



INSTITUTO NACIONAL DE CIBERSEGURIDAD



Jornada Operativa de Parques Eólicos 2025

MEJORAS EN LA OPERATIVA, LOGÍSTICA Y SEGURIDAD (SAFETY & CYBERSECURITY)



Implicaciones de los cambios normativos en la configuración y seguridad de los parques

Enrique Redondo Martínez

Responsable de ciberseguridad, Sectores Estratégicos, INCIBE



MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN
E INTELIGENCIA ARTIFICIAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD



Balance de ciberseguridad 2024



GOBIERNO
DE ESPAÑA

MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN
E INTELIGENCIA ARTIFICIAL

incibe
INSTITUTO NACIONAL DE CIBERSEGURIDAD



+16,6%
más que en 2023

97.348
incidentes de
ciberseguridad

183.851
sistemas vulnerables

Un sistema vulnerable es como una casa con una cerradura rota, más fácil para los intrusos entrar y causar problemas.

! Cualquier problema digital que ponga en riesgo los datos o la seguridad de los dispositivos, como, por ejemplo, un virus informático.



DEL TOTAL DE INCIDENTES DE CIBERSEGURIDAD

Se ven afectadas
31.540 empresas
españolas
43,18% más que en 2023



65.808 ciudadanos
son víctimas de
incidentes
12,07% más que en 2023

12,07% más que en 2023

341
operadores esenciales
e importantes*

Empresas o servicios que son muy importantes para el funcionamiento diario de la sociedad. Incluye sectores, como la energía, el agua o las comunicaciones.



*Entidades alineadas con lo dispuesto para la tipología de operadores en la directiva NIS2

