a3Sec

<SHIELDING DIGITAL ASSETS GLOBALLY>

>_

DESMITIFICANDO NIS2

Guía práctica de cumplimiento de la directiva

a3Sec.com

Guía de implantación NIS2

Objeto

La directiva NIS2 no pone el foco en los operadores de servicios esenciales y los proveedores de servicios digitales, sino que se centra en las entidades esenciales e importantes en función de su tamaño, repercusión y sector.

Esta directiva pretende ser un marco de referencia para ayudar a las infraestructuras esenciales de los servicios básicos e importantes a estar preparadas y a combatir las amenazas cibernéticas.

- **Desarrollo y registro europeo de vulnerabilidades** (vulnerabilidades descubiertas en toda Europa).

- **CyCLONE o la red de organizaciones de enlace para crisis cibernéticas**, lo que facilitará, junto con un grupo de cooperación, una estrecha colaboración en el intercambio de información y el conocimiento de la situación. Establecerá vínculos entre el nivel técnico, entre los CSIRT (red de equipos de respuesta ante incidentes de seguridad cibernética) y la red política de la Unión Europea.

- **Informe anual sobre el estado de la ciberseguridad en la Unión Europea**, que mantendrá informados a los estados miembros en materia de ciberseguridad, las áreas de mejora y la situación concerniente a las amenazas cibernéticas.

- **Documentación de todos los proveedores de servicios digitales transfronterizos:** Crear y mantener un informe de todas las entidades que prestan servicios transfronterizos, como la computación en la nube, los servicios de centros de datos, los servicios de DNS, los registros de nombres de dominio de nivel superior (TLD), los registros de nombres de dominio, etc.

- **Permitir las evaluaciones entre homólogos de los Estados miembros para ayudarles a mantener al día sus ciber estrategias.**

Obligatoriedad de cumplimiento

La Directiva NIS2 exige la aplicación de nuevas medidas en materia de:

- Análisis de riesgos y seguridad de la información.
- Continuidad de la actividad empresarial.
- Seguridad en la cadena de distribución.
- Gestión de incidentes y de las prácticas de desarrollo de sistemas de información (revelación de vulnerabilidades, criptografía, cifrado o autenticación de doble factor).

* Además, puede exigir también que adopte el uso de determinados procesos, servicios, productos y bienes de las tecnologías de información y la comunicación (TIC) que se hayan incorporado en virtud de la ley en materia de seguridad prevista en la ENISA (Agencia de la Unión Europea para la Ciberseguridad).

Alcance

Entidades Esenciales	Entidades Importantes
Grandes operadores de **once** sectores esenciales y casos especiales.	Grandes operadores de **siete** sectores importantes y operadores de tamaño mediano.
Gran umbral con: Más de 50 empleados. Volumen de negocios superior a 50 millones de euros. Un balance superior a 43 millones de euros.	**Umbral medio con:** 50 a 25 empleados. Volumen de negocios entre 10 y 50 millones de euros. Un balance inferior a 43 millones de euros.
1. Energía (electricidad, sistemas urbanos de calefacción y de refrigeración, crudo, gas, hidrógeno,) 2. Transporte (aéreo, ferroviario, fluvial, vial). 3. Entidades bancarias. 4. Infraestructuras de los mercados financieros. 5. Sanidad (servicios públicos, laboratorios, I+D, fármacos). 6. Suministradores y distribuidores de agua potable. 7. Compañías dedicadas a la recogida, eliminación o el tratamiento de aguas residuales urbanas. 8. Infraestructura digital (proveedor de puntos de intercambio de internet (IXP), proveedores de servicios DNS, registros de nombres de dominio de nivel superior (TLD), servicios del centro de datos, proveedores de servicios de computación en la nube, redes de distribución de contenido, servicios de confianza. 9. Gestión de servicios TIC (de empresa a empresa; proveedores de servicios gestionados y proveedores de servicios de seguridad gestionados) 10. Administración Pública 11. Espacio.	1. Servicios postales y de mensajería. 2. Gestión de residuos. 3. Sustancias químicas. 4. Alimentos. 5. Industria (tecnología e ingeniería). 6. Servicios digitales (mercados en línea, motores de búsqueda en línea, redes sociales). 7. Investigación.
Las entidades esenciales deberán someterse a supervisión **de manera pro activa.**	Las entidades importantes quedarán sujetas a un régimen de supervisión **pasivo.**
En caso de las entidades esenciales, las multas administrativas pueden ser de hasta 10 millones de euros o de hasta el 2% del volumen de negocios total anual a nivel mundial de la empresa a la que pertenezca la entidad durante el ejercicio anterior.	En el caso de las entidades importantes, la directiva NIS2 permite la aplicación de multas administrativas de hasta 7 millones de euros o de hasta el 1,4% del volumen de negocios total anual a nivel mundial de la empresa a la que pertenezca la entidad durante el ejercicio anterior, lo que es definitivamente una cifra mayor.
En caso de incumplimiento, las sanciones son significativamente más elevadas para las entidades esenciales.	En caso de incumplimiento, las entidades importantes se enfrentarán a sanciones más leves que las entidades esenciales.

