Notificación importante desde Intec Cybersecurity

Entrada en vigor de la normativa europea en ciberseguridad NIS2

INTEC

REAL CYBERSECURITY

Red Nacional de SOC

CSIRT.es

FIRST

ISO 9001

ISO/IEC 20000-1

ISO 22301

ISO/IEC 27001

NOTIFICACION

- Se notifica a todos los interesados que desde el 18 de octubre de 2024 es de **obligado cumplimiento la Directiva Europea NIS2.**

- Dicha directiva es la legislación en materia de ciberseguridad adoptada para toda la Unión Europa que entró en vigor en Enero de 2023.

- https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963

INTEC
REAL CYBERSECURITY

¿Esto qué significa?

- Hay una serie de sectores empresariales que están obligados a adaptarse a dicha norma debiendo **cumplir con unos mínimos en ciberseguridad.**

- Hay un régimen sancionador de hasta 10M€ o hasta un 2% de la facturación para la empresa y consecuencias para los órganos de dirección como su cese del puesto.

- Las empresas podrán ser sometidas a supervisión y en casos graves de incumplimiento se les podrá suspender la actividad.

Red Nacional de SOC

INTEC
REAL CYBERSECURITY

Sectores implicados

Anexo I: Sectores de alta criticidad

* Las imágenes han sido obtenidas de la web del Incibe.

- Nuevo NIS2
- Más tipos en NIS2

Red Nacional de SOC
CSIRT.es
FIRST
ISO 9001
ISO/IEC 20000-1
ISO 22301
ISO/IEC 27001

INTEC
REAL CYBERSECURITY

Sectores implicados

Red Nacional de SOC

INTEC
REAL CYBERSECURITY

Sectores implicados

Red Nacional de SOC

INTEC
REAL CYBERSECURITY

Supervisión y auditorías

Supervisión *ex ante* y *ex post*

Las autoridades de cada sector deben supervisar el cumplimiento de esta directiva y podrán adoptar un enfoque de gestión de riesgos para priorizar estas tareas.

Las actividades de supervisión serán realizadas por profesionales cualificados.

Esenciales *(a priori y a posteriori)*

- A. Inspecciones *in situ* y a distancia incluidas aleatorias.
- B. Auditorías de seguridad periódicas y específicas.
- C. Auditorías *ad hoc* (tras un incidente).
- D. Análisis de seguridad.
- E. Solicitudes de información necesaria para evaluar las medidas de gestión de riesgos adoptadas.
- F. Solicitudes de acceso a datos e información para supervisión.
- G. Solicitudes de pruebas de la aplicación de las políticas de ciberseguridad, como, por ejemplo, los resultados de las auditorías.

Importantes *(a posteriori)*

- A. Inspecciónes *in situ* y supervisión a posteriori.
- B. Auditorías de seguridad específicas.
- C. Análisis de seguridad.
- D. Solicitudes de información necesaria para evaluar a posteriori las medidas de gestión de riesgos adoptadas.
- E. Solicitudes de acceso a datos e información para supervisión.
- F. Solicitudes de pruebas de la aplicación de las políticas de ciberseguridad, como, por ejemplo, los resultados de las auditoría.

Red Nacional de SOC

INTEC
REAL CYBERSECURITY

Régimen sancionador

Entidad esencial	Entidad importante
Un máximo de al menos 10.000.000 euros o hasta el 2% del volumen de negocios total anual a escala mundial de la empresa a la que pertenezca la entidad esencial en el ejercicio precedente, optándose por la de mayor cuantía.	Un máximo de al menos 7.000.000 euros o el 1,4% del volumen de negocios total anual a nivel mundial de la empresa a la que pertenece la entidad importante en el ejercicio precedente, optándose por la de mayor cuantía.

Equipos directivos

La alta dirección tiene la responsabilidad última de la gestión de los riesgos de ciberseguridad en entidades esenciales e importantes. El incumplimiento por parte de la dirección de los requisitos que establece la NIS2 podría tener graves consecuencias, incluyendo responsabilidad, prohibiciones temporales y multas administrativas, según lo previsto en la legislación nacional de la aplicación.

Los equipos directivos de las entidades esenciales e importantes son responsables de:

Aprobar

Aprobar la adecuación de las medidas de gestión de riesgos de ciberseguridad adoptadas por la entidad.

Supervisar

Supervisar la aplicación de las medidas de gestión de los riesgos.

Formarse

Formarse con el fin de adquirir suficientes conocimientos y habilidades para identificar riesgos y evaluar las prácticas de gestión de riesgos de ciberseguridad y su impacto en los servicios prestados por la entidad.

Ofrecer

Una formación similar a sus empleados de forma regular.

Responsabilizarse

Del incumplimiento.

Red Nacional de SOC · CSIRT.es · FIRST · ISO 9001 · ISO/IEC 20000-1 · ISO 22301 · ISO/IEC 27001

Más información

- Aplica a partir de mediana empresa (a más de 49 trabajadores o un volumen de más de 10M€) y a ciertas microempresas una vez se haya hecho la transposición en España.

- Si su empresa está afectada por esta directiva y necesita más información, contáctenos al email comercial@inteccybersecurity.com.

* Toda la información ha sido obtenida del Incibe (Instituto Nacional de Ciberseguridad de España) y del CCN-CNI, la fecha tope para que España realizase la transposición era el 17 de Octubre pero a día de hoy (05/11/2024) no tenemos noticias que así sea.