Perfil de Cumplimiento Especifico
CCN-STIC 892

Perfil de Cumplimiento Especifico para organizaciones en el ámbito de aplicación de la Directiva NIS2 (PCE-NIS2)

Abril 2024

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.04.23 17:33:39 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-158-2
Fecha de Edición: abril de 2024

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN

1. El objeto de este documento es mostrar el Perfil de Cumplimiento Específico que se ha desarrollado para dar respuesta a las disposiciones de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión. (Directiva NIS2, en adelante), por parte de aquellas organizaciones en el ámbito de aplicación del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS, en adelante), o que lo adopten voluntariamente.

2. PERFILES DE CUMPLIMIENTO ESPECÍFICOS EN EL ENS

2. En virtud del principio de proporcionalidad y para facilitar la conformidad con el Esquema Nacional de Seguridad (ENS) a determinadas entidades o sectores de actividad concretos, se podrán implementar perfiles de cumplimiento específicos que comprenderán aquel conjunto de medidas de seguridad que, trayendo causa del preceptivo análisis de riesgos, resulten de aplicación para una concreta categoría de seguridad.
3. Un perfil de cumplimiento específico es un conjunto de medidas de seguridad, comprendidas o no en el Real Decreto 311/2022, de 3 de mayo, que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreto y para una determinada categoría de seguridad.
4. Las Guías CCN-STIC, del Centro Criptológico Nacional, podrán establecer perfiles de cumplimiento específicos para entidades o sectores concretos, que incluirán la relación de requisitos, medidas y refuerzos que en cada caso resulten aplicables, o los criterios para su determinación.
5. El Centro Criptológico Nacional, en el ejercicio de sus competencias, validará y publicará los correspondientes perfiles de cumplimiento específicos que se definan, como se dispone en el artículo 30.3 del ENS, permitiendo a aquellas entidades comprendidas en su ámbito de aplicación alcanzar una mejor y más eficiente adaptación al ENS, racionalizando los recursos requeridos sin menoscabo de la protección perseguida y exigible, todo ello de acuerdo con las instrucciones técnicas de seguridad y guías de seguridad aprobadas conforme a lo previsto en la disposición adicional segunda.
6. Las auditorías se realizarán en función de la categoría del sistema y, en su caso, del perfil de cumplimiento específico que corresponda, según lo dispuesto en el Anexo I y Anexo III del ENS, y de conformidad con lo regulado en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de la Información.

3. APLICABILIDAD DEL ENS AL CUMPLIMIENTO DE LA DIRECTIVA NIS2

3.1 Ámbito de aplicación del ENS respecto a NIS2

7. El Real Decreto 311/2022, de 3 de mayo, por el que se regula ENS, es una norma jurídica de obligado cumplimiento, según su art. 2, para los sistemas de información de, entre otros:

   - Todo el sector público español, según lo determina el art. 2 de la Ley 40/2015.
   - Las entidades del sector privado, cuando, en virtud de una relación contractual, convenio o encomienda de gestión, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por éstas de sus competencias y potestades administrativas.
   - Las entidades titulares de sistemas que tratan información clasificada en base a la Ley 9/1968, de 5 de abril, sobre secretos oficiales (LSO) y demás normativa derivada.

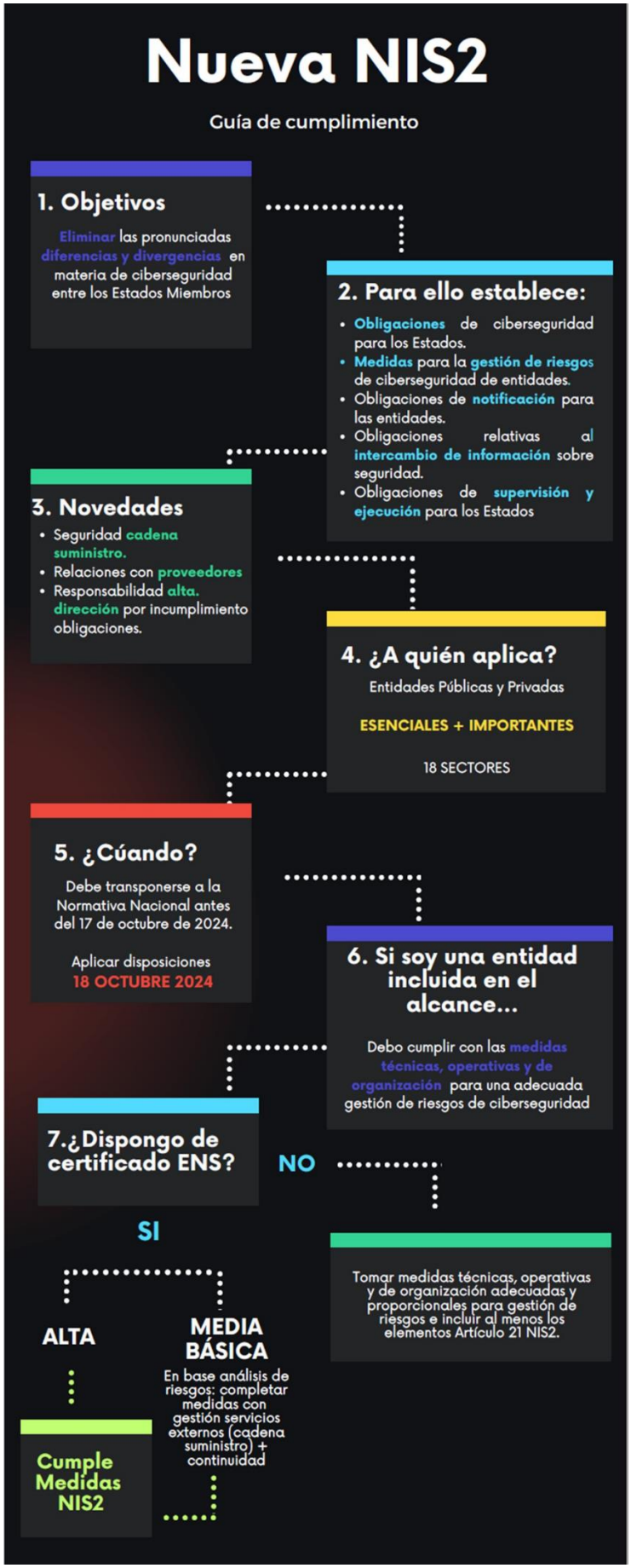
8. En este sentido, todas las entidades públicas dentro del ámbito de aplicación del Artículo 2 de la Directiva NIS2, así como muchas de privadas, se consideran asimismo sujetos obligados por el ENS.

9. Debido a esta circunstancia y a que, como puede verse en la tabla del apartado 3.3 y en el mapeo del Anexo I al final de este documento, el ENS permite a las organizaciones cumplir con los requisitos básicos comunes que determina la Directiva NIS2, es que se ha elaborado este Perfil de Cumplimiento Específico (PCE-NIS2) tras realizar un análisis de riesgos contemplando las vulnerabilidades y amenazas generalizadas a las que hacen frente el conjunto de entidades públicas o privadas dentro del ámbito de aplicación del Artículo 2 de la Directiva NIS2.

10. A tal fin, con el objetivo de garantizar la máxima seguridad de los sistemas de información y comunicaciones concernidos, se da cumplimiento al mandato impuesto al CCN validando este **Perfil de Cumplimiento Especifico para garantizar un nivel mínimo de seguridad en organizaciones en el ámbito de aplicación del ENS y de la Directiva NIS2 (PCE-NIS2)**.

11. No obstante, asumiendo que una Directiva Europea es un instrumento jurídico que requiere su transposición al ordenamiento jurídico de los estados miembros, cuando dicha transposición se lleve a cabo y entre en vigor en España, el Centro Criptológico Nacional determinará en su caso si se requiere realizar algún ajuste a este PCE-NIS2.

12. Una organización con su sistema de información actualmente certificado en categoría ALTA del ENS, con alcance adecuado, cumple con los requisitos de ciberseguridad de la Directiva NIS2. En cambio, si no está certificado del ENS, o lo está en categorías MEDIA o BÁSICA, podrá adoptar este PCE-NIS2 para cumplir.


Nueva NIS2
Guía de cumplimiento
1. Objetivos
Eliminar las pronunciadas diferencias y divergencias en materia de ciberseguridad entre los Estados Miembros
2. Para ello establece:
Obligaciones de ciberseguridad para los Estados.
Medidas para la gestión de riesgos de ciberseguridad de entidades.
Obligaciones de notificación para las entidades.
Obligaciones relativas al intercambio de información sobre seguridad.
Obligaciones de supervisión y ejecución para los Estados
3. Novedades
Seguridad cadena suministro.
Relaciones con proveedores
Responsabilidad alta. dirección por incumplimiento obligaciones.
4. ¿A quién aplica?
Entidades Públicas y Privadas
ESENCIALES + IMPORTANTES
18 SECTORES
5. ¿Cúando?
Debe transponerse a la Normativa Nacional antes del 17 de octubre de 2024.
Aplicar disposiciones
18 OCTUBRE 2024
6. Si soy una entidad incluida en el alcance...
Debo cumplir con las medidas técnicas, operativas y de organización para una adecuada gestión de riesgos de ciberseguridad
7.¿Dispongo de certificado ENS?
NO
SI
Tomar medidas técnicas, operativas y de organización adecuadas y proporcionales para gestión de riesgos e incluir al menos los elementos Artículo 21 NIS2.
ALTA
MEDIA BÁSICA
En base análisis de riesgos: completar medidas con gestión servicios externos (cadena suministro) + continuidad
Cumple Medidas NIS2

3.2 La exigencia de garantías respecto a la Directiva NIS2

13. Para las entidades de su ámbito de aplicación, la Directiva NIS2 exige en los siguientes preceptos y de manera muy específica, la adopción de medidas concretas, a saber:

Mandato Directiva NIS2	Regulado En el RD-L 12/2018	Regulado En el RD 43/2021	Necesidad expresada en la Directiva NIS2	Acción vinculada con el RD 311/2022 (ENS)
Art. 5. Armonización mínima	Art. 16 y Art. 18		*La presente Directiva no será óbice para que los Estados miembros adopten o mantengan disposiciones que garanticen un nivel más elevado de ciberseguridad, siempre y cuando tales disposiciones sean compatibles con las obligaciones establecidas en el Derecho de la Unión.*	Se ha desarrollado un Perfil de Cumplimiento Específico de los regulados en el art. 30 del RD 311/2022 (ENS), denominado **Perfil de Cumplimiento Especifico para garantizar un nivel mínimo de seguridad en organizaciones en el ámbito de aplicación del ENS y de la Directiva NIS2 (PCE-NIS2).**
Art. 21. Medidas para la gestión de riesgos de ciberseguridad			*1. Los Estados miembros velarán por que las entidades esenciales e importantes tomen las medidas técnicas, operativas y de organización adecuadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de los sistemas de redes y de información que utilizan dichas entidades en sus operaciones o en la prestación de sus servicios y prevenir o minimizar las repercusiones de los incidentes en los destinatarios de sus servicios y en otros servicios.* *Teniendo en cuenta la situación y, en su caso, las normas europeas e internacionales pertinentes, así como el coste de su aplicación, las medidas a que se refiere el párrafo primero garantizarán un nivel de seguridad de los sistemas de redes y de información adecuado en relación con los riesgos planteados. Al evaluar la proporcionalidad de dichas 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, incluidas sus repercusiones sociales y económicas.*	Este Perfil de Cumplimiento Específico (PCE-NIS2) hace posible que las medidas a las que se refiere la Directiva NIS2 se satisfagan mediante su aplicación a las entidades esenciales e importantes. Asimismo, dentro del marco creado por el precitado PCE-NIS2, de estimarse necesario, podrán aprobarse **Instrucciones Técnicas de Seguridad o mandatos equivalentes** que desarrollen los extremos de seguridad que fueren necesarios y que puedan involucrar medidas de naturaleza jurídica, organizativa, técnica y de personal, compendio normativo y documental que podrá incluir las **Guías** complementarias de desarrollo que se consideren convenientes.

