centro criptológico nacional

Perfil de Cumplimiento Específico
CCN-STIC 852

Perfil de Cumplimiento Específico Organismos Pagadores

Mayo 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
2023.07.20 09:26:47 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-23-070-X
Fecha de Edición: mayo de 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

En virtud del principio de proporcionalidad y para facilitar la conformidad con el Esquema Nacional de Seguridad (ENS) a determinadas entidades o sectores de actividad concretos, se podrán implementar perfiles de cumplimiento específicos que comprenderán aquel conjunto de medidas de seguridad que, trayendo causa del preceptivo análisis de riesgos, resulten de aplicación para una concreta categoría de seguridad.

Las Guías CCN-STIC, del Centro Criptológico Nacional, podrán establecer perfiles de cumplimiento específicos para entidades o sectores concretos, que incluirán la relación de medidas y refuerzos que en cada caso resulten aplicables, o los criterios para su determinación.

El Centro Criptológico Nacional, en el ejercicio de sus competencias, validará y publicará los correspondientes perfiles de cumplimiento específicos que se definan, permitiendo a aquellas entidades comprendidas en su ámbito de aplicación alcanzar una mejor y más eficiente adaptación al ENS, racionalizando los recursos requeridos sin menoscabo de la protección perseguida y exigible.

Las auditorías se realizarán en función de la categoría del sistema y, en su caso, del perfil de cumplimiento específico que corresponda, según lo dispuesto en el Anexo I y Anexo III del Real Decreto 311/2022, de 3 de mayo, y de conformidad con lo regulado en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de la Información.

A tal fin, tras realizar un estudio de las necesidades de seguridad, de los recursos y tras un análisis de riesgos contemplando las vulnerabilidades y amenazas a las que se ven expuestas de los Organismos Pagadores y con el objetivo de garantizar la máxima seguridad de los sistemas de información, se da cumplimiento al mandato impuesto al CCN validando el siguiente Perfil de Cumplimiento Específico para Organismos Pagadores, que permita la implantación del ENS en los mismos, con necesidades de seguridad de categoría MEDIA.

En el proceso de elaboración del perfil específico de cumplimiento de los organismos pagadores de las ayudas de los fondos europeos, se ha procedido a realizar un análisis exhaustivo de la normativa implicada, de los requisitos impuestos por el legislador europeo[1], los requerimientos derivados del Esquema Nacional de Seguridad [Real Decreto 311/2022], de 3 de mayo, implicaciones de terceros en las actividades y funciones y particularidades propias del sujeto obligado. Para este proceso se ha contado con la colaboración del organismo de coordinación nacional y de organismos representativos.

[1] Principalmente Reglamento (UE) 2021/2116 del Parlamento Europeo y del Consejo de 2 de diciembre de 2021 sobre la financiación, la gestión y el seguimiento de la política agrícola común y por el que se deroga el Reglamento (UE) n.o. 1306/2013 y Reglamento Delegado (UE) 2022/127 de la Comisión de 7 de diciembre de 2021 que completa el Reglamento (UE) 2021/2116 del Parlamento Europeo y del Consejo con normas relativas a los organismos pagadores y otros órganos, la gestión financiera, la liquidación de cuentas, las garantías y el uso del euro.

Gracias a la colaboración de éstos, el CCN ha podido diseñar y desplegar un perfil adaptado a la realidad legislativa y particularidades de los organismos objeto de análisis.

Como elemento final, se ha incluido la herramienta en Excel que recoge a modo de ayuda, información relacionada con la aplicación del perfil y sinergias de las normas que afectan a los organismos pagadores.

2. OBJETO

Esta guía es el resultado de la aplicación del artículo 30 del Real Decreto 311/2022, de 3 de mayo. en base a lo cual y conforme a los principios de proporcionalidad y eficiencia y eficacia, se presenta el Perfil de Cumplimiento Especifico de Organismos Pagadores y de Coordinación, particularizando y adaptando determinados requisitos del Esquema Nacional de Seguridad para estos sujetos.

No olvidemos que estos organismos, deben cumplir con los requisitos establecidos por el legislador europeo y que implican necesariamente un sistema de seguridad de la información basado en el estándar de seguridad[2]. Los organismos pagadores podrán beneficiarse indirectamente mediante la aplicación de este perfil, de la implementación de un único marco de seguridad[3] para sus sistemas de información. No obstante, los requerimientos de certificación se pueden modular en base a la responsabilidad de la gestión y control de gasto anual bajo el límite de 400 millones EUR[4].

El CCN no ha sido ajeno a las diferencias significativas existentes entre organismo pagadores en base a la responsabilidad en la gestión de las cuantías de las ayudas FEADER y Feaga, y el Perfil de Cumplimiento presentado, considera diferentes niveles de exigencia en base a esta obligación de certificación que recae sobre algunos de ellos.

Los organismos deberán analizar el grado de exigencia que les es de aplicación conforme al legislador europeo y proceder a desplegar los requisitos establecidos. [5]

---

[2] Reglamento Delegado (UE) 2022/127 de la Comisión de 7 de diciembre de 2021 que completa el Reglamento (UE) 2021/2116 del Parlamento Europeo y del Consejo con normas relativas a los organismos pagadores y otros órganos, la gestión financiera, la liquidación de cuentas, las garantías y el uso del euro (en adelante, Reglamento Delegado (UE) nº 2022/127), Anexo I, 3 INFORMACIÓN Y COMUNICACIÓN, letra B), "La seguridad de los sistemas de información deberá estar certificada de conformidad con la norma ISO 27001: Information Security management systems – Requirements (ISO) (Sistemas de gestión de la seguridad de la información-Requisitos) (ISO)."

[3] Reglamento Delegado (UE) nº 2022/127, Anexo I, 3 INFORMACIÓN Y COMUNICACIÓN, letra B), "Los Estados miembros podrán certificar, previa autorización de la Comisión, la seguridad de sus sistemas de información de conformidad con otras normas aceptadas si estas normas garantizan un nivel de seguridad equivalente, como mínimo, al previsto en la norma ISO 27001."

[4] Reglamento Delegado (UE) nº 2022/127 Anexo I, 3 INFORMACIÓN Y COMUNICACIÓN, letra B), "(…) *no se aplicará a los organismos pagadores responsables de la gestión y control de un gasto anual no superior a 400 millones EUR, si el Estado miembro en cuestión ha informado a la Comisión de su decisión de aplicar.*"

No es objeto de esta guía realizar un análisis pormenorizado de las normas y desplegar una equivalencia de la conformidad a nivel europeo y la aplicación diferenciada de los controles y refuerzos del ENS.[6]

Tampoco es objeto de esta guía, analizar la exigencia de certificación de otras normas que no sea el propio ENS, por cuanto cada organismo deberá analizar la necesidad de someterse a otros procesos de certificación, y específicamente aquellos relacionados con las exigencias del legislador europeo.

3. ALCANCE: ORGANISMOS PAGADORES Y DE COORDINACIÓN

Este perfil, es aplicable exclusivamente a los organismos pagadores y de coordinación de los fondos europeos agrícolas, de conformidad con lo dispuesto en el Reglamento Delegado (UE) 2022/127 de la Comisión de 7 de diciembre de 2021 que completa el Reglamento (UE) 2021/2116 del Parlamento Europeo y del Consejo con normas relativas a los organismos pagadores y otros órganos, la gestión financiera, la liquidación de cuentas, las garantías y el uso del euro Anexo I, 3 Información y Comunicación, letra B), al considerarse posible la certificación de sistemas de información de los organismos pagadores nacionales, con otras normas que garanticen un nivel equivalente a lo previsto en la ISO 27001.

Tal y como establece el Reglamento (UE) 2021/2116 del Parlamento Europeo y del Consejo de 2 de diciembre de 2021 sobre la financiación, la gestión y el seguimiento de la política agrícola común y por el que se deroga el Reglamento (UE) n.o. 1306/2013, en su artículo 9.1, los organismos pagadores serán los servicios u organismos de los Estados miembros y, en su caso, de las regiones responsables de la gestión y el control de los gastos Fondo Europeo Agrícola de Garantía (FEAGA) y del Fondo Europeo Agrícola de Desarrollo Rural (FEADER).

El régimen de la Unión Europea posibilita a los Estados Miembros, a autorizar la designación de varios organismos pagadores a nivel regional, estableciendo en estos casos un único [7]organismo de coordinación nacional.

Además, el legislador europeo ha considerado la posibilidad de que los organismos pagadores puedan delegar la realización de tareas, a excepción de los pagos. [8]

Y esta es la situación presente, de manera que en España se considera un Organismo de Coordinación y varios organismos pagadores.

---

[6] Reglamento Delegado (UE) nº 2022/127, Anexo I, 3 INFORMACIÓN Y COMUNICACIÓN, letra B), "Los Estados miembros podrán certificar, previa autorización de la Comisión, la seguridad de sus sistemas de información de conformidad con otras normas aceptadas si estas normas garantizan un nivel de seguridad equivalente, como mínimo, al previsto en la norma ISO 27001."

[7] Reglamento (UE) 2021/2116; artículo 10 "*Los Estados miembros que autoricen a más de un organismo pagador también designarán un organismo público de coordinación (…)*"

[8] Reglamento (UE) 2021/2116; artículo 9.1.1 "*A excepción de la realización de los pagos, los organismos pagadores podrán delegar la realización de las tareas a que se refiere el párrafo primero*."

Por ello, el perfil se dirige a; [9]

a) Organismo de Coordinación Nacional; Fondo Español de Garantía Agraria, Organismo Autónomo (FEGA O.A.). Organismo de coordinación[10], entendiendo por tal el organismo encargado, entre otras cuestiones, de centralizar la información que deba ponerse a disposición de la Comisión Europea, adoptar o coordinar medidas destinadas a resolver las deficiencias, fomentar y, cuando sea posible, garantizar la aplicación armonizada de la normativa de la Unión.

b) Organismos Pagadores; Las comunidades autónomas dispondrán de un único organismo pagador de las ayudas respecto de las que tengan competencia de gestión y control del pago del gasto, con cargo a los fondos europeos; Fondo Europeo Agrícola de Garantía (FEAGA) y del Fondo Europeo Agrícola de Desarrollo Rural (FEADER).

   Estos organismos, a nivel de exigencias de seguridad de la información y del presente perfil, se diferencian en: [11]

   a. con un gasto superior a 400 millones de euros.

   b. con un gasto no superior a 400 millones de euros.

c) Organismos Delegados[12]; Los organismos pagadores pueden delegar la realización de tareas, salvo la delegación del pago, de conformidad con Reglamento (UE) 2021/2116, previa celebración de acuerdo escrito, cerciorándose de la existencia de sistemas eficaces previos para garantizar las tareas delegadas y verificación del cumplimiento de las obligaciones. [13]

---

[9] Real Decreto 92/2018 de 2 de marzo, por el que se regula el régimen de los organismos pagadores y de coordinación con los fondos europeos agrícolas, FEAGA y FEADER

[10] Considérese lo dispuesto en relación con organismo pagador a nivel nacional, en el artículo 9.2.3 del Reglamento (UE) 2021/2116; "Cuando *se establezcan organismos pagadores a nivel regional, los Estados miembros autorizarán, además, un organismo pagador a nivel nacional para los regímenes de ayuda que, por su naturaleza, deben gestionarse a nivel nacional, o encomendarán la gestión de dichos regímenes a sus organismos pagadores regionales*."

[11] Diferencia con un impacto significativo, dado que conforme al Reglamento Delegado (UE) nº 2022/127, Anexo I Criterios de Autorización, artículo 1.3 Información y Comunicación, letra B) Seguridad de los Sistemas de Información;

"*Lo dispuesto en los párrafos primero y segundo no se aplicará a los organismos pagadores responsables de la gestión y control de un gasto anual no superior a 400 millones EUR, si el Estado miembro en cuestión ha informado a la Comisión de su decisión de aplicar, en lugar de ello, una de las normas siguientes:*

—International Standards Organisation 27002: Code of practice for Information Security management (Organización internacional de normalización 27002: Código de prácticas para la gestión de la seguridad de la información) (ISO),

—Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch/IT Baseline Protection Manual (Manual de protección informática de base) (BSI),

—Information Systems Audit and Control Association: Control objectives for Information and related Technology (Asociación para la auditoría y el control de los sistemas de información: Objetivos de control para la información y tecnologías afines) (COBIT)."

[12] No se ha particularizado la delegación de competencias en relación con medidas de intervención, conforme al Artículo 3 del Reglamento Delegado (UE) 2022/127.

[13] Para mayor detalle, ver Reglamento Delegado (UE) nº 2022/127, Anexo I, 1. ENTORNO INTERIOR, Letra D) Delegación

Considerando la diferenciación de sujetos que pueden existir en el ecosistema de gestión de ayudas FEAGA y FEADER, a los efectos del Real Decreto 311/2022, de 3 de mayo, se debe considerar:

a) Todos los sujetos son organismos sometidos a la normativa administrativa, siendo sujetos del sector público y por tanto siendo de aplicación el Real Decreto 311/2022, de 3 de mayo.

b) Los organismos pagadores que realicen actos de delegación deberán considerar la existencia de una delegación de funciones asimiladas a una cadena de suministro [op.ext.3], y en todo caso seguirán siendo plenamente responsables de la legalidad y regularidad de las operaciones subyacentes[14], manteniendo la diligencia debida, requiriendo sistemas eficaces en los organismos delegados y verificando el cumplimiento de la normativa.

c) El organismo de coordinación puede ser a su vez un organismo de pago, pudiendo acogerse al perfil de cumplimiento, en base al límite de gasto anual 400 millones EUR.

Por último, debe considerarse la existencia de otras entidades públicas[15] cuyas competencias y funciones se circunscriban a servicios tecnológicos, gestión de la infraestructura y arquitectura, gestión de las comunicaciones e interconexiones de sistemas, coordinación de servicios tecnológicos con terceros, redundancias de sistemas y servicios, planes y estrategias de continuidad y otras medidas asimiladas. Esta circunstancia adquiere una mayor importancia en los organismos pagadores, que han de enfocar sus esfuerzos en el cumplimiento de estructura y organización interna declarada por el legislador europeo. Por eso, determinadas medidas de seguridad pueden delegarse a estas entidades, en su ejecución, pero no en su responsabilidad, por cuanto el organismo deberá cerciorarse de la ejecución y verificar que se mantiene el cumplimiento requerido por la medida. Cuando se realice una delegación, deberá figurar en la declaración de aplicabilidad del perfil correspondiente, la concreta delegación y alcance de esta, y las medidas del organismo para cerciorarse y verificar el cumplimiento por parte de la entidad pública delegada.

3.1 METODOLOGÍA SEGUIDA PARA EL DESARROLLO DEL PERFIL

Este perfil ha sido desarrollado gracias a la interactuación del sujeto afectado, que ha participado mediante una representación muestra, en reuniones de trabajo, que han servido para poder conocer los riesgos presentes y adaptar las medidas necesarias que han permitido presentar la aplicación del ENS de manera proporcional para los organismos pagadores nacionales.

[14] Anexo I Real Decreto 311/2011, Recursos Externos [op.ext] “Cuando la organización utilice recursos externos (servicios, productos, instalaciones o personal), mantendrá la plena responsabilidad de los riesgos para la información tratada o los servicios prestados, debiendo adoptar las medidas necesarias para ejercer su responsabilidad y mantener el control en todo momento.”

[15] Sometidas a todos los efectos al cumplimiento del Real Decreto 311/2022.

Estas reuniones han sido constantes a lo largo de varios meses y han permitido conocer al sujeto objeto y las diferencias entre ellos, analizar los requerimientos legales particulares, conocer la tendencia de seguridad presentada, y adaptar los requisitos del Esquema Nacional, en un perfil de cumplimiento que trata de garantizar la conformidad del ENS y el pleno respeto a lo dispuesto por el legislador europeo.

Para la elaboración de este perfil ha sido indispensable la colaboración del organismo de coordinación nacional, que ha sido un canal imprescindible para unificar criterios y necesidades. El legislador europeo ha sido respetuoso con la distribución territorial y competencial de los Estados miembros, por cuanto se ha permitido la existencia de un organismo coordinador nacional [FEGA] y diferentes organismos pagadores. [16] No obstante, esta previsión, implica 17 sistemas de información diferenciados en nuestro Estado, bajo el paraguas de las autonomías y sus estrategias diferenciadas de seguridad, además del propio sistema del organismo de coordinación nacional.

Las principales conclusiones de esta metodología se han materializado en el perfil que se presenta, y que pueden concretarse en:

a) Los organismos pagadores [y de coordinación] tienen particularidades como sujeto del sector público, tanto a nivel funcional y competencial, como en su propio sistema de información, interconexiones, dependencias, delegaciones y supervisiones, que hacen conveniente la materialización de un perfil de cumplimiento especifico.

b) Los organismos pagadores presentan diferencias en relación con las obligaciones de seguridad impuestas por el legislador europeo, por cuanto se hace recomendable una modulación de las obligaciones impuestas a nivel nacional para la seguridad de la información.

c) A nivel nacional, cuentan con un organismo de coordinación nacional que desarrolla, además, una labor de ayuda y colaboración en materia de seguridad con todos los organismos.

d) Se presentan a nivel general, dependencias de los organismos pagadores autonómicos con otras entidades públicas con competencias tecnológicas y que tendrán un impacto significativo en el cumplimiento de la seguridad y en las evidencias presentables en auditorias, y especialmente en aquellas desarrolladas para verificar el cumplimiento de la normativa europea en materia de ayudas agrarias.[17]

e) Los organismos pagadores están obligados por dos normas de efecto directo, a desarrollar un sistema de gestión de seguridad de la información, por cuanto se

[16] Considérese lo dispuesto en relación con organismo pagador a nivel nacional, en el artículo 9.2.3 del Reglamento (UE) 2021/2116; “Cuando se establezcan organismos pagadores a nivel regional, los Estados miembros autorizarán, además, un organismo pagador a nivel nacional para los regímenes de ayuda que, por su naturaleza, deben gestionarse a nivel nacional, o encomendarán la gestión de dichos regímenes a sus organismos pagadores regionales.””

