REGUVARA · GUÍA PRÁCTICA GRATUITA

NIS2: preparar los canales de notificación y las evidencias

Un primer paso práctico para dirección, TI/seguridad, asesoría jurídica y cumplimiento. Orientación sobre el ámbito, los principales plazos de notificación y cinco acciones iniciales.

Objetivo: hacer visibles rápidamente las preguntas adecuadas. Esta guía no determina de forma vinculante si una entidad jurídica concreta está dentro del ámbito de NIS2.

1. Evaluar inicialmente el ámbito de aplicación

• Relacionar la actividad, el servicio y la entidad jurídica con los sectores de los anexos I y II de la Directiva NIS2. El nombre del sector, por sí solo, no determina la inclusión.

• Comprobar tamaño, vínculos societarios, tipo de servicio, designaciones críticas, excepciones y normas del Estado miembro correspondiente. Algunas entidades o servicios pueden estar incluidos con independencia del umbral de tamaño habitual.

• Para cada entidad potencialmente afectada, documentar países, centros, servicios, autoridad competente, obligaciones de registro y contacto, y el razonamiento.

2. Fases de notificación de la UE para un incidente significativo

Fase	Base de la UE conforme al artículo 23	Pregunta de preparación
Alerta temprana	Sin demora indebida y, como máximo, en las 24 horas siguientes a tener conocimiento del incidente significativo.	¿Quién inicia el cómputo, decide e identifica a la autoridad adecuada?
Notificación del incidente	Sin demora indebida y, como máximo, en las 72 horas desde que se tiene conocimiento; evaluación inicial de gravedad e impacto e indicadores, si están disponibles.	¿Cómo se recopilan en paralelo hechos, marcas de tiempo y cuestiones pendientes?
Informe intermedio	Si lo solicita el CSIRT o la autoridad competente.	¿Quién registra los cambios y responde a las preguntas de seguimiento?
Informe final	Por regla general, en el plazo de un mes desde la notificación del incidente. Si el incidente sigue en curso, en ese momento se presenta un informe de situación y el informe final dentro del mes siguiente a su gestión.	¿Quién confirma el plazo nacional y el contenido requerido?

Estos plazos se refieren a incidentes significativos y al momento en que se tiene conocimiento de ellos. Los prestadores de servicios de confianza están sujetos a una regla especial de 24 horas para notificar incidentes. Comprueba la transposición nacional, las normas sectoriales y otras leyes de la UE aplicables.

HOJA DE TRABAJO

Del texto legal al primer proceso de trabajo

NIS2 exige medidas técnicas, operativas y organizativas proporcionadas y basadas en el riesgo. Esta síntesis ayuda a reunir a las primeras personas responsables.

3. Temas contemplados en el artículo 21

Las medidas protegen las redes y los sistemas de información utilizados para los servicios, incluido su entorno físico. Su alcance y diseño dependen del riesgo y la proporcionalidad.

Área	Ejemplo de pregunta de trabajo
Análisis de riesgos y seguridad de sistemas	¿Qué servicios, sistemas, amenazas y dependencias se incluyen? ¿Quién actualiza la evaluación?
Gestión de incidentes	¿Cómo se organizan la detección, clasificación, contención, escalado, preservación de pruebas y revisión posterior?
Continuidad y crisis	¿Están documentados y probados las copias de seguridad, la recuperación, las funciones de crisis y los objetivos de restablecimiento?
Cadena de suministro	¿Se registran proveedores directos, dependencias críticas e información de seguridad?
Adquisición y desarrollo seguros	¿Cómo se seleccionan y mantienen los sistemas de forma segura y se gestionan o divulgan las vulnerabilidades?
Revisión de eficacia	¿Cómo determina la organización si funcionan las medidas de seguridad?
Higiene cibernética y formación	¿Qué prácticas básicas y formaciones están previstas y documentadas?
Criptografía	¿Qué normas se aplican a la criptografía y, cuando proceda, al cifrado?
Personal, accesos y activos	¿Cómo se controlan permisos, cambios de personal, activos y accesos?
Autenticación y comunicación	¿Dónde son adecuadas la MFA o la autenticación continua, las comunicaciones seguras y los canales de emergencia?

4. Cinco primeros pasos útiles

- Designar a una persona responsable de coordinar las preguntas sobre el ámbito y los asuntos pendientes.
- Inventariar servicios, entidades jurídicas, sistemas y proveedores directos críticos.
- Nombrar responsables de dirección, incidentes, TI/seguridad, asesoría jurídica/cumplimiento y comunicación, con suplentes.
- Verificar la autoridad nacional competente, el CSIRT, el registro, el canal de notificación y las obligaciones sectoriales.
- Realizar un breve ejercicio: detectar un incidente, registrar cuándo se conoció, escalarlo y reunir los hechos.

NIS2 no se aplica automáticamente a todas las empresas. El ámbito depende, entre otros factores, de la actividad, el tamaño, la entidad jurídica, el Estado miembro, los casos especiales y las normas sectoriales.

FUENTES Y ESTADO JURÍDICO

Fuente principal: Directiva (UE) 2022/2555, en particular los artículos 2-4, 20, 21 y 23 y los anexos I-II. La propuesta COM(2026) 13 final no es legislación vigente. El 8 de octubre de 2026, el procedimiento 2026/0012(COD) del Parlamento Europeo estaba pendiente de decisión de comisión; el 24 de septiembre de 2026 se había publicado un proyecto de informe. La transposición nacional y las normas sectoriales no se han revisado país por país.
NIS2 Directive (EUR-Lex) · European Commission FAQ · National transposition · EP procedure 2026/0012(COD) · COM(2026) 13 proposal