derten CIBERSEGURIDAD

Afrontando los desafíos de la seguridad de la información en Euskadi:

"Implementación de sistemas de gestión efectivos"

Hoy, hablaremos sobre...

Amaia Chaparro
Directora Área SGSI
DERTEN

- ✓ Estrategia y nuevos retos
- ✓ Normativas y certificaciones relevantes
- ✓ SGSI: Modelo GRC
- ✓ Objetivos
- ✓ Enfoque

derten CIBERSEGURIDAD

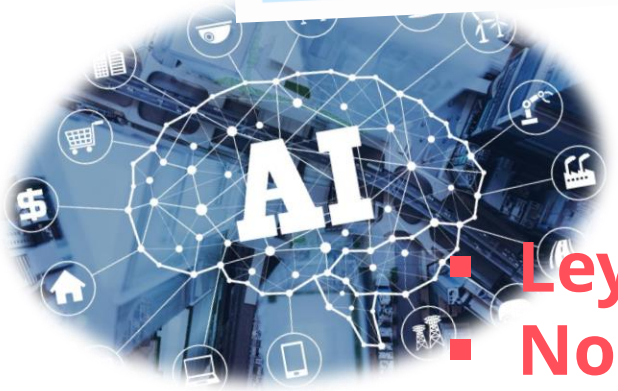
¡Última hora!

¡Compartir para ganar!

421 sondas del Sistema de Alerta Temprana (SAT) de Internet.
71 sondas para APT.
115.000 sensores para la detección de código dañino.

https://unodecadacincodelitos.com

→ Aumento del 352,1% desde 2015



- **Ley de Cibersolidaridad y Ciberresiliencia.**
- **Normativa Europea DORA y NIS2.**
- **Nuevas soluciones: BAS, Cibervigilancia, SOC …**
- **IA ¿seguridad?**

