icav
Ilustre Colegio de Abogados de Valencia

CV CA Consejo Valenciano de Colegios de la Abogacía

GENERALITAT VALENCIANA
Conselleria de Justicia e Interior

Seguridad de la información o ciberseguridad

ponente **D. SANTIAGO ESCOBAR ROMÁN**
fecha **11/06/2024**

Ciberataques

El ciberataque a la Dirección General de Tráfico que ha afectado a millones de conductores: preguntas y respuestas

Publicado 7/6/2024 17:25

Claves

- Los datos de millones de conductores fueron robados después de que la Dirección General de Tráfico (DGT) sufriera un ciberataque
- Se han robado datos como la matrícula, marca y modelo del vehículo, nombre, domicilio y población del titular y los datos del seguro vigente
- Con la información expuesta, los ciberdelincuentes podrían enviar ataques de *phishing* personalizados haciéndose pasar por la DGT o incluso suplantar la identidad de los afectados

29/05/2024 18:14 ACTUALIZADO: 29/05/2024 21:46

Uno de los proveedores de **Iberdrola sufrió un ciberataque entre el 5 y 7 de mayo** provocando "el acceso parcial a información" de alrededor de **850.000 clientes**, según ha adelantado este miércoles *El Español*. Los datos que quedaron expuestos fueron los nombres, los apellidos, sus respectivos números de DNI y otros datos de contacto.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Ciberataques

More than 200 ‘life-saving’ operations cancelled by NHS hospitals after cyberattack

Exclusive: Hundreds of patients urgently referred for suspected cancer had appointments cancelled

Rebecca Thomas Health Correspondent • 8 hours ago • Comments

June 2024

Cyber attack on a video portal in Japan

Nico Nico Douga / ニコニコ動画 - Japan

June 3, 2024

Ransomware at a service provider for the healthcare sec

Synnovis - London, United Kingdom

June 6, 2024

Cyber attack on a health care system in Italy

ASST-Rhodense - Garbagnate Milanese, Lombardy, Italy

June 2024 ?

Cyber attack on a retail chain in Russia

Verny / Верный - Russia

June 2024 ?

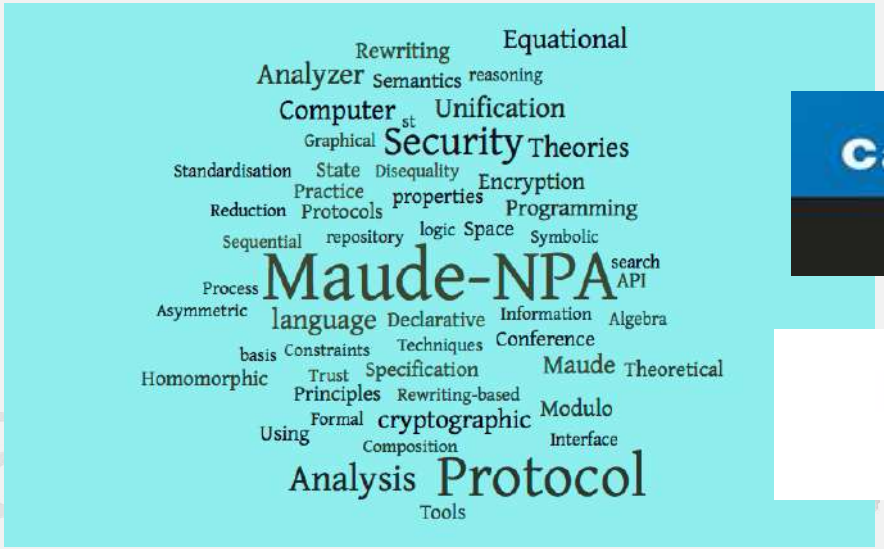
Cyber attack on a municipality in Wisconsin, USA

Village of Elm Grove - Elm Grove, Wisconsin, USA (Waukesha County)

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Santiago Escobar Román

- Ingeniero en Informática
- Doctor en Informática
- Catedrático de Universidad
- Más de 100 artículos en revistas y conferencias
- Más de 50 charlas invitadas
- Equipo de desarrollo internacional:
  - Lenguaje de programación Maude
  - Análisis de protocolos Maude-NPA
- Experiencia:
  - Logic-based Analysis
  - Model Checking
  - Program Verification
  - Secure Software Dev
  - Security Protocols
  - Cyber Physical Systems



Colaboraciones

Financiación

Difusión

¿En qué se basa nuestra moderna sociedad digital?

