Prioridades TIC de la Agencia de Ciberseguridad de Cataluña

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya

La Agencia de **Ciberseguridad** de Catalunya

Objetivo

Garantizar la ciberseguridad
en todo el territorio de **Catalunya**

Nuestros pilares

Desplegar

un servicio público de ciberseguridad ejecutando políticas públicas.

Impulsar

una cultura de ciberseguridad que permita alcanzar una ciudadanía digital plena en materia de ciberseguridad.

Garantizar

la ciberseguridad de la Administración de la Generalitat de Catalunya, de su sector público y del resto de entidades e instituciones públicas.

Potenciar

el sector económico de la ciberseguridad como sector estratégico.

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya

Volumetría de actividad de la Agencia de Ciberseguridad

En la Generalitat de Catalunya **gestionamos un incidente de seguridad cada**

4,03h

Generalitat de Catalunya

24 Departamentos y organismos relevantes

+2.200 Sistemas de información

+220m Usuarios

Ámbitos

Salud

Universidades

Administración local

Centros de investigación

Infraestructuras críticas

>4.400M
Ataques detectados durante el último año

=2,175
incidentes de seguridad anuales gestionados

+24
Programas de seguridad / año

OAT
Entidad certificadora del ENS

Internet Segura
Conscienciación y sensibilización de la sociedad

+70
Más de 70 normas y estándares

Datos memoria Agencia Ciberseguridad de Catalunya 2022

Focalizamos la actuación en los ámbitos sensibles: **Salud, Universidad y Administración local**

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya

Contexto **actual**

Salud
Ámbito hospitalario

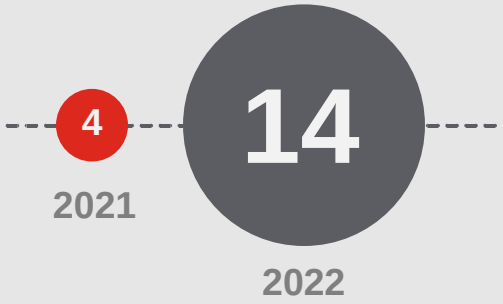
Una encuesta a **649** entitades sanitarias confirma que, el año 2022, el

53%

sufrieron ataques de *ramsomware*.

La Agencia de Ciberseguridad de Catalunya ha identificado **3 ámbitos** que, por su nivel de criticidad y el incremento de actividad beligerante, requieren una atención específica:

El *ransomware* contra hospitales en Espanya se ha multiplicado por 2,5



Evolución del número de incidentes de *ransomware* en el sector hospitalario de España (Double Extortion)

Según una encuesta a **145** profesionales de TI del sector sanitario:

al **86%**

de las organizaciones, el *ransomware* ha provocado el **parón de la actividad operativa**.

Contexto **actual**

Universidad

Ámbito universitario

En los últimos tiempos se han sufrido **3 ciberataques graves dirigidos a 3 universidades y 5 más dirigidos a 3 centros de investigación en Catalunya**

Los últimos ciberataques a las universidades y a los centros de investigación catalanes han seguido la **tendencia mundial de crecimiento del volumen y virulencia de ciberataques a este tipo de entidades.**

Los autores acostumbran a ser organizaciones criminales con el objetivo de obtener un beneficio económico vía chantaje o causar indisponibilidad:

- **Cifrando la información crítica** para el funcionamiento de la entidad y las copias de seguridad asociadas pidiendo un rescate a cambio de la clave de descifrado.
- **Robando información sensible** y pidiendo un pago a cambio de no hacerla pública.
- **Suplantando proveedores**, socios o empleados para cometer fraude económico.
- **Realizando ataques de denegación de servicio** para interrumpir la prestación de los servicios públicos.

Contexto **actual**

Administración local

Ámbito local

¿A qué problemáticas nos enfrentamos?
Los incidentes de ciberseguridad son una amenaza creciente para el ámbito local, en general, y para los ayuntamientos, en particular.

¿Qué necesidad han generado?
Frente a esta situación, el gobierno catalán ve necesario **preparar el sector público municipal** para poder **enfrentarse a los incidentes de seguridad** que puedan impactar en el servicio al ciudadano.

Con este objetivo, la Agencia de Ciberseguridad de Catalunya trabaja para diseñar y ejecutar un **modelo de ciberseguridad común** para el mundo local, evolucionando la primera versión del modelo desplegado el 2022 y teniendo en cuenta la complejidad y heterogeneidad del ecosistema.

