casmar®

DESICO

Seguridad bajo normativa

Colaboradores:

ACAES
Associació Catalana d'Empreses de Seguretat

Fundación Borredá
al servicio de la seguridad

ÍNDICE

Introducción a la Guía de Seguridad Bajo Normativa

NIS2, CER y LINCE: lo que sabemos hasta ahora y cómo empezar a prepararse.

En un entorno cada vez más regulado, la **seguridad bajo normativa** se ha convertido en un aspecto estratégico para cualquier empresa del sector. Con la llegada de nuevas directivas y normativas como **NIS2** (sobre ciberseguridad), la **CER** (Protección y Resiliencia de Entidades Críticas) o el esquema de certificación **LINCE**, el cumplimiento normativo ya no es una opción: es una exigencia real con impacto directo en operaciones, contratos y oportunidades de negocio.

¿Qué sabemos hasta ahora?

- **NIS2** ya está en vigor, pero su transposición en España se encuentra aún en fase de anteproyecto. Es la nueva versión de la directiva europea de ciberseguridad que amplía su alcance a más sectores (incluyendo el tecnológico) y refuerza los requisitos de seguridad para entidades críticas. Obliga a implementar medidas de gestión de riesgos, notificación de incidentes en 24 horas y posibles sanciones por incumplimiento. Los proveedores de servicios digitales pueden verse afectados si prestan servicios esenciales a clientes regulados.

- La normativa **CER** complementa a la NIS2 al centrarse en la resiliencia física y operativa de entidades críticas (energía, transporte, salud, etc.). Acaba de publicarse la propuesta de su anteproyecto de Ley que confirma la inclusión de sectores como la seguridad privada entre los estratégicos. Obliga a las entidades críticas a evaluar todo tipo de riesgos, implementar Planes de Resiliencia, controlar el acceso de personal sensible y notificar en 24 horas de cualquier incidente. Incluye un régimen sancionador para su incumplimiento.

- El esquema **LINCE** ya es un requisito común en licitaciones públicas y proyectos con alta sensibilidad. Su objetivo: certificar la confianza de productos y servicios de seguridad TIC, para su uso en sistemas de organismos sujetos al ENS, con un reconocimiento oficial del Centro Criptológico Nacional (CCN).

¿A quién afecta realmente?

No solo a grandes compañías o infraestructuras críticas. NIS2, por ejemplo, se aplicará a muchas medianas empresas de sectores como la energía, transporte, sanidad, tecnología, gestión de agua, servicios digitales o servicios en la nube. También a sus proveedores. Es decir, si formas parte de la cadena, te afecta directa o indirectamente.

¿Qué implicación supone ignorar estas normativas?

Además de arriesgarse a sanciones económicas importantes, ignorarlas implica asumir riesgos operativos y reputacionales. Si no te adaptas, podrías quedar fuera de ciertos contratos, perder clientes clave o estar expuesto a sanciones y, naturalmente, a ciberataques. Cumplir no es solo una obligación, es una forma de proteger tu negocio y una estrategia de posicionamiento en el mercado.

Esta guía práctica te ayudará a **entender lo esencial** de cada normativa, identificar si te afecta y dar los **primeros pasos para prepararte**, con un enfoque claro y útil.

NIS2

Guía práctica sobre la Directiva NIS2

Anteproyecto de Ley de Coordinación Y Gobernanza de la Ciberseguridad

La importancia de la futura Ley NIS2

La **Directiva NIS2** (UE 2022/2555), que refuerza el marco de ciberseguridad en Europa, tiene como objetivo reforzar la ciberseguridad en entidades esenciales e importantes, alineando a los Estados Miembros de la UE bajo criterios comunes.