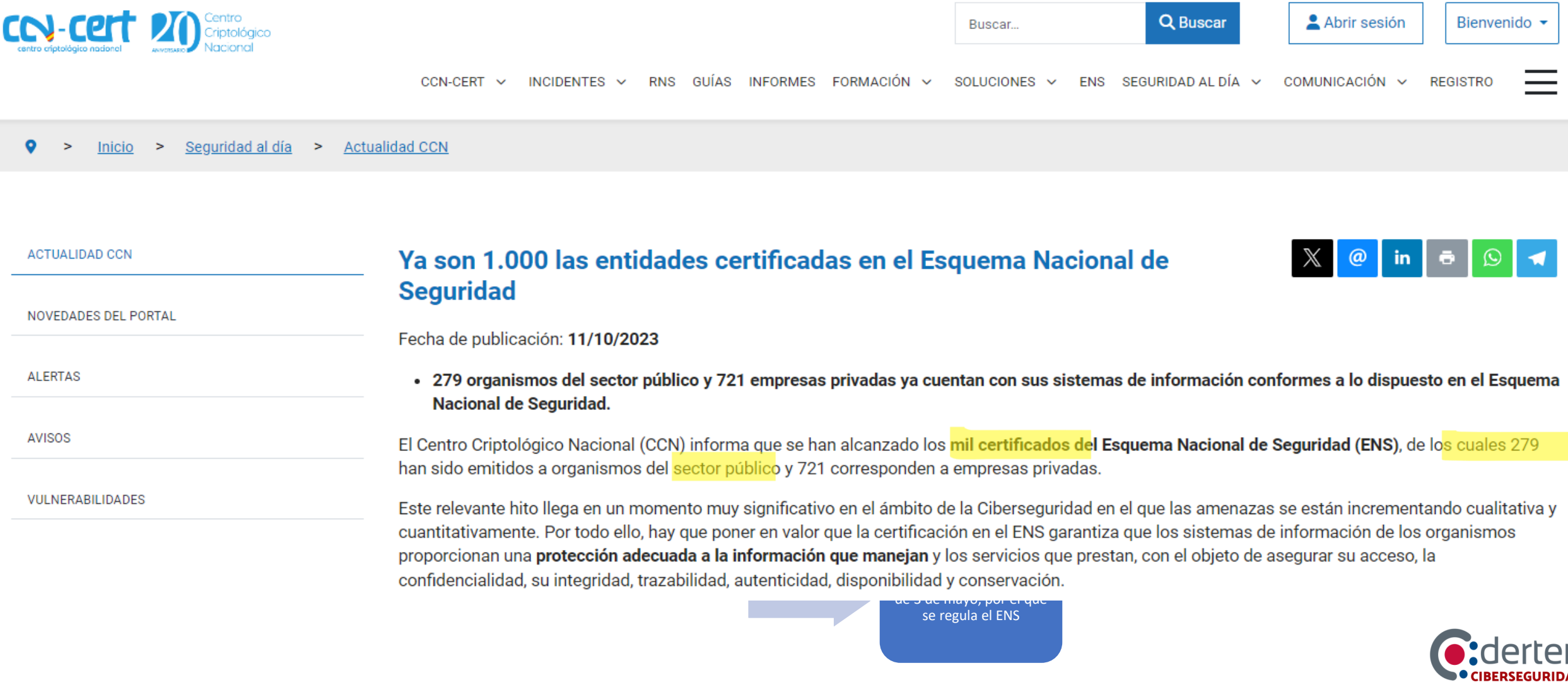
Normas más relevantes

- **Esquema Nacional de Seguridad**: para las AAPP, empresas semipúblicas y empresas proveedoras. Nivel medio, bajo y alto.
- **RGPD, LOPDGDD, Ley AVPD**: adapta el RGPD de la UE al marco de la CAE.
- Repercusión de utilización de **IA** en las organizaciones.
- Plan de infraestructuras críticas (**PIC**).
- **NIS2**: legislación a escala de la UE (12 sectores).
- **Reglamento IA:** Repercusión de utilización de IA en las organizaciones.
- **Normas específicas** para sectores de negocio concretos:
  - **ISO/IEC 27001**: estándar internacional para la seguridad de la información. Sector privado.
  - **TISAX**: estándar de seguridad para la industria automotriz.
  - **DORA**: Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero. Sector financiero.

NIS2 Directive

Normas más relevantes

~~Ley 11/2007, de 22 de junio, de acceso~~



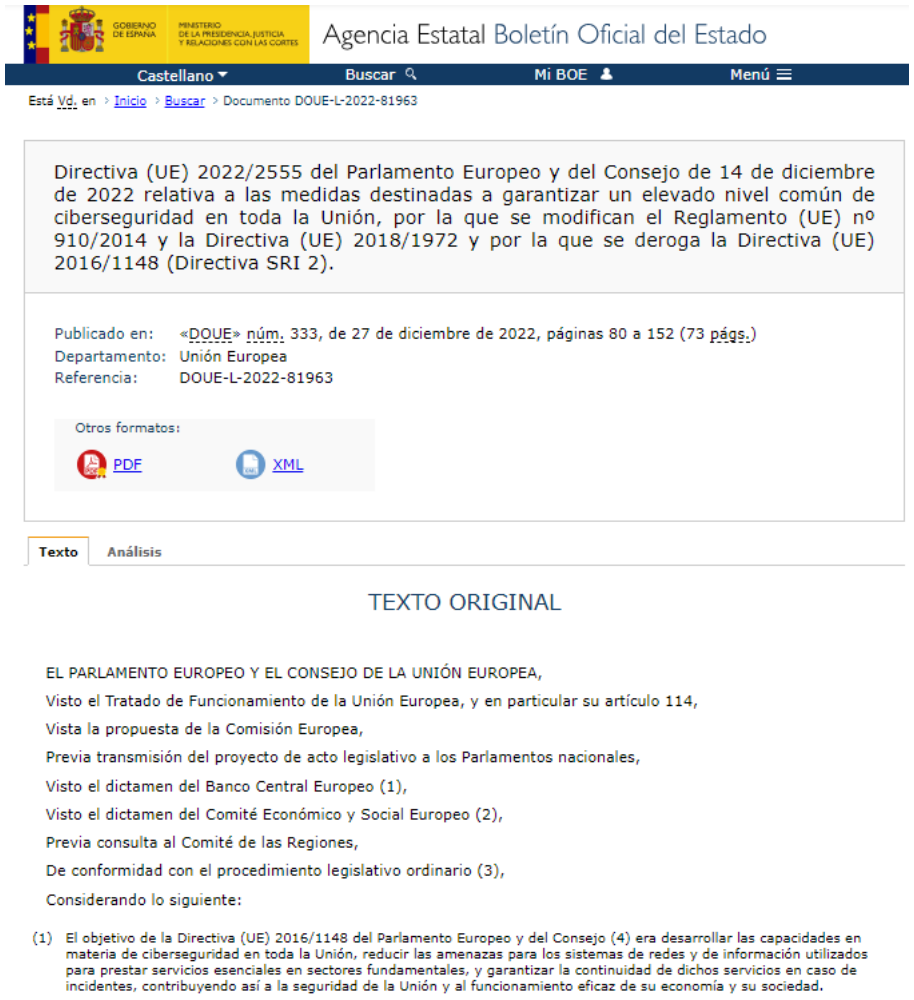
Normas más relevantes

Tabla 22: Desglose de multas por temas				
Importe de multas en euros según el tema	**2022**	**2023**	**% relativo**	**Δ% anual**
Seis temas con mayor importe total en 2023	**14.241.901€**	**26.433.600 €**	**89%**	**86%**
Quiebras de seguridad	821.800 €	12.907.000 €	43%	1471%
Entidades financieras / acreedoras	596.200 €	5.321.000 €	18%	792%
Derechos protección datos	5.900 €	2.633.400 €	9%	44534%
Contratación fraudulenta	706.800 €	2.571.500 €	9%	264%
Telecomunicaciones	632.000 €	1.942.000 €	7%	207%
Servicios de Internet	11.479.201 €	1.058.700 €	4%	-91%
Otros	**6.533.460 €**	**3.383.810 €**	**11%**	**-48%**
TOTAL	**20.775.361 €**	**29.817.410 €**	**100%**	**44%**

RGPD
REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

derten CIBERSEGURIDAD

Normas más relevantes



Agencia Estatal Boletín Oficial del Estado

Castellano | Buscar | Mi BOE | Menú

Está Vd. en › Inicio › Buscar › Documento DOUE-L-2022-81963

Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

Publicado en: «DOUE» núm. 333, de 27 de diciembre de 2022, páginas 80 a 152 (73 págs.)
Departamento: Unión Europea
Referencia: DOUE-L-2022-81963

