centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 808

ENS. Verificación del cumplimiento

Octubre 2023

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.01.09 16:33:46 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-23-277-4
Fecha de Edición: octubre 2023

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

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) busca cumplir tres (3) grandes objetivos.

- En primer lugar, alinear el ENS con el marco normativo y el contexto estratégico existente para garantizar la seguridad en la administración digital.

  Se trata de reflejar con claridad el ámbito de aplicación del ENS en beneficio de la ciberseguridad y de los derechos de los ciudadanos, así como de actualizar las referencias al marco legal vigente y de revisar la formulación de ciertas cuestiones a la luz de éste, conforme a la Estrategia Nacional de Ciberseguridad 2019 y el Plan Nacional de Ciberseguridad, de forma que se logre simplificar, precisar o armonizar los mandatos del ENS, eliminar aspectos que puedan considerarse excesivos, o añadir aquellos otros que se identifican como necesarios.

- En segundo lugar, introducir la capacidad de ajustar los requisitos del ENS, para garantizar su adaptación a la realidad de ciertos colectivos o tipos de sistemas, atendiendo a la semejanza que presentan una multiplicidad de entidades o servicios en cuanto a los riesgos a los que están expuestos sus sistemas de información y sus servicios.

  Ello aconseja la inclusión en el ENS del concepto de «Perfil de Cumplimiento Específico» que, aprobado por el Centro Criptológico Nacional, permita alcanzar una adaptación del ENS más eficaz y eficiente, racionalizando los recursos requeridos sin menoscabo de la protección perseguida y exigible.

- En tercer lugar, facilitar una mejor respuesta a las tendencias en ciberseguridad, reducir vulnerabilidades y promover la vigilancia continua mediante la revisión de los principios básicos, de los requisitos mínimos y de las medidas de seguridad.

Esta guía de verificación del cumplimiento del Esquema Nacional de Seguridad se encuadra dentro de los requisitos del artículo 31 (Auditoría de la seguridad) y del anexo III (Auditoría de la Seguridad) del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS); todo ello según lo previsto en el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en el artículo 4 de dicha ley y en la Instrucción Técnica de Seguridad de Auditoría de Seguridad de los Sistemas de Información.

En este sentido, esta guía será de uso para los sistemas de información comprendidos en el ámbito de aplicación previsto en el artículo 2 de la Ley 40/2015, de 1 de octubre, al que se añaden los sistemas que tratan información clasificada, sin perjuicio de la normativa que resulte de aplicación, pudiendo resultar necesario complementar las medidas de seguridad del Real Decreto 311/2022, de 3 de mayo, con otras específicas para tales sistemas, derivadas de los compromisos internacionales contraídos por España o su pertenencia a organismos o foros internacionales en la materia.

Asimismo, los requisitos del ENS serán de aplicación a los sistemas de información de las entidades del sector privado, cuando de acuerdo con la normativa aplicable y en virtud de una relación contractual presten servicios a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.

Los sistemas de categoría BÁSICA:

- Requerirán de una autoevaluación para su declaración de la conformidad que deberá realizarse al menos cada dos (2) años o cuando se produzcan modificaciones sustanciales en el sistema.
- La autoevaluación podrá ser desarrollada por el mismo personal que administra el sistema de información o en quién éste delegue.
- El resultado de la autoevaluación debe estar documentado, indicando si cada medida de seguridad está implantada y sujeta a revisión regular, así como las evidencias que sustentan la valoración anterior.
- Los informes de autoevaluación serán analizados por el responsable de la seguridad competente, que elevará las conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.
- Un sistema de categoría BÁSICA puede someterse igualmente a una auditoría formal de certificación de la conformidad, por parte de una Entidad de Certificación (EC) acreditada o un Órgano de Auditoría Técnica (OAT) del Sector Público, siendo esta posibilidad siempre la deseable.

Los sistemas de categoría MEDIA o ALTA:

- Precisarán de una auditoría formal, para su certificación de la conformidad, al menos cada dos (2) años, y con carácter extraordinario, siempre que se produzcan modificaciones sustanciales en el sistema de información, en su alcance o en su categoría, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoría extraordinaria determinará la fecha de cómputo para el cálculo de los dos (2) años, establecidos para la realización de la siguiente auditoría regular ordinaria.
- Deberá desarrollarse con las garantías metodológicas y de independencia, profesionalidad y adecuación requeridas.
- El informe de auditoría dictaminará sobre el grado de cumplimiento, identificando e incluyendo los hallazgos y evidencias de conformidad y no conformidad. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas.

- Los informes de auditoría serán analizados por el responsable de la seguridad competente, que presentará sus conclusiones al responsable del sistema para que, en su caso, adopte las medidas correctoras adecuadas.

Conviene recordar que el objetivo de la Auditoría de Certificación del ENS es aportar la confianza de que el sistema de información ha sido auditado por un tercero independiente, imparcial y capacitado. De otra parte, la finalidad de la auditoría interna realizada por miembros de la propia organización, o bien realizada por auditores externos en modalidad de prestación de servicios, es la mejora del sistema, ya que se busca confirmar la eficacia del sistema de gestión u obtener información que permita alcanzarla.

Pese a que el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad no prescribe explícitamente la realización obligatoria de auditorías internas, denominadas en algunos casos auditorías de primera parte, el artículo 27 de dicho cuerpo legal exige la **aplicación de los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información**; exigencia que, trayendo causa del objeto del ENS, expresado en su artículo 1, se concreta igualmente en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información, cuando se hace referencia al grado de confianza en las revisiones de la Dirección y en las auditorías internas del auditado.

Por otro lado, un sistema de información de categoría MEDIA y ALTA requiere disponer de un SGSI para la gestión de su seguridad, como se determina en la medida de seguridad [op.pl.2] sobre arquitectura de seguridad. Bajo esta premisa, cabe decir que cualquier sistema de gestión está basado en la mejora continua, ya sea siguiendo el ciclo de Deming (PDCA) o cualquier otro con el mismo fin.

Por consiguiente, la realización de auditorías internas (de primera parte) constituye una actividad fundamental para sistemas de categorías MEDIA y ALTA, y recomendable para los sistemas de categoría BÁSICA, puesto que constituyen la mejor forma de demostrar que el sistema es capaz de ir mejorando, todo ello con independencia de la realización de las preceptivas Auditorías de Certificación.

En consecuencia, es conveniente o necesario -atendiendo a la categoría de seguridad del sistema auditado- realizar auditorías internas anuales de seguimiento, al menos de las medidas de seguridad del Anexo II del ENS implantadas. Actividad auditora que podrá desplegarse a lo largo del tiempo que media entre Auditorías de Certificación consecutivas.

Asimismo, el RD 311/2022, de 3 de mayo, como se señala en su artículo 1, está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, es decir, para asegurar el acceso, confidencialidad, integridad, trazabilidad, autenticidad, disponibilidad y conservación de los datos, informaciones y servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias, aunque también

es posible que resulten de aplicación otros requisitos legales que el auditor debe tener en cuenta.

Estos requisitos de auditoría adicionales no están dentro del objeto y alcance de la auditoría requerida por el RD 311/2022, de 3 de mayo. Sin embargo, en determinadas situaciones, la necesidad de una mayor eficiencia en la aplicación de los recursos (tanto del equipo auditor como del personal involucrado en el sistema de información auditado) puede aconsejar la realización conjunta de estas auditorías.

En definitiva, la presente guía viene a complementar a la guía *CCN-STIC-802 Esquema Nacional de Seguridad. Guía de auditoría* y está sujeta a lo que señala la *Guía CCN-CERT IC-01/19 ENS. Criterios Generales de Auditoría y Certificación*.

2. OBJETO

El objeto de esta guía es servir de itinerario de auditoría para la evaluación de la conformidad con el ENS de los sistemas de información concernidos, aplicable a cualquier categoría de seguridad (BÁSICA, MEDIA o ALTA), por parte de:

- Las Entidades de Certificación (EC), acreditadas o en proceso de acreditación, así como los Órganos de Auditoría Técnica (OAT) del Sector Público reconocidos, o en proceso de reconocimiento, para adaptar adecuadamente sus listas de comprobación o checklist de auditoría; y
- Los responsables de realizar auditorías internas periódicas (de primera parte), como elemento fundamental de mejora continua de la seguridad del sistema de información y del sistema de gestión aplicado sobre el mismo.

3. ALCANCE

Esta guía es de aplicación a cualquier entidad que deba cumplir con los preceptos del Esquema Nacional de Seguridad (RD 311/2022, de 3 de mayo), con independencia de su naturaleza, dimensión y categoría de sus sistemas.

4. CÓMO UTILIZAR ESTA GUÍA

Esta guía pretende ser una ayuda para el trabajo de campo de los auditores, pudiendo ser adaptada y empleada directamente como *checklist*, disponiéndose al efecto de un anexo en formato Excel, sin perjuicio de emplear un asistente de autoevaluación/certificación que se materialice en una solución automatizada.

La solución AMPARO del CCN-CERT permite la automatización del proceso de verificación y facilita la gestión de los diferentes sistemas auditados de forma alineada con esta guía.

4.1 APLICABILIDAD DE UNA MEDIDA DE SEGURIDAD

Debe tenerse en cuenta que en el RD 311/2022, de 3 de mayo, algunas de las medidas de seguridad preceptivas que determina el anexo II pueden ser excluidas debido a la particular naturaleza del sistema y su entorno de operación, por lo que dichas exclusiones deberán estar debidamente justificadas en la Declaración de Aplicabilidad correspondiente a dicho sistema de información.

Del mismo modo, las medidas de seguridad del anexo II podrán ser compensadas, ampliadas con requisitos de "REFUERZO", equilibradas con medidas complementarias de vigilancia, o incluso adaptadas a requisitos pensados inicialmente para sistemas de categoría superior, siempre que a consecuencia del análisis de riesgos se consideren necesarios para mitigar aquellos riesgos evaluados como no asumibles para el sistema de información concernido.

Por todo ello, para cada una de las medidas de seguridad del anexo II del ENS, se debe indicar de forma diferenciada, por un lado, si la medida aplica o bien ha sido excluida en la Declaración de Aplicabilidad, y por otro, si la medida ha sido auditada o, por alguna razón, no ha podido serlo.

4.2 MEDIDAS DE SEGURIDAD

Las medidas de seguridad que se determinan en el anexo II del RD 311/2022, de 3 de mayo, son un conjunto de disposiciones encaminadas a proteger al sistema de información de los riesgos a los que estuviere sometido, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, protección, detección y reacción, disuasión o recuperación.

Asimismo, aplicando las que correspondan de dichas medidas de seguridad, se logra el cumplimiento de los principios básicos y requisitos mínimos establecidos en el ENS.

Dichas medidas serán proporcionales a las dimensiones de seguridad relevantes para el sistema a proteger y a la categoría del mismo.

Cada medida de seguridad se puede llegar a segregar en dos (2) tipos de requisitos: requisitos "BASE" y requisitos de "REFUERZO"; estos últimos, caso de aparecer para una determinada medida, podrán ser obligatorios o potestativos.

4.2.1 Requisitos "BASE"

Los requisitos "BASE" constituyen las mínimas exigencias de cumplimiento, siempre preceptivas (obligatorias), para todas y cada una de las 73 medidas de seguridad del anexo II del ENS.

En el RD 311/2022, de 3 de mayo, numerosas medidas de seguridad pueden desglosarse en varios requisitos "BASE" de seguridad, facilitando la concreción en su implementación y su posterior auditoría.

4.2.2 Requisitos de "REFUERZO"

Para ciertas medidas de su anexo II, del RD 311/2022, de 3 de mayo, se han establecido requisitos de "REFUERZO".

Algunos de dichos requisitos de "REFUERZO" son preceptivos para las categorías superiores (MEDIA o ALTA), mientras que otros son potestativos, para posibilitar que la organización decida si conviene o no implementarlos, al objeto de alcanzar un mayor refuerzo de su nivel de seguridad, especialmente cuando el resultado del análisis de riesgos así lo aconseje o alguna otra norma legal, o su desarrollo, lo determine.

4.3 MEDIDAS COMPENSATORIAS

Las medidas de seguridad referenciadas en el anexo II del ENS podrán ser reemplazadas por otras compensatorias, siempre y cuando se justifique documentalmente que protegen, igual o mejor, el riesgo sobre los activos (anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III del RD 311/2022, de 3 de mayo.

Como parte integral de la Declaración de Aplicabilidad se indicará, de forma detallada, la correspondencia entre las medidas compensatorias implementadas y las medidas del anexo II que compensan.

Por todo ello, para cada una de las medidas de seguridad del anexo II del ENS, se deberá indicar si se ha empleado alguna medida compensatoria que la reemplace.

El empleo y modo de justificar las medidas compensatorias, se desarrolla en la guía *CCN-STIC 819 Medidas Compensatorias*.

4.4 MEDIDAS COMPLEMENTARIAS DE VIGILANCIA

Una medida complementaria de vigilancia es aquella que complementa y equilibra los requisitos exigibles que se han implementado para una determinada medida de seguridad, ya sea de "BASE" o de "REFUERZO", cuando éstos no son suficientes, a juicio de la organización, para poder alcanzar el cumplimiento del ENS para dicha medida. También pueden complementar a una medida compensatoria que no consigue igualar o mejorar el riesgo de la medida original.

En ocasiones, dicha medida complementaria de vigilancia será transitoria (limitada en el tiempo) hasta que se puedan implementar todos los requisitos requeridos por la medida de seguridad del ENS o para la efectividad plena de la medida compensatoria que se haya decidido implementar como alternativa.

4.5 GRADO DE IMPLEMENTACIÓN DE UNA MEDIDA DE SEGURIDAD

En la mayoría de las medidas de seguridad se puede distinguir una parte formal, que define la medida de forma documentada, una parte material, que es la materialización de la misma y las mediciones necesarias para su gestión y mejora continuada a lo largo del tiempo.

Atendiendo al estado de implementación en que se encuentre cada una de las medidas de seguridad del anexo II del ENS, se pueden considerar como 'no implementadas', 'en proceso de implementación' o 'implementadas'.

En base a ello, se ha establecido una clasificación, con mayor nivel de detalle, referida al grado de implementación de cada una de las medidas de seguridad, que se muestra en forma de tabla a continuación:

ESTADO DE IMPLEMENTACIÓN	GRADO DE IMPLEMENTACIÓN	DESCRIPCIÓN
No implementada NI	G0	**Medida de seguridad pendiente de implementación.** En el grado G0 de implementación, la medida de seguridad no está siendo aplicada y quizá ni siquiera se contempla que lo sea en un futuro. Pese a ello, la medida sí debería aplicarse, atendiendo a la declaración de aplicabilidad del sistema o a lo dispuesto en el anexo II del ENS, en los niveles (dimensiones) de seguridad y en la categoría de seguridad correspondientes.
En proceso de implementación P	G1	**Medida de seguridad con implementación iniciada.** En el grado G1 de implementación, la medida de seguridad existe, en el mejor de los casos, a nivel de piloto o prototipo y se han planificado o iniciado los trabajos necesarios para su implementación.
		Medida de seguridad en implementación. En el grado G1 de implementación, la medida de seguridad está implementada en su parte material, pero la eficacia de la medida depende de la capacidad y buena voluntad de las personas, entre otras razones porque no está documentada (parte formal). Tampoco puede considerarse conocida por todos los interesados, al no haber directrices para ello.
Implementada I	G2	**Medida de seguridad implementada.** En el grado G2 de implementación, la medida de seguridad está definida de forma documentada y, si corresponde, contempla la realización de procesos asociados y la determinación de métricas. En este grado, hay normativa establecida y procedimientos para garantizar la reacción profesional ante posibles incidencias. Además, se ejerce un mantenimiento regular sobre la medida. *NOTA: Parte de la documentación puede estar embebida en determinada herramienta, por lo que dicha documentación puede referenciarse, o reproducirse, según aconseje cada caso particular y refrende el auditor.*
		Medida de seguridad medible y gestionable. En el grado G2 de implementación, se dispone de métricas e indicadores para conocer el desempeño (eficacia y eficiencia) de la medida, lo que posibilita su gestión. *NOTA: En el grado G2 de madurez, el funcionamiento de las principales medidas de seguridad y los procesos asociados están bajo control, pudiéndose ajustar en función de las desviaciones observadas en los indicadores.*
		Medida de seguridad en ciclo de mejora continua. El grado G2 de implementación también se centra en mantener la mejora continua de la medida de seguridad y los procesos asociados. Se alcanza cuando se rectifica y mejora la efectividad de la medida de seguridad con la suficiente continuidad y en base a las métricas e indicadores recopilados.

4.6 NOTAS AL AUDITOR

Algunos requisitos "BASE" y requisitos de "REFUERZO", según constan en esta guía para cada una de las medidas de seguridad del anexo II del ENS, llevan anotaciones que ayudan a interpretar la Norma.

No obstante, tampoco se ha considerado necesario ampliar mucho más los comentarios, dado que para ese fin ya se dispone de la guía *CCN-STIC 804 ENS. Guía de implantación* que

ilustra detalladamente posibles formas de implementar cada uno de los requisitos de las medidas que sean de aplicación.

Un aspecto relevante, respecto a la auditoría de la parte formal de las medidas de seguridad, es la evidencia de la aprobación formal de documentos en todo el marco normativo y documental del sistema. Dicha aprobación se considerará fehaciente cuando:

a. El documento esté firmado electrónicamente por el/los responsables(s) pertinentes.

b. El documento esté impreso y firmado por el/los responsables(s) pertinentes, conservándose la copia original del mismo.

c. El documento haya sido aprobado en una reunión formal del órgano o comité competente, donde los responsables estén involucrados, y su aprobación conste reflejada en el acta de la sesión.

5. VERIFICACIÓN DEL CUMPLIMIENTO DEL ENS

Este epígrafe contempla, por un lado, la verificación del cumplimiento del articulado del ENS, y, por otro lado, la conformidad de las medidas de seguridad contempladas en su anexo II.

Para cada una de las medidas de seguridad de los tres (3) grupos considerados por el ENS (margo organizativo, marco operacional y medidas de protección) el presente epígrafe indicará cómo verificar el cumplimiento respecto a las disposiciones del ENS, desarrollando, cuando proceda y para cada una de ellas, los requisitos “BASE” y de “REFUERZO”.

Hay que significar que las propuestas de verificación son generalistas para cualquier organización, por lo que el auditor podría requerir adaptarlas al entorno en el que se encuentre y opere el sistema de información auditado.

Las verificaciones a realizar para cada una de las medidas de seguridad del anexo II del ENS, agrupadas en requisitos “BASE” y refuerzos adicionales, se han coloreado según el convenio especificado en la siguiente tabla:

CÓDIGO DE COLORES EMPLEADO
Requisito “BASE” exigible a todas las categorías
Requisito “BASE”, o de “REFUERZO”, exigible a categorías MEDIA y ALTA
Requisito “BASE”, o de “REFUERZO”, exigible a categoría ALTA
Requisito de “REFUERZO” a considerar

Adicionalmente, en las diferentes cuestiones de verificación, o subcontroles, que se proponen para cada una de las medidas de seguridad del anexo II del ENS, se distinguen los requisitos que se consideran esenciales para la categoría correspondiente, mediante el empleo de sombreado de color gris junto a un icono que recuerda que, si alguno de ellos no se cumple, el auditor debe considerar la medida de seguridad en su conjunto como ‘no implementada’.

En este sentido, se considerará una medida 'en proceso de implementación' cuando, aun cumpliéndose todos los requisitos que se consideran esenciales (sombreados de color gris), la medida no se encuentre completamente 'implementada' por faltar algún requisito.

CÓDIGO DE COLORES COMPLEMENTARIO EMPLEADO	
NI	Requisito "ESENCIAL" (sombreado en color gris)

Por último, se ha añadido, para cada artículo y medida de seguridad, un apartado con la propuesta de posibles evidencias que podría recabar el auditor durante la auditoría, como constancia de cumplimiento, sin menoscabo de que el auditor considere reducirlas, o ampliarlas, en base a su experiencia profesional y a la naturaleza del sistema de información y de la organización auditada.

6. VALORACIÓN DE LA IMPLANTACIÓN DE LAS MEDIDAS DE SEGURIDAD

Es habitual el empleo de niveles de madurez para caracterizar la implementación de un proceso. El modelo de madurez de capacidad (Capability Maturity Model, CMM) permite describir las características que hacen un proceso efectivo, midiendo el grado o nivel de profesionalización de la actividad.

Un proceso es una colección de actividades o tareas relacionadas y estructuradas que, en una secuencia específica, proporciona un servicio para la organización.

Para la valoración de la implantación de las medidas de seguridad, estás se analizarán como procesos y se estimará su nivel de madurez usando el modelo de madurez de capacidad (CMM).

Se identifican cinco (5) "niveles de madurez", de modo que una organización que tenga institucionalizadas todas las prácticas incluidas en un nivel y sus inferiores, se considera que ha alcanzado ese nivel de madurez:

a) **L0 – Inexistente.**

No existe un proceso que soporte el servicio requerido.

b) **L1 - Inicial. Ad hoc.**

Las organizaciones en este nivel no disponen de un ambiente estable para la prestación del servicio requerido. Aunque se utilicen técnicas correctas de ingeniería, los esfuerzos se ven minados por falta de planificación. El éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobrecostes. El resultado es impredecible. A menudo las soluciones se implementan de forma reactiva a los incidentes.

Los procedimientos de trabajo, cuando existen, son informales, incompletos y no se aplican de forma sistemática.

c) **L2 - Reproducible, pero intuitivo.**

En este nivel las organizaciones disponen de unas prácticas institucionalizadas de gestión, existen unas métricas básicas y un razonable seguimiento de la calidad.

Existen procedimientos de trabajo, pero no están suficientemente documentados o no cubren todos los aspectos requeridos.

d) **L3 - Proceso definido.**

Además de una buena gestión, a este nivel las organizaciones disponen de normativa y procedimientos detallados y documentados de coordinación entre grupos, formación del personal, técnicas de ingeniería, etc.

e) **L4 - Gestionado y medible.**

Se caracteriza porque las organizaciones disponen de un conjunto de métricas de efectividad y eficiencia, que se usan de modo sistemático para la toma de decisiones y la gestión de riesgos. El servicio resultante es de alta calidad.

f) **L5 – Optimizado.**

La organización completa está volcada en la mejora continua de los procesos. Se hace uso intensivo de las métricas y se gestiona el proceso de innovación.

Para cada medida de seguridad que sea de aplicación al sistema de información se exigirá un determinado nivel de madurez. Los niveles mínimos de madurez requeridos por el ENS en función de la categoría del sistema son:

Categoría del sistema	Nivel mínimo de madurez requerido
BÁSICA	L2 – Reproducible, pero intuitivo
MEDIA	L3 – Proceso definido
ALTA	L4 – Gestionado y medible

6.1 CUMPLIMIENTO DE ARTÍCULOS DEL ENS

Disposición adicional segunda del ENS	**Desarrollo del ENS. ITS y guías de seguridad**		
	Aplica: SI ☐ NO ☐ **Artículo auditado**: SI ☐ NO ☐		
Propuestas de evidencias			
	☐ Repositorio con las guías CCN-STIC de uso frecuente y permisos de acceso al mismo. ☐ Registro de legislación y normativa aplicable (Incluyendo las ITS)		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Disposición adicional segunda del ENS	¿La organización conoce y mantiene actualizada la relación de las Instrucciones Técnicas de Seguridad (ITS) y guías de seguridad (especialmente las CCN-STIC) que son de aplicación a sus sistemas de información?		☐ SI ☐ NO
Disposición adicional segunda del ENS	¿Se dispone de acceso a dichas guías CCN-STIC por parte del personal con necesidad de conocer, ya sea en el portal del CCN, o en repositorios de la organización para las guías de uso frecuente?		☐ SI ☐ NO
Disposición adicional segunda del ENS	¿La organización dispone o conoce los documentos *abstract* del CCN CERT y los tiene en cuenta en cuanto a las recomendaciones e implementaciones de medidas de seguridad?		☐ SI ☐ NO

Art. 28	**Declaración de aplicabilidad**
	Aplica: SI ☐ NO ☐ **Artículo auditado**: SI ☐ NO ☐
Propuestas de evidencias	
	☐ Declaración de Aplicabilidad. ☐ Evidencia de haberse suscrito la Declaración de Aplicabilidad por parte del Responsable de Seguridad.