Internet se fundamenta en un cifrado que genera una clave dividida en dos partes, una que solo conoce el emisor y la otra, el receptor

SANTIAGO ESCOBAR ROMÁN

03 MAY 2016 - 17:19 CEST

La paradoja de los ciberataques: así se aprovechan los 'hackers' de los avances para proteger la seguridad

El desarrollo de mecanismos de cifrado de la información virtualmente irrompibles permite que los delincuentes puedan bloquear un disco duro sin que sea posible recuperar los datos

SANTIAGO ESCOBAR ROMÁN

23 MAY 2021 - 05:20 CEST

Frases célebres

"Se piensa que lo justo es lo igual, pero no para todos, sino para los iguales. Se piensa por el contrario que lo justo es lo desigual, pero no para todos, sino para los desiguales" Aristóteles

"La ciencia siempre se ha preciado de ser empírica y creer solamente aquello que pudiera verificarse" Bertrand Russell

"El único sistema completamente seguro es aquel que está apagado, encerrado en un bloque de cemento y sellado en una habitación rodeada de alambradas y guardias". Gene Spafford

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Sistema seguro

- La pregunta clave es ¿qué se entiende por un sistema seguro?
  1. adj. Libre y exento de riesgo
  2. adj. Cierto, indubitable.
  3. adj. Que no falla o que ofrece confianza.

  (Real Academia Española).
- El término "seguro" se entiende en la actualidad no como lo describe la Real Academia Española, conocido en el mundo anglosajón como "safe" (inofensivo), sino como protegido ante ataques exteriores, conocido en el mundo anglosajón como "secure" (seguridad).
- Es decir, se puede decir que algo es seguro si dispone de mecanismos, políticas, controles y protecciones para evitar un acceso indeseado.
- Un sistema se desea que sea totalmente seguro (en ambos sentidos "safe and secure").

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Digitalización e Inteligencia Artificial
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Safety (and Security)

China / Science

Scientists find security risk in RISC-V open-source chip architecture that China hopes can help sidestep US sanctions

- Northwestern Polytechnical University, a major defence research institute in C allows attackers to bypass security protections
- US lawmakers reportedly consider sanctions to restrict RISC-V access becaus technology transfer and Chinese adoption of architecture

FORBES > INNOVATION > CYBERSECURITY

Apple Addresses Critical Security Vulnerability For Windows 10 And 11 Users

Davey Winder Senior
Veteran cybersecurity
hacker, author

0

Thousands of LG Smart TVs Vulnerable to Root Access Security Flaws

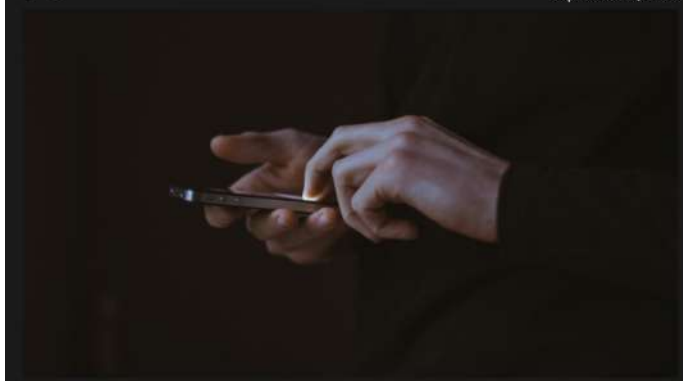
Security researchers have discovered four vulnerabilities affecting various versions of WebOS, which is used in LG Smart TVs. Learn about the nature of these flaws and the risks arising from them.

VISA: un fallo de seguridad permite eludir el PIN

Publicado el 31 agosto 2020 por David Salces Guillem

LISTENING TO AN IPHONE WITH AM RADIO

by: Danie Conradie
36 Comments
September 18, 2020



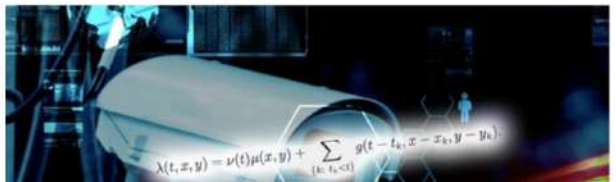
Electronic devices can be surprisingly leaky, often spraying out information for anyone close by to receive.