Otros formatos: PDF XML

Texto | Análisis

TEXTO ORIGINAL

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 114,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de acto legislativo a los Parlamentos nacionales,

Visto el dictamen del Banco Central Europeo (1),

Visto el dictamen del Comité Económico y Social Europeo (2),

Previa consulta al Comité de las Regiones,

De conformidad con el procedimiento legislativo ordinario (3),

Considerando lo siguiente:

(1) El objetivo de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo (4) era desarrollar las capacidades en materia de ciberseguridad en toda la Unión, reducir las amenazas para los sistemas de redes y de información utilizados para prestar servicios esenciales en sectores fundamentales, y garantizar la continuidad de dichos servicios en caso de incidentes, contribuyendo así a la seguridad de la Unión y al funcionamiento eficaz de su economía y su sociedad.

17/10/2024??

NIS2 Directive

derten CIBERSEGURIDAD

Estrategia de seguridad, nuevos retos

- La Unión Europea publicó el Reglamento del Parlamento Europeo y del Consejo por el que se establece el Programa Europa Digital para el período 2021-2027

- **Objetivos específicos:**

  - Informática de alto rendimiento.
  - Inteligencia artificial.
  - **Ciberseguridad y confianza.**
  - Competencias digitales avanzadas.
  - Despliegue, mejor uso de las capacidades digitales e interoperabilidad.

Estrategia de seguridad, nuevos retos

- La pandemia de la COVID-19 puso de relieve más que nunca la necesidad de ahondar en la modernización de la administración, y esto pasa por la digitalización de las relaciones entre las personas y las administraciones.
- El PEGIPGD 2030 (Ardatz) pretende contribuir a avanzar hacia una administración pública que:

  – Disponga de una **gobernanza de los datos** y de la información segura, que protege los datos personales y que genera valor social y económico.

- Un buen gobierno necesita de una buena administración con instrumentos como: **gobernanza de los datos y de la información.**

derten CIBERSEGURIDAD

Estrategia de seguridad, nuevos retos

- La **Seguridad** de la información y **continuidad de negocio** cobran una **nueva dimensión**.
- Obligatorio establecer una **estrategia de seguridad** para **reducir el riesgo** y **garantizar la continuidad del negocio** (Plan Director de Seguridad).
- **Nuevos retos** para todos:
  - ✓ Cumplimiento de normativas de seguridad.
  - ✓ Gobernanza de datos, innovación
  - ✓ Mantenimiento de reputación y confianza.

Estrategia de seguridad, nuevos retos

I Revolución industrial	II Revolución industrial	III Revolución industrial	
Ahorro de costes	Producción masiva	Reducción estructural	Personalización
Máquina	Proceso	Web	Datos
Tecnología	Logística	Innovación	Inteligencia

Figura 6. Evolución tecnológica y de la gestión. Adaptado a partir de "Transformación digital para las Administraciones Públicas. Crear valor para la ciudadanía del siglo XXI. Sergio Jiménez. Innap Innova. INAP, Instituto de Administración Pública, 2019.

Transformación digital

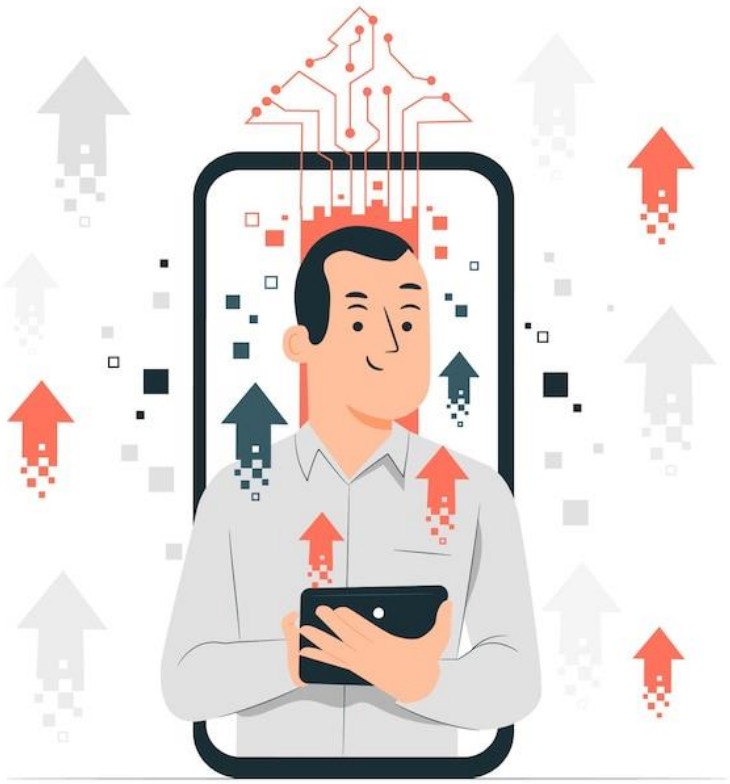
- **Cambio →** **oportunidades y riesgos**.

  - Transferencia de los riesgos (de clientes, etc.)