	☐ Evidencia de otros documentos vinculados a la Declaración de Aplicabilidad, como pueden ser los estudios que justifiquen las medidas compensatorias, o las medidas complementarias de vigilancia, que se hayan podido aplicar.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Art. 28.2	¿Se dispone de un documento formal que relacione las medidas y refuerzos de seguridad indicados en el anexo II del RD 311/2022 de 3 de mayo, con indicación de su aplicabilidad al sistema de información? *NOTA: A la Declaración de Aplicabilidad se le designa habitualmente en otros marcos normativos, como puede ser la norma ISO/IEC 27001, como SOA (por sus siglas en inglés de Statement of Applicability).*		☐ SI ☐ NO
Art. 28.2	¿Dicha Declaración de Aplicabilidad está suscrita por el Responsable de Seguridad como prueba de su compromiso respecto a la supervisión del cumplimiento de las medidas de seguridad en ella reflejadas?		☐ SI ☐ NO
Art. 28.3	En caso de identificar la organización medidas que no aplican, pero que sí que lo harían en base a la categoría y niveles de las dimensiones del sistema de información, ¿Justifica suficientemente la Declaración de Aplicabilidad la exclusión de las mismas? *NOTA: Pese a no ser exigible, es una buena práctica no solo justificar en la Declaración de Aplicabilidad las medidas que se excluyan, sino todas, indicando muy brevemente cómo se cumple cada medida y, si procede, referencia a los documentos relevantes del sistema que estén vinculados a ellas.*		☐ SI ☐ NO
Art. 28.3	En el caso de aplicar medidas compensatorias, ¿se ha justificado formalmente en la Declaración de Aplicabilidad la necesidad de aplicar tales medidas compensatorias y la justificación de que dichas medidas		☐ SI ☐ NO

	protegen, igual o mejor, al riesgo sobre los activos y sobre el sistema de información en su conjunto? *NOTA: Cómo justificar formalmente las medidas compensatorias se detalla en la guía "CCN-STIC 819 Medidas compensatorias".*		
Apartado 4.4 de esta guía, avalado por el apartado 8 del Anexo II del RD 311/2022.	En el caso de aplicar medidas complementarias de vigilancia ¿se indica formalmente en la Declaración de Aplicabilidad si dichas medidas complementarias son transitorias, o no, y se justifica que la medida que ha sido complementada, tal vez por estar en proceso de implantación, protege de forma análoga al sistema de información?		☐ SI ☐ NO

Art. 30	**Perfiles de cumplimiento**		
	Aplica: SI ☐ NO ☐ **Artículo auditado**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Declaración de Aplicabilidad.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Art. 30	En caso de que la organización se acoja a un perfil de cumplimiento específico, aplicable a la entidad y validado por el CCN, ¿se ha recogido y justificado su aplicación en la Declaración de Aplicabilidad?		☐ SI ☐ NO

Art. 32	**Informe del estado de la seguridad (INES)**
	Aplica: SI ☐ NO ☐ **Artículo auditado**: SI ☐ NO ☐
Propuesta de evidencias	

	☐ Acceso electrónico al último informe INES de la organización		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Art. 32	Si se trata de una organización titular de algún sistema de información comprendido en el ámbito de aplicación del artículo 2 del ENS ¿se aporta y se actualiza la información necesaria, al menos anualmente, para dar cumplimiento a la ITS de informe del estado de la seguridad (INES), lo que permite al CCN consolidar la información para elaborar un perfil general del estado de la seguridad que propicie adoptar medidas para la mejora continua de los sistemas?		☐ SI ☐ NO

Art. 38	**PROCEDIMIENTOS DE DETERMINACIÓN DE LA CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD.**		
	Aplica: SI ☐ NO ☐ **Artículo auditado**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Uso correcto del distintivo de ENS.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Art. 38.2	¿Se da publicidad en las páginas web o en las sedes electrónicas a las Declaraciones y Certificaciones de Conformidad con el ENS, atendiendo a lo indicado en la ITS correspondiente y se incluye un enlace en el Distintivo de Conformidad al documento correspondiente? *NOTA: Únicamente aplica a aquellas organizaciones que ya estuvieran certificadas al realizar la auditoría.*		☐ SI ☐ NO

Art.40 y 41	**Categorización de los sistemas de información**
	Medida aplica: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐

Propuesta de evidencias			
	☐ Documento de valoración de servicios e información. ☐ Documento formal en el que los responsables de los servicios y de la información suscriben las valoraciones. ☐ Documento formal en el que el Responsable de Seguridad categoriza el sistema.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Art. 41	¿Los responsables de la información y los responsables de los servicios han valorado los activos esenciales que son de su competencia en las cinco dimensiones de la seguridad?		☐ SI ☐ NO
Art.40 Art. 41	¿Se dispone de un documento formal que recoja dichas valoraciones y evidencia de la conformidad respecto a las mismas de los responsables de la información y los servicios afectados? ¿Se han tenido en cuenta todos los aspectos identificados en el anexo I del ENS como punto de entrada para realizar la valoración?		☐ SI ☐ NO
Art. 41	¿El Responsable de Seguridad determina la categoría del sistema mediante un documento formal, en base a las valoraciones de servicios e información soportados por el sistema de información que han realizado sus responsables? ¿En caso de que haya diferentes responsables de seguridad se ha realizado un comité para tomar en cuenta las decisiones de todos ellos?		☐ SI ☐ NO

6.2 CUMPLIMIENTO DE MEDIDAS DE SEGURIDAD

6.2.1 Marco Organizativo

El marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad.

Org.1	**Política de seguridad**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Documento formal conteniendo la política de Seguridad de la Información (PSI) acorde al contenido esperado. ☐ En su caso, evidencia de su publicación, y de su difusión interna. ☐ Posible procedimiento de identificación de la legislación aplicable y registro actualizado conteniendo la misma. ☐ Acta de constitución del Comité de Seguridad y designación inicial de sus miembros y aceptación de las responsabilidades. ☐ Diferentes actas de designación y/o cese de miembros del Comité de Seguridad a lo largo del tiempo. ☐ Documento de aceptación de las funciones de los roles del ENS y miembros del Comité de Seguridad.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Org.1 NI	**¿Se dispone en la organización de una Política de Seguridad de la Información (PSI) o, en su caso, se ha adherido a la política de seguridad de la institución de la que depende o está vinculada?**		☐ SI ☐ NO
☐ NI	¿La PSI de la organización <u>ha sido aprobada</u> por el titular del órgano superior correspondiente, en caso de pertenecer al sector público, o por la dirección general, en caso de pertenecer al sector privado, teniendo en cuenta los diferentes supuestos que determina el artículo 12 del RD 311/2022, de 3 de mayo? ¿La PSI se revisa a intervalos planificados? En caso de que se hayan adherido a una política de otra AAPP se debe asegurar que está vigente, que es adecuada y es conforme a toda la legislación vigente.		
☐	La PSI de la organización, en calidad de documento calificado como público, ¿ha sido publicada y dada a conocer a empleados y colaboradores de la organización? En caso de pertenecer al sector público, ¿ha sido publicada en el Boletín Oficial correspondiente (del Estado, de la Comunidad Autónoma, de la Provincia…)?		

Org.1 NI	**La Política de Seguridad de la Información (PSI) ¿Está estructurada de forma que incluya, con claridad, al menos el contenido que señala el RD 311/2022, de 3 de mayo?**		☐ SI ☐ NO
☐ NI	¿La PSI determina precisa los objetivos o misión de la organización? *NOTA: En algunos organismos, pertenecientes al sector público, dicha información se publica aparte mediante un decreto de estructura. En este caso, la PSI deberá referenciar el documento correspondiente.*		
☐ NI	¿Se determina en la PSI el marco legal y regulatorio en el que se desarrollarán las actividades? *NOTA: No debe interpretarse como la necesidad de incluir de forma exhaustiva en la política una relación de normas jurídicas, lo que trae a causa que la PSI esté permanentemente desactualizada ante los continuos cambios legislativos; lo que debe definirse es el marco basado en normas españolas y europeas relacionadas con la Administración electrónica, la ciberseguridad y seguridad de la información en general, así como la protección de datos, , e indicando que se dispone de un procedimiento de identificación de la legislación aplicable y de actualización permanente de un registro donde se conservan referencias a dichas normas actualizadas.*		
☐ NI	Como desarrollo del marco legal y regulatorio determinado en la PSI ¿se dispone de un procedimiento de identificación de la legislación aplicable que tenga en cuenta los orígenes a consultar, el encargado de hacerlo, su registro, etc.? ¿se dispone asimismo de un registro de normativa jurídica actualizado, que indique la situación en que se encuentran las normas relacionadas con la Administración electrónica, la ciberseguridad y seguridad de la información en general, así como la protección de datos (entrada en vigor, fecha de aplicación, posible norma que la deroga, etc.)?		
☐ NI	¿Se determinan en la PSI 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?		
☐	Si la Organización se acoge a un Modelo de Gobernanza estándar, ¿la PSI detalla los responsables, sus atribuciones y los mecanismos de coordinación y resolución de conflictos? *NOTA: Son especialmente relevantes el Responsable de la Información, el Responsable del Servicio, el Responsable de la Seguridad, el Responsable del Sistema y, en su caso, los posibles administradores de seguridad. También es una muy buena práctica incluir al DPD para asesoramiento en materia de protección de datos personales.*		
☐	Si la Organización se acoge a un Modelo de Gobernanza por bloques de responsabilidad, frecuente en las organizaciones que se acogen al Perfil Específico de Cumplimiento de Requisitos Esenciales de Seguridad (PCE-RES) ¿la PSI detalla al Responsable de Gobierno, al Responsable de Vigilancia y al Responsable de Operación, como integrantes de los diferentes roles y funciones del ENS?		
☐ NI	Se define la estructura del Comité de Seguridad, junto a otros comités técnicos o grupos de trabajo que puedan llegar a definirse, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización? *Nota: En el Modelo de Gobernanza por bloques de responsabilidad, el Responsable de Gobierno integra las funciones del Comité de Seguridad, del Responsable de la Información y del Responsable del Servicio, pudiendo delegarse alguna de sus funciones en otra persona.*		

☐	¿Se dispone de un acta del Comité de Seguridad donde se designen sus miembros, o las altas y bajas que se puedan llegar a producir?
☐	¿Se dispone de un documento de aceptación de la designación y de las responsabilidades inherentes a la misma por parte de los diferentes roles del ENS y de los miembros del Comité de Seguridad y demás comités técnicos?
☐ NI	¿Se señalan las directrices para la estructuración de la documentación de seguridad del sistema de información, su gestión y acceso? *NOTA: Puede hacerse referencia al desarrollo de la PSI mediante el Marco Normativo interno (normas internas, procedimientos, instrucciones técnicas, etc.). Asimismo, señalar se dispone de un repositorio o un gestor documental regido por una norma interna de gestión de la documentación en cuanto a elaboración, aprobación, conservación, estructura, acceso, etc., de los documentos del sistema de gestión de la seguridad aplicado sobre el/los sistema(s) de información*

Org.2	**Normativa de seguridad**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
Org.2	☐ Documento o documentos relevantes de normativa de seguridad, acorde con el contenido esperado. ☐ Evidencia de su aceptación por empleados y colaboradores.		
	☐ Evidencia de que la documentación de seguridad se ha elaborado siguiendo las guías CCN-STIC apropiadas.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Org.2 NI	**¿Se dispone de normativa interna de la organización donde se determine el uso correcto de equipos, servicios e instalaciones, así como lo que se considera uso indebido?** *NOTA: Aunque se pueda contar con diferentes documentos conteniendo normativa especializada de seguridad, se considera muy útil disponer de un documento consolidado, aunque esté más resumido, que pueda difundirse internamente, a disposición de empleados y colaboradores.*		☐ SI ☐ NO
☐ NI	¿La normativa interna de seguridad ha sido aprobada por la autoridad, órgano o persona competente en la fijación de normas internas de la organización		

☐ NI	¿El documento de normativa interna de seguridad señala claramente la responsabilidad del personal con respecto al cumplimiento o violación de dicha normativa: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente?
☐	¿La normativa interna de seguridad ha sido conocida y aceptada por empleados y colaboradores de la organización mediante la suscripción de la misma por medio de documento formal firmado?

Org.2.r1.1	**¿Se dispone de documentación de seguridad, desarrollada según lo reflejado en las guías CCN-STIC que resulten de aplicación?**		☐ SI ☐ NO

Org.3	**Procedimientos de seguridad**
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐
Propuesta de evidencias	
	☐ Documentos relevantes de procedimientos de seguridad con evidencia de su aprobación. ☐ En su caso, evidencia de su publicación o difusión interna en la organización. ☐ Evidencia de procedimiento donde se indique como se trata la información en función de su nivel de seguridad.
	☐ Evidencia de validación de los procedimientos que corresponda por la autoridad competente.

	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Org.3 NI	**¿Se dispone de un conjunto de procedimientos documentados que determinan cómo realizar las tareas habituales?**		☐ SI ☐ NO

☐	¿Los procedimientos de seguridad hacen referencia a la normativa interna de seguridad (o políticas internas de segundo nivel) que desarrollan? *NOTA: Una norma indica qué debe y/o qué no debe hacerse; en cambio, un procedimiento indica cómo debe hacerse lo que determinan las normas.*
☐ NI	¿Los procedimientos de seguridad determinan claramente cómo debe realizarse cada tarea?
☐	¿Los procedimientos de seguridad determinan claramente quién debe realizar cada tarea? por ejemplo, mediante una matriz RACI.
☐	¿Los procedimientos de seguridad se han comunicado a quienes los deben conocer?
☐	Cuando sea aplicable, ¿los procedimientos de seguridad indican cómo identificar y reportar comportamientos anómalos?

☐	¿Se dispone de algún procedimiento de seguridad donde se indique la forma en que debe tratarse la información, en consideración al nivel en qué se ha valorado ésta respecto a la seguridad (Bajo, Medio o Alto)? *NOTA: Se precisará, por ejemplo, como efectuar su control de acceso, su almacenamiento, copias de seguridad, el etiquetado de los soportes que la contengan, su transmisión telemática, y cualquier otra actividad que se considere relevante respecto a la información.*
☐ NI	¿Los procedimientos de seguridad han sido aprobados por quién dispone la PSI, o bien por quién se determina en la norma interna de gestión de la documentación?

Org.3.r1.1	**¿Además de su aprobación por la propia organización, se han validado los procedimientos de seguridad por la autoridad correspondiente?**		☐ SI ☐ NO

Org.4	**Proceso de autorización**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Documentos o registros, con el contenido esperado, de diferentes tipos de autorizaciones. ☐ Si se emplea una herramienta de *ticketing* que las consolide, evidencia de *tickets* de peticiones de autorización. ☐ Lista de personal autorizado a transportar de forma recurrente determinados soportes de información.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Org.4 NI	**¿Se registran las autorizaciones concedidas a efectos de trazabilidad, siguiendo un procedimiento formal establecido en la organización?** *NOTA: Puede llegar a emplearse una herramienta de 'ticketing', quizá la misma que se emplea para la gestión de incidentes o peticiones de servicio, habitualmente diferenciando los diferentes tipos de registro, de modo que quede constancia al menos de qué se ha autorizado, a quién, cuando, por quién y en qué intervalo temporal. No obstante, no es imprescindible unificar todos los flujos de autorización, aunque deseable, pudiéndose emplear modelos de solicitud (formularios) en diferentes formatos.*		☐ SI ☐ NO

☐	¿Se gestionan las autorizaciones para la utilización de instalaciones, ya sean habituales o alternativas, como puede ser un CPD o sala técnica?
☐ NI	¿Se gestionan las autorizaciones para la entrada de equipos en producción, especialmente los equipos que involucren criptografía?
☐ NI	¿Se gestionan las autorizaciones para la entrada de aplicaciones en producción?
☐ NI	¿Se gestionan las autorizaciones para el establecimiento de enlaces de comunicaciones con otros sistemas? *NOTA: Las autorizaciones pueden corresponder a enlaces entre sistemas propios, por ejemplo, entre sedes, o de terceros, como puede ser con un proveedor.*
☐ NI	¿Se gestionan las autorizaciones para la utilización de medios de comunicación, habituales y alternativos? *NOTA: Podría tratarse de una conexión remota VPN contra la red de la organización, determinada salida a Internet, la solicitud de apertura de puertos en un cortafuegos (FW) corporativo, etc.*
☐	¿Se gestionan las autorizaciones para la utilización de soportes de información, ya sean éstas puntuales para un caso de uso concreto, o recurrentes, en base a una lista de autorizados? *NOTA: Puede abarcar la copia y traslado de información en pendrives, discos USB, etc. Asimismo, la solicitud de desbloqueo de puertos USB si están por defecto bloqueados mediante alguna directiva técnica. NOTA2: En ocasiones, los responsables de los soportes pueden contar con la autorización implícita para transportarlos.*
☐	¿Se gestionan las autorizaciones para la salida de los equipos móviles corporativos fuera del perímetro físico de la organización, ya sean éstas puntuales para un caso de uso concreto, o recurrentes, en base a una lista de autorizados? *NOTA: Se entiende por equipos móviles a los ordenadores portátiles, tabletas, teléfonos inteligentes u otros de naturaleza análoga.*
☐	¿Se gestionan las autorizaciones para el empleo de equipos móviles particulares para tareas de la organización (BYOD)? *NOTA: Se entiende por equipos móviles a los ordenadores portátiles, tabletas, teléfonos inteligentes u otros de naturaleza análoga.*
☐	¿Se gestionan las autorizaciones para la utilización de servicios de terceros, bajo contrato o convenio, concesión, encargo, etc.? *NOTA: Se entiende por servicios de terceros los de almacenamiento remoto en la nube, backup remoto, otras cuentas de correo, aplicaciones entregadas como servicio (SaaS) como puede ser una gestión de inventario o una herramienta de ticketing, etc.*
☐	Si procede, ¿se gestionan otro tipo de autorizaciones? *NOTA: Las autorizaciones previstas en esta medida de seguridad no son una lista cerrada. Dependen del contexto interno y externo de la Organización, así como de la evolución tecnológica.*

6.2.2 Marco Operacional

El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

6.2.2.1 Marco Operacional (PLANIFICACIÓN)

Op.pl.1	**Análisis de riesgos**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia de la fecha de finalización de la última iteración de análisis de riesgos. ☐ Documentación de la última iteración de análisis de riesgos y, en su caso, de la herramienta empleada. ☐ Evidencia de las salvaguardas que se hayan determinado.		
	☐ Documento de metodología del análisis de riesgos. ☐ Evidencia de la herramienta empleada. ☐ Evidencia de la valoración de activos. ☐ Evidencia de la identificación de las amenazas. ☐ Evidencia del cálculo del riesgo inicial y residual. ☐ Evidencia del umbral o apetito de riesgo. ☐ Evidencia del Plan de Tratamiento de Riesgos (PTR).		
	☐ Documento resumen para la exposición de la gestión de riesgos al Comité de Seguridad. ☐ Evidencia de aprobación formal de la gestión de riesgos y de aceptación de los riesgos residuales.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.pl.1 (NI)	**¿Se dispone de un análisis de riesgos documentado, cuya última iteración se ha realizado en fecha adecuada?** *NOTA: El análisis de riesgos debe realizarse al menos una vez al año o siempre que el sistema de información experimente cambios relevantes.*		☐ SI ☐ NO

☐	¿Se han detectado cambios relevantes en el sistema de información que hayan requerido realizar una nueva iteración del análisis de riesgos antes de que hubiera transcurrido un año desde la anterior?
☐	¿Se dispone de un acta del Comité de Seguridad aprobando la última iteración del análisis de riesgos, las salvaguardas empleadas para mitigar los riesgos considerados inaceptables, así como los riesgos residuales resultantes?
☐ NI	¿Se han identificado los activos esenciales (servicios e información que éstos manejan), así como el resto de activos más relevantes del sistema de información?
☐ NI	¿Se han identificado las amenazas más probables respecto al sistema de información y sus activos más relevantes?
☐ NI	¿Se han determinado las salvaguardas que pueden mitigar las posibles amenazas para el sistema de información?
☐ NI	¿Se han identificado y valorado los principales riesgos residuales que permanecen tras la aplicación de las salvaguardas?
☐ NI	¿Se ha definido un plan de tratamiento de riesgos para mitigar los riesgos?

Op.pl.1.r1	**Para categoría MEDIA, ¿Se ha realizado un análisis de riesgos semiformal, con una metodología específica en base a un catálogo básico de amenazas y una semántica definida?** *NOTA: Puede estar basado en hojas Excel o en una herramienta como puede ser PILAR.*		☐ SI ☐ NO

☐	Además de identificarse, ¿se valoran cualitativamente los activos más valiosos del sistema de información?
☐	¿Se ha definido un umbral de valor del riesgo a partir del cual se considera éste inaceptable (apetito de riesgo)?
☐	Además de identificarse, ¿se cuantifican los impactos que podrían llegar a producir las amenazas más probables?
☐	Además de determinarse, ¿se han valorado las salvaguardas que se emplearán para protegerse de las amenazas en base al valor del riesgo que éstas representan?
☐	¿Se ha valorado el riesgo residual resultante de aplicar las salvaguardas?

	NOTA: La forma habitual de presentar el resultado de aplicar las salvaguardas es mediante un Plan de Tratamiento de Riesgos (PTR), que contiene el riesgo inicial, las salvaguardas determinadas para mitigarlo y el riesgo residual. Adicionalmente, para su seguimiento, el PTR suele contener el responsable de cada salvaguarda, su prioridad, las fechas de inicio y final, el estado en que se encuentra su implementación (planificada, en proceso, finalizada), etc.		
Op.pl.1.r2	**Para categoría ALTA, ¿se ha realizado un análisis de riesgos formal, con una metodología específica en base a un fundamento matemático estandarizado y reconocido internacionalmente?**		☐ SI ☐ NO
☐	¿Se han valorado no solo las amenazas más probables, sino también las posibles dentro de lo razonable?		
☐	¿Se ha comparado el riesgo residual con el apetito de riesgo para determinar si todavía están presentes riesgos inaceptables por la organización que deban seguir tratándose?		
☐	Además de valorarse el riesgo residual, ¿se ha asumido formalmente éste? *NOTA: Una práctica habitual es que sea el Comité de Seguridad quien asuma en su caso la gestión completa de riesgos, incluyendo el plan para tratarlos: El apetito de riesgo, el riesgo inicial, las salvaguardas y los riesgos residuales resultantes.*		

Op.pl.2	**Arquitectura de seguridad**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Planos de CPD y salas técnicas, incluyendo sus instalaciones (climatización, extinción, alimentación eléctrica, etc.). ☐ Documentación y diagramas de red, incluyendo comunicaciones y líneas de defensa. ☐ Documentos de arquitectura del sistema.		
	☐ Procedimiento de gestión de la documentación. ☐ Posible relación de documentos del sistema de gestión aplicado sobre el sistema de información. ☐ Informes de auditorías internas realizadas, especialmente del año que no coincide con la auditoría de certificación. ☐ Registro de seguimiento de las acciones correctivas, y de mejora, detectadas en las auditorías internas.		
	☐ Informes de auditorías internas del sistema, realizadas cada año. ☐ Registro de seguimiento de las acciones correctivas, y de mejora, detectadas en las auditorías. ☐ Evidencias de acciones de mejora del SGSI que no provengan de las auditorías internas o externas. ☐ Evidencias de controles técnicos de validación de entrada, intermedios o de salida.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**

Op.pl.2 (NI)	**¿Se dispone de documentación y diagramas en el ámbito del sistema de información, incluyendo instalaciones físicas, equipos, comunicaciones y líneas de defensa?**		☐ SI ☐ NO
☐ (NI)	¿Se dispone de documentación de las instalaciones, incluyendo áreas y puntos de acceso? *NOTA: Especial mención a los CPD, otras salas técnicas y de comunicaciones, salas de monitorización, zonas de carga y descarga, zonas de acceso público, etc.*		
☐ (NI)	¿Se dispone de documentación y diagramas del sistema, incluyendo equipos (servidores, estaciones de trabajo, etc.), diferentes redes internas y conexiones externas, puntos de acceso, consolas de administración, etc.		
☐ (NI)	¿Se dispone de documentación y diagramas de las líneas de defensa, puntos de interconexión a otros sistemas o a otras redes, incluyendo internet o redes públicas en general, cortafuegos, balanceadores, enrutadores, segmentación de redes, etc.? *NOTA1: Los diagramas deberían contener el direccionamiento IP de los diferentes componentes y pueden ser documentos, el resultado de consultas mediante herramientas gráficas de análisis y monitorización de redes, o una combinación de ambos.* *NOTA2: Este tipo de diagramas son información sensible que debe ser custodiada, dado que su conocimiento por terceros no autorizados podría favorecer a un posible atacante.*		
☐	Para quienes desarrollan software (soluciones con cierta complejidad como puede ser un ERP para gestionar ayuntamientos), ¿se dispone de diagramas con la estructura de capas y módulos de la solución, incluyendo las capas de integración o interfaces para comunicarse con otras soluciones o elementos, como pueden ser firma electrónica, interoperabilidad, etc.?		
☐	¿Se dispone de documentación de los sistemas 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, incluyendo el detalle de los protocolos de acceso empleados como, por ejemplo, LDAP?		
Op.pl.2.r1	**¿Se dispone de un sistema de gestión de seguridad de la información aplicado sobre el/los sistemas(s) de información?**		☐ SI ☐ NO
☐	¿Se realizan auditorías internas de cumplimiento del ENS, contemplando todos los requisitos aplicables según la categoría del sistema y las posibles exclusiones justificadas, si se materializan éstas el año que no corresponde la auditoría de certificación (que es bienal)?		
☐	¿Se realizan auditorías internas de cumplimiento del ENS, contemplando al menos la mitad de los requisitos aplicables según la categoría del sistema y las posibles exclusiones justificadas, si se materializan éstas anualmente?		
☐	¿Se realiza el seguimiento de las consecuentes acciones correctivas y de mejora derivadas de las auditorías internas, persiguiendo la mejora continua del sistema?		