Art. 31. Aspectos generales relativos a la supervisión y la ejecución	Art. 32 y Art. 34	Art. 15	*1. Los Estados miembros velarán por que sus autoridades competentes supervisen efectivamente y adopten las medidas necesarias para garantizar el cumplimiento de la presente Directiva.*	Una forma eficaz de mantener un grado de supervisión razonable de las medias de seguridad que deben adoptar las entidades del ámbito de aplicación de la transposición de la Directiva NIS2 es mediante el **Esquema de Certificación de la Conformidad con el ENS en base al PCE-NIS2**.
Art. 32. Medidas de supervisión y ejecución relativas a entidades esenciales			*1. Los Estados miembros garantizarán que las medidas de supervisión o ejecución impuestas a las entidades esenciales en relación con las obligaciones establecidas en la presente Directiva sean efectivas, proporcionadas y disuasorias, teniendo en cuenta las circunstancias de cada caso individual…*	Las Entidades de Certificación (EC), acreditadas por la Entidad Nacional de Acreditación (ENAC); así como los Órganos de Auditoría Técnica (OAT) de la Administración, reconocidos por el Centro Criptológico Nacional (CCN), garantizarán y certificarán el cumplimiento del PCE-NIS2.
Art. 33. Medidas de supervisión y ejecución en relación con entidades importantes			*1. Cuando dispongan de pruebas, indicios o información de que una entidad importante presuntamente no cumple la presente Directiva, en particular sus artículos 21 y 23, los Estados miembros garantizarán que las autoridades competentes actúen, cuando proceda, a través de medidas de supervisión a posteriori. Los Estados miembros velarán por que esas medidas sean eficaces, proporcionadas y disuasorias, teniendo en cuenta las circunstancias de cada caso…*	El Perfil de Cumplimiento Específico (PCE-NIS2), en el marco de la Certificación de Conformidad con el ENS, debe ser objeto de una auditoría interna anual, así como de una auditoría de renovación de la Certificación de Conformidad cada 2 años.

3.3 Obligaciones para las entidades incluidas en el alcance

14. La Directiva NIS2 establece obligaciones para las entidades incluidas en su alcance, que se resumen en los siguientes puntos:

ARTÍCULO	OBLIGACIÓN
CAPITULO I – DISPOSICIONES GENERALES	
3	**Registro de entidades esenciales e importantes**
Remitir información a la autoridad competente: Datos de contacto, sector y subsector, tipo de servicio, los Estados miembros donde se prestan servicios. Notificar cambios.	
CAPITULO IV – MEDIDAS PARA LA GESTIÓN DE RIESGOS DE CIBERSEGURIDAD Y OBLIGACIONES DE NOTIFICACIÓN	
20	**Gobernanza**

ARTÍCULO	OBLIGACIÓN
Aprobar las medidas de gestión de los riesgos de ciberseguridad, supervisar su puesta en práctica y responder por el incumplimiento.	
Asistir de forma periódica a formaciones específicas: órganos de dirección y fomentar en resto empleados.	
21	**Medidas para la gestión de riesgos de ciberseguridad**
Adoptar medidas técnicas, operativas y de organización adecuadas para gestionar los riesgos. Considerar vulnerabilidades específicas y evaluaciones coordinadas de riesgos. Adoptar medidas correctoras en caso de incumplimiento.	
23	**Obligaciones de notificación**
Notificar a las autoridades competentes o al CSIRT cualquier incidente que tenga un impacto significativo en la prestación de sus servicios. Incluir información repercusiones transfronterizas. Alerta temprana (24h), 72h (excepción prestador de servicios de confianza 24h), informe intermedio e informe final (1 mes).	
Notificar a los destinatarios de sus servicios los incidentes susceptibles de afectar negativamente a la prestación de dicho servicio, si procede. Si procede, notificar la ciberamenaza y las medidas o soluciones.	
24	**Utilización de esquemas europeos de certificación de la ciberseguridad**
Se podrá requerir el uso de productos, servicios y procesos TIC particulares certificados.	
Serán alentadas a utilizar servicios de confianza cualificados	
CAPITULO V – JURISDICCIÓN Y REGISTRO	
26	**Jurisdicción y Territorialidad**
Designar un representante en la Unión en el caso de que la entidad contemplada en el apartado 1b) no esté establecida en la Unión, pero ofrece servicios dentro de esta.	
27	**Registro de entidades**
Las entidades a que se refiere el artículo 28.1 deben remitir a las autoridades competentes la información requerida y notificar cualquier cambio en la misma. Cuando aplique, remitir por el mecanismo de auto notificación (Artículo 3 apartado 4).	
28	**Base de datos de nombres de dominio y datos de registro**
Los registros de dominio de primer nivel y entidades que prestan servicios de registro de dominio deben recopilar y mantengan datos precisos y completos sobre el registro de nombres de dominio en una base de datos e información de contacto.	
Disponer de políticas y procedimientos, incluyendo procedimientos de verificación, para garantizar que las bases de datos incluyan información precisa y completa y poner a disposición del público.	
Publicar, sin demora indebida después del registro de un nombre de dominio, los datos de registro de dominio que no sean de carácter personal.	
Las entidades que prestan servicios de registro de nombres de dominio de primer nivel deben conceder acceso a datos específicos sobre el registro de nombres de dominio, previa solicitud lícita y debidamente justificada, a los solicitantes de acceso legítimos y responder a todas las solicitudes de acceso 72h. Las políticas y los procedimientos de divulgación de dichos datos deben ponerse a disposición del público.	
Los registros de nombres de dominio de primer nivel y las entidades que prestan servicios de servicios de registro de nombres de dominio deben cooperar entre sí.	
CAPITULO VI – INTERCAMBIO DE INFORMACIÓN	
29	**Mecanismos de intercambio de información sobre ciberseguridad**
Intercambio voluntario de información de ciberseguridad entre entidades esenciales e importantes y otras entidades no incluidas en el alcance de Directiva. Si es relevante, con proveedores o prestadores de servicios. Comunidades de entidades esenciales e importantes.	
Las entidades esenciales e importantes notificarán a las autoridades competentes su participación (incorporación y retirada) en los mecanismos de intercambio de información.	
30	**Notificación voluntaria de información pertinente**

ARTÍCULO	OBLIGACIÓN
Las entidades esenciales e importantes podrán notificar, de forma voluntaria, a las autoridades competentes o a los CSIRT cualquier incidente, ciberamenaza y cuasi incidente. Opción de notificación de otras entidades.	
CAPITULO VII – SUPERVISIÓN Y EJECUCIÓN	
32	**Medidas de supervisión y ejecución en el caso de entidades esenciales**
Garantizar que la persona física responsable o que actúe como representante de una entidad esencial está facultada para garantizar el cumplimiento de las obligaciones establecidas en la presente Directiva.	

3.4 Medidas para la gestión de riesgos de ciberseguridad

15. El artículo 21 sobre medidas para la gestión de riesgos de ciberseguridad, de la Directiva NIS2, señala una serie de medidas de seguridad encaminadas a proteger a las entidades esenciales e importantes en su ámbito de aplicación.

16. En la tabla que sigue, se muestra la correlación o mapeo entre dichas medidas generales de la Directiva NIS2 y medidas de seguridad concretas del Anexo II del ENS.

Medidas generales de la Directiva NIS2	Medidas de seguridad del ENS relacionadas
Art. 21 a) las políticas de seguridad de los sistemas de información y análisis de riesgos.	**[org.1]** Política de Seguridad **[org.2]** Normativa de Seguridad **[op.pl.1]** Análisis de riesgos
Art. 21 b) La gestión de incidentes.	**[op.exp.7]** Gestión de incidentes
Art 21 c) La continuidad de las actividades, como la gestión de copias de seguridad y la recuperación en caso de catástrofe, y la gestión de crisis.	**[op.cont.4]** Medios alternativos **[mp.info.6]** Copias de seguridad **[op.cont.1]** Análisis de impacto (BIA) **[op.con.2]** Plan de Continuidad **[op.cont.3]** Pruebas periódicas
Art. 21 d) 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.	**[op.ext.3]** Protección de la cadena de suministro **[op.ext.1]** Contratación y acuerdos de nivel de servicio **[op.ext.2]** Gestión diaria **[op.ext.4]** Interconexión de sistemas
Art. 21 e) La seguridad en la adquisición, y el desarrollo y mantenimiento de sistemas de redes y de información, incluida la gestión y divulgación de las vulnerabilidades.	**[op.pl.3]** Adquisición de nuevos componentes **[op.pl.5]** Componentes certificados **[mp.sw.1]** Desarrollo de aplicaciones **[mp.sw.2]** Aceptación y puesta en servicio **[op.exp.4]** Mantenimiento y actualizaciones de seguridad **[op.mon.3]** Vigilancia
Art. 21 f) Las políticas y los procedimientos para evaluar la eficacia de las medidas para la gestión de riesgos de ciberseguridad.	**[op.mon.2]** Sistema de métricas **[op.exp.9]** Registro de la gestión de incidentes
Art. 21 g) Las prácticas básicas de ciber-higiene y formación en ciberseguridad.	**[mp.pr.3]** Concienciación **[mp.per.4]** Formación
Art. 21 h) Las políticas y procedimientos relativos a la utilización de criptografía y, en su caso, de cifrado.	**[op.exp.10]** Protección de claves criptográficas **[mp.si.2]** Criptografía

Art. 21 i) La seguridad de los recursos humanos, las políticas de control de acceso y la gestión de activos;	**[mp.per.1]** Caracterización del puesto de trabajo **[mp.per.2]** Deberes y obligaciones **[op.acc.1]** Identificación **[op.acc.2]** Requisitos de acceso **[op.acc.3]** Segregación de funciones y tareas **[op.acc.4]** Proceso de gestión de derechos de acceso **[op.acc.5]** Mecanismos de autenticación (usuarios externos) **[op.acc.6]** Mecanismos de autenticación (usuarios de la organización) **[op.exp.1]** Inventario de activos
Art. 21 j) El uso de soluciones de autenticación multifactorial o de autenticación continua, comunicaciones de voz, vídeo y texto seguras y sistemas seguros de comunicaciones de emergencia en la entidad, cuando proceda.	**[op.acc.5]** Mecanismos de autenticación (usuarios externos) **[op.acc.6]** Mecanismos de autenticación (usuarios de la organización) **[mp.com.2]** Protección de la confidencialidad

17. Asimismo, se considera relevante trazar la responsabilidad de los órganos de dirección que determina el artículo 20 de la Directiva NIS2 con los artículos y medidas de seguridad del ENS:

Disposiciones de la Directiva NIS2	Disposiciones del ENS relacionadas
Art. 20.1 Los Estados miembros velarán por que los órganos de dirección de las entidades esenciales e importantes aprueben las medidas para la gestión de riesgos de ciberseguridad adoptadas por dichas entidades para dar cumplimiento al artículo 21, supervisen su puesta en práctica y respondan por el incumplimiento por parte de las entidades de dicho artículo.	**Art. 6.** La seguridad como un proceso integral **Art. 11.** Diferenciación de responsabilidades **Art. 12.** Política de seguridad y requisitos mínimos de seguridad. **Art. 13.** Organización e implantación del proceso de seguridad. **[org.1]** Política de seguridad

4. SOBRE ESTE PCE-NIS2

4.1 Alcance del Documento

18. Este documento sobre el PCE-NIS2:

- Describe los principales requisitos de la Directiva NIS2.
- Analiza los requisitos de la Directiva NIS2 en relación con los requisitos vigentes en materia de ciberseguridad del ENS, con el fin de identificar las medidas de seguridad necesarias del Anexo II, así como aquellas en las que se requieren determinados refuerzos.
- Establece una metodología para alinear otros marcos (‘frameworks’ en inglés) de Seguridad con la Directiva NIS2;
- Tiene en cuenta los controles de la norma ISO/IEC 27001:2022 sobre Sistemas de gestión de la seguridad de la información.

19. En resumen, permite compatibilizar las disposiciones de la Directiva NIS2 con dos (2) certificaciones distintas: la primera el ENS, al incardinarse el PCE-NIS2 en dicha norma jurídica de obligado cumplimiento; y la segunda la ISO 27001 en base al

mapeo entre las medidas de seguridad del Anexo II del ENS y los controles del Anexo A de la ISO/IEC 27001:2022, y viceversa, disponible en la guía "***CCN-STIC 825 ENS Certificaciones 27001***" y su "***CCN-STIC 825 Anexo independiente***".