Como nos relacionamos con el ecosistema

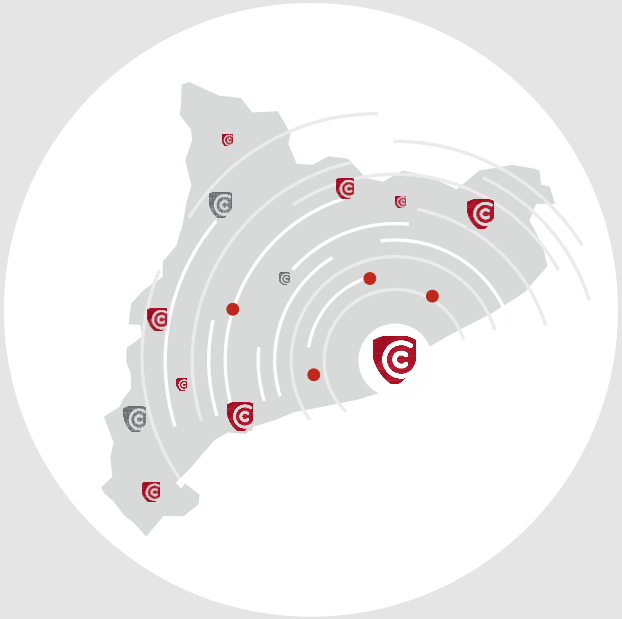
AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya

Centro de Innovación y Competencias en **Ciberseguridad**

Objetivo

Fomentar la **ciberesiliencia** en el desarrollo de **capacidades** y **competencias** en ciberseguridad en todo el territorio de Catalunya



Nuestras bases

Liderazgo

Reforzamos el liderazgo y la estrategia en capacidades operativas, tecnológicas, académicas, sociales e industriales

Innovación

Impulsamos la innovación y el impacto a través de la captación de fondos

Conocimiento

Integramos el conocimiento y recursos orientados a la excelencia, la innovación, los datos, la formación, el talento y la colaboración internacional