Op.pl.2.r2	**¿Se dispone de un sistema de gestión de seguridad de la información, orientado a la mejora continua, aplicado sobre el/los sistemas(s) de información?**		☐ SI ☐ NO
☐	¿Se realizan auditorías internas de cumplimiento del ENS, contemplando todos los requisitos aplicables según la categoría del sistema y las posibles exclusiones justificadas, si se materializan éstas el año que no corresponde la auditoría de certificación (que es bienal)?		
☐	¿Se realiza el seguimiento de las consecuentes acciones correctivas y de mejora derivadas de las auditorías internas, persiguiendo la mejora continua del sistema?		
☐	¿Se realizan otras acciones encaminadas a la mejora continua del sistema?		
Op.pl.2.r3	**¿Se dispone de controles técnicos internos para aumentar la seguridad?**		☐ SI ☐ NO
☐	¿Los controles técnicos internos validan los datos de entrada, incluyendo rangos y formatos válidos? *NOTA: Los controles técnicos de validación podrían complementarse con soluciones de análisis de comportamiento de los usuarios.*		
☐	¿Los controles intermedios se aplican a la interoperabilidad entre aplicaciones del Sistema de Información, verificando rangos y formatos válidos de intercambio de información, rechazando aquellos no previstos?		
☐	¿Los mensajes de error de las aplicaciones, especialmente las del tipo web expuestas a Internet, proporcionan únicamente un código que pueda consultarse al CAU o al servicio de soporte, sin mostrar información explícita y detallada del tipo de error producido, que pueda darle pistas a un posible atacante?		
☐	¿Los mensajes de error en la autenticación de un usuario, se limitan a señalar que alguno de los datos introducido no es correcto o, por el contrario, identifica explícitamente que el error está en alguno concreto de ellos (por ejemplo, en el ID de usuario o en la contraseña)?		

Op.pl.3	**Adquisición de nuevos componentes**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Detalle del proceso de adquisiciones. ☐ Evidencia de adquisiciones acordes a la arquitectura y, en su caso, contemplando adicionalmente formación. ☐ Evidencia de adquisiciones alineadas con los activos contemplados en el análisis de riesgos o con el PTR. ☐ Caso del sector público, evidencias de pliegos de prescripciones técnicas (PPT) y de pliegos de cláusulas administrativas particulares (PCAP) correspondientes a los últimos procesos de adquisición de productos y/o servicios.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**

Op.pl.3 NI	**¿Se realiza una planificación previa a la adquisición de nuevos componentes del sistema, teniendo en cuenta, por ejemplo, la obsolescencia de los actualmente en producción, la finalización de contratos, los cambios del contexto, etc.?**		☐ SI ☐ NO
☐	¿El proceso de adquisición tiene en cuenta las conclusiones del análisis de riesgos, o bien trae a causa que deba realizarse una nueva iteración de dicho análisis, debido a los cambios que introduce en el sistema de información?		
☐	Para los nuevos componentes a ser adquiridos ¿se verifica que sean acordes o compatibles con la arquitectura de seguridad implementada o escogida para la organización?		
☐	¿Se dispone de un proceso formalizado de planificación para la adquisición de nuevos componentes?		
☐ NI	¿El proceso de adquisiciones contempla conjuntamente las necesidades de financiación, de formación y las técnicas (características, configuración, soporte y mantenimiento)? *NOTA: La principal razón de ser de esta medida es que no se realicen adquisiciones de componentes en la organización considerando únicamente cuestiones económicas, sino que se base en razones técnicas que contemplen requisitos de seguridad para minimizar el riesgo.*		

Op.pl.4	**Dimensionamiento / gestión de la capacidad**		
Categoría / dimensión **D**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Estudio previo de capacidad, contemplando todos los aspectos necesarios. ☐ Evidencia de adquisiciones dimensionadas de forma alineada con el estudio previo.		
	☐ Plan de Capacidad, contemplando todos los aspectos necesarios. ☐ Evidencia de herramientas de monitorización de la capacidad.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.pl.4 NI	**Con carácter previo a la entrada en producción del sistema ¿se consideran las necesidades de capacidad?**		☐ SI ☐ NO
☐ NI	¿Se han considerado las necesidades de software y hardware, al menos con carácter previo a la puesta en explotación de los sistemas? *NOTA: Se entiende por software y hardware a las aplicaciones, CPU y memoria de servidores y estaciones de trabajo, VM necesarias, balanceadores de ser necesarios, etc.*		

☐	¿Se ha realizado un estudio respecto a las necesidades de almacenamiento de información durante procesamiento y durante el período que deba retenerse, al menos con carácter previo a la puesta en explotación de los sistemas?		
☐	¿Se ha realizado un estudio respecto a las necesidades de capacidad de procesamiento, ya sea en hosts físicos, entornos virtualizados, o entornos de computación en la Nube, al menos con carácter previo a la puesta en explotación del sistema?		
☐	¿Se ha realizado un estudio respecto a las necesidades de comunicaciones (líneas y ancho de banda necesario), al menos con carácter previo a la puesta en explotación del sistema?		
☐	¿Se ha realizado un estudio respecto a las necesidades de personal y carga de trabajo en cuánto a su número y cualificaciones profesionales, al menos con carácter previo a la puesta en explotación del sistema?		
☐	¿Se ha realizado un estudio respecto a las necesidades de instalaciones, al menos con carácter previo a la puesta en explotación del sistema? *NOTA: Se entiende por necesidad de instalaciones a la posibilidad de adición de racks a los CPD, bahías libres en racks existentes, número de bocas libres en conmutadores, número máximo de VPN contra un cortafuegos, además de potencia frigorífica suficiente en los CPD, % de carga libre en los SAI, etc.*		
Op.pl.4.r1	**¿Se puede evidenciar que el estudio de capacidad no solo se realiza con carácter previo a la entrada en producción del sistema, sino que se mantiene actualizado durante todo el ciclo de vida del mismo?**		☐ SI ☐ NO
☐	¿Se puede evidenciar la existencia de un Plan de Capacidad, que se mantiene actualizado durante todo el ciclo de vida del sistema?		
☐	¿Se emplean herramientas y recursos para la monitorización de la capacidad? *NOTA: La monitorización es básica para poder elaborar un plan de capacidad. Incluso existen herramientas que conservan datos históricos y permiten ver tendencias gráficamente, durante determinado período de tiempo seleccionado, posibilitando así poder tomar decisiones respecto a la previsión del consumo de recursos y su posible necesidad de ampliación.*		

Op.pl.5	**Componentes certificados**
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐
Propuesta de evidencias	
	☐ Evidencia de inclusión en el catálogo CPSTIC como producto cualificado (o aprobado). ☐ Evidencia de otras certificaciones reconocidas de producto o servicio.
	☐ Evidencia de producto aprobado libre de emanaciones TEMPEST. ☐ Evidencia de lista de componentes Software.

	Aspectos a evaluar	Hallazgos del auditor / referencia a las evidencias	Cumple
Op.pl.5 NI	**¿Se utiliza 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 deban formar parte de la arquitectura de seguridad del sistema?**		☐ SI ☐ NO
☐ NI	¿Se emplea el catálogo CPSTIC para seleccionar productos de terceros, o servicios externos, que formen parte de la arquitectura de seguridad? *NOTA: El catálogo CPSTIC se publica como guía CCN-STIC 105, estando sujeta a un proceso de actualización frecuente.*		
☐ NI	¿Caso de no existir en el catálogo CPSTIC, o ante cualquier causa de fuerza mayor, se emplean otros productos certificados según se indica en el art. 19 del RD 311/2022, de 3 de mayo? *NOTA: En dicho supuesto podrían ser aceptables productos al corriente de otras certificaciones de seguridad de producto, como es Common Criteria (norma ISO/IEC 15408), u otras equivalentes de índole internacional, que no sean del propio fabricante.*		
☐	Si el sistema suministra un servicio de seguridad a un tercero, bajo el alcance del ENS, ¿el producto o productos que se suministren dicho servicio han sido incluidos en el CPSTIC tras superar un proceso de cualificación, o bien aportan una certificación que cumple con los requisitos funcionales de seguridad y de aseguramiento de acuerdo a lo establecido en el art. 19 del RD 311/2022, de 3 de mayo?		
☐	¿En los casos en los que no existan productos o servicios certificados se tienen en cuenta las taxonomías de referencia y se han formalizado qué criterios se van a llevar a cabo por los responsables de la organización?		
Op.pl.5.r1	**¿Se protege la información frente a amenazas TEMPEST de acuerdo a la normativa en vigor?** *NOTA: Se entiende por amenazas TEMPEST aquellas 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 por cauces no previstos.* *NOTA: Un método utilizado a menudo para la protección TEMPEST es el acondicionamiento de equipos y locales con diferentes sistemas de apantallamiento, ya sean temporales o permanentes. Algunos de los sistemas más utilizados son:* • *Armarios apantallados* • *Salas apantalladas.*		☐ SI ☐ NO

	• *Apantallamientos fuertes, como Jaulas de Faraday.* • *Apantallamientos débiles, como telas o pinturas metalizadas.*		
Op.pl.5.r2	**¿Cada producto y servicio incluye en su descripción una lista de componentes software empleados (módulos, librerías, etc.), acorde a lo especificado en [mp.sw.1.r5]?** *NOTA: El objetivo de esta medida es llegar a determinar que una vulnerabilidad anunciada (CVE), detectada en un módulo, componente o librería de desarrollo, pueda tener afectación a las aplicaciones actualmente empleadas en la organización.*		☐ SI ☐ NO

6.2.2.2 Marco operacional (CONTROL DE ACESO)

Op.acc.1	**Identificación**		
Categoría / dimensión **T A**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia de métodos de identificación. ☐ Evidencia de que los identificadores son únicos. ☐ Evidencia de deshabilitación de cuentas y su control hasta la supresión definitiva. ☐ Protocolo o sistemática empleada para las bajas de usuarios		
	☐ Procedimiento formal de bajas de usuarios ☐ Listas actualizadas de usuarios para acceder a diferentes recursos		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.acc.1 (NI)	**¿Se dispone de un control de acceso comprendiendo un conjunto de actividades preparatorias y ejecutivas tendentes a permitir o denegar a una entidad, usuario o proceso, el acceso a un recurso del sistema para la realización de cualquier acción?**		☐ SI ☐ NO

☐	Si se utiliza un identificador único, ¿se emplean métodos de identificación previstos en la normativa de aplicación, entre ellos, sistemas de clave concertada y cualquier otro que las administraciones consideren válido? *NOTA: Se considerarán válidos en los términos y condiciones establecidos en la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas y otras normas que la desarrollen.*
☐ NI	Cada entidad (entidad, usuario o proceso) que accede al sistema, ¿cuenta con un identificador singular que permita conocer el destinatario y asignarle los derechos de acceso que le correspondan?
☐	Cuando el usuario tiene diferentes roles frente al sistema (como ciudadano o usuario final, como trabajador del organismo o como administrador de los sistemas, por ejemplo), ¿se le asignan identificadores singulares para cada perfil, de forma que se recaben los correspondientes registros de actividad en base a los privilegios correspondientes a cada perfil para poder conocer las acciones realizadas?
☐ NI	Cuando el usuario deja la organización, cuando el usuario cesa en la función para la cual se requería la cuenta de usuario o, cuando la persona que la autorizó da orden en sentido contrario ¿Son deshabilitadas/bloqueadas inmediatamente las cuentas de usuario?
☐ NI	Una vez deja de ser necesaria una cuenta, ¿Se retiene deshabilitada durante un período finito y determinado para atender a las necesidades de trazabilidad de los registros asociados a la misma, antes de su eliminación?
☐	En las comunicaciones electrónicas, ¿las partes intervinientes se identifican con los mecanismos previstos alineados con el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo (Reglamento eIDAS) y con la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza? *NOTA: La correspondencia entre la dimensión de seguridad AUTENTICIDAD del ENS y el nivel de seguridad del referido Reglamento Europeo, será respectivamente: bajo con BAJO del ENS, sustancial o alto con MEDIO del ENS, y alto con ALTO del ENS.*

Op.acc.1.r1	**¿La identificación del usuario permite al Responsable del sistema y/o al Responsable de la seguridad del sistema singularizar a la persona asociada al mismo, así como sus responsabilidades en el sistema?**		☐ SI ☐ NO

☐	¿Los datos de identificación son utilizados por el sistema para determinar los privilegios del usuario conforme a los requisitos de control de acceso establecidos en la documentación de seguridad?
☐	¿Se dispone de una lista actualizada de usuarios autorizados para acceder a los diferentes recursos, mantenida por el personal de administración (Responsable/Administrador del Sistema y/o Responsable/Administrador de la Seguridad del sistema)? *NOTA: Puede llevarse a cabo con ayuda de herramientas y utilidades centralizadas.*

Op.acc.2	**Requisitos de acceso**		
Categoría / dimensión **C I T A**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia de mecanismos de protección de los recursos. ☐ Evidencia de asignación de responsables de los recursos. ☐ Evidencia de criterios de acceso a los recursos.		
	☐ Evidencia de atributos de seguridad de los usuarios (individuales y de grupo). ☐ Evidencia de granularidad de un usuario respecto a sus privilegios de acceso.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.acc.2 (NI)	**¿Los recursos del sistema están protegidos con algún mecanismo que impida su utilización, salvo por las entidades que disfruten de derechos de acceso suficientes?**		☐ SI ☐ NO
☐	¿Se han determinado y se conocen las personas responsables de los diferentes recursos del sistema de información?		
☐ (NI)	¿Los derechos de acceso de cada recurso, se establecen según las decisiones de la persona responsable del recurso, ateniéndose a la política y/o normativa de seguridad del sistema?		
☐	¿Se controla el acceso a los componentes del sistema operativo, y a sus ficheros o registros de configuración?		
Op.acc.2.r1	**¿Se gestionan los privilegios de los usuarios de forma armonizada con los recursos del sistema a los que tengan, o no, necesidad de acceder?**		☐ SI ☐ NO
☐	¿Disponen todos los usuarios autorizados de un conjunto de atributos de seguridad (privilegios) que puedan ser mantenidos individualmente?		
☐	¿Se han implementado los privilegios de acceso de modo que restrinjan con la suficiente granularidad el tipo de acceso que un usuario pueda tener (lectura, escritura, modificación, borrado, etc.)?		
Op.acc.2.r2	**¿Se dispone de soluciones que permiten establecer controles de acceso a los dispositivos en función de la política de seguridad de la organización?**		☐ SI ☐ NO

Op.acc.3	**Segregación de funciones y tareas**		
Categoría / dimensión **C I T A**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Organigrama detallado de la organización que evidencie la segregación de funciones		
	☐ Evidencia de la existencia y control de cuentas con privilegios de auditoría. ☐ Evidencia de acceso, mediante cuentas de administración, únicamente desde determinados dispositivos.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.acc.3 (NI)	**¿Se segregan aquellas funciones que, ante determinadas circunstancias, podrían culminar en conflicto de interés como, por ejemplo, desarrollo y operación?**		☐ SI ☐ NO
☐ (NI)	¿Se evita, siempre que sea posible, que las capacidades de desarrollo y operación recaigan en la misma persona o en el mismo equipo? *Nota: Cuando no sea posible, la organización deberá evidenciarlo.*		
☐ (NI)	¿Se evita, siempre que sea posible, ¿que las personas que autorizan sean las mismas que controlan el uso? *Nota: Cuando no sea posible, la organización deberá evidenciarlo*		
Op.acc.3.r1	**¿Se previenen más circunstancias de conflicto de interés, como puede ser, evitando concurran las funciones de configuración y las de mantenimiento?**		☐ SI ☐ NO
☐	¿Se evita, siempre que sea posible, que una misma persona aúne funciones de configuración y de mantenimiento del sistema? *Nota: Cuando no sea posible, la Organización deberá evidenciarlo.*		
☐	¿Quienes realizan funciones de auditoría o supervisión, no realizan ninguna otra función relacionada con lo auditado o supervisado? *Nota: Esto afecta, en relación a las auditorías, especialmente al auditor interno, ya sea éste de la propia organización o contratado como prestación de servicios a una empresa externa. Las entidades de certificación acreditadas (EC), así como los Órganos de Auditoría Técnica reconocidos (OAT) del Sector Público, ya están implícitamente segregados, a la vez que disponen de mecanismos para preservar la independencia e imparcialidad.*		
Op.acc.3.r2	**¿Se controlan las cuentas con privilegios y los mecanismos desde los cuales se pueden autenticar?**		☐ SI ☐ NO
☐	¿Se dispone de cuentas con privilegios de auditoría, estrictamente controladas y personalizadas?		

	Nota: Estas cuentas de auditoría son especialmente indicadas para auditorías técnicas, dado que en las auditorías de cumplimiento no se requiere acceso al sistema de información. En estas últimas el auditor solicita que desea ver y es el auditado quien accede y muestra, habitualmente de forma interactiva, aunque la auditoría sea en remoto.		
Op.acc.3.r3	**¿Se controlan el acceso a la información de seguridad del sistema?**		☐ SI ☐ NO
☐	El acceso a la información de seguridad del sistema ¿está permitido únicamente a los administradores de seguridad y/o administradores del sistema autorizados, utilizando los mecanismos de acceso imprescindibles? *NOTA: Se consideran mecanismos de acceso imprescindibles aquellos que se han acordado para mantener la operativa, minimizando el riesgo al reducirse la superficie de exposición. Pueden ser la consola, una interfaz web, acceso remoto, etc.).*		

Op.acc.4	**Proceso de gestión de derechos de acceso**		
Categoría / dimensión **C I T A**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia de auditorías de revisión de los permisos de acceso. ☐ Evidencia de concesiones y revocaciones de accesos por el personal autorizado. ☐ En su caso, la política de control de acceso. ☐ En su caso, la política de acceso remoto.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.acc.4 NI	**¿Se gestionan los derechos de acceso, en base al principio de mínimo privilegio?**		☐ SI ☐ NO
☐ NI	¿Está cualquier acceso prohibido, salvo que se disponga de autorización expresa?		
☐ NI	¿Se aplica una política de mínimo privilegio que reduce al mínimo imprescindible para cumplir con sus obligaciones los privilegios de cada entidad, usuario o proceso?		
☐ NI	¿Se asignan los privilegios de forma que las entidades, usuarios o procesos únicamente acceden al conocimiento de aquella información requerida para cumplir sus obligaciones o funciones?		

	NOTA: en base a los principios de necesidad de conocer y responsabilidad de compartir, siendo la información patrimonio de la organización, toda aquella y sólo aquella que resulte necesaria para el usuario, estará a su disposición con las medidas de seguridad correspondientes.
☐ NI	¿Únicamente el personal con competencia para ello, puede conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por el responsable de los mismos?
☐	¿Se revisan los permisos de acceso de forma periódica?
☐	¿Se ha establecido una política específica de acceso remoto, que señale la obligación de requerirse autorización expresa?

Op.acc.5	**Mecanismos de autenticación (usuarios externos)**		
Categoría / dimensión **C I T A**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia del proceso de entrega y aceptación de credenciales por los usuarios. ☐ Evidencia de deshabilitación / retirada de credenciales a los usuarios. ☐ Políticas técnicas configuradas mostrando cómo se limita el número de intentos y se fuerza cambio de credenciales. ☐ Evidencia de que la información suministrada en los accesos está restringida al mínimo imprescindible. ☐ Política técnica configurada mostrando complejidad de contraseñas acorde con la política establecida. ☐ Evidencia de empleo de contraseñas de un solo uso (OTP). ☐ Evidencia de que los certificados empleados son cualificados. ☐ Evidencia de que se configuran los certificados protegidos mediante un segundo factor (p.ej. PIN). ☐ Evidencia de empleo de certificados cualificados en soporte físico, protegidos mediante un segundo factor.		
	☐ Evidencia de que el sistema registra los accesos con éxito y los fallidos ☐ Evidencia de que se informa al usuario del último acceso efectuado con su identidad.		
	☐ Evidencia de que se han definido puntos en los que el sistema requiere una renovación de la autenticación, si procede. ☐ Evidencia de suspensión de las credenciales tras un período definido de no utilización.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.acc.5 NI	**¿Se mantiene la seguridad de las cuentas y las credenciales de los usuarios externos, mediante mecanismos de control de acceso?**		☐ SI ☐ NO

☐ NI	¿Se activan las credenciales únicamente cuando éstas están bajo el control exclusivo y efectivo del usuario, o se fuerza un cambio de credenciales al primer acceso del mismo?
☐	Antes de activar el mecanismo de autenticación, ¿el usuario reconoce que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, la protección de su confidencialidad y el deber de notificación inmediata en caso de pérdida?
☐	Antes de proporcionar las credenciales de autenticación a las entidades, usuarios o procesos, ¿se identifican y registran éstos previamente de manera fidedigna ante el sistema, ante un Prestador Cualificado de Servicios de Confianza, o en un proveedor de identidad electrónica? *NOTA: Dicho proveedor ha de ser reconocido por las administraciones públicas, de conformidad con lo dispuesto en la Ley 39/2015, de 1 de octubre.*
☐	¿Se dispone de evidencias de que el usuario reconoce que ha recibido las credenciales y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, protección de su confidencialidad y notificación inmediata en caso de pérdida?
☐ NI	¿Se cambian las credenciales con la periodicidad marcada por la política de la organización?
☐ NI	¿Se retiran y deshabilitan las credenciales cuando se detecta su pérdida o falta de control exclusivo por parte del usuario?
☐ NI	¿Se retiran y deshabilitan las credenciales cuando la entidad (persona, equipo o proceso) que se autentica termina su relación con el sistema?
☐	¿La información suministrada en los accesos se restringe a la mínima imprescindible? *NOTA: Se evita todo aquello que pueda revelar información sobre el sistema o la cuenta, sus características, su operación o su estado. Las credenciales solamente se validarán cuando se tengan todos los datos necesarios y, si se rechaza, no se informará del motivo del rechazo.*
☐ NI	¿Se limita el número de intentos permitidos, bloqueando la oportunidad de acceso una vez superado tal número, requiriendo una intervención específica para reactivar la cuenta, que se describe en la documentación?
☐ NI	¿Informa el sistema al usuario de sus obligaciones inmediatamente después de obtener éste el acceso?
NOTA: Para categorías BÁSICA y MEDIA, debe cumplirse al menos con una de las medidas de refuerzo R1, R2, R3 o R4, que siguen a continuación, mientras que, para categoría ALTA, se requiere cumplir con R2 o R3 o R4 y siempre con R5.	
Op.acc.5.r1 NI	**¿Se emplea una contraseña como mecanismo de autenticación, con garantías razonables?** ☐ SI ☐ NO
☐ NI	¿Se imponen normas de complejidad mínima y robustez, frente a ataques de adivinación?