    → Externalización de procesos/servicios.
    → Cumplir requisitos:
      - Seguridad de la Información.
      - Continuidad/Resiliencia

- **Evolución →**

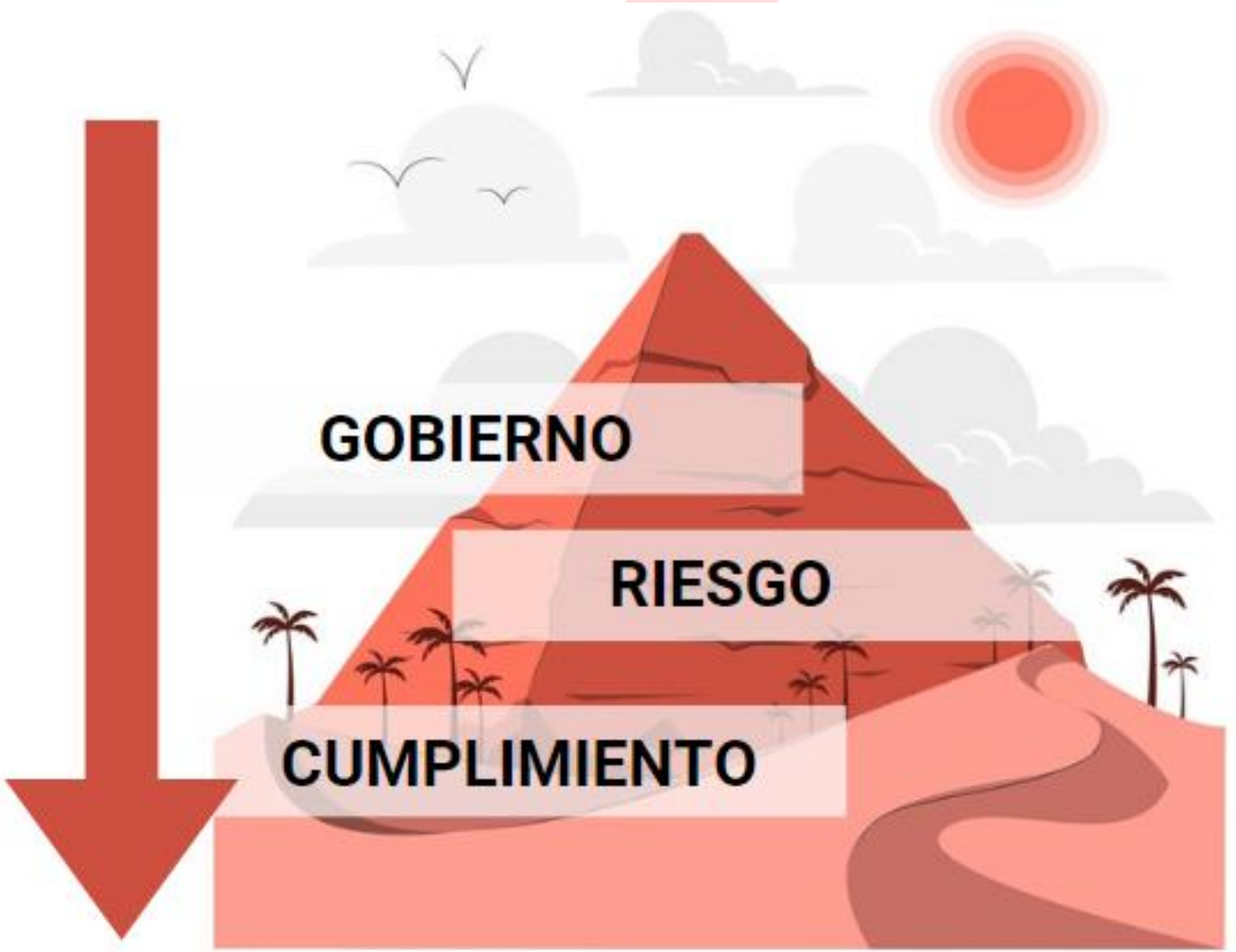
  → Soluciones tecnológicas (**Ciberseguridad)**
  → Soluciones de Gestión (**Consultoría SGSI)**



- **Innovación, confianza y reputación→ ROI**

derten CIBERSEGURIDAD

Modelo GRC



SG

SI

derten CIBERSEGURIDAD

¿Qué es un SGSI?

Sistema de Gestión de Seguridad de la Información y de Resiliencia Operativa Digital:

- Es un conjunto de **políticas**, **procedimientos** y **directrices** de administración de los activos de información esenciales en una organización.

- Tiene como objetivo **evaluar** y tratar los **riesgos** asociados con los datos e información que se manejan y a la continuidad de los servicios.