Police Across Canada Are Using Policing Algorithms, Report Finds

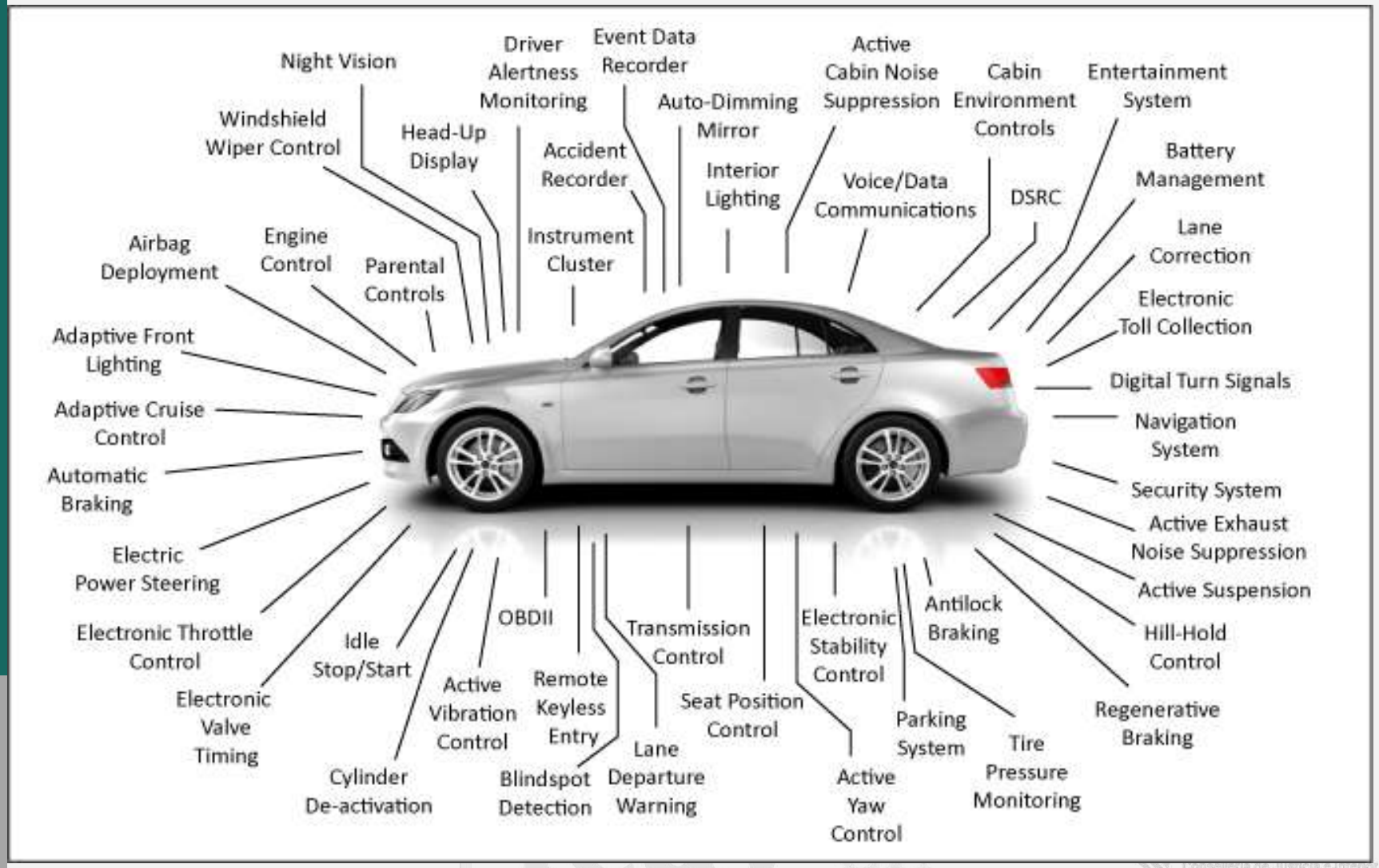
Police across Canada are increasingly adopting algorithmic technology to predict crime. The authors of a new report say human rights are threatened by the practice.

By Nathan Munn

September 1, 2020, 12:00pm Share Tweet Snap



Ciberseguridad



Dispositivos con riesgos:

- Dispositivos programables (PLC, IoT).
- Ordenadores, tablets, teléfonos móviles
- Servidores de sitios web o servicios web
- Servidores back-end con bases de datos
- Nodos intermediarios para almacenar info
- Firewalls, routers and switches.
- DNI, tarjetas de créditos

Situaciones comunes de ciberseguridad

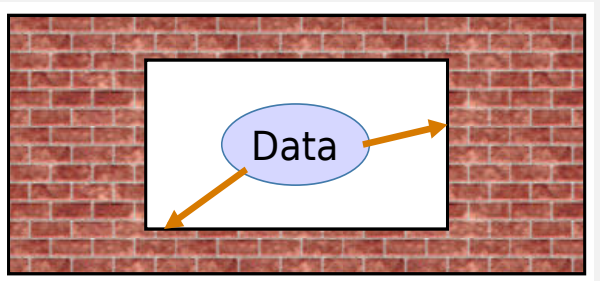
- Comunicaciones seguras, p.ej. a través del teléfono, email, o servicios de mensajería como WhastApp. El objetivo principal es: confidencialidad e integridad de la información transmitida. Pero también cuestiones de autenticación del emisor, información liberada de forma inadvertida, uso de mecanismos de cifrado y descifrado, etc.

- Banca por Internet. El objetivo principal es: confidencialidad de las transacciones e integridad de la información. Pero también, prevención de transacciones falsas, imposibilidad de repudiación de una transacción (muy importante en sistemas como eBay o Amazon), o autenticación del usuario detrás de una venta o una compra (de nuevo muy importante en sistemas como eBay o Amazon).