Esta directiva, que España debía transponer antes de octubre de 2024, ha sido materializada en primera instancia en el anteproyecto de la Ley de Coordinación y Gobernanza de Ciberseguridad (futura transposición de la Directiva NIS2). Una vez aprobada la versión definitiva, esta ley permitirá dar un salto cualitativo en cuanto a las medidas de ciberseguridad de las entidades esenciales e importantes nacionales y en el modelo de gobernanza de la Seguridad de España, con la generación del Centro Nacional de Ciberseguridad.

¿A quién afecta?

La Directiva NIS2 **amplía significativamente el alcance** respecto a la anterior NIS1. Ya no se centra solo en operadores de servicios esenciales dependientes de sistemas de información y ciertos proveedores de servicios digitales: ahora incluye un gran número de organizaciones de un listado ampliado de sectores, incluyendo a la administración y a **empresas medianas y grandes** que prestan servicios esenciales o importantes para la economía y la sociedad. Y, por extensión de sus obligaciones, a sus proveedores.

La NIS2 distingue dos categorías:

1. Entidades Esenciales

Estarán obligadas a cumplir con medidas estrictas de ciberseguridad, notificación y supervisión activa. Aplica a empresas medianas o grandes (más de 50 empleados o 10 millones de euros de facturación) en estos sectores.

2. Entidades Importantes

Tendrán obligaciones similares, pero con un régimen de control más reactivo (por ejemplo, tras incidentes).

Categoría	Sectores Incluidos	Supervisión
Entidades Esenciales	- Energía (electricidad, gas, petróleo) - Transporte (aéreo, ferroviario, marítimo, por carretera) - Salud (hospitales, laboratorios, farmacéuticas) - Agua potable y aguas residuales - Banca y mercados financieros - Infraestructura digital (centros de datos, servicios DNS, nube) - Administración pública - Espacio (infraestructuras satelitales)	Supervisión **proactiva** por la autoridad competente
Entidades Importantes	- Servicios postales y de mensajería - Gestión de residuos - Industria alimentaria (producción y distribución) - Fabricantes de equipos críticos (medicina, electrónica, maquinaria) - Servicios digitales (redes sociales, plataformas online) - Actividades de I+D en sectores críticos	Supervisión **reactiva** (tras incidentes o indicios)

¿Y si mi empresa trabaja para una entidad afectada?

Aunque no estés directamente afectada (no perteneces a estos sectores) si prestas servicios o integras soluciones para entidades esenciales o importantes, es probable que te exijan garantías de cumplimiento (seguridad técnica, procesos, formación, etc.). Esto ya está ocurriendo en licitaciones y homologaciones.

Obligaciones clave:

Las obligaciones clave de la NIS2 para las empresas afectadas se centran en reforzar su ciberseguridad interna, gestionar riesgos de terceros y mejorar la capacidad de respuesta ante incidentes.

1. **Gestión de riesgos:** Evaluar riesgos periódicamente, aplicar medidas técnicas y organizativas (como control de accesos y protección de sistemas).
2. **Gobernanza:** La alta dirección debe implicarse: aprobar políticas, formarse y asumir responsabilidad en caso de negligencia.
3. **Responsable de Seguridad de la información:** Se designará a una persona, unidad u órgano colegiado como responsable de la seguridad de la información, el cual ejercerá las funciones de punto de contacto y coordinación técnica con las autoridades de control.
4. **Notificación de incidentes:** Informar incidentes graves en 24h, ampliar en 72h y entregar informe final.
5. **Cadena de suministro:** Evaluar riesgos de terceros, exigir medidas a proveedores y supervisar servicios externalizados.
6. **Gestión de vulnerabilidades:** Detectar, corregir y seguir alertas de seguridad; mantener sistemas actualizados.
7. **Formación:** Formar a toda la plantilla en seguridad, desde directivos hasta personal técnico.
8. **Supervisión y sanciones:** Autoridades podrán auditar y sancionar hasta con 10M€ o el 2% del volumen global.

¿Cómo prepararse?

