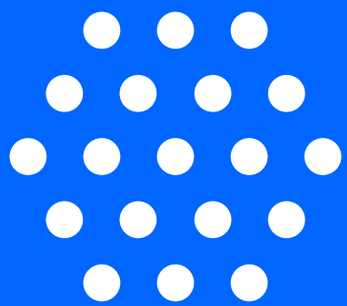
60. UE (2022) - Directive (EU) 2022/2557 on the resilience of critical entities (CER)

61. OFCOM - Statement on Network and Service Resilience Guidance

62. World Economic Forum (WEF) (Abril 2025) - The Cyber Resilience Compass: Journeys Towards Resilience.

63. UE (2022) - Directive (EU) 2022/2555 - NIS 2 on measures for a high common level of cybersecurity across the Union

Seguridad digital:
resiliencia, innovación y confianza



Sigue la conversación en:
nuestra Web, Linkedin o
suscríbete a nuestra Newsletter

Telefónica

Políticas Públicas Digitales, Regulación y Competencia

2025