- Voto electrónico. El objetivo principal es: confidencialidad de la acción de votar y secreto del voto efectuado. Pero también, control de quién puede votar, cuándo y cómo, privacidad del hecho de haber votado o no, o disponibilidad de los sistemas para efectuar el voto.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Confidencialidad

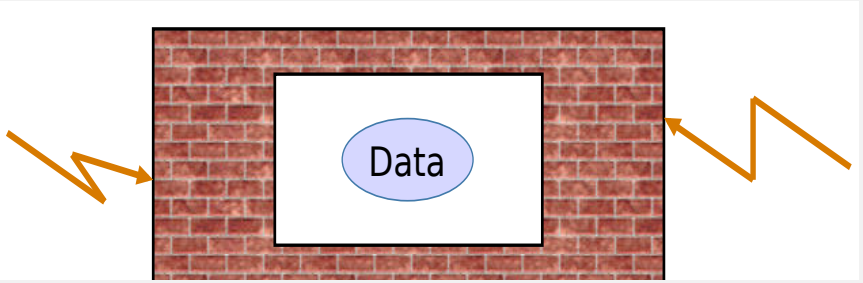


Confidencialidad: mantener los datos o acciones del sistema ocultos hacia el exterior. Las propiedades más cercanas a la confidencialidad serían justamente:

- Protección de los datos. Por ejemplo, mantener la información sanitaria de un individuo segura dentro del sistema de información de un hospital o del Ministerio de Sanidad.
- Anonimidad. Por ejemplo, el Instituto de Estadística genera información sobre los ciudadanos totalmente desligada de los nombres y apellidos o de información delicada como sexo o dirección.
- Secreto. Por ejemplo, los gobiernos deben mantener cierta información clasificada fuera del alcance de los ciudadanos, como ubicaciones de instalaciones militares críticas para la seguridad nacional.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Integridad

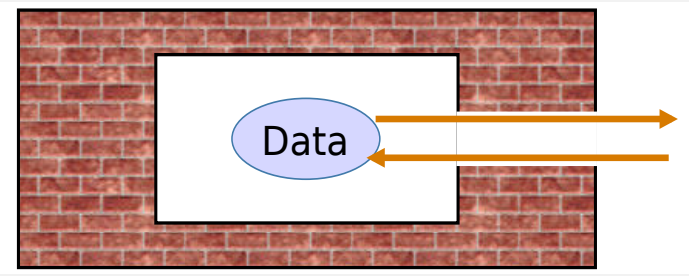


Integridad: evitar el acceso malintencionado a los datos o acciones del sistema. Las propiedades más cercanas a la integridad serían justamente:

- Corrupción. Por ejemplo, los bancos deben asegurarse que nadie se infiltra en sus sistemas y modifica el balance de las cuentas.
- Falsificación (Forgery). Por ejemplo, los bancos deben asegurarse que todas las transacciones que modifican el balance de una cuenta son legítimas y no son transacciones fraudulentas.
- Consistencia. Por ejemplo, los bancos deben asegurarse que cuando haya un movimiento de dinero entre cuentas, el estado final de las cuentas es consistente con dicho movimiento

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Disponibilidad



Disponibilidad: flujo de información de entrada y salida del sistema. La disponibilidad puede estar ligada a información estadística o probabilística, aunque no siempre. Las propiedades más cercanas a la disponibilidad serían justamente:

- Confiabilidad (Reliability). Por ejemplo, las personas estamos acostumbrados a que servicios como Facebook o WhatsApp no fallen y cuando dejan de funcionar se produce un caos mediático importante.
- Tolerante a fallos. Por ejemplo, sistemas que incorporen partes redundantes por si hay fallos en las partes principales y los auxiliares deben ponerse a funcionar.
- Denegación de servicio. Por ejemplo, este tipo de ataques se ha vuelto muy común en los últimos años y existen multitud de noticias en la prensa.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Otras propiedades

- No-repudiación. Por ejemplo, los bancos no pueden permitir que una vez hecha una transacción, uno de los participantes se retracte y desee deshacerla. Sin embargo, eso es muy común en sistema de pago electrónico como eBay o Amazon, donde la confianza entre el cliente y la empresa es más importante para la empresa que la confianza entre la empresa y los vendedores de productos.
- Reparto equitativo (Fairness). Por ejemplo, las empresas de juegos online o la reciente tecnología detrás del Bitcoin no pueden permitir que un jugador (o participante) tenga ventaja sobre otros jugadores.
- Privacidad. No se debe confundir con confidencialidad ni con secreto, aunque estén muy ligadas. Por ejemplo, Facebook debe tanto proteger los videos y fotos de sus usuarios como evitar el robo de cuentas de usuario, haciéndose pasar por un usuario legítimo; cosa que no cumple de forma reiterada, como el escándalo de Facebook y “Cambridge Analytica” o diversos anuncios de prensa sobre malas prácticas informáticas.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Instituto Nacional Ciberseguridad (INCIBE)

OSI Oficina de Seguridad del Internauta

IS4K INTERNET SEGURA FORKiDS

protege tu empresa

incibe-cert_

Plan de Recuperación, Transformación y Resiliencia

017 Teléfono 017

INCIBE - Informe Ciberseguridad 2023

INCIBE - Informe Ciberseguridad 2023

+8.800 *accesos e intentos de acceso*
no autorizados a información de una red o sistema informático de empresas, ciudadanía o familias españolas
(por ejemplo, un extraño entra a una casa, sin permiso).