NIS 2: Sectores de alta criticidad



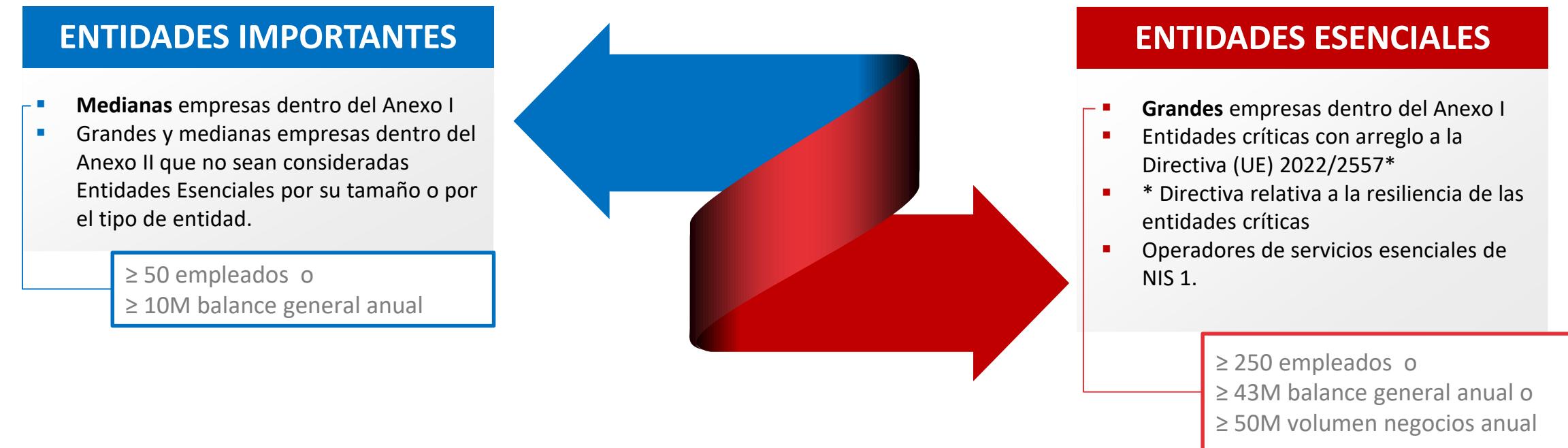
◆ Nuevo NIS2

◆ Más tipos en NIS2

NIS 2: Otros sectores críticos



NIS 2: Sujetos obligados



* Hay excepciones

NIS 2: Medidas de ciberseguridad

Artículo 21.2 a  Gestión de riesgos y política de seguridad <ul style="list-style-type: none">■ Marco de gobierno de la ciberseguridad■ Roles y responsabilidades■ Postura de ciberseguridad■ Medidas para mitigar los riesgos	Artículo 21.2 b  Gestión de Incidentes <ul style="list-style-type: none">■ Detección, notificación y respuesta■ Planes y procedimientos	Artículo 21.2 c  Continuidad de negocio <ul style="list-style-type: none">■ Desarrollo de planes (crisis, continuidad, contingencias) que aseguren continuidad en caso de incidente■ Realizar formación y simulacros de continuidad de negocio	Artículo 21.2 d  Seguridad cadena suministro <ul style="list-style-type: none">■ Evaluar riesgos de ciberseguridad en la cadena de suministro■ Medidas de mitigación■ Evaluar riesgos e impactos en la cadena de suministro	Artículo 21.2 e  Adquisición, desarrollo y mantenimiento de sistemas y redes <ul style="list-style-type: none">■ Escaneo de vulnerabilidades, y test de penetración regulares■ Medidas de mitigación de vulnerabilidades■ Ciberhigiene y formación frecuentes
Artículo 21.2 f  Eficacia de las medidas <ul style="list-style-type: none">■ Políticas y procedimientos de evaluación de medidas■ Auditorías y pruebas frecuentes	Artículo 21.2 g  Concienciación y formación <ul style="list-style-type: none">■ Programa integral de formación y concienciación■ Formación continua■ Formación y testeo aplicados para reforzar lo aprendido	Artículo 21.2 h  Cifrado <ul style="list-style-type: none">■ Utilizar cifrado para preservar integridad, confidencialidad y autenticidad de los datos■ Implementar prácticas de gestión de claves■ Pruebas y formación sobre cifrado	Artículo 21.2 i  RRHH, Control de acceso, gestión activos <ul style="list-style-type: none">■ Procedimientos para empleados con acceso a info. sensible■ Formación y pruebas sobre control de acceso■ Evaluar las medidas sobre el inventario de activos	Artículo 21.2 j  Autenticación y transferencia de información <ul style="list-style-type: none">■ Implementar 2FA o autenticación continua, para voz, video, texto y comunicaciones

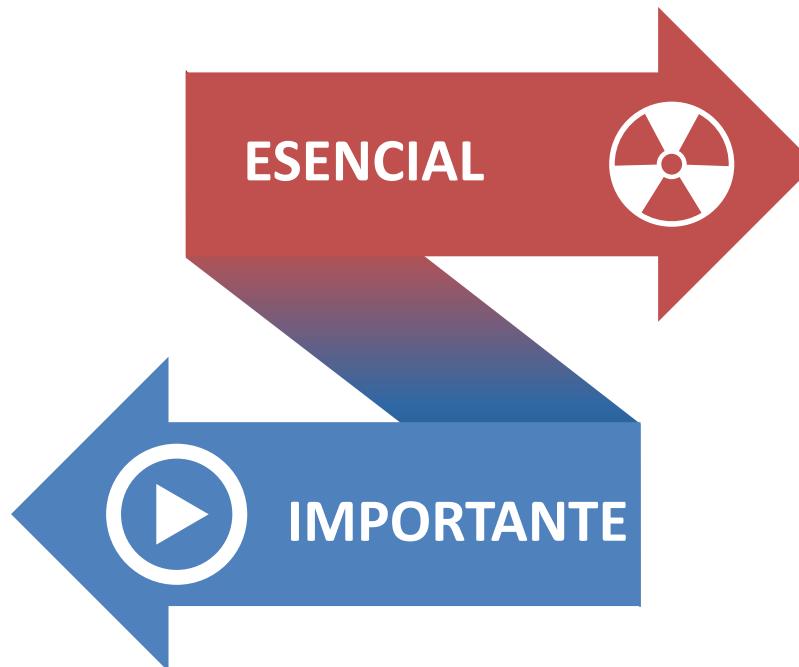
NIS 2: Sanciones

7.000.000 €

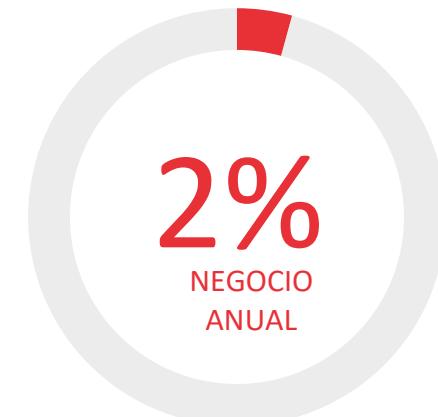


ENTIDADES IMPORTANTES

Multas administrativas de hasta **7 millones de €** o **1,4% volumen negocios anual**, la cuantía mayor



10.000.000€



ENTIDADES ESSENCIALES

Multas administrativas de hasta **10 millones de €** o **2% volumen negocios anual**, la cuantía mayor

* La personas físicas que representen a la entidad podrán ser responsables del incumplimiento.



ES-ISAC Energía, julio 2024

- ❖ Personalización de los servicios de INCIBE al sector
- ❖ Nuevas iniciativas



es-isac-energia@incibe.es

Gracias