- Permite gestionar la **integridad**, **confidencialidad** y **disponibilidad, trazabilidad y autenticidad** de los activos críticos y los sistemas de información y procesos esenciales que los manejan.

derten CIBERSEGURIDAD

Objetivos y ventajas de implantar el Sistema

- **Asegurar** los activos información.
- **Reducir el riesgo.**
- Cumplimiento de las **normativas vigentes en seguridad**.
- Crear un **marco de trabajo** en materia de seguridad.
- Asentar y formalizar **la conciencia de seguridad**.
- Garantizar la **continuidad del negocio.**
- Alcanzar un **equilibrio** entre inversión y seguridad.
- Incremento de la **competitividad, posicionamiento y prestigio en el mercado.**

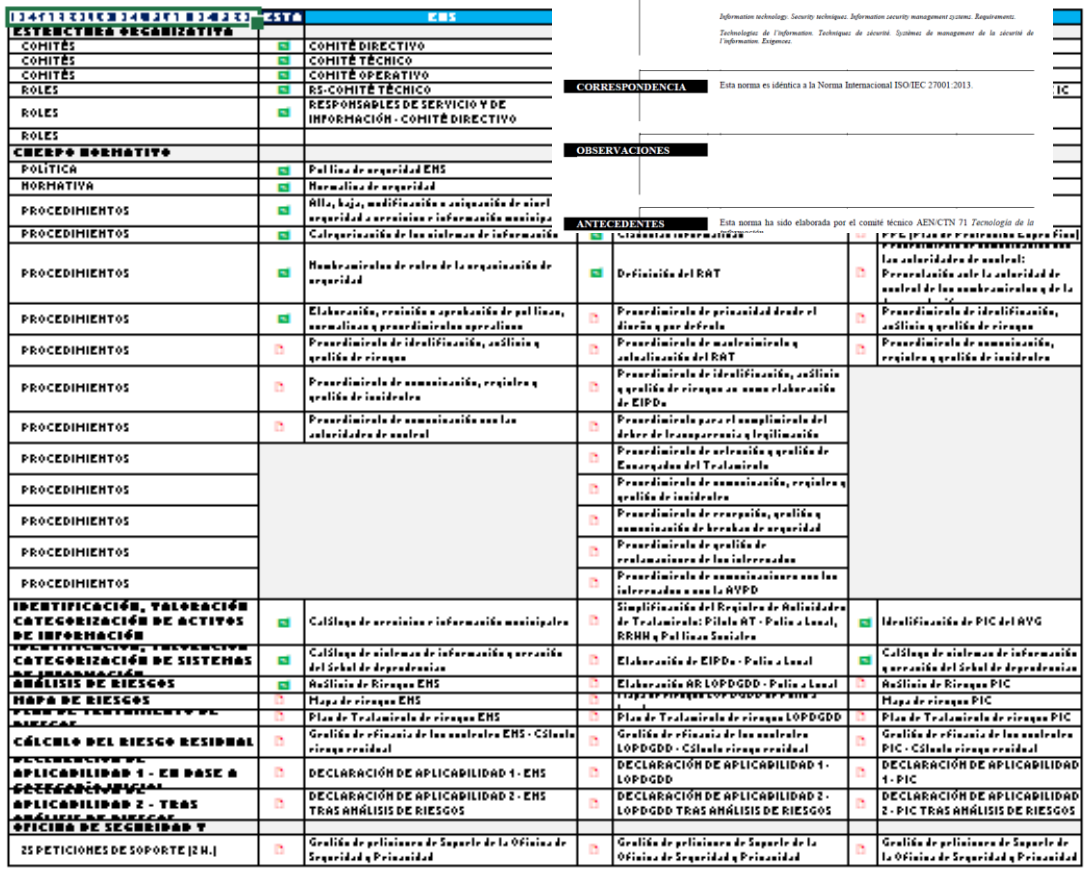
Ciclo PDCA de mejora continua

- Para **implantar el SGSI** se debe **utilizar el Ciclo de Deming o PDCA.**
- Estructurar **todos los procesos** de un sistema de gestión basado en la **mejora continua**.


CYBER SCAPE
2023
Network & Infrastructure Security
Advanced Threat Protection
NAC
SDN
DDoS Protection
DNS Security
Network Firewall
SASE
Deception
ICS + OT
Network Analysis & Forensics
Web Security
Endpoint Security
Endpoint Prevention
Endpoint Detection & Response
Application Security
WAF & Application Security
Application Security Testing
Risk & Compliance
Risk Assessment & Visibility
Risk Quantification
Pen Testing & Breach Simulation
Security Ops & Incident Response
SIEM
Security Incident Response
Security Analytics
Threat Intelligence
IoT
IoT Devices
Connected Home
Messaging Security
Identity & Access Management
Authentication
IDaaS
Privileged Management
Identity Governance
Consumer Identity
Digital Risk Management
Security Consulting & Services
Blockchain
Fraud & Transaction Security
Cloud Security
Container
Infrastructure
CASB
"La potencia, sin enfoque, no sirve para nada"

LEGAL SCAPE

Estándares



norma española

UNE-ISO/IEC 27001

Noviembre 2014

TÍTULO Tecnología de la información

Técnicas de seguridad

Sistemas de Gestión de Seguridad de la Información (SGSI)

Requisitos

Information technology. Security techniques. Information security management systems. Requirements.

Technologies de l'information. Techniques de sécurité. Systèmes de management de la sécurité de l'information. Exigences.