+9.000 *ataques*
que han inutilizado los dispositivos de organizaciones o ciudadanos.

+28.000 *casos de fraude*
reportados por las víctimas.

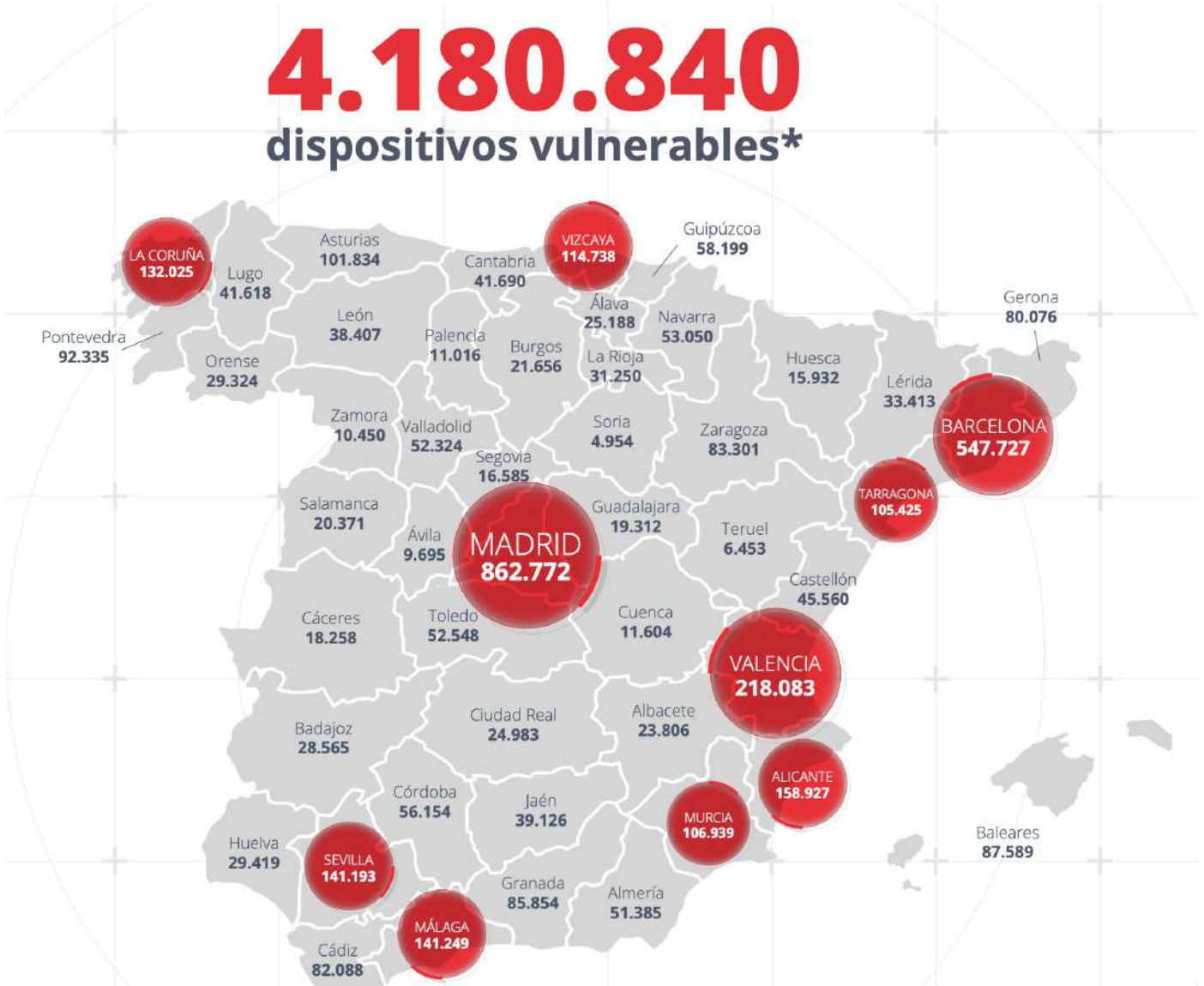
+26.000 *dispositivos dañados*
por *software* malicioso.

+7.000 *sitios detectados*
que albergaban contenido abusivo y la correspondiente retirada de los mismos.

