CÁTEDRA INCIBE
Digitalización y Ciberseguridad Hídrica

CATALAN WATER PARTNERSHIP

Universitat de Girona

cynexia cybersecurity

Josep Martí
Consultor Ciberseguridad

GRC – ENS – NIS2
Lead Auditor ISO27001
Auditor sistema ciberseguridad IT/OT

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

CÁTEDRA INCIBE
Digitalización y Ciberseguridad Hídrica

CATALAN WATER PARTNERSHIP

Universitat de Girona

cynexia cybersecurity

Formación en ciberseguridad del sector hídrico

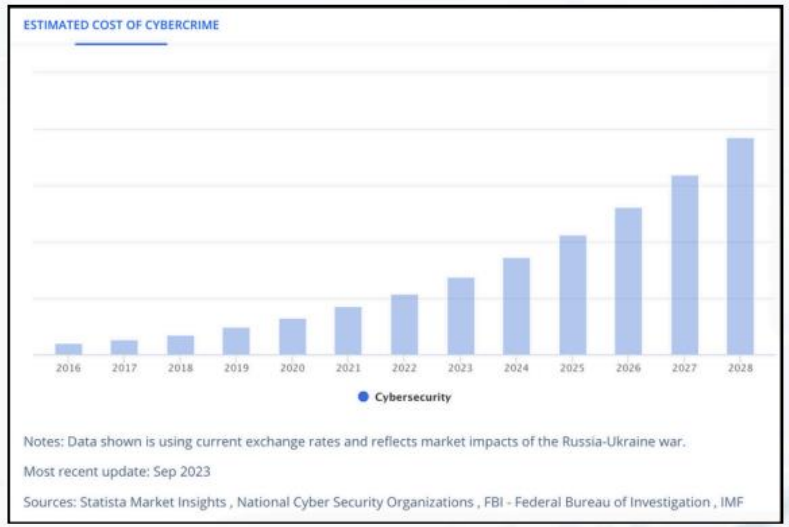
MODULO 1 – Casos hacking industrial
MODULO 2 – Conceptos de Ciberseguridad
MODULO 3 – OSINT superfície de ataque
MODULO 4 – Cumplimiento Normativo

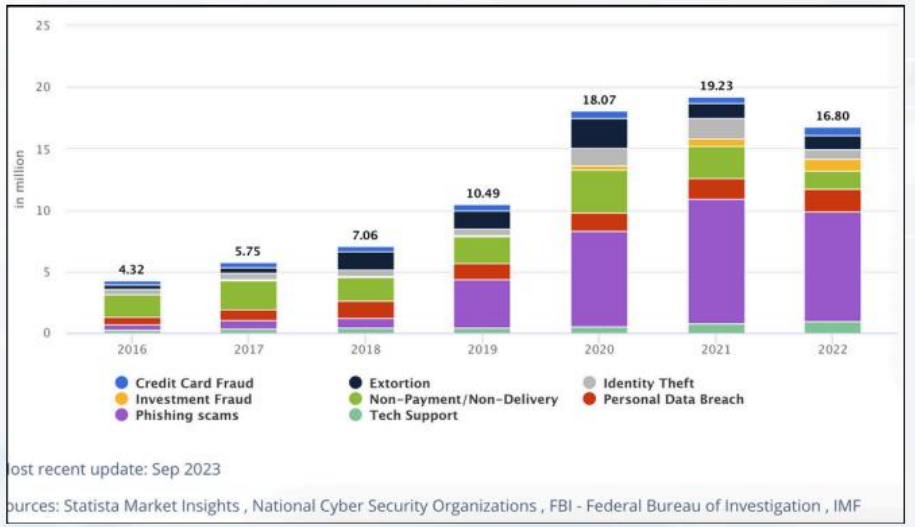
Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

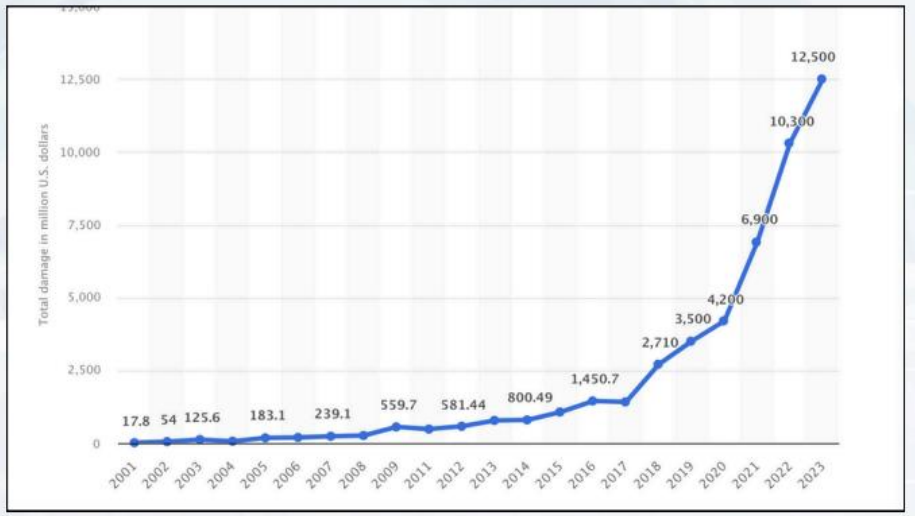
Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD





- Ciberataques con más impacto económico.
- Aumento de ataques (en todos los entornos).
- Aumento de la inversión en prevención y respuesta.
- Nuevas normativas específicas en ciberseguridad.



Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

	Fecha	Naturaleza del ataque	Impacto
Chinese infiltration of U.S. Water Systems (China)	Febrero 2024	Infiltración en infraestructura critica	Potencial daño a infraestructura crítica
Muleshoe, Texas, Water facility hack (EE.UU)	Enero 2024	Provoco desbordamiento de tanque de agua	El tanque se desbordó durante 35-45 minutos; sin impacto en el agua potable
Southern Water (Reino Unido)	Febrero 2024	Filtración de datos personales y operativos	Acceso a datos personales de clientes y empleados, compromiso del sistema informático interno
Danish Water Utility Plant (Dinamarca)	Diciembre 2024	Vulneración por deficiente ciberseguridad	Interrupción de servicio durante varias horas
FCC-Aqualia, Lleida	Mayo 2023	Secuestro de datos; Ransomware	Datos personales

Caso - Danish Water

1. Estado Previo

- Controles de Seguridad débiles

2. Vector acceso

- Actores pro-rusos
- Compromiso remote
- RDP, VPN, dashboards expuestos

3. Compromiso

- Acceso control Operativo
- Inutilizar sistemas
- 50 hogares fuera de servicio

4. consecuencias

- Corte temporal del suministro
- Imposibilidad gestión
- Operaciones parciales en manual

5. Detección y reacción

- Incidente reportado publicamente
- Identificada necesidad urgente

6. Enseñanzas

- Caso paradigmático informes oficiales
- Importania coordinacion operadores locales, CERT nacional

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Caso - Danish Water

December

2024

27 Jan 2025

Denmark warns of cyber threats to its water infrastructure

Denmark's cybersecurity authority has identified a 'very high' risk of cyberattacks on the country's water infrastructure.

CENTRE FOR CYBER SECURITY

THREAT ASSESSMENT

The cyber threat against the Danish water sector

February • 2025

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

MODULO 2 – Conceptos de Ciberseguridad

- Ecosistema de Amenazas
- IT vs OT
- Protocolos Industriales y sus debilitades
- Anatomía de un Ataque
- Estrategia Defensiva Integrada

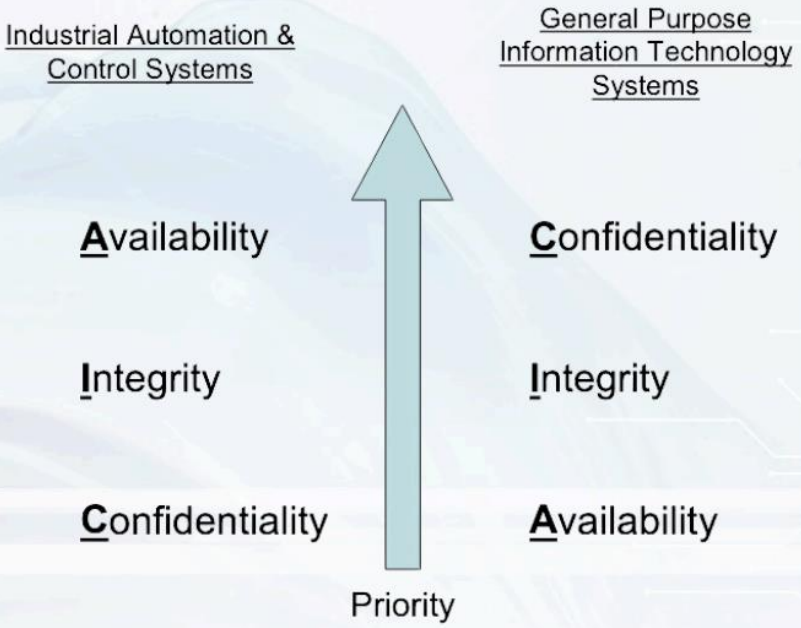
Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Ecosistema de Amenazas