[17] Considérese aquellos procesos de revisión desarrollados bajo el amparo del artículo 55 del Reglamento (UE) 2021/2116, considerando el sistema de seguridad de la información que se requiere a los organismos pagadores en el Reglamento Delegado (UE) 2022/127.

hace necesario facilitar el cumplimiento de ambas normas, bajo las premisas que el legislado nos ha dado. [18]

f) Existe una tendencia común al estudio y despliegue de las herramientas de seguridad del CCN, por parte de los organismos o de sus responsables tecnológicos, por cuanto muchos de los controles de seguridad, se podrían desplegar con mayor facilidad de la que inicialmente se preveía.

3.2 ANÁLISIS DE REQUISITOS LEGISLADOR EUROPEO

Por eso en la elaboración de este perfil de cumplimiento especifico se ha tenido especial cuidado en integrar la voluntad del legislador europeo [y nacional]. Este análisis era necesario para poder conocer la naturaleza, finalidad, objeto, y, en definitiva, razón de ser de los Organismos Pagadores. Y para ello, se debería conocer en detalle la normativa europea y su conexión con la normativa de desarrollo nacional.

Gracias a este análisis se pudieron conocer los servicios y la información manejada por los organismos y trazar inicialmente una categoría, ajustada con los requisitos y criterios presentes en el Real Decreto 311/2022, de 3 de mayo.

No siendo una enumeración taxativa, sino meramente enunciativa en base a la importancia que han tenido en el presente, se han considerado[19]:

Rango	Norma	Descripción	
Norma (UE)	**Reglamento (UE) 2021/2116**	Reglamento (UE) 2021/2116 del Parlamento Europeo y del Consejo de 2 de diciembre de 2021 sobre la financiación, la gestión y el seguimiento de la política agrícola común y por el que se deroga el Reglamento (UE) n.o 1306/2013	Deroga el anterior y modifica parte del contenido. Esta modificado posteriormente por el Reglamento Delegado (UE) 2022/127 de la Comisión de 7 de diciembre de 2021 que completa el Reglamento (UE) 2021/2116 del Parlamento Europeo y del Consejo con normas relativas a los organismos pagadores y otros órganos, la gestión financiera, la liquidación de cuentas, las garantías y el uso del euro
Norma (UE)	**Reglamento (UE) 2021/2115 del Parlamento Europeo y del Consejo**	Reglamento (UE) 2021/2115 del Parlamento Europeo y del Consejo, de 2 de diciembre de 2021, por el que se establecen normas en relación con la ayuda a los planes estratégicos que deben elaborar los Estados miembros en el marco de la política agrícola común (planes estratégicos de la PAC), financiada con cargo al Fondo Europeo Agrícola de Garantía (FEAGA) y al Fondo Europeo Agrícola de Desarrollo Rural (Feader), y por el que se derogan los	Fija pautas para definición y condiciones de los planes estratégicos de la PAC, intervenciones en sectores concretos, y puntos asociados a objetivos e Indicadores

[18] Tanto a nivel nacional, el Real Decreto 311/2022, habilitando el desarrollo de perfiles de cumplimiento especifico, como a nivel europeo el Reglamento Delegado (UE) 2022/127, con su capacidad de "autorizar" certificaciones de sistemas de seguridad de la información equivalentes a la ISO 27001,

[19] Aunque no se han incluido específicamente, se ha tenido en cuenta Reglamento (UE/EURATOM) 2020/2093 del Consejo, Reglamento (UE/EURATOM) 2018/1046 del Parlamento Europeo y del Consejo, Reglamento (UE) 1306/2013 del Parlamento Europeo y del Consejo, Reglamento Delegado (UE) 907/2014 de la Comisión, Reglamento de Ejecución (UE) 908/2014 de la Comisión, y Reglamento de Ejecución (UE) 2022/128 de la Comisión de 21 de diciembre de 2021.

Rango	Norma	Descripción	
		Reglamentos (UE) n.º 1305/2013 y (UE) n.º 1307/2013	
Norma (UE)	**Reglamento Delegado (UE) 2022/127**	Reglamento Delegado (UE) 2022/127 de la Comisión de 7 de diciembre de 2021 que completa el Reglamento (UE) 2021/2116 del Parlamento Europeo y del Consejo con normas relativas a los organismos pagadores y otros órganos, la gestión financiera, la liquidación de cuentas, las garantías y el uso del euro	Completa información del Reglamento (UE) 2021/2016 relacionado con gestión, cuentas y garantías. Importante Anexos relacionados.
Norma (UE)	**Reglamento de Ejecución (UE) 2022/128**	Reglamento de Ejecución (UE) 2022/128 de la Comisión, de 21 de diciembre de 2021, por el que se establecen disposiciones de aplicación del Reglamento (UE) 2021/2116 del Parlamento Europeo y del Consejo sobre los organismos pagadores y otros órganos, la gestión financiera, la liquidación de cuentas, los controles, las garantías y la transparencia	Desarrolla puntos del Reglamento (UE) 2021/2116 relacionados con autorizaciones a OOPP de los organismos pagadores y los organismos de coordinación. Establece pautas de seguimiento y supervisión
Norma (UE)	**Reglamento Delegado (UE) 2023/57**	Reglamento Delegado (UE) 2023/57 de la Comisión, de 31 de octubre de 2022, que modifica y corrige el Reglamento Delegado (UE) 2022/127 por el que se completa el Reglamento (UE) 2021/2116 del Parlamento Europeo y del Consejo.	Correcciones Reglamento Delegado (UE) 2021/127
Norma (ESP)	**Ley 30/2022**	Ley 30/2022, de 23 de diciembre, por la que se regulan el sistema de gestión de la Política Agrícola Común y otras materias conexas	Normas básicas y de coordinación del sistema de ayudas agrícolas (PAC) y régimen sancionador.
Norma (ESP)	**Real Decreto 1046/2022**	Real Decreto 1046/2022, de 27 de diciembre, por el que se regula la gobernanza del Plan Estratégico de la Política Agrícola Común en España y de los fondos europeos agrícolas FEAGA y Feader	Establece el régimen de organismos pagadores y de coordinación de los fondos europeos agrícolas, FEAGA y FEADER, establece al FEGA como organismo de coordinación. También recoge la necesidad de que en cada Comunidad Autónoma exista un organismo pagador de los gastos originados por el FEAGA y el FEADER y una autoridad competente, encargada, tanto de autorizar el precitado organismo, como de vigilar y controlar su correcto funcionamiento.
Norma (ESP)	**Real Decreto 515/2013**	Real Decreto 515/2013, de 5 de julio, por el que se regulan los criterios y el procedimiento para determinar y repercutir las responsabilidades por incumplimiento del Derecho de la Unión Europea	Regula el proceso derivado del incumplimiento de Derechos de la UE

De todas estas normas, resultaba de gran impacto una de ellas, que debió ser analizada con mayor detalle y atención; Reglamento Delegado (UE) 2022/127 en relación con el Reglamento (UE) 2021/2116. Esta norma desarrolla en su Anexo I, los requerimientos de seguridad que los organismos pagadores deben mantener y despliega requisitos asociados a los servicios y la seguridad de la información. [20]

[20] Punto que nos recuerda el Real Decreto 1046/2022 en su artículo 9, "4. 4. La seguridad de los sistemas de información deberá adecuarse a lo previsto en el anexo I apartado 3.b) del Reglamento Delegado (UE) 2022/127 de la Comisión, de 7 de diciembre de 2021, que completa el Reglamento (UE) 2021/2116 del Parlamento Europeo y del Consejo con normas relativas a los organismos pagadores y otros órganos, la gestión financiera, la liquidación de cuentas, las garantías y el uso del euro.
Todas las comunicaciones entre los organismos pagadores y el organismo de coordinación de organismos pagadores se realizarán cumpliendo los principios de seguridad de la información."

Reglamento (UE) 2021/2116	
Articulo	**Punto de referencia**
Art.9	Criterios de autorización de organismos pagadores.
Art.10	Organismo de coordinación Cuando exista más de un organismo pagador deberá designarse un organismo de coordinación nacional.
Art. 12	Organismos de certificación.
Art. 67	Conservación e intercambio de datos.
Art. 91	Confidencialidad.
Art. 99	Información a los beneficiarios de la publicación de datos que les conciernen
Art. 101	CAPÍTULO V Protección de datos de carácter personal.

Reglamento Delegado (UE) 2022/127	
Articulo	**Punto de referencia**
Art.1	Condiciones para la autorización de los organismos pagadores.
Art.2	Condiciones para la autorización de los organismos coordinadores.
Art.3	Obligaciones de los organismos pagadores en lo que respecta a la intervención pública.

Anexo I	3. INFORMACIÓN Y COMUNICACIÓN
A) Comunicación	Se adoptarán procedimientos necesarios para aplicar la normativa de la Unión Europea (Entre otros, registros, instrucciones, bases de datos y listas de control)
B) Seguridad de los sistemas de información	La seguridad de los sistemas de información deberá estar certificada de conformidad con la norma ISO 27001.
	Los **Estados miembros podrán certificar**, previa **autorización** de la Comisión, la seguridad de sus sistemas de información de conformidad con otras normas aceptadas, si estas normas garantizan un nivel de seguridad equivalente, como mínimo, al previsto en la norma ISO 27001.
	No se aplicará a los organismos pagadores responsables de la gestión y control de un gasto anual **no superior a 400 millones EUR**, si **el Estado miembro en cuestión ha informado a la Comisión** de su decisión de aplicar, en lugar de ello, una de las normas siguientes: a) 27002 b) BSI c) COBIT
	Los organismos encargados de gestión y control de un gasto de la Unión anual no superior a 400 millones EUR, bajo la decisión del Estado miembro, pueden no requerir proceso de certificación

4. NORMAS DE SEGURIDAD.

4.1 ENS RD 311/2022

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el nuevo Esquema Nacional de Seguridad, aprueba nuestro marco (legal) de ciberseguridad.
El Esquema Nacional de Seguridad contiene los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades sometidas a su aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios.

Los sistemas de información sometidos a la aplicación del ENS serán objeto de un proceso para determinar su conformidad con el ENS, y a tal efecto, los sistemas de categoría MEDIA o ALTA precisarán de una auditoría para la certificación de su conformidad, mientras que los sistemas de categoría BÁSICA solo requerirán de una autoevaluación para su declaración de la conformidad, sin perjuicio de que se puedan someter igualmente a una auditoria de certificación.[21]

De las conclusiones obtenidas durante el proceso de análisis y adaptación de este perfil, se ha extraído que la categoría recomendada para los organismos pagadores es la categoría MEDIA. No así existen adaptaciones en relación con medidas concretas, y en base a las responsabilidades por la gestión de los gastos europeos.

4.2 ISO/IEC 27001

Actualmente la ISO/IEC 27001:2013 / UNE-EN ISO/IEC 27001:2017, Sistemas de Gestión de la Seguridad de la Información, convive con la nueva versión de la norma ISO /IEC[22] 27001:2022 Information security, cybersecurity and privacy protection. Esta convivencia será a lo largo de 36 meses, periodo de adaptación en el que las entidades deberán adecuar sus sistemas a la última versión de la norma.

La ISO 27001, es una norma de carácter voluntario que emplea la estructura de alto nivel, de las normas ISO, Anexo (L) por lo tanto mantiene la compatibilidad con otras normas y cuyo clausulado es complementado mediante un Anexo (A) que contiene el listado de controles de seguridad que las organizaciones deben desplegar en los sistemas. Esta norma internacional especifica los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información en el contexto de una organización, e incluye los requisitos para la apreciación y el tratamiento de los riesgos de seguridad de información. Esta

[21] No olvidemos que a los efectos de lo establecido en el artículo 31 del Real Decreto 311/2022, apartado 2, "La auditoría se realizará en función de la categoría del sistema y, en su caso, del perfil de cumplimiento específico que corresponda, según lo dispuesto en los anexos I y III y de conformidad con lo regulado en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información"
[22] ISO (Organización Internacional de Normalización) e IEC (la Comisión Electrotécnica Internacional) constituyen el sistema especializado para la normalización a nivel mundial.

noma es certificable y puede complementarse, con otras fuentes de controles, las medidas que incluye para la seguridad de los sistemas de las organizaciones[23].

4.3 ANÁLISIS DE EQUIVALENCIA ENTRE NORMAS DE SEGURIDAD.

A lo largo del proceso de elaboración de este perfil, se fueron produciendo diferentes cambios, tanto a nivel legislativo como a nivel de normas de seguridad.

Actualmente coexisten dos normas ISO 27001(la versión del año 2013 y la versión del año 2022), ambas normas certificables. Por eso, era necesario realizar un análisis de equivalencia de ambas normas y posteriormente, de estas con el ENS.

4.3.1 ISO 27001:2013 – ENS

A alto nivel, del análisis efectuado se puede considerar que la ISO 27001 en su versión 2013, requiere controles adicionales para poder ser equivalente al ENS en toda su aplicación, dado que no considera determinadas medidas de seguridad que, si son contempladas por el Anexo II del Real Decreto 311/2022, de 3 de mayo.

No obstante, el estándar ISO es flexible en este sentido y permite añadir sistema de fuentes a sus controles del anexo A, por cuanto se pueden añadir todas aquellas medidas y/o refuerzos del Anexo II del Real Decreto 311/2022, de 3 de mayo, que no son considerados por la norma del año 2013.

Por otro lado, a nivel del ENS se deben considerar los controles de continuidad y alternatividad [op.cont.] para lograr la equivalencia completa, dado que para el ENS no son controles aplicables en la categoría MEDIA.

4.3.2 ISO 27001:2013 - ISO 27001:2022

La ISO/ IEC 27001:2022 “Information security, cybersecurity and privacy protection — Information security management systems — Requirements”, heredera de la anterior ISO / IEC 27001:2013 tras la correspondiente revisión y evolución, presenta un cambio significativo en la estructura del Anexo A, al reagruparse los controles en cuatro grandes bloques; Controles organizacionales; Controles de personas; Controles físicos, Controles tecnológicos.

De los 114 controles, se ha pasado a 93, que han sido reestructurados en 4 grandes dominios o capítulos y se han añadido controles nuevos:

5.7 Inteligencia de amenazas
5.23 Seguridad de la información para el uso de servicios en la nube
5.30 Preparación de las TIC para la continuidad del negocio
7.4 Vigilancia de la seguridad física
8.9 Gestión de la configuración
8.10 Eliminación de información

[23] Por ejemplo, pueden añadirse los controles de la ISO 27017, relacionados con seguridad en el cloud. ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

8.11 Enmascaramiento de datos
8.12 Prevención de fuga de datos
8.16 Actividades de seguimiento
8.22 Filtrado web
8.28 Codificación segura

Los capítulos son:

37	Capítulo 5	Controles organizacionales	Bloque general de seguridad
8	Capítulo 6	Controles de personas	Se refiere a individuos
14	Capítulo 7	Controles físicos	Se refiere a objetos físicos
34	Capítulo 8	Controles tecnológicos	Se refiere a tecnología

4.3.3 ISO /IEC 27002: 2022: Código de prácticas para la gestión de la seguridad de la información

La ISO /IEC 27002: 2022, está diseñada para que sea utilizada como una guía de aplicación o referente, para determinar e implementar controles para el tratamiento de riesgos de seguridad de la información en un Sistema de gestión de seguridad de la información (SGSI) basado en ISO/IEC 27001. También puede usarse como un documento de orientación e implementación de los controles de seguridad de la información comúnmente aceptados, por cuanto puede enriquecer otros marcos de seguridad, como Esquema Nacional de Seguridad.

Esta norma no es certificable, por lo que los sistemas basados en la misma pueden ser susceptibles de ser certificables bajo la norma de requisitos ISO 27001.

A nivel general la norma versión 2022 dispone de unas medidas más alineadas con el Real Decreto 311/2022, de 3 de mayo, al haber desplegado controles muy necesarios en el nuevo escenario de ciberseguridad.