Op.acc.5.r2 NI	**¿Se requiere una contraseña de un solo uso (OTP) como complemento a la contraseña de usuario?**		☐ SI ☐ NO
Op.acc.5.r3 NI	**¿Se emplean certificados cualificados como mecanismo de autenticación?**		☐ SI ☐ NO
☐ NI	¿Se le facilitan las credenciales al usuario tras un registro previo, presencial o telemático, usando certificado electrónico cualificado		
☐ NI	¿El uso del certificado está protegido por un segundo factor, del tipo PIN o biométrico?		
Op.acc.5.r4 NI	**¿Se emplean certificados en soporte físico (tarjeta o similar) como mecanismo de autenticación?**		☐ SI ☐ NO
☐ NI	¿Los certificados emplean algoritmos, parámetros y dispositivos autorizados por el CCN? *NOTA: Se relacionan en la guía CCN-STIC 807 sobre Criptología de empleo en el ENS.*		
☐ NI	¿Se le facilitan las credenciales al usuario tras un registro previo, presencial o telemático, usando certificado electrónico cualificado?		
☐ NI	¿El uso del certificado está protegido por un segundo factor, del tipo PIN o biométrico?		
Op.acc.5.r5	**¿Se registran los accesos, o su intento, y se informa al usuario?**		☐ SI ☐ NO
☐	¿El sistema registra los accesos con éxito y los fallidos?		
☐	¿Se le informa al usuario del último acceso efectuado con su identidad?		
Op.acc.5.r6	**¿Se definen puntos en los que el sistema requiere una renovación de la autenticación del usuario?**		☐ SI ☐ NO
Op.acc.5.r7	**¿Se suspenden las credenciales tras un período definido de no utilización?**		☐ SI ☐ NO

Op.acc.6	Mecanismos de autenticación (usuarios de la organización)		
Categoría / dimensión **C I T A**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia del proceso de entrega y aceptación de credenciales por los usuarios. ☐ Evidencia de deshabilitación / retirada de credenciales a los usuarios. ☐ Políticas técnicas configuradas mostrando cómo se limita el número de intentos y se fuerza el cambio de credenciales. ☐ Evidencia de que la información suministrada en los accesos está restringida al mínimo imprescindible. ☐ Evidencia de doble factor de autenticación.		
	☐ Evidencias de registros de acceso. ☐ Evidencia de que se informa al usuario del último acceso.		
	☐ Evidencias de que se aplica la ITS de interconexión de sistemas de información, cuando ésta se promulgue, o en su defecto la guía CCN-STIC 811 sobre Interconexión en el ENS. ☐ Evidencia de que para el acceso remoto se requiere autorización específica, se cifra su tráfico, se recogen pistas de auditoría y es deshabilitado fuera de los períodos establecidos de utilización.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.acc.6 NI	**¿Se dispone implementados mecanismos de control de acceso, alineados con el proceso de altas y bajas de empleados / usuarios internos de la organización?**		☐ SI ☐ NO
☐ NI	¿Se activan las credenciales únicamente cuando éstas están bajo el control exclusivo y efectivo del usuario, o se fuerza un cambio de credenciales al primer acceso del mismo?		
☐	Antes de proporcionar las credenciales a los usuarios, ¿estos han conocido y aceptado la política de seguridad del organismo en los aspectos que les afecten?		
☐	¿Reconoce el usuario que ha recibido las credenciales y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, protección de su confidencialidad y notificación inmediata en caso de pérdida?		
☐ NI	¿Se cambian las credenciales con la periodicidad marcada por la política de la organización?		
☐ NI	¿Se retiran y deshabilitan las credenciales cuando la entidad (persona, equipo o proceso) que se autentica termina su relación con el sistema?		

☐ NI	¿Se deshabilitan o regeneran las credenciales cuando se detecta o sospecha su pérdida o revelación a personas no autorizadas?		
☐	¿Se previenen ataques que puedan revelar información del sistema sin llegar a acceder al mismo? ¿la información suministrada en los accesos se restringe a la mínima imprescindible?		
☐ NI	¿Se limita el número de intentos permitidos, bloqueando la oportunidad de acceso una vez superado tal número, requiriendo la intervención de los administradores de seguridad para reactivar la cuenta?		
☐	¿Informa el sistema al usuario de sus obligaciones inmediatamente después de obtener éste el acceso?		
NOTA: Para categorías BÁSICA, debe cumplirse al menos con una de las medidas de refuerzo R1, R2, R3 o R4 y siempre con R8 y R9; para categoría MEDIA, se requiere cumplir con una de las medidas R1, R2, R3 o R4 y siempre con R5, R8 y R9; mientras que para categoría ALTA cumplir con una de las medidas R1, R2, R3, o R4 y siempre con R5, R6, R7, R8 y R9.			
Op.acc.6.r1 NI	**¿Se emplea una contraseña como mecanismo de autenticación, con garantías razonables?**		☐ SI ☐ NO
☐ NI	Si se emplea una contraseña como mecanismo de autenticación, ¿se verifica que el acceso se realiza únicamente desde zonas controladas y sin atravesar zonas no controladas?		
☐ NI	Si se emplean contraseñas o similares, ¿se imponen normas de longitud, complejidad mínima y robustez, frente a ataques de adivinación?		
Op.acc.6.r2 NI	**¿Se requiere 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»?**		☐ SI ☐ NO
Op.acc.6.r3 NI	**¿Se emplean certificados cualificados como mecanismo de autenticación?**		☐ SI ☐ NO
☐	¿Se encuentra protegido el uso del certificado mediante un segundo factor, del tipo PIN o biométrico?		
Op.acc.6.r4 NI	**¿Se emplean certificados cualificados en soporte físico (tarjeta o similar) como mecanismo de autenticación?**		☐ SI ☐ NO

☐	¿Se encuentra protegido el uso del certificado mediante un segundo factor, del tipo PIN o biométrico?		
Op.acc.6.r8 (NI)	**¿Se requiere un doble factor de autenticación para el acceso desde zonas no controladas (R2, R3 o R4)?** *NOTA: Se entiende por zona controlada aquella que no es de acceso público, sino que para llegar al equipo desde el que se accede, el usuario se ha identificado de alguna forma (control de acceso a las instalaciones) diferente al mecanismo de autenticación lógica frente al sistema.*		☐ SI ☐ NO
Op.acc.6.r9 (NI)	**Respecto a los accesos remotos ¿Se contemplan aspectos de seguridad y autorización?**		☐ SI ☐ NO
☐	¿Se han implementado los requisitos de seguridad que resultan de la aplicación de la ITS de Interconexión de sistemas de información, cuando ésta se promulgue, o en su defecto la guía CCN-STIC 811 sobre Interconexión en el ENS?		
☐ (NI)	¿Los accesos remotos son autorizados por la autoridad correspondiente en la organización?		
☐ (NI)	¿Está cifrado el tráfico de los accesos remotos? *NOTA: Por ejemplo, mediante el empleo de Redes Privadas Virtuales (VPN).*		
☐	Si la utilización de determinado acceso remoto no se produce de manera constante, ¿se encuentra éste deshabilitado, volviéndole a habilitar únicamente cuando sea necesario?		
☐	¿Se recogen registros de auditoría de este tipo de conexiones?		
Op.acc.6.r5	**¿Se registran las trazas de acceso y se informa de la más reciente al usuario?**		☐ SI ☐ NO
☐	¿Se registran tanto los accesos fallidos, como los que han tenido éxito?		
☐	¿Se informa al usuario del último acceso realizado con su identidad?		
Op.acc.6.r6	**¿Se han definido aquellos puntos en los que el sistema requiere de una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión establecida?**		☐ SI ☐ NO
Op.acc.6.r7	**¿Se suspenden las credenciales tras un periodo definido de no utilización?**		☐ SI ☐ NO

6.2.2.3 Marco Operacional (EXPLOTACIÓN)

Op.exp.1	**Inventario de activos**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia del inventario de activos, que incluya al responsable de cada activo. ☐ Evidencia de verificaciones periódicas del inventario.		
	☐ Evidencia de herramienta de monitorización / descubrimiento de activos. ☐ Evidencia de herramienta que muestre relaciones y dependencias entre activos.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.exp.1 (NI)	**¿Se dispone de un inventario de todos los elementos del sistema?** *NOTA: Es admisible el concepto de inventario federado, que consiste en la suma de varios inventarios independientes que en su conjunto constituyen el inventario completo, aunque siempre es más efectivo disponer de un único inventario con diferentes criterios de acceso a los activos.*		☐ SI ☐ NO
☐ (NI)	¿Se mantiene el inventario de activos actualizado, quedando claramente definido quién(es) tiene(n) dicha responsabilidad?		
☐	Especialmente para categorías MEDIA y ALTA, ¿se realizan verificaciones periódicas respecto a la exactitud del inventario? *NOTA: Algunas herramientas de inventario disponen de funciones de autodescubrimiento de los activos presentes en la red.*		
☐ (NI)	¿Se detalla en el inventario la naturaleza de cada activo, identificando a su responsable? *NOTA: Se entiende por responsable del activo a la persona que toma las decisiones relativas al mismo.*		
Op.exp.1.r1	**¿Forma parte del inventario el etiquetado del equipamiento y del cableado?**		☐ SI ☐ NO
Op.exp.1.r2	**¿Se dispone de herramientas que permitan visualizar de forma continua el estado de todos los equipos en la red?** *NOTA: en particular, interesa visualizar al menos servidores y dispositivos de red y de comunicaciones.*		☐ SI ☐ NO

Op.exp.1.r3	**¿Se dispone de herramientas que permitan categorizar los activos críticos por contexto de la organización y riesgos de seguridad?** *NOTA: Un inventario puede ser textual o gráfico (mostrando relaciones entre activos y sus dependencias); en este segundo caso estaríamos refiriéndonos a una Base de Datos de Gestión de la Configuración (CMDB). La identificación de activos de algunas herramientas de gestión de riesgos, disponen de algunas de dichas funcionalidades.*		☐ SI ☐ NO
Op.exp.1.r4	**¿Se mantiene actualizada una relación formal de los componentes software de terceros, empleados en el despliegue del sistema?** *Nota Esta lista incluirá librerías software y los servicios requeridos para su despliegue (plataforma o entorno operacional).*		☐ SI ☐ NO

Op.exp.2	**Configuración de seguridad**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia de guías de bastionado, particularizadas a los equipos relevantes del sistema. ☐ Evidencia de listas de comprobación cumplimentadas (checklist) de los equipos bastionados. ☐ Evidencias al azar, solicitadas por el auditor, para verificar que diferentes aspectos considerados en las guías de bastionado se hayan configurado en la realidad.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.exp.2 NI	**¿Se realiza una configuración de seguridad (bastionado) a los equipos, previamente a su puesta en producción?**		☐ SI ☐ NO
☐ NI	¿Se han configurado los equipos, previamente a su entrada en operación, retirándoles cuentas y contraseñas standard?		
☐	¿Se han configurado los equipos, previamente a su entrada en operación, aplicándoles la regla de 'mínima funcionalidad', es decir, que el sistema proporcione la funcionalidad mínima imprescindible para que la organización alcance sus objetivos?		

NI	*NOTA: la 'mínima funcionalidad' se traduce en que el sistema no proporcione funciones injustificadas (de operación, administración o auditoría) al objeto de reducir al mínimo su superficie de exposición, eliminándose o desactivándose aquellas funciones que sean innecesarias o inadecuadas al fin que se persigue.*
☐ NI	¿Se han configurado los equipos, previamente a su entrada en operación, de manera que se aplique la regla de 'seguridad por defecto'? *NOTA: La 'seguridad por defecto' se concreta estableciendo medidas de seguridad respetuosas con el usuario y que le protejan, salvo que éste se exponga conscientemente a un riesgo; En otras palabras, para reducir la seguridad el usuario tiene que realizar acciones conscientes, por lo que el uso natural, en los casos que el usuario no ha consultado el manual, ni realizado acciones específicas, será un uso seguro.*
☐	¿Se han configurado y gestionado las máquinas virtuales, previamente a su entrada en operación, de un modo igual de seguro al empleado para las máquinas físicas? *NOTA: La gestión del parcheado, cuentas de usuarios, software antivirus, etc. se realizará como si se tratara de máquinas físicas, incluyendo la máquina anfitriona.*

Op.exp.3	**Gestión de la configuración de seguridad**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Registros (quizás en una herramienta de *ticketing*) que evidencien la gestión continua de la configuración de seguridad. ☐ Informes de Auditoria de bastionado		
	☐ Informe de verificaciones de ausencia de elementos no autorizados en el sistema. ☐ Lista de servicios autorizados en servidores y en estaciones de trabajo.		
	☐ Evidencia del número e identificación de los administradores de las configuraciones de seguridad del sistema operativo y las aplicaciones. ☐ Evidencia de la realización de copias de seguridad de las configuraciones.		
	☐ Evidencia de herramienta o procedimiento de actualización de la configuración de seguridad. ☐ Evidencia de herramientas de monitorización de la seguridad.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.exp.3 NI	**¿Se gestiona de forma continua la configuración de los componentes del sistema?**		☐ SI ☐ NO
☐	¿Se gestiona de forma continua la configuración de los componentes del sistema, manteniéndose en todo momento la regla de 'funcionalidad mínima'?		

NI	*NOTA: la 'mínima funcionalidad' se traduce en que el sistema no proporcione funciones injustificadas (de operación, administración o auditoría) al objeto de reducir al mínimo su perímetro de exposición, eliminándose o desactivándose aquellas funciones que sean innecesarias o inadecuadas al fin que se persigue.*		
☐	¿Se gestiona de forma continua la configuración de los componentes del sistema, manteniéndose en todo momento la regla de 'mínimo privilegio'?		
☐ NI	¿Se gestiona de forma continua la configuración de los componentes del sistema, de modo que el sistema se adapta a las posibles nuevas necesidades, previamente autorizadas?		
☐ NI	¿Se gestiona de forma continua la configuración de los componentes del sistema, de modo que el sistema reacciona a posibles vulnerabilidades notificadas?		
☐ NI	¿Se gestiona de forma continua la configuración de los componentes del sistema, de modo que el sistema reacciona a posibles incidentes?		
☐ NI	¿Se gestiona de forma continua la configuración de los componentes del sistema, de modo que la configuración de seguridad únicamente puede editarse por personal debidamente autorizado?		
Op.exp.3.r1	**¿Se dispone, para los componentes del sistema, de configuraciones autorizadas, mantenidas y verificadas, junto a la identificación de servicios autorizados?**		☐ SI ☐ NO
☐	¿Se dispone de configuraciones hardware/software autorizadas y mantenidas regularmente para los servidores, elementos de red y estaciones de trabajo?		
☐	¿Se verifica periódicamente la configuración hardware/software del sistema, para asegurarse que no se han introducido ni instalado elementos no autorizados?		
☐	¿Se mantiene una lista de servicios autorizados para servidores y estaciones de trabajo?		
Op.exp.3.r2	**¿Se han establecido responsabilidades sobre la configuración de seguridad del sistema?**		☐ SI ☐ NO
☐	¿La configuración de seguridad del sistema operativo y aplicaciones, tanto de estaciones y servidores, como de la electrónica de red del sistema, es responsabilidad de un número muy limitado de administradores del sistema?		
Op.exp.3.r3	**¿Se realizan copias de seguridad de la configuración del sistema?**		☐ SI ☐ NO
☐	¿Se realizan copias de seguridad de la configuración del sistema de forma que sea posible reconstruir éste, en parte o en su totalidad, tras un incidente?		
Op.exp.3.r4	**¿Se mantiene actualizada la configuración de seguridad del sistema operativo y de las aplicaciones?**		☐ SI ☐ NO

☐	¿La configuración de seguridad del sistema operativo y de las aplicaciones se mantiene actualizada a través de una herramienta automática, o mediante un procedimiento manual, que permite la instalación de las correspondientes modificaciones de versión y actualizaciones de seguridad oportunas?		
Op.exp.3.r5	**¿Se dispone de herramientas de monitorización de la seguridad?**		☐ SI ☐ NO
☐	¿Se dispone de herramientas que permitan conocer el estado de seguridad de la configuración de los dispositivos de red de forma periódica y, en el caso de que resulte deficiente, poder corregirlo?		

Op.exp.4	**Mantenimiento y actualizaciones de seguridad**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencias de contratos de mantenimiento del equipamiento físico y lógico relevante. ☐ Protocolo o sistemática seguida para la actualización y mantenimiento de los sistemas. ☐ Evidencias de actualizaciones.		
	☐ Evidencia de pruebas de preproducción previas a la instalación de parches o versiones completas. ☐ Procedimiento formal de actualización y mantenimiento de sistemas.		
	☐ Evidencias de planes de vuelta atrás previos a la actualización de sistemas.		
	☐ Evidencias de actualización del firmware de los dispositivos.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.exp.4 (NI)	**¿Se realiza, de forma sistemática, el mantenimiento del equipamiento físico y lógico del sistema?**		☐ SI ☐ NO
☐ (NI)	¿En lo relativo a instalación y mantenimiento del equipamiento físico y lógico que constituye el sistema, se atiende a las especificaciones de los fabricantes? *NOTA: Esta atención se concreta en un seguimiento continuo de los anuncios de defectos. Se entiende por mantenimiento del equipamiento, por ejemplo, a la liberación de espacio en disco cuando sea necesario, limpieza de archivos obsoletos, comprobación de las luces de estado en las máquinas físicas, verificación del funcionamiento correcto de aparatos, instalación de parches de seguridad cuando se requiera, etc.*		
☐	¿Se dispone de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones? *NOTA: La priorización debe tener en cuenta la variación del riesgo en función de la aplicación o no del parche o de la actualización disponible.*		
☐	¿El mantenimiento es realizado únicamente por personal debidamente autorizado?		

Op.exp.4.r1	**Antes de poner en producción una nueva versión o una versión parcheada, ¿se comprueba en un entorno de prueba controlado, consistente en cuanto a configuración con el entorno de producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario?**		☐ SI ☐ NO
Op.exp.4.r2	**Antes de la aplicación de las configuraciones, parches y actualizaciones de seguridad, ¿se prevé un mecanismo de vuelta atrás para revertirlos en caso de la aparición de efectos adversos?**		☐ SI ☐ NO
Op.exp.4.r3	**¿Se comprueba de forma periódica la actualización e integridad del firmware utilizado en los dispositivos hardware del sistema (infraestructura de red, BIOS, etc.)?**		☐ SI ☐ NO
Op.exp.4.r4	**¿Se despliega una estrategia de monitorización continua de amenazas?** *NOTA: ¿Esta detalla los indicadores críticos de seguridad a emplear, la política de aplicación de parches de seguridad y los criterios de revisión regular y excepcional de las amenazas sobre el sistema?*		☐ SI ☐ NO

Op.exp.5	**Gestión de cambios**
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐
Propuesta de evidencias	
	☐ Evidencia de un registro de peticiones de cambio (RFC), quizá en una herramienta de *ticketing*. ☐ Evidencia de aprobación adicional de los cambios de riesgo ALTO de forma previa antes de su implantación por parte del Responsable de Seguridad.

	☐ Informes de pruebas de preproducción. ☐ Evidencia de informes de riesgos asociados a determinados cambios. ☐ Informes de pruebas de aceptación. ☐ Evidencia de actualización de configuración (inventario, manuales, diagramas de red…), tras un cambio implementado. ☐ Actas de posibles reuniones del CAB o de quienes tienen asignada la potestad de autorizar los cambios.		
	☐ Evidencia de plan de marcha atrás respecto a un cambio. ☐ Evidencia de comunicación de fallos al Responsable de Seguridad. ☐ Evidencia de documentación del impacto de los cambios en la seguridad del sistema.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.exp.5 NI	**¿Se gestionan los cambios que se realizan en el sistema de información?**		☐ SI ☐ NO
☐ NI	¿Se planifican los cambios para reducir el impacto sobre la prestación de los servicios afectados? ¿Se han definido ventanas de mantenimiento acordadas con los usuarios? *NOTA: Para ello, todas las peticiones de cambio se registrarán asignándoseles un número de referencia que permita su seguimiento, de forma equivalente a como se registran los incidentes.*		
☐	Para cada petición de cambio ¿se registra suficiente información para que quien deba autorizarla no tenga dudas al respecto y pueda gestionarla hasta su desestimación o implementación?		
☐	Las pruebas de preproducción, siempre que sea posible realizarlas, ¿se efectúan en equipos equivalentes a los de producción, al menos en los aspectos específicos del cambio?		
☐	¿Se determina mediante análisis de riesgos si los cambios son relevantes para la seguridad del sistema? ¿Se puede evidenciar que aquellos cambios que implican una situación de riesgo ALTO son aprobados explícitamente, de forma previa a su implementación, por el Responsable de Seguridad además de quienes tengan competencia asignada para ello?		
☐	Una vez implementado un cambio, ¿Se realizan las pruebas de aceptación convenientes?		
☐	Si las pruebas de aceptación son positivas, ¿se actualiza la documentación de configuración (diagramas de red, manuales, el inventario, etc.), siempre que proceda?		
Op.exp.5.r1	**¿Se prevé algún mecanismo de vuelta atrás de los cambios, se documentan éstos y se notifican al Responsable de Seguridad los fallos detectados?**		☐ SI ☐ NO
☐	Antes de la aplicación de los cambios, ¿se prevé un mecanismo de vuelta atrás para revertirlos en caso de la aparición de efectos adversos?		

☐	Tras la implantación de un cambio ¿son comunicados al responsable designado en la estructura de seguridad todos los fallos detectados en el software y en el hardware?
☐	¿Se documentan todos los cambios, incluyendo una valoración del impacto que dicho cambio supone en la seguridad del sistema?

Op.exp.6	**Protección frente a código dañino**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de Evidencias			
	☐ Evidencia en los equipos de la instalación de una solución antimalware para su protección. ☐ Evidencia de consola centralizada de la solución antimalware y su configuración. ☐ Licencia de uso de la solución antimalware, con número máximo de equipos gestionados.		
	☐ Normativas, procedimientos o instrucciones que regulen la gestión de la protección antimalware. ☐ Contrato o acuerdo de soporte de la solución antimalware. ☐ Informes generados por la solución antimalware.		
	☐ Evidencia de verificaciones de la solución antimalware. ☐ Evidencia de otras soluciones antimalware adicionales, por ejemplo, en el FW. ☐ Lista blanca de aplicaciones autorizadas.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.exp.6 (NI)	**¿Se dispone de una solución de protección contra código dañino (antivirus, EDR o solución similar) desplegada en todos los puestos de trabajo, servidores y elementos perimetrales del sistema?**		☐ SI ☐ NO
☐ (NI)	¿Se ha configurado la solución antimalware instalada en los puestos de usuario de forma adecuada, implementando protección en tiempo real de acuerdo a las recomendaciones del fabricante y las características del entorno operativo?		
☐ (NI)	¿Se ha instalado dicho software de protección frente a código dañino en todos los equipos, incluyendo puestos de usuario, servidores y elementos perimetrales?		
☐	¿Se trata de una solución corporativa con consola centralizada de administración?		

