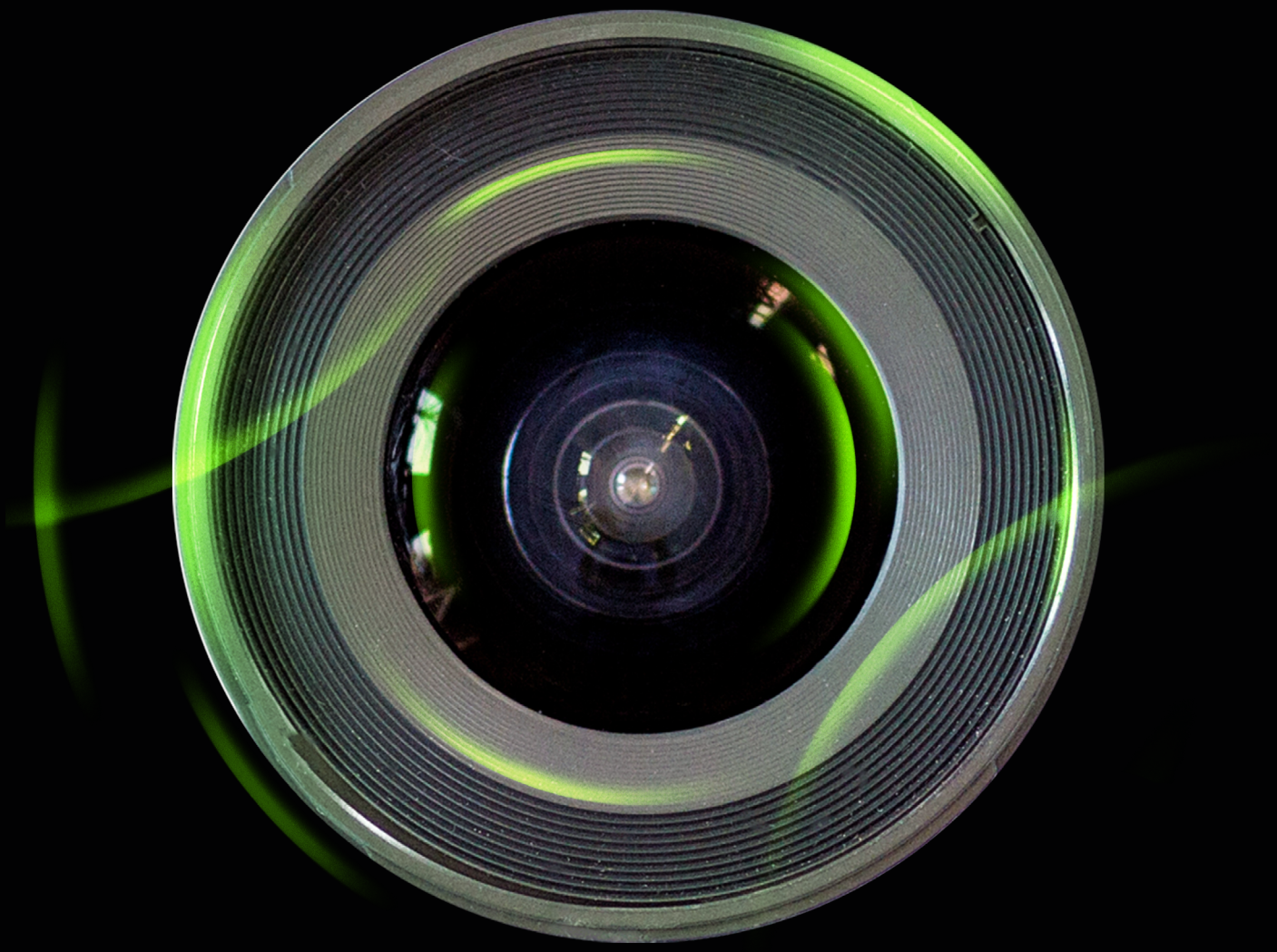
Deloitte.