4.2 Organismos de certificación del ENS

20. Las Certificaciones de Conformidad con el ENS las pueden expedir los siguientes organismos de certificación que se basarán entre otras, en la norma ISO/IEC 17065:2012:
    - Una Entidad de Certificación (EC) acreditada por la Entidad Nacional de Acreditación (ENAC).
    - Un Órgano de Auditoría Técnica (OAT) del Sector Público, reconocido por el Centro Criptológico Nacional (CCN).
    - En determinados casos específicos, directamente el CCN.

4.3 Demostrar el cumplimiento de la Directiva NIS2

21. Con el fin de demostrar el cumplimiento de las medidas para la gestión de riesgos de ciberseguridad y en ausencia de esquemas europeos de certificación de la ciberseguridad adecuados que se hayan adoptado de conformidad con el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, los Estados miembros, consultando al Grupo de Cooperación y al Grupo Europeo de Certificación de la Ciberseguridad, deben promover el uso de las normas europeas e internacionales pertinentes por parte de las entidades esenciales e importantes, o pueden exigir a las entidades que utilicen productos, servicios y procesos de TIC certificados.
22. A los efectos de demostrar la conformidad con determinados requisitos del artículo 21 sobre medidas para la gestión de riesgos de ciberseguridad de la Directiva NIS2, es que se ha elaborado este Perfil de Cumplimiento Específico como unos requisitos mínimos de Certificación de la Conformidad comunes, que tengan en cuenta el grado de criticidad de sus sectores y el tipo de servicio que prestan, minimizando el impacto en las actividades de la entidad de que se trate.
23. Debe tenerse en consideración que ante la disparidad de sectores que conforman las entidades esenciales, así como las importantes, una de las medidas de seguridad es la [op.pl.1] Análisis de riesgos, que permite incorporar medidas de seguridad adicionales de mitigación de riesgos para aquellas organizaciones que así lo requieran.
24. La frecuencia de las Auditorías de Certificación de la Conformidad con el ENS (también en base a este PCE-NIS2) se realizará cada dos (2) años, o siempre que se hubieren producido modificaciones sustanciales en los sistemas de información concernidos que induzcan a pensar en una alteración del nivel de riesgo aceptable, garantizándose la idoneidad y la actualización de las listas de las entidades esenciales e importantes, así como de las entidades que prestan

servicios de registro de nombres de dominio, que se hayan certificado bajo este PCE-NIS2 del ENS.

25. El CCN velará para que las funciones de supervisión o auditoría en relación con las entidades esenciales e importantes se lleven a cabo por profesionales cualificados, con las competencias necesarias para llevar a cabo dichas tareas de acuerdo a los requisitos establecidos en la guía "***CCN-CERT IC-01/19 criterios generales de auditoría y certificación***" en que también se rigen los organismos de certificación del ENS de forma adicional a la norma ISO/IEC 17065:2012.

5. DISTINCIÓN ENTRE ENTIDADES ESENCIALES E IMPORTANTES

5.1 Entidades esenciales

26. Se consideran entidades esenciales según el art. 3.1 de la Directiva NIS2:

a) entidades de alguno de los tipos mencionados en el anexo I que superen los límites máximos previstos en el artículo 2, apartado 1, del anexo de la Recomendación 2003/361/CE para las medianas empresas;
b) prestadores cualificados de servicios de confianza y registros de nombres de dominio de primer nivel, así como proveedores de servicios de DNS, independientemente de su tamaño;
c) proveedores de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles para el público que sean consideradas medianas empresas con arreglo al artículo 2 del anexo de la Recomendación 2003/361/CE;
d) entidades de la Administración pública a que se refiere el artículo 2, apartado 2, letra f) inciso i); [Entidad de la Administración pública central, definida por un Estado miembro de conformidad con el Derecho nacional].
e) cualquier otra entidad de uno de los tipos mencionados en los anexos I o II que un Estado miembro identifique como entidad esencial en virtud del artículo 2, apartado 2, letras b) a e); [La entidad sea el único proveedor en un Estado miembro de un servicio esencial para el mantenimiento de actividades sociales o económicas críticas; una perturbación del servicio prestado por la entidad pudiera tener repercusiones significativas sobre la seguridad pública, el orden público o la salud pública; una perturbación del servicio prestado por la entidad pudiera inducir riesgos sistémicos significativos, en particular para los sectores en los que tal perturbación podría tener repercusiones de carácter transfronterizo; la entidad sea crítica a la luz de su importancia específica a nivel nacional o regional para el sector o tipo de servicio en concreto o para otros sectores interdependientes en el Estado miembro].
f) entidades identificadas como entidades críticas con arreglo a la Directiva (UE) 2022/2557 a que se refiere el artículo 2, apartado 3, letra f), de la presente Directiva;
g) si así lo dispone el Estado miembro, las entidades identificadas por dicho Estado miembro antes del 16 de enero de 2023 como operadores de servicios esenciales de conformidad con la Directiva (UE) 2016/1148 o el Derecho nacional.

5.2 Entidades importantes

27. Se consideran entidades importantes las entidades de uno de los tipos mencionados en los anexos I o II de la Directiva NIS2 que no puedan considerarse entidades esenciales.

5.3 Otras entidades comprendidas en el ámbito de aplicación

28. Los Estados miembros también deben disponer que, determinadas pequeñas empresas y microempresas tal como se definen en el artículo 2, apartados 2 y 3 de la Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas (DO L 124 de 20.5.2003, p. 36), que cumplan criterios específicos que pongan de manifiesto su papel clave para la sociedad, la economía o para determinados sectores o tipos de servicios, queden comprendidas en el ámbito de aplicación de la presente Directiva

6. DECLARACIÓN DE APLICABILIDAD

6.1 Consideraciones previas

29. Como es sabido, la declaración de aplicabilidad comprende el conjunto de medidas de seguridad que son de aplicación para el cumplimiento del ENS en un sistema concreto. Tal conjunto de medidas dependerá de la categoría del sistema y de los niveles asociados a las dimensiones de seguridad.
30. En el Anexo II del RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, se tiene en cuenta para cada medida de seguridad, no únicamente la aplicabilidad de requisitos base, sino la de posibles refuerzos obligatorios.
31. Se ha determinado así, para aquellas organizaciones en el ámbito de la Directiva NIS2, las medidas que son de aplicación, y, en caso de aplicar, la exigencia de los diferentes requisitos base y de los posibles refuerzos obligatorios, mediante una tabla modulada mediante los comentarios del apartado 5 de este mismo documento.
32. Debe tenerse en cuenta que existe una multiplicidad de tipos de organizaciones, englobadas dentro de las **entidades esenciales** y las **entidades importantes**, según dispone el artículo 3.1 de la directiva NIS2. En consecuencia, podría ser que una de esas organizaciones, en base a sus especificidades (al riesgo), categorizara su sistema de categoría ALTA, por lo que ajustara su Declaración de Aplicabilidad a requisitos más exigentes del ENS que los determinados en este Perfil de Cumplimiento Específico.
33. En la tabla de criterios de aplicación se reproduce literalmente la exigencia de requisitos base y refuerzos obligatorios del Anexo II del ENS para cada una de las categorías del sistema, adicionando a la derecha la columna ‘Aplicación’ con los

requisitos específicos para este perfil, junto a una columna 'Ref' con la referencia al detalle de aplicación para aquellas medidas con exigencias superiores a las determinadas por la categoría del ENS que se considera.

6.2 Detalle de la Declaración de Aplicabilidad

Dimensiones								
Afectadas	CAT B	CAT M	CAT A	Medida	Importantes	Esenciales	Aplicación[1]	Ref
Categoría	aplica	aplica	aplica	org.1	SI	SI	BÁSICA	
Categoría	aplica	aplica	aplica	org.2	SI	SI	BÁSICA	
Categoría	aplica	aplica	aplica	org.3	SI	SI	BÁSICA	
Categoría	aplica	aplica	aplica	org.4	SI	SI	BÁSICA	
Categoría	aplica	+ R1	+ R2	op.pl.1	SI *	SI	MEDIA	**71**
Categoría	aplica	+ R1	+ R1 + R2 + R3	op.pl.2	SI	SI	MEDIA	
Categoría	aplica	aplica	aplica	op.pl.3	SI	SI	BÁSICA	
D	aplica	+ R1	+ R1	op.pl.4	SI	SI	Bajo	
Categoría	n.a.	aplica	aplica	op.pl.5	SI	SI	MEDIA (+R1+R2)	**7.2**
T A	aplica	+ R1	+ R1	op.acc.1	SI	SI	Medio	
C I T A	aplica	aplica	+ R1	op.acc.2	SI	SI	Alto	
C I T A	n.a.	aplica	+ R1	op.acc.3	SI	SI	Medio	
C I T A	aplica	aplica	aplica	op.acc.4	SI	SI	Bajo	
C I T A	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5	op.acc.5	SI *	SI	Medio	**7.3**
C I T A	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9	op.acc.6	SI *	SI	Medio	**7.4**
Categoría	aplica	aplica	aplica	op.exp.1	SI*	SI	BÁSICA (+R1+R2+R3+R4)	**7.5**
Categoría	aplica	aplica	aplica	op.exp.2	SI	SI	BÁSICA	
Categoría	aplica	+ R1	+ R1 + R2 + R3	op.exp.3	SI	SI	MEDIA	
Categoría	aplica	+ R1	+ R1 + R2	op.exp.4	SI	SI	BÁSICA (+R4)	**7.6**
Categoría	n.a.	aplica	+ R1	op.exp.5	SI	SI	MEDIA	
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	op.exp.6	SI	SI	MEDIA	
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3	op.exp.7	SI	SI	ALTA	
T	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5	op.exp.8	SI	SI	Medio	
Categoría	aplica	aplica	aplica	op.exp.9	SI	SI	BÁSICA	
Categoría	aplica	+ R1	+ R1	op.exp.10	SI	SI	BÁSICA	
Categoría	n.a.	aplica	aplica	op.ext.1	SI	SI	MEDIA	
Categoría	n.a.	aplica	aplica	op.ext.2	SI	SI	MEDIA	
Categoría	n.a.	n.a.	aplica	op.ext.3	SI	SI	ALTA (+R1+R2+R3)	**7.7**
Categoría	n.a.	aplica	+ R1	op.ext.4	SI	SI	ALTA	
Categoría	aplica	+ R1	+ R1 + R2	op.nub.1	SI	SI	ALTA	
D	n.a.	aplica	aplica	op.cont.1	SI	SI	Alto	
D	n.a.	n.a.	aplica	op.cont.2	SI	SI	Alto (+R1+R2)	**7.8**

[1] En la columna "Aplicación", se reflejará la categoría (BÁSICA, MEDIA, ALTA) que corresponda en caso de que en esa medida se vean afectadas las cinco (5) dimensiones de seguridad (Confidencialidad-C, Integridad-I, Autenticidad-A, Trazabilidad-T, Disponibilidad-D). En caso, de que no se vean afectadas las cinco (5) dimensiones, se reflejará el nivel a aplicar (Bajo, Medio, Alto).