4.3.4 ISO 27001: 2022-ENS

Se ha realizado una equivalencia global de los controles del Anexo A de la ISO 27001:2022 y del Real Decreto 311/2022, de 3 de mayo, para poder evidenciar la sinergia de las dos normas, y alinear el perfil especifico de seguridad de organismos pagadores. [24]

[24] Este perfil no aspira a ser la guía de referencia del ENS con la ISO 27001. Ver Guía CCN STIC 825 ENS – Certificaciones 27001

Identificación	Nivel de equivalencia	Detalle
	Equivalente	En el análisis de requisitos del control analizado, se ha concluido que existe plena equivalencia. Ambas normas exigen idénticos requisitos o las medidas detalladas resultan asimilables. Las finalidades de seguridad para el control analizado son equivalentes en ambas normas.
	Parcialmente equivalente	En el análisis de requisitos del control analizado, se ha concluido que no existe plena equivalencia. Las normas no son igual de exigentes en los requisitos descritos. Parte de los requisitos del control analizado resulta equivalente pero no pueden considerarse cubiertos todos los extremos del control. Puede ser necesario complementar el control con otros controles diseminados por la norma, o bien es posible que la norma no haya considerado los requisitos del control no cubiertos. Si bien la finalidad puede ser similar, una de las normas es más exigente y su finalidad resulta más extensa.
	Nula	En el análisis de requisitos del control analizado, se ha concluido que no existe equivalencia. Alguna de las normas no considera el control analizado. Una de las normas ha desplegado un control con una finalidad que no es perseguida por la otra norma.

Ver anexo del presente perfil para conocer el detalle del análisis efectuado. Este anexo puede ayudar a los sujetos objeto a alinear sus sistemas de gestión actualmente desplegados con el Real Decreto 311/2022.

4.3.5 Conclusión análisis normas de seguridad

De todo lo anterior, podemos considerar:

a) Análisis del Real Decreto 311/2022 y la ISO 27001: 2013.

- El nivel de equivalencia de ambas normas es bajo, dado que el Real Decreto ha evolucionado en rigurosidad y seguridad, mientras que la norma se mantiene en un discreto plano de seguridad que no considera el perfil de las nuevas amenazas y riesgos de seguridad.

b) Análisis del Real Decreto 311/2022 y la ISO 27001: 2022.

- El nivel de equivalencia es bueno. Ambas normas han evolucionado en el plano de seguridad y consideración de nuevos riesgos, en un entorno cloud y de dependencia de proveedores. [25]
- La equivalencia se puede considerar mediante un perfil de cumplimiento que parta de una categoría MEDIA y considere la modulación concreta;
    i. Reducción de algún requisito establecido en medidas de categoría MEDIA ya que la norma ISO no considera con tanto rigor la medida (por ejemplo, configuración o componentes certificados).
    ii. Aplicar algún refuerzo no aplicable inicialmente en una categoría MEDIA.
    iii. Aplicar las medidas de continuidad que han de considerarse en un escenario de seguridad bajo la ISO.

[25] Se ha analizado con relación a la aplicación directa sobre un sujeto susceptible de certificar su sistema bajo el estándar ISO.

4.4 ANÁLISIS DE SISTEMAS Y ALCANCES DE LOS ORGANISMOS PAGADORES. SITUACIÓN DE PARTIDA: CERTIFICACIONES Y ALCANCES

4.4.1 Introducción.

A lo largo del proceso de elaboración de este perfil, se fueron analizando las diferencias de los organismos pagadores y específicamente, los sistemas de información desplegados y procesos de adecuación seguidos.

Hasta la fecha de recogida de la información, eran 10 organismos, incluido FEGA, los que habían desarrollado procesos de certificación basados en la ISO/IEC 27001:2013. Además, existen 6 organismos, incluido FEGA, que habían realizado procesos de conformidad con el ENS, 5 de los cuales lo hicieron en categoría MEDIA y uno en categoría BÁSICA. Además, existe una entidad que ha realizado una AUTOEVALUACIÓN.

También se ha analizado la categorización presentada, de manera que, salvo excepciones, todos los sistemas se orientan a una categoría MEDIA.

4.4.2 Análisis de Inventarios de información y servicios.

Para poder realizar una propuesta de inventario de servicios e información de los sujetos, se tomó en consideración el inventario de FEGA y de algunos organismos pagadores territoriales muestra.

Para realizar una propuesta debe considerarse que cada organismo tiene sus propias particularidades, pero debemos ceñirnos a lo requerido por el ENS sin desviar la atención de la normativa europea.

Por ello, se ha considerado que puede ser de utilidad presentar un modelo de inventario neutro, que agrupe los requerimientos del legislador nacional y europeo, y que analice bajo las premisas del anexo I del Real Decreto 311/2022, de 3 de mayo, la categoría requerida del sistema.

Cod.	Impacto [DP][26]	INFORMACION	Descripción	Cod.	Competencia Organismo Pagador - Obligado	SERVICIO	Descripción
Inf.01	**Si**	**Información técnica**	Información relacionada con la gestión de las ayudas Feaga y FEADER. Incluye registros y gestión del expediente, verificaciones, documentación y requerimientos al solicitante. Información relacionada con los registros auxiliares (animales, explotaciones...) Se incluye información relacionada con acciones de coordinación con el organismo coordinador.	**Ser.01**	**Si**	**Servicio Técnico**	Se incluyen las actividades relacionadas con las solicitudes presentadas y la verificación de los requisitos de estas, análisis y registro de las deudas y coordinación con el organismo de coordinación nacional. Incluye acciones para consultas de "Registros auxiliares" (registro de animales, explotación...) Incluyen acciones de soporte a la ciudadanía y terceros y todas las gestiones para mantener las aplicaciones y plataformas asociadas a las solicitudes.
Inf.02		**Información de pagos**	Se incluyen datos relacionados con las cuentas bancarias, procesos de abono, acreditaciones, aseguramientos, cálculos, seguimientos y controles básicos.	**Ser.02**	**Si**	**Servicio de Pagos**	Están incluidos los abonos ordinarios, anticipos e intereses, incluyendo el análisis de las condiciones y el seguimiento de estos, y de las liquidaciones.

[26] Afecta a Dato personal. Considere el impacto a la hora de realizar la valoración.

Cod.	Impacto [DP][25]	INFORMACION	Descripción	Cod.	Competencia Organismo Pagador - Obligado	SERVICIO	Descripción
Inf.03		**Información contable**	Toda la información asociada a la contabilidad obligada y operaciones de Feaga y FEADER. Partidas, gastos y justificaciones. Declaraciones y documentos validados.	**Ser.03**	**Si**	**Servicio de Contabilidad**	Incluye las acciones de contabilidad, con los registros contables y sus requisitos de exhaustividad y exactitud, gestión de productos almacenados y operaciones y las declaraciones periódicas requeridas (mensuales, trimestrales y anuales).
Inf.04		**Información de auditoria**	Información de control y evidencias relacionada con el seguimiento de los requisitos y controles exigibles.	**Ser.04**	**Si**	**Servicio de Auditoría Interna**	Actividades propias de los procesos de auditoria relativas a acreditaciones documentales del cumplimiento de los procedimientos asociados a autorización, contabilidad, pago, anticipo, garantía y deudas y evaluaciones individuales de verificación.
Inf.05	**Si**	**Información de control interno**	Información relacionada con el control interno del organismo, exámenes, informes, documentos examinados, propuestas…	**Ser.05**	**Si**	**Servicio de Seguimiento y Control Interno**	Actividades relacionadas con el examen de las solicitudes y peticiones presentadas y actividades de prevención del fraude e irregularidades en el proceso de ayudas.
Inf.06		**Información de almacén y productos**	Información de productos y de intervenciones en almacén, inventario y trazadas, controles, stock, albaranes y movimientos, contabilización, controles…	**Ser.06**		**Operaciones de almacenamiento público**	Actividades relativas a operaciones e intervenciones en almacenamientos, incluyendo inventarios, contratos, consolidaciones, actividades contables, canalización de la información y control y supervisión mediante actividades anuales (visitas e inspecciones).
Inf.07		**Información Recursos Humanos**	Información relacionada con el personal del organismo, perfiles, acreditaciones, recursos preventivos y de vigilancia. Planes de formación, evaluaciones, homologaciones. Perfil de personal de formación. Evaluación y eficacia. Información relacionada con las acciones de personas becadas y desarrollando formación profesional.	**Ser.07**		**Recursos humanos**	Gestión de personal y prevención de riesgos / vigilancia de la salud. Todas las actividades relacionadas con las becas de formación, formación en prácticas. Acciones de formación personal sector público no relacionada con seguridad de la información, normas de seguridad, privacidad y concienciación.
Inf.08		**Información actividades públicas**	Información relacionada con acciones propias de una entidad del sector público, incluyendo servicios de transparencia (información que debe hacerse pública, gestión del registro de entrada y salida, boletines, información de actividad) Información relacionada con el presupuesto anual y seguimiento del mismo. Información asociada a los procesos de contratación pública (contratos menores, Pliegos, actas...) Información y complementos presentados a organismos pagadores relacionados con denuncias o incumplimientos, sugerencias y mejoras. Información relacionada con reconocimientos, propuestas, premiados, comunicaciones, actividades de promoción y publicidad	**Ser.08**		**Servicios públicos**	Actividades relacionadas con administración electrónica (incluidas aquellas derivadas a portales de otras administraciones), servicios a la ciudadanía y terceros, acciones para dar cumplimiento a las imposiciones de trasparencia, actividades de archivo público, registro administrativo de entradas y salidas, actividades para generar información pública y suscripciones / boletines de las actividades públicas. Incluye acciones de presupuesto y gestión económica / Tesorería Incluye todas las actividades derivadas de los procesos de contratación pública. Denuncias, quejas y sugerencias Referencias promocionales, reconocimientos, premios y distinciones.
Inf.09	**Si**	**Información judicializada**	Información asociada a reclamaciones, información de juzgados, recursos, sentencias…	**Ser.09**		**Recursos y reclamaciones**	Expedientes y reclamaciones. Acciones de carácter judicial, juzgados y tribunales, recursos, responsabilidad patrimonial, …
Inf.10	**Si**	**Información de ayudas**	Información de otras ayudas y solicitudes de subvenciones, incluyendo formularios, documentos solicitados, acreditaciones, justificaciones, memorias…	**Ser.10**		**Ayudas y subvenciones**	Gestiones de ayudas y subvenciones diferenciadas, tales como ayudas generales para el desarrollo rural y litoral, ayudas a personas en riesgo de exclusión social y colectivos vulnerables, ayudas Fondo Europeo de Ayuda a los más desfavorecidos (FEAD)…
Inf.11		**Información del sistema de gestión**	Información relacionada con el sistema de gestión y su mejora (incluidas las valoraciones, declaraciones de aplicabilidad, informes de seguimiento, auditorias, procedimientos, instrucciones, análisis, informes, actas,	**Ser.11**	**Si**	**Sistema de gestión**	Sistema de gestión de seguridad de la información. Incluye acciones de valoraciones y alcances, actividades organizativas (roles, segregaciones, comités...), la gestión de riesgos y continuidad (análisis de riesgos y análisis de impacto), gestiones de la configuración

Cod.	Impacto [DP][26]	INFORMACION	Descripción	Cod.	Competencia Organismo Pagador - Obligado	SERVICIO	Descripción
			planes de acción, planes de formación, evaluaciones y rendimientos …) Incluye la información asociada al cumplimiento de la normativa de protección de datos (ejercicios de derechos, deberes de información, consentimientos, riesgos y evaluaciones de impacto, registros de actividades, informes y memorias...) Información relacionada con la seguridad física de las instalaciones (incluidas las grabaciones y mantenimientos de los elementos de seguridad que intervienen) Información de visitas, accesos y motivaciones (persona, fecha, motivo, e interlocutor)				(infraestructura y arquitectura, aplicaciones y plataformas), seguridad de los puestos, las actividades formativas de seguridad y protección de datos, concienciación y sensibilización. Se incluyen todas las actividades de seguridad de instalaciones, control de accesos y videovigilancia y registro de visitas a instalaciones. Actividades derivadas del cumplimiento y diligencia de la normativa de protección de datos.

4.5 PROPUESTA DE ALCANCE UNIFICADO BAJO UN PERFIL DE CUMPLIMIENTO

Para facilitar la homogeneización en la valoración de los servicios y la información y un modelo de sistema, se propone una categorización MEDIA conforme al Anexo I del Real Decreto 311/2022, de 3 de mayo, valorándose en base a lo dispuesto en el Anexo I de este y particularizando los criterios mediante lo dispuesto en guía CCN-STIC 803.

Asimismo, se proponen los siguientes alcances para los sistemas de información, de manera que un mismo alcance pueda servir para evidenciar un sistema de gestión de seguridad de la información bajo el perfil de seguridad especifico de organismo pagador desarrollado al amparo de lo dispuesto en el artículo 30 del Real Decreto 311/2022 [equivalente a la ISO 27001].

Propuesta A:

Los sistemas de información que dan soporte a los servicios prestados de **gestión de las ayudas y pagos de los fondos FEAGA y FEADER** bajo la competencia del organismo pagador, de acuerdo con la Declaración de Aplicabilidad del perfil de cumplimiento específico para organismos pagadores.

Propuesta B[27]:

Sistema de información necesario para la prestación de servicios necesarios para la **gestión de las ayudas y pagos bajo la competencia del organismo pagador de los fondos FEAGA y FEADER** (*solicitud, tramitación, gestión, propuesta de pago, autorización, control, ejecución del pago, gestión de anticipos y garantías, gestión de la deuda, tesorería y contabilidad*), conforme a (*los requisitos de seguridad establecidos en el Real Decreto 311/2022, de acuerdo con*) la Declaración de Aplicabilidad del perfil de cumplimiento específico para organismos pagadores.

[27] Esta propuesta se ajusta a la mayoría de los alcances presentados por los organismos pagadores analizados durante los trabajos. En ella se detallan los procesos asociados a los servicios competenciales.

4.6 CONFORMIDAD DE ENS PARA LA UE

Dada la previsión contenida en el Reglamento Delegado (UE) nº 2022/127, por la cual los Estados miembros podrán certificar, previa autorización de la Comisión, la seguridad de sus sistemas de información de conformidad con otras normas aceptadas si estas normas garantizan un nivel de seguridad equivalente, como mínimo, al previsto en la norma ISO 27001, debe considerarse la posibilidad de que la Comisión autorice a España para certificar los sistemas conforme a lo establecido en este perfil.

4.7 PERFIL DE CUMPLIMIENTO ESPECÍFICO PARA ORGANISMOS PAGADORES.

Se presenta un Perfil de Cumplimiento Específico adaptado a Organismos Pagadores. No obstante, dada la particularidad existente, y que los Organismos están sometidos a responsabilidades diferenciadas en base a la gestión y control de un gasto anual limitado en base a la cantidad de 400 millones EUR, el perfil se presenta en dos (2) niveles de cumplimiento de ENS, esto es:

a) Perfil de Cumplimiento Específico para organismos pagadores que gestionan ayudas por cuantía superior a 400 millones de euros.

b) Perfil de Cumplimiento Específico para organismos pagadores que gestionan ayudas por cuantía inferior a 400 millones de euros.

Esta diferencia de cuantía implica que los organismos pueden estar obligados a certificar sus sistemas de gestión conforme a la norma ISO 27001 cuando son responsables de la gestión y control de cuantías superiores a 400 millones EUR o, por el contrario, cuando el importe es inferior, se permite desplegar un sistema de gestión basado en el Código de Buenas prácticas para la Gestión de la Seguridad de la información basadas en la ISO 27002.

Y el CCN no puede ser ajeno a la diferenciación y nos obliga a aceptar el menor riesgo que percibe el legislador europeo y la rebaja de condiciones en el despliegue de una norma de seguridad. Por eso a la hora de diseñar este perfil especifico se ha considerado una diferencia en la aplicación de algunas medidas, siendo más estrictas o en su caso, rebajándose, en base a lo requerido por el Reglamento Delegado (UE) 2022/127 a un organismo. Si se exige la certificación en la ISO, el perfil de cumplimiento será riguroso y más estricto, mientras que, si se permite el despliegue de buenas prácticas de la ISO 27002, el perfil podrá presentar rebajas de requisitos de alguna medida.

A continuación, se muestra cómo se presenta el perfil de cumplimiento:

Dimensiones						
Afectadas	CAT B	CAT M	CAT A			
				Control	Aplicación PG [28]	Aplicación PP [29]
Categoría	aplica	aplica	aplica	medida.1	CATEGORIA	CATEGORIA
Categoría	aplica	aplica	aplica	medida.2	CATEGORIA	CATEGORIA

4.8 MEDIDAS COMPARTIDAS CON OTRAS ENTIDADES DEL SECTOR PÚBLICO

Ya se ha puesto de manifiesto la existencia de dos particularidades en relación con los organismos pagadores, por un lado, la posibilidad de realizar delegaciones en otras entidades y organismos, tal y como se reconoce por el legislador europeo[30], siempre con la prohibición expresa de delegación de la realización del pago.

Por otro lado, dentro del propia sinergia del sector público, puede ser habitual la existencia de entidades públicas con competencia en infraestructuras o servicios concretos, afectando a la gestión de medidas de seguridad y que coexistirán con la responsabilidad del organismo pagador en las mismas.

Algunos de los activos -CI, implicados en la seguridad decaen en la responsabilidad de Direcciones o de Organismos Públicos autonómicos, diferentes al propio Organismo Pagador. Por ejemplo, a nivel de red o comunicaciones no dependerá del Organismo Pagador la gestión de la red, o a nivel de infraestructura o Centro de Procesamiento de Datos, no es el Organismo el propietario y depende de la Dirección General / Consejería de la que depende orgánicamente.

Dada esta particularidad se ha añadido en el Anexo I, una distribución de responsabilidades en el cumplimiento del control que puede ser útil en los procesos de certificación o de distribución de cargas y modelados del cumplimiento de los controles presentes en el perfil de cumplimiento específico, es decir, mayor o menor rigurosidad en el cumplimiento de un control para el organismo pagador.