☐ NI	¿Se requiere una contraseña de administración o se dispone de cualquier otro mecanismo que impida que el usuario final detenga o altere el funcionamiento de la solución?		
☐ NI	La licencia de uso de la solución ¿cubre la totalidad de equipos operativos presentes en la organización?		
☐	¿Se dispone de garantías de que todo fichero procedente de fuentes externas será analizado antes de trabajar con él?		
☐	¿Está amparada la solución antimalware por un acuerdo de soporte y actualización, tanto del software cómo de la base de datos de detección?		
☐	¿Los elementos de seguridad, como los cortafuegos (FW), disponen de solución antimalware especializada que, por ejemplo, verifique navegación web y correos recibidos?		
☐	¿Se verifica regularmente la configuración de la(s) solución(es) antimalware para garantizar que se adecuan a las operaciones de los sistemas protegidos?		
☐	¿Se comprueba regularmente que las bases de datos de detección de código dañino se estén actualizando con la frecuencia prevista?		
Op.exp.6.r1	**¿Se ejecutan análisis y escaneos, de forma regular en los sistemas, en búsqueda de código dañino?**		☐ SI ☐ NO
☐	¿Existe algún mecanismo o procedimiento que escanee regularmente los sistemas para detectar código dañino?		
☐	¿Se revisan regularmente los informes de resultados generados como consecuencia de los escaneos de los sistemas, así como otra información generada de forma consolidada desde la consola de administración?		
Op.exp.6.r2	**Al arrancar los sistemas, ¿se analizan las funciones críticas en prevención de modificaciones no autorizadas?**		☐ SI ☐ NO
Op.exp.6.r3	**¿Se ha implementado una lista blanca que impida la ejecución de aplicaciones no autorizadas previamente y, en consecuencia, que no estén en dicha lista?**		☐ SI ☐ NO
Op.exp.6.r4	**¿Se han implementado soluciones de seguridad orientadas a detectar, investigar y resolver actividades sospechosas en los equipos (EDR - Endpoint Defense and Response)?**		☐ SI ☐ NO
Op.exp.6.r5	**¿La solución antimalware, además de implementar protección en tiempo real, permite realizar configuraciones avanzadas y revisar el sistema al arrancar, así como cada vez que se conecte algún dispositivo extraíble?**		☐ SI ☐ NO

Op.exp.7	**Gestión de incidentes**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Proceso de tratamiento de incidentes. ☐ Evidencia de que se distinguen y tratan adecuadamente los incidentes que afecten a datos personales.		
	☐ Evidencia de instrumentos para notificar incidentes al CCN-CERT cuando corresponda. ☐ Evidencia de que se dispone de una completa gestión de incidentes.		
	☐ Evidencia de recursos (procedimientos, casos de uso, etc.) de configuración dinámica del sistema ante incidentes, que podrían apoyarse, si es posible, en determinados scripts.		
	☐ Evidencia de herramientas que automaticen la configuración dinámica del sistema ante alertas o incidentes.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.exp.7 NI	**¿Se dispone de un proceso integral para tratar los incidentes que puedan tener un impacto en la seguridad del sistema?**		☐ SI ☐ NO
☐ NI	¿Se dispone 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?		
☐ NI	La gestión de incidentes que afecten a datos personales, ¿tiene en cuenta lo dispuesto en el RGPD y en la LO 3/2018 (LOPDGDD), en especial su disposición adicional primera, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en el RD 311/2022, de 3 de mayo?		
Op.exp.7.r1	**¿Se dispone de soluciones de ventanilla única para la notificación de incidentes al CCN-CERT? ¿permite la distribución de notificaciones a las diferentes entidades de manera federada, si es el caso, utilizando para ello dependencias administrativas jerárquicas?**		☐ SI ☐ NO
Op.exp.7.r2	**El proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, ¿consiste en una completa gestión de los mismos?**		☐ SI ☐ NO
☐	El proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, ¿incluye la implementación de medidas urgentes según convenga al caso?		

	NOTA: Se entiende por medidas urgentes la posibilidad de detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, etc.		
☐	El proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, ¿incluye la asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente?		
☐	El proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, ¿incluye instrumentos o directrices para informar a los responsables de la información y servicios afectados, respecto al incidente acaecido y las actuaciones llevadas a cabo para su resolución?		
☐	El proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, ¿incluye medidas para prevenir que se repita el incidente, incluir en los procedimientos de usuario la identificación y forma de tratar el incidente y actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes?		
Op.exp.7.r3	**¿Dispone la organización de recursos para la configuración dinámica del sistema, reaccionando a anuncios de ciberamenazas y/o a la detección de las mismas?**		☐ SI ☐ NO
☐	¿Dispone la organización de procedimientos y casos de uso que permitan, de forma manual o semiautomática, apoyándose en determinados casos en scripts, la configuración dinámica del sistema de modo que se detenga, desvíe, o limite el ataque lo antes posible? *NOTA: 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.*		
☐	¿La organización adapta los procedimientos de reconfiguración dinámica reaccionando a los anuncios recibidos del CCN-CERT relativos a ciberamenazas sofisticadas y campañas de ataques?		
Op.exp.7.r4	**¿Se dispone de herramientas que automaticen el proceso de prevención y respuesta, mediante la detección e identificación de anomalías, segmentación dinámica de la red para reducir la superficie de ataque, el aislamiento de dispositivos críticos, etc.?**		☐ SI ☐ NO

Op.exp.8	**Registro de la actividad**
Categoría / dimensión **T**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐
Propuesta de evidencias	
	☐ Evidencia de los registros de actividad conservados.

	☐ Evidencia de configuración de los registros de actividad (LOGS) en los servidores.		
	☐ Evidencia de revisión de los registros de actividad centralizados. ☐ Evidencia de servidores NTP o equivalentes. ☐ Documentación de seguridad del sistema sobre gestión de registros de actividad. ☐ Evidencia de protección del acceso a los registros de actividad		
	☐ Evidencia de herramientas de análisis de LOGS. ☐ Evidencia de sistemas automáticos de recolección de registros y correlación de eventos (tipo SIEM).		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.exp.8 (NI)	**¿Se registran los eventos y actividades de usuarios y entidades que acceden a los sistemas?**		☐ SI ☐ NO
☐ (NI)	¿Se registran las actividades del sistema generando un registro de auditoría que incluye, al menos, el identificador del usuario o entidad asociado al evento, fecha y hora, sobre qué información se realiza el evento, tipo de evento y el resultado del evento (fallo o éxito), según la política de seguridad y los procedimientos asociados a la misma?		
☐ (NI)	¿Se han activado los registros de actividad en los servidores?		
Op.exp.8.r1	**¿Se gestionan los registros de actividad?**		☐ SI ☐ NO
☐	¿Se dispone de un almacenamiento centralizado de registros de actividad que facilite su análisis y revisión? ¿se realiza una revisión, aunque sea informal, de dichos registros? *NOTA1: por ejemplo, un servidor centralizado de registros y tal vez un panel de control donde se visualicen aspectos relevantes de los registros de actividad, lo que ha de permitir detectar posibles patrones anormales y anomalías con mayor facilidad. Por ejemplo, una posible detección es aislar de forma centralizada todos los logs de acceso fuera del horario laboral y durante los festivos, para aquellas organizaciones cuyo desempeño no sea 24x7.* *NOTA2: La medida [op.mon.3], sobre Vigilancia, complementa a esta medida*		
Op.exp.8.r2	**¿Se sincronizan los relojes del sistema?**		☐ SI ☐ NO
☐	¿Dispone el sistema de elementos de referencia de tiempo (servidores NTP, sellado de tiempo…) para facilitar las funciones de registro de eventos y auditoría? *NOTA: La modificación de la referencia de tiempo del sistema debe ser una función de administración y, en caso de realizarse su sincronización con otros dispositivos, deberán utilizarse mecanismos de autenticación e integridad.*		

Op.exp.8.r3	**En la documentación de seguridad del sistema, ¿se indican los eventos de seguridad que serán auditados y el tiempo de retención de los registros antes de ser eliminados?**		☐ SI ☐ NO
Op.exp.8.r4	**Los registros de actividad y, en su caso, las copias de seguridad ¿únicamente pueden ser accedidos, alterarse o eliminarse por personal debidamente autorizado?**		☐ SI ☐ NO
Op.exp.8.r5	**¿Se dispone de herramientas para apoyar la gestión de los registros de actividad?**		☐ SI ☐ NO
☐	¿El sistema implementa herramientas para analizar y revisar de forma centralizada la actividad del sistema y la información de auditoría en búsqueda de comprometimientos de la seguridad posibles o reales?		
☐	¿Se dispone de un sistema automático de recolección de registros, correlación de eventos y respuesta automática ante los mismos, como puede ser un SIEM?		

Op.exp.9	**Registro de la gestión de incidentes**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia de que se registran los incidentes clasificándolos por tipología. ☐ Evidencia de acciones adoptadas, en base al análisis de los incidentes registrados.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.exp.9 (NI)	**¿Se realiza un proceso de extracción de conclusiones y aprendizaje, a partir de los incidentes de seguridad registrados?**		☐ SI ☐ NO
☐ (NI)	¿Se registran los reportes iniciales, intermedios y finales, las actuaciones de emergencia y las modificaciones del sistema derivadas de un incidente?		
☐	¿Se registran aquellas evidencias que pueda dirimirse en un ámbito jurisdiccional, especialmente cuando el incidente pueda comportar acciones disciplinarias sobre el personal interno, sobre proveedores externos o en la persecución de delitos? *NOTA: En la determinación de la composición y detalle de estas evidencias, así como la forma de preservar la cadena de custodia, se recurrirá a asesoramiento legal especializado y/o a peritos judiciales.*		
☐	Como consecuencia del análisis de los incidentes, ¿se revisan aquellos eventos que deben seguir auditándose y la necesidad de reducirlos o incrementarlos?		

☐ NI	¿Se realiza un aprendizaje, a partir del análisis de los incidentes registrados, que permita poner de manifiesto aspectos a mejorar en la seguridad del sistema?
☐ NI	Para aprender de los incidentes, ¿se registran éstos indicando su tipología concreta y no solo diferenciando los de seguridad de los que no lo son? *NOTA: Se dispone de una clasificación o taxonomía de los ciberincidentes en la guía CCN-STIC 817 Gestión de ciberincidentes.*

Op.exp.10	**Protección de claves criptográficas**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia de gestión segura de claves criptográficas.		
	☐ Evidencia de algoritmos empleados para generación de claves.		
	☐ Evidencia de cifradores empleados.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.exp.10 NI	**¿Se gestionan de forma segura las claves criptográficas?**		☐ SI ☐ NO
☐	¿Se protegen las claves criptográficas durante todo su ciclo de vida? *NOTA: El ciclo de vida comprende (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.*		
☐	¿Los medios de generación de claves están aislados de los medios de explotación? *NOTA: Se consideran medios aislados, por ejemplo, el disponer de CA independiente en caso de generación de certificados propios.*		
☐	Las claves retiradas de operación que deban ser archivadas, ¿lo son en medios aislados de los de explotación?		
Op.exp.10.r1	**¿Se emplean algoritmos y parámetros autorizados por el CCN para generar las claves criptográficas?**		
Op.exp.10.r2	**¿Se emplean cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación?** *NOTA: Por ejemplo, se dispone de la guía CCN-STIC 807 Criptología de empleo en el Esquema Nacional de Seguridad.*		

6.2.2.4 Marco Operacional (RECURSOS EXTERNOS)

Op.ext.1	**Contratación y acuerdos de nivel de servicio**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencias de acuerdos de nivel de servicio (ANS/SLA) suscritos con proveedores. ☐ Certificados de conformidad con el ENS de los sistemas de proveedores relevantes.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.ext.1 NI	**¿Se suscriben acuerdos de nivel de servicio con los proveedores, a la vez que se les requiere estar en posesión del correspondiente certificado de conformidad respecto al ENS?**		☐ SI ☐ NO
☐ NI	Con anterioridad a la efectiva utilización de los recursos externos, ¿se establece contractualmente un Acuerdo de Nivel de Servicio (ANS/SLA) que incluya las características del servicio prestado, lo que debe entenderse como 'servicio mínimo admisible', así como, la responsabilidad del proveedor y las consecuencias de eventuales incumplimientos?		
☐	¿Se exige a los proveedores, relevantes para el ENS, que estén en posesión de la correspondiente certificación de conformidad para el sistema de información que soporta los servicios prestados a la organización, con igual o superior categoría y alcance suficiente?		

Op.ext.2	**Gestión diaria**
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐
Propuesta de evidencias	
	☐ Evidencia de seguimiento de proveedores. ☐ Actas de posibles reuniones de seguimiento con un proveedor. ☐ Informes de gestión/informes de nivel de servicio, proporcionado por el proveedor. ☐ Evidencia de designación del punto de contacto del proveedor (POC) ☐ Evidencia de mecanismo establecido para notificar incidentes al proveedor (portal cliente, correo electrónico…). ☐ Evidencia de incidentes abiertos a un proveedor y su seguimiento.

	Aspectos a evaluar	Hallazgos del auditor / referencia a las evidencias	Cumple
Op.ext.2 (NI)	**¿Se dispone de mecanismos de seguimiento y supervisión del desarrollo del servicio, así como de reporte y coordinación ante posibles incidencias?**		☐ SI ☐ NO
☐	¿Se dispone de 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? *NOTA: Algunos proveedores facilitan, de motu proprio o bajo solicitud, informes de cumplimiento del servicio.*		
☐	¿Se ha establecido un mecanismo y los procedimientos de coordinación necesarios para llevar a cabo las tareas de mantenimiento de los sistemas comprendidos en el acuerdo, que contemplarán los supuestos de ocurrencia de posibles incidentes y desastres?		
☐	¿Se ha designado por parte del proveedor un punto de contacto (POC) para cualquier cuestión relacionada con el servicio? ¿Se ha establecido el mecanismo establecido de contacto, especialmente para notificar incidentes del servicio?		
☐	¿Se ha pactado con proveedores la entrega periódica de informes de servicio?		
☐	¿Se realizan reuniones de seguimiento con determinados proveedores relevantes?		

Op.ext.3	**Protección de la cadena de suministro**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Estudio de impacto respecto a producirse un posible incidente en los proveedores. ☐ Evidencia de que se contempla en el BIA la dependencia de proveedores. ☐ Análisis de riesgos incluyendo proveedores y posible Plan de Tratamiento (PTR) de los riesgos asociados a la cadena de suministro.		
	☐ Plan de Continuidad con referencia a la cadena de suministro. ☐ Pruebas del Plan de continuidad en relación al escenario de indisponibilidad proveedores.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.ext. 3 (NI)	**¿Se analizan los riesgos y se adoptan medidas respecto a un posible incidente originado en la cadena de suministro?**		☐ SI ☐ NO
☐	¿Se puede evidenciar que se analiza el impacto que puede tener sobre el sistema un incidente accidental o deliberado que tenga su origen en la cadena de suministro?		

	NOTA: Suele analizarse incluyendo a la cadena de suministro en el Análisis de Riesgos, así como en el BIA (caso de disponerse de él).		
☐	¿Se puede evidenciar que se estiman los riesgos sobre el sistema por causa de un incidente accidental o deliberado que tenga su origen en la cadena de suministro? *NOTA: Suele analizarse incluyendo a la cadena de suministro en el Análisis de Riesgos*		
☐	¿Se puede evidenciar que se adoptan medidas de contención de los impactos estimados sobre el sistema debido a un incidente accidental o deliberado que tenga su origen en la cadena de suministro? *NOTA: Estas medidas habitualmente se encontrarán en el Plan de Tratamiento de Riesgos (PTR).*		
Op.ext.3.r1	**¿Se considera la cadena de suministro en el Plan de Continuidad de la organización y en sus pruebas?**		☐ SI ☐ NO
☐	¿El Plan de Continuidad de la organización tiene en cuenta la dependencia de proveedores externos críticos?		
☐	¿Se realizan pruebas o ejercicios de continuidad, incluyendo escenarios en los que falla un proveedor?		
Op.ext.3.r2	**¿Se ha implementado 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?**		☐ SI ☐ NO
Op.ext.3.r3	**¿Se mantiene actualizado un registro formal que contiene 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]?** *NOTA Esta lista será proporcionada por el proveedor de la aplicación, librería o producto suministrado*		☐ SI ☐ NO

Op.ext.4	**Interconexión de sistemas**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia de autorizaciones de interconexiones. ☐ Evidencia de documentación de las interconexiones.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**

Op.ext.4 NI	**¿Requieren autorización y se documentan todas las interconexiones de sistemas?** *NOTA: Se dispone la Guía CCN-STIC 811 sobre Interconexión en el ENS*		☐ SI ☐ NO
☐	¿Son objeto de una autorización previa todos los intercambios de información y prestación de servicios con otros sistemas? *NOTA: Todo flujo de información estará prohibido salvo autorización expresa.*		
☐	¿Se documenta explícitamente para cada interconexión las características de la interfaz, los requisitos de seguridad y protección de datos y la naturaleza de la información intercambiada?		
Op.ext.4.r1	**Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, ¿se acompañan las medidas de seguridad locales de los correspondientes mecanismos y procedimientos de coordinación para la atribución y ejercicio efectivos de las responsabilidades de cada sistema?**		☐ SI ☐ NO

6.2.2.5 Marco Operacional (SERVICIOS EN LA NUBE)

Op.nub.1	**Protección de servicios en la nube**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Informe o checklist de verificación de requisitos de seguridad de la solución en la nube. ☐ Evidencia de conformidad con el ENS de la solución en la nube. ☐ Evidencia de pruebas de penetración.		
	☐ Certificado de conformidad con el ENS del sistema de información que soporta la solución en la nube. ☐ Referencia a inclusión en el catálogo CPSTIC si es una solución de seguridad en la nube.		
	☐ Evidencia del empleo de las guías CCN-STIC para la configuración de seguridad del sistema en la nube.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**

Op.nub.1 NI	**¿Los sistemas de información que soportan servicios prestados desde la nube cumplen con las medidas de seguridad pertinentes?**		☐ SI ☐ NO
☐ NI	Los servicios Cloud que se consumen, ¿disponen de una configuración de seguridad implementada de acuerdo a las guías CCN-STIC que sean de aplicación o a las recomendaciones del fabricante?		
☐ NI	Los sistemas de información que soportan servicios en la nube suministrados por terceros ¿son conformes con el ENS, o cumplen con las medidas desarrolladas en una guía CCN-STIC, que incluirá, entre otros, requisitos relativos a pruebas de penetración (pentesting), transparencia, cifrado y gestión de claves, así como, jurisdicción de los datos?		
Op.nub.r1	**¿Están certificados los servicios en la nube suministrados por terceros?**		☐ SI ☐ NO
☐	Los servicios en la nube suministrados por terceros, ¿Están 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, o el sistema de información que los soporta está certificado del ENS?		
☐	Si el servicio en la nube es un servicio de seguridad ¿Cumple con los requisitos establecidos en [op.pl.5] correspondientes a certificación de seguridad?		
Op.nub.r2	**La configuración de seguridad de los sistemas que proporcionan servicios en la nube. ¿se realiza según la correspondiente Guía CCN-STIC de Configuración de Seguridad Específica, orientadas tanto al usuario como al proveedor?**		☐ SI ☐ NO

6.2.2.6 Marco Operacional (CONTINUIDAD DEL SERVICIO)

Op.cont.1	**Análisis de impacto**		
Categoría / dimensión **D**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Análisis de Impacto en el Negocio (BIA), incluyendo cálculos de RTO y RPO, con su fecha de actualización. ☐ Diagrama de dependencias de los activos que soportan los servicios. ☐ Evidencia de aprobación del BIA.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**

Op.cont.1 (NI)	**¿Se ha realizado un análisis de impacto (BIA) en los servicios en el ámbito del ENS?**		☐ SI ☐ NO
☐	¿El análisis de impacto (BIA) se actualiza al menos cada año y siempre que varíen las circunstancias, de modo que permita en todo momento determinar los requisitos de disponibilidad de cada servicio (impacto de una interrupción durante un periodo de tiempo determinado)?		
☐	Como consecuencia del BIA ¿se determinan los elementos que son críticos para la prestación de cada servicio? ¿se han determinado las dependencias entre ellos de forma que se pongan de manifiesto los elementos que son críticos para la prestación de los servicios?		

Op.cont.2	**Plan de continuidad**		
Categoría / dimensión **D**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Plan de Continuidad acorde con el BIA. ☐ Otros planes de continuidad de la organización vinculados. ☐ Evidencias de formación relacionada con el Plan de Continuidad.		
	☐ Planes de Recuperación (DRP) específicos, de emergencia, etc., asociados al Plan de Continuidad general. ☐ Evidencias de comprobaciones tras la discontinuidad del sistema.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.cont.2 (NI)	**¿Se dispone de un Plan de Continuidad documentado, coherente con los resultados del BIA?**		☐ SI ☐ NO
☐ (NI)	En el Plan de Continuidad ¿se identifican las funciones, responsabilidades y actividades a realizar?		
☐	En el Plan de Continuidad ¿existe 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, aunque sea con menor rendimiento?		
☐	En el Plan de Continuidad ¿todos los medios alternativos están planificados y se han materializado mediante acuerdos o contratos con los proveedores correspondientes?		
☐	¿Las personas afectadas por el Plan de Continuidad reciben formación específica relativa a su papel en dicho plan?		
☐	¿El Plan de Continuidad es parte integral y armónica de los planes de continuidad de la organización, armonizados con otras materias ajenas a la seguridad?		
☐	El Plan de Continuidad ¿es acorde con los resultados del BIA?		

Op.cont.2.r1	**Partiendo del Plan de Continuidad general ¿existen definidos planes de emergencia, contingencia o recuperación, en consonancia?** *NOTA: Si se realiza el Plan de Continuidad considerando diferentes escenarios de contingencia, puede establecerse para dichos escenarios un conjunto de Planes de Recuperación ante Desastres (DRP) específicos.*		☐ SI ☐ NO
Op.cont.2.r2	**Ante una caída o discontinuidad del sistema, ¿se comprueba la integridad del sistema operativo, firmware y ficheros de configuración de los equipos afectados?**		☐ SI ☐ NO

Op.cont.3	**Pruebas periódicas**		
Categoría / dimensión **D**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Informe de las pruebas de continuidad, con relación de fases y su duración individual, además de la total de la prueba. ☐ Comparativa de las pruebas con los RTO obtenidos en el BIA. ☐ Posibles *tickets* con acciones correctivas, consecuencia de pruebas del Plan de Continuidad no satisfactorias.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.cont.3 NI	**¿Se realizan pruebas periódicas del Plan de Continuidad?**		☐ SI ☐ NO
☐	¿Se puede evidenciar la realización de pruebas periódicas para localizar y, en su caso, corregir los errores o deficiencias que puedan existir entre lo previsto en el plan y el resultado de ejecutarlo?		
☐	¿Las pruebas de continuidad se planifican con antelación, dividiéndose en fases, para poder incidir en aquellas que sean más determinantes con miras a poder reducir los tiempos de recuperación, caso de constatar durante la prueba que se incumplen los RTO establecidos en el BIA?		
☐ NI	¿Se elabora un informe al finalizar la prueba del plan, que indique claramente aquellos aspectos que se pueden mejorar o, en su caso, corregir? ¿Se toma en cuenta los resultados de las pruebas para alinear estos tiempos con lo identificado en los BIAS?		

☐	¿Se registran en alguna herramienta las acciones correctivas o de mejora necesarias, para poder efectuar su seguimiento?

Op.cont.4	**Medios alternativos**		
Categoría / dimensión **D**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Inventario constando los medios alternativos involucrados en la recuperación. ☐ Contratos y cuerdos de nivel de servicio de los medios alternativos contratados a terceros. ☐ Evidencia de personal alternativo. ☐ Evidencia de instalaciones alternativas. ☐ Evidencia de medios de comunicaciones alternativos.		
	☐ Evidencia de transferencia automática a los medios alternativos.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.cont.4 (NI)	**¿Está prevista la disponibilidad de medios alternativos para poder seguir prestando servicio cuando los medios habituales no estén disponibles?**		☐ SI ☐ NO
☐	¿Se dispone inventario de los medios alternativos y sus componentes están actualizados?		
☐ (NI)	¿Se ha establecido un tiempo máximo para que los medios alternativos entren en funcionamiento?		
☐	¿Los medios alternativos están sometidos a las mismas garantías de seguridad que los medios originales?		
Op.cont.4	**¿Se cubren los elementos relevantes del sistema?**		☐ SI ☐ NO
☐	¿Se cubren los servicios contratados a terceros?		
☐	¿Se dispone de instalaciones alternativas?		
☐	¿Se dispone de personal alternativo?		
☐	¿Se dispone de equipamiento informático alternativo?		
☐	¿Se dispone de medios de comunicación alternativos		

Op.cont.4.r1	**¿Dispone el sistema de elementos hardware y/o software que permitan la transferencia de los servicios automáticamente a los medios alternativos?**		☐ SI ☐ NO

6.2.2.7 Marco Operacional (MONITORIZACIÓN DEL SISTEMA)

Op.mon.1	**Detección de intrusión**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia de la herramienta de IPS/IDS. ☐ Para el sector público, posible evidencia de sonda tipo SAT-INET del CCN-CERT.		
	☐ Evidencia de las reglas definidas en el IPS/IDS.		
	☐ Evidencia del procedimiento de respuesta a las alertas generadas por el IDS.		
	☐ Evidencia de acciones automáticas generadas por el IDS.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.mon.1.1 (NI)	**¿Se dispone de herramientas de detección y/o prevención de intrusiones (IDS/IPS)?**		☐ SI ☐ NO
☐ (NI)	¿Se dispone de elementos que analicen el tráfico de red y muestren eventos de seguridad en caso de detectar posibles intrusiones en la misma? *NOTA: Por ejemplo, sondas IDS/IPS, capacidad IDS/IPS en los cortafuegos, panel de monitorización de eventos en Cloud, sonda SAT-INET del CCN-CERT, etc.*		
Op.mon.1.r1	**¿Dispone el sistema de herramientas de detección y/o prevención de intrusiones basadas en reglas?**		☐ SI ☐ NO
☐	¿Se han configurado reglas específicas para la generación de eventos de seguridad y la detección de intrusiones?		
Op.mon.1.r2	**¿Se dispone de procedimientos de respuesta a las alertas generadas por el sistema de detección y/o prevención de intrusiones?**		☐ SI ☐ NO
Op.mon.1.r3	**¿El sistema ejecuta <u>automáticamente</u> acciones predeterminadas de respuesta a las alertas generadas**		☐ SI ☐ NO

	por las herramientas de detección y/o prevención de intrusiones? *NOTA: Dichas acciones automáticas pueden incluir la finalización del proceso que está ocasionando la alerta, la inhabilitación de determinados servicios, la desconexión de usuarios y el bloqueo de cuentas.*		

Op.mon.2	**Sistema de métricas**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia del nivel de implementación de las medidas, por ejemplo, adicionando a la Declaración de Aplicabilidad una columna específica con el 'grado de implementación' o, en su defecto, el 'nivel de madurez'. ☐ Evidencia de la recopilación de información para el informe INES.		
	☐ Evidencia de métricas e indicadores asociados a la gestión de incidentes. ☐ Evidencia de métricas e indicadores asociados a los recursos destinados a la seguridad.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.mon.2 (NI)	**Atendiendo a la categoría de seguridad del sistema, ¿se recopilan los datos necesarios para conocer el grado de implementación de las medidas de seguridad que resulten aplicables y, en su caso, tratándose de organizaciones en el ámbito del ENS para proveer el informe anual requerido por el artículo 32 (Informe INES)?**		☐ SI ☐ NO
Op.mon.2.r1	**¿Se evalúa el comportamiento del sistema de gestión de incidentes implementado en la organización?**		☐ SI ☐ NO
☐	¿Se recopilan los datos precisos que posibiliten evaluar el comportamiento del sistema de gestión de incidentes, de acuerdo con la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad y con la correspondiente guía CCN-STIC? *NOTA: Se dispone de la guía CCN-STIC 817 Gestión de ciberincidentes donde se muestra una serie de métricas e indicadores relacionados.*		

Op.mon.2.r2	**¿Se evalúa la eficiencia del sistema de gestión de la seguridad?**		☐ SI ☐ NO
☐	¿Se recopilan los datos precisos para conocer la eficiencia del sistema de seguridad, en relación con los recursos consumidos, en términos de horas y presupuesto?		