Dimensiones								
Afectadas	CAT B	CAT M	CAT A	Medida	Importantes	Esenciales	Aplicación[1]	Ref
D	n.a.	n.a.	aplica	op.cont.3	SI	SI	Alto	
D	n.a.	n.a.	aplica	op.cont.4	SI	SI	Alto (+R1)	7.9
Categoría	aplica	+ R1	+ R1 + R2	op.mon.1	SI	SI	MEDIA	
Categoría	aplica	+ R1 + R2	+ R1 + R2	op.mon.2	SI	SI	ALTA	
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 +R6	op.mon.3	SI *	SI	BÁSICA (+R2+R6)	7.10
Categoría	aplica	aplica	aplica	mp.if.1	SI	SI	MEDIA	
Categoría	aplica	aplica	aplica	mp.if.2	SI	SI	MEDIA	
Categoría	aplica	aplica	aplica	mp.if.3	SI	SI	MEDIA	
D	aplica	+ R1	+ R1	mp.if.4	SI	SI	Medio	
D	aplica	aplica	aplica	mp.if.5	SI	SI	Medio	
D	n.a.	aplica	aplica	mp.if.6	SI	SI	Medio	
Categoría	aplica	aplica	aplica	mp.if.7	SI	SI	MEDIA	
Categoría	n.a.	aplica	aplica	mp.per.1	SI *	SI	MEDIA (R1)	711
Categoría	aplica	+ R1	+ R1	mp.per.2	SI	SI	ALTA	
Categoría	aplica	aplica	aplica	mp.per.3	SI	SI	BÁSICA	
Categoría	aplica	aplica	aplica	mp.per.4	SI	SI	BÁSICA	
Categoría	aplica	+ R1	+ R1	mp.eq.1	SI	SI	BÁSICA	
A	n.a.	aplica	+ R1	mp.eq.2	SI	SI	Medio	
Categoría	aplica	aplica	+ R1 + R2	mp.eq.3	SI	SI	MEDIA (R1)	7.12
C	aplica	+ R1	+ R1	mp.eq.4	SI	SI	Bajo	
Categoría	aplica	aplica	aplica	mp.com.1	SI	SI	BÁSICA	
C	aplica	+ R1	+ R1 + R2 + R3	mp.com.2	SI	SI	ALTO (R4+R5)	7.13
I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	mp.com.3	SI	SI	Medio	
Categoría	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4	mp.com.4	SI	SI	MEDIA	
C	n.a.	aplica	aplica	mp.si.1	SI	SI	Medio	
C I	n.a.	aplica	+ R1 + R2	mp.si.2	SI	SI	Alto	
Categoría	aplica	aplica	aplica	mp.si.3	NO	SI	BÁSICA	
Categoría	aplica	aplica	aplica	mp.si.4	NO	SI	BÁSICA	
C	aplica	+ R1	+ R1	mp.si.5	SI	SI	Bajo	
Categoría	n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4	mp.sw.1	SI	SI	MEDIA	
Categoría	aplica	+ R1	+ R1	mp.sw.2	SI	SI	BÁSICA	
Categoría	aplica	aplica	aplica	mp.info.1	SI	SI (DNS)	BÁSICA	7.14
C	n.a.	aplica	aplica	mp.info.2	NO	NO	N/A	
I A	aplica	+ R1 + R2 + R3	+ R1 + R2 + R3 + R4	mp.info.3	NO	SI (PSC)	Alto	7.15
T	n.a.	n.a.	aplica	mp.info.4	NO	SI (PSC)	Alto	7.16
C	aplica	aplica	aplica	mp.info.5	SI	NO	Bajo	
D	aplica	+ R1	+ R1 + R2	mp.info.6	SI	SI	Alto	
Categoría	aplica	aplica	aplica	mp.s.1	SI	SI	BÁSICA	
Categoría	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3	mp.s.2	SI	SI	MEDIA	
Categoría	aplica	aplica	+ R1	mp.s.3	SI	SI	MEDIA	
D	n.a.	aplica	+ R1	mp.s.4	SI	SI* (DNS)	Alto	5.17

Detalles del criterio específico de aplicación de la medida en el apartado 7 de este documento.

Se considera que la medida, salvo excepciones, no será de aplicación al PCE-NIS2.

6.3 Medidas que son de aplicación

34. Aplican al presente PCE-NIS2 **72 de las 73 medidas de seguridad** definidas en el Anexo II del RD 311/2022.

35. Diecisiete (17) de dichas medidas de seguridad se adoptan de las requeridas para sistemas de categoría ALTA, otras treinta (30) para sistemas de categoría MEDIA y otras veinticinco (25) para sistemas de categoría BÁSICA.

36. Asimismo, algunas de dichas medidas de seguridad se han potenciado mediante determinados refuerzos, en otros casos se ha especificado cuales de ellas no serían de aplicación según se trate de entidades esenciales o importantes. También existen consideraciones para diecisiete (17) medidas, las cuales se han marcado con referencias de color azul al apartado 5 de este PCE-NIS2.

37. Se muestran a continuación aquellas medidas que no aplican de base en el PCE-NIS2, aunque podrían incorporarse para mitigar aquellos riesgos evaluados como inaceptables por una organización específica tras realizar el correspondiente análisis de riesgos:

    Medidas de Protección:

    [mp.info.2] Calificación de la Información

7. CRITERIOS DE APLICACIÓN DE MEDIDAS

7.1 [op.pl.1] Análisis de Riesgos

38. En el caso de las entidades Importantes se realizará un análisis de riesgos para categoría BASICA, mientras que las entidades esenciales requerirán el refuerzo R1 para categoría MEDIA consistente en un mayor nivel de formalismo en el análisis.

7.2 [op.pl.5] Componentes certificados

39. Además de adoptar los requisitos base del ENS para categorías MEDIA o ALTA (son equivalentes), centrados en el empleo de componentes certificados, se atenderá al refuerzo R1 que focaliza en evitar emanaciones comprometedoras, como son las emisiones electromagnéticas no intencionadas, producidas por equipos eléctricos y electrónicos que, detectadas y analizadas, puedan llevar a la obtención de información a un posible atacante por cauces no previstos.

40. Adicionalmente se atenderá al refuerzo R2 consistente en identificar los módulos, componentes software y librerías empleadas en las aplicaciones en producción, de modo que, ante una posible vulnerabilidad anunciada en alguno de ellos, se conozca su afectación a los sistemas de la organización. Dicha medida considera tanto los desarrollos propios, como los externalizados.

7.3 [op.acc.5] Mecanismo de autenticación (usuarios externos)

41. En el caso de las entidades Importantes no será necesario aplicar el refuerzo R3 sobre certificados.

7.4 [op.acc.6] *Mecanismo de autenticación (usuarios de la organización)*

42. En el caso de las entidades Importantes no será necesario aplicar el refuerzo R3 sobre certificados.

7.5 [op.exp.1] Inventario de activos

43. Además de adoptar los requisitos base del ENS para categorías BÁSICA, MEDIA o ALTA (puesto que son los mismos), consistentes en mantener el inventario de activos actualizado y completo, indicando para cada activo a su responsable (quién adopta decisiones relativas al mismo), se adoptará el refuerzo R1 consistente en incorporar al inventario referencia al etiquetado del equipamiento y del cableado vinculado.
44. Adicionalmente se atenderá al refuerzo R2 sobre identificación de activos mediante soluciones de autodescubrimiento y visualización del estado de los mismos.
45. Asimismo, se atenderá al refuerzo R3 que consiste en categorizar los activos críticos según el contexto de la organización y los riesgos de seguridad, con la ayuda de herramientas.
46. También el refuerzo R4, que ya se ha considerado en el refuerzo R2 de [op.pl.5] consistente en identificar los módulos, componentes software y librerías empleadas en las aplicaciones en producción, de modo que, ante una posible vulnerabilidad anunciada en alguno de ellos, se conozca su afectación a los sistemas de la organización. Dicha medida considera tanto los desarrollos propios, como los externalizados.
47. En el caso de las entidades importantes no será necesario que apliquen los refuerzos R1, R2 y R3.

7.6 [op.exp.4] Mantenimiento y actualizaciones de seguridad

48. Además del adoptar los requisitos base del ENS para categoría BÁSICA, consistentes en atender a las especificaciones de los fabricantes en lo relativo al mantenimiento de sistemas, disponiendo de un procedimiento al efecto para su actualización y aplicación de parches y determinando que el precitado mantenimiento únicamente será realzado por personal debidamente autorizado, se atenderá al refuerzo R4 relativo a monitorización continua.
49. Dicho refuerzo R4 determina desplegar una estrategia de monitorización de amenazas y vulnerabilidades, detallándose indicadores críticos de seguridad, la política de aplicación de parches a los componentes software de las aplicaciones,

así como los criterios de revisión (regular o excepcional) de las amenazas sobre el sistema.

7.7 [op.ext.3] Protección de la cadena de suministro

50. Además del adoptar los requisitos base del ENS para categoría ALTA, consistentes en incorporar los proveedores relevantes al análisis de riesgos y al BIA, se atenderá al refuerzo R1 consistente en considerar los proveedores externos críticos en el Plan de Continuidad y considerar en las pruebas del plan escenarios de indisponibilidad de un proveedor.
51. Asimismo, de considerará el refuerzo R2 consistente en implementar un sistema de protección de los procesos y flujos de información en las relaciones en línea (online) entre los distintos integrantes de la cadena de suministro.
52. También el refuerzo R3, que ya se ha considerado en el refuerzo R2 de [op.pl.5] y en el refuerzo R4 de [op.exp.1], consistente en identificar los módulos, componentes software y librerías empleadas en las aplicaciones en producción, de modo que, ante una posible vulnerabilidad anunciada en alguno de ellos, se conozca su afectación a los sistemas de la organización. Dicha medida considera tanto los desarrollos propios, como los externalizados, siempre que se empleen módulos, componentes y librerías de terceros.

7.8 [op.cont.2] Plan de continuidad

53. Además del adoptar los requisitos base del ENS para categoría ALTA, consistentes en desarrollará un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales y que tenga en cuenta responsabilidades, coordinación para la entrada en servicio de los medios alternativos, la formación de las personas respecto al plan y su integración armónica con otros planes de la organización, se considerará el refuerzo R1 que establece la necesidad de planes de recuperación específicos, o de contingencia, para diferentes escenarios del plan de continuidad, en consonancia con el BIA.
54. Asimismo, se considerará el refuerzo R2, consistente en verificar la integridad del sistema operativo, el firmware y los archivos de configuración, tras una caída del sistema y antes de reanudar el servicio.

7.9 [op.cont.4] Medios Alternativos

55. Además del adoptar los requisitos base del ENS para categoría ALTA, consistentes en prever la disponibilidad de medios alternativos para poder seguir prestando servicio cuando los medios habituales no estén disponibles en los ámbitos: servicios contratados a terceros, instalaciones alternativas, personal alternativo, equipamiento informático alternativo y medios de comunicación alternativos, establecer un tiempo máximo de transición y asegurar las mismas garantías de seguridad en los medios alternativos que en los principales, se atenderá al refuerzo R1.

56. Dicho refuerzo R1 consiste en automatizar la transición de los medios principales a los medios alterativos, siempre que sea posible (sean tecnológicos).

7.10 [op.mon.3] Vigilancia

57. Además del adoptar los requisitos base del ENS para categoría BÁSICA, consistentes en disponer de un sistema automático de recolección de eventos de seguridad, se atenderá al refuerzo R2 consistente en disponer de soluciones de vigilancia que permitan determinar la superficie de exposición con relación a vulnerabilidades y deficiencias de configuración, ya sean estas internas o externalizadas en un SOC en modalidad de contratación de servicios.
58. Asimismo, se considerará el refuerzo R6 consistente en que, periódicamente, o tras incidentes que hayan desvelado vulnerabilidades del sistema no tratadas, se realizarán verificaciones de configuración, análisis de vulnerabilidades y pruebas o test de penetración.
59. En el caso de las entidades Importantes no será necesario aplicar el refuerzo R6 sobre inspecciones de Seguridad.

7.11 [mp.per.1] Caracterización del puesto de trabajo

60. Además del adoptar los requisitos base del ENS para categorías MEDIA y ALTA (son equivalentes), consistentes en determinar las responsabilidades en materia de seguridad y definir los requisitos en materia de confidencialidad de las personas que vayan a ocupar el puesto, se atenderá el refuerzo R1.
61. Dicho refuerzo R1 consistirá en que los administradores de seguridad/sistema dispongan de la Habilitación Personal de Seguridad (HPS), necesaria en base al riesgo, o como requisito de seguridad para un sistema específico, siendo otorgada por la autoridad competente.
62. En el caso de las entidades importantes no será exigible que se realice el proceso de investigación de antecedentes.

7.12 [mp.eq.3] Protección de dispositivos portátiles

63. Además del adoptar los requisitos base del ENS para categoría MEDIA, consistentes en inventariar los dispositivos portátiles incluyendo la identificación de la persona responsable de cada uno de ellos, se realizará un control regular de dichos equipos, se dotará de un procedimiento operativo para informar al equipo de gestión de incidentes de su posible pérdida o sustracción, se controlará los servicios accesibles cuando el portátil se conecte remotamente y se evitará que el equipo contenga claves de acceso remoto a la organización, se atenderá al refuerzo R1.
64. Dicho refuerzo R1 consistirá en proteger el dispositivo portátil mediante cifrado del disco duro cuando el nivel de confidencialidad de la información almacenada en el mismo sea de nivel MEDIO o ALTO.