1. Evalúa si tu empresa está afectada

- Verifica si perteneces a uno de los sectores cubiertos por NIS2 (energía, transporte, agua, salud, infraestructura digital, servicios públicos, etc.).
- Determina si tu organización es de tipo esencial o importante, según su tamaño e impacto.
- Analiza a tus clientes y considera si pueden solicitarte el cumplimiento de obligaciones relacionadas con esta normativa.

2. Implica a la dirección

- Informa a la alta dirección sobre los riesgos y sus nuevas responsabilidades.
- Establece un plan de gobierno de la ciberseguridad con roles claros.
- Designa a un Responsable de Seguridad de la Información

3. Haz un diagnóstico inicial de ciberseguridad

- Revisa tus políticas, controles y recursos actuales.
- Identifica vulnerabilidades técnicas y organizativas.
- Evalúa la madurez de tu sistema de gestión de ciberseguridad (puedes usar marcos como ISO 27001, ENS, NIST...).
- Realiza una evaluación de los riesgos que puedan afectarte.

4. Diseña un plan de acción

- Establece objetivos realistas y fases: corto, medio y largo plazo.
- Prioriza medidas básicas como:
  - Gestión de accesos y contraseñas
  - Segmentación de red
  - Actualización de software y sistemas
  - Seguridad en adquisición, desarrollo y mantenimiento de redes y SI
  - Políticas y procedimientos auditoría
  - Ciberhigiene y formación cíber
  - Criptografía y, en su caso, cifrado
  - Recursos humanos y gestión de activos
  - Autenticación
  - Copias de seguridad
  - Formación continua

5. Revisa contratos y terceros

- Asegúrate de que tus proveedores y socios cumplen con unos requisitos mínimos de seguridad.
- Incluye cláusulas específicas de NIS2 en nuevos contratos.
- Asegúrate de que eres notificado de incidentes que puedan afectarte.

6. Prepara los procesos de notificación

- Establece protocolos claros para detectar, evaluar y reportar incidentes.
- Designa responsables y canales de comunicación interna y externa.
- Simula incidentes para mejorar tu capacidad de respuesta.

7. Forma y sensibiliza a tu equipo

- Diseña un plan de concienciación para toda la plantilla.
- Ofrece formaciones específicas a IT, seguridad y directivos.
- Realiza simulacros o ejercicios tipo phishing.

8. Documenta y revisa

- Registra todas las acciones, medidas y auditorías.
- Prepara la documentación necesaria ante una inspección.
- Actualiza el plan periódicamente y tras incidentes.

Sanciones

La NIS2 prevé sanciones económicas muy elevadas para quienes incumplan. Hablamos de hasta 10 millones de euros o el 2% del volumen de negocio global anual (el que sea mayor), dependiendo del tipo de infracción.

Las sanciones pueden aplicarse por:

- No adoptar las medidas mínimas de ciberseguridad requeridas.
- No notificar incidentes graves en tiempo.
- Ocultar brechas de seguridad.
- Falta de cooperación con las autoridades competentes.

Además, los directivos pueden ser considerados responsables, y el impacto reputacional puede ser igual de grave que el económico.

CER

Guía práctica sobre la Ley CER

Anteproyecto de Ley de Protección y Resiliencia de Entidades Críticas

La importancia de la futura Ley CER

La futura Ley de Protección y Resiliencia de las Entidades Críticas (Ley CER) permitirá proteger los servicios esenciales que sostienen nuestra vida diaria: desde el suministro eléctrico hasta el transporte, pasando por sectores como la salud, el agua o la seguridad. La Directiva europea 2022/2557 sobre la resiliencia de las entidades críticas, que España debía transponer antes de octubre de 2024, ha sido materializada en primera instancia en el anteproyecto de ley aprobado por el Consejo de Ministros el 3 de junio de 2025. Aunque se trata de un anteproyecto que probablemente sufra algunas modificaciones y vaya acompañado de algún reglamento que lo desarrolle, marca ya una dirección clara en materia de seguridad y continuidad operativa para operadores públicos y privados.