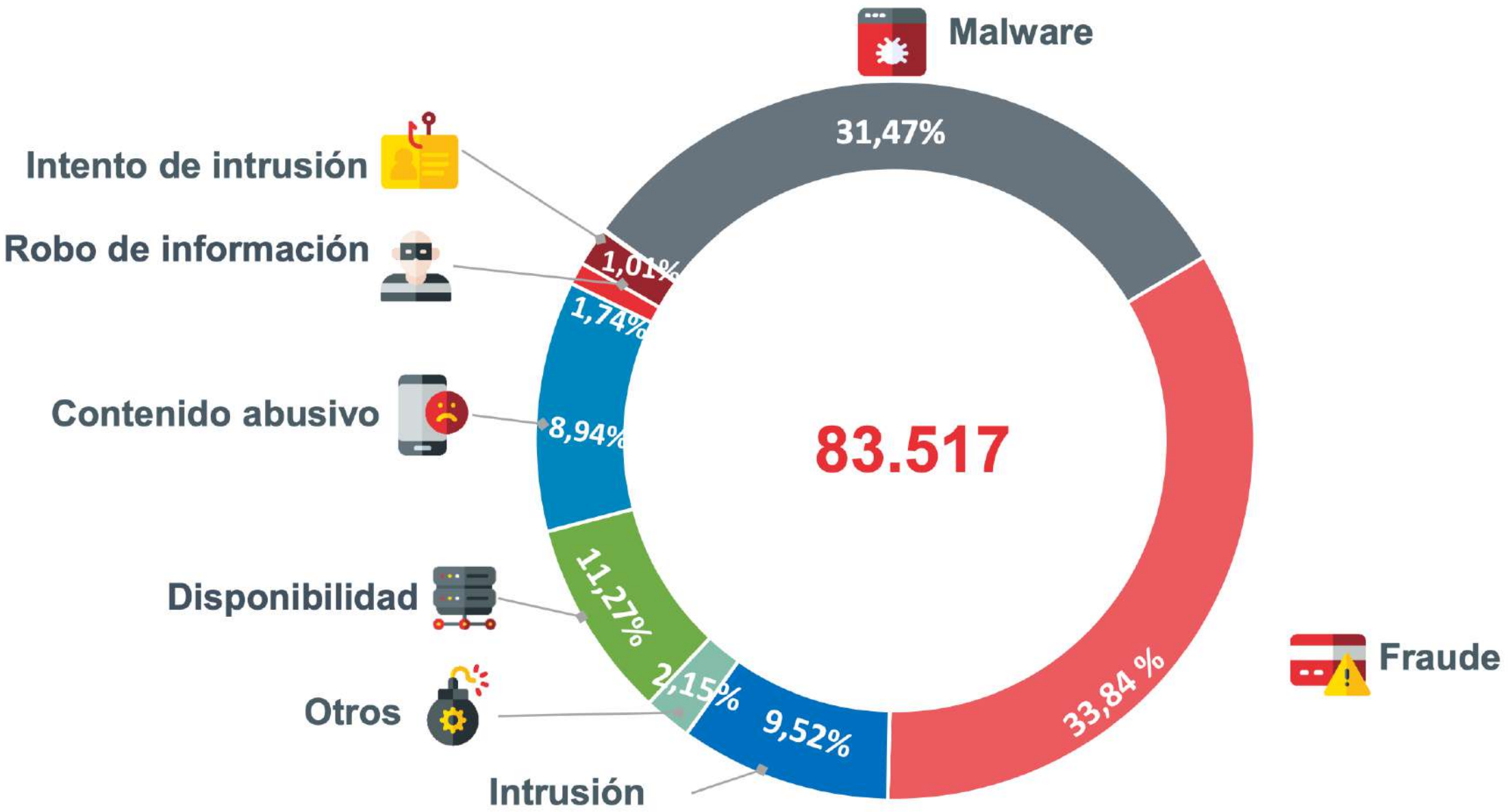
+1.400 *accesos no autorizados*
a datos importantes, como contraseñas, números de tarjetas de crédito o información personal ***(por ejemplo, alguien entra en un espacio digital y se lleva cosas valiosas sin permiso).***