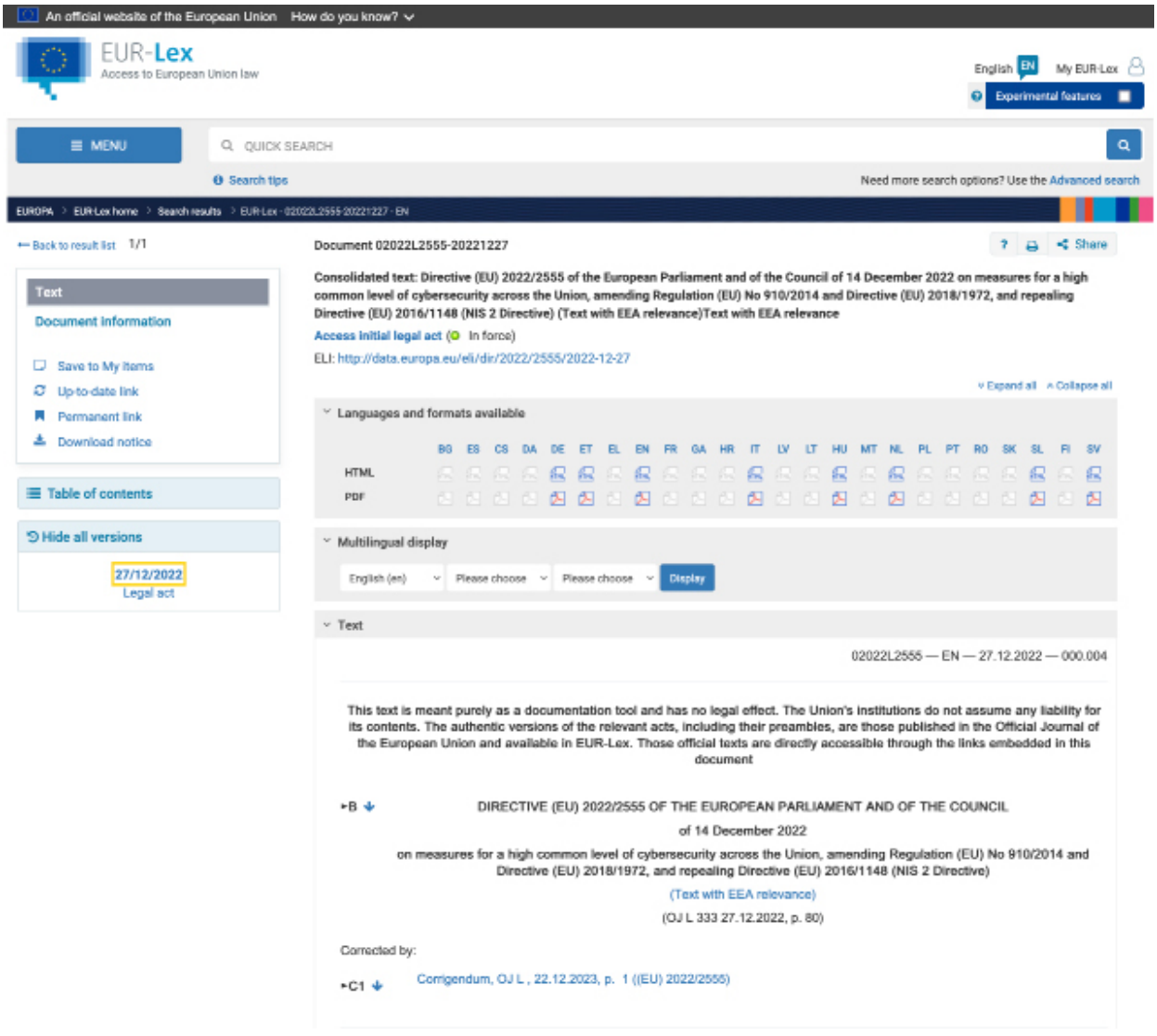
Tanto las entidades esenciales como las entidades importantes deberían tener en cuenta el impacto por incumplimiento sobre su negocio, ya que NIS2 establece medidas de suspensión y ejecución relativas tanto a entidades esenciales como a entidades importantes, que pueden conllevar en el caso de las entidades esenciales a la destitución del CEO y que obliga a estas entidades a establecer medidas de continuidad para evitar el cese total o temporal de sus operaciones.

Normativa de aplicación

NIS2.

Visitar el enlace:

[EUR-Lex - 02022L2555-20221227 - ES - EUR-Lex (europa.eu)]



>_

Playbook cumplimiento

1 / Conseguir soporte en la gestión: La Alta Dirección debe mostrar compromiso para su aplicación (a pesar de su obligatoriedad, debe mostrarse el compromiso) así como proporcionar los recursos suficientes para su rápida implementación y garantizar su cumplimiento.