Esta ley sustituye y amplía el marco actual de infraestructuras críticas, dando un paso más allá al exigir no solo protección frente a amenazas deliberadas, sino frente a todo tipo de amenazas, incorporando también capacidad real de respuesta y recuperación. Además, actualiza los sectores estratégicos, refuerza la coordinación con las fuerzas de seguridad y da lugar al nuevo Centro Nacional para la Protección y Resiliencia de las Entidades Críticas (CNPREC).

En resumen: si tu empresa presta un servicio esencial, esta ley te va a afectar. Y es mejor estar preparado.

¿A quién afecta?

La futura Ley CER afectará a todas las entidades públicas y privadas que presten servicios esenciales en sectores estratégicos dentro de España. Se incluyen sectores tradicionales (energía, salud, transporte), pero también se incorporan nuevos como:

- Hidrógeno
- Aguas residuales
- Sistemas urbanos de calefacción/refrigeración
- Seguridad Privada

Las empresas que sean designadas como entidades críticas por gestionar 1 o más infraestructuras críticas (según el nuevo Catálogo Nacional de Entidades Críticas y Estratégicas), estarán obligadas a cumplirla. Serán identificadas en función de su relevancia y del riesgo que la interrupción del servicio que prestan represente para la sociedad.

Obligaciones clave

Las organizaciones afectadas por la futura Ley CER deberán:

1. **Designar una responsable de seguridad y resiliencia:** Se establecerá una persona, unidad u órgano como responsable de estas obligaciones y punto de contacto único con las autoridades competentes.
2. **Realizar una Evaluación de Riesgos:** Las entidades realizarán una evaluación de riesgos de origen natural o humano, incluyendo riesgos de naturaleza intersectorial, accidentes, catástrofes naturales, emergencias de salud pública, amenazas híbridas y otras amenazas antagónicas, incluyendo delitos de terrorismo y crimen organizado.
3. **Elaboración de Plan de Resiliencia:** Las entidades deben elaborar un plan que se base en la evaluación de riesgos e incorpore medidas técnicas, organizativas y de seguridad, que aseguren la resiliencia y recuperación ante incidentes que puedan afectar sus servicios esenciales.
4. **Actualizar los procedimientos y protocolos de seguridad:** Es necesario revisar y renovar continuamente los protocolos internos para asegurar que se adaptan a las nuevas amenazas y requisitos legales. Esta adaptación irá enfocada a responder, resistir y mitigar las consecuencias de los incidentes.
5. **Formar y concienciar al personal y gestionar su protección y la de la cadena de suministro:** Se debe capacitar al personal en materia de seguridad y evaluar los riesgos asociados a proveedores y terceros, garantizando que toda la cadena cumpla con estándares adecuados. Debe considerarse un plan de concienciación del personal y las contratas, así como realizar ejercicios periódicos.
6. **Comprobación de idoneidad del personal crítico:** La directiva incluye mecanismos para permitir la comprobación de antecedentes penales a los empleados y contratas que tengan acceso a funciones o áreas sensibles para prevenir riesgos internos.
7. **Notificación de incidentes:** las entidades deberán notificar cualquier incidente que perturben de manera significativa el servicio esencial prestado, en un plazo máximo de 24 horas.
8. **Esquema de certificación:** Se prevé el desarrollo de un esquema de certificación que deberá ser superado por todas las entidades críticas, y que permitirá evaluar y certificar sus requisitos de resiliencia.
9. **Colaborar con las Fuerzas y Cuerpos de Seguridad:** Las entidades deben participar activamente en los planes de actuación coordinados con las autoridades para mejorar la protección y respuesta ante incidentes.
10. **Alinear prácticas con los planes estratégicos sectoriales:** Las entidades tienen que adaptar sus procedimientos a las directrices y planes aprobados por el nuevo Centro Nacional para la Protección y Resiliencia de las Entidades Críticas (CNPREC).