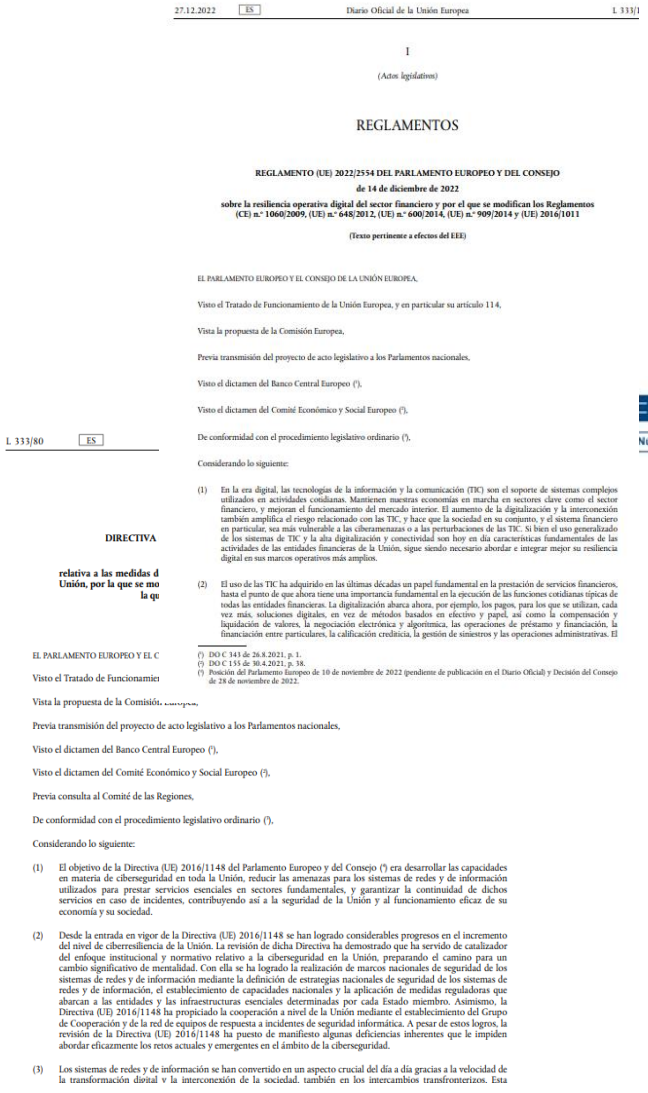
CORRESPONDENCIA Esta norma es idéntica a la Norma Internacional ISO/IEC 27001:2013.

OBSERVACIONES

ANTECEDENTES Esta norma ha sido elaborada por el comité técnico AEN/CTN 71 *Tecnología de la*

	ESTÁ	EMS			
ESTRUCTURA ORGANIZATIVA					
COMITÉS	✓	COMITÉ DIRECTIVO			
COMITÉS	✓	COMITÉ TÉCNICO			
COMITÉS	✓	COMITÉ OPERATIVO			
ROLES	✓	RS-COMITÉ TÉCNICO			
ROLES	✓	RESPONSABLES DE SERVICIO Y DE INFORMACIÓN - COMITÉ DIRECTIVO			
ROLES					
CUERPO NORMATIVO					
POLÍTICA	✓	Política de seguridad EMS			
NORMATIVA	✓	Normativa de seguridad			
PROCEDIMIENTOS	✓	Alta, baja, modificación o asignación de nivel seguridad a servicios e información municipa			
PROCEDIMIENTOS	✓	Categorización de los sistemas de información	✓	Sistemas información	PPE (Plan de Protección Empresarial)
PROCEDIMIENTOS	✓	Nombramiento de roles de la organización de seguridad	✓	Definición del RAT	Procedimiento de comunicación a las autoridades de control: Procedimiento ante la autoridad de control de los nombramientos y de la
PROCEDIMIENTOS	✓	Elaboración, revisión y aprobación de política, normativa y procedimientos operativos	✓	Procedimiento de privacidad desde el diseño y por defecto	Procedimiento de identificación, análisis y gestión de riesgos
PROCEDIMIENTOS	✓	Procedimiento de identificación, análisis y gestión de riesgos	✓	Procedimiento de mantenimiento y actualización del RAT	Procedimiento de comunicación, registro y gestión de incidentes
PROCEDIMIENTOS	✓	Procedimiento de comunicación, registro y gestión de incidentes	✓	Procedimiento de identificación, análisis y gestión de riesgos en una elaboración de EIPDs	
PROCEDIMIENTOS	✓	Procedimiento de comunicación con las autoridades de control	✓	Procedimiento para el cumplimiento del deber de transparencia y legitimación	
PROCEDIMIENTOS			✓	Procedimiento de selección y gestión de Encargados del Tratamiento	
PROCEDIMIENTOS			✓	Procedimiento de comunicación, registro y gestión de incidentes	
PROCEDIMIENTOS			✓	Procedimiento de recuperación, gestión y comunicación de brechas de seguridad	
PROCEDIMIENTOS			✓	Procedimiento de gestión de reclamaciones de los interesados	
PROCEDIMIENTOS			✓	Procedimiento de comunicaciones con los interesados a una la AVPD	
IDENTIFICACIÓN, VALORACIÓN CATEGORIZACIÓN DE ACTIVOS DE INFORMACIÓN	✓	Catálogo de servicios e información municipales	✓	Simplificación del Registro de Actividades de Tratamiento: Pilulo AT - Policía Local, RRHH y Policías Sociales	Identificación de PIC del AVG
IDENTIFICACIÓN, TRAVERSAL CATEGORIZACIÓN DE SISTEMAS DE INFORMACIÓN	✓	Catálogo de sistemas de información y servicios del Sobal de dependencias	✓	Elaboración de EIPDs - Policía Local	Catálogo de sistemas de información y servicios del Sobal de dependencias
ANÁLISIS DE RIESGOS	✓	Análisis de Riesgos EMS	✓	Elaboración AR LOPDGDD - Policía Local	Análisis de Riesgos PIC
MAPA DE RIESGOS	✓	Mapa de riesgos EMS	✓	Mapa de riesgos LOPDGDD	Mapa de riesgos PIC
PLAN DE TRATAMIENTO DE RIESGOS	✓	Plan de Tratamiento de riesgos EMS	✓	Plan de Tratamiento de riesgos LOPDGDD	Plan de Tratamiento de riesgos PIC
CÁLCULO DEL RIESGO RESIDUAL	✓	Gestión de eficiencia de los controles EMS - Cálculo riesgo residual	✓	Gestión de eficiencia de los controles LOPDGDD - Cálculo riesgo residual	Gestión de eficiencia de los controles PIC - Cálculo riesgo residual
DECLARACIÓN DE APLICABILIDAD 1 - EN BASE A CATEGORIZACIÓN	✓	DECLARACIÓN DE APLICABILIDAD 1 - EMS	✓	DECLARACIÓN DE APLICABILIDAD 1 - LOPDGDD	DECLARACIÓN DE APLICABILIDAD 1 - PIC
APLICABILIDAD 2 - TRAS ANÁLISIS DE RIESGOS	✓	DECLARACIÓN DE APLICABILIDAD 2 - EMS TRAS ANÁLISIS DE RIESGOS	✓	DECLARACIÓN DE APLICABILIDAD 2 - LOPDGDD TRAS ANÁLISIS DE RIESGOS	DECLARACIÓN DE APLICABILIDAD 2 - PIC TRAS ANÁLISIS DE RIESGOS
OFICINA DE SEGURIDAD Y					
25 PETICIONES DE SOPORTE (2 H.)	✓	Gestión de peticiones de Soporte de la Oficina de Seguridad y Privacidad	✓	Gestión de peticiones de Soporte de la Oficina de Seguridad y Privacidad	Gestión de peticiones de Soporte de la Oficina de Seguridad y Privacidad