2 / Configurar su aplicación como la gestión de un proyecto, deben establecerse los roles involucrados de forma formal para que una Directiva tan compleja sea implantada de forma eficaz. Además, es necesario tener claros los hitos para su implementación, responsabilidades y las consecuencias del incumplimiento.

3 / Realizar una formación inicial: En NIS2, se hace mucho hincapié en esto, si todos los involucrados en el proyecto disponen desde el inicio de qué es necesario hacer y por qué es necesario, será mucho más sencilla la involucración de todas las partes para que el proyecto se realice de forma satisfactoria.

4 / Redactar una política de primer nivel sobre la Seguridad de los Sistemas de Información: Aunque no es obligatoria, es una buena práctica, de forma que tengamos claro qué necesitamos conseguir en materia de ciberseguridad, cuáles son los principales roles y responsabilidades y cómo se medirán los logros al respecto.

5 / Definir la Metodología de Gestión de Riesgos: NIS2 impone requisitos específicos sobre cómo debe hacerse esta gestión de riesgos, es decir, deberemos disponer de un documento donde se establezca la Metodología de Gestión de Riesgos.

6 / Realizar la evaluación y el tratamiento de los riesgos: Debemos identificar qué podría poner en riesgos nuestros sistemas de información; mediante un listado de activos y amenazas y vulnerabilidades relacionadas, evaluando el alcance de los mismos en relación a su probabilidad de ocurrencia y al impacto que generarían en la organización si llegaran a materializarse.

Los riesgos mayores necesitan ser tratados, implementando las medidas de ciberseguridad establecidas en el artículo 21.

7 / Redactar y aprobar un Plan de Tratamiento de Riesgos: Cuando los riesgos hayan sido identificados y la evaluación realizada, se deberá crear un Plan concreto para la eliminación o mitigación de estos riesgos y aún más importante, deberá conseguir la aprobación por parte de los directivos de dicho plan. El PTR es un plan de implementación y suele incluir todos los controles de ciberseguridad aplicados (actividades, proceso y tecnologías) junto con la información del propietario del activo, información sobre el rol/roles que se encargaría de la implementación del control y los plazos establecidos para la implementación de dicho PTR.

8 / Implementar medidas de ciberseguridad: NIS2 obliga a implementar varias medidas de seguridad, basándose en el análisis de riesgos realizado:

QUÉ DEBEMOS DOCUMENTAR	ARTÍCULO DE LA NIS 2	CÓMO DOCUMENTARLO
Los órganos de gestión deben aprobar las medidas de gestión de riesgos de ciberseguridad	Artículo 20, párrafo 1	Plan de Tratamiento de Riesgos
Los órganos de gestión deben supervisar la implementación de medidas de gestión de riesgos de ciberseguridad	Artículo 20, párrafo 1	Informe de Medición + Informe de Auditoría Interna + Acta de Revisión de la Gestión
Los miembros de los órganos de gestión están obligados a seguir la formación y deben ofrecer una formación similar a sus empleados periódicamente	Artículo 20, párrafo 2	Plan de Formación y Concienciación
Las entidades deben tomar las medidas técnicas, operativas y de organización adecuadas y proporcionadas para gestionar los riesgos	Artículo 21, párrafo 1	Tabla de Tratamiento de Riesgos + Plan de Tratamiento de Riesgos + varias políticas y procedimientos mencionados a continuación
Al evaluar la proporcionalidad de las medidas, se tendrá debidamente en cuenta el grado de exposición de la entidad a los riesgos, el tamaño de la entidad y la probabilidad de que se produzcan incidentes y su gravedad, incluyendo su repercusión social y económica	Artículo 21, párrafo 1	Metodología de Evaluación de Riesgos + Tabla de Evaluación de Riesgos
Política de análisis de riesgos	Artículo 21, párrafo 2, punto a	Metodología de Evaluación de Riesgos
Política de seguridad de los sistemas de información	Artículo 21, párrafo 2, punto a	Política de Seguridad de los Sistemas de Información
Gestión de incidentes	Artículo 21, párrafo 2, punto b	Procedimiento de Gestión de Incidentes + Registro de Incidentes
Énfasis en la resiliencia	Artículo 21, párrafo 2, punto c	Plan de Continuidad de las Actividades
Gestión de copias de seguridad	Artículo 21, párrafo 2, punto c	Política de Copias de Seguridad
Recuperación en caso de catástrofe	Artículo 21, párrafo 2, punto c	Plan de Recuperación en caso de Catástrofe
Gestión de crisis	Artículo 21, párrafo 2, punto c	Plan de Gestión de Crisis
La seguridad de la cadena de suministro, incluidos los aspectos de seguridad relativos a las relaciones entre cada entidad y sus proveedores o prestadores de servicios directos	Artículo 21, párrafo 2, punto d	Política de Seguridad de los Proveedores + Cláusulas de Seguridad para Proveedores y Socios + Declaración de Privacidad
La seguridad en la adquisición, el desarrollo y el mantenimiento de sistemas de redes y de información	Artículo 21, párrafo 2, punto e	Política de Desarrollo Seguro + Especificaciones sobre Requisitos del Sistema de Información

QUÉ DEBEMOS DOCUMENTAR	ARTÍCULO DE LA NIS 2	CÓMO DOCUMENTARLO
Las políticas y los procedimientos para evaluar la eficacia de las medidas para la gestión de riesgos de ciberseguridad	Artículo 21, párrafo 2, punto f	Metodología de Medición + Informe de Medición + Procedimiento de Auditoría Interna + Lista de Verificación de la Auditoría Interna + Informe de Auditoría Interna + Procedimiento de Revisión de la Gestión
Las prácticas básicas de ciber higiene	Artículo 21, párrafo 2, punto g	Política de Seguridad de TIC
La formación en ciberseguridad	Artículo 21, párrafo 2, punto g	Plan de Formación y Concienciación
Las políticas y procedimientos relativos a la utilización de criptografía y cifrado	Artículo 21, párrafo 2, punto h	Política sobre el Uso del Cifrado
La seguridad de los Recursos Humanos	Artículo 21, párrafo 2, punto i	Política de Seguridad para Recursos Humanos
Las políticas de control de acceso	Artículo 21, párrafo 2, punto i	Política de Control de Acceso
La gestión de activos	Artículo 21, párrafo 2, punto i	Procedimiento de Gestión de Activos + Inventario de Activos
El uso de soluciones de autenticación multifactorial o de autenticación continua	Artículo 21, párrafo 2, punto j	Política de autenticación
La seguridad de las comunicaciones de voz, vídeo y texto	Artículo 21, párrafo 2, punto j	Política de Transferencia de Información + Política de Comunicación Segura
La seguridad de los sistemas de comunicaciones de emergencia	Artículo 21, párrafo 2, punto j	Política de Comunicación Segura
La consideración de las vulnerabilidades específicas de cada proveedor y prestador de servicios directo y la calidad general de los productos y las prácticas en materia de ciberseguridad de los proveedores y prestadores de servicios, incluidos sus procedimientos de desarrollo seguro	Artículo 21, párrafo 3	Política de Seguridad de los Proveedores + Informe de la Evaluación y Tratamiento de Riesgos
La adopción de medidas correctivas adecuadas y proporcionadas	Artículo 21, párrafo 4	Procedimiento de Acciones Correctivas + Formulario de Acciones Correctivas
La notificación al CSIRT o a la autoridad competente cualquier incidente significativo	Artículo 23, párrafo 1	Notificación de incidentes significativos al CSIRT/Autoridad competente
La notificación a los destinatarios de sus servicios los incidentes significativos susceptibles de afectar negativamente a la prestación de dichos servicios	Artículo 23, párrafo 1	Notificación de incidentes significativos a los destinatarios de servicios

QUÉ DEBEMOS DOCUMENTAR	ARTÍCULO DE LA NIS 2	CÓMO DOCUMENTARLO
La comunicación a los destinatarios de servicios que potencialmente se vean afectados por una ciber amenaza significativa cualquier medida o solución que dichos destinatarios puedan adoptar para hacer frente a esa amenaza. También hay que informar a esos destinatarios de la propia ciber amenaza significativa	Artículo 23, párrafo 2	Notificación de incidentes significativos a los destinatarios de servicios
Una alerta temprana: indica si cabe sospechar que el incidente significativo responde a una acción ilícita o malintencionada o puede tener repercusiones transfronterizas	Artículo 23, párrafo 4, punto a	Alerta Temprana de Incidente Significativo
Una notificación del incidente que contenga una evaluación inicial del incidente significativo, incluyendo su gravedad e impacto, así como indicadores de compromiso, cuando estén disponibles	Artículo 23, párrafo 4, punto b	Notificación de incidentes significativos al CSIRT/ Autoridad competente
Un informe intermedio con actualizaciones pertinentes sobre la situación	Artículo 23, párrafo 4, punto c	Informe Intermedio de Incidente Significativo
Un informe final, a más tardar, un mes después de presentar la notificación del incidente	Artículo 23, párrafo 4, punto d	Informe Final de Incidente Significativo
Un informe de situación en el caso de que el incidente siga en curso en el momento de la presentación del informe final	Artículo 23, párrafo 4, punto e	(No especificado)

9 / Configurar la seguridad de la cadena de suministros: Se ha de realizar una evaluación de riesgos formal de los proveedores, lo que incluye la evaluación de sus vulnerabilidades así como estudiar sus procedimientos de desarrollo de software e incluyendo en los acuerdos firmados con ellos, cláusulas de seguridad y supervisando periódicamente su actitud ante la seguridad.

10 / Configurar la evaluación de la efectividad de la ciberseguridad:
La Dirección debe supervisar la implementación de las medidas de ciberseguridad de la siguiente forma:

a) Medir y supervisar continuamente la ciberseguridad para detectar posibles desviaciones

b) Realizar auditorías periódicas para detectar posibles no conformidades

c) Revisiones periódicas de la gestión con sesiones formales dedicadas a revisar todos los aspectos relacionados con la ciberseguridad

Para todo ello, debemos contar con documentos claves como una Metodología de Medición, un Procedimiento de Auditoría Interna y un Procedimiento de Revisión de la Gestión.

11 / Configurar la notificación de incidentes:
Notificar al CSIRT (o autoridad competente) y a los destinatarios de los servicios, los incidentes significativos.

Las entidades están obligadas a presentar varios tipos de informes al CSIRT:
* Una alerta temprana
* Una notificación de incidente
* Un informe intermedio
* Un informe final
* Un informe intermedio

12 / Establecer una formación continua en ciberseguridad

Capítulo IV, Medidas para la Gestión de Riesgos y obligaciones de notificación. TODOS LOS EMPLEADOS, INCLUIDA LA DIRECCIÓN, DEBEN REALIZAR FORMACIÓN EN CIBERSEGURIDAD.

Las referencias normativas de NIS2 con respecto a formación son las siguientes:

Artículo 20 - Gobernanza.

Artículo 21- Medidas para la gestión de riesgos de ciberseguridad.

Artículo 22- Evaluaciones coordinadas de los riesgos de seguridad de las cadenas de suministro críticas a escala en la Unión.

Artículo 23- obligaciones de notificación.

Artículo 24 - Utilización de esquemas europeos de certificación de la ciberseguridad.

Artículo 25 - Normalización.

Debemos definir claramente y en primer lugar:
* Qué temas a tratar en la formación
* Cómo configurar el proceso de formación
* Qué métodos utilizar para impartir la formación periódicamente

El temario de la formación debería incluir, para todos los empleados (incluyendo directivos y empleados de nivel medio):
* Fundamentos básicos de la Directiva NIS2
* Prácticas de ciber higiene (artículo 21, párrafo 2, punto g)
* Gestión de incidentes (artículo 21, párrafo 2 , punto b)
* Copias de seguridad (artículo 21, párrafo 2, punto c)
* Continuidad de las actividades (artículo 21, párrafo 2, punto c)
* Uso de soluciones de autenticación multifactorial o de autenticación continua (artículo 21, párrafo 2, punto j)

13) Auditorías internas periódicas

Aunque no se mencionan en NIS2, ISO 27001 y otras normas internacionales sugieren que la auditoría interna es la mejor práctica para que los órganos de dirección logren supervisar la implementación de las medidas de seguridad.

Si no se identifican las no conformidades mediante auditoría interna, la dirección nunca podrá tener una imagen completa del estado de la ciberseguridad, lo que podría llevar a incidentes y conllevar responsabilidades.

14) Revisiones periódicas en la gestión

Reunión formal en la que los órganos de dirección necesitan recibir toda la información relevante sobre ciberseguridad (informes de medición, informes de auditoría interna, etc.) para tomar decisiones importantes en materia de ciberseguridad.

Tras esta revisión y en función de sus resultados, se pueden proponer acciones correctivas, redefinir los roles importantes y las responsabilidades, establecer nuevos objetivos de seguridad, definir el presupuesto de ciberseguridad, etc.

>_

Notificación de incidentes

Definiciones

* Incidente: Todo hecho que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos, transmitidos o tratados, o los servicios ofrecidos por sistemas de redes y de información o accesibles a través de ellos.

NIS2 exige SÓLO la notificación de los INCIDENTES SIGNIFICATIVOS, es decir, "cualquier incidente que tenga un impacto significativo en la prestación" de los servicios que prestan las entidades esenciales o importantes, si:

a) Ha causado o puede causar graves perturbaciones operativas en los servicios o pérdidas económicas para la entidad afectada; (que podrían medirse mediante indicadores que nos mostrará en qué se ve afectado el servicio, la duración del incidente o el número de destinatarios de los servicios afectados" sin entrar a valorar qué se considera como "pérdida económica grave o un perjuicio material o inmaterial considerable".

b) Ha afectado o puede afectar a otras personas físicas o jurídicas al causar perjuicios materiales o inmateriales considerables.

¿A quién notificar los incidentes?

* Al equipo de respuesta a incidentes de seguridad informática (CSIRT) o a una autoridad competente (autoridades designadas directamente por los Estados miembros para ser responsables de la ciberseguridad y de las tareas de supervisión).

* Los destinatarios de servicios esenciales o importantes que puedan verse afectados por el incidente significativo.

¿Cómo se notifican los incidentes significativos?

El artículo 23 obliga a las empresas a notificar los incidentes significativos de la siguiente forma:

Requisitos de la NIS2	Artículo correspondiente de la NIS2	Cuándo notificar	Qué notificar	Nombre sugerido para el documento
Una notificación (para los destinatarios de servicios que están potencialmente afectados por una ciber amenaza significativa)	Artículo 23, párrafo 2	Sin demora indebida	Cualquier medida o solución que esos destinatarios puedan aplicar en respuesta a la amenaza; también se notificará la propia ciber amenaza significativa a esos destinatarios	Notificación de incidentes significativos a los destinatarios de servicios
Una alerta temprana (para CSIRT o autoridad competente)	Artículo 23, párrafo 4, punto a	Sin demora indebida y, en cualquier caso, dentro de las 24 horas desde que se haya tenido constancia del incidente significativo	Indica si cabe sospechar que el incidente significativo responde a una acción ilícita o malintencionada o puede tener repercusiones transfronterizas	Alerta Temprana de Incidente Significativo
Una notificación del incidente (para CSIRT o autoridad competente)	Artículo 23, párrafo 4, punto b	Sin demora indebida y, en cualquier caso, dentro de las 72 horas desde que se haya tenido constancia del incidente significativo	Contiene una evaluación inicial del incidente significativo, incluyendo su gravedad e impacto, así como indicadores de compromiso, cuando estén disponibles	Notificación de Incidentes Significativos al CSIRT/ Autoridad competente
Un informe intermedio (para CSIRT o autoridad competente)	Artículo 23, párrafo 4, punto c	A petición de un CSIRT o de la autoridad competente	Actualizaciones pertinentes sobre la situación	Informe Intermedio de Incidente Significativo
Un informe final (para CSIRT o autoridad competente)	Artículo 23, párrafo 4, punto d	A más tardar, un mes después de presentar la notificación del incidente	(I) una descripción detallada del incidente, incluyendo su gravedad e impacto; (II) el tipo de amenaza o causa principal que probablemente haya desencadenado el incidente; (III) las medidas paliativas aplicadas y en curso; (IV) cuando proceda, las repercusiones transfronterizas del incidente.	Informe Final de Incidente Significativo
Un informe de situación (para CSIRT o autoridad competente)	Artículo 23, párrafo 4, punto e	En el caso de que el incidente siga en curso	(no especificado)	Informe de Situación de Incidente Significativo

Anexo I

SECTORES DE ALTA CRITICIDAD

Sector	Subsector	Tipo de entidad
1. Energía	a) Electricidad	— Las empresas eléctricas, tal como se definen en el artículo 2, punto 57, de la Directiva (UE) 2019/944 del Parlamento Europeo y del Consejo (1), que desempeñan la función de «suministro» tal como se define en el artículo 2, punto 12, de dicha Directiva — Gestores de redes de distribución, tal como se definen en el artículo 2, punto 29, de la Directiva (UE) 2019/944 — Gestores de redes de transporte, tal como se definen en el artículo 2, punto 35, de la Directiva (UE) 2019/944 — Productores, tal como se definen en el artículo 2, punto 38, de la Directiva (UE) 2019/944 — Gestores del mercado de la electricidad designados, tal como se definen en el artículo 2, punto 8, del Reglamento (UE) 2019/943 del Parlamento Europeo y del Consejo (2) — Participantes en el mercado, tal como se definen en el artículo 2, punto 25, del Reglamento (UE) 2019/943, que presten servicios de agregación, respuesta de la demanda o almacenamiento de energía, tal como se definen en el artículo 2, puntos 18, 20 y 59, de la Directiva (UE) 2019/944 — Operadores de un punto de recarga que sean responsables de la gestión y explotación de un punto de recarga, que preste un servicio de recarga a los usuarios finales, incluso en nombre y por cuenta de un proveedor de servicios de movilidad
	b) Calefacción y refrigeración urbanas	— Operadores de calefacción urbana o refrigeración urbana, tal como se definen en el artículo 2, punto 19, de la Directiva (UE) 2018/2001 del Parlamento Europeo y del Consejo (3)
	c) Aceite	— Operadores de oleoductos de transporte de petróleo — Operadores de instalaciones de producción, refinado y tratamiento de petróleo, almacenamiento y transporte — Entidades centrales de almacenamiento, tal como se definen en el artículo 2, letra f), de la Directiva 2009/119/CE del Consejo (4)
	d) Gas	— Empresas suministradoras, tal como se definen en el artículo 2, punto 8, de la Directiva 2009/73/CE del Parlamento Europeo y del Consejo (5) — Gestores de redes de distribución, tal como se definen en el artículo 2, punto 6, de la Directiva 2009/73/CE — Gestores de redes de transporte, tal como se definen en el artículo 2, punto 4, de la Directiva 2009/73/CE — Gestores de redes de almacenamiento, tal como se definen en el artículo 2, punto 10, de la Directiva 2009/73/CE — Gestores de redes de GNL, tal como se definen en el artículo 2, punto 12, de la Directiva 2009/73/CE — Empresas de gas natural, tal como se definen en el artículo 2, punto 1, de la Directiva 2009/73/CE — Operadores de instalaciones de refino y tratamiento de gas natural
	e) Hidrógeno	— Operadores de producción, almacenamiento y transporte de hidrógeno
2. Transporte	a) Aire	— Compañías aéreas, tal como se definen en el artículo 3, punto 4, del Reglamento (CE) n.o 300/2008, utilizadas con fines comerciales — Las entidades gestoras de aeropuertos, tal como se definen en el artículo 2, punto 2, de la Directiva 2009/12/CE del Parlamento Europeo y del Consejo (6), los aeropuertos, tal como se definen en el artículo 2, punto 1, de dicha Directiva, incluidos los aeropuertos principales enumerados en la sección 2 del anexo II del Reglamento (UE) n.o 1315/2013 del Parlamento Europeo y del Consejo (7), y entidades que explotan instalaciones auxiliares en los aeropuertos — Operadores de control de gestión de tránsito que presten servicios de control de tránsito aéreo (ATC), tal como se definen en el artículo 2, punto 1, del Reglamento (CE) n.o 549/2004 del Parlamento Europeo y del Consejo (8)

Sector	Subsector	Tipo de entidad
2. Transporte	b) Ferrocarril	— Administradores de infraestructuras, tal como se definen en el artículo 3, punto 2, de la Directiva 2012/34/UE del Parlamento Europeo y del Consejo (9) — Las empresas ferroviarias, tal como se definen en el artículo 3, punto 1, de la Directiva 2012/34/UE, incluidos los explotadores de instalaciones de servicio, tal como se definen en el artículo 3, punto 12, de dicha Directiva
	c) Agua	— Las empresas de transporte fluvial, marítimo y costero de pasajeros y mercancías, tal como se definen para el transporte marítimo en el anexo I del Reglamento (CE) n.o 725/2004 del Parlamento Europeo y del Consejo (10), sin incluir los buques individuales explotados por dichas empresas — Los organismos gestores de los puertos, tal como se definen en el artículo 3, punto 1, de la Directiva 2005/65/CE del Parlamento Europeo y del Consejo (11), incluidas sus instalaciones portuarias, tal como se definen en el artículo 2, punto 11, del Reglamento (CE) n.o 725/2004, y las entidades que explotan obras y equipos contenidos en los puertos — Operadores de servicios de tráfico marítimo (VTS), tal como se definen en el artículo 3, letra o), de la Directiva 2002/59/CE del Parlamento Europeo y del Consejo (12)
	d) Carretera	— Autoridades viarias, tal como se definen en el artículo 2, punto 12, del Reglamento Delegado (UE) 2015/962 de la Comisión (13), responsables del control de la gestión del tráfico, excluidas las entidades públicas para las que la gestión del tráfico o el funcionamiento de sistemas de transporte inteligentes no constituyan una parte esencial de su actividad general — Operadores de sistemas de transporte inteligentes, tal como se definen en el artículo 4, punto 1, de la Directiva 2010/40/UE del Parlamento Europeo y del Consejo (14)
3. Entidades bancarias		Las entidades de crédito, tal como se definen en el artículo 4, punto 1, del Reglamento (UE) n.o 575/2013 del Parlamento Europeo y del Consejo (15)
4. Infraestructuras de los mercados financieros		— Gestores de centros de negociación, tal como se definen en el artículo 4, punto 24, de la Directiva 2014/65/UE del Parlamento Europeo y del Consejo (16) — Las entidades de contrapartida central (ECC), tal como se definen en el artículo 2, punto 1, del Reglamento (UE) n.o 648/2012 del Parlamento Europeo y del Consejo (17)
5. Sanidad		— Prestadores de asistencia sanitaria, tal como se definen en el artículo 3, letra g), de la Directiva 2011/24/UE del Parlamento Europeo y del Consejo (18) — Laboratorios de referencia de la UE a que se refiere el artículo 15 del Reglamento (UE) 2022/2371 del Parlamento Europeo y del Consejo (19) — Entidades que lleven a cabo actividades de investigación y desarrollo de medicamentos, tal como se definen en el artículo 1, punto 2, de la Directiva 2001/83/CE del Parlamento Europeo y del Consejo (20) — Entidades que fabriquen productos farmacéuticos básicos y preparados farmacéuticos a que se refiere la sección C, división 21, de la NACE Rev. 2 — Entidades que fabriquen productos sanitarios considerados esenciales durante una emergencia de salud pública (lista de productos sanitarios esenciales para emergencias de salud pública) en el sentido del artículo 22 del Reglamento (UE) 2022/123 del Parlamento Europeo y del Consejo (21)
6. Suministradores y distribuidores de gua potable		Los suministradores y distribuidores de agua destinada al consumo humano, tal como se define en el artículo 2, punto 1, letra a), de la Directiva (UE) 2020/2184 del Parlamento Europeo y del Consejo (22), excluidos los distribuidores para los que la distribución de agua destinada al consumo humano no sea una parte esencial de su actividad general de distribución de otros productos básicos y bienes
7. Compañías dedicadas a la recogida, eliminacióno el tratamiento de aguas residuales urbanas		Las empresas que recojan, eliminen o traten las aguas residuales urbanas, las aguas residuales domésticas o las aguas residuales industriales, tal como se definen en el artículo 2, puntos 1, 2 y 3, de la Directiva 91/271/CEE del Consejo (23), con exclusión de las empresas para las que la recogida, la eliminación o el tratamiento de las aguas residuales urbanas, domésticas o industriales constituyan una parte no esencial de su actividad general

Sector	Subsector	Tipo de entidad
8. Infraestructura digital		— Proveedores de puntos de intercambio de Internet — Proveedores de servicios DNS, excluidos los operadores de servidores de nombres raíz — Registros de nombres de TLD — Proveedores de servicios de computación en la nube — Proveedores de servicios de centros de datos — Proveedores de redes de distribución de contenidos — Prestadores de servicios de confianza — Proveedores de redes públicas de comunicaciones electrónicas — Proveedores de servicios de comunicaciones electrónicas disponibles al público
9. Gestión de servicios TIC (business-to-business)		— Proveedores de servicios gestionados — Proveedores de servicios de seguridad gestionados
10. Administración pública		— Entidades de la administración pública de las administraciones centrales definidas por un Estado miembro de conformidad con el Derecho nacional — Entidades de la administración pública a nivel regional, tal como las define un Estado miembro de conformidad con el Derecho nacional
11. Espacio		Operadores de infraestructuras terrestres, que sean propiedad de los Estados miembros o de entidades privadas, estén gestionados y explotados por ellos, que apoyen la prestación de servicios espaciales, excluidos los proveedores de redes públicas de comunicaciones electrónicas

Anexo II

OTROS SECTORES CRÍTICOS

Sector	Subsector	Tipo de entidad
1. Servicios postales y de mensajería		Los proveedores de servicios postales, tal como se definen en el artículo 2, punto 1 bis, de la Directiva 97/67/CE, incluidos los proveedores de servicios de mensajería.
2. Gestión de residuos		Empresas que lleven a cabo la gestión de residuos, tal como se define en el artículo 3, punto 9, de la Directiva 2008/98/CE del Parlamento Europeo y del Consejo (1), excluidas las empresas para las que la gestión de residuos no sea su actividad económica principal
3. Sustancias químicas		Las empresas que lleven a cabo la fabricación de sustancias y la distribución de sustancias o mezclas, tal como se contempla en el artículo 3, puntos 9 y 14, del Reglamento (CE) n.o 1907/2006 del Parlamento Europeo y del Consejo (2), y las empresas que lleven a cabo la producción de artículos, tal como se definen en el artículo 3, punto 3, de dicho Reglamento, a partir de sustancias o mezclas
4. Alimentos		Las empresas alimentarias, tal como se definen en el artículo 3, punto 2, del Reglamento (CE) n.o 178/2002 del Parlamento Europeo y del Consejo (3), que se dediquen a la distribución al por mayor y a la producción y transformación industrial
5. Industria (tecnología e ingenieria)	Fabricación de productos sanitarios y productos sanitarios para diagnóstico in vitro	Entidades que fabriquen productos sanitarios, tal como se definen en el artículo 2, punto 1, del Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo (4), y entidades que fabriquen productos sanitarios para diagnóstico in vitro, tal como se definen en el artículo 2, punto 2, del Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo (5) con excepción de las entidades fabricantes de productos sanitarios a que se refiere el quinto guión del punto 5 del anexo I de la presente Directiva
	b) Fabricación de productos informáticos, electrónicos y ópticos	Empresas que ejerzan cualquiera de las actividades económicas contempladas en la sección C, división 26, de la NACE Rev. 2
	c) Fabricación de material eléctrico	Empresas que ejerzan cualquiera de las actividades económicas contempladas en la sección C, división 27, de la NACE Rev. 2
	d) Fabricación de maquinaria y equipo n.c.o.p.	Empresas que ejerzan cualquiera de las actividades económicas contempladas en la sección C, división 28, de la NACE Rev. 2
	e) Fabricación de vehículos automóviles, remolques y semirremolques	Empresas que ejerzan cualquiera de las actividades económicas contempladas en la sección C, división 29, de la NACE Rev. 2
	f) Fabricación de otro equipo de transporte	Empresas que ejerzan cualquiera de las actividades económicas contempladas en la sección C, división 30, de la NACE Rev. 2
6. Servicios digitales		— Proveedores de mercados en línea — Proveedores de motores de búsqueda en línea — Proveedores de plataformas de servicios de redes sociales
7. Investigación		Organismos de investigación