7.13 [mp.com.2] Protección de la confidencialidad

65. Además del adoptar los requisitos base del ENS para categoría ALTA, consistentes en emplear redes privadas virtuales (VPN) para que la comunicación discurra cifrada por redes externas al propio dominio de seguridad, se atenderá al refuerzo R4 consistente en el empleo de cifradores.
66. Asimismo, se considerará el refuerzo R5 consistente en cifrar toda la información transmitida por cualquier otro medio, además de las VPN.
67. Adicionalmente, se garantizarán comunicaciones de voz, vídeo y texto seguras, así como sistemas seguros de comunicaciones de emergencia en la entidad, cuando proceda.

7.14 [mp.info.1] Datos personales

68. Esta medida siempre será exigible, pero especialmente a los proveedores de servicios de DNS como evidencian informes de alguna Autoridad de Control. En relación a los servicios prestados por las entidades a interesados que residan en la UE siempre deben tenerse en consideración las disposiciones del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD) y demás normativa aplicable de protección de datos. Especial atención al art. 3 del RD 311/2022, de 3 de mayo, por el que se regula el ENS.

7.15 [mp.info.3] Firma electrónica

69. Será exigible especialmente a los Prestadores de servicios de confianza (PSC/TSP).

7.16 [mp.info.4] Sellos de tiempo

70. Será exigible especialmente a los Prestadores de servicios de confianza (PSC/TSP).

7.17 [mp.s.4] Protección frente a la denegación de servicio

71. Se aplicará para los Proveedores de Servicio de DNS el refuerzo R2 Ataques propios.

(espacio dejado en blanco exprofeso)

ANEXO I. MAPEO ENTRE LA DIRECTIVA NIS2 Y EL ENS

*Nota: Se dispone de la guía "**CCN-STIC 825 ENS - CERTIFICACIONES 27001**", así como de su anexo "**CCN-STIC 825 ENS - Anexo Independiente - Mapeo RD 311/2022 (ENS)- ISO 27001:2022**", las cuales permiten mapear a su vez la siguiente tabla entre NIS2 y ENS con el estándar internacional ISO/IEC 27001:2022.*

Requisito o planteamiento de la Directiva NIS2 y su transposición en España	Artículos del ENS (RD 311/222) y medidas relacionadas de su Anexo II
DIRECTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.o 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).	
Artículo 20 NIS2 sobre Gobernanza	
Art. 20.1 NIS2. Los Estados miembros velarán por que los órganos de dirección de las entidades esenciales e importantes aprueben las medidas para la gestión de riesgos de ciberseguridad adoptadas por dichas entidades para dar cumplimiento al artículo 21, supervisen su puesta en práctica y respondan por el incumplimiento por parte de las entidades de dicho artículo.	El **Artículo 13**. Organización e implantación del proceso de seguridad, señala: a) El responsable de la información determinará los requisitos de la información tratada b) El responsable del servicio determinará los requisitos de los servicios prestados. c) El responsable de la seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones. d) El responsable del sistema, por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad. Todos estos roles conforman el Comité de Seguridad de la Información, comité idóneo para aprobar las medidas para mitigar los riesgos evaluados como inaceptables en la gestión de riesgos de ciberseguridad de la organización. **Asimismo, existe vinculación con:** **Artículo 6**. La seguridad como un proceso integral. **Artículo 11**. Diferenciación de responsabilidades. **Artículo 12**. Política de seguridad y requisitos mínimos de seguridad. **[org.1]** Política de seguridad.
Art. 20.1 NIS2. Los Estados miembros garantizarán que los miembros de los órganos de dirección de las entidades esenciales e importantes deban asistir a formaciones y alentarán a estas entidades para que ofrezcan formaciones similares a sus empleados periódicamente al objeto de adquirir conocimientos y destrezas suficientes que les permitan detectar riesgos y evaluar las prácticas de gestión de riesgos de ciberseguridad y su repercusión en los servicios proporcionados por la entidad.	**[mp.per.4.1] Formación.** Se formará regularmente al personal en aquellas materias relativas a seguridad de la información que requiera el desempeño de sus funciones, en particular en lo relativo a: a) Configuración de sistemas. b) Detección y reacción ante incidentes. c) Gestión de la información en cualquier soporte en el que se encuentre. Se cubrirán al menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción. Además, se evaluará la eficacia de las acciones formativas llevadas a cabo. **[mp.per.3] Concienciación**. Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos. En particular, se recordará periódicamente: **[mp.per.3.1]** La normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales.

Requisito o planteamiento de la Directiva NIS2 y su transposición en España	Artículos del ENS (RD 311/222) y medidas relacionadas de su Anexo II
	[mp.per.3.2] La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado. **[mp.per.3.3]** El procedimiento para informar sobre incidentes de seguridad, sean reales o falsas alarmas.
Artículo 21 NIS2 sobre Medidas para la gestión de riesgos de ciberseguridad	
Artículo 21.1 NIS2. Los Estados miembros velarán por que las entidades esenciales e importantes tomen las medidas técnicas, operativas y de organización adecuadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de los sistemas de redes y de información que utilizan dichas entidades en sus operaciones o en la prestación de sus servicios y prevenir o minimizar las repercusiones de los incidentes en los destinatarios de sus servicios y en otros servicios. Teniendo en cuenta la situación y, en su caso, las normas europeas e internacionales pertinentes, así como el coste de su aplicación, las medidas a que se refiere el párrafo primero garantizarán un nivel de seguridad de los sistemas de redes y de información adecuado en relación con los riesgos planteados. Al evaluar la proporcionalidad de dichas 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, incluidas sus repercusiones sociales y económicas.	**Artículo 2. Ámbito de aplicación del ENS.** 1. El presente real decreto es de aplicación a todo el sector público, en los términos en que este se define por el artículo 2 de la Ley 40/2015, de 1 de octubre, y de acuerdo con lo previsto en el artículo 156.2 de la misma. 2. Asimismo, sin perjuicio de la aplicación de la Ley 9/1968, de 5 de abril, de Secretos Oficiales y otra normativa especial, este real decreto será de aplicación a los sistemas que tratan información clasificada, pudiendo resultar necesario adoptar medidas complementarias de seguridad, específicas para dichos sistemas, derivadas de los compromisos internacionales contraídos por España o de su pertenencia a organismos o foros internacionales. 3. Este real decreto también se aplica a los sistemas de información de las entidades del sector privado, incluida la obligación de contar con la política de seguridad a que se refiere el artículo 12, cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.
Artículo 21.2 NIS2. Las medidas a que se hace referencia en el apartado 1 se fundamentarán en un enfoque basado en todos los peligros que tenga por objeto proteger los sistemas de redes y de información y el entorno físico de dichos sistemas frente a incidentes, e incluirán al menos los siguientes elementos:	Las medidas se concretan en los apartados que siguen…
Artículo 21.2 a) Las políticas de seguridad de los sistemas de información y análisis de riesgos. Considerando 79 Las medidas para la gestión de riesgos de ciberseguridad también deben abordar la seguridad física y del entorno de los sistemas de redes y de información, mediante la introducción de medidas para proteger dichos sistemas de redes y de información frente a fallos del sistema, errores humanos, actos malintencionados o fenómenos naturales, de conformidad con las normas europeas o internacionales	**Políticas de seguridad (PSI y normativa interna) en el ENS** **[org.1] Política de Seguridad:** La política de seguridad, que se aprobará de conformidad con lo dispuesto en el artículo 12 de este real decreto, se plasmará en un documento en el que, de forma clara, se precise, al menos, lo siguiente: **[org.1.1]** Los objetivos o misión de la organización. **[org.1.2]** El marco legal y regulatorio en el que se desarrollarán las actividades. **[org.1.3]** Los roles o funciones de seguridad, definiendo para cada uno los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación. **[org.1.4]** La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, las personas integrantes y la relación con otros elementos de la organización. **[org.1.5]** Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso. **[org.2] Normativa de seguridad:** Se dispondrá de una serie de documentos que describan:

Requisito o planteamiento de la Directiva NIS2 y su transposición en España	Artículos del ENS (RD 311/222) y medidas relacionadas de su Anexo II
	[org.2.1] El uso correcto de equipos, servicios e instalaciones, así como lo que se considerará uso indebido. **[org.2.2]** La responsabilidad del personal con respecto al cumplimiento o violación de la normativa: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente. **[org.2.r1.1] Refuerzo opcional R1-Documentos específicos.** Se dispondrá de una documentación de seguridad, desarrollada según lo reflejado en las guías CCN-STIC que resulten de aplicación. **[op.pl.1]** Análisis de riesgos. **Refuerzo R1-Análisis de riesgos semiformal** **Arquitectura de seguridad** **Refuerzo R1 – Sistema de gestión** **[op.pl.2.r1.1]** Sistema de gestión, relativo a la planificación, organización y control de los recursos relativos a la seguridad de la información. **Protección de las instalaciones e infraestructuras [mp.if]** **[mp.if.1]** Áreas separadas y con control de acceso **[mp.if.2]** Identificación de las personas **[mp.if.3]** Acondicionamiento de los locales **[mp.if.4]** Energía eléctrica **[mp.if.5]** Protección frente a incendios **[mp.if.6]** Protección frente a inundaciones **[mp.if.7]** Registro de entrada y salida de equipamiento
Artículo 21.2 b) La gestión de incidentes.	**[op.exp.7.1]** Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, que incluya el informe de eventos de seguridad y debilidades, detallando los criterios de clasificación y el escalado de la notificación. **[op.exp.7.2]** La gestión de incidentes que afecten a datos personales tendrá en cuenta lo dispuesto en el Reglamento General de Protección de Datos; la Ley Orgánica 3/2018, de 5 de diciembre, en especial su disposición adicional primera, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en este real decreto. **Refuerzo R1-Notificación.** **[op.exp.7.r1.1]** Se dispondrá de soluciones de ventanilla única para la notificación de incidentes al CCN-CERT, que permita la distribución de notificaciones a las diferentes entidades de manera federada, utilizando para ello dependencias administrativas jerárquicas. **Refuerzo R2 –Detección y Respuesta.** El proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema ([op.exp.7.1]) deberá incluir: **[op.exp.7.r2.1]** Implantación de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso. **[op.exp.7.r2.2]** Asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente. **[op.exp.7.r2.3]** Informar del incidente a los responsables de la información y servicios afectados y de las actuaciones llevadas a cabo para su resolución. **[op.exp.7.r2.4]** Medidas para:

Requisito o planteamiento de la Directiva NIS2 y su transposición en España	Artículos del ENS (RD 311/222) y medidas relacionadas de su Anexo II
	a) Prevenir que se repita el incidente. b) Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente. c) Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes. **Refuerzo R3-Reconfiguración dinámica.** La reconfiguración dinámica del sistema persigue detener, desviar o limitar ataques, acotando los daños. **[op.exp.7.r3.1]** La reconfiguración dinámica incluye, por ejemplo, cambios en las reglas de los enrutadores (routers), listas de control de acceso, parámetros del sistema de detección / prevención de intrusiones y reglas en los cortafuegos y puertas de enlace, aislamiento de elementos críticos y aislamiento de las copias de seguridad. **[op.exp.7.r3.2]** El organismo adaptará los procedimientos de reconfiguración dinámica reaccionando a los anuncios recibidos del CCN-CERT relativos a ciberamenazas sofisticadas y campañas de ataques. **[op.exp.9] Registro de la gestión de incidentes** **[op.mon.1] Detección de intrusión** **[op.mon3] Vigilancia** **Asimismo, se encuentra vinculación con:** **Artículo 24**. Registro de actividad y detección de código dañino **Artículo 25**. Incidentes de seguridad **Artículo 33**. Capacidad de respuesta a incidentes de seguridad **Artículo 34**. Prestación de servicios de respuesta a incidentes de seguridad de entidades del sector público
Artículo 21.2 c) La continuidad de las actividades, como la gestión de copias de seguridad y la recuperación en caso de catástrofe, y la gestión de crisis.	**Continuidad de los servicios:** **[op.cont.1.1]** Se realizará un análisis de impacto que permita determinar los requisitos de disponibilidad de cada servicio (impacto de una interrupción durante un periodo de tiempo determinado), así como los elementos que son críticos para la prestación de cada servicio. Se desarrollará un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales. Dicho plan contemplará los siguientes aspectos: **[op.cont.2.1]** Se identificarán funciones, responsabilidades y actividades a realizar. **[op.cont.2.2]** Existirá una previsión para coordinar la entrada en servicio de los medios alternativos de forma que se garantice poder seguir prestando los servicios esenciales de la organización. **[op.cont.2.3]** Todos los medios alternativos estarán planificados y materializados en acuerdos o contratos con los proveedores correspondientes. **[op.cont.2.4]** Las personas afectadas por el plan recibirán formación específica relativa a su papel en dicho plan. **[op.cont.2.5]** El plan de continuidad será parte integral y armónica de los planes de continuidad de la organización en otras materias ajenas a la seguridad. **Refuerzo R1-Plan de emergencia y contingencia.** **[op.cont.2.r1.1]** Cuando se determine la necesidad de continuidad de los sistemas, deberá existir un plan de emergencia y contingencia en consonancia. En función del análisis de Impacto, se determinarán los aspectos a cubrir. **Refuerzo R2-Comprobación de integridad.** **[op.cont.2.r2.1]** Ante una caída o discontinuidad del sistema, se deberá comprobar la integridad del sistema operativo, del firmware y de los ficheros de configuración.