Normativas



27.12.2022 ES Diario Oficial de la Unión Europea L 333/1

I

(Actos legislativos)

REGLAMENTOS

REGLAMENTO (UE) 2022/2554 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 14 de diciembre de 2022

sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 y (UE) 2016/1011

(Texto pertinente a efectos del EEE)

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 114,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de acto legislativo a los Parlamentos nacionales,

Visto el dictamen del Banco Central Europeo (1),

Visto el dictamen del Comité Económico y Social Europeo (2),

De conformidad con el procedimiento legislativo ordinario (3),

Considerando lo siguiente:

(1) En la era digital, las tecnologías de la información y la comunicación (TIC) son el soporte de sistemas complejos utilizados en actividades cotidianas. Mantienen nuestras economías en marcha en sectores clave como el sector financiero, y mejoran el funcionamiento del mercado interior. El aumento de la digitalización y la interconexión también amplifica el riesgo relacionado con las TIC, y hace que la sociedad en su conjunto, y el sistema financiero en particular, sea más vulnerable a las ciberamenazas o a las perturbaciones de las TIC. Si bien el uso generalizado de los sistemas de TIC y la alta digitalización y conectividad son hoy en día características fundamentales de las actividades de las entidades financieras de la Unión, sigue siendo necesario abordar e integrar mejor su resiliencia digital en sus marcos operativos más amplios.

(2) El uso de las TIC ha adquirido en las últimas décadas un papel fundamental en la prestación de servicios financieros, hasta el punto de que ahora tiene una importancia fundamental en la ejecución de las funciones cotidianas típicas de todas las entidades financieras. La digitalización abarca ahora, por ejemplo, los pagos, para los que se utilizan, cada vez más, soluciones digitales, en vez de métodos basados en efectivo y papel, así como la compensación y liquidación de valores, la negociación electrónica y algorítmica, las operaciones de préstamo y financiación, la financiación entre particulares, la calificación crediticia, la gestión de siniestros y las operaciones administrativas. El

(1) DO C 343 de 26.8.2021, p. 1.
(2) DO C 155 de 30.4.2021, p. 38.
(3) Posición del Parlamento Europeo de 10 de noviembre de 2022 (pendiente de publicación en el Diario Oficial) y Decisión del Consejo de 28 de noviembre de 2022.

L 333/80 ES

DIRECTIVA

relativa a las medidas d
Unión, por la que se mo
la qu

EL PARLAMENTO EUROPEO Y EL C

Visto el Tratado de Funcionamien

Vista la propuesta de la Comisión

Previa transmisión del proyecto de acto legislativo a los Parlamentos nacionales,

Visto el dictamen del Banco Central Europeo (1),

Visto el dictamen del Comité Económico y Social Europeo (2),

Previa consulta al Comité de las Regiones,

De conformidad con el procedimiento legislativo ordinario (3),

Considerando lo siguiente:

(1) El objetivo de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo (4) era desarrollar las capacidades en materia de ciberseguridad en toda la Unión, reducir las amenazas para los sistemas de redes y de información utilizados para prestar servicios esenciales en sectores fundamentales, y garantizar la continuidad de dichos servicios en caso de incidentes, contribuyendo así a la seguridad de la Unión y al funcionamiento eficaz de su economía y su sociedad.