¿Cómo prepararse?

1. **Evaluar si se pertenece a un sector afectado:** Es fundamental identificar si tu empresa o entidad forma parte de los sectores estratégicos o críticos que la Ley CER contempla, ya que esto definirá las obligaciones que debes cumplir.
2. **Analizar los riesgos actuales:** Realiza un diagnóstico de los riesgos y vulnerabilidades que puedan afectar la continuidad y seguridad de los servicios esenciales que ofreces, considerando amenazas tanto físicas como digitales.
3. **Desarrollar un Plan de Resiliencia:** Aunque aún no sea obligatorio, es recomendable empezar a elaborar un plan que contemple medidas de prevención, respuesta y recuperación ante incidentes que puedan afectar la entidad.
4. **Mantenerse actualizado sobre la normativa:** La Ley CER está en proceso de desarrollo y reglamentación, por lo que es clave seguir de cerca las novedades para adaptar las medidas de manera oportuna, en particular todo lo relativo a los esquemas de certificación.
5. **Medidas específicas adelantadas:** El Anteproyecto de Ley menciona dos medidas de seguridad que deben tenerse en cuenta para la protección de las infraestructuras críticas y que actualmente presentan algunas dificultades legales para su implantación en general: controles de acceso biométrico y sistemas anti dron.

Sanciones

El anteproyecto de la ley CER prevé sanciones económicas muy elevadas para quienes incumplan. Hablamos de hasta 10 millones de euros o el 2% del volumen de negocio global anual (el que sea mayor), dependiendo del tipo de infracción.

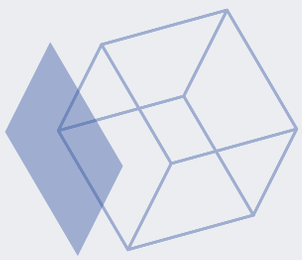
Las sanciones pueden aplicarse por:

- Incumplimiento en la obligación de notificar incidentes.
- No elaborar el Plan de Resiliencia.
- Incumplir medidas de protección exigidas.
- Obstaculizar la labor del CNPREC o de las Fuerzas de Seguridad.
- No verificar adecuadamente el perfil del personal con acceso a información o infraestructura sensible.

Nota final: complementariedad con NIS2.

Aunque tienen enfoques distintos, la **Ley CER** y la **Directiva NIS2** se complementan. Mientras la NIS2 se centra principalmente en la **ciberseguridad** de redes y sistemas de información, la CER aborda la **resiliencia física y operativa** de entidades que prestan servicios esenciales. Juntas forman el nuevo marco europeo de referencia en **seguridad y continuidad para infraestructuras críticas.**

Prepararse para una, sin dejar de lado la otra, es clave para cualquier organización que opere en sectores estratégicos.



LINCE

Guía práctica sobre LINCE (Esquema Nacional de Evaluación de Ciberseguridad)

¿Qué es LINCE y por qué importa?

LINCE es un esquema nacional de evaluación y certificación de la seguridad en productos TIC, impulsado por el **CCN** (Centro Criptológico Nacional). A diferencia de otros esquemas más complejos o costosos, LINCE está diseñado para ser ágil, accesible y proporcional, permitiendo evaluar la robustez de productos software o hardware frente a ataques comunes.
En un entorno donde cada vez más organizaciones operan bajo marcos normativos como NIS2 o CER, disponer de productos certificados bajo LINCE puede marcar la diferencia a nivel de cumplimiento, confianza y competitividad.

¿A quién afecta?