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

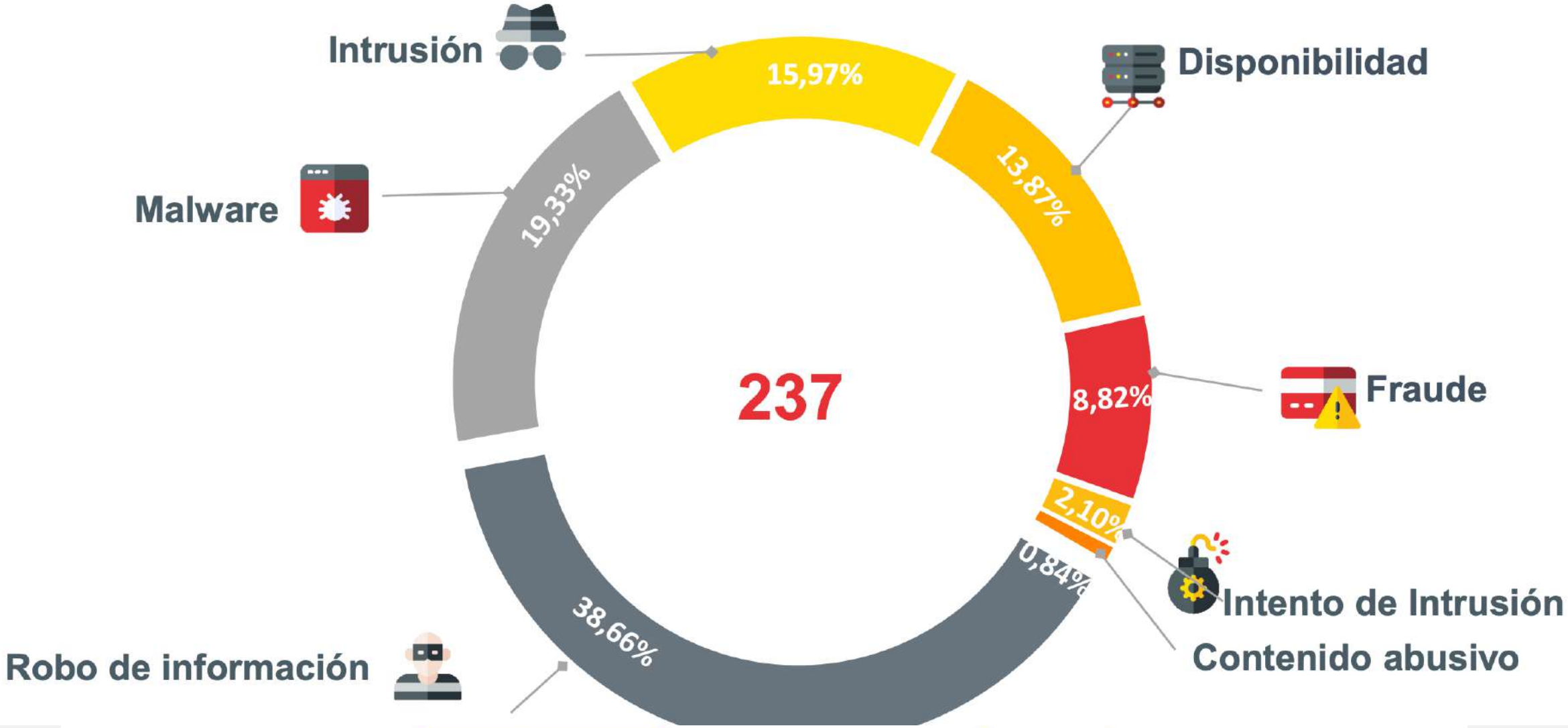
INCIBE - Informe Ciberseguridad 2023



INCIBE 2023 – Incidentes ciberseguridad



INCIBE 2023 – Servicios Esenciales



INCIBE 2023 – Sectores

Informe criminalidad Ministerio Interior

HECHOS CONOCIDOS	2018	2019	2020	2021	2022
ACCESO E INTERCEPTACIÓN ILÍCITA	3.384	4.004	4.653	5.342	5.578
AMENAZAS Y COACCIONES	12.800	12.782	14.066	17.319	15.982
CONTRA EL HONOR	1.448	1.422	1.550	1.426	1.191
CONTRA PROPIEDAD INDUST./INTELEC.	232	197	125	137	114
DELITOS SEXUALES(*)	1.581	1.774	1.783	1.628	1.646
FALSIFICACIÓN INFORMÁTICA	3.436	4.275	6.289	10.476	12.569
FRAUDE INFORMÁTICO	136.656	192.375	257.907	267.011	335.995
INTERFERENCIA DATOS Y EN SISTEMA	1.192	1.473	1.590	2.138	1.662
Total HECHOS CONOCIDOS	**160.729**	**218.302**	**287.963**	**305.477**	**374.737**

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración

Respuesta Europa - Cyber Resilience Act (CRA)

Objetivos

Establecer requisitos obligatorios de ciberseguridad para el HW y SW en todo su ciclo de vida

Asegurar que los productos tengan menos vulnerabilidades.
Fabricantes responsables de la ciberseguridad de sus productos

Mejorar la transparencia de la seguridad de los productos de HW y SW

Redundará en una mejor protección

Certificación de productos
Marcado CE

Respuesta Europa - Network and Information Security (NIS 2)

Transposición a la legislación española: antes del 17 de octubre de 2024

Aplica a entidades públicas y privadas que sean **mediana** o **gran empresa** distinguiendo entre entidades **esenciales** e **importantes**

Sanciones de hasta 10M€ o 2% volumen negocio anual para entidades **esenciales**, y hasta 7M€ o 1.4% para **importantes**

Anexos I y II tipifican las **actividades** que se consideran críticas y sujetas a esta normativa

Aplica un régimen de supervisión por parte de las **autoridades** competentes mediante **inspecciones y auditorías**

Adoptar medidas de **gobernanza, gestión de riesgos** de ciberseguridad e información

Notificar los incidentes relevantes de ciberseguridad con impacto significativo al **CSIRT** o autoridad competente correspondiente