Requisito o planteamiento de la Directiva NIS2 y su transposición en España	Artículos del ENS (RD 311/222) y medidas relacionadas de su Anexo II
	[op.cont.3.1] Se realizarán pruebas periódicas para localizar y, en su caso, corregir los errores o deficiencias que puedan existir en el plan de continuidad. **[op.cont.4.1]** Estará prevista la disponibilidad de medios alternativos para poder seguir prestando servicio cuando los medios habituales no estén disponibles. En concreto, se cubrirán los siguientes elementos del sistema: a) Servicios contratados a terceros. b) Instalaciones alternativas. c) Personal alternativo. d) Equipamiento informático alternativo. e) Medios de comunicación alternativos. **[op.cont.4.2]** Se establecerá un tiempo máximo para que los medios alternativos entren en funcionamiento. **[op.cont.4.3]** Los medios alternativos estarán sometidos a las mismas garantías de seguridad que los originales. **Refuerzo R1-Automatización de la transición a medios alternativos.** **[op.cont.4.r1.1]** El sistema dispondrá de elementos hardware o software que permitan la transferencia de los servicios automáticamente a los medios alternativos. **Dimensionamiento / Gestión de la Capacidad:** Con carácter previo a la puesta en explotación, se realizará un estudio que cubrirá los siguientes aspectos: **[op.pl.4.1]** Necesidades de procesamiento. **[op.pl.4.2]** Necesidades de almacenamiento de información: durante su procesamiento y durante el periodo que deba retenerse. **[op.pl.4.3]** Necesidades de comunicación. **[op.pl.4.4]** Necesidades de personal: cantidad y cualificación profesional. **[op.pl.4.5]** Necesidades de instalaciones y medios auxiliares. **Copias de seguridad:** **[mp.info.6.1]** Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente. La periodicidad y los plazos de retención de estas copias de seguridad se determinarán en la normativa interna de la organización relativa a copias de seguridad. **[mp.info.6.2]** Los procedimientos de respaldo establecidos indicarán: a) Frecuencia de las copias. b) Requisitos de almacenamiento en el propio lugar. c) Requisitos de almacenamiento en otros lugares. d) Controles para el acceso autorizado a las copias de respaldo. **Refuerzo R1-Pruebas de recuperación.** **[mp.info.6.r1.1]** Los procedimientos de copia de seguridad y restauración deben probarse regularmente. Su frecuencia dependerá de la criticidad de los datos y del impacto que cause la falta de disponibilidad. **Refuerzo R2-Protección de las copias de seguridad.** **mp.info.6.r2.1]** Al menos, una de las copias de seguridad se almacenará de forma separada en lugar diferente, de tal manera que un incidente no pueda afectar tanto al repositorio original como a la copia simultáneamente.
Artículo 21.2 d) 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.	**Servicios externos (cadena de suministro):** **[op.ext.1.1]** Con anterioridad a la efectiva utilización de los recursos externos se establecerá contractualmente un Acuerdo de Nivel de Servicio, que incluirá las características del servicio prestado, lo que debe entenderse como «servicio mínimo admisible», así como, la responsabilidad del prestador y las consecuencias de eventuales incumplimientos.

Requisito o planteamiento de la Directiva NIS2 y su transposición en España	Artículos del ENS (RD 311/222) y medidas relacionadas de su Anexo II
	[op.ext.2.1] Un sistema rutinario para medir el cumplimiento de las obligaciones de servicio, incluyendo el procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado ([op.ext.1]). **[op.ext.2.2]** El mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas comprendidos en el acuerdo, que contemplarán los supuestos de incidentes y desastres. **[op.ext.3.1]** Se analizará el impacto que puede tener sobre el sistema un incidente accidental o deliberado que tenga su origen en la cadena de suministro. **[op.ext.3.2]** Se estimará el riesgo sobre el sistema por causa del impacto estimado en el punto anterior. **[op.ext.3.3**] Se tomarán medidas de contención de los impactos estimados en los puntos anteriores. **[op.ext.3.r1.1]** Refuerzo R1-Plan de contingencia. El plan de continuidad de la organización deberá tener en cuenta la dependencia de proveedores externos críticos. **[op.ext.3.r1.2] Refuerzo R1-Plan de contingencia.** Se deberán realizar pruebas o ejercicios de continuidad, incluyendo escenarios en los que falla un proveedor. **[op.ext.3.r2.1] Refuerzo R2-Sistema de gestión de la seguridad.** Se implementará un sistema de protección de los procesos y flujos de información en las relaciones en línea (online) entre los distintos integrantes de la cadena de suministro. [**op.ext.3.r3.1] Refuerzo R3-Lista de componentes software.** Se mantendrá actualizado un registro formal que contenga los detalles y las relaciones de la cadena de suministro de los diversos componentes utilizados en la construcción de programas informáticos, acorde a lo especificado en [mp.sw.1.r5]. Esta lista será proporcionada por el proveedor de la aplicación, librería o producto suministrado. **[op.ext.4.1]** Todos los intercambios de información y prestación de servicios con otros sistemas deberán ser objeto de una autorización previa. Todo flujo de información estará prohibido salvo autorización expresa. **[op.ext.4.2]** Para cada interconexión se documentará explícitamente: las características de la interfaz, los requisitos de seguridad y protección de datos y la naturaleza de la información intercambiada. **Refuerzo R1-Coordinación de actividades.** **[op.ext.4.r1.1]** Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, las medidas de seguridad locales se acompañarán de los correspondientes mecanismos y procedimientos de coordinación para la atribución y ejercicio efectivos de las responsabilidades de cada sistema. **Protección de servicios en la Nube (Quién utilice dichos servicios):** **[op.nub.1.1]** Los sistemas que suministran un servicio en la nube a organismos del sector público deberán cumplir con el conjunto de medidas de seguridad en función del modelo de servicio en la nube que presten: Software como Servicio (Software as a Service, SaaS), Plataforma como Servicio (Platform as a Service, PaaS) e Infraestructura como Servicio (Infrastructure as a Service, IaaS) definidas en las guías CCN-STIC que sean de aplicación. **[op.nub.1.2]** Cuando se utilicen servicios en la nube suministrados por terceros, los sistemas de información que los soportan deberán ser conformes con el ENS o cumplir con las medidas desarrolladas en una guía CCN-STIC que incluirá, entre otros, requisitos relativos a: a) Auditoría de pruebas de penetración (pentesting). b) Transparencia. c) Cifrado y gestión de claves. d) Jurisdicción de los datos. **Refuerzo R1- Servicios certificados.** **[op.nub.1.r1.1]** Cuando se utilicen servicios en la nube suministrados por terceros, estos deberán estar certificados bajo una metodología de certificación reconocida por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información.

Requisito o planteamiento de la Directiva NIS2 y su transposición en España	Artículos del ENS (RD 311/222) y medidas relacionadas de su Anexo II
	[op.nub.1.r1.2] Si el servicio en la nube es un servicio de seguridad deberá cumplir con los requisitos establecidos en [op.pl.5]. **Refuerzo R2-Guías de Configuración de Seguridad Específicas.** **[op.nub.1.r2.1]** La configuración de seguridad de los sistemas que proporcionan estos servicios deberá realizarse según la correspondiente guía CCN-STIC de Configuración de Seguridad Específica, orientadas tanto al usuario como al proveedor.
Artículo 21.2 e) La seguridad en la adquisición, el desarrollo y el mantenimiento de sistemas de redes y de información, incluida la gestión y divulgación de las vulnerabilidades.	**Adquisición de nuevos componentes:** Se establecerá un proceso formal para planificar la adquisición de nuevos componentes del sistema, proceso que: **[op.pl.3.1]** Atenderá a las conclusiones del análisis de riesgos ([op.pl.1]). **[op.pl.3.2]** Será acorde a la arquitectura de seguridad escogida ([op.pl.2]). **[op.pl.3.3]** Contemplará las necesidades técnicas, de formación y de financiación, de forma conjunta. **Componentes certificados:** **[op.pl.5.1].** Se utilizará el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del CCN, para seleccionar los productos o servicios suministrados por un tercero que formen parte de la arquitectura de seguridad del sistema y aquellos que se referencien expresamente en las medidas de este real decreto. En caso de que no existan productos o servicios en el CPSTIC que implementen las funcionalidades requeridas, se utilizarán productos certificados de acuerdo a lo descrito en el artículo 19. Una Instrucción Técnica de Seguridad detallará los criterios relativos a la adquisición de productos de seguridad. **[op.pl.5.2]** Si el sistema suministra un servicio de seguridad a un tercero bajo el alcance del ENS, el producto o productos que en los que se sustente dicho servicio debe superar un proceso de cualificación y ser incluido en el CPSTIC, o aportar una certificación que cumpla con los requisitos funcionales de seguridad y de aseguramiento de acuerdo a lo establecido en el artículo 19. **Refuerzo opcional R1-Protección de emisiones electromagnéticas.** **[op.pl.5.r1.1]** La información deberá ser protegida frente a las amenazas TEMPEST de acuerdo con la normativa en vigor. **Refuerzo opcional R2 - Lista de componentes software.** **[op.pl.5.r2.1]** Cada producto y servicio incluirá en su descripción una lista de componentes software, acorde a lo especificado en [mp.sw.1.r5]. **Mantenimiento y actualizaciones de seguridad:** Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente: **[op.exp.4.1]** Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas, lo que incluirá un seguimiento continuo de los anuncios de defectos. **[op.exp.4.2]** Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la implantación o no de la actualización. **[op.exp.4.3]** El mantenimiento solo podrá realizarse por personal debidamente autorizado. **Refuerzo R4 - Monitorización continua.** **[op.exp.4.r4.1]** Se desplegará a nivel de sistema una estrategia de monitorización continua de amenazas y vulnerabilidades. Esta estrategia detallará: 1. Los indicadores críticos de seguridad a emplear. 2. La política de aplicación de parches de seguridad de los componentes software relacionados en las listas de [op.exp.1.r4], [op.ext.3.r3] y [mp.sw.1.r5]). 3. Los criterios de revisión regular y excepcional de las amenazas sobre el sistema.