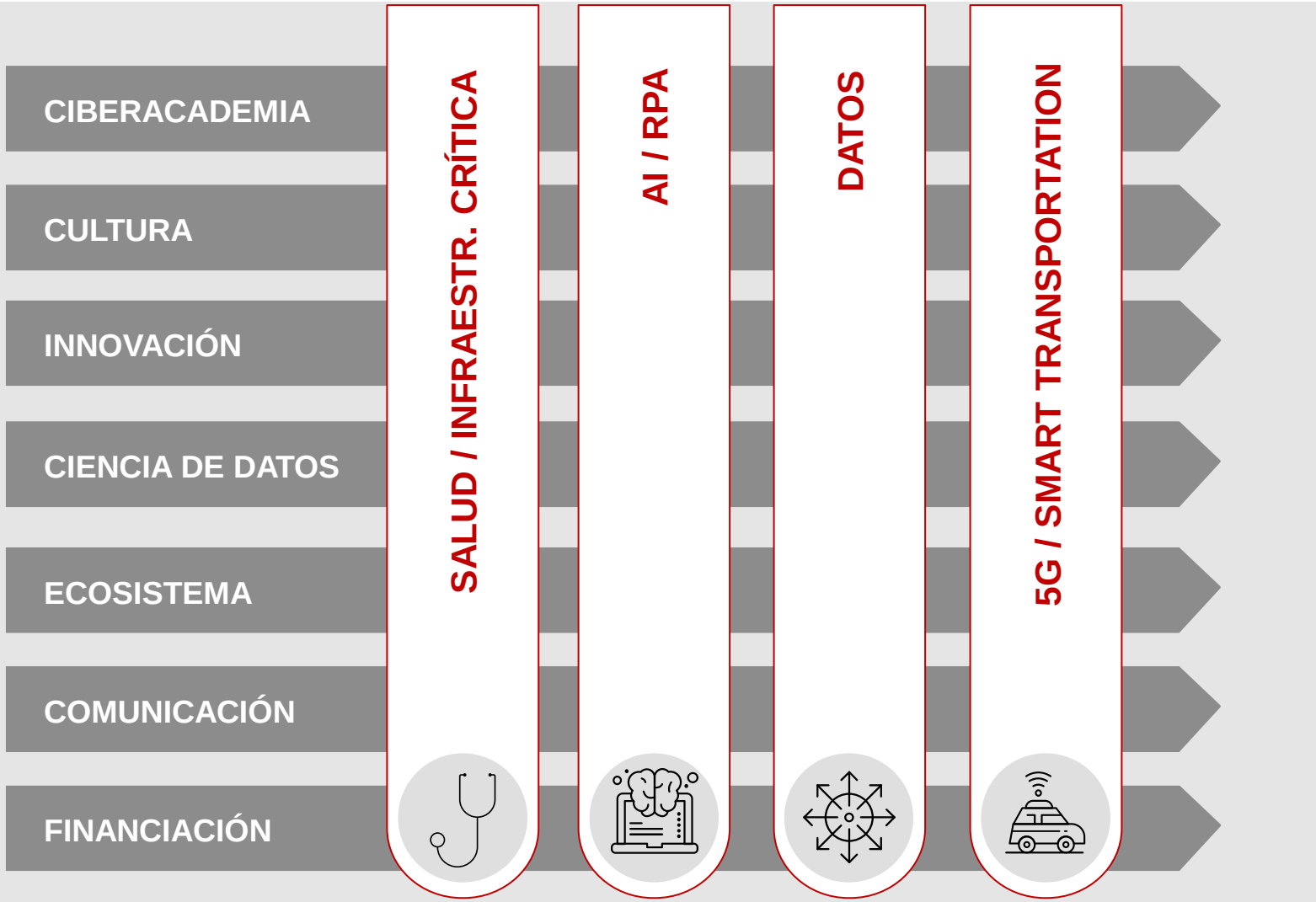
Ecosistema

Garantizamos altos estándares en ciberseguridad con orientación al mercado / ecosistema

Orientación al ecosistema

Centro de Innovación y Competencias en Ciberseguridad

Creación **de iniciativas con impacto** en todo el ecosistema catalán



Potenciar las **capacidades de excelencia operativa**

Prioridades TIC de Europa en materia de Ciberseguridad

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya

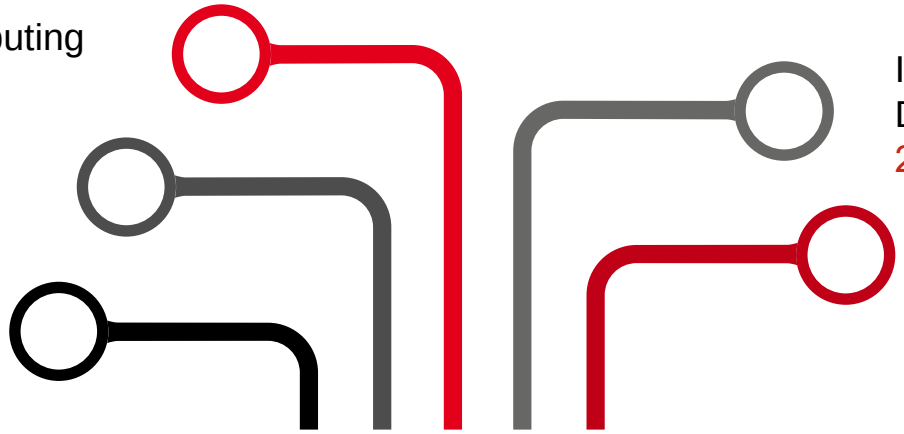
Prioridades TIC de Europa en materia de Ciberseguridad

El presupuesto del programa Europeo DIGITAL es de **7.588 Millones €** del 21-27

High performance computing
2.227 Millones €

Ciberseguridad
1.650 Millones €

Competencias Digitales Avanzadas
577 Millones €



Inteligencia Artificial, Cloud y Datos
2.062 Millones €

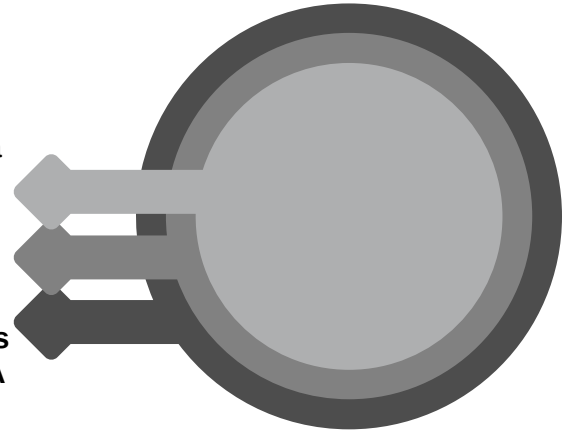
Despliegues y buenas practicas
1.072 Millones €