LINCE impacta principalmente a tres tipos de actores:

1. **Fabricantes y desarrolladores de productos TIC** que quieren optar a integrarse en entidades sujetas al Esquema Nacional de Seguridad (ENS), infraestructuras críticas, entornos clasificados o aparecer en el **CPSTIC** (Catálogo de Productos y Servicios de Seguridad TIC del CCN).
2. **Integradores y empresas instaladoras**, que deben utilizar productos previamente certificados para determinados entornos de seguridad.
3. **Clientes institucionales y empresas del sector estratégico,** que requieren garantías técnicas de seguridad al seleccionar proveedores o tecnologías.

Recientemente, se ha extendido esta categoría de productos a los productos de seguridad física tradicional: CCTV, control de accesos, detección de intrusión, etc.

Este esquema está especialmente orientado a productos usados en administraciones públicas, operadores críticos o empresas sujetas a regulación en ciberseguridad. Los productos y servicios que aparezcan el catálogo serán aptos para sistemas de información de categoría bajo o medio según ENS, no existiendo actualmente ningún esquema de certificación para productos destinados a sistemas de categoría alta.

Obligaciones clave

Aunque obtener la certificación LINCE no es obligatorio en todos los contextos, en ciertos entornos (como los regulados por ENS o NIS2) es un requisito explícito. Para acceder a la certificación, las empresas deben:

- Diseñar productos con criterios de seguridad desde el inicio.
- Entregar una documentación técnica rigurosa y transparente.
- Superar una evaluación técnica realizada por un laboratorio acreditado por el CCN.
- Incorporar mejoras o mitigar vulnerabilidades si se detectan durante la evaluación.
- Aceptar los tiempos, costes y compromisos de mantenimiento asociados al proceso.

Una vez aprobado, el producto entra en el CPSTIC, lo que le confiere un reconocimiento institucional que facilita su uso en entornos sensibles.

¿Cómo prepararse?

Prepararse para LINCE requiere un enfoque multidisciplinar, combinando diseño técnico, cumplimiento normativo y estrategia de producto. Algunos pasos clave:

- **Identifica si tu producto es candidato** para esta certificación: ¿Está dirigido a entornos críticos o públicos? ¿Sus clientes exigen garantías adicionales?
- **Evalúa tu estado actual** frente a los requisitos de LINCE, y realiza un gap analysis.
- **Fortalece la arquitectura de seguridad** del producto, incluyendo cifrado, control de accesos, trazabilidad, etc.
- **Recoge y organiza toda la documentación técnica**, incluyendo diagramas, pruebas, informes y manuales.
- **Consulta con laboratorios acreditados** para conocer plazos, costes y condiciones del proceso.
- **Asegúrate de que tus equipos de desarrollo, compliance y legal estén coordinados.**

Sanciones

Aunque LINCE no impone sanciones legales, la no certificación puede suponer una exclusión práctica de contratos públicos, proyectos críticos o entornos regulados. En un escenario donde la confianza técnica y la trazabilidad de seguridad son esenciales, no contar con un producto evaluado puede ser un gran hándicap frente a la competencia.

Además, en ciertos procesos de compra pública o en entornos regulados (como operadores esenciales), usar productos certificados puede ser una obligación directa o indirecta.

Nota Final: LINCE como complemento a otras normativas

LINCE no es un marco aislado: es una pieza clave del ecosistema de ciberseguridad nacional, que complementa a NIS2 y a la Ley CER. Mientras que estas dos regulaciones establecen obligaciones para las organizaciones, LINCE proporciona las herramientas para que los productos que usan cumplan con esos estándares. Una empresa que certifique sus soluciones bajo LINCE está dando un paso proactivo hacia el cumplimiento normativo y la protección real de sus clientes.

Cuadro Comparativo

Aspecto	NIS2	CER (Ley de Protección y Resiliencia)	LINCE (Esquema de Evaluación CCN)
¿Qué es?	Directiva europea y futura ley española sobre ciberseguridad para sectores esenciales y críticos.	Directiva europea y futura ley española sobre protección y resiliencia de entidades críticas.	Esquema nacional de certificación de productos TIC.
Objetivo principal	Reforzar la ciberseguridad de organizaciones esenciales y digitalmente dependientes.	Asegurar la continuidad de servicios esenciales en sectores estratégicos.	Validar la seguridad de productos TIC de forma ágil y accesible.
¿A quién afecta?	Empresas y operadores esenciales de sectores como energía, salud, transporte, digital...	Entidades críticas públicas y privadas (ej. agua, energía, transporte, seguridad privada...)	Fabricantes de productos TIC (y de productos de seguridad física, recientemente), integradores y usuarios institucionales y sujetos a ENS.
Obligaciones clave	Gestión de riesgos, ciberseguridad, notificación de incidentes, gobernanza, cadena de suministro.	Evaluación de riesgos, planes de resiliencia, control de personal, notificación de incidentes, esquemas de certificación, colaboración institucional.	Evaluación técnica, documentación, mejora continua, uso de laboratorios acreditados. Los sistemas de información de categoría bajo o medio según ENS obligados a usar productos certificados LINCE.
Nivel de aplicación	Organizacional (políticas, procesos, gobernanza), operativo y técnico (medidas, notificaciones).	Estratégico y estructural (planes nacionales y sectoriales), organizacional (evaluaciones de riesgos y planes) operativo y técnico (medidas, notificaciones).	Técnico (seguridad del producto y su entorno).
Sanciones o consecuencias	Multas (hasta 10 M€ o el 2% del volumen global de negocio), pérdida reputacional.	Multas (hasta 10 M€ o el 2% del volumen global de negocio), pérdida reputacional.	No hay sanciones, pero la falta de certificación puede impedir participar en proyectos clave.
Relación entre ellas	Norma marco de ciberseguridad a nivel europeo.	Complementa a NIS2 con un enfoque más físico y operativo sobre entidades críticas.	Complementa a ambas como herramienta técnica para cumplir requisitos de seguridad.
Estado actual en España	Anteproyecto de Ley (enero 2025), pero en proceso de transposición en España (plazo: octubre 2024).	Anteproyecto de Ley (mayo 2025), pero en proceso de transposición en España (plazo: octubre 2024).	Activo y en expansión, promovido por el CCN.

Check List

Checklist NIS2 (Ciberseguridad general y normativa europea)

- ☐ ¿Pertenezco a un sector esencial o importante?
- ☐ ¿Tengo identificado quién lidera la ciberseguridad en mi organización?
- ☐ ¿He realizado una evaluación de riesgos reciente?
- ☐ ¿Tengo planes de respuesta ante incidentes cibernéticos?
- ☐ ¿Conozco las obligaciones de notificación de incidentes en plazos cortos (24-72h)?
- ☐ ¿Mis proveedores cumplen también con requisitos de seguridad?

Checklist CER (Protección de entidades críticas)

- ☐ ¿Estoy dentro de un sector considerado estratégico o crítico?
- ☐ ¿Tengo identificados los servicios esenciales que presto?
- ☐ ¿Tengo identificado quién lidera la resiliencia en mi organización?
- ☐ ¿He desarrollado o previsto un Plan de Resiliencia (prevención, respuesta y recuperación)?
- ☐ ¿Tengo capacidad para evaluar los incidentes y notificarlos, en caso de ser necesario, en un plazo reducido (24 horas)?
- ☐ ¿Mi personal que accede a sistemas críticos pasa controles de antecedentes?
- ☐ ¿Tengo relación con el **CNPIC** (Centro Nacional para la Protección de Infraestructuras Críticas) /**CNPREC** (Centro Nacional para la Protección y Resiliencia de las Entidades Críticas) o estoy al tanto de sus requisitos?
- ☐ ¿Controlo la seguridad en mi cadena de suministro?

Checklist LINCE (Certificación de productos TIC de seguridad)

- ☐ ¿Diseño, fabrico o instalo productos de ciberseguridad (firewalls, soluciones de cifrado, etc.)?
- ☐ ¿Diseño, fabrico o instalo productos de seguridad física (CCTV, control de accesos, detección de intrusión, etc.)?
- ☐ ¿Mis productos están dirigidos a entornos sensibles o sector público?
- ☐ ¿Sé si necesito una certificación del Esquema LINCE para poder ofrecerlos?
- ☐ ¿Conozco los requisitos técnicos y niveles de evaluación exigidos?
- ☐ ¿He contactado con un laboratorio acreditado o tengo un plan para ello?

Glosario esencial – Normativas NIS2, CER y LINCE

Ciberseguridad
Protección de sistemas informáticos frente a ataques, accesos no autorizados o fallos que puedan poner en riesgo datos o servicios.

NIS2
Nueva directiva europea que obliga a empresas clave a reforzar su ciberseguridad y a notificar incidentes graves.

Entidades críticas
Empresas u organizaciones que prestan servicios esenciales (como energía, agua, salud o seguridad), cuyo fallo afectaría al país.

Resiliencia
Capacidad de una organización para prevenir, resistir y recuperarse de incidentes graves, ya sean tecnológicos, físicos o humanos.

CER (Ley de Protección y Resiliencia de las Entidades Críticas)
Normativa española en desarrollo que regula cómo deben protegerse los servicios esenciales en sectores estratégicos.

Notificación de incidentes
Obligación de informar a las autoridades competentes cuando ocurre un ciberataque o fallo que afecte a servicios clave.

Evaluación de riesgos
Análisis de amenazas potenciales para tomar decisiones de prevención y respuesta.

LINCE
Esquema español que certifica que un producto TIC (como un firewall o sistema de cifrado) ha superado pruebas de seguridad.

Producto TIC de seguridad
Herramienta o sistema que protege infraestructuras digitales, como antivirus, firewalls o sistemas de autenticación.

CNPIC / CNPREC
Organismos del Ministerio del Interior encargados de coordinar la protección de infraestructuras críticas en España. El CNPIC será sustituido por el nuevo CNPREC con la Ley CER.

Operador crítico
Empresa, pública o privada, que gestiona un servicio esencial y debe aplicar medidas de protección y planes de resiliencia.

Plan de resiliencia
Documento obligatorio que recoge cómo una entidad se prepara, responde y se recupera ante posibles crisis o ataques.

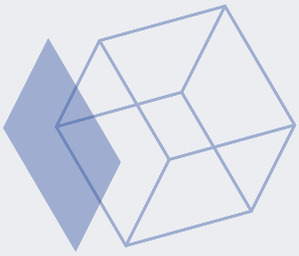
GDPR
Reglamento europeo que tiene como objetivo reforzar y unificar la protección de datos personales para todos los individuos dentro de la Unión Europea.

Tabla de Enlaces y Contactos Oficiales por Normativa

Normativa	Enlaces Oficiales	Organismos/ Contacto Útil
NIS2	Directiva NIS2 (UE)	- OCC: https://occ.ser.mir.es - CCN-CERT: https://ccn-cert.cni.es - INCIBE: incibe.es - Foro nacional de ciberseguridad: Guía
CER	Directiva CER (UE) Ministerio del Interior	- Secretaría de Estado de Seguridad - Futuro CNPREC (Centro Nacional de Protección y Resiliencia de Entidades Críticas)
LINCE	Guía LINCE – CCN Catálogo CPSTIC	- CCN-CERT - Contacto: ccn-cert@cni.es

¿Cómo usar esta tabla?

- **Haz clic en los enlaces** para acceder a los textos legales o guías prácticas.
- **Consulta los organismos clave** si necesitas orientación, certificación o asistencia técnica.
- **Incluye esta tabla como anexo** o inserta como gráfica adaptada al diseño de tu guía o dossier.



Información actualizada en Mayo de 2025