Requisito o planteamiento de la Directiva NIS2 y su transposición en España	Artículos del ENS (RD 311/222) y medidas relacionadas de su Anexo II
	Asimismo, existe vinculación con: **[op.exp.2]** Configuración de seguridad **[op.exp.3]** Gestión de la configuración de seguridad **[op.exp.5]** Gestión de cambios **[op.exp.6]** Protección frente a código dañino. ***[mp.sw.1]Desarrollo de aplicaciones*** **[mp.sw.1.1]** El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción, ni datos de producción en el de desarrollo. **Refuerzo R1-Mínimo privilegio.** [mp.sw.1.r1.1] Las aplicaciones se desarrollarán respetando el principio de mínimo privilegio, accediendo únicamente a los recursos imprescindibles para su función, y con los privilegios que sean indispensables. **Refuerzo R2-Metodología de desarrollo seguro.** [mp.sw.1.r2.1] Se aplicará una metodología de desarrollo seguro reconocida que: a) Tendrá en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida. b) Incluirá normas de programación segura, especialmente: control de asignación y liberación de memoria, desbordamiento de memoria (overflow). c) Tratará específicamente los datos usados en pruebas. d) Permitirá la inspección del código fuente. **Refuerzo R3-Seguridad desde el diseño.** [mp.sw.1.r3.1] Los siguientes elementos serán parte integral del diseño del sistema: a) Los mecanismos de identificación y autenticación b) Los mecanismos de protección de la información tratada. c) La generación y tratamiento de pistas de auditoría. **Refuerzo R4-Datos de pruebas.** **[mp.sw.1.r4.1]** Preferiblemente, las pruebas previas a la implantación o modificación de los sistemas de información no se realizarán con datos reales. En caso de que fuese necesario recurrir a datos reales se garantizará el nivel de seguridad correspondiente. **[mp.sw.2] Aceptación y puesta en servicio** Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación. **[mp.sw.2.1]** Se comprobará que: a) Se cumplen los criterios de aceptación en materia de seguridad. b) No se deteriora la seguridad de otros componentes del servicio.

Requisito o planteamiento de la Directiva NIS2 y su transposición en España	Artículos del ENS (RD 311/222) y medidas relacionadas de su Anexo II
	Refuerzo R1- Pruebas. **[mp.sw.2.r1.1]** Las pruebas se realizarán en un entorno aislado (preproducción). **Refuerzo R2-Inspección de código fuente.** **[mp.sw.2.r2.1]** Se realizará una auditoría de código fuente.
Artículo 21.2 f) Las políticas y los procedimientos para evaluar la eficacia de las medidas para la gestión de riesgos de ciberseguridad.	**Artículo 31. Auditoría de la seguridad.** 1. Los sistemas de información comprendidos en el ámbito de aplicación de este real decreto serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del ENS. Con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales en los sistemas de información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoria extraordinaria determinará la fecha de cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría regular ordinaria, indicados en el párrafo anterior. **Disposición adicional segunda. Desarrollo del Esquema Nacional de Seguridad.** Para el mejor cumplimiento de lo establecido en este real decreto, el CCN, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC), particularmente de la serie 800, que se incorporarán al conjunto documental utilizado para la realización de las auditorías de seguridad. **Anexo III. Auditoría de la seguridad** **1. Objeto de la auditoría** 1.1 La seguridad de los sistemas de información de una organización será auditada en los siguientes términos, al objeto de constatar: a) Que la política de seguridad define los roles y funciones de los responsables del sistema, la información, los servicios y la seguridad del sistema de información. b) Que existen procedimientos para resolución de conflictos entre dichos responsables. c) Que se han designado personas para dichos roles a la luz del principio de «diferenciación de responsabilidades». d) Que se ha realizado un análisis de riesgos, con revisión y aprobación anual. e) Que se cumplen las recomendaciones de protección descritas en el anexo II, sobre Medidas de Seguridad, en función de las condiciones de aplicación en cada caso. f) f) Que existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección, tomando como base la Declaración de Aplicabilidad regulada en el artículo 28 de este real decreto. **[org.3] Procedimientos de seguridad** Se dispondrá de una serie de documentos que detallen de forma clara y precisa cómo operar los elementos del sistema de información: a) [org.3.1] Cómo llevar a cabo las tareas habituales. b) [org.3.2] Quién debe hacer cada tarea. c) [org.3.3] Cómo identificar y reportar comportamientos anómalos. d) [org.3.4.] La forma en que se ha de tratar la información en consideración al nivel de seguridad que requiere, precisando cómo efectuar: a) Su control de acceso.

Requisito o planteamiento de la Directiva NIS2 y su transposición en España	Artículos del ENS (RD 311/222) y medidas relacionadas de su Anexo II
	b) Su almacenamiento. c) La realización de copias. d) El etiquetado de soportes. e) Su transmisión telemática. f) Cualquier otra actividad relacionada con dicha información. **Refuerzo R1-Validación de procedimientos**. [**org.3.r1.1]** Se requerirá la validación de los procedimientos de seguridad por la autoridad correspondiente. **[op.mon.2] Sistema de métricas**
Artículo 21.2 g) Las prácticas básicas de ciber-higiene y formación en ciberseguridad.	**[mp.per.4.1] Formación.** Se formará regularmente al personal en aquellas materias relativas a seguridad de la información que requiera el desempeño de sus funciones, en particular en lo relativo a: d) Configuración de sistemas. e) Detección y reacción ante incidentes. f) Gestión de la información en cualquier soporte en el que se encuentre. Se cubrirán al menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción. Además, se evaluará la eficacia de las acciones formativas llevadas a cabo. **[mp.per.3] Concienciación**. Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos. En particular, se recordará periódicamente: **[mp.per.3.1]** La normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales. **[mp.per.3.2]** La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado. **[mp.per.3.3]** El procedimiento para informar sobre incidentes de seguridad, sean reales o falsas alarmas.
Artículo 21.2 h) Las políticas y procedimientos relativos a la utilización de criptografía y, en su caso, de cifrado.	**Protección de las claves criptográficas:** **[op.exp.10.1]** Las claves criptográficas se protegerán durante todo su ciclo de vida: (1) generación, (2) transporte al punto de explotación, (3) custodia durante la explotación, (4) archivo posterior a su retirada de explotación activa y (5) destrucción final. **[op.exp.10.2]** Los medios de generación estarán aislados de los medios de explotación. **[op.exp.10.3]** Las claves retiradas de operación que deban ser archivadas, lo serán en medios aislados de los de explotación. **Protección de los soportes de información:** Esta medida se aplica, en particular, a todos los dispositivos removibles cuando salen de un área controlada. Se entenderán por dispositivos removibles, los CD, DVD, discos extraíbles, pendrives, memorias USB u otros de naturaleza análoga. **[mp.si.2.1]** Se usarán mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida. **[mp.si.2.2]** Se emplearán algoritmos y parámetros autorizados por el CCN. **Refuerzo R1– Productos certificados.** **[mp.si.2.r1.1]** Se emplearán productos certificados conforme a lo establecido en [op.pl.5]. **Refuerzo R2-Copias de seguridad.** **[mp.si.2.r2.1]** Las copias se seguridad se cifrarán utilizando algoritmos y parámetros autorizados por el CCN. **Protección de los equipos portátiles:** **Refuerzo R1– Cifrado del disco.**

Requisito o planteamiento de la Directiva NIS2 y su transposición en España	Artículos del ENS (RD 311/222) y medidas relacionadas de su Anexo II
	– **[mp.eq.3.r1.1]** Se protegerá el dispositivo portátil mediante cifrado del disco duro cuando el nivel de confidencialidad de la información almacenada en el mismo sea de nivel MEDIO. **Protección de las comunicaciones:** **[mp.com.2.1]** Se emplearán redes privadas virtuales cifradas cuando la comunicación discurra por redes fuera del propio dominio de seguridad. **Refuerzo R1-Algoritmos y parámetros autorizados.** **[mp.com.2.r1.1]** Se emplearán algoritmos y parámetros autorizados por el CCN. **Refuerzo R2-Dispositivos hardware.** **[mp.com.2.r2.1]** Se emplearán, dispositivos hardware en el establecimiento y utilización de la red privada virtual. **Refuerzo R3-Productos certificados.** **[mp.com.2.r3.1]** Se usarán productos o servicios que cumplan lo establecido en [op.pl.5]. **Refuerzo R4-Cifradores.** **[mp.com.2.r4.1]** Se emplearán cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación. **Refuerzo R5-Cifrado de información especialmente sensible.** **[mp.com.2.r5.1]** Se cifrará toda la información transmitida. **Asimismo, existe vinculación con:** **[mp.info.3]** Firma electrónica **[mp.info.4]** Sellos de tiempo
Artículo 21.2 i) La seguridad de los recursos humanos, las políticas de control de acceso y la gestión de activos.	**Gestión del personal (Caracterización del puesto de trabajo):** **[mp.per.1.1]** Para cada puesto de trabajo, relacionado directamente con el manejo de información o servicios, se definirán las responsabilidades en materia de seguridad, que estarán basadas en el análisis de riesgos. **[mp.per.1.2]** Se definirán los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular, en términos de confidencialidad. Dichos requisitos se tendrán en cuenta en la selección de la persona que vaya a ocupar el puesto, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias, de conformidad con el ordenamiento jurídico y el respeto a los derechos fundamentales. **Refuerzo R1-Habilitación Personal de Seguridad.** **[mp.per.1.r1.1]** Los administradores de seguridad/sistema tendrán una Habilitación Personal de Seguridad (HPS) otorgada por la autoridad competente, como consecuencia de los resultados del análisis de riesgos previo o como requisito de seguridad de un sistema específico. **Deberes y Obligaciones:** Se informará a cada persona que trabaje en el sistema de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad, contemplando: **[mp.per.2.1]** Las medidas disciplinarias a que haya lugar. **[mp.per.2.2]** Contemplando tanto el periodo durante el cual se desempeña el puesto, como las obligaciones en caso de término de la asignación, o traslado a otro puesto de trabajo. **[mp.per.2.3]** El deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que esté adscrito al puesto de trabajo, como posteriormente a su terminación. **[mp.per.2.4]** En caso de personal contratado a través de un tercero:

Requisito o planteamiento de la Directiva NIS2 y su transposición en España	Artículos del ENS (RD 311/222) y medidas relacionadas de su Anexo II
	• [mp.per.2.4.1] Se establecerán los deberes y obligaciones de cada parte y del personal contratado. • [mp.per.2.4.2] Se establecerá el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones. **Refuerzo R1-Confirmación expresa.** **[mp.per.2.r1.1]** Se ha de obtener la confirmación expresa de que los usuarios conocen las instrucciones de seguridad necesarias y obligatorias y su aceptación, así como los procedimientos necesarios para llevarlas a cabo de manera adecuada. **Proceso de autorización:** Se establecerá un proceso formal de autorizaciones que cubra todos los elementos del sistema de información: **[org.4.1]** Utilización de instalaciones, habituales y alternativas. **[org.4.2]** Entrada de equipos en producción, en particular, equipos que involucren criptografía. **[org.4.3]** Entrada de aplicaciones en producción. **[org.4.4]** Establecimiento de enlaces de comunicaciones con otros sistemas. **[org.4.5]** Utilización de medios de comunicación, habituales y alternativos. **[org.4.6]** Utilización de soportes de información. **[org.4.7]** Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, tabletas, teléfonos móviles u otros de naturaleza análoga. **[org.4.8]** Utilización de servicios de terceros, bajo contrato o convenio, concesión, encargo, etc. **Control de acceso:** • **[op.acc.1]** Identificación • **[op.acc.2]** Requisitos de acceso • **[op.acc.3]** Segregación de funciones y tareas • **[op.acc.4]** Proceso de gestión de derechos de acceso • **[op.acc.5]** Mecanismo de autenticación (usuarios externos) • **[op.acc.6]** Mecanismo de autenticación (usuarios de la organización) **Inventario de activos:** **[op.exp.1.1]** Se mantendrá un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su responsable; es decir, la persona que toma las decisiones relativas al mismo. **Refuerzo R1-Inventario de etiquetado.** **[op.exp.1.r1.1]** El etiquetado del equipamiento y del cableado formará parte del inventario. **Refuerzo R2-Identificación periódica de activos.** **[op.exp.1.r2.1]** Se dispondrá de herramientas que permitan visualizar de forma continua el estado de todos los equipos en la red, en particular, los servidores y los dispositivos de red y de comunicaciones. **Refuerzo R3-Identificación de activos críticos.** **[op.exp.1.r3.1]** Se dispondrá de herramientas que permitan categorizar los activos críticos por contexto de la organización y riesgos de seguridad. **Refuerzo R4-Lista de componentes software.**

Requisito o planteamiento de la Directiva NIS2 y su transposición en España	Artículos del ENS (RD 311/222) y medidas relacionadas de su Anexo II
	[op.exp.1.r4.1] Se mantendrá actualizada una relación formal de los componentes software de terceros empleados en el despliegue del sistema. Esta lista incluirá librerías software y los servicios requeridos para su despliegue (plataforma o entorno operacional). El contenido de la lista de componentes será equivalente a lo requerido en [mp.sw.1.r5]. **Arquitectura de seguridad:** La seguridad del sistema será objeto de un planteamiento integral detallando, al menos, los siguientes aspectos: [**op.pl.2.1]** Documentación de las instalaciones, incluyendo áreas y puntos de acceso. **[op.pl.2.2]** Documentación del sistema, incluyendo equipos, redes internas y conexiones al exterior, y puntos de acceso al sistema (puestos de trabajo y consolas de administración). **[op.pl.2.3]** Esquema de líneas de defensa, incluyendo puntos de interconexión a otros sistemas o a otras redes (en especial, si se trata de internet o redes públicas en general); cortafuegos, DMZ, etc.; y la utilización de tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa. **[op.pl.2.4]** Sistema de identificación y autenticación de usuarios, incluyendo el uso de claves concertadas, contraseñas, tarjetas de identificación, biometría, u otras de naturaleza análoga, y el uso de ficheros o directorios para autenticar al usuario y determinar sus derechos de acceso. **Asimismo, existe vinculación con:** **[op.exp.8]** Registro de la actividad **[op.mon.3]** Vigilancia **[mp.eq.1]** Puesto de trabajo despejado **[mp.eq.2]** Bloqueo de puesto de trabajo **[mp.eq.3]** Otros dispositivos conectados a la red **[mp.s.3]** Protección de la navegación web **[mp.info.5]** Limpieza de documentos **[mp.info.1]** Datos personales
Artículo 21.2 j) El uso de soluciones de autenticación multifactorial o de autenticación continua, comunicaciones de voz, vídeo y texto seguras y sistemas seguros de comunicaciones de emergencia en la entidad, cuando proceda.	**Autenticación multifactorial (MFA):** **Refuerzo R8-Doble factor para acceso desde o a través de zonas no controladas.** Se denomina «zona controlada» aquella que no es de acceso público, requiriéndose que el usuario, antes de tener acceso al equipo, se haya autenticado previamente de alguna forma (control de acceso a las instalaciones), diferente del mecanismo de autenticación lógica frente al sistema. Un ejemplo de zona no controlada es Internet. **[op.acc.6.r8.1]** Para el acceso desde o a través de zonas no controladas se requerirá un doble factor de autenticación: R2, R3 o R4. **Refuerzo R2-Contraseña + otro factor de autenticación.** **[op.acc.6.r2.1]** Se requerirá un segundo factor tal como «algo que se tiene», es decir, un dispositivo, una contraseña de un solo uso (OTP, en inglés) como complemento a la contraseña de usuario, o «algo que se es». **Refuerzo R3-Certificados.** **[op.acc.6.r3.1]** Se emplearán certificados cualificados como mecanismo de autenticación. [op.acc.6.r3.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico. **Refuerzo R4-Certificados en dispositivo físico.** **[op.acc.6.r4.1]** Se emplearán certificados cualificados como mecanismo de autenticación, en soporte físico (tarjeta o similar) usando algoritmos, parámetros y dispositivos autorizados por el CCN. [op.acc.6.r4.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

Requisito o planteamiento de la Directiva NIS2 y su transposición en España	Artículos del ENS (RD 311/222) y medidas relacionadas de su Anexo II
	Asimismo, existe vinculación con: **[mp.com.1]** Perímetro seguro **[mp.com.2]** Protección de la confidencialidad **[mp.com.3]** Protección de la integridad y de la autenticidad **[mp.com.4]** Separación de flujos de información en la red **[mp.s.1]** Protección del correo electrónico **[mp.s.2]** Protección de servicios y aplicaciones web **[mp.s.4]** Protección frente a denegación de servicio

ANEXO II. SECTORES DE ATA CRITICIDAD Y OTROS SECTORES CRÍTICOS

Se reproducen a continuación los Anexos I y II de la DIRECTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (NIS2):

REGLAMENTO DELEGADO (UE) …/... DE LA COMISIÓN de 25.7.2023 por el que se completa la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo estableciendo una lista de servicios esenciales		
Sector de la energía:	Subsector de la electricidad:	i suministro de electricidad (empresas eléctricas); ii explotación, mantenimiento y desarrollo de una red de distribución de electricidad (gestores de redes de distribución); iii explotación, mantenimiento y desarrollo de una red de transporte de electricidad (gestores de redes de transporte); iv generación de electricidad (productores); v servicios de los operadores designados para el mercado de la electricidad (operadores designados para el mercado de la electricidad); vi respuesta de demanda (participantes en el mercado de la electricidad); vii agregación de la electricidad (participantes en el mercado de la electricidad); viii almacenamiento de energía (participantes en el mercado de la electricidad);
	Subsector «sistemas urbanos de calefacción y refrigeración»: suministro de calefacción o refrigeración urbanas (operadores de sistemas urbanos de calefacción o refrigeración);	
	subsector del petróleo:	i transporte de petróleo (operadores de oleoductos de transporte de petróleo); ii producción de petróleo (operadores de producción de petróleo); iii refinado y tratamiento de petróleo (operadores de instalaciones de refinado y tratamiento de petróleo); iv almacenamiento de petróleo (operadores de almacenamiento de petróleo); v gestión de las reservas de petróleo, incluidas las reservas de emergencia y las reservas específicas de petróleo (entidades centrales de almacenamiento);

	Subsector del gas:	i suministro de gas (empresa suministradora); ii distribución de gas (gestores de la red de distribución); iii transporte de gas (gestores de la red de transporte); iv almacenamiento de gas (gestores del sistema de almacenamiento); v explotación de una red de gas natural licuado (GNL) (gestores de la red de GNL); vi producción de gas natural (compañías de gas natural); vii compra de gas natural (compañías de gas natural); viii refinado y tratamiento de gas natural un (gestores de instalaciones de refinado y tratamiento de gas natural);
	Subsector del hidrógeno:	i producción de hidrógeno (operadores de producción de hidrógeno); ii almacenamiento de hidrógeno (operadores de almacenamiento de hidrógeno); iii transporte de hidrógeno (operadores de transporte de hidrógeno);
Sector del transporte:	Subsector del transporte aéreo:	i servicios de transporte aéreo utilizados con fines comerciales (pasajeros y carga) (compañías aéreas); ii explotación, gestión y mantenimiento de los aeropuertos y de la infraestructura de la red aeroportuaria (entidades gestoras de aeropuertos); iii servicios de control del tránsito aéreo (operadores de control de la gestión del tránsito aéreo);
	Subsector del transporte por ferrocarril:	i servicios de transporte ferroviario (pasajeros y mercancías) (empresas ferroviarias); ii explotación, gestión y mantenimiento de la infraestructura ferroviaria, incluidas las estaciones de viajeros, las terminales de mercancías, las zonas de operaciones ferroviarias y los centros de control del tráfico (administradores de infraestructuras); iii explotación, gestión y mantenimiento de las instalaciones de servicio ferroviario (explotadores de instalaciones de servicio); iv explotación, gestión y mantenimiento de la gestión del tráfico ferroviario, control-mando y señalización, así como de las instalaciones y sistemas de telecomunicaciones utilizados para el control-mando y la señalización (administradores de infraestructuras);
	Subsector del transporte marítimo y fluvial:	i servicios de transporte por vías navegables interiores, marítimo y costero (pasajeros y mercancías) (compañías de transporte por vías navegables interiores, marítimo y costero de pasajeros y mercancías);

		ii explotación, gestión y mantenimiento de puertos e instalaciones portuarias, y explotación de obras y equipos dentro de los puertos, incluidos el aprovisionamiento de combustible, la manipulación de la carga, el amarre, los servicios de pasajeros, la recogida de desechos generados por buques y residuos de carga, el practicaje, el remolque y los servicios de seguridad (organismos gestores de los puertos y entidades que operan obras y equipos que se encuentran en los puertos);
	Subsector del transporte por carretera	iii control de la gestión del tráfico, incluidos los aspectos relacionados con los servicios de planificación, control y gestión de la red viaria, con exclusión de la gestión del tráfico o la explotación de sistemas de transporte inteligentes cuando no constituyan una parte esencial de la actividad general de las entidades públicas (autoridades viarias); iv servicios de sistemas de transporte inteligentes (operadores de sistemas de transporte inteligentes);
	Subsector de los transportes públicos: servicios públicos de transporte de viajeros por ferrocarril y otros tipos de vía férrea y de transporte por carretera (operadores de servicio público);	
Sector bancario:		i recepción de depósitos (entidades de crédito); ii préstamos (entidades de crédito);
Sector de infraestructuras de los mercados financieros:		i gestión de un centro de negociación (gestores de centros de negociación); ii gestión de los sistemas de compensación (entidades de contrapartida central);
Sector de la salud		i prestación de servicios sanitarios (prestadores de asistencia sanitaria); ii análisis realizados por un laboratorio de referencia de la Unión Europea (laboratorios de referencia de la UE); iii investigación y desarrollo de medicamentos (entidades que realizan actividades de investigación y desarrollo sobre los medicamentos); iv fabricación de productos farmacéuticos de base y de preparaciones farmacéuticas de base (entidades que fabrican productos farmacéuticos y preparaciones farmacéuticas de base); v fabricación de productos sanitarios considerados esenciales durante una emergencia de salud pública (entidades que fabrican productos sanitarios); vi distribución de medicamentos (entidades titulares de una autorización de distribución);
Sector del agua potable: suministro y distribución de agua potable, excluida la		

distribución de agua destinada al consumo humano cuando dicho servicio sea una parte no esencial de la actividad general de los distribuidores que distribuyen otros productos básicos y bienes (proveedores y distribuidores de agua destinada al consumo humano);		
Sector de las aguas residuales: recogida, tratamiento y eliminación de aguas residuales, con exclusión de la recogida, eliminación o tratamiento de las aguas residuales urbanas, de las aguas residuales domésticas o de las aguas residuales industriales, cuando no constituyan una parte esencial de las actividades generales de las empresas (empresas de recogida, eliminación o tratamiento de aguas residuales urbanas, domésticas e industriales);		
Sector de la infraestructura digital:		i prestación y explotación del servicio de puntos de intercambio de Internet (proveedores de puntos de intercambio de Internet); ii prestación de servicios de sistema de nombres de dominio (DNS), excluidos los servicios relacionados con servidores raíz (proveedores de servicios de DNS); iii explotación y administración de registros de nombres de dominio de primer nivel (registros de nombres de dominio de primer nivel); iv prestación de servicios de computación en nube (proveedores de servicios de computación en nube); v prestación de servicios de centros de datos (proveedores de servicios de centros de datos); vi suministro de redes de distribución de contenidos (proveedores de redes de distribución de contenidos); vii prestación de servicios de confianza (proveedores de servicios de confianza); viii prestación de servicios de comunicaciones electrónicas a disposición del público (proveedores de servicios de comunicaciones electrónicas); ix Suministro de redes públicas de comunicaciones electrónicas (proveedores de redes públicas de comunicaciones electrónicas);
Sector de la administración pública: servicios prestados por entidades de la		

administración pública en el sentido del artículo 2, punto 10), de la Directiva (UE) 2022/2557, a nivel central, tal como lo definen los Estados miembros de conformidad con la legislación nacional (entes públicos de la Administración central);		
Sector del espacio: explotación de infraestructuras terrestres, cuya propiedad, gestión y explotación corresponde a Estados miembros o entidades privadas, que apoyan la prestación de servicios espaciales, excluidos los proveedores de redes públicas de comunicaciones electrónicas (operadores de infraestructuras terrestres);		
Sector de la producción, transformación y distribución de alimentos (empresas alimentarias dedicadas exclusivamente a la logística y a la distribución al por mayor y a la producción y transformación industrial a gran escala):		i producción y transformación industrial de alimentos a gran escala; ii servicios de la cadena alimentaria, incluidos el almacenamiento y la logística; iii distribución al por mayor de alimentos.


PUBLICACIONES
Pd
DE DEFENSA


GOBIERNO
DE ESPAÑA
MINISTERIO
DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL
DE PUBLICACIONES
Y PATRIMONIO CULTURAL