Directiva CER

Directiva (UE) 2022/2557
relativa a la resiliencia de las entidades críticas

Contenidos

Introducción

En respuesta a las amenazas y atentados sufridos por parte de la Unión Europea y otros países, en 2004 se publicó el Programa Europeo de Protección de Infraestructuras Críticas (PEPIC), que tenía como objetivo elaborar una estrategia para la protección de los servicios esenciales, así como de las infraestructuras críticas. Cuatro años después, el 23 de diciembre de 2008, se publicó la Directiva (UE) 2008/114/CE del Consejo sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección. Ambas publicaciones establecían que la responsabilidad de proteger las infraestructuras críticas correspondía a los Estados miembro y a los operadores de las mismas, determinando la necesidad de desarrollar una serie de obligaciones y actuaciones que debían incorporarse a las legislaciones nacionales.

Por esta razón, se elaboró la transposición de la Directiva (UE) 2008/114/CE en la Ley 8/2011 por la que se establecen medidas para la protección de las infraestructuras críticas (comúnmente conocida como Ley de Protección de Infraestructuras Críticas o LPIC).

El pasado 27 de diciembre de 2022 se publicó la nueva "Directiva (UE) 2022/2557 del parlamento europeo y del consejo relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo" (en adelante, Directiva CER) en el Diario Oficial de la Unión Europea (DOUE), cuyo objetivo es aumentar la resiliencia de las entidades críticas y su capacidad para prestar sus servicios esenciales.

El presente artículo tiene como objetivo resumir la Directiva CER, identificando sus principales impactos, especialmente para las entidades críticas. De esta manera, se pretende contestar a las siguientes preguntas:

- ¿Qué relación existe entre las Directiva NIS 2 y CER?
- ¿A quién aplica la Directiva CER?
- ¿Cuáles son los principales organismos vinculados a la Directiva CER?
- ¿En qué consistirán las estrategias de ciberresiliencia?
- ¿Qué impacto tendrá la Directiva CER sobre las entidades afectadas?
- ¿Qué requerimientos de notificación de incidentes tendrán que cumplir las entidades afectadas?
    - ¿Qué es un efecto perturbador de carácter significativo?
    - ¿Qué información mínima deberán incluir las notificaciones?
    - ¿Cuál es flujo de notificación que tendrán que tomar como referencia los Estados Miembro y las entidades?
- ¿Cuáles serán las funciones y competencias de las autoridades competentes de cada Estado miembro?
- ¿Cómo será el régimen sancionador en los Estados miembro?
- ¿Cuáles son los próximos pasos?

¿Qué relación existe entre las Directivas **NIS 2 y CER**?

Teniendo en cuenta la importancia de la ciberseguridad para la resiliencia de las entidades críticas, siempre que sea posible, debe seguirse un enfoque coherente entre la Directiva CER y la Directiva NIS 2 (Directiva (UE) 2022/2555 del parlamento europeo y del consejo relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión). Esta última impone unos requisitos exhaustivos a un amplio conjunto de entidades para garantizar su ciberseguridad. En este sentido, dado que la ciberseguridad se trata de manera suficiente en la Directiva NIS 2, las materias reguladas por dicha Directiva deben quedar excluidas del ámbito de aplicación de la Directiva CER.

En este sentido, existen las siguientes relaciones o implicaciones entre ambas directivas:

- Estrategia para la resiliencia de las entidades críticas: estas estrategias que deben desarrollar los Estados miembro deberán contemplar la coordinación entre las autoridades competentes que se designen en las Directivas CER y NIS 2, teniendo como objetivo el intercambio de información sobre riesgos, amenazas e incidentes.
- Identificación de las entidades críticas: las autoridades competentes de la Directiva CER deberán notificar a las autoridades competentes de la Directiva NIS 2 la identidad de las entidades críticas en el plazo de 1 mes desde su identificación.
- Supervisión y ejecución: cuando se ejerzan las labores de supervisión con arreglo a la Directiva CER, las autoridades competentes deberán informar a las autoridades competentes de la Directiva NIS 2 para que estas ejerzan las labores de supervisión correspondientes y acordes a los requisitos exigidos por la misma.

¿**A quién aplica** la Directiva CER?

La Directiva CER obliga a los Estados miembro a adoptar medidas específicas destinadas a garantizar la prestación, sin obstrucciones en el mercado interior, de servicios esenciales para el mantenimiento de las funciones sociales o actividades económicas vitales, en particular, las obligaciones de identificar las entidades críticas y apoyarlas en el cumplimiento de las obligaciones impuestas a las mismas.

En este sentido, las entidades críticas serán identificadas por los Estados miembro quienes, además, realizarán la notificación correspondiente a las mismas basándose en unos criterios preestablecidos. Se entenderá como entidad crítica cualquier entidad pública o privada identificada por un Estado miembro siempre que cumpla con los criterios preestablecidos y pertenezca a alguno de los siguientes sectores[1]:

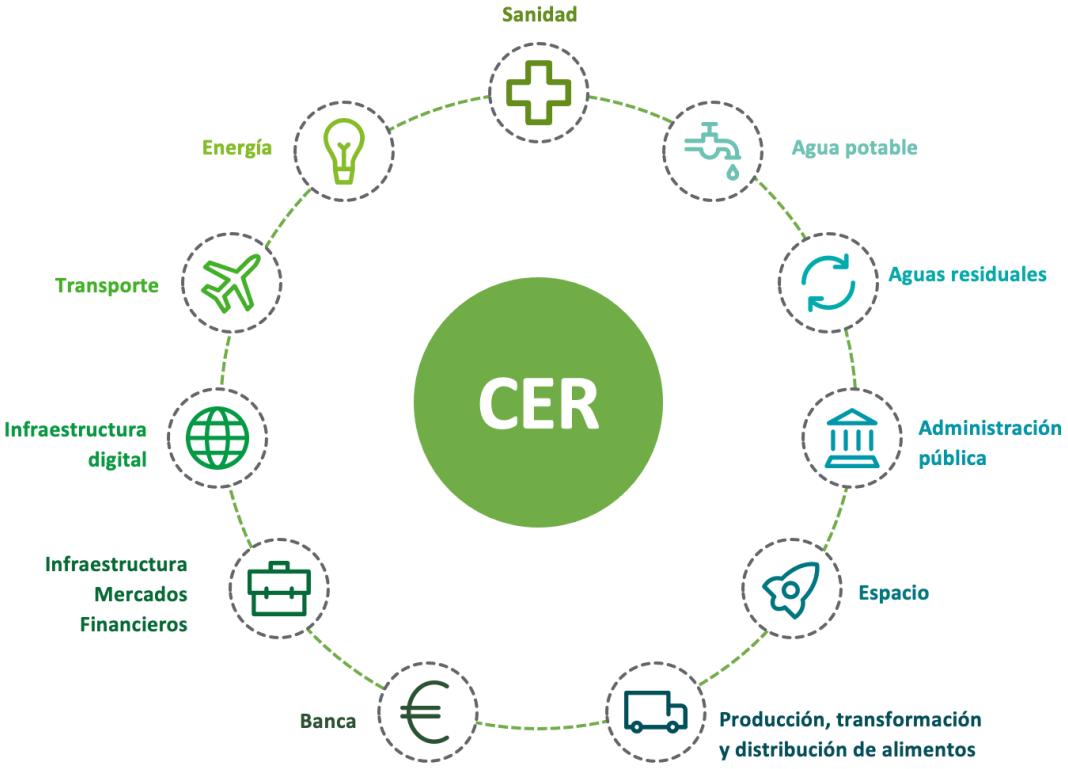


Ilustración 1 - Sectores bajo la aplicabilidad de la Directiva CER

1 *Para conocer el detalle sobre el tipo de entidades que están bajo cada uno de estos sectores es necesario consultar el anexo de la Directiva CER.*

Los criterios preestablecidos mencionados anteriormente son los siguientes:

- Si la entidad presta uno o más servicios esenciales[2];
- Si la entidad opera en el territorio de dicho Estado miembro y su infraestructura crítica[3] está situada en él, y
- Si un incidente tuviese efectos perturbadores significativos en la prestación, por parte de la entidad, de uno o más servicios esenciales, o en la prestación de otros servicios esenciales que dependen de dicho servicio.

Adicionalmente, dentro de estas **entidades críticas se incluye la tipología de entidades críticas de especial importancia europea**, que serán aquellas que presten los mismos servicios esenciales o similares a/o en seis o más Estados miembro y, además, haya sido designada como tal por las autoridades competentes.

Por otro lado, es importante tener en cuenta que los Estados miembro deben asegurarse de que el artículo 11 *"Cooperación entre los Estados Miembros"* y los capítulos III *"Resiliencia de entidades críticas"*, IV *"Grupo de resiliencia de entidades críticas"* y VI *"Supervisión y ejecución"* no se apliquen a las entidades críticas que hayan identificado en los sectores de banca, infraestructura de mercados financieros e infraestructura digital, dado que están recogidas en el Reglamento (UE) 2022/2554 sobre la resiliencia operativa digital del sector financiero (conocido como DORA). En este sentido, los Estados miembro podrán adoptar o mantener disposiciones de Derecho nacional a fin de alcanzar un mayor nivel de resiliencia de dichas entidades críticas, a condición de que tales disposiciones sean coherentes con el Derecho de la Unión aplicable.

2 *Servicio esencial es aquel que es crucial para el mantenimiento de funciones sociales vitales, las actividades económicas, la salud pública y la seguridad o el medio ambiente.*

3 *Se denomina infraestructura crítica a un elemento, instalación, equipo, red o sistema, parte de un elemento, instalación o equipo, que es necesario para la prestación de un servicio esencial.*

¿Cuáles son los principales **organismos vinculados** a la Directiva CER?

- **Autoridades competentes**, cuyo cometido será la supervisión de las entidades críticas y la correcta aplicación de la Directiva. Las autoridades competentes con arreglo a la Directiva CER y las autoridades competentes con arreglo a la Directiva NIS 2 deben cooperar e intercambiar información en relación con los riesgos, amenazas e incidentes relacionados con la ciberseguridad y los riesgos, amenazas e incidentes no relacionados con ella que afecten a las entidades críticas, así como, sobre las medidas adoptadas por las autoridades competentes designadas en ambas directivas.

- **Punto de contacto único**, designado por el Estado miembro y cuyo cometido será asegurar la cooperación transfronteriza entre todas las Autoridades Competentes designadas en dicho Estado.

- **Grupo de Resiliencia de las Entidades Críticas**, que debe adoptar directrices no vinculantes para especificar con más detalle las medidas técnicas, organizativas y de seguridad. Además, facilitará la cooperación entre los Estados miembro y el intercambio de información relacionados con la Directiva CER. El Grupo de Resiliencia de las Entidades Críticas debe cooperar con el Grupo de Cooperación establecido en virtud de la Directiva NIS 2 con vistas a apoyar un marco global para la resiliencia cibernética y no cibernética de las entidades críticas. En este sentido, ambos grupos deben entablar un diálogo periódico a fin de promover la cooperación entre las autoridades competentes de ambas directivas.

¿En qué consistirán las **estrategias de ciberresiliencia**?

Los Estados miembro desarrollarán estrategias de ciberresiliencia, las cuales establecerán los objetivos estratégicos a nivel nacional y las medidas de actuación con el objetivo de alcanzar y mantener un alto nivel de resiliencia.

¿Cuál será el objetivo de las estrategias?

- Marcar los objetivos estratégicos y prioridades en cuanto a la resiliencia de las entidades críticas.
- Establecer un marco de gobernanza.
- Desarrollar las medidas necesarias para aumentar la resiliencia global de las entidades críticas.
- Describir el proceso por el que se identificará a las entidades críticas.
- Describir el proceso de apoyo a las entidades críticas, incluyendo medidas para mejorar la cooperación entre el sector público y privado, así como las entidades públicas y privadas.
- Elaborar las listas de las principales autoridades y partes interesadas, distintas de las entidades críticas.
- Establecer un marco de actuación para la coordinación entre las autoridades competentes designadas por la presente directiva y la Directiva NIS 2, a efectos de intercambio de información sobre los riesgos, amenazas e incidentes.
- Describir las medidas ya adoptadas para facilitar el cumplimiento de las obligaciones relacionadas con la resiliencia de las entidades críticas.

¿Qué **impacto** tendrá la Directiva CER sobre las **entidades afectadas**?

Las entidades críticas que hayan sido designadas como tal por la Directiva CER deberán tener en consideración distintos aspectos, como son la evaluación de riegos y las medidas de resiliencia.

Evaluación de riesgos por parte de entidades críticas

El artículo 12 establece la necesidad por parte de las entidades críticas de realizar análisis de riesgos. Para ello, contarán con un plazo de nueve meses desde que se les notifique como entidad crítica, y posteriormente, deberán actualizarlo siempre que sea necesario y como mínimo, cada cuatro años.

En estas evaluaciones de riesgos, se tendrán en cuenta los riesgos naturales y de origen humano pertinentes que puedan dar lugar a un incidente, entre ellos, los de naturaleza intersectorial o transfronteriza, los accidentes, las catástrofes naturales, las emergencias de salud pública y las amenazas híbridas y otras amenazas antagónicas, incluidos los delitos de terrorismo establecidos en la Directiva (UE) 2017/541 relativa a la lucha contra el terrorismo.

Podrán considerarse como válidas otras evaluaciones de riesgos realizadas en virtud de obligaciones establecidas en otros actos jurídicos, pero serán las autoridades competentes quienes decidan la validez, o no, de las mismas.

Medidas de resiliencia de entidades críticas

El artículo 13 estipula que las entidades críticas deberán adoptar medidas técnicas, organizativas y de seguridad adecuadas para garantizar su resiliencia. Estas medidas formarán parte de un plan de resiliencia o documento equivalente, el cual, deberá describir las medidas para:

- Evitar que se produzcan incidentes, considerando con la debida atención medidas de reducción del riesgo de catástrofes y de adaptación al cambio climático;
- Garantizar una protección física de las instalaciones y de la infraestructura crítica, contando con vallas, barreras, herramientas, etc.
- Responder y resistir a las consecuencias de los incidentes y mitigarlas, considerando la aplicación de procedimientos y protocoles de gestión de riesgos y crisis.
- Recuperarse de incidentes, considerando las medidas de continuidad de las actividades.
- Garantizar una gestión adecuada de la protección de los empleados.
- Concienciar al personal acerca de las medidas existentes en las entidades.

¿Qué requerimientos de **notificación de incidentes** tendrán que cumplir las entidades afectadas?

El artículo 15 dicta que los Estados miembro deberán asegurarse de que las entidades críticas notifiquen todos los incidentes que puedan perturbar de forma significativa la prestación de servicios esenciales.

¿Qué es un efecto perturbador de carácter significativo?

Para determinar el carácter significativo de un efecto perturbador, deberán considerarse los siguientes criterios:

- El número de usuarios que dependen del servicio esencial.
- El grado en que otros sectores y subsectores dependen del servicio esencial.
- Las repercusiones que los incidentes podrían tener, en términos de grado y duración, en las actividades económicas y sociales, el medio ambiente, la seguridad y la protección públicas o la salud de la población.
- La cuota de mercado de la entidad en el mercado del servicio o servicios esenciales de que se trate.
- La zona geográfica que podría verse afectada por un incidente, incluido cualquier repercusión transfronteriza, teniendo en cuenta la vulnerabilidad asociada al grado de aislamiento de ciertos tipos de zonas geográficas.
- La importancia de la entidad para mantener un nivel suficiente de servicio esencial, teniendo en cuenta la disponibilidad de medios alternativos para la prestación de dicho servicio esencial.

¿Qué información deberán incluir las notificaciones?

Las notificaciones deberán incluir toda la información que esté disponible y sea necesaria para que la autoridad competente pueda comprender la naturaleza, la causa y las posibles consecuencias del incidente, incluyendo cualquier tipo de información para determinar las posibles repercusiones transfronterizas del incidente.

¿Cuál es flujo de notificación que tendrán que tomar como referencia los Estados Miembro y las entidades[4]?

Las entidades críticas deberán notificar sin demora indebida a la autoridad competente los incidentes que perturben o puedan perturbar de forma significativa la prestación de servicios esenciales. En este sentido, las entidades críticas deberán presentar, en un plazo de veinticuatro horas a partir del momento en que tengan conocimiento de un incidente, una notificación inicial seguida, en su caso, de un informe detallado, a más tardar en un plazo de un mes. A fin de determinar la magnitud de la perturbación, se deberán tener en cuenta los siguientes parámetros:

- El número y el porcentaje de usuarios afectados por la perturbación.
- La duración de la perturbación.
- La zona geográfica afectada por la perturbación, teniendo en cuenta si la zona está aislada geográficamente.

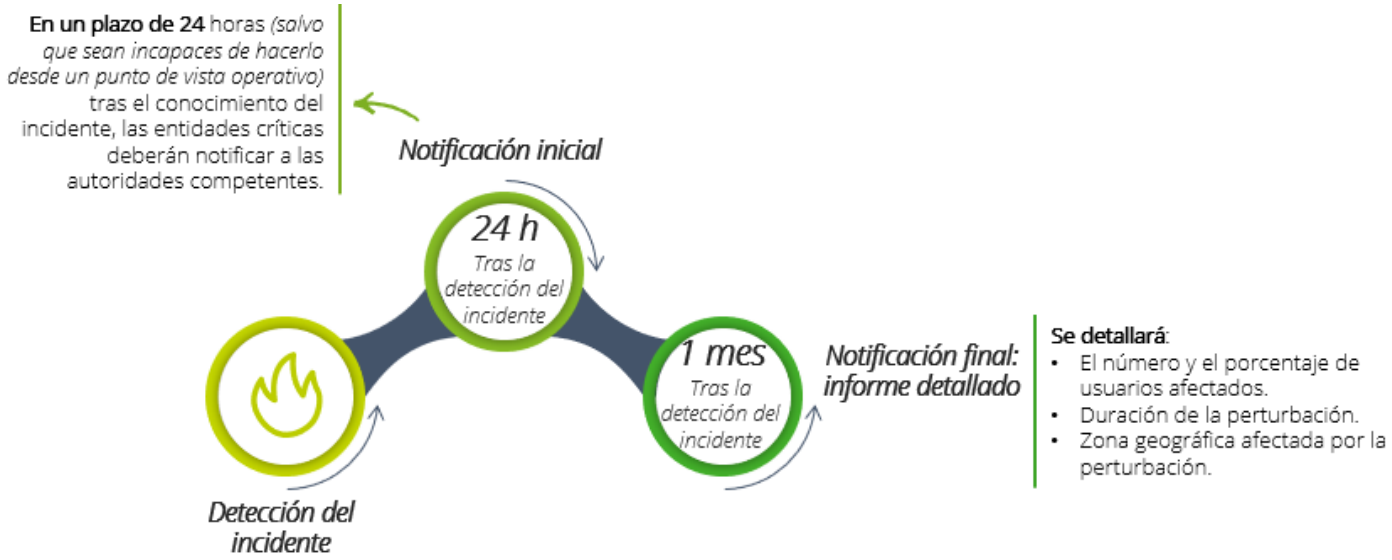


Ilustración 2 - Periodos de notificación de incidentes con impacto significativo

4 *Las entidades deberán esperar hasta la transposición de la Directiva a la legislación española para conocer los detalles más concretos sobre este flujo (umbrales, plantillas, etc.).*

¿Cuáles serán las **funciones y competencias** de las **autoridades competentes** de cada Estado miembro?

En el artículo 21 de la Directiva CER se establecen una serie de facultades mínimas que los Estados miembro deberán conceder a las autoridades competentes referentes a la supervisión de las entidades críticas. A continuación, se muestran dichas facultades:

Facultades de las autoridades competentes

Inspecciones in situ de las infraestructuras críticas y de las instalaciones que utilice la entidad crítica para prestar sus servicios esenciales
Realizar u ordenar auditorías de las entidades críticas
Exigir que las entidades con arreglo a la NIS 2 que hayan sido identificadas como entidades críticas de acuerdo a CER faciliten: • Información necesaria para evaluar si las medidas adoptadas garantizan la resiliencia. • Pruebas de aplicación efectiva de dichas medidas.
Requerir que las entidades críticas adopten las medidas necesarias y proporcionales para subsanar cualquier incumplimiento

Tabla 1 - Facultades de las autoridades competentes

¿Cómo será el **régimen sancionador** en los Estados miembro?

En el artículo 22, se establece que los Estados miembro tendrán de plazo hasta el 17 de octubre de 2024 para establecer el régimen sancionador. Las sanciones que se establezcan deberán ser proporcionales y disuasorias.

A diferencia de la Directiva NIS 2, la Directiva CER no indica unas multas administrativas de referencia a tener en cuenta por los Estados miembro.

¿Cuáles son los **próximos pasos**?

A fecha de 17 de enero de 2023, ha comenzado el periodo de transposición de la Directiva para los Estados miembro de la UE a su legislación nacional. Este plazo finalizará el 17 de octubre de 2024, momento en el cual ya se deberán haber completado las labores de adaptación y publicación de las transposiciones.

De la misma forma, con la misma fecha límite, la Comisión Europea comunicará a los Estados miembro el régimen establecido y las medidas adoptadas en relación con las sanciones.

En este periodo de tiempo, los Estados miembro establecerán el detalle sobre las medidas de resiliencia de las entidades críticas, los criterios de las evaluaciones de riesgos a realizar por éstas y las condiciones y consideraciones sobre notificación de incidentes.

Además, los Estados miembro tendrán el 17 de julio de 2026 como fecha límite para identificar a las entidades críticas.

En este sentido, las entidades deben tener en cuenta tanto esta Directiva como otras que se están publicando para aumentar el nivel de resiliencia frente a las amenazas que pueden suponer un peligro. Entre ellas, se encuentran la Directiva NIS 2, el Reglamento DORA, el Reglamento sobre la Ciberseguridad y sus esquemas de certificación, o el futuro Reglamento para la Ciberresiliencia.

Es por ello, que deben trabajar en la adaptación coordinada a las diferentes normativas, tal y como se ha establecido en las propias regulaciones, en las que hay una coordinación entre las mismas, tanto para los distintos organismos europeos como para las propias entidades.

Finalmente, será necesario tener en cuenta cómo serán las transposiciones de estas Directivas CER y NIS 2, para conocer algunos de los detalles que actualmente quedan pendientes para poder proteger los servicios esenciales y las entidades críticas.

Deloitte.