- Oportunistas (Script Kiddies)
- Organizaciones Criminales
- Hacktivistas
- ATP
- Estados Nación
- Insiders

IT vs OT

	Entorno ICS	Entorno IT
Objetivo	Control y gestión de procesos industriales	Gestión de datos e información empresarial
Arquitectura	Jerárquica (SCADA, PLC, sensores)	Distribuida (servidores, estaciones de trabajo)
Protocolos	OPCUA, S7, FINS, PROFINET, [...]	HTTPS, SMTP, RDP, DNS, [...]
Actualizaciones	Ciclos de vida largos, difícil de actualizar	Actualizaciones frecuentes y parches
Ejemplos	PLCs (Siemens, Allen-Bradley), SCADA (Wonderware, Ignition)	Sistemas ERP (SAP, Oracle)



Protocolos industriales y sus debilidades

MODBUS TCP 502
- Texto plano
- Sin autenticación nativa
- Vulnerable manipulación

FINS (Omron)
- Texto plano
- Sin cifrado
- Sin autenticación

Profinet
- Vulnerabilidades
- Ampliamente usado
- Broadcast por diseño
- Sin autenticación

OPC Classic vs OPC UA
- Sin cifrado
- Dependencia DCOM Win

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Protocolos industriales y sus debilidades

MODBUS TCP 502
- Texto plano
- Sin autenticación nativa
- Vulnerable manipulación

FINS (Omron)
- Texto plano
- Sin cifrado
- Sin autenticación

Profinet
- Vulnerabilidades
- Ampliamente usado
- Broadcast por diseño
- Sin autenticación

OPC Classic vs OPC UA
- Sin cifrado
- Dependencia DCOM Win

Contramedidas
- Segmentar y aislar OT
- VPN, túnles TLS
- FW IDS IPS
- White list
- Monitoreo

Contramedidas
- Evitar exposición a redes
- FW IDS IPS
- Deshabilitar FINS no usa
- Monitoreo

Contramedidas
- Firmwares actualizados
- Segmentar red
- Monitoreo
- FW IDS IPS

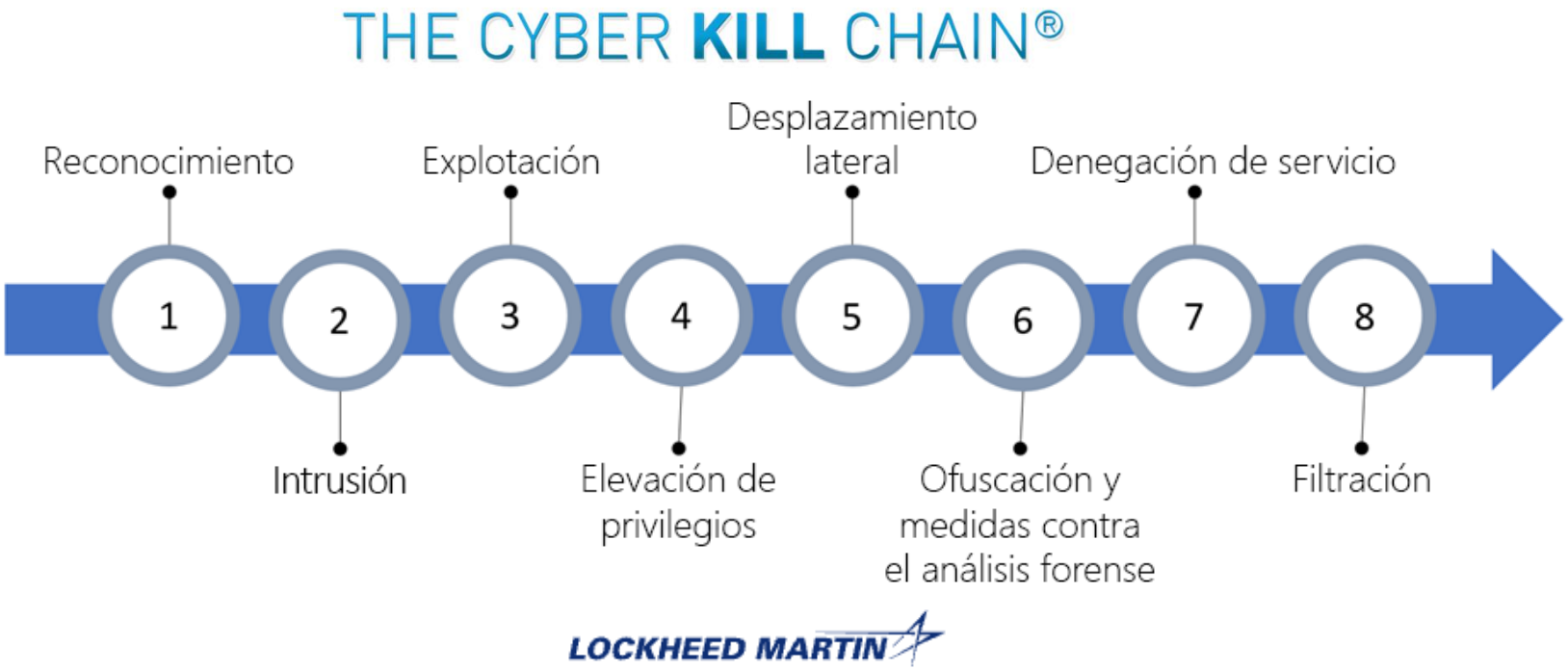
Contramedidas
- VPN
- Segmentación
- OPC UA