Op.mon.3	**Vigilancia**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia del sistema empleado para recolección de eventos de seguridad.		
	☐ Evidencia del sistema de correlación de LOGS. ☐ Evidencia de sistemas de detección y análisis de vulnerabilidades.		
	☐ Evidencia de sistema de generación de alertas según el tráfico de red. ☐ Evidencia de contrato de prestación de servicios de vigilancia y monitorización remota, tipo SOC, de estar externalizado ☐ Evidencia de limitación y monitorización de posibilidades de minería de datos. ☐ Evidencia de acciones correctivas derivadas de los informes de análisis de vulnerabilidades. ☐ Evidencia de pruebas de penetración y acciones correctivas derivadas. ☐ Evidencia de informes de verificación de la configuración y acciones correctivas derivadas.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Op.mon.3 (NI)	**¿Se dispone de un sistema automático de recolección de eventos de seguridad?**		☐ SI ☐ NO
☐ (NI)	¿Se dispone de un sistema automático de recolección de eventos de seguridad, como puede ser un servidor *syslog* en base, por ejemplo, al protocolo del mismo nombre?		
Op.mon.3.r1	**¿Se dispone de un sistema para la correlación de eventos?**		☐ SI ☐ NO
☐	¿Se dispone de un sistema automático de recolección de eventos de seguridad que permita la correlación de los mismos? *NOTA: Por ejemplo, un repositorio centralizado de eventos, un SIEM, paneles de control de monitorización de eventos en soluciones Cloud, etc.*		
Op.mon.3.r2	**¿Se dispone de análisis dinámico de vulnerabilidades?**		☐ SI

			☐ NO
☐	¿Se dispone de soluciones de vigilancia que permitan determinar la superficie de exposición con relación a vulnerabilidades y deficiencias de configuración?		
Op.mon.3.r3	**¿Se dispone de sistemas para detección de amenazas avanzadas?**		☐ SI ☐ NO
☐	¿Se dispone de sistemas para la detección de amenazas avanzadas y comportamientos anómalos?		
☐	¿Se dispone de sistemas para la detección de amenazas persistentes avanzadas (Advanced Persistent Threat - APT) mediante la detección de anomalías significativas en el tráfico de la red?		
Op.mon.3.r4	**¿Se dispone de observatorios de cibervigilancia, propios o contratados como prestación de servicios?**		☐ SI ☐ NO
☐	¿Se dispone de observatorios digitales con fines de cibervigilancia dedicados a la detección y seguimiento de anomalías, que pudieran representar indicadores de amenaza, en contenidos digitales? *NOTA: Puede tratarse, por ejemplo, de un SOC interno, o externo, contratado como prestación del servicio de monitorización remota y gestión de alertas; servicios de vigilancia, por ejemplo, de existencia de cuentas de la Organización comprometidas tras ataques de phishing, exfiltraciones de datos en un ciberincidente, o simplemente en venta en la 'Dark web'.*		
Op.mon.3.r5	**¿Se dispone de medidas frente a la minería de datos?**		☐ SI ☐ NO
☐	¿Se aplican medidas para prevenir, detectar y reaccionar frente a intentos de minería de datos, limitando las consultas y monitorizando su volumen y frecuencia?		
☐	¿Se dispone de medidas que alerten a los administradores de seguridad de comportamientos sospechosos en tiempo real que puedan representar intentos de minería de datos?		
Op.mon.3.r6	**¿Se realizan inspecciones y auditorías técnicas periódicamente o tras un incidente?**		☐ SI ☐ NO
☐	¿Se verifica la configuración periódicamente y tras incidentes que hayan desvelado vulnerabilidades del sistema, ya sean estas nuevas, o que hubieran sido subestimadas en su momento?		
☐	¿Se realiza un análisis de vulnerabilidades periódicamente y tras incidentes que hayan desvelado vulnerabilidades del sistema, ya sean estas nuevas, o que hubieran sido subestimadas en su momento?		
☐	¿Se realizan pruebas de penetración periódicamente y tras incidentes que hayan desvelado vulnerabilidades del sistema, ya sean estas nuevas, o que hubieran sido subestimadas en su momento?		

Op.mon.3.r7.1	**En las interconexiones que lo requieran, se aplican controles en los flujos de intercambio de información a través del uso de metadatos?**		☐ SI ☐ NO

6.2.3 MEDIDAS DE PROTECCIÓN

Las medidas de protección estarán dirigidas a proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.

6.2.3.1 Medidas de Protección (PROTECCIÓN DE LAS INTALACIONES E INFRAESTRUCTURAS)

Mp.if.1	**Áreas separadas y con control de acceso**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia existencia de CPD y salas técnicas. ☐ Evidencia existencia de mecanismos de seguridad para controlar el acceso. ☐ Evidencia existencia de elementos de vigilancia y planos de ubicación debidamente protegidos. ☐ Evidencia existencia de mecanismos de cierre en los racks.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.if.1 NI	**¿Se instala el equipamiento del sistema de información en áreas dotadas de adecuadas medidas de seguridad?**		☐ SI ☐ NO
☐ NI	¿Se instala el equipamiento del sistema de información, en la medida de lo posible, en áreas separadas específicas para su función dotadas con medidas de seguridad, como puede ser un CPD o una sala técnica?		
☐ NI	¿Se controlan los accesos a CPD y salas técnicas de forma que sólo se pueda acceder por las entradas previstas?		
☐ NI	¿Se dispone de mecanismos de seguridad para restringir el acceso únicamente al personal autorizado?		
☐	Si el CPD es compartido por varias organizaciones, ¿se dispone de mecanismos de cierre en los armarios donde se ubique el equipamiento propio, o en las jaulas que albergan un conjunto de armarios, de forma que ningún tercero no autorizado pueda tener acceso?		
☐	¿Se dispone de cámaras de videovigilancia (CCTV) y/o detectores de intrusión para proteger las instalaciones, especialmente fuera del horario laboral?		

Mp.if.2	Identificación de las personas		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Protocolo de solicitud y concesión de autorizaciones de acceso a CPD, esporádicas y permanentes. ☐ Evidencia del sistema de gestión y control de accesos. ☐ Evidencia de consultas a la base de datos de entradas y salidas del CPD. ☐ Libro de visitas del CPD. ☐ Evidencia de comunicado de confirmación de acceso a las visitas, incluyendo normas de uso del CPD.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.if.2.1 NI	**¿Se dispone de una sistemática de control de acceso a los CPD?**		☐ SI ☐ NO
☐	¿Se dispone de procedimientos de solicitud de acceso a CPD y salas técnicas, gestionando la concesión de autorizaciones temporales y permanentes?		
☐ NI	¿Se dispone de un sistema de control de acceso que identifique a las personas que accedan a los CPD donde hay equipamiento esencial para el sistema de información, registrando las correspondientes entradas y salidas?		
☐	¿Se les comunica a las visitas externas junto a la autorización de acceso (por ejemplo, por correo electrónico), un ejemplar de las normas de uso del CPD?		
☐	¿Dichas normas de uso determinan que las visitas externas estén siempre acompañadas?		
☐	¿Se dispone de mecanismos ágiles para poder determinar quién estaba presente en el CPD, o sala técnica, en el momento de producirse un incidente de seguridad?		

Mp.if.3	Acondicionamiento de los locales
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐
Propuesta de evidencias	
	☐ Evidencia de gráficos o listados de evolución de temperatura (T) y humedad relativa (HR) en el CPD o sala técnica. ☐ Evidencia de cables de alimentación y de señal, organizados y etiquetados. ☐ Evidencia de posible herramienta software de representación del conexionado entre el equipamiento.

	☐ Evidencia de contratos de mantenimiento y boletines de la última revisión del equipamiento auxiliar.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.if.3.1 (NI)	**¿Se acondicionan y controlan ambientalmente los locales donde se ubica el equipamiento y componentes esenciales de los sistemas de información, así como se dispone en ellos de un trazado organizado e identificado de los cables de señal y de alimentación?**		☐ SI ☐ NO
☐ (NI)	¿Se controlan las condiciones de temperatura y humedad en los locales donde se ubica el equipamiento, de modo que se asegure su eficaz funcionamiento de acuerdo a las especificaciones del fabricante? *NOTA: La exigencia de esta medida será variable en función del tamaño del CPD y de la criticidad de los sistemas de información albergados, contemplándose en el análisis de riesgos.*		
☐	¿Los equipos de climatización, están amparados por el correspondiente contrato de mantenimiento con revisiones periódicas?		
☐	¿Se ha implementado en los locales donde se ubica el equipamiento y componentes esenciales de los sistemas de información, la protección frente a las amenazas identificadas en el análisis de riesgos?		
☐ (NI)	¿Está protegido eficazmente el cableado en los locales donde se ubica el equipamiento y componentes esenciales de los sistemas de información, de modo que se asegure su función frente a incidentes fortuitos o deliberados?		
☐	¿Están organizados y peinados el cableado y las fibras ópticas en los armarios rack, mediante sistemas pasacables? ¿están etiquetados los extremos de cables y fibras? ¿las canalizaciones de cables entre racks están protegidas, organizadas y con la separación adecuada entre alimentación y datos?		

Mp.if.4	**Energía eléctrica**		
Categoría / dimensión **D**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia SAI y generadores, % de carga y duración baterías. ☐ Posible acuerdo de aprovisionamiento preferente de gasóleo para generadores eléctricos. ☐ Evidencia de contratos de mantenimiento y boletines de la última revisión. ☐ Informes de baja/media/alta tensión.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.if.4.1 (NI)	**Los locales donde se ubican los sistemas de información y sus componentes esenciales (CPD, sala técnica),**		☐ SI ☐ NO

	¿disponen de tomas de energía eléctrica adecuadas, de modo que se garantice tanto el suministro como el correcto funcionamiento de las luces de emergencia?		
Mp.if.4.r1.1	**En caso de fallo del suministro principal, ¿se garantiza el abastecimiento eléctrico durante el tiempo requerido, de forma armonizada con el BIA?** **¿se realizan pruebas de carga o en vacío de los grupos electrógenos?** *NOTA: La exigencia de esta medida será variable en función del tamaño del CPD y de la criticidad de los sistemas de información albergados, contemplándose en el análisis de riesgos y/o en el BIA.*		☐ SI ☐ NO
☐	En caso de no disponerse de generador eléctrico de gasóleo (grupo electrógeno), ¿la duración de las baterías del SAI permite soportar cortes de suministro lo suficientemente amplios para cubrir los requisitos del BIA o, al menos, para permitir una parada ordenada de los equipos?		
☐	¿En caso de disponerse de generador eléctrico, ¿la capacidad del depósito de gasóleo o suministro de GAS es suficiente para mantener la alimentación eléctrica del equipamiento el tiempo requerido? ¿la duración de las baterías del SAI es suficiente para la puesta en marcha del generador? *NOTA: Únicamente en caso de ser necesario el uso del grupo electrógeno para el mantenimiento de la alimentación eléctrica debido al tamaño y condiciones del CPD.*		
☐	¿Los SAI (incluyendo las baterías internas o, en su caso, las bancadas externas) y los generadores eléctricos, en el caso de disponerse de éstos últimos, están amparados por un contrato de mantenimiento, con revisiones periódicas? ¿se dispone de partes de mantenimiento acordes a la legislación vigente y a las instrucciones de los fabricantes?		

Mp.if.5	**Protección frente a incendios**		
Categoría / dimensión **D**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia de los sistemas de detección y alerta. ☐ Evidencia de los sistemas de extinción. ☐ Evidencia de contratos de mantenimiento y partes de mantenimiento conforme a la legislación vigente.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**

Mp.if.5.1 NI	**Los locales donde se ubican los sistemas de información y sus componentes esenciales (CPD y salas técnicas) ¿están protegidos frente a los incendios atendiendo, al menos, a la normativa industrial de aplicación?** *NOTA: La exigencia de esta medida será variable en función del tamaño del CPD y de la criticidad de los sistemas de información albergados, contemplándose en el análisis de riesgos. En ocasiones, será necesario disponer de sistemas de extinción automática.*		☐ SI ☐ NO
☐ NI	¿Se dispone de sistemas de detección de incendios?		
☐	Si se activa un sensor (o en ocasiones dos de ellos para obviar falsos positivos), ¿la centralita de alarmas envía mensajes por los cauces previstos al personal de seguridad o de mantenimiento, a un centro externo coordinador de avisos de alarma, dispara una sirena, etc.?		
☐ NI	¿Se dispone de sistemas, manuales o automáticos, de extinción de incendios?		
☐ NI	¿Los sistemas de detección y extinción están amparados por un contrato de mantenimiento, con revisiones periódicas?		

Mp.if.6	**Protección frente a inundaciones**		
Categoría / dimensión **D**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia de los sistemas detectores de líquidos. ☐ Evidencia de la existencia de bombas de achique, si procede. ☐ Evidencia de posibles contratos de mantenimiento y boletines de la última revisión.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.if. 6.1 NI	**Los locales donde se ubican los sistemas de información y sus componentes esenciales ¿están protegidos frente a incidentes causados por el agua?**		☐ SI ☐ NO

	NOTA: En función de la ubicación del CPD (Sótano o planta elevada), de la existencia de suelo técnico, etc., podrá variar el nivel de exigencia de esta medida (empleo de detectores de líquidos, bombas de achique automáticas, etc.)		
☐	¿Se dispone de sistemas de detección de humedad y de líquidos, habitualmente bajo el suelo técnico de CPD y salas técnicas, con atención a las pérdidas de los equipos de refrigeración ubicados en la sala, especialmente si funcionan con agua?		
☐	¿Se dispone bombas de achique automático en pozuelas de recogida de aguas o, en su defecto, de la preinstalación para ubicar una bomba portátil?		
☐	¿Los sistemas de detección de líquidos y de achique están amparados por un contrato de mantenimiento, con revisiones periódicas? ¿se realizan pruebas de arranque de las bombas de achique?		

Mp.if.7	**Registro de entrada y salida de equipamiento**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia del registro de entrada/salida		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.if.7.1 (NI)	**¿Se lleva un registro pormenorizado de cualquier entrada y salida de equipamiento esencial, incluyendo la identificación de la persona que autoriza el movimiento?**		☐ SI ☐ NO
☐ (NI)	¿Se mantiene un registro de todo hardware y equipamiento esencial que entra y sale del CPD y salas técnicas, incluyendo la identificación de la persona que autoriza el movimiento y cualquier otra información que la Organización estime conveniente?		
☐	En caso de no ser el comportamiento habitual en la organización, ¿Se registra la entrada y salida de equipamiento portátil, por ejemplo, equipos personales y otros medios?		

6.2.3.2 Medidas de Protección (GESTIÓN DEL PERSONAL)

Mp.per.1	**Caracterización del puesto de trabajo**
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐

Propuesta de evidencias			
	☐ Análisis de riesgos, incluyendo puestos de trabajo. ☐ Perfiles de puesto de trabajo y RPT. ☐ Requisitos de los diferentes puestos de trabajo respecto a la seguridad, como complemento de la RPT. ☐ Requisitos en pliegos para el personal contratado en modalidad de prestación de servicios.		
	☐ Evidencia de obtención de la HPS		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.per.1	**Para cada puesto de trabajo, relacionado directamente con el manejo de información o servicios en el ámbito del ENS, ¿se definen las responsabilidades en materia de seguridad?**		☐ SI ☐ NO
☐	El análisis de riesgos realizado para dar cumplimiento a las disposiciones del ENS ¿tiene en cuenta las personas y sus responsabilidades respecto a la seguridad del sistema de información?		
☐ NI	Para cada puesto de trabajo, relacionado directamente con el manejo de información o servicios, ¿se han definido las responsabilidades en materia de seguridad?		
☐	¿Se definen los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular en términos de confidencialidad, ya sea personal propio o contratado como prestación de servicios? *NOTA: 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.*		
Mp.per.1.r1	**¿Disponen los administradores de seguridad/sistema 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?**		☐ SI ☐ NO

Mp.per.2	Deberes y obligaciones
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐
Propuesta de evidencias	

	☐ Acuerdos de confidencialidad suscritos por los empleados. ☐ Acuerdos de confidencialidad suscritos con las empresas de servicios, abarcando a los colaboradores. ☐ Pliegos y/o contratos suscritos con los prestadores de servicios en el ámbito del ENS.		
	☐ Aceptación formal de los empleados respecto a deberes y responsabilidades de seguridad inherentes a su desempeño.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.per.2 NI	**¿Se han definido, y se informa, a cada persona que trabaja en el sistema, de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad?**		☐ SI ☐ NO
☐ NI	¿Se informa al personal propio, que trabaja en el sistema, de los deberes y responsabilidades en materia de seguridad incluyen tanto el periodo durante el cual se desempeña el puesto, como posteriormente a su terminación? *NOTA: por ejemplo, a través de la presentación de una normativa de uso del sistema.*		
☐ NI	¿Se informa al personal propio, que trabaja en el sistema, de las medidas disciplinarias a que haya lugar en caso de incumplimiento de los deberes y responsabilidades en materia de seguridad?		
☐ NI	¿Se suscriben cláusulas de confidencialidad con los empleados? ¿si se trata de una organización del sector privado, que presta servicios, dichas cláusulas incluyen la confidencialidad de la información de los clientes que puedan llegar a conocer? *NOTA: Respecto al empleado público, ya sea este funcionario o personal laboral, la confidencialidad es inherente a su condición, según el artículo 53.12 sobre Principios Éticos del Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público, no siendo, en consecuencia, necesario que suscribiera una cláusula de confidencialidad. sí se requiere para cualquier empleado del sector privado.*		
☐ NI	¿Se suscriben acuerdos de confidencialidad con las organizaciones que le prestan servicios, que incluyan a todo el personal que éstas asignen al contrato? *NOTA: Si el prestador de servicios no dispone de certificación del ENS, deberá evidenciar que a su vez le ha hecho firmar a su personal asignado al contrato una cláusula de confidencialidad respecto a la información de los clientes.*		
☐	¿Se establece en relación al personal contratado, que trabaja a través de un tercero en el sistema, de los deberes y obligaciones de cada parte y de dicho personal externo?		
☐	¿Se establece en relación al personal contratado, que trabaja a través de un tercero en el sistema, el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones?		
Mp.per.2.r1	**¿Se obtiene la confirmación expresa por parte de los usuarios de conocer las instrucciones de seguridad necesarias y obligatorias, así como los procedimientos necesarios para llevarlas a cabo de manera adecuada?**		☐ SI ☐ NO

Mp.per.3	Concienciación		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Plan de Concienciación (o Plan de Formación y Concienciación si están agrupados). ☐ Evidencia de las últimas campañas de concienciación y receptores de las mismas.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.per.3 (NI)	**¿Se realizan las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos?**		☐ SI ☐ NO
☐	¿Existe un mínimo de planificación anual, que podrá ajustarse en función de las circunstancias, respecto a las acciones y campañas de concienciación?		
☐ (NI)	¿Se recuerda periódicamente en las acciones de concienciación la normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales?		
☐ (NI)	¿Se recuerda periódicamente en las acciones de concienciación la identificación de incidentes, actividades o comportamientos sospechosos, que deban ser reportados para permitir su tratamiento por personal especializado, así como la necesidad de notificarlos sin dilación por los canales establecidos?		
☐ (NI)	¿Se recuerda periódicamente en las acciones de concienciación el procedimiento para informar sobre incidentes de seguridad, sean estos reales o falsas alarmas?		

Mp.per.4	Formación
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐
Propuesta de evidencias	
	☐ Plan de Formación (o Plan de Formación y Concienciación si están agrupados). ☐ Evidencia del programa de las formaciones realizadas. ☐ Evidencia de la eficacia de las acciones formativas (pruebas, encuestas, certificados). ☐ Evidencia de los asistentes a las formaciones (listas de inscritos).

	☐ Evidencia de certificados aportados por el personal, incluso de acciones formativas no organizadas por la entidad.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.per.4 (NI)	**¿Se forma regularmente al personal de la organización en aquellas materias relativas a seguridad de la información que requiera el desempeño de sus funciones?**		☐ SI ☐ NO
☐ (NI)	¿Se dispone de un Plan de Formación general, orientado a las necesidades del personal, que incluya acciones formativas respecto a la seguridad de la información, donde conste la formación concreta realizada por el personal de la organización y la planificada para ser llevada a cabo?		
☐	¿La formación incluye, al menos, lo relativo a configuración de sistemas, detección y reacción ante incidentes y gestión de la información en cualquier soporte en el que se encuentre?		
☐ (NI)	¿Se diferencia la formación impartida al personal general, de la específica para directivos, para técnicos y especialmente para personas con responsabilidades de seguridad?		
☐	¿Se evalúa la eficacia de las acciones formativas llevadas a cabo?		
☐	¿Existe control de los asistentes a cada una de las acciones formativas, ya sean esta impartidas presencialmente, en remoto directo mediante plataformas de videoconferencia on-line, o en remoto diferido desde plataformas con acceso a cursos 'enlatados' accesibles al ritmo de quién los cursa?		
☐	¿Se solicitan formaciones específicas, o certificaciones concretas de seguridad, al personal externo contratado en modalidad de prestación de servicios, en función del desempeño?		

6.2.3.3 Medidas de Protección (PROTECCIÓN DE LOS EQUIPOS)

Mp.eq.1	**Puesto de trabajo despejado**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia de puesto de trabajo despejado de soportes.		
	☐ Evidencia de lugares cerrados empleados para ubicar soportes conteniendo información calificada como 'no pública'.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.eq.1 (NI)	**¿Los puestos de trabajo permanecen despejados, sin que exista material distinto del necesario en cada momento?**		☐ SI ☐ NO

	NOTA: Entendemos por 'material' a todo tipo de soportes conteniendo información calificada como 'no pública' (lápices USB, papeles, etc.)		
Mp.eq.1.r1	**Una vez usado, y siempre que sea factible, ¿el material se almacena en lugar cerrado?** *NOTA: Se entiende por 'lugar cerrado' aquel asegurado por un sistema de cierre, por ejemplo, los cajones del escritorio, armarios o taquillas.*		☐ SI ☐ NO

Mp.eq.2	**Bloqueo del puesto de trabajo**		
Categoría / dimensión **A**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia de GPO o directiva de configuración de bloqueo. ☐ Evidencia de que no puede modificarse desde el puesto de usuario.		
	☐ Evidencia de configuración que fuerce la cancelación de sesiones pasado determinado tiempo de inactividad.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.eq.2 (NI)	**¿El puesto de trabajo se bloquea al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso?**		☐ SI ☐ NO
Mp.eq.2.r1	**Pasado un cierto tiempo, superior al de bloqueo, ¿se cancelan todas las sesiones abiertas desde dicho puesto de trabajo?**		☐ SI ☐ NO

Mp.eq.3	**Protección de dispositivos portátiles**
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐
Propuesta de evidencias	
	☐ Evidencia de procedimiento de actualización del inventario y verificaciones (referido a los portátiles).

	☐ Procedimiento y cauces para comunicar la pérdida o robo de portátiles. ☐ Política o normativa de uso seguro y de acceso remoto seguro para portátiles.		
	☐ Evidencia de cifrado de los discos de los portátiles.		
	☐ Evidencia de filtros visuales 'antispy' en los portátiles ☐ Evidencia de normativa que prohíba el empleo del portátil en entornos no controlados.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.eq.3 NI	**¿Se adopta un conjunto de medidas que permita mantener la protección de los equipos portátiles, especialmente los que abandonan el perímetro físico de la organización, a niveles acordes con los requerimientos de seguridad?**		☐ SI ☐ NO
☐ NI	Como concreción de la medida [op.ext.1] sobre inventario de activos, ¿se lleva un inventario de los equipos portátiles junto con una identificación de la persona responsable del mismo?		
☐	¿Puede evidenciarse una verificación regular de que los equipos portátiles estén positivamente bajo el control de a quién se les ha asignado?		
☐	¿Se ha establecido normativa de uso de los equipos portátiles, así como de acceso remoto mediante los mismos?		
☐ NI	¿Se ha establecido un procedimiento operativo de seguridad para informar al servicio de gestión de incidentes de pérdidas o sustracciones de equipos portátiles?		
☐	En caso de robo, siempre que la organización evalúe dicha funcionalidad conveniente en función del riesgo ¿se puede borrar de forma remota el dispositivo?		
☐ NI	Cuando un equipo portátil se conecta remotamente a través de redes que no están bajo el estricto control de la organización, ¿el ámbito de operación del sistema limita la información y los servicios accesibles a los mínimos imprescindibles, requiriendo autorización previa de los responsables de la información y los servicios afectados? *NOTA: Este punto es de aplicación a conexiones a través de internet y otras redes que no sean de confianza.*		
☐	¿Se evita, en la medida de lo posible, que los equipos portátiles contengan claves de acceso remoto a la organización, que no sean imprescindibles? *NOTA: Se considerarán claves de acceso remoto aquellas que sean capaces de habilitar un acceso a otros equipos de la organización, u otras de naturaleza análoga.*		
Mp.eq.3.r1	**¿Se protege el portátil mediante cifrado del disco duro cuando el nivel de confidencialidad de la información almacenada en el mismo sea de nivel MEDIO?**		☐ SI ☐ NO

Mp.eq.3.r2	**El uso de equipos portátiles fuera de las instalaciones de la organización, ¿se restringe a entornos protegidos, donde el acceso sea controlado, a salvo de hurtos y miradas indiscretas?**		☐ SI ☐ NO

Mp.eq.4	**Otros equipos conectados a la red**		
Categoría / dimensión **C**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia de configuración de dispositivos que permitan garantizar el control de flujo. ☐ Evidencia de funcionalidad de borrado de información en los dispositivos con capacidad de almacenarla.		
	☐ Evidencia de empleo de componentes certificados para otros dispositivos conectados a la red.		
	☐ Evidencia de herramientas de monitorización y/o autodescubrimiento de dispositivos.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.eq.4 (NI)	**¿Se controlan los dispositivos presentes en el sistema, especialmente en lo que se refiere al flujo de información y su almacenamiento?**		☐ SI ☐ NO
☐ (NI)	¿Cuentan los dispositivos presentes en el sistema con una configuración de seguridad adecuada, de manera que se garantice el control del flujo definido de entrada y salida de la información? *NOTA: Especial atención respecto a los elementos del tipo impresoras, Internet de las Cosas (IoT) y Sistemas de Control Industrial (ICS), conectados a la red.*		
☐	¿Proporcionan los dispositivos presentes en la red, que dispongan de algún tipo de almacenamiento temporal o permanente de información, la funcionalidad necesaria para eliminar dicha información almacenada, de ser necesario? *NOTA: un ejemplo de verificación, al llegar al final de su vida útil, puede ser una impresora multifunción de red que almacena trabajos de impresión en su disco duro interno, provenientes de los diferentes usuarios del sistema.*		
Mp.eq.4.r1	**¿Se emplean, cuando sea posible, productos o servicios que cumplan lo establecido en la medida [op.pl.5] sobre componentes certificados?**		☐ SI ☐ NO
Mp.eq.4.r2	**¿Se dispone de soluciones que permitan visualizar los dispositivos presentes en la red, controlar su**		☐ SI ☐ NO

	conexión/desconexión a la misma y verificar su configuración de seguridad?		

6.2.3.4 Medidas de Protección (PROTECCIÓN DE LAS COMUNICACIONES)

Mp.com.1	**Perímetro seguro**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia de equipos cortafuegos y su definición de reglas. ☐ Evidencia de autorizaciones para definir nuevas reglas caso de requerirse nuevos flujos.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.com.1.1 (NI)	**¿Se dispone de algún sistema que asegure el perímetro lógico?** *NOTA: Dispositivos del tipo Cortafuegos, o de naturaleza similar.*		☐ SI ☐ NO
☐ (NI)	¿Se dispone de un sistema de protección perimetral que separe la red interna del exterior?		
☐ (NI)	Caso de disponerse de varias sedes o centros de datos ¿disponen todos ellos de protección perimetral?		
☐ (NI)	El sistema empleado para asegurar el perímetro ¿es atravesado por todo el tráfico, sin excepción?		
☐	¿Requieren estar autorizados previamente todos los flujos de información a través del perímetro de seguridad de la organización?		

Mp.com.2	**Protección de la confidencialidad**
Categoría / dimensión **C**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐
Propuesta de evidencias	
	☐ Evidencia empleo de VPN.
	☐ Evidencia de los algoritmos de cifrado que se emplean en las VPN.
	☐ Evidencia de empleo de dispositivos hardware para establecer las VPN.

	☐ Evidencia de utilización de cifradores		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.com.2 (NI)	**¿Se emplean redes privadas virtuales cuando la comunicación discurre por redes fuera del propio dominio de seguridad, por lo que deba cifrarse?**		☐ SI ☐ NO
Mp.com.2.r1	**¿Se emplean algoritmos y parámetros autorizados por el CCN para cifrar las comunicaciones que discurran fuera del dominio de seguridad?** *NOTA: Se dispone de las guías CCN-STIC 836 Seguridad en Redes Privadas Virtuales (VPN) y CCN-STIC 807 Criptología de empleo en el ENS.*		☐ SI ☐ NO
Mp.com.2.r2 Mp.com.2.r3	**Respecto a las VPN ¿se emplean dispositivos con garantías adicionales?**		☐ SI ☐ NO
☐	¿Se emplean dispositivos hardware en el establecimiento y utilización de la red privada virtual?		
☐	Para el establecimiento y utilización de la red privada virtual ¿se usan productos o servicios que cumplan lo señalado en la medida [op.pl.5] sobre componentes certificados?		
Mp.com.2.r4	**¿Se emplean cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación?**		☐ SI ☐ NO
Mp.com.2.r5	**¿Se cifra toda la información transmitida?**		☐ SI ☐ NO

Mp.com.3	**Protección de la integridad y de la autenticidad**
Categoría / dimensión **I A**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐
Propuesta de evidencias	
	☐ Evidencia de enlaces SSL o IP-SEC. ☐ Evidencia de desarrollo seguro frente a ataques activos. ☐ Informes de las pruebas de penetración. ☐ Evidencia del empleo de certificados cualificados.

	☐ Detalle de los algoritmos de cifrado, empleados en las VPN. ☐ Evidencia de empleo de VPN con algoritmos de cifrado autorizados por el CCN.		
	☐ Evidencia de empleo de dispositivos hardware para establecer las VPN.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.com.3 NI	**¿Se emplean mecanismos para garantizar la autenticidad y la integridad de las comunicaciones con el exterior?**		☐ SI ☐ NO
☐ NI	En comunicaciones con puntos exteriores al propio dominio de seguridad, ¿se asegura la autenticidad del otro extremo del canal de comunicación antes de intercambiar información? *NOTA: Se puede asegurar la autenticidad mediante el uso de protocolos con autenticación de extremos, por ejemplo, mediante el empleo de TLS, SSL y otros protocolos seguros, autenticación mediante certificados, etc.*		
☐ NI	¿Se previenen ataques activos garantizando que al ser detectados se activarán los procedimientos previstos para el tratamiento del incidente? *NOTA: Se considerarán ataques activos la alteración de la información en tránsito, la inyección de información espuria y el secuestro de la sesión por una tercera parte.*		
☐	¿Se emplea como mecanismo de identificación y autenticación únicamente alguno los previstos en la normativa de aplicación del ordenamiento jurídico?		
Mp.com.3.r1 Mp.com.3.r2	**¿Se protegen las comunicaciones mediante redes privadas virtuales (VPN)?**		☐ SI ☐ NO
☐	¿Se emplean redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad, por lo que deba cifrarse?		
☐	¿Se emplean algoritmos y parámetros autorizados por el CCN para cifrar las comunicaciones que discurran fuera del dominio de seguridad? *NOTA: Se relacionan en la guía CCN-STIC 807 sobre Criptología de empleo en el ENS.*		
Mp.com.3.r3 Mp.com.3.r4	**¿Se emplean dispositivos con garantías adicionales respecto a las VPN?**		☐ SI ☐ NO
☐	¿Se emplean dispositivos hardware en el establecimiento y utilización de la red privada virtual?		
☐	Para el establecimiento y utilización de la red privada virtual ¿se usan productos o servicios que cumplan lo establecido en la medida [op.pl.5] sobre componentes certificados?		
Mp.com.3.r5.1	**¿Se emplean cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación?**		☐ SI ☐ NO

Mp.com.4	**Separación de flujos de información en la red**
Categoría / dimensión	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐

Categoría	**Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia de segmentación de red, incluyendo diagramas o listado de segmentos, si se dispone. ☐ Evidencia de monitorización de la interconexión de segmentos de red.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.com.4	**¿Se ha segmentado la red, segregando el tráfico?**		☐ SI ☐ NO
☐ NI	¿Se han separado en segmentos los flujos de información, segregando el tráfico por la red, de modo que cada equipo únicamente tenga acceso a la información que necesita?		
☐	Si se emplean comunicaciones inalámbricas, ¿se concentran éstas mediante un segmento separado?		
NOTA: Para categoría MEDIA, debe cumplirse al menos con una de las medidas de refuerzo R1, R2 o R3, que siguen a continuación, mientras que para categoría ALTA, se requiere cumplir con R2 o R3 y siempre con R4.			
Mp.com.4.r1	**¿Se han segregado al menos 3 segmentos de red mediante VLAN?**		☐ SI ☐ NO
☐	¿Los segmentos de red se han implementado por medio de redes de área local virtuales (Virtual Local Area Network - VLAN)?		
☐	¿Se ha segregado en distintas subredes la red que conforma el sistema, contemplando como mínimo la red de usuarios, la de servicios y la de administración?		
Mp.com.4.r2 NI	**¿Se han implementado los segmentos de red por medio de redes privadas virtuales (Virtual Private Network - VPN)?**		☐ SI ☐ NO
Mp.com.4.r3	**¿Se han implementado los segmentos de red con medios físicos separados?**		☐ SI ☐ NO
Mp.com.4.r4	**¿Se dispone de controles de entrada a los segmentos, así como monitorización?**		☐ SI ☐ NO
☐	¿Se dispone de control de entrada de los usuarios que llegan a cada segmento y control de entrada y salida de la información disponible en cada segmento?		
☐	¿El punto de interconexión entre subredes está particularmente asegurado, mantenido y monitorizado?		

6.2.3.5 Medidas de Protección (PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN)

Mp.si.1	**Marcado de soporte**		
Categoría / dimensión **C**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia de calificación de los documentos del SGSI asociado al sistema de información. ☐ Evidencia del marcado de soportes con el mayor nivel de seguridad de la información que contienen. ☐ Evidencia de una norma o directrices respecto a cómo valorar y calificar la información.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.si.1	**¿Se identifican los soportes que contienen información sensible con el nivel de seguridad de mayor calificación de la información contenida?** *NOTA: El concepto soportes de información incluye al papel impreso, pendrives, discos externos, DVD, etc.*		☐ SI ☐ NO
☐	¿Los soportes de información que contienen información que, según su nivel de seguridad, o su calificación, debe protegerse con medidas de seguridad específicas, llevan las marcas, o metadatos correspondientes, que indican el mayor nivel de seguridad de la información contenida?		
☐ NI	¿Se indica en los documentos y registros del sistema de gestión de la seguridad de la información, aplicado sobre el sistema de información, su nivel de calificación?		
☐ NI	¿Se dispone de una norma, o de instrucciones precisas, sobre cómo valorar y calificar la información, de modo que concuerde con el marcado de los soportes?		
Mp.si.1.r1	**¿La organización determina el empleo de marcas de agua para garantizar un uso adecuado de la información digital, llevándolo a la práctica?**		☐ SI ☐ NO
☐	¿La política de seguridad de la organización define marcas de agua para asegurar el uso adecuado de la información que se maneja?		
☐	La información digital (documentos electrónicos, material multimedia…) ¿incluyen una marca de agua según la política de seguridad?		
☐	Los equipos o dispositivos a través de los que se accede a aplicaciones, escritorios remotos o virtuales, datos…, ¿presentan una marca de agua en pantalla según la política de seguridad?		

Mp.si.2	Criptografía		
Categoría / dimensión **C I**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Normativa, o directrices, respecto al cifrado de soportes (dispositivos removibles). ☐ Evidencia de cifrado de soportes (dispositivos removibles).		
	☐ Evidencia de cifrado de las copias de seguridad. ☐ Evidencia de la certificación o cualificación de los productos de cifrado.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.si.2.1 NI	**¿Se emplean mecanismos criptográficos para proteger los dispositivos removibles cuando es necesario?** *NOTA: se entiende por dispositivos removibles a los soportes tipo CD, DVD, discos extraíbles, pendrives, memorias USB, y otros de naturaleza análoga.*		☐ SI ☐ NO
☐	¿Se usan mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida en los dispositivos removibles cuando salen del área controlada?		
☐	¿Se emplean algoritmos y parámetros autorizados por el CCN cuando los dispositivos removibles salen del área controlada? *NOTA: Se relacionan en la guía CCN-STIC 807 sobre Criptología de empleo en el ENS.*		
Mp.si.2.r1	**¿Se emplean productos certificados conforme a lo establecido en [op.pl.5] sobre componentes certificados?**		☐ SI ☐ NO
Mp.si.2.r2	**¿Las copias se seguridad se cifran utilizando algoritmos y parámetros autorizados por el CCN?**		☐ SI ☐ NO

Mp.si.3	Custodia
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐
Propuesta de evidencias	
	☐ Evidencia de medidas de seguridad en la custodia de soportes.

	☐ Ficha técnica del fabricante de los soportes con condiciones ambientales de almacenamiento. ☐ Evidencia de contrato y acuerdos con un tercero que custodie los soportes de la organización.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.si.3 (NI)	**¿Se garantiza la seguridad en la custodia de los soportes de información?**		☐ SI ☐ NO
☐ (NI)	¿Se aplica la debida diligencia y control a los soportes de información, ya sean fijos o extraíbles, que permanecen bajo la responsabilidad de la organización, garantizando el control de acceso mediante medidas físicas o lógicas, según corresponda? NOTA: Entenderemos por soportes fijos los contenidos en las cabinas de discos, las NAS, almacenamiento en servidores, etc.; y por soportes extraíbles, por ejemplo, los cartuchos de cinta individuales o las bandejas de un robot de cintas.		
☐	¿Se respetan las exigencias de mantenimiento del fabricante, en especial, en lo referente a temperatura, humedad y otros agentes medioambientales? *NOTA: podrían considerarse dichas condiciones ambientales únicamente en aquellos dispositivos de almacenamiento (granjas NAS y cabinas de discos), o en soportes extraíbles de alta densidad como son determinados cartuchos de cinta.*		
☐	Si se externaliza la custodia de soportes en una tercera entidad ¿se ha suscrito un contrato o acuerdo del servicio donde consten las medidas de seguridad aplicadas?		

Mp.si.4	**Transporte**
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐
Propuesta de evidencias	
	☐ Registro de entrada / salida de soportes. ☐ Verificación del cifrado de soportes. ☐ Evidencia de maletín de transporte. ☐ Evidencia de contrato y acuerdos con tercero que transporta los soportes de la organización.

	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.si.4 (NI)	**¿Se garantiza la seguridad en el transporte de los soportes de información?**		☐ SI ☐ NO
☐ (NI)	¿Se dispone de un registro de entrada / salida que identifique al transportista que entrega/recibe el soporte? *NOTA: Esta medida está pensada especialmente para transportes esporádicos, por ejemplo, de copias especiales de seguridad o soportes conteniendo información de elevado nivel de sensibilidad. Los transportes recurrentes de copias de seguridad hacia otra ubicación, por ejemplo, diarios, realizados por*		

	el mismo transportista, se podrían reflejar como una única entrada especificando periodicidad en dicho registro, mientras no se produzcan cambios en el protocolo o sistemática empleada.
☐	Si se designan responsables de la organización autorizados para el transporte de determinados soportes, ¿disponen o queda reflejada la correspondiente autorización acorde con los medios transportados?
☐	¿Se dispone de un procedimiento rutinario que coteje las salidas con las llegadas y levante las alarmas pertinentes cuando se detecte algún incidente?
☐	¿Se utilizan los medios de protección criptográfica correspondientes al mayor nivel de seguridad de la información contenida? *NOTA: Se relacionan en la guía CCN-STIC 807 sobre Criptología de empleo en el ENS.*
☐	Si se externaliza el transporte de soportes en una tercera entidad ¿se ha suscrito un contrato o acuerdo del servicio donde consten las medidas de seguridad aplicadas?
☐	¿Se transportan los soportes dentro de un maletín de seguridad, por ejemplo, cerrado mediante candados de apertura por llave, del que el transportista no dispone de la misma?

Mp.si.5	**Borrado y destrucción**		
Categoría / dimensión **C**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Registro de borrado y/o destrucción de soportes. ☐ Verificación del borrado seguro de soportes. ☐ Verificación de destrucción de soportes. ☐ Evidencia de contrato y acuerdos con tercero que borra o destruye de forma segura los soportes de la organización.		
	☐ Evidencia del empleo de productos certificados o cualificados para el borrado y/o la destrucción.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.si.5 (NI)	**¿Se garantiza el borrado seguro o la destrucción de los soportes tras su utilización?**		☐ SI ☐ NO
☐ (NI)	Los soportes que vayan a ser reutilizados para otra información, o liberados a otra organización, ¿son objeto de un borrado seguro de su contenido que no permita su recuperación? *NOTA: Por ejemplo, la reutilización de equipos entre el personal de la entidad, devolución de equipos en préstamo o renting, dispositivos de almacenamiento desechados, donaciones, etc.*		
☐	¿Cuándo la naturaleza del soporte no permita un borrado seguro antes de destinarlo a otro fin, ¿es éste destruido de forma que no pueda ser reutilizado para otro sistema?		

☐	¿Se dispone de un registro con identificación de los soportes borrados o destruidos, la herramienta y método empleado, quién lo realizó, etc.?
☐	Si se externaliza el borrado seguro y/o la destrucción de soportes en una tercera entidad, ¿se ha suscrito un contrato o acuerdo del servicio donde consten las medidas de seguridad aplicadas?
☐	Si se externaliza el borrado seguro y/o la destrucción de soportes en una tercera entidad, ¿suministra ésta un certificado de borrado o destrucción segura donde consten las referencias y números de serie de los soportes tratados? *NOTA: No se trata de un certificado general indicando los kilos de material destruido, tal vez siguiendo normas ambientales, sino focalizando en los soportes concretos en base a eliminar de forma irreversible la información contenida.*

Mp.si.5.r1	**¿Se emplean productos o servicios que cumplen lo establecido en [op.pl.5] sobre componentes certificados?**		☐ SI ☐ NO
Mp.si.5.r2	**Una vez finalizado el ciclo de vida del soporte de información ¿Es destruido éste de forma segura conforme a los criterios establecidos por el CCN?**		☐ SI ☐ NO

6.2.3.6 Medidas de Protección (PROTECCIÓN DE LAS APLICACIONES INFORMÁTICAS)

Mp.sw.1	**Desarrollo de aplicaciones**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia de separación de los entornos de producción y desarrollo. ☐ Evidencia de medidas de seguridad del repositorio de código fuente. ☐ Metodología de desarrollo seguro empleada. ☐ Evidencia de que la metodología de desarrollo seguro empleada incide en la seguridad. ☐ Evidencia de la seguridad en los datos de prueba reales, si procede.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.sw.1 (NI)	**¿Está separado a todos los efectos el entorno de desarrollo del de producción?** *NOTA: habitualmente se dispone de entornos de desarrollo, preproducción o test, y producción.*		☐ SI ☐ NO
☐	¿Se han separado ambos entornos, realizándose el desarrollo sobre sistemas diferenciados de los productivos?		

☐	¿Existen herramientas de desarrollo o datos de prueba en el entorno de producción, o elementos productivos o datos reales en el entorno de desarrollo?		
☐	¿Se han aplicado medidas de seguridad sobre los repositorios de código fuente?		
Mp.sw.1.r1	**¿Las aplicaciones se desarrollarán respetando el principio de mínimo privilegio (con los privilegios que sean indispensables), accediendo únicamente a los recursos imprescindibles para su función?**		☐ SI ☐ NO
Mp.sw.1.r2	**¿Se aplica una metodología de desarrollo seguro reconocida?**		☐ SI ☐ NO
☐	¿La metodología aplicada tiene en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida?		
☐	¿La metodología aplicada incluye normas de programación segura, como son el control de asignación y liberación de memoria, desbordamiento de memoria (*overflow*), etc.?		
☐	¿La metodología aplicada tiene en cuenta los datos empleados en las pruebas?		
☐	¿La metodología aplicada permite la inspección del código fuente?		
Mp.sw.1.r3 NI	**¿Se tienen en cuenta aspectos de seguridad como parte integral del diseño del sistema?**		☐ SI ☐ NO
☐ NI	¿Forman parte integral del diseño del sistema los mecanismos de identificación y autenticación?		
☐ NI	¿Forman parte integral del diseño del sistema los mecanismos de protección de la información tratada?		
☐	¿Forman parte integral del diseño del sistema los mecanismos de generación y tratamiento de pistas de auditoría?		
Mp.sw.1.r4	**¿Se aseguran los datos reales empleados para las pruebas previas, evitando su uso en la medida de lo posible?**		☐ SI ☐ NO
☐	¿Se evita realizar con datos reales las pruebas previas a la implementación o modificación de los sistemas de información?		
☐	En caso de que fuese necesario recurrir a datos reales para las pruebas previas, ¿se garantiza el nivel de seguridad correspondiente?		

Mp.sw.1.r5	**¿El desarrollador elabora y mantiene actualizada una relación formal de los componentes software de terceros empleados en la aplicación o producto?** *NOTA: Se mantendrá un histórico de los componentes utilizados en las diferentes versiones del software. El contenido mínimo de la lista de componentes, que contendrá, al menos, la identificación del componente, el fabricante y la versión empleada, se concretará en una guía CCN-STIC del CCN.*		☐ SI ☐ NO

Mp.sw.2	**Aceptación y puesta en servicio**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia de pruebas y verificación de los criterios de aceptación en materia de seguridad. ☐ Evidencia de verificaciones de integridad respecto a la seguridad de otras aplicaciones y/o elementos. ☐ Informes de pentesting.		
	☐ Si procede, guías de instalación y configuración segura del sistema, facilitadas por los proveedores. ☐ Si procede, guías de uso seguro del sistema, facilitadas por los proveedores. ☐ Si procede, guías de relación entre cliente y proveedor, facilitadas por los proveedores.		
	☐ Evidencia del entorno de preproducción o test para pruebas		
	☐ Evidencia de auditorías de código fuente		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.sw.2 NI	**Antes de su paso a producción, ¿se comprueba el correcto funcionamiento de la aplicación y de sus aspectos de seguridad?**		☐ SI ☐ NO
☐ NI	Antes del paso a producción de las aplicaciones, ¿se comprueban los criterios de aceptación en materia de seguridad? *NOTA: Se han verificado, en la medida de lo posible, el cumplimiento de requisitos de seguridad, por ejemplo, realizando pruebas básicas de funcionamiento, mediante solicitud de certificaciones, solicitud de manuales de seguridad, verificando configuraciones de seguridad, etc.*		
☐	Antes del paso a producción de las aplicaciones, ¿se comprueba que no se deteriora la seguridad de otros componentes del servicio?		

Mp.sw.2 NI	**¿Caso de aplicaciones desarrolladas externamente implementadas en modo local (on-premise), el proveedor aporta suficientes evidencias de la seguridad de la aplicación?**		☐ SI ☐ NO
☐ NI	¿Aporta el proveedor que implementa la solución un ejemplar particularizado para el cliente que contrata del manual '*Guía de instalación y configuración segura del sistema*' dirigida a los administradores? *NOTA: Puede consultarse su estructura recomendada en la guía CCN-STIC 858 sobre implantación de soluciones on-premise.*		
☐ NI	¿Aporta el proveedor que implementa la solución un ejemplar particularizado para el cliente que contrata del manual '*Guía de uso seguro del sistema*' dirigida a los usuarios? *NOTA: Puede consultarse su estructura recomendada en la guía CCN-STIC 858 sobre implantación de soluciones on-premise.*		
☐	¿Aporta el proveedor que implementa la solución un ejemplar particularizado para el cliente que contrata del manual '*Guía de la relación entre cliente y proveedor*' dirigida a los administradores? *NOTA: Puede consultarse su estructura recomendada en la guía CCN-STIC 858 sobre implantación de soluciones on-premise*		
Mp.sw.2.r1	**¿Se realizan las pruebas en un entorno aislado de preproducción?**		☐ SI ☐ NO
Mp.sw.2.r2	**¿Se realizan auditorías de código fuente?**		☐ SI ☐ NO

6.2.3.7 Medidas de Protección (PROTECCIÓN DE LA INFORMACIÓN)

Mp.info.1	**Datos personales**
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐
Propuesta de evidencias	
	☐ Política de protección de datos y/o de seguridad de la información. ☐ Documento de designación formal del DPD y de su notificación a la AEPD. ☐ Registro de las Actividades de Tratamiento (RAT). ☐ Estudio de necesidad / conveniencia de realizar EIPD. ☐ AA.RR. de seguridad de la información, incluyendo aspectos de protección de datos personales, u otro AA.RR. adicional específico. ☐ Procedimiento para dar cumplimiento al ejercicio de derechos.

	☐ Evidencia de incidentes registrados marcados como que afectan a datos personales y, en su caso, evidencia de la intervención del DPD o de quién asuma dicha función caso de no ser obligatoria su designación. ☐ Procedimiento de evaluación y tratamiento de brechas de seguridad (violaciones de datos personales). ☐ Evidencia de elementos para garantizar el secreto estadístico, si procede.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.info.1	**Cuando el sistema trate datos personales, ¿el Responsable de Seguridad recoge los requisitos de protección de datos que sean fijados por el responsable o por el encargado del tratamiento, contando con el asesoramiento del DPD, y que sean necesarios implementar en los sistemas de acuerdo a la naturaleza, alcance, contexto y fines del mismo, así como de los riesgos para los derechos y libertades de acuerdo a lo establecido en los artículos 24 y 32 del RGPD, y de acuerdo a la evaluación de impacto en la protección de datos, si se ha llevado a cabo?**		☐ SI ☐ NO

☐	¿Se dispone de una política de protección de datos o se referencia la protección de datos en la política de seguridad de la información?
☐ NI	En su caso, ¿se ha designado un Delegado de Protección de Datos (DPD) y ha sido dicha designación notificada a la AEPD, especialmente si la organización pertenece al sector público o se ve afectada por los supuestos del art. 37.1 RGPD y 34 LOPDGDD?
☐ NI	¿Se dispone de un registro de las actividades de tratamiento (RAT), que distinga los tratamientos como responsable y como encargado del tratamiento? *NOTA: Dicho registro debe ser publicado caso de tratarse de una organización perteneciente al sector público (portal de transparencia).*
☐	¿Se ha determinado la necesidad/conveniencia de realizar una EIPD para determinados tratamientos?
☐	¿El análisis de riesgos tiene en cuenta la protección de datos personales?
☐	¿Se da cumplimiento al deber de informar por parte de la organización y se ha establecido un procedimiento para el ejercicio de derechos por parte de los interesados?
☐	¿Se identifica los incidentes de seguridad que afectan a datos personales, desencadenando acciones específicas como puede ser dar aviso al DPD?
☐ NI	Los incidentes de seguridad que consistan en una brecha de seguridad ¿Contemplan procedimientos frente a las violaciones de datos personales y la evaluación de si se requiere dar aviso a la AEPD o autoridad de control correspondiente y, en su caso, a los propios interesados?

Mp.info.2	Calificación de la información		
Categoría / dimensión **C**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Norma de calificación. ☐ Norma de valoración de la información y categorización del sistema ☐ Evidencia de valoración de la información por sus responsables. ☐ Relación de medidas de seguridad en función del nivel de calificación de la información y del tratamiento. ☐ Relación de medidas de seguridad en función del nivel de seguridad de la información y del tratamiento.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.info.2 NI	**¿Se han establecido criterios de calificación (o clasificación si se trata de información clasificada en base a la LSO o tratados internacionales) que permitan ajustar los requisitos de seguridad a dichos criterios?**		☐ SI ☐ NO
☐ NI	¿Se ha establecido alguna escala de calificación para la información sensible, como puede ser información 'USO OFICIAL", o bien se ha establecido una escala sujeta a normativa legal como es el caso de los sistemas que manejan información clasificada: ('SECRETO', 'RESERVADO', 'CONFIDENCIAL' o 'DIFUSIÓN LIMITADA'?		
☐ NI	¿Se ha establecido algún ámbito de distribución o difusión de la información, como puede ser información 'pública', 'de uso interno', 'restringida', etc.?		
☐ NI	¿Se han establecido medidas de seguridad específicas, en función del nivel de seguridad de la información de que se trate, o de su calificación, en relación al tratamiento realizado respecto a ella?		
☐	¿La PSI, o alguna norma interna o procedimiento que la desarrolle, recoge directa o indirectamente los criterios que en la organización determinan el nivel de seguridad requerido, atendiendo a la categorización del sistema y la valoración de los servicios soportados y la información manejada por éstos?		
☐	¿El responsable de cada información sigue los criterios determinados en el ENS para asignar a cada información el nivel de seguridad requerido, y es responsable de su documentación y aprobación formal?		
☐	¿Se le ha otorgado en exclusiva al responsable de cada información la potestad de modificar el nivel de seguridad requerido, de acuerdo a las disposiciones del ENS?		

Mp.info.3	Firma electrónica		
Categoría / dimensión **I A**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Nivel de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Relación de tipos de firma electrónica empleados. ☐ Evidencia de almacenamiento seguro de los certificados empleados.		
	☐ Evidencia de gestión de los certificados digitales, indicando si son cualificados o no, CA emisora, caducidad, etc.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.info.3 NI	**¿Se emplea un tipo de firma electrónica previsto en el vigente ordenamiento jurídico?**		☐ SI ☐ NO
☐ NI	Tratándose de una Administración Pública, ¿se utilizan cualesquiera de los procedimientos y formas señalados en la Ley 39/2015, en la Ley 40/2015, ambas de 1 de octubre, y en la Ley 6/2020, de 11 de noviembre, en relación con la utilización de certificados electrónicos para firma electrónica, sello electrónico y autenticación de sitio web u otros mecanismos admitidos por la normativa vigente? *NOTA: Únicamente debe considerarse la firma electrónica en el ámbito del sistema de información, como puede ser en un portal web o en la sede electrónica que se encuentren en el alcance.*		
☐ NI	Tratándose de un proveedor de la Administración Pública (como lo son todas las organizaciones obligadas por el ENS), ¿Se emplean asimismo certificados electrónicos reconocidos o cualificados para aquellos servicios que le presta a la Administración?		
Mp.info.3.r1	**¿Cuándo se emplean sistemas de firma electrónica avanzada, basados en certificados, éstos son cualificados?**		☐ SI ☐ NO
☐	¿Se emplean certificados electrónicos cualificados de proveedores que consten en la relación oficial española o europea? *NOTA: Pueden consultarse la relación española en: https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/Prestadores.aspx concretamente en la "Lista de confianza de prestadores cualificados de servicios electrónicos de confianza (TSL)" o en la "Trusted List Browser" de la European Commission, según establece el Reglamento Europeo eIDAS: https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home*		
☐	Tratándose de un prestador de servicios de confianza, por ejemplo, una CA emisora de certificados electrónicos, ¿cumple con la normativa vigente en España, como es la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza? ¿está certificado eIDAS?		
Mp.info.3.r2	**¿Se emplean algoritmos y parámetros de cifrado autorizados por el CCN o por un esquema nacional o europeo?**		☐ SI ☐ NO

Mp.info.3.r3	**Cuando proceda, ¿se garantiza la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, sin perjuicio de que se pueda ampliar este período de acuerdo con lo establecido en la Política de Firma Electrónica y de Certificados que sea de aplicación?** *NOTA: A tal fin se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación.*		☐ SI ☐ NO
Mp.info.3.r4	**¿Se usará firma electrónica avanzada basada en certificados cualificados complementada por un segundo factor del tipo «algo que se sabe» o «algo que se es»?**		☐ SI ☐ NO
Mp.info.3.r5	**¿Se usa firma electrónica cualificada, empleando productos certificados conforme a lo establecido en [op.pl.5]?**		☐ SI ☐ NO

Mp.info.4	**Sellos de tiempo**		
Categoría / dimensión **T**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia de gestión de los sellos de tiempo, indicando si son cualificados o no, CA emisora, caducidad, etc. ☐ Evidencia de almacenamiento seguro de los sellos de tiempo empleados.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.info.4	**¿Se adoptan determinadas cautelas para la utilización de sellos de tiempo?**		☐ SI ☐ NO
☐ NI	¿Se aplican los sellos de tiempo a aquella información que sea susceptible de ser utilizada como evidencia electrónica en el futuro?		

☐	Los datos pertinentes para la verificación posterior de la fecha ¿son tratados con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad?		
☐	¿Se renuevan regularmente los sellos de tiempo, hasta que la información protegida ya no sea requerida por el proceso administrativo al que da soporte? ¿Cómo se aplica el procedimiento de resellado?		
☐	¿Se emplean "sellos cualificados de tiempo electrónicos" atendiendo a lo dispuesto en el Reglamento (UE) nº 910/2014 (eIDAS), relativo a la identificación electrónica, y normativa de desarrollo?		
Mp.info.4.r1	**¿Se emplean productos certificados?**		☐ SI ☐ NO
☐	Para el Sellado de Tiempo ¿se utilizan productos certificados, según se determina en [op.pl.5]?		
☐	¿Se asigna una fecha y hora a los documentos electrónicos, conforme a lo establecido en la guía CCN-STIC-807 Criptología de empleo en el ENS?		

Mp.info.5	**Limpieza de documentos**		
Categoría / dimensión **C**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencia de documentos en la sede electrónica, portal web, etc., libres de metadatos no deseados. ☐ Normativa de revisión y limpieza de metadatos no deseados. ☐ Evidencia de herramienta de limpieza de metadatos o manual indicando como hacerlo manualmente.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.info.5 (NI)	**¿Se retira de los documentos electrónicos toda la información adicional contenida en campos ocultos, metadatos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento?**		☐ SI ☐ NO
☐	¿Se dispone de normativa específica que obligue a revisar, y en su caso a eliminar, los metadatos de un documento, especialmente antes de que éste abandone el perímetro de la organización, por ejemplo, subido a un portal web o adjunto a un correo electrónico?		
☐ (NI)	¿Se dispone de herramientas automáticas de revisión y limpieza de metadatos o, en su defecto, de documentación que expliquen cómo llevarlo a cabo manualmente en función del tipo de documento?		

Mp.info.6	Copias de seguridad		
Categoría / dimensión **D**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐ **Medida compensatoria**: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Normativa relativa a copias de seguridad. ☐ Evidencia de que las copias de seguridad están configuradas y se realizan de acuerdo a la normativa específica. ☐ Comparativa entre el RPO del BIA (si se dispone) con la normativa de copias de seguridad. ☐ Evidencia almacenamiento de copias dentro y/o fuera de las instalaciones. ☐ Evidencias de realización de copias y actuaciones en caso de error. ☐ Informes del proveedor, caso de copia externalizadas.		
	☐ Evidencia de pruebas de restauración.		
	☐ Evidencia de almacenamiento de copias en otros lugares. ☐ Normativa determinando requisitos de almacenamiento en otros lugares.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.info.6 (NI)	**¿Se realizan copias de seguridad que permitan recuperar los datos perdidos accidental o intencionadamente?**		☐ SI ☐ NO
☐ (NI)	¿Se realizan copias de seguridad con la periodicidad y plazos de retención requeridos por los servicios que soporta el sistema de información? *NOTA: Asimismo debe establecerse su forma, por ejemplo, totales diarias, totales semanales más incrementales diarias, etc.*		
☐	¿Las copias de seguridad se realizan acorde a lo que se determinan en normativa y/o procedimientos relativos a copias de seguridad?		
☐	¿La normativa de copias de seguridad está armonizada con el RPO calculado en el BIA, caso de disponerse de este último?		
☐	¿Si la herramienta informa, se ha determinado cómo actuar en caso de fallo en su realización?		
☐ (NI)	Si se externalizan las copias ¿Se reciben informes detallados del proveedor?		
Mp.info.6.r1	**¿La organización ha establecido y aprobado procedimientos formales de copia de seguridad y restauración?**		☐ SI ☐ NO
☐	¿Se prueban regularmente los procedimientos de copia de seguridad y restauración, con una frecuencia dependiendo de la criticidad de los datos y del impacto que causaría la falta de disponibilidad? ¿se ha determinado como actuar en el caso de detectarse desviaciones respecto a lo previsto?		

☐	¿Los procedimientos de respaldo establecen la frecuencia de las copias de seguridad?		
☐	¿Los procedimientos de respaldo establecen la necesidad de realizar copias semanales, mensuales, etc., adicionalmente a las copias diarias? *NOTA: Esta práctica es útil en el caso, por ejemplo, de un ataque de Ransomware donde deban desestimarse varias copias contaminadas.*		
☐	¿Los procedimientos de respaldo establecen los controles para el acceso autorizado a las copias de respaldo?		
☐	¿Los procedimientos de respaldo establecen los requisitos de almacenamiento en el propio lugar en que se realizan las copias?		
Mp.info.6.r2	**¿Se preservan las copias de seguridad de aquellos riesgos que también podrían afectar a la información original?**		☐ SI ☐ NO
☐	¿La normativa de respaldo establece los requisitos de almacenamiento en otros lugares?		
☐	¿Al menos una de las copias de seguridad se almacena de forma separada en lugar diferente, de tal manera que un incidente no pueda afectar simultáneamente tanto al repositorio original como a la copia? *NOTA: está ganando adeptos el llamado método del '3, 2, 1' que consiste en realizar tres (3) copias de seguridad, en al menos dos (2) tipos de soporte distintos, y una (1) de ellas almacenada en otra ubicación.*		

6.2.3.8 Medidas de Protección (PROTECCIÓN DE LOS SERVICIOS)

Mp.s.1	**Protección del correo electrónico**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Normativa de uso seguro del correo electrónico. ☐ Opciones empleadas para el cifrado de mensajes de correo electrónico, caso de ser necesario. ☐ Configuración y logs del filtro 'antispam'. ☐ Evidencia del análisis y protección antivirus del correo electrónico y de otras amenazas. ☐ Campañas de concienciación y de formación sobre el uso seguro del correo electrónico. ☐ Bastionado empleado para proteger el servidor de correo, si es propio.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.s.1 (NI)	**¿Se protege el correo electrónico frente a las amenazas que le son propias?**		☐ SI ☐ NO

☐	¿Se protege la información distribuida por medio de correo electrónico, tanto en el cuerpo de los mensajes, como en los anexos? ¿Si se emplea criptografía, ésta es acorde con la información a proteger?		
☐ NI	¿Se protege el servidor de correo electrónico, cuando es interno y/o gestionado por la propia organización, mediante una arquitectura y configuración de seguridad adecuadas a la relevancia del servicio de correo dentro del sistema de información, atendiendo a lo dispuesto en [op.exp.2]?		
Mp.s.1 NI	**¿Se protege a la organización frente a problemas que se materializan por medio del correo electrónico?**		☐ SI ☐ NO
☐ NI	¿Se dispone de herramientas de filtrado del correo no deseado o 'spam'?		
☐ NI	¿Se dispone de herramientas de protección contra el código dañino que pueda estar presente en los mensajes de correo electrónico?		
☐	¿Se dispone de herramientas que detecten el código móvil de tipo micro aplicación, en su expresión inglesa '*applet*'?		
Mp.s.1 NI	**¿Se han establecido para el personal normas de uso seguro del correo electrónico?**		☐ SI ☐ NO
☐	¿Se establecen en la normativa limitaciones al uso del correo electrónico como soporte de comunicaciones privadas?		
☐ NI	¿Se organizan actividades de concienciación y formación relativas al uso del correo electrónico?		

Mp.s.2	**Protección de servicios y aplicaciones web**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencias de desarrollo seguro de aplicaciones web.		
	☐ Informes de auditorías técnicas de 'caja negra'. ☐ Informes de auditorías técnicas de 'caja blanca'. ☐ Procedimiento de auditoría.		
	☐ Evidencias de prevención de ataques a 'proxies' y 'cachés'.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.s.2 NI	**Cuando la información requiera control de acceso ¿Se garantiza la imposibilidad de acceder a la información obviando la autenticación?**		☐ SI ☐ NO

☐ NI	¿Se evita que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado?		
☐ NI	¿Se previenen ataques de manipulación de URL?		
☐ NI	¿Se previenen ataques de manipulación de '*cookies*'?		
☐ NI	¿Se previenen ataques de inyección de código?		
☐ NI	¿Se previenen intentos de escalado de privilegios?		
☐ NI	¿Se previenen ataques de '*cross site scripting*'?		
NOTA: Para categorías BÁSICA y MEDIA, debe cumplirse al menos con una de las medidas de refuerzo R1 o R2, que siguen a continuación, mientras que, para categoría ALTA, se requiere cumplir con R2 y R3.			
Mp.s.2.r1	**¿Se realizan auditorías de seguridad de 'caja negra' sobre las aplicaciones web?**		☐ SI ☐ NO
☐	¿Se realizan auditorías técnicas de seguridad de "caja negra", de forma periódica, sobre las aplicaciones web durante la fase de desarrollo y antes de la fase de producción?		
☐	¿La frecuencia de las auditorías técnicas de seguridad está definido en un procedimiento de auditoría?		
Mp.s.2.r2	**¿Se realizan auditorías de seguridad de 'caja blanca' sobre las aplicaciones web?**		☐ SI ☐ NO
☐	¿Se realizan auditorías de seguridad de "caja blanca" sobre las aplicaciones web durante la fase de desarrollo?		
☐	¿Se emplean metodologías definidas y herramientas automáticas de detección de vulnerabilidades en la realización de las auditorías técnicas de seguridad sobre las aplicaciones web?		
☐	Una vez finalizada una auditoría técnica de seguridad, ¿se analizan los resultados y se solventan las vulnerabilidades encontradas mediante los procedimientos elaborados al efecto para la gestión de cambios?		
Mp.s.2.r3	**¿Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como "proxies" y, sistemas especiales de**		☐ SI ☐ NO

	almacenamiento de alta velocidad, conocidos en terminología inglesa como "cachés"?		

Mp.s.3	**Protección de la navegación web**		
Categoría / dimensión **Categoría**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Normativa de uso seguro de navegación web. ☐ Evidencias de campañas sobre navegación web segura. ☐ Evidencia de las acciones formativas dirigidas al personal encargado de la monitorización. ☐ Evidencias de protecciones implementadas frente a amenazas de la navegación web. ☐ Política de cookies.		
	☐ Evidencias de listas negras de URL o destinos no permitidos. ☐ Evidencias de registros de monitorización de la navegación web.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.s.3 NI	**¿Se protege, frente a las amenazas que le son propias, el acceso de los usuarios internos a navegar por internet?**		☐ SI ☐ NO
☐ NI	¿Se ha establecido una normativa destacando el uso de internet que se autoriza y las limitaciones de uso personal? ¿se concreta el uso permitido de conexiones cifradas?		
☐ NI	¿Se llevan a cabo regularmente actividades de concienciación sobre higiene en la navegación web, fomentando el uso seguro y alertando de usos incorrectos?		
☐	¿Se forma al personal encargado de la administración del sistema en monitorización del servicio y respuesta a incidentes?		
☐	¿Se protege la información de resolución de direcciones web y de establecimiento de conexiones?		
☐ NI	¿Se protege a la organización en general y al puesto de trabajo en particular frente a problemas que se materializan vía navegación web? NOTA: Por ejemplo, efectuando una configuración de seguridad de los navegadores siguiendo determinadas orientaciones de guías de configuración segura como es la *CCN-CERT BP/17 Recomendaciones de seguridad de Mozilla Firefox*.		

☐	¿Se protege contra la actuación de programas dañinos tales como páginas activas, descargas de código ejecutable, etc., previniendo la exposición del sistema a vectores de ataque del tipo spyware, ransomware, etc.?		
☐	¿Se ha establecido una política ejecutiva de control de cookies?		
Mp.s.3.r1	**¿Se han establecido restricciones a la navegación y monitorización de la misma?**		☐ SI ☐ NO
☐	¿Se registra el uso de la navegación web, estableciendo los elementos que se registran, el periodo de r tención de estos registros y el uso que el organismo prevé hacer de ellos?		
☐	¿Se ha establecido una función para la ruptura de canales cifrados a fin de inspeccionar su contenido, indicando qué se analiza, qué se registra, durante cuánto tiempo se retienen los registros y qué uso prevé hacer el organismo de estas inspecciones? *NOTA: Sin perjuicio que se puedan autorizar accesos cifrados singulares a destinos de confianza.*		
☐	¿Se ha establecido una lista negra de destinos vetados?		
Mp.s.3.r2	**¿Se ha establecido una lista blanca de destinos accesibles, de modo que todo acceso fuera de los lugares en la lista blanca esté vetado, salvo autorización singular expresa?**		☐ SI ☐ NO

Mp.s.4	**Protección frente a la denegación de servicio**		
Categoría / dimensión **D**	**Medida aplica**: SI ☐ NO ☐ **Medida auditada**: SI ☐ NO ☐ **Grado de implementación**: SI ☐ EN PROCESO ☐ NO ☐		
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia**: SI ☐ NO ☐		
Propuesta de evidencias			
	☐ Evidencias de elementos de protección tecnológica contra ataques de denegación de servicio. ☐ Evidencia de gestión de la capacidad, especialmente de comunicaciones. ☐ Filtros de configuración DDOS en los firewalls		
	☐ Procedimiento de reacción a ataques de denegación de servicio. ☐ Acuerdo de protección frente a ataques de denegación de servicio suscrito con el proveedor de acceso a internet. ☐ implantación de Herramienta específica de DDOS por parte de la organización.		
	Aspectos a evaluar	**Hallazgos del auditor / referencia a las evidencias**	**Cumple**
Mp.s.4 (NI)	**¿Se han establecido medidas preventivas frente a ataques de denegación de servicio (DoS) y denegación de servicio distribuido (DDoS)?**		☐ SI ☐ NO

☐	¿Se ha planificado y dotado al sistema de capacidad suficiente para atender a la carga prevista con holgura?		
☐	¿Se han desplegado tecnologías para prevenir los ataques conocidos?		
Mp.s.4.r1	**¿Se han establecido sistemas detección, notificación y tratamiento de ataques de DoS o DDoS?**		☐ SI ☐ NO
☐	¿Se ha establecido un sistema de detección y tratamiento de ataques de denegación de servicio (DoS y DDoS)?		
☐	¿Se han establecido procedimientos de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones?		
☐	¿Se dispone de un acuerdo suscrito con el proveedor de comunicaciones para que aporte protección frente a ataques de denegación de servicio como alternativa o complemento a los medios propios de detección y respuesta?		
Mp.s.4.r2	**¿Se detecta y se evita el lanzamiento de ataques desde las propias instalaciones, perjudicando a terceros?**		☐ SI ☐ NO

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