Prioridades TIC de Europa en materia de Ciberseguridad

Distribución de las principales oportunidades de fondos europeas en ciberseguridad del 2024

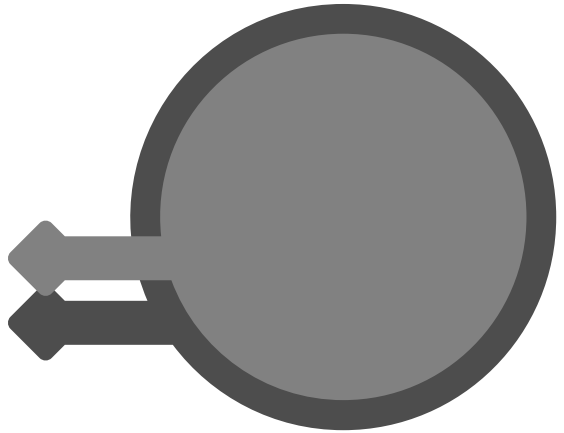
DIGITAL ECCC

- **24 M€ Persistencia post cuántica**
- **30 M€ SOC - IA**
- **30 M€ Capacidades Cumplimiento CRA**



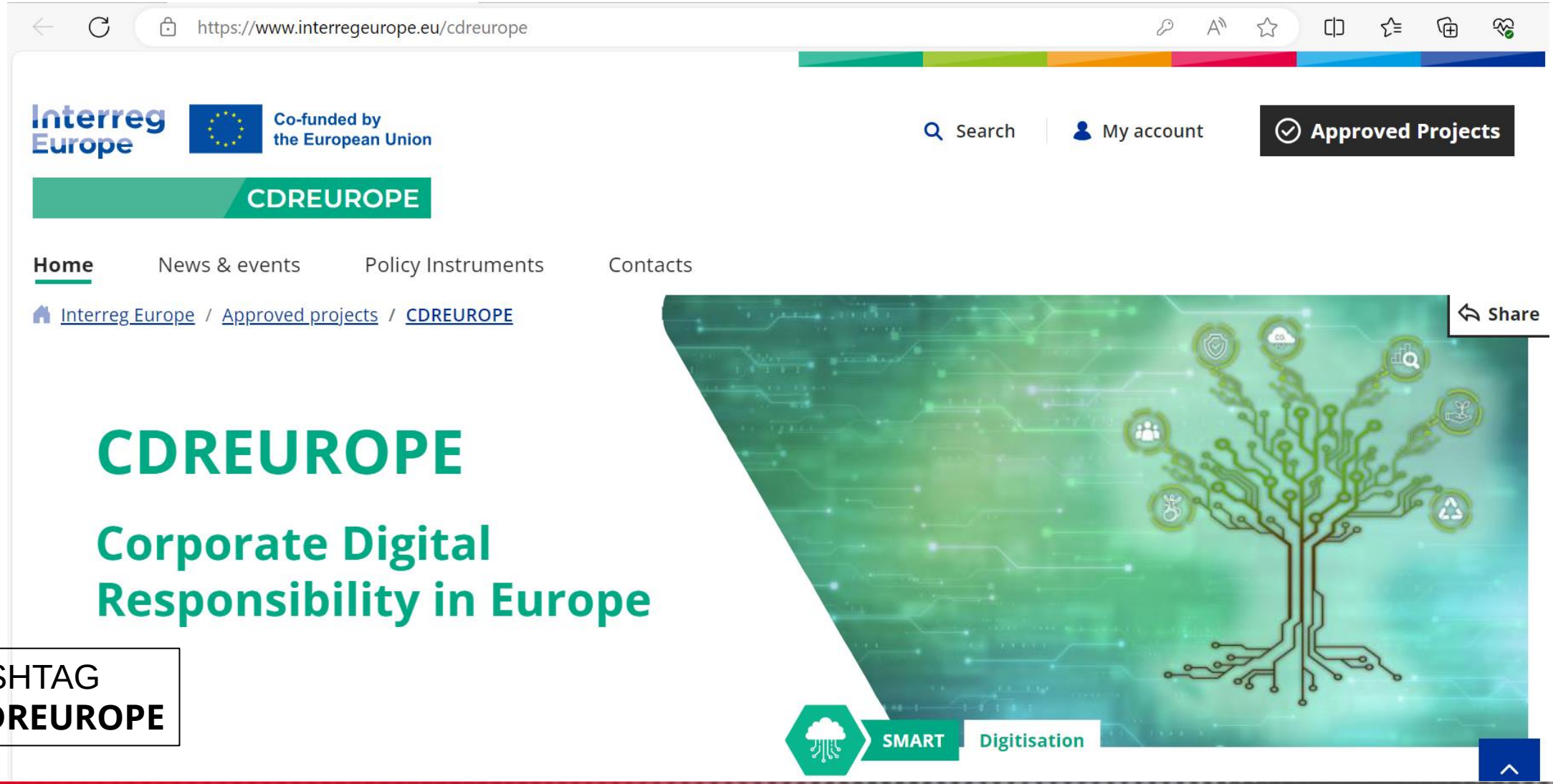
HORIZON EUROPE Clúster 3 - Ciber

- **23.4 M€ Persistencia post Cuántica (RI)**
- **37 M€ Desarrollo de Herramientas (I)**



(*) No incluidas las oportunidades orientadas a NCC

Prioridades TIC de Europa en materia de Ciberseguridad



HASHTAG
#CDREUROPE

Gracias

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya

Nueva normativa europea en ciberseguridad

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya

Nueva normativa europea en ciberseguridad

Reglamento de Ciberresiliencia

El reglamento europeo de Ciberresiliencia establece requisitos de ciberseguridad obligatorios para los fabricantes de productos digitales que deseen comercializarlos en los países miembro.

Establecimiento de 4 objetivos específicos:

- Mejorar la seguridad de los productos con elementos digitales desde su diseño y en todo su ciclo de vida.
- Establecer un marco de trabajo sobre ciberseguridad coherente que facilite el trabajo a los fabricantes de *hardware* i *software.*
- Mejorar la transparencia de la seguridad de los productos con elementos digitales.
- Permitir que negocios y consumidores utilicen productos con elementos digitales de manera segura.

Texto aprobado el septiembre de 2022 y en trámites parlamentarios. Cuando entre en vigor, los actores implicados tendrán 24 meses para adaptarse completamente

Reglamento DORA

El reglamento europeo *Digital Operational Resilience Act* (DORA) establece requisitos homogéneos a la Unión para que las organizaciones del sector financiero garanticen que pueden resistir y responder a cualquier tipo de incidente cibernético.

Esta norma se basa en 5 pilares fundamentales:

- Gestión de riesgos
- Notificación de incidentes
- Pruebas de resiliencia en la operativa digital
- Gestión del riesgo de terceras partes
- Compartición de intel·ligència de la información

Aprobado el diciembre de 2022, las organizaciones afectadas tendrán 2 años para adaptarse completamente

Nueva normativa europea en ciberseguridad

Esquema Nacional de Seguridad

El ENS es una norma del estado español que regula un conjunto de principios básicos y requerimientos mínimos para a una protección adecuada de los sistemas, los datos, las comunicaciones y los sistemas electrónicos en el sector público. El ENS va en la línea europea de dotar de mayor protagonismo a la ciberseguridad al nivel de la seguridad nacional.

El 2022 se actualizó el ENS y se estableció:

- Establece un protocolo de actuación delante de incidentes cibernéticos.
- Introduce el principio de vigilancia continua que comprende la prevención, la detección, la respuesta y la conservación.
- Incorpora una nueva familia de medidas en el marco operacional de Servicios en la nube.

Real Decreto 311/2022, del 3 de mayo, por el cual se regula el Esquema Nacional de Seguridad

Directiva NIS 2

La renovada Directiva europea de *Network and Information Systems* (NIS 2) tiene por objetivo mejorar la resiliencia y la respuesta a incidentes cibernéticos de entidades públicas y privadas, con el objetivo de establecer unos requisitos comunes entre los estados miembros.
Los principales cambios respecto la NIS se resumen en:

- Elabora una nueva clasificación de los proveedores de servicios en entidades esenciales e importantes.
- Establece un procedimiento sancionador y una compilación de sanciones mínimas.
- Se refuerzan los requerimientos de seguridad para cada uno de los sectores y entidades.
- Se establecen medidas para mejorar la cooperación entre los estados miembros.

La directiva NIS 2 se va a aprobar el desembre de 2022 y los estados miembros tienen 21 meses para transponerla

Directiva NIS 2