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
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Anatomía de un ataque

FASE 1:
Reconocimiento

- Shodan Scan
- Google Dorking
- Ingeniería social
- Subdomain Enumeration



Estrategia defensiva integrada

- CAPA 1: Perímetro
  - Firewalls NG con DPI
  - VPN MFA
  - Geoblocking
- CAPA 2: Network
  - Segmentación
  - Micro-segmentación por función
- CAPA 3: Endpoint
  - Antimalware Estaciones ingenieria
  - USB control
- CAPA 4: Aplicación
  - Hardening sistemes SCADA
  - Gestión de Vulnerabilidades
  - Backup y procedimientos de recuperación
- CAPA 5: Datos
  - Cifrado comunicacióones
  - Integridad de lògica de PLC
  - Auditoría de configuración

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

MODULO 3 - OSINT

- Qué és OSINT?
- Google Dorking
- Contexto Shodan

CÁTEDRA INCIBE
Digitalización y Ciberseguridad Hídrica

CWP
CATALAN WATER PARTNERSHIP

Universitat de Girona

cynexia
cybersecurity

OSINT

Open Source Intelligence: Metodología para la investigación y captura de información basada en fuentes abiertas accessible a través de Internet.

Google Dorking

Buscador e indexador de páginas webs, servicios accesibles públicamente a través de internet.

Shodan

Buscador e Indexador de dispositivos y servicios accesibles públicamente a través de internet

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

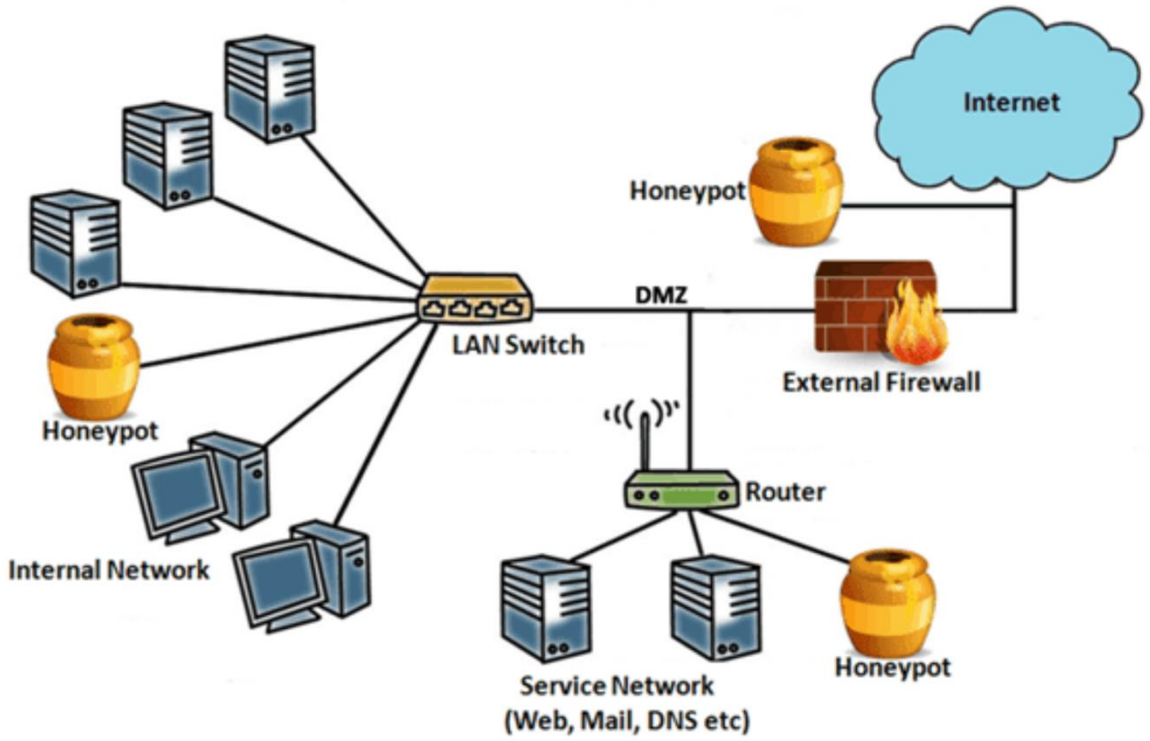
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