Adoptar **medidas técnicas, operativas y organizativas proporcionadas** para gestionar los **riesgos** de ciberseguridad así como para prevenir y minimizar el **impacto** de posibles ciberincidentes

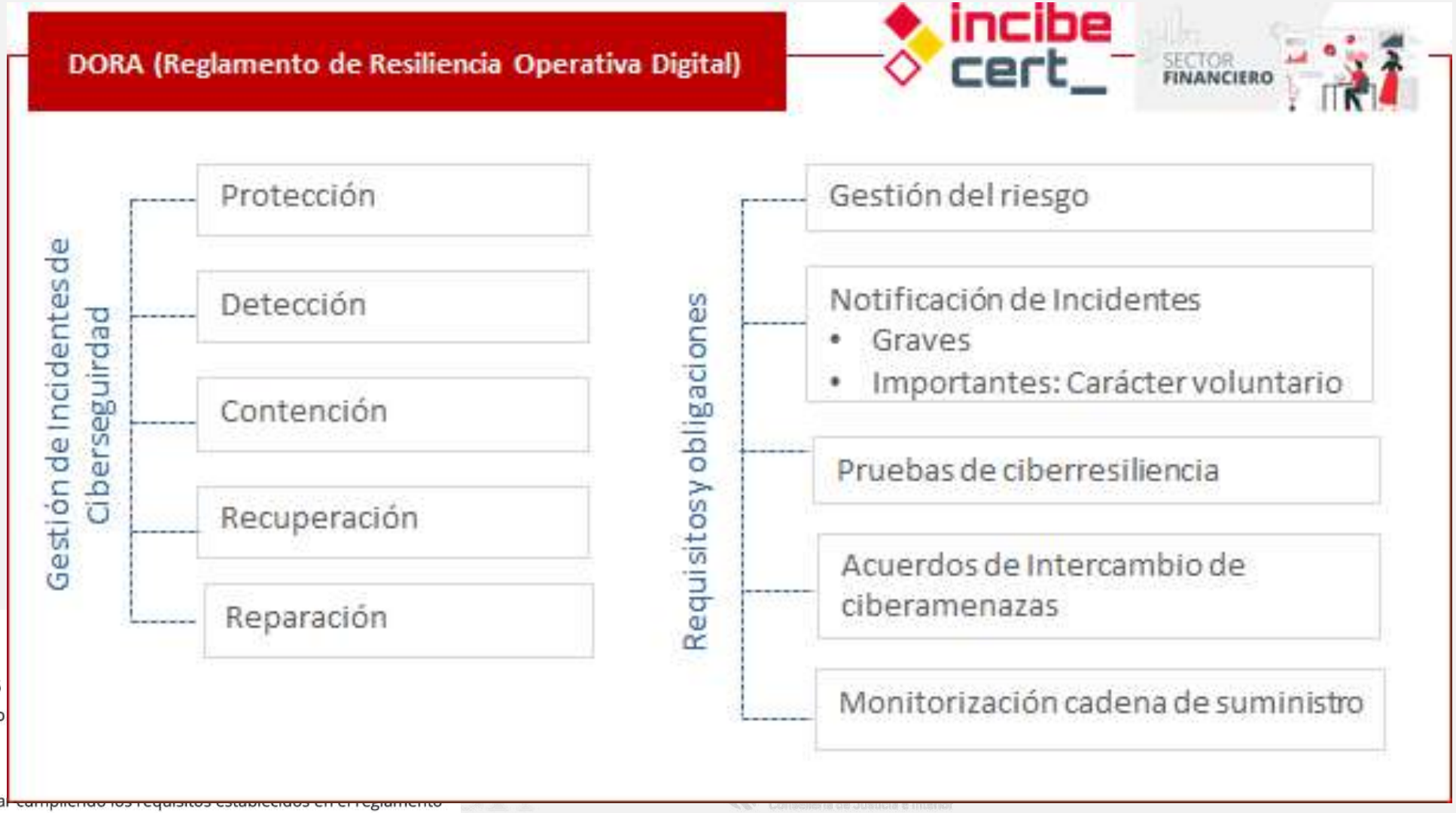
Gestión de riesgos con sus proveedores y prestadores de servicios directos para garantizar la seguridad en **cadena de suministro** TIC

Aumenta la **responsabilidad de los órganos de dirección**

Adoptar **prácticas de ciberhigiene** como confianza cero, actualización dispositivos, segmentación de la red, la gestión de la identidad y el acceso o la concienciación de los usuarios, y han de organizar **formaciones** para su personal y **sensibilizar** sobre las ciberamenazas

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Digitalización e Inteligencia Artificial
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

DORA (Digital Operational Resilience Act) – Sector Financiero (Bancos, Seguros, Fondos, etc)



1. **16 de enero de 2023**
   Entrada en vigor de DORA.
2. **17 de enero 2023 a 16 de enero 2025**
   Las entidades financieras tienen un plazo
   reglamento DORA.
3. **17 de enero 2025**
   Las entidades financieras tienen que esta
   DORA.

Muchas gracias