(2) Desde la entrada en vigor de la Directiva (UE) 2016/1148 se han logrado considerables progresos en el incremento del nivel de ciberresiliencia de la Unión. La revisión de dicha Directiva ha demostrado que ha servido de catalizador del enfoque institucional y normativo relativo a la ciberseguridad en la Unión, preparando el camino para un cambio significativo de mentalidad. Con ella se ha logrado la realización de marcos nacionales de seguridad de los sistemas de redes y de información mediante la definición de estrategias nacionales de seguridad de los sistemas de redes y de información, el establecimiento de capacidades nacionales y la aplicación de medidas reguladoras que abarcan a las entidades y las infraestructuras esenciales determinadas por cada Estado miembro. Asimismo, la Directiva (UE) 2016/1148 ha propiciado la cooperación a nivel de la Unión mediante el establecimiento del Grupo de Cooperación y de la red de equipos de respuesta a incidentes de seguridad informática. A pesar de estos logros, la revisión de la Directiva (UE) 2016/1148 ha puesto de manifiesto algunas deficiencias inherentes que le impiden abordar eficazmente los retos actuales y emergentes en el ámbito de la ciberseguridad.

(3) Los sistemas de redes y de información se han convertido en un aspecto crucial del día a día gracias a la velocidad de la transformación digital y la interconexión de la sociedad, también en los intercambios transfronterizos. Esta

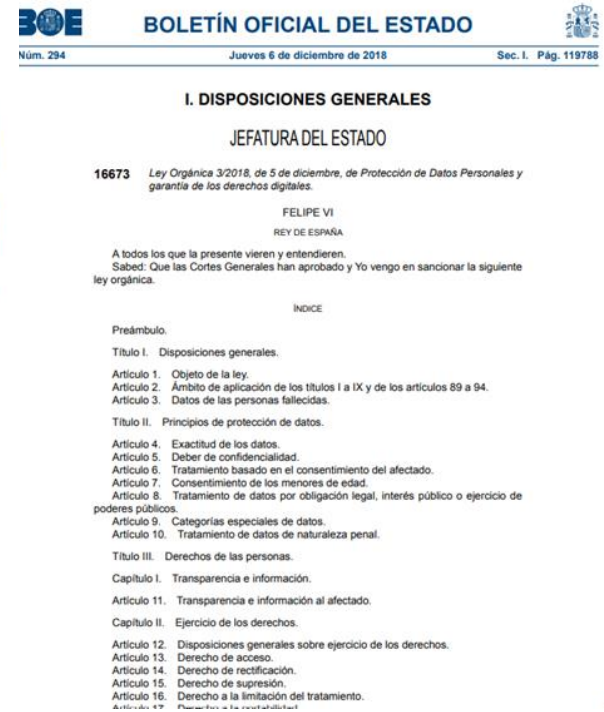
BOLETÍN OFICIAL DEL ESTADO
Núm. 106 Miércoles 4 de mayo de 2022 Sec. I. Pág. 61715

I. DISPOSICIONES GENERALES

MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

7191 *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.*

ÍNDICE



BOLETÍN OFICIAL DEL ESTADO
Núm. 294 Jueves 6 de diciembre de 2018 Sec. I. Pág. 119788

I. DISPOSICIONES GENERALES

JEFATURA DEL ESTADO

16673 *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.*

FELIPE VI

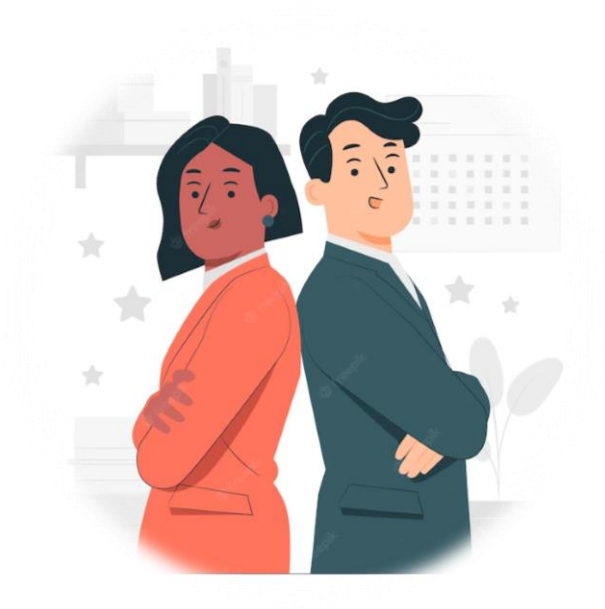
REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley orgánica.

ÍNDICE

Itinerario del cliente en derten CIBERSEGURIDAD



Acompañamiento y soporte a la implantación:

- Ámbito técnico, CISO y gobernanza de la seguridad.
- Ámbito legal y cumplimiento normativo.

derten CIBERSEGURIDAD

Mila esker

Gracias

Amaia Chaparro
Mail: amaia.chaparro@derten.com
Tel: 696 354 579