FASE 1 Reconocimiento inicial

DEMO

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Honeypots


Internet
Honeypot
DMZ
LAN Switch
External Firewall
Honeypot
Router
Internal Network
Service Network
(Web, Mail, DNS etc)
Honeypot

✅ HOY MISMO:

:: Buscar su empresa en Shodan
:: Googlearse: 'site:sudominio.es filetype:pdf'
:: Verificar subdominios en crt.sh
:: Revisar HavelBeenPwned

✅ ESTA SEMANA:

:: Auditar todos los sistemas con acceso a internet
:: Cambiar TODAS las contraseñas por defecto
:: Implementar VPN para acceso a SCADA
:: Segregar red OT de red IT

✅ 3 MESES:

:: Implementar monitorización continua
:: Formar al personal en seguridad
:: Plan de respuesta a incidentes
:: Auditoría externa profesional

CÁTEDRA INCIBE
Digitalización y Ciberseguridad Hídrica

CATALAN WATER PARTNERSHIP

Universitat de Girona

cynexia cybersecurity

MODULO 4 – Cumplimiento Normativo

NIS2 Directive

ens Esquema Nacional de Seguridad

International Organization for Standardization ISO 27001

IEC 62443

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

CÁTEDRA INCIBE
Digitalización y Ciberseguridad Hídrica

CWP
CATALAN WATER PARTNERSHIP

Universitat de Girona

cynexia
cybersecurity

LA RESPUESTA DE EUROPA: NIS2

NIS2 Directive

GESTIÓN DE RIESGOS DE SEGURIDAD

Implementación de políticas de análisis de riesgos, seguridad de la cadena de suministro, políticas de copias de seguridad (backups) y recuperación de desastres.

GESTION DE INCIDENTES

Notificación obligatoria de incidentes de seguridad significativos en un plazo de 24 horas (notificación preliminar) y 72 horas (notificación del incidente).

AUDITORIAS

Se reforzarán los requisitos de auditoría y supervisión por parte de las autoridades competentes.

FORMACIÓN Y CONCIENCIACIÓN

Obligación de formar al personal en ciberseguridad para aumentar la resiliencia humana ante amenazas.

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

CÁTEDRA INCIBE
Digitalización y Ciberseguridad Hídrica

CWP
CATALAN WATER PARTNERSHIP

Universitat de Girona

cynexia
cybersecurity

¿ A quién afecta?

NIS2 Directive

ENTITADES ESENCIALES

Las más críticas para la sociedad
Aquí encontramos Energía, transporte, banca, sanidad y agua.

ENTIDADES IMPORTANTES

Otros Sectores vitals para la economia y el dia a dia, como empresas de servicios digitales (mercados en linea), servicios postales, alimentación, gestion de residuos y fabricación de productov estratégicos.

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

LA RESPUESTA DE EUROPA: NIS2

Cronología NIS2

16/01/2023 Entrada en vigor.

17/10/2023 La comisión revisa las directivas y reporta al Parlamento Europeo.

17/10/2024 Data límite para la transposición de los estados miembros

17/04/2025 Publicación listado entidades importanes y esenciales.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

LA RESPUESTA DE EUROPA: NIS2

Sanciones

EMPRESAS ESENCIALES	Multas de hasta 10 millones de euros o el 2% de la facturación mundial anual, la cantidad que sea superior.
EMPRESAS IMPORTANTES	Multas de hasta 7 millones de euros o el 1,4% de la facturación mundial anual, la cantidad que sea superior.
RESPONSABILIDAD PERSONAL	Posibilidad de que los directivos puedan ser considerados responsables si no toman las medidas adecuadas de ciberseguridad.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

ESQUEMA NACIONAL DE SEGURIDAD

- Establece principios básicos
- Ámbito Español
- Complementario NIS2
- Marco Certificable

Frameworks referencia

International Organization for Standardization
ISO
27001

IEC
62443

Gracias