Es importante que los organismos pagadores añadan la correspondiente justificación en sus declaraciones de aplicabilidad, especifiquen las funciones delegadas y detallen claramente los controles que van a desarrollar para cerciorarse y verificar el cumplimiento. Entre estas medidas pueden encontrarse auditorías internas o externas.

[28] En la columna “Aplicación PG”, se reflejará la categoría (BÁSICA, MEDIA, ALTA) que se aplicará en caso de perfil general de Organismo Pagador responsable de la gestión y gastos por importe superior a 400 millones EUR.

[29] En la columna “Aplicación PP”, se reflejará la categoría (BÁSICA, MEDIA, ALTA) que se aplicará en caso de perfil particular de Organismo Pagador responsable de la gestión y gastos por importe inferior a 400 millones EUR.

[30] Reglamento (UE) 2021/2116, artículo 9

En el marco de la estrategia nacional de aumentar la seguridad en el sector público, se recomienda que se desplieguen las herramientas que ofrecemos desde el CCN[31].

Considerando la necesaria existencia de un organismo central de coordinación (por mandato del legislador europeo) y considerando la existencia de una Autoridad Nacional que vigila e impulsa el cumplimiento de la seguridad de los servicios e información:

a) Las herramientas y Guías del CCN pueden ser una gran alianza para unificar criterios de seguridad, imponiéndose sobre las diferencias de gestión autonómica y facilitando la comprensión a la Comisión en la aplicación de la seguridad, dotando de confianza mutua, creando sinergias entre sujetos similares, y todo ello en base a la existencia de 17 organismos pagadores a controlar en un estado.

b) Las premisas dadas por un organismo de coordinación nacional, pueden ser una gran alianza para unificar criterios de valoración, herramientas y servicios de seguridad y componentes adecuados para la gestión de las ayudas y fondos europeos.

5. DECLARACIÓN DE APLICABILIDAD DEL PERFIL DE CUMPLIMIENTO ESPECIFICO DE ORGANISMO PAGADOR

La declaración de aplicabilidad es el conjunto de medidas que son de aplicación para el cumplimiento del ENS. El conjunto de medidas dependerá de los niveles asociados a las dimensiones de seguridad.

Se ha determinado que, para garantizar la seguridad en los sistemas a los que hace referencia este Perfil de Cumplimiento Específico, la relación de medidas que son de aplicación y la exigencia en el nivel de seguridad de cada medida aplicada, es la que se indica en la siguiente tabla.

Dado que puede resultar diferente el grado de aplicación del control para cada tipo de perfil de organismo pagador, se presenta una separación en la tabla de medidas aplicables.

Mediante el símbolo “*”, se indica que la medida afectada dispone de criterios específicos de aplicación, los cuales se detallan en el apartado “6. CRITERIOS DE APLICACIÓN DE MEDIDAS”.

Por tanto, cuando una medida se vea afectada, se especificará con un asterisco “*” en la tabla siguiente, sobre la categoría. Se podrá referenciar un cambio de categoría o un refuerzo que debe ser aplicado (+R).

[31] Ver sección soluciones de seguridad en web https://www.ccn-cert.cni.es/soluciones-seguridad.html

Dimensiones Afectadas	CAT B	CAT M	CAT A	Control	Aplicación PG [32]	Aplicación PP [33]
Categoría	aplica	aplica	aplica	org.1	MEDIA	MEDIA
Categoría	aplica	aplica	aplica	org.2	MEDIA	MEDIA
Categoría	aplica	aplica	aplica	org.3	MEDIA	MEDIA
Categoría	aplica	aplica	aplica	org.4	MEDIA	MEDIA
Categoría	aplica	+ R1	+ R2	op.pl.1	ALTA *	BASICA *
Categoría	aplica	+ R1	+ R1 + R2 + R3	op.pl.2	MEDIA(+R2) *	MEDIA
Categoría	aplica	aplica	aplica	op.pl.3	MEDIA	MEDIA
D	aplica	+ R1	+ R1	op.pl.4	MEDIA	MEDIA *
Categoría	n.a.	aplica	aplica	op.pl.5	MEDIA	NA[34]
T A	aplica	+ R1	+ R1	op.acc.1	MEDIA	MEDIA (-)
C I T A	aplica	aplica	+ R1	op.acc.2	ALTA *	MEDIA
C I T A	n.a.	aplica	+ R1	op.acc.3	MEDIA*	MEDIA *
C I T A	aplica	aplica	aplica	op.acc.4	MEDIA	MEDIA
C I T A	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5	op.acc.5	MEDIA	MEDIA
C I T A	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 +R9	op.acc.6	MEDIA	MEDIA
Categoría	aplica	aplica	aplica	op.exp.1	MEDIA (+R4) *	MEDIA
Categoría	aplica	aplica	aplica	op.exp.2	MEDIA	MEDIA
Categoría	aplica	+ R1	+ R1 + R2 + R3	op.exp.3	ALTA *	MEDIA
Categoría	aplica	+ R1	+ R1 + R2	op.exp.4	ALTA *	BASICA *
Categoría	n.a.	aplica	+ R1	op.exp.5	ALTA *	MEDIA
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	op.exp.6	MEDIA	BASICA *
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3	op.exp.7	MEDIA	MEDIA
Categoría	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5	op.exp.8	MEDIA	BASICA(+R3) *
Categoría	aplica	aplica	aplica	op.exp.9	MEDIA	MEDIA
Categoría	aplica	+ R1	+ R1	op.exp.10	MEDIA	MEDIA

[32] En la columna “Aplicación PG”, se reflejará la categoría (BÁSICA, MEDIA, ALTA) que se aplicará en caso de perfil general de Organismo Pagador.
La categoría o los requisitos de la categoría MEDIA, pueden presentarse moduladas en virtud del principio de proporcionalidad y buscando una eficaz y eficiente aplicación del ENS. Cuando resulte diferenciado el grado de aplicación del control, se especificará mediante las siguientes referencias: (PG). Se especificará un asterisco, la particularidad de la aplicación de la categoría, y se podrá referenciar un refuerzo que debe ser aplicado (+R).

[33] En la columna “Aplicación PP”, se reflejará la categoría (BÁSICA, MEDIA, ALTA) que se aplicará en caso de perfil particular de Organismo Pagador.
La categoría o los requisitos de la categoría MEDIA pueden presentarse moduladas en virtud del principio de proporcionalidad y buscando una eficaz y eficiente aplicación del ENS. Cuando resulte diferenciado el grado de aplicación del control, se especificará mediante las siguientes referencias: (PP) Perfil particular. Se especificará un asterisco, la particularidad de la aplicación de la categoría, y se podrá referenciar un refuerzo que debe ser aplicado (+R).

[34] No aplica

Dimensiones						
Afectadas	CAT B	CAT M	CAT A	Control	Aplicación PG [32]	Aplicación PP [33]
Categoría	n.a.	aplica	aplica	op.ext.1	MEDIA	MEDIA
Categoría	n.a.	aplica	aplica	op.ext.2	MEDIA	MEDIA
Categoría	n.a.	n.a.	aplica	op.ext.3	ALTA *	N/A
Categoría	n.a.	aplica	+ R1	op.ext.4	MEDIA	MEDIA *
Categoría	aplica	+ R1	+ R1 + R2	op.nub.1	MEDIA	BASICA *
D	n.a.	aplica	aplica	op.cont.1	MEDIA	MEDIA
D	n.a.	n.a.	aplica	op.cont.2	ALTA *	N/A
D	n.a.	n.a.	aplica	op.cont.3	ALTA *	N/A
D	n.a.	n.a.	aplica	op.cont.4	ALTA *	N/A
Categoría	aplica	+ R1	+ R1 + R2	op.mon.1	MEDIA	MEDIA
Categoría	aplica	+ R1 + R2	+ R1 + R2	op.mon.2	MEDIA	MEDIA
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 +R6	op.mon.3	MEDIA	BÁSICA (+R1)*
Categoría	aplica	aplica	aplica	mp.if.1	MEDIA	MEDIA
Categoría	aplica	aplica	aplica	mp.if.2	MEDIA	MEDIA
Categoría	aplica	aplica	aplica	mp.if.3	MEDIA	MEDIA
D	aplica	+ R1	+ R1	mp.if.4	MEDIA	MEDIA *
D	aplica	aplica	aplica	mp.if.5	MEDIA	MEDIA
D	n.a.	aplica	aplica	mp.if.6	MEDIA	MEDIA
Categoría	aplica	aplica	aplica	mp.if.7	MEDIA	MEDIA
Categoría	n.a.	aplica	aplica	mp.per.1	MEDIA	MEDIA
Categoría	aplica	+ R1	+ R1	mp.per.2	MEDIA	BÁSICA*
Categoría	aplica	aplica	aplica	mp.per.3	MEDIA	MEDIA
Categoría	aplica	aplica	aplica	mp.per.4	MEDIA	MEDIA
Categoría	aplica	+ R1	+ R1	mp.eq.1	MEDIA	MEDIA
A	n.a.	aplica	+ R1	mp.eq.2	ALTA *	MEDIA
Categoría	aplica	aplica	+ R1 + R2	mp.eq.3	ALTA *	BASICA (+R2)*
C	aplica	+ R1	+ R1	mp.eq.4	MEDIA	BASICA *
Categoría	aplica	aplica	aplica	mp.com.1	MEDIA	MEDIA
C	aplica	+ R1	+ R1 + R2 + R3	mp.com.2	MEDIA	MEDIA
I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	mp.com.3	MEDIA	MEDIA
Categoría	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4	mp.com.4	MEDIA	MEDIA
C	aplica	aplica	aplica	mp.si.1	MEDIA	MEDIA
C I	n.a.	aplica	+ R1 + R2	mp.si.2	MEDIA (+R2) *	BASICA *
Categoría	aplica	aplica	aplica	mp.si.3	MEDIA	MEDIA
Categoría	aplica	aplica	aplica	mp.si.4	MEDIA	MEDIA
C	aplica	+ R1	+ R1	mp.si.5	MEDIA	MEDIA
Categoría	n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4	mp.sw.1	MEDIA	MEDIA
Categoría	aplica	+ R1	+ R1	mp.sw.2	MEDIA	MEDIA
Categoría	aplica	aplica	aplica	mp.info.1	MEDIA	MEDIA
C	n.a.	aplica	aplica	mp.info.2	MEDIA	MEDIA
I A	aplica	+ R1 + R2 + R3	+ R1 + R2 + R3 + R4	mp.info.3	MEDIA	MEDIA
T	n.a.	n.a.	aplica	mp.info.4	ALTA*	NA
C	aplica	aplica	aplica	mp.info.5	MEDIA	MEDIA
D	aplica	+ R1	+ R1 + R2	mp.info.6	MEDIA (+R2) *	BASICA *
Categoría	aplica	aplica	aplica	mp.s.1	MEDIA	MEDIA
Categoría	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3	mp.s.2	MEDIA	MEDIA

Dimensiones Afectadas	CAT B	CAT M	CAT A	Control	Aplicación PG [32]	Aplicación PP [33]
Categoría	aplica	aplica	+ R1	mp.s.3	MEDIA	MEDIA
D	n.a.	aplica	+ R1	mp.s.4	MEDIA	MEDIA*

5.1 MEDIDAS DE APLICACIÓN

De las 73 medidas de seguridad definidas en el Anexo II del RD 3/2010, serán de aplicación las relacionadas con categoría MEDIA, con ciertas apreciaciones y refuerzos, así como aquellas de categoría ALTA que se especifican en este perfil.

Marco Organizativo (4):

[org.1] Política de seguridad

[org.2] Normativa de seguridad

[org.3] Procedimientos de seguridad

[org.4] Proceso de autorización

Marco Operacional (32):

[op.pl] Planificación

[op.pl.1] Análisis de riesgos

[op.pl.2] Arquitectura de seguridad

[op.pl.3] Adquisición de nuevos componentes

[op.pl.4] Dimensionamiento /gestión de la capacidad

[op.pl.5] Componentes certificados

[op.acc.] Control de acceso

[op.acc.1] Identificación

[op.acc.2] Requisitos de acceso

[op.acc.3] Segregación de funciones y tareas

[op.acc.4] Proceso de gestión de derechos de acceso

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

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

[op.exp.] Explotación

[op.exp.1] Inventario de activos

[op.exp.2] Configuración de seguridad

[op.exp.3] Gestión de la configuración de seguridad

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

[op.exp.5] Gestión de cambios

[op.exp.6] Protección frente a código dañino

[op.exp.7] Gestión de incidentes

[op.exp.8] Registro de la actividad

[op.exp.9] Registro de la gestión de incidentes

[op.exp.10] Protección de claves criptográficas

[op.ext.] Servicios externos

[op.ext.1] Contratación y acuerdos de nivel de servicio

[op.ext.2] Gestión diaria

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

[op.ext.4] Interconexión de sistemas

[op.nub.] Servicios en la nube

[op.nub.1] Protección de servicios en la nube

[op.cont.] Continuidad de servicio

[op.cont.1] Análisis de impacto

[op.cont.2] Plan de continuidad

[op.cont.3] Pruebas periódicas

[op.cont.4] Medios alternativos

[op.mon.] Monitorización del sistema
[op.mon.1] Detección de intrusión
[op.mon.2] Sistema de métricas
[op.mon.3] Vigilancia

Medidas de Protección (36):

[mp.if.] Protección de las instalaciones e infraestructuras
[mp.if.1] Áreas separadas y con control de acceso
[mp.if.2] Identificación de las personas
[mp.if.3] Acondicionamiento de los locales
[mp.if.4] Energía eléctrica
[mp.if.5] Protección frente a incendios
[mp.if.6] Protección frente a inundaciones
[mp.if.7] Registro de entrada y salida de equipamiento
[mp.per.] Gestión del personal
[mp.per.1] Caracterización del puesto de trabajo
[mp.per.2] Deberes y obligaciones
[mp.per.3] Concienciación
[mp.per.4] Formación
[mp.eq.] Protección de los equipos
[mp.eq.1] Puesto de trabajo despejado
[mp.eq.2] Bloqueo de puesto de trabajo
[mp.eq.3] Protección de equipos portátiles
[mp.eq.4] Otros dispositivos conectados a la red
[mp.com] Protección de las comunicaciones
[mp.com.1] Perímetro seguro
[mp.com.2] Protección de la confidencialidad
[mp.com.3] Protección de la integridad y de la autenticidad
[mp.com.4] Separación de flujos de información en la red
[mp.si.] Protección de los soportes de información
[mp.si.1] Marcado de soportes
[mp.si.2] Criptografía
[mp.si.3] Custodia
[mp.si.4] Transporte
[mp.si.5] Borrado y destrucción
[mp.sw.] Protección de las aplicaciones informáticas
[mp.sw.1] Desarrollo de aplicaciones
[mp.sw.2] Aceptación y puesta en servicio
[mp.info.] Protección de la información
[mp.info.1] Datos personales
[mp.info.2] Calificación de la información
[mp.info.3] Firma electrónica
[mp.info.4] Sellos de tiempo
[mp.info.5] Limpieza de documentos
[mp.info.6] Copias de seguridad (backup)
[mp.s.] Protección de los servicios
[mp.s.1] Protección del correo electrónico
[mp.s.2] Protección de servicios y aplicaciones web
[mp.s.3]Protección de la navegación web
[mp.s.4] Protección frente a denegación de servicio

6. CRITERIOS DE APLICACIÓN DE MEDIDAS

6.1 [op.pl.1] Análisis de riesgos

[PG] Perfil General:

Serán de aplicación los requisitos de categoría MEDIA, junto con el "Refuerzo R2" Análisis de riesgos formal.

[PP] Perfil Particular:

Serán de aplicación los requisitos de categoría BÁSICA.

6.2 [OP.PL.2] Arquitectura de Seguridad

[PG] Perfil General:

Serán de aplicación los requisitos de categoría MEDIA, junto con el "Refuerzo R2-Sistema de gestión de la seguridad con mejora continua".

- [op.pl.2.r2.1] Sistema de gestión de la seguridad de la información, con actualización y aprobación periódica.

6.3 [OP.PL.4] Dimensionamiento/gestión de la capacidad

[PP] Perfil Particular:

Se aplicará la categoría MEDIA, sin aplicar el requisito [op.pl.4.r1.2] del "Refuerzo R1 –Mejora continua de la gestión de la capacidad":

- [op.pl.4.r1.2] Se emplearán herramientas y recursos para la monitorización de la capacidad.

6.4 [OP.PL.5] Componentes certificados

[PP] Perfil Particular:

No será de aplicación este control.

6.5 [OP.ACC.1] Identificación

[PP] Perfil Particular:

Serán de aplicación los requisitos de categoría MEDIA, no siendo aplicable el requisito [op.acc.1.r1.3] del "Refuerzo R1-Identificación avanzada":

- [op.acc.1.r1.3] Se asegurará la existencia de una lista actualizada de usuarios autorizados y mantenida por el administrador del sistema/de la seguridad del sistema.

6.6 [OP.ACC.2] Requisitos de acceso

[PG] Perfil General:

Será aplicable la medida en su categoría ALTA, "Refuerzo R1-Segregación rigurosa".

6.7 [OP.ACC.3] Segregación de funciones y tareas

[PG] Perfil General:

Será de aplicación los requisitos de categoría MEDIA pudiendo excluirse el requisito,

- [op.acc.3.1] Siempre que sea posible, las capacidades de desarrollo y operación no recaerán en la misma persona.

[PP] Perfil Particular:

Será de aplicación los requisitos de categoría MEDIA salvo:

- [op.acc.3.1] Siempre que sea posible, las capacidades de desarrollo y operación no recaerán en la misma persona.
- [op.acc.3.2] Siempre que sea posible, las personas que autorizan y controlan el uso serán distintas.

6.8 [OP.EXP.1] Inventario de activos

[PG] Perfil General:

Será de aplicación los requisitos de categoría MEDIA, junto con el "Refuerzo R4-Lista de componentes software."

- [op.exp.1.r4.1] Se mantendrá actualizada una relación formal de los componentes software de terceros empleados en el despliegue del sistema. Esta lista incluirá librerías software y los servicios requeridos para su despliegue (plataforma o entorno operacional). El contenido de la lista de componentes será equivalente a lo requerido en [mp.sw.1.r5].

Esta medida incluirá el requerimiento para portátiles y dispositivos, incorporando el "propietario del activo" o usuario asignado [mp.eq.3.1]

6.9 [OP.EXP.3] Gestión de la configuración de seguridad

[PG] Perfil General:

Será de aplicación los requisitos de categoría ALTA con los refuerzos;

"Refuerzo R2-Responsabilidad de la configuración."

- [op.exp.3.r2.1] La configuración de seguridad del sistema operativo y aplicaciones, tanto de estaciones y servidores como de la electrónica de red del sistema, será responsabilidad de un número muy limitado de administradores del sistema.

"Refuerzo R3-Copias de seguridad."

- [op.exp.3.r3.1] Se realizarán copias de seguridad de la configuración del sistema de forma que sea posible reconstruirlo en parte o en su totalidad tras un incidente.

6.10 [OP.EXP.4] Mantenimiento y actualizaciones de seguridad

[PG] Perfil General:

Será de aplicación los requisitos de categoría ALTA

Es necesario asociar el "Refuerzo R2 – Prevención de fallos" con el control [op.exp.5] y su gestión adecuada mediante un plan de marcha atrás.

- [op.exp.4.r2.1] Antes de la aplicación de las configuraciones, parches y actualizaciones de seguridad se preverá un mecanismo para revertirlos en caso de la aparición de efectos adversos.

[PP] Perfil Particular:

Será de aplicación los requisitos de categoría BASICA.

6.11 [OP.EXP.5] Gestión de cambios

[PG] Perfil General:

Será de aplicación los requisitos de categoría ALTA.

Es necesario asociar el "Refuerzo R1- Prevención de fallos" con el control [op.exp.4]

6.12 [OP.EXP.6] Protección frente a código dañino

[PP] Perfil Particular:

Será de aplicación los requisitos de categoría BASICA

6.13 [OP.EXP.8] Registro de la actividad

[PP] Perfil Particular:

Será de aplicación la categoría BASICA, requiriéndose el "Refuerzo 3 Retención de registros".

- [op.exp.8.r3.1] En la documentación de seguridad del sistema se deberán indicar los eventos de seguridad que serán auditados y el tiempo de retención de los registros antes de ser eliminados. Para los usuarios internos, será suficiente con el registro activo del dominio y de las aplicaciones autorizadas con una retención base de 6 meses.

6.14 [OP. EXT.3] Protección de la cadena de suministro

[PG] Perfil General:

Será de aplicación la categoría ALTA.

Este control se relacionará con los controles del bloque de controles [op.cont.]

6.15 [OP. EXT.4] Interconexión de sistemas [35]

[PG] Perfil General:

Será de aplicación la categoría MEDIA, salvo el requerimiento establecido en

- [op.ext.4.1] Todos los intercambios de información y prestación de servicios con otros sistemas deberán ser objeto de una autorización previa. Todo flujo de información estará prohibido salvo autorización expresa.

Para aquellas interconexiones con otras entidades públicas, serán consideradas autorizadas por defecto y como regla general, salvo prohibición expresa del Responsable de Seguridad.

[PP] Perfil Particular:

Será de aplicación la categoría MEDIA, con las salvedades establecidas en los requerimientos:

- [op.ext.4.1] Todos los intercambios de información y prestación de servicios con otros sistemas deberán ser objeto de una autorización previa. Todo flujo de información estará prohibido salvo autorización expresa.

Para aquellas interconexiones con otras entidades públicas, serán consideradas autorizadas por defecto y como regla general, salvo prohibición expresa del Responsable de Seguridad.

- [op.ext.4.2] Para cada interconexión se documentará explícitamente: las características de la interfaz, los requisitos de seguridad y protección de datos y la naturaleza de la información intercambiada.

Se considerará exclusivamente el diagrama general de red de la entidad superior jerárquica y/o entidad pública implicada en los procesos de redes e interconexiones.

6.16 [OP.NUB.1] Protección de los servicios en la nube

[PP] Perfil Particular:

Será de aplicación la categoría BASICA.

6.17 [OP.CONT.2] Plan de continuidad

[PG] Perfil General:

Será de aplicación la categoría ALTA.

---

[35] A todos los efectos se considerará lo establecido en el ENS relacionado con el uso de los servicios y de las infraestructuras comunes de las Administraciones Públicas.
Artículo 29 Infraestructuras y servicios comunes
La utilización de infraestructuras y servicios comunes de las administraciones públicas, incluidos los compartidos o transversales, facilitará el cumplimiento de lo dispuesto en este real decreto. Los supuestos concretos de utilización de estas infraestructuras y servicios serán determinados por cada administración pública.

6.18 [OP.CONT.3] Pruebas periódicas

[PG] Perfil General:

Será de aplicación la categoría ALTA.

6.19 [OP.CONT.4] Medios alternativos

[PG] Perfil General:

Será de aplicación la categoría ALTA.

6.20 [OP.MON.3] Vigilancia.

[PP] Perfil Particular:

Será de aplicación la categoría BASICA., y el "Refuerzo R1-Correlación de eventos."

- [op.mon.3.r1.1] Se dispondrá de un sistema automático de recolección de eventos de seguridad que permita la correlación de estos.

6.21 [MP.IF.4] Energía Eléctrica

[PP] Perfil Particular:

Será de aplicación la categoría MEDIA, sin aplicarse el Refuerzo R1-Suministro eléctrico de emergencia.

- [mp.if.4.r1.1] En caso de fallo del suministro principal, el abastecimiento eléctrico deberá estar garantizado durante el tiempo suficiente para una terminación ordenada de los procesos y la salvaguarda de la información.

6.22 [MP.PER.2] Deberes y obligaciones

[PP] Perfil Particular:

Será de aplicación la categoría BASICA.

6.23 [MP.EQ.2] Bloqueo de puesto de trabajo

[PG] Perfil General:

Será de aplicación la categoría ALTA, con la aplicación del Refuerzo R1-Cierre de sesiones.

- [mp.eq.2.r1.1] Pasado un cierto tiempo, superior al anterior, se cancelarán las sesiones abiertas desde dicho puesto de trabajo.

El organismo deberá vigilar las particularizaciones, que podrían desplegarse en una Guía CCN-STIC, de la configuración de seguridad adaptada al Organismo y a este perfil.

6.24 [MP.EQ.3] Protección de dispositivos portátiles

[PG] Perfil General:

Será de aplicación la categoría ALTA

Debe considerarse, el cifrado del disco duro del equipo portátil, como indica el "Refuerzo R1 – Cifrado del disco", si del inventario de información se contempla que la misma tiene un nivel MEDIO.

[PP] Perfil Particular:

Aplicara la categoría Básica con el "Refuerzo R2– Entornos protegidos."

- [mp.eq.3.r2.1] El uso de dispositivos portátiles fuera de las instalaciones de la organización se restringirá a entornos protegidos, donde el acceso sea controlado y a salvo de hurtos y miradas indiscretas.

6.25 [MP.EQ.4] Otros dispositivos conectados a la red

[PG] Perfil Particular:

Será de aplicación la categoría BASICA.

6.26 [MP.SI.2] Criptografía

[PG] Perfil General:

Será de aplicación la categoría MEDIA, junto con el Refuerzo R2-Copias de seguridad.

- [mp.si.2.r2.1] Las copias se seguridad se cifrarán utilizando algoritmos y parámetros autorizados por el CCN.

[PP] Perfil Particular:

Será de aplicación la categoría BASICA.

6.27 [MP.INFO.4] Sellos de tiempo

[PG] Perfil General:

Será de aplicación la categoría ALTA.

6.28 [MP.INFO.6] Copias de Seguridad

[PG] Perfil General:

Será de aplicación la categoría MEDIA, junto con los requisitos del "Refuerzo R2-Protección de las copias de seguridad."

- [mp.info.6.r2.1] Al menos, una de las copias de seguridad se almacenará de forma separada en lugar diferente, de tal manera que un incidente no pueda afectar tanto al repositorio original como a la copia simultáneamente.

Esto estará asociado a los resultados de la valoración derivada de [mp.info.2] y los riesgos [op.pl.1] e impacto [op.cont.1].

Este control tendrá referencia con el "Refuerzo R3-Copias de seguridad."

- [op.exp.3.r3.1] Se realizarán copias de seguridad de la configuración del sistema de forma que sea posible reconstruirlo en parte o en su totalidad tras un incidente.

Se considera Refuerzo R2-Protección de las copias de seguridad, para elementos críticos que requieran su almacenamiento en lugar diferente

[PP] Perfil Particular:

Se aplicará la categoría BASICA.

6.29 [MP.S.4] Protección frente a denegación de servicio

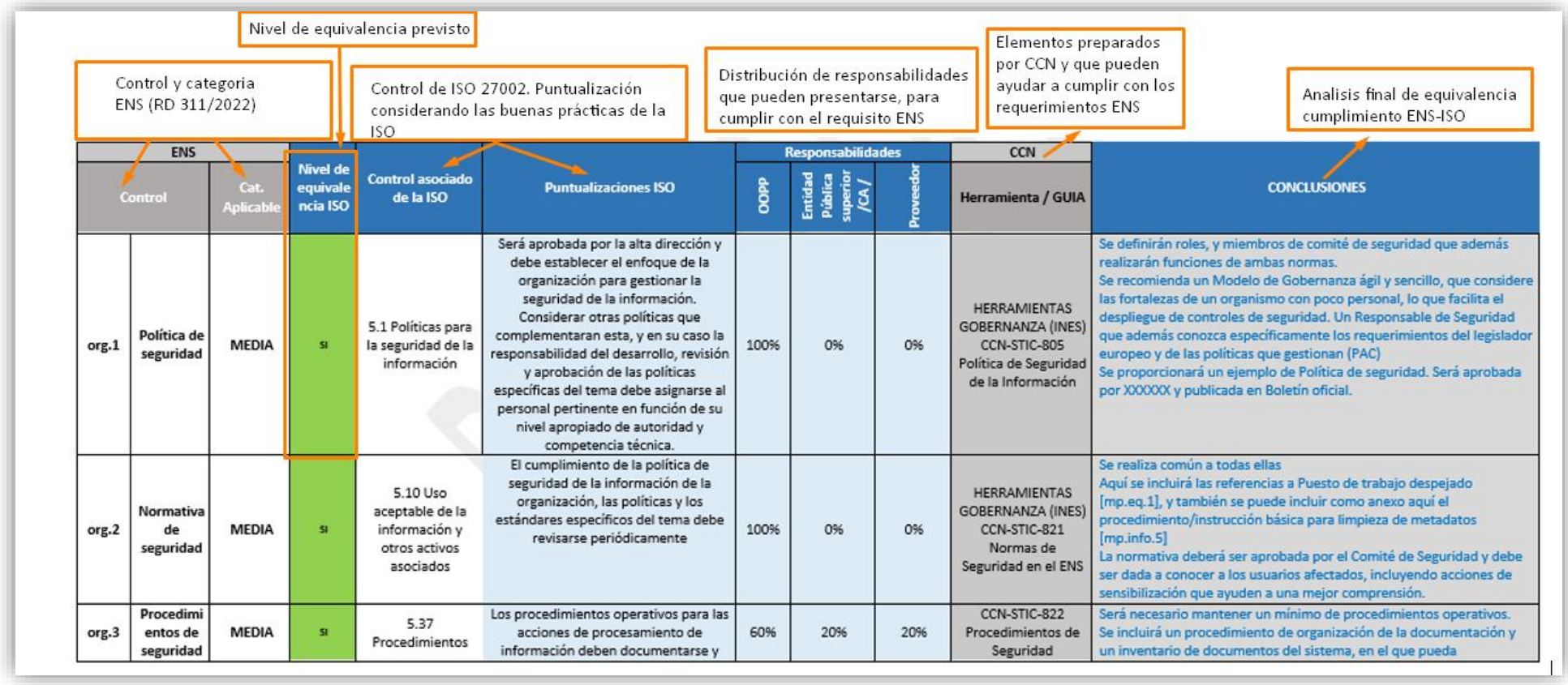
[PP] Perfil Particular:

Será aplicable la categoría MEDIA con la puntualización respecto al requisito [mp.s 4.1], siendo este asociado al control [OP.PL.4], y resultando suficiente el cumplimiento con este.

7. Anexo I – Equivalencia y cumplimiento de controles

Para que un Organismo Pagador pueda someterse a un único proceso de acreditación, que le permita obtener una certificación conforme al ENS y la ISO 27001, su Sistema de Gestión de Seguridad de la Información debe considerar los requisitos de ambas normas.

Como interpretar el contenido de la tabla presentada:



ENS			Nivel de equivalencia ISO	Control asociado de la ISO	Puntualizaciones ISO	Responsabilidades			CCN	CONCLUSIONES
Control		Cat. Aplicable				OOPP	Entidad Pública superior /CA /	Proveedor	Herramienta / GUIA	
org.1	Política de seguridad	MEDIA	SI	5.1 Políticas para la seguridad de la información	Será aprobada por la alta dirección y debe establecer el enfoque de la organización para gestionar la seguridad de la información. Considerar otras políticas que complementaran esta, y en su caso la responsabilidad del desarrollo, revisión y aprobación de las políticas específicas del tema debe asignarse al personal pertinente en función de su nivel apropiado de autoridad y competencia técnica.	100%	0%	0%	HERRAMIENTAS GOBERNANZA (INES) CCN-STIC-805 Política de Seguridad de la Información	Se definirán roles, y miembros de comité de seguridad que además realizarán funciones de ambas normas. Se recomienda un Modelo de Gobernanza ágil y sencillo, que considere las fortalezas de un organismo con poco personal, lo que facilita el despliegue de controles de seguridad. Un Responsable de Seguridad que además conozca específicamente los requerimientos del legislador europeo y de las políticas que gestionan (PAC) Se proporcionará un ejemplo de Política de seguridad. Será aprobada por XXXXXX y publicada en Boletín oficial.
org.2	Normativa de seguridad	MEDIA	SI	5.10 Uso aceptable de la información y otros activos asociados	El cumplimiento de la política de seguridad de la información de la organización, las políticas y los estándares específicos del tema debe revisarse periódicamente	100%	0%	0%	HERRAMIENTAS GOBERNANZA (INES) CCN-STIC-821 Normas de Seguridad en el ENS	Se realiza común a todas ellas Aquí se incluirá las referencias a Puesto de trabajo despejado [mp.eq.1], y también se puede incluir como anexo aquí el procedimiento/instrucción básica para limpieza de metadatos [mp.info.5] La normativa deberá ser aprobada por el Comité de Seguridad y debe ser dada a conocer a los usuarios afectados, incluyendo acciones de sensibilización que ayuden a una mejor comprensión.
org.3	Procedimientos de seguridad	MEDIA	SI	5.37 Procedimientos	Los procedimientos operativos para las acciones de procesamiento de información deben documentarse y	60%	20%	20%	CCN-STIC-822 Procedimientos de Seguridad	Será necesario mantener un mínimo de procedimientos operativos. Se incluirá un procedimiento de organización de la documentación y un inventario de documentos del sistema, en el que pueda

Por ello, un Organismo deberá considerar lo siguiente:

ENS				Nivel de equivalencia ISO	Control asociado de la ISO	Puntualizaciones ISO	Responsabilidades				CCN	CONCLUSIONES
Control		Cat. Aplicable PG	Cat. Aplicable PP				OOPP	OODD	Entidad Pública superior /CA / OOCC	Proveedor	Herramienta / GUIA	
org.1	Política de seguridad	MEDIA	MEDIA	SI	5.1 Políticas para la seguridad de la información	Será aprobada por la alta dirección y debe establecer el enfoque de la organización para gestionar la seguridad de la información. Considerar otras políticas que complementaran ésta, y en su caso la responsabilidad del desarrollo, revisión y aprobación de las políticas específicas por parte del al personal pertinente en función de su nivel de autoridad y competencia técnica.	100%		0%	0%	HERRAMIENTAS GOBERNANZA (INES) CCN-STIC-805 Política de Seguridad de la Información	Se definirán roles, y miembros de comité de seguridad que además realizarán funciones para ambas normas. Se recomienda un Modelo de Gobernanza ágil y sencillo, que considere las fortalezas del organismo, su estructura funcional y clara separación, lo que facilita el despliegue de controles de seguridad. Un Responsable de Seguridad que además conozca específicamente los requerimientos del legislador europeo y de las políticas que gestionan (PAC). Se elaborará una Política de seguridad común, que será aprobada por el Comité y se publicará en el Boletín oficial.
org.2	Normativa de seguridad	MEDIA	MEDIA	SI	5.10 Uso aceptable de la información y otros activos asociados	El cumplimiento de la política de seguridad de la información de la organización, las políticas y los estándares específicos del debe revisarse periódicamente.	30%	10%	50%	10%	HERRAMIENTAS GOBERNANZA (INES) CCN-STIC-821 Normas de Seguridad en el ENS	Se realiza común a los mandatos de ambas normas Aquí se incluirá las referencias a Puesto de trabajo despejado [mp.eq.1], pudiendo incluirse como anexo el procedimiento/instrucción básica para limpieza de metadatos [mp.info.5]. La normativa deberá ser aprobada por el Comité de Seguridad y debe ser dada a conocer a los usuarios afectados, incluyendo acciones de sensibilización [mp.per.4] que ayuden a una mejor comprensión.
org.3	Procedimientos de seguridad	MEDIA	MEDIA	SI	5.37 Procedimientos operativos documentados	Los procedimientos operativos para las acciones de tratamiento de la información deben documentarse y ponerse a disposición del personal que los necesite.	40%	10%	20%	30%	CCN-STIC-822 Procedimientos de Seguridad AMPARO	Será necesario mantener un mínimo de procedimientos operativos. Se incluirá un procedimiento de organización de la documentación [7.5 Documented information] y un inventario de documentos del sistema, en el que pueda comprobarse su fecha de creación, fecha de revisión y la sensibilidad de la información contenida.
org.4	Proceso de autorización	MEDIA	MEDIA	PARCIAL	5.2 Funciones y responsabilidades de seguridad de la información	Si bien la ISO no es tan específica, permite desplegar un proceso particularizado de autorización. Por ello se debe priorizar el mandato de ENS sobre la ISO.	90%		10%	0%	HERRAMIENTAS GOBERNANZA (INES) CCN-STIC-801 Esquema Nacional de Seguridad. Responsabilidades y funciones	Si bien la ISO no es tan específica, permite desplegar un proceso particularizado de autorización. Deben considerarse las pretensiones del I Anexo I- Articulo 1 del Reglamento Delegado (UE) 2022/127; Letra B): *"iv) la apropiada formación del personal en todos los niveles operativos, incluso en materia de sensibilización ante el fraude, y se disponga de una política que permita rotar al personal que ocupe puestos sensibles o aumentar la supervisión,"* y *"v) la adopción de medidas apropiadas para evitar y detectar que se produzca un conflicto de intereses, en el sentido del artículo 61 del Reglamento (UE, Euratom) 2018/1046, en lo relacionado con la ejecución de funciones del organismo pagador en relación con personas con influencia y que ocupen un puesto de responsabilidad dentro y fuera del organismo pagador. En caso de riesgo de conflicto de intereses, se tomarán medidas para garantizar la aplicación de dicho artículo."*
op.pl.1	Análisis de riesgos	ALTO *	BASICA *	SI	6.1 – Acciones para abordar riesgos y oportunidades	Se debe documentar el criterio seguido para la aceptación del riesgo, identificar propietarios de los mismos, priorizando los	100%		0%	0%	HERRAMIENTAS GOBERNANZA (INES) Pilar µPILAR	Ambas normas convergen y puede emplearse la misma metodología de riesgos para desplegar este control. Se recomienda emplear PILAR como herramienta y desplegar una declaración de aplicabilidad compartida de ambas normas.

ENS				Nivel de equivalencia ISO	Control asociado de la ISO	Puntualizaciones ISO	Responsabilidades				CCN	CONCLUSIONES
Control		Cat. Aplicable PG	Cat. Aplicable PP				OOPP	OODD	Entidad Pública superior /CA / OOCC	Proveedor	Herramienta / GUIA	
						tratamientos y asumiendo los riesgos residuales.					CCN-STIC 470-473 CCN-STIC 410 Análisis de riesgos en sistemas de la Administración	El Comité de Seguridad aprobará los riesgos y el plan de tratamiento y recibirá información de la gestión de estos. El Responsable de Seguridad debe aprobar la declaración de aplicabilidad.
op.pl.2	**Arquitectura de Seguridad**	**MEDIA (+R2*)**	**MEDIA**	**SI**	Clausula 4.4 Sistema de gestión de la seguridad de la información 8.27 Arquitectura de sistemas seguros y principios de ingeniería	La organización debe establecer, implementar, mantener y mejorar de manera continua un Sistema De Gestión De La Seguridad De La Información, de acuerdo con los requisitos de la norma internacional. Los principios para diseñar sistemas seguros deben establecerse, documentarse, mantenerse y aplicarse a cualquier actividad de desarrollo de sistemas de información.	40%	10%	20%	30%	HERRAMIENTAS GOBERNANZA (INES)	Ambos sistemas se apoyan en un sistema de Seguridad de la Información. No obstante, para Perfil particular, se considerará suficiente un sistema con un ciclo de mejora (PDCA) e información básica del sistema. Parte de la información será documentada por un tercero que proveerá el servicio (por ejemplo, servicios de red) y en su caso, el titular del servicio (Organismos de la Comunidad Autónoma de la que dependerá el OOPP).
op.pl.3	**Adquisición de nuevos componentes**	**MEDIA**	**MEDIA**	**PARCIAL**	5.8 Seguridad de la información en la gestión de proyectos	Los procesos de adquisición se integrarán en proyectos completos y globales, que contemplarán muchos elementos y entre ellos debería incluirse, la adquisición de componentes, riesgos, arquitectura y necesidades. La seguridad de la información debe integrarse en las actividades de gestión de proyectos de la organización.	80%		10%	10%	HERRAMIENTAS GOBERNANZA (INES) Catalogo CCN-STIC 105 Guías CCN STIC 140	Es importante considerar el proceso global, y de manera transversal. Así se documentará y se incluirán requisitos de seguridad en los procesos de contratación Debe considerarse la normativa específica de contratación pública.
op.pl.4	**Dimensionamiento/gestión de la capacidad**	**MEDIA**	**MEDIA (*)**	**SI**	8.6 Gestión de capacidad	Planificación, monitorización y ajuste. Debe considerarse una dual estrategia; aumentando la capacidad y/o reduciendo la demanda.	50%	10%	20%	20%	HERRAMIENTAS GOBERNANZA (INES) LORETO CCn-STIC-820 Protección contra Denegación de Servicio	Ambas normas pueden converger perfectamente. Es recomendable la automatización, que puede ser mediante un proveedor que nos ayude a gestionar las mediciones, alertas y planificaciones. Los servicios en la nube pueden ser ayuda, dada la escalabilidad de los mismos. Considérese el control [op.nub.1]
op.pl.5	**Componentes certificados**	**MEDIA**	**(NA) (*)**	**No**	No se contempla expresamente	No existe este control en la ISO. No obstante, puede asociarse a los activos, al mapeo de los mismos y los riesgos que pueden derivarse. Contar con productos y servicios acreditados, puede mejorar la seguridad del OOPP.	40%	10%	20%	30%	HERRAMIENTAS GOBERNANZA (INES) PILAR	Este control puede excluirse en el Perfil Particular [PP], por no ser contemplado en la ISO y no tener un gran impacto en los servicios de los OOPP. Para los Perfil General [PG], se debe trabajar un inventario de los componentes afectados o integrar esta característica en el inventario de activos, incluyendo el análisis de inclusión en el catálogo CCN STIC 105 o certificación equivalente (por ejemplo, Common Criteria). Se debe considerar en previsiones futuras de adquisición de nuevos componentes Considérese [op.pl.3]. Debe considerarse para productos y para servicios de seguridad.

ENS				Nivel de equivalencia ISO	Control asociado de la ISO	Puntualizaciones ISO	Responsabilidades				CCN	CONCLUSIONES
Control		Cat. Aplicable PG	Cat. Aplicable PP				OOPP	OODD	Entidad Pública superior /CA / OOCC	Proveedor	Herramienta / GUIA	
op.acc. 1	Identificación	MEDIA	MEDIA *	SI	5.16 Gestión de identidades	Se debe administrar el ciclo de vida completo de las identidades	80%	10%	0%	10%	HERRAMIENTAS GOBERNANZA (INES)	Ambos controles permiten la gestión de las identidades de manera completa. Es recomendable que la entidad mantenga un inventario de servicios (incluyendo aquellos que son proporcionados por servicios en la nube). En este registro se puede controlar la metodología de identificación. Pueden trazarse mediante el directorio activo los registros o trazas y mantener los registros y retenciones asociadas con los registros de actividad.
op.acc. 2	Requisitos de acceso	ALTA*	MEDIA	SI	5.15 Control de acceso	Las reglas para controlar el acceso físico y lógico a la información y otros activos asociados deben establecerse e implementarse en función de los requisitos de negocio y de seguridad de la información Hay varias formas de implementar el control de acceso pudiendo desplegar elementos dinámicos.	80%	10%	0%	10%	HERRAMIENTAS GOBERNANZA (INES) EMMA CARLA	Los requisitos de los servicios y las consideraciones de riesgo deben ser la base para definir los derechos de acceso, las herramientas y la granularidad. Las reglas de control de acceso se pueden implementar en diferentes granularidades, que van desde cubrir redes o sistemas completos hasta campos de datos específicos, y también pueden considerar propiedades como la ubicación del usuario o el tipo de conexión de red que se utiliza para el acceso (afectará significativamente a costes y recursos).
op.acc. 3	Segregación de funciones y tareas	MEDIA*	MEDIA*	SI	5.3 Segregación de funciones	Deben segregarse los deberes y las áreas de responsabilidad en conflicto	50%	10%	20%	20%	HERRAMIENTAS GOBERNANZA (INES) EMMA CARLA	Siempre que sea difícil segregar, se deben considerar otros controles, como el seguimiento de las actividades, las pistas de auditoría y la supervisión de la gestión. Para mantener el control debería disponerse de un inventario de operaciones, que permita diferenciar las segregaciones y sobre quien recaen. Por ejemplo, en temas de cambio; derechos de acceso, código y desarrollo, sistema en producción, aplicaciones, BBDD accesos remotos, ... Deben considerarse las previsiones del l Anexo I- Articulo 1.1 del Reglamento Delegado (UE) 2022/127.
op.acc. 4	Proceso de gestión de derechos de acceso	MEDIA	MEDIA	SI	5.18 Derechos de acceso 8.2 Derechos de acceso privilegiado	Concesión y revocación de los derechos de acceso Revisión y cambio o terminación del empleo. La asignación y el uso de derechos de acceso privilegiado deben restringirse y administrarse.	40%	10%	20%	30%	HERRAMIENTAS GOBERNANZA (INES) EMMA CARLA	Ambas normas convergen, si bien en el caso de la ISO deben considerarse previsiones contenidas en varios controles. Es importante considerar que este control afecta a todo usuario, por lo que deben gestionarse los usuarios de terceros.
op.acc. 5	Mecanismo de autenticación (usuarios externos)	MEDIA	MEDIA	PARCIAL	5.18 Derechos de acceso 8.5 Autenticación segura	Garantizar que los derechos de acceso se activen (por ejemplo, por parte de los proveedores de servicios) solo después de que los procedimientos de autorización se completen con éxito	60%	10%	10%	20%	HERRAMIENTAS GOBERNANZA (INES)	Es un control que afecta de manera directa a las entidades que sean titulares de sedes y servicios publicados que permitan a los usuarios externos los accesos. En este caso la ISO no particulariza tanto el control, si bien estima los requisitos impuestos por el ENS. Considerar las responsabilidades del proveedor (desarrollador y mantenedor de servicios) y el titular de los mismos que pueden ser empleados por el OOPP
op.acc. 6	Mecanismo de autenticación (usuarios	MEDIA	MEDIA	SI	8.5 Autenticación segura	Las tecnologías y los procedimientos de autenticación segura se implementarán en función de las restricciones de acceso a la información y la política específica sobre el control de acceso.	70%		10%	20%	HERRAMIENTAS GOBERNANZA (INES)	El control de la ISO permite adaptar a los requisitos del ENS las autenticaciones, modulándose. Los refuerzos contenidos en la categoría Alta pueden mejorar la seguridad del acceso y son contemplados por la ISO 27002: (...)

ENS				Nivel de equivalencia ISO	Control asociado de la ISO	Puntualizaciones ISO	Responsabilidades				CCN	CONCLUSIONES
Control		Cat. Aplicable PG	Cat. Aplicable PP				OOPP	OODD	Entidad Pública superior /CA / OOCC	Proveedor	Herramienta / GUIA	
	de la organización)											k) finalizar sesiones inactivas después de un período definido de inactividad, l) restringir los tiempos de duración de la conexión para proporcionar seguridad adicional para aplicaciones de alto riesgo y reducir la ventana de oportunidad para el acceso no autorizado. Existirán muchos servicios en remoto o mediante nube por lo que pueden derivarse como procedimientos, autenticaciones por contraseña y un segundo factor.
op.exp.1	Inventario de activos	MEDIA (+R4)	MEDIA	SI	5.9 Inventario de información y otros activos asociados	Se debe desarrollar y mantener un inventario de información y otros activos asociados, incluidos los propietarios.	50%	10%	20%	20%	PILAR EMMA GOBERNANZA (INES)	Es importante gestionar los inventarios de activos, que pueden ser mediante herramientas sencillas o con más complejidad dependiendo del volumen de activos y del presupuesto del OOPP. Debe considerarse el propietario del activo, y específicamente [mp.eq.3.1] inventario de equipos portátiles junto con una identificación de la persona responsable del mismo y un control regular de que está positivamente bajo su control. Los inventarios deben garantizar su actualización, por lo que deben realizarse revisiones periódicas; y aplicar automáticamente una actualización tras el proceso de instalación, cambio o eliminación de un activo. La ubicación de un activo debe incluirse en el inventario según corresponda. Hay que tener en cuenta que este inventario ayudará en el caso de ambas normas, a la gestión de riesgos, las actividades de auditoría, la gestión de vulnerabilidades y la planificación la contingencia y de las acciones de recuperación. Considerar el control [op.pl.5]
op.exp.2	Configuración de seguridad	MEDIA	MEDIA	PARCIAL	8.9 Gestión de la configuración	Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, monitorizarse y revisarse.	50%	10%	10%	30%	CLARA ROCIO EMMA ESE ANA Guías especificas CCN-STIC HERRAMIENTAS GOBERNANZA (INES)	La configuración contará con las diferentes herramientas desplegadas en el CCN, y especialmente CLARA. En la documentación de sistema se considerarán las guías de bastionado y la documentación de aquellas herramientas que ayudan a gestionar posibles desviaciones o vulnerabilidades. Deberá desplegarse los requerimientos del ENS para poder mantener una configuración adecuada . Se considerarán las guías específicamente publicadas. Por razón de la superficie de exposición, aquellos activos que estén solo en el ámbito interno y que no presente riesgos significativos, podrán ser configurados con una plantilla genérica de seguridad.
op.exp.3	Gestión de la configuración de seguridad	ALTA*	MEDIA	PARCIAL	8.9 Gestión de la configuración	Plantillas estándar para la configuración de seguridad de hardware, software, servicios y redes Las plantillas deben revisarse periódicamente y actualizarse La organización debe definir e implementar	50%	10%	10%	30%	CLARA ROCIO EMMA ESE ANA Guías especificas CCN-STIC	La organización debe definir e implementar procesos y herramientas para hacer cumplir la configuración. En los procesos se considerarán las copias de las configuraciones lo que nos permitirá alinear ambas normas. Los servicios en la nube serán bastionados conforme a las guías del CCN STIC aplicables. En la documentación de sistema se considerarán las guías de bastionado

ENS				Nivel de equivalencia ISO	Control asociado de la ISO	Puntualizaciones ISO	Responsabilidades				CCN	CONCLUSIONES
Control		Cat. Aplicable PG	Cat. Aplicable PP				OOPP	OODD	Entidad Pública superior /CA / OOCC	Proveedor	Herramienta / GUIA	
						procesos y herramientas para hacer cumplir la configuración					HERRAMIENTAS GOBERNANZA (INES)	y la documentación de aquellas herramientas que ayudan a gestionar posibles desviaciones o vulnerabilidades.
op.exp .4	**Mantenimiento y actualizaciones de seguridad**	**ALTA***	**BASICA ***	**PARCIAL**	7.13 Mantenimiento de equipos 8.8 Vulnerabilidades técnicas	Proceso y registro de mantenimientos Proceso de identificar vulnerabilidades técnicas, evaluar, desplegar y controlar. Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a tales vulnerabilidades y se deben tomar las medidas apropiadas.	50%	10%	10%	30%	ANA CLARA ROCIO PILAR HERRAMIENTAS GOBERNANZA (INES)	En el caso del ENS es más estricto en sus requisitos, pero pueden lograrse las equivalencias mediante los controles identificados y desplegando en el sistema: 1.- Procedimiento interno para la identificación de vulnerabilidades en sus productos y servicios, considerando el inventario de activos como requisito previo, el proveedor del software, las funciones y responsabilidades asociadas con la gestión de vulnerabilidades, la monitorización, la evaluación de riesgos - vulnerabilidades, la actualización, seguimiento y la notificación, el acceso y la divulgación de vulnerabilidades incluyendo los requisitos en los contratos aplicables de proveedores, soportes y licencias. Un proceso eficaz de gestión de vulnerabilidades técnicas debe estar alineado con gestión de incidentes, para comunicar datos sobre vulnerabilidades a respuesta a incidentes y proporcionar procedimientos técnicos que se llevarán a cabo en caso de que ocurra un incidente. 2.- Se pueden utilizar herramientas de escaneo de vulnerabilidades, pruebas de penetración o evaluaciones de vulnerabilidad por parte de personas competentes y autorizadas. 3.- La organización debería recibir informes de vulnerabilidad de fuentes internas o externas; analizarlos y verificarlos; desarrollar soluciones (actualizaciones o parches); realizar pruebas y desplegar la producción. 4.- En el caso de los servicios en la nube, se deriva parte o incluso toda la responsabilidad al proveedor, para la gestión de vulnerabilidades técnicas de sus servicios y se incluirán procesos para informar de las acciones a los clientes OOPP. 5.- No puede aislarse en ninguna de las dos normas, la gestión de cambios y, puede aprovecharse el propio ciclo degestión de cambios.6.- Si no es posible realizar pruebas adecuadas de las actualizaciones, por ejemplo, debido al coste o falta de recursos, se puede considerar retrasar el despliegue para evaluar los riesgos asociados. 7.- Las pruebas de penetración también son un método para identificar vulnerabilidades. 8.- Cuando se produzcan parches o actualizaciones de software, la organización puede considerar proporcionar un proceso de actualización automatizado en el que estas actualizaciones se instalen en los sistemas o productos afectados sin necesidad de intervención por parte del usuario final.
op.exp .5	**Gestión de cambios**	**ALTA***	**MEDIA**	**SI**	8.32 Gestión del cambio	Los cambios en la organización, procesos, instalaciones y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios.	50%	10%	10%	30%	HERRAMIENTAS GOBERNANZA (INES)	Con carácter general ambas normas nos exigen un proceso documentado que incluirá una planificación y evaluación del impacto potencial de los cambios, comunicaciones a las partes interesadas, pruebas (en entornos

ENS				Nivel de equivalencia ISO	Control asociado de la ISO	Puntualizaciones ISO	Responsabilidades				CCN	CONCLUSIONES
Control		Cat. Aplicable PG	Cat. Aplicable PP				OOPP	OODD	Entidad Pública superior /CA / OOCC	Proveedor	Herramienta / GUIA	
												controlados) y aceptación de pruebas funcionales y de seguridad y la autorización de cambios. Es innegable que existirán situaciones que requieran cambios de emergencia y contingencia, que serán la excepción al proceso pero que exigirán una revisión completa de seguridad posterior.
op.exp .6	**Protección frente a código dañino**	**MEDIA**	**BASICA ***	**SI**	8.7 Protección contra malware	Se debe implementar la protección contra el malware, incluyendo acciones de concienciación del usuario.	10%		0%	90%	µCLAUDIA MARTA MARIA ADA HERRAMIENTAS GOBERNANZA (INES)	Ambas normas convergen perfectamente si bien es necesario que el control sea liderado por los requisitos del ENS. Debemos considerar el impacto de este control en el control [op.exp.4] Mantenimiento y controles de continuidad [op.cont.]. Considerar el control [mp.per. 3]
op.exp .7	**Gestión de incidentes**	**MEDIA**	**MEDIA**	**PARCIAL**	5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información 5.25 Evaluación y decisión sobre eventos de seguridad de la información	En el caso de la ISO son varios los controles que debemos considerar para poder cubrir los requisitos del ENS. 5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información 5.25 Evaluación y decisión sobre eventos de seguridad de la información 5.26 Respuesta a incidentes de seguridad de la información 5.27 Aprendiendo de los incidentes de seguridad de la información	40%	10%	10%	40%	LUCIA CCN-STIC-817 Esquema Nacional de Seguridad. Gestión de Ciberincidentes HERRAMIENTAS GOBERNANZA (INES)	Dado que existen dependencias jerárquicas y/o públicas es necesario considerar la estructura de las administraciones públicas y la gestión de central a través de la plataforma LUCIA. Deberemos considerar diferentes puntos del control para desplegar un proceso que estará alineado con la Guía CCN-STIC 817 y con la Guía de Ciberincidentes Nacional. Debe considerarse el modelo de medidas a desplegar y muy especialmente los recursos que pueden precisarse. Es conveniente que el proceso sea liderado por ENS para poder dar cumplimiento a ambas normas.
op.exp .8	**Registro de la actividad**	**MEDIA**	**BASICA (+R3)**	**PARCIAL**	8.15 Registro 8.17 Sincronización de reloj	Se deben activar, proteger, almacenar y analizar registros de actividades, excepciones, fallos y otros eventos relevantes.	30%	10%	0%	60%	MONICA GLORIA REYES (CARMEN Y LUCIA) CCN-STIC-831 Registro de la actividad de los usuarios	La norma ENS es más estricta en cuanto requisitos que la ISO, pero esta, permite desplegar el proceso con los puntos de seguridad que precisamos. Con respecto a los eventos (*), deberían considerarse para los Perfil General: : a) Eventos de autenticación de usuarios y administradores. (incluidas las alertas del sistema de control de acceso y los accesos con éxito y fallidos) b) Eventos de acciones realizadas sobre ficheros y objetos. c) Eventos de exportación (upload) e importación (download). d) Eventos de acciones sobre cuentas de usuarios.(incluidas creación, modificación o supresión de derechos o de identidades) e) Eventos de acciones realizadas por usuarios privilegiados. f) Todos aquellos eventos adicionales reflejados en las diferentes políticas de seguridad (incluidas cambios en la configuración del sistema; uso de programas de utilidad y otras aplicaciones; activación y desactivación de sistemas de protección, como sistemas antivirus y sistemas de detección de intrusos)

ENS				Nivel de equivalencia ISO	Control asociado de la ISO	Puntualizaciones ISO	Responsabilidades				CCN	CONCLUSIONES
Control		Cat. Aplicable PG	Cat. Aplicable PP				OOPP	OODD	Entidad Pública superior /CA / OOCC	Proveedor	Herramienta / GUIA	
												Si bien para categoría MEDIA no es necesario automatizar el proceso de revisión, es recomendable contar con una herramienta de gestión de eventos e información de seguridad (SIEM) o un servicio equivalente para almacenar, correlacionar, normalizar y analizar la información de registro y generar alertas. Los SIEM tienden a requerir una configuración cuidadosa para optimizar sus beneficios. Las configuraciones para considerar incluyen la identificación y selección de fuentes de registro apropiadas, ajuste y prueba de reglas y desarrollo de casos de uso. Los servicios en la nube deberían mantener su propio servicio de registro de actividades y gestión de alertas. Los servicios dependientes de otra administración serán responsabilidad de ésta. No obstante, es conveniente que se tracen en el inventario de registros de actividades o logs. Es recomendable que si el OOPP está analizando soluciones en el mercado que cubran los requerimientos del ENS, tenga en cuenta que estas se encuentren en CCN-STIC-105 Catálogo de Productos y Servicios de Seguridad de las TIC 7.2.6 FAMILIA: SISTEMAS DE GESTIÓN DE EVENTOS DE SEGURIDAD
op.exp .9	**Registro de la gestión de incidentes**	**MEDIA**	**MEDIA**	**PARCIAL**	5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información 5.28 Recolección de evidencia	Existirá un registro de actividades de gestión de incidentes; así como pautas relacionadas con el manejo de la evidencia digital (ver 5.28) y el análisis de causa raíz o procedimientos post mort	40%		10%	50%	LUCIA CCN-STIC-817 Esquema Nacional de Seguridad. Gestión de Ciberincidentes HERRAMIENTAS GOBERNANZA (INES)	A nivel general la ISO es flexible a la hora de desplegar los requisitos de ENS. Para facilitar el registro de la información precisa, se recomienda el uso de formularios de incidentes para ayudar al personal a recabar toda la información necesaria. Se debe tener en cuenta que a efectos del ENS existirán procesos de retroalimentación con otras entidades y en base a esta información se podrá reportar los eventos de seguridad de la información necesarios A nivel de requerimientos legales en determinadas situaciones el OOPP deberá elaborar informes de incidentes, dentro de plazos definidos
op.exp .10	**Protección de claves criptográficas**	**MEDIA**	**MEDIA**	**PARCIAL**	8.24 Uso de criptografía	Deben definirse e implementarse reglas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas. El nivel de protección requerido deriva de la propia clasificación de la información tanto para el tipo, fortaleza y calidad del algoritmo criptográfico requerido. La organización determinará los estándares que se adoptarán, así como los algoritmos criptográficos, la fuerza del cifrado y las prácticas de uso, para una implementación efectiva en toda la organización (qué solución se utiliza y para qué procesos)	40%	10%	10%	40%	CCN-STIC-807 Criptología de empleo en el ENS HERRAMIENTAS GOBERNANZA (INES)	La propia ISO deriva a los requerimientos legales. Para implementar las reglas de la organización para el uso eficaz de la criptografía, se deben tener en cuenta la legislación y las restricciones que podrían aplicarse al uso de técnicas criptográficas y a los problemas de las transmisiones de información cifrada. Por ello se hace preciso que el ENS lidere junto con los requerimientos contenidos en la Guía CCN STIC 807 Y CCN STIC 221, los algoritmos empleados. Deben inventariarse y mantenerse un análisis de los algoritmos empleados. Los servicios gestionados por terceros y especialmente aquellos en la nube deben considerar los requisitos de este control y el OOPP debe comprobar que se cumplen. A los efectos de los gestores de claves, debe considerarse CCN-STIC-105

ENS				Nivel de equivalencia ISO	Control asociado de la ISO	Puntualizaciones ISO	Responsabilidades				CCN	CONCLUSIONES
Control		Cat. Aplicable PG	Cat. Aplicable PP				OOPP	OODD	Entidad Pública superior /CA / OOCC	Proveedor	Herramienta / GUIA	
												Catálogo de Productos y Servicios de Seguridad de las TIC, 7.2.7 FAMILIA: DISPOSITIVOS PARA GESTIÓN DE CLAVES CRIPTOGRÁFICAS
op.ext. 1	**Contratación y acuerdos de nivel de servicio**	**MEDIA**	**MEDIA**	**SI**	5.19 Seguridad de la información en las relaciones con los proveedores 5.20 Abordar la seguridad de la información en los acuerdos con los proveedores	Deben identificarse e implementarse procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor. Los requisitos de seguridad de la información pertinentes deben establecerse y acordarse con cada proveedor en función del tipo de relación.	70%	10%	10%	10%	HERRAMIENTAS GOBERNANZA (INES) CCN-STIC-823 Utilización de servicios en la nube Guía CCN-STIC 821 ENS. Apéndice VI. NP 50 Acuerdo de confidencialidad para terceros feb-18 ENS. Apéndice VII. NP 60 Modelo de contenido de buenas prácticas para terceros	A nivel de ENS se requiere no solo la gestión de los requisitos de seguridad sino la gestión de los niveles de servicio y la disponibilidad, que puede afectar de manera muy directa a la continuidad y al servicio. Es recomendable disponer de un registro que trace todos los contratos afectados y permita un control de los proveedores, sus requisitos de seguridad y los accesos a la información y al sistema. Pueden existir servicios derivados de una entidad jerárquica superior y/o entidad pública. En tal caso el OOPP debe considerar sus necesidades y documentarlo para evidenciar la correcta gestión.
op.ext. 2	**Gestión diaria**	**MEDIA**	**MEDIA**	**PARCIAL**	5.22 Seguimiento, revisión y gestión del cambio de los servicios de los proveedores	Debe realizarse un proceso para gestionar la relación entre la organización y el proveedor para: monitorizar y realizar un seguimiento de los niveles de desempeño de los servicios y verificar el cumplimiento de los acuerdos. Se deben definir las responsabilidades para ello.	70%	10%	10%	10%	HERRAMIENTAS GOBERNANZA (INES) CCN-STIC-844 Manual de usuario de INES CCN-STIC-823 Utilización de servicios en la nube CCN-STIC-815 Indicadores y métricas en el ENS Guía CCN-STIC 821 ENS. Apéndice VI. NP 50 Acuerdo de confidencialidad para terceros feb-18 ENS. Apéndice VII. NP 60 Modelo de contenido de buenas prácticas para terceros	Se deben revisar, validar y actualizar periódicamente sus acuerdos con las partes externas para asegurarse de que siguen siendo necesarios y aptos para su propósito, y que se incluyen las cláusulas de seguridad de la información pertinentes. Para mantener un cumplimiento claro del ENS deberían requerirse en los procesos de contratación (pliegos y contratos menores) informes periódicos que presenten indicadores y mediciones / tendencias y que sirvan para valorar el servicio, los acuerdos requeridos y las necesidades del servicio dado. Estos informes deben contener métricas generales y aquellas otras que permitan presentar reportes a través de la solución INES
op.ext. 3	**Protección de la**	**ALTA (*)**	**NA**	**SI**	5.21 Gestión de la	Los procesos y procedimientos deben definirse e implementarse para abordar los	70%	10%	10%	10%	HERRAMIENTAS GOBERNANZA	Dada la criticidad de los servicios de terceros y especialmente dependencias que pueden generarse es conveniente considerarlo, al

ENS				Nivel de equivalencia ISO	Control asociado de la ISO	Puntualizaciones ISO	Responsabilidades				CCN	CONCLUSIONES
Control		Cat. Aplicable PG	Cat. Aplicable PP				OOPP	OODD	Entidad Pública superior /CA / OOCC	Proveedor	Herramienta / GUIA	
	cadena de suministro				seguridad de la información en la cadena de suministro de TIC	riesgos de seguridad de la información asociados con los servicios de TIC y la cadena de suministro de productos.					(INES) PILAR INES AMPARO CCN-STIC-823 Utilización de servicios en la nube Guía CCN-STIC 821 ENS. Apéndice VI. NP 50 Acuerdo de confidencialidad para terceros feb-18 ENS. Apéndice VII. NP 60 Modelo de contenido de buenas prácticas para terceros	menos en el Perfil General [PG]. En el análisis de riesgos de la entidad, deberían considerarse los servicios y las subcontrataciones. Se deben considerar los requerimientos legales implicados. Se debería exigir que los proveedores [y organismos delegados o entidades públicas presentes en el sistema], propaguen los requisitos de seguridad a lo largo de la cadena de suministro si subcontratan y que los productos TIC mantengan requisitos de seguridad [op.pl.5] y prácticas de seguridad adecuadas a lo largo de la cadena de suministro. Se debería solicitar a los proveedores información de los componentes de software utilizados en los productos.
op.ext.4	**Interconexión de sistemas**	**MEDIA**	**MEDIA ***	**No**	8.23 Segregación en redes	Las redes a menudo se extienden más allá de los límites de la organización, ya que se forman asociaciones que requieren la interconexión o el intercambio de redes y de información, que pueden aumentar el riesgo.	50%		10%	40%	HERRAMIENTAS GOBERNANZA (INES) CCN-STIC-811 Interconexión en el ENS	Este control es de requerimiento directo por el ENS y no por la ISO. Es derivable a otros controles para acreditar su cumplimiento. Se debe mantener un diagrama actualizado y la autorización previa, y el análisis de los requisitos de seguridad y protección de datos y la naturaleza de la información intercambiada.
op.nub.1	**Protección de servicios en la nube**	**MEDIA**	**BASICA**	**PARCIAL**	5.23 Seguridad de la información para el uso de servicios en la nube	Los procesos y procedimientos deben definirse e implementarse para abordar los riesgos de seguridad de la información asociados con los servicios de TIC y la cadena de suministro de productos.	60%	10%	0%	30%	HERRAMIENTAS GOBERNANZA (INES) CCN-STIC-823 Utilización de servicios en la nube	Los requisitos de la ISO están muy alineados con el ENS. Se debe recabar del proveedor información que describa los componentes de software. Los servicios en la nube deben considerar los requerimientos derivados de las Guías del CCN correspondientes. Deben considerarse los pliegos y contratos menores para el cumplimiento de este control.
op.cont.1	**Análisis de impacto**	**MEDIA**	**MEDIA**	**SI**	5.29 Seguridad de la información durante la interrupción 5.30 Preparación de las TIC para la continuidad del negocio	Como parte del análisis de impacto se deben considerar y priorizar las consecuencias de la pérdida de confidencialidad e integridad de la información, además de la necesidad de mantener la disponibilidad.	70%	10%	10%	10%	HERRAMIENTAS GOBERNANZA (INES) CCN-STIC 470 Manual de usuario PILAR. Análisis del impacto y continuidad del negocio PILAR	Se deben considerar los servicios y las criticidades, permitiendo detectar RTO y RPO. Se deben considerar y priorizar las consecuencias de la pérdida de confidencialidad e integridad de la información, además de la necesidad de mantener la disponibilidad. Los altos impactos y baja probabilidad (salida del análisis de riesgos [op.pl.1]) Deben ayudar a la preparación de las situaciones de contingencia.
op.cont.2	**Plan de continuidad**	**ALTA ***	**NA**	**SI**	5.29 Seguridad de la información durante la interrupción 5.30 Preparación de	La organización debe planificar cómo mantener la seguridad de la información en un nivel adecuado durante la interrupción.	70%	10%	10%	10%	CCN-STIC 470 Manual de usuario PILAR. Análisis del impacto y	Deben conocerse que controles de seguridad de la información, sistemas y herramientas de apoyo, han de estar preparadas ante un evento catastrófico. Se deben considerar los controles de seguridad que no operaran durante

ENS				Nivel de equivalencia ISO	Control asociado de la ISO	Puntualizaciones ISO	Responsabilidades				CCN	CONCLUSIONES
Control		Cat. Aplicable PG	Cat. Aplicable PP				OOPP	OODD	Entidad Pública superior /CA / OOCC	Proveedor	Herramienta / GUIA	
					las TIC para la continuidad del negocio						continuidad del negocio PILAR HERRAMIENTAS GOBERNANZA (INES)	una caída y controles de compensación para los controles de seguridad de la información que no se pueden mantener durante la interrupción.
op.cont.3	**Pruebas periódicas**	**ALTA ***	**NA**	**SI**	5.30 Preparación de las TIC para la continuidad del negocio	La preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.	70%	10%	10%	10%	CCN-STIC 470 Manual de usuario PILAR. Análisis del impacto y continuidad del negocio PILAR HERRAMIENTAS GOBERNANZA (INES)	La necesidad de preparación de las TIC para la continuidad del negocio puede resultar de las evaluaciones de riesgos. La evaluación debe incluir todos los tipos de escenarios, incluidos aquellos con alto impacto y baja probabilidad, a menudo llamados escenarios extremos pero plausibles. Es importante considerar las pruebas de continuidad asociadas a los servicios del OOPP, trazar los tiempos y analizar desviaciones. Pueden considerarse pruebas desde diferentes perspectivas, tanto simulacros como pruebas de papel.
op.cont.4	**Medios alternativos**	**ALTA ***	**NA**	**PARCIAL**	8.14 Redundancia de instalaciones de procesamiento de información	Las instalaciones de procesamiento de información deben implementarse con suficiente redundancia para cumplir con los requisitos de disponibilidad.	70%	10%	10%	10%	CCN-STIC 470 Manual de usuario PILAR. Análisis del impacto y continuidad del negocio PILAR HERRAMIENTAS GOBERNANZA (INES)	Se acotará el alcance del ENS a los requerimientos del propio control de la ISO por cuanto, se acotará a las instalaciones. La organización debe diseñar e implementar una arquitectura de sistemas con la redundancia adecuada para cumplir con estos requisitos. Los servicios en la nube permiten el cumplimiento de este control.
op.mon.1	**Detección de intrusión**	**MEDIA**	**MEDIA**	**PARCIAL**	8.21 Seguridad de los servicios de red	Los servicios de red incluyen la provisión de conexiones, servicios de red privada y soluciones de seguridad de red administrada, como firewalls y sistemas de detección de intrusos. Estos servicios pueden variar desde ancho de banda simple no administrado hasta medidas complejas.	20%		10%	70%	HERRAMIENTAS GOBERNANZA (INES) CCN-STIC-811 Interconexión en el ENS CCN-STIC-816 Seguridad en Redes Inalámbricas en el ENS	Los servicios de red están en su mayor parte cubiertos por el responsable de la infraestructura quien dotara de estas herramientas a la red. Los OOPP deberán presentar evidencias de la existencia de esta responsabilidad en la infraestructura. Los servicios en la nube incluyen este punto requerido.
op.mon.2	**Sistema de métricas**	**MEDIA**	**MEDIA**	**PARCIAL**	9 – Evaluación del desempeño 9.1 – Monitorización, medidas, análisis y evaluación.	La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información. Las métricas pueden servir para ambos sistemas, pero a efectos de la ISO , deben incluirse el seguimiento de los objetivos de seguridad	80%		10%	10%	HERRAMIENTAS GOBERNANZA (INES) CCN-STIC-815 Indicadores y métricas en el ENS CCN-STIC-844 Manual de usuario	Se debe imponer el criterio de ENS para recopilar las métricas requeridas para el informe de seguridad INES. Además, es conveniente tener en cuenta las mediciones de niveles de madurez y niveles de implantación conforme a la Guía CCN-STIC 808. La entidad podría desplegar en el sistema un catálogo de métricas generales asociadas a una Declaración de Aplicabilidad y ampliar mediciones a controles y objetivos de seguridad de la ISO.

ENS				Nivel de equivalencia ISO	Control asociado de la ISO	Puntualizaciones ISO	Responsabilidades				CCN	CONCLUSIONES
Control		Cat. Aplicable PG	Cat. Aplicable PP				OOPP	OODD	Entidad Pública superior /CA / OOCC	Proveedor	Herramienta / GUIA	
											de INES CCN-STIC-808 Verificación del cumplimiento de las medidas en el ENS	Para lograr la equivalencia deben considerarse los objetivos de seguridad y métricas apropiadas.
op.mon.3	**Vigilancia**	**MEDIA**	**BASICA (+R1)***	**SI**	5.7 Inteligencia de amenazas 8.16 Actividades de monitorización	Se recopilará información relacionada con las amenazas a la seguridad y se analizaran para generar información	20%		10%	70%	HERRAMIENTAS GOBERNANZA (INES) ANA GLORIA ESE CARMEN Guías especificas CCN-STIC	Se dispondrá de soluciones de vigilancia que permitan determinar la superficie de exposición con relación a vulnerabilidades y deficiencias de configuración. Para ello pueden desplegar funciones mediante soluciones del CCN o en su caso, análisis de CVE mediante fuentes y listas oficiales. Por ejemplo, los avisos de vulnerabilidades se pueden registrar y analizar en el sistema, y se pueden analizar los impactos y los riesgos derivados. Muchos de los servicios dependen de la entidad jerárquica superior y/o entidad pública, por lo que es complicado gestionar este control directamente. En otras ocasiones la información la proporcionan proveedores o asesores independientes, autoridades de control o grupos de expertos de inteligencia de amenazas. Para la ISO hablamos de inteligencia de amenazas y requiere conexión con los controles 5.25 Eventos de seguridad , 8.7 Protección frente a malware , 8.16 Monitorización o 8.22 Filtrado web, para mantener la calidad de la información sobre amenazas.
mp.if.1	**Áreas separadas y con control de acceso**	**MEDIA**	**MEDIA**	**SI**	7.1 Perímetro de seguridad física	Existirán perímetros de seguridad, en las zonas con protección según la información y/o activos que contienen.	10%	0%	10%	80%	HERRAMIENTAS GOBERNANZA (INES)	Es más que factible que el CPD sea titularidad de una entidad jerárquica superior y/o otra entidad pública, por lo que estos controles para el CPD no son responsabilidad del OOPP. En todo caso, los servicios contratados a un proveedor implicarán estas medidas, que serán exigidas en el proceso de contratación. Puede considerarse un protocolo de gestión del llaves como procedimiento para administrar estos elementos físicos o las cerraduras de combinación de las oficinas, habitaciones e instalaciones, implicadas.
mp.if.2	**Identificación de las personas**	**MEDIA**	**MEDIA**	**SI**	7.2 Controles físicos de entrada	Separaciones de áreas de entrega y carga y descarga. Control de visitas, incluyendo el personal de proveedores, la inspección de entregas y albaranes. Monitorización de procesos técnicos de controles de acceso.	30%	0%	0%	70%	HERRAMIENTAS GOBERNANZA (INES)	Es más que factible que el CPD sea titularidad de una entidad jerárquica superior y/o entidad pública, por lo que estos controles no son responsabilidad del OOPP. En todo caso, los servicios contratados a un proveedor implicarán estas medidas, que serán exigidas en el proceso de contratación.
mp.if.3	**Acondicionamiento de los locales**	**MEDIA**	**MEDIA**	**PARCIAL**	7.8 Ubicación y protección de equipos	No hay una equivalencia exacta al control Queda absorbido por otros controles 7.3 Aseguramiento de oficinas, salas e instalaciones 7.8 Ubicación y protección de equipos 7.12 Seguridad del cableado	10%	0%	10%	80%	HERRAMIENTAS GOBERNANZA (INES)	Debe considerarse la dependencia de entidades jerárquicas superiores y/u otra entidad pública y de los proveedores clave para cumplir este control. El cumplimiento de este control mediante la ISO, recae en varios controles. Así el control 7.8 Ubicación y protección de equipos, refiere la necesidad de desplegar controles para minimizar el riesgo de posibles amenazas físicas y ambientales; por ejemplo, robo, fuego, explosivos, humo, agua,

ENS				Nivel de equivalencia ISO	Control asociado de la ISO	Puntualizaciones ISO	Responsabilidades				CCN	CONCLUSIONES
Control		Cat. Aplicable PG	Cat. Aplicable PP				OOPP	OODD	Entidad Pública superior /CA / OOCC	Proveedor	Herramienta / GUIA	
												o fallos en el suministro de agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo; o riesgos derivados de las condiciones ambientales, como la temperatura y la humedad, que deben monitorizarse para detectar condiciones que puedan afectar negativamente el funcionamiento de las instalaciones de procesamiento de información.
mp.if.4	**Energía eléctrica**	**MEDIA**	**MEDIA ***	**SI**	7.11 Utilidades de apoyo	Las instalaciones de procesamiento de información deben estar protegidas contra cortes de energía y otras interrupciones causadas por fallos en los servicios de soporte	10%	0%	10%	80%	HERRAMIENTAS GOBERNANZA (INES)	Debe considerarse la dependencia de entidades jerárquicas superiores y/o otra entidad pública y de los proveedores clave para cumplir este control. Con la información disponible deberemos desplegar el análisis de riesgos y contemplar los impactos.
mp.if.5	**Protección frente a incendios**	**MEDIA**	**MEDIA**	**SI**	7.5 Protección contra amenazas físicas y ambientales	Se debe diseñar e implementar la protección contra amenazas físicas y ambientales, como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura.	10%	0%	10%	80%	HERRAMIENTAS GOBERNANZA (INES)	Debe considerarse la dependencia de entidades jerárquicas superiores y/o otra entidad pública y de los proveedores clave para cumplir este control. Con la información disponible deberemos desplegar el análisis de riesgos y contemplar los impactos.
mp.if.6	**Protección frente a inundaciones**	**MEDIA**	**MEDIA**	**SI**	7.5 Protección contra amenazas físicas y ambientales	Se debe diseñar e implementar la protección contra amenazas físicas y ambientales, como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura.	10%	0%	10%	80%	HERRAMIENTAS GOBERNANZA (INES)	Fuera de las propias dependencias de las instalaciones el OOPP puede considerar disponer de planos que identifiquen bajantes y otros elementos similares. El OOPP puede conocer el impacto en la posición de la oficina mediante el análisis de las zonas geográficas que se han inundado anteriormente por estadísticas oficiales existentes. https://www.miteco.gob.es/es/agua/temas/gestion-de-los-riesgos-de-inundacion/snczi/
mp.if.7	**Registro de entrada y salida de equipamiento**	**MEDIA**	**MEDIA**	**SI**	7.2 Controles físicos de entrada	Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso apropiados.	10%	0%	10%	80%	HERRAMIENTAS GOBERNANZA (INES)	Además del propio registro se deben considerar, otras medidas complementarias, como el acceso controlado a las áreas de carga y descarga y el diseño de estas áreas de modo que el equipamiento y mercancías, puedan cargarse y descargarse, sin que el personal de entrega obtenga acceso no autorizado a otras partes del edificio; Se debe exigir a los titulares de los CPD la presencia de personal del OOPP o en su caso que las entregas entrantes se revisen contra el albarán, se analice si hay evidencia de manipulación del paquete y en su caso inspeccionarse en busca de materiales peligrosos. Las entradas deben estar trazadas con la gestión de activos [op.exp.1] y 5.9 y 7.10 de la ISO.
mp.per.1	**Caracterización del puesto de trabajo**	**MEDIA**	**MEDIA**	**SI**	6.1 Cribado	Los controles de verificación de antecedentes de todos los candidatos para convertirse en personal deben llevarse a cabo antes de unirse a la organización y de manera continua de acuerdo con las leyes, regulaciones y código ético, y ser proporcionales a los objetivos de la organización, la clasificación de la	10%		90%	0%	HERRAMIENTAS GOBERNANZA (INES)	Todas las previsiones descritas están alineadas con el Anexo I- Articulo 1.1 del Reglamento Delegado (UE) 2022/127 (Letra B)) Punto importante es tener verificaciones de idoneidad en el puesto y competencia necesaria para desempeñar la función de seguridad que pueda llevar aparejada y muy especialmente la confidencialidad. Además, se han de considerar otras medidas como las acciones de formación (fraude), política de rotación, medidas frente a conflicto de

ENS				Nivel de equivalencia ISO	Control asociado de la ISO	Puntualizaciones ISO	Responsabilidades				CCN	CONCLUSIONES
Control		Cat. Aplicable PG	Cat. Aplicable PP				OOPP	OODD	Entidad Pública superior /CA / OOCC	Proveedor	Herramienta / GUIA	
						información a la que se accede y los riesgos percibidos. Este control debe complementarse con 6.2 Términos y condiciones de empleo						intereses (cargo de responsabilidad; puesto sensible relacionado con verificación, autorización, ejecución del pago y contabilidad),..
mp.per .2	**Deberes y obligaciones**	**MEDIA**	**BASICO***	**PARCIAL**	6.2 Términos y condiciones de empleo	Los acuerdos deben establecer las responsabilidades del personal y de la organización para la seguridad de la información. Este control debe complementarse con 6.4 Proceso disciplinario	60%		40%	0%	HERRAMIENTAS GOBERNANZA (INES) Guía CCN-STIC 821 Esquema Nacional de Seguridad. Normas de seguridad	Puede prepararse un Onboarding o Welcome a los usuarios (incluidos el personal de proveedores) en el que se incluya toda la información requerida para el acceso y manejo del sistema, y de la información / servicios. En relación a la confirmación expresa, el Perfil Particular [PP] será menos estricto, bastando con la evidencia del envío y recepción de los correos electrónicos pertinentes. Debe considerarse el control [org.2]. Pueden desplegarse diferentes medios para permitir el cumplimiento de este control (portal del empleado o banner en sistema que informen en el arranque de equipos, entre otras).
mp.per .3	**Concienciación**	**MEDIA**	**MEDIA**	**SI**	6.3 Concienciación, educación y capacitación en seguridad de la información	El personal de la organización y las partes interesadas relevantes deben recibir una adecuada concienciación, educación y capacitación en seguridad de la información y actualizaciones periódicas de las políticas y procedimientos de la organización, según corresponda para su función. Este control se debe complementar con el control 5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información	80%		10%	10%	HERRAMIENTAS GOBERNANZA (INES) ATENEA VANESA ELENA	Los OOPP deben disponer de un plan que considere acciones innovadoras para la debida concienciación. Puede utilizar diferentes medios de entrega, incluidos los basados en aula online o webinar, en información en una web, y otros. El personal técnico debe mantener actualizados sus conocimientos suscribiéndose a boletines y revistas o asistiendo a congresos y eventos destinados a la mejora técnica y profesional. **El programa de sensibilización debe incluir una serie de actividades a través de canales adecuados, como campañas, folletos, carteles, boletines, sitios web, sesiones informativas, módulos de aprendizaje y correos electrónicos. La comprensión del personal debe evaluarse al final de una actividad de sensibilización. El CCN dispone de herramientas que pueden ayudar a ello y otras autoridades de seguridad también (INCIBE, ENISA...)
mp.per .4	**Formación**	**MEDIA**	**MEDIA**	**SI**	6.3 Concientización, educación y capacitación en seguridad de la información	El personal de la organización y las partes interesadas relevantes deben recibir una adecuada concienciación, educación y capacitación en seguridad de la información y actualizaciones periódicas de las políticas y procedimientos de la organización, según corresponda para su función laboral.	80%		10%	10%	HERRAMIENTAS GOBERNANZA (INES) ATENEA VANESA ELENA	Los OOPP deberán disponer de un plan de formación adecuado y mantener un seguimiento de la eficacia de las acciones desplegadas. El CCN dispone de herramientas que pueden ayudar a ello y otras autoridades de seguridad también (INCIBE, ENISA...) El personal de proveedores o de las entidades públicas deberán estar formados en seguridad, siendo responsabilidad de estas, su ejecución.
mp.eq. 1	**Puesto de trabajo despejado**	**MEDIA**	**MEDIA**	**SI**	7.7 Escritorio despejado y pantalla limpia	Deben definirse y aplicarse reglas claras de escritorio, papeles y medios de almacenamiento y/o extraíbles, así como reglas para pantallas limpias en las instalaciones del organismo.	100%		0%	0%	HERRAMIENTAS GOBERNANZA (INES)	Ambas normas están en clara sinergia por lo que el OOPP debe considerar la protección de la información (especialmente aquella que por las funciones desarrolladas deba someterse a confidencialidad o se considere sensible o crítica). Debe considerarse la seguridad de la información en papel o en medios de almacenamiento como USB o similares, y debe tratar de archivarse en lugares con cierres operativos, bajo llave (caja fuerte, armario o archivador u otro tipo de mobiliario de

ENS				Nivel de equivalencia ISO	Control asociado de la ISO	Puntualizaciones ISO	Responsabilidades				CCN	CONCLUSIONES
Control		Cat. Aplicable PG	Cat. Aplicable PP				OOPP	OODD	Entidad Pública superior /CA / OOCC	Proveedor	Herramienta / GUIA	
												seguridad) cuando haya cesado la necesidad de uso y cuando no se pueda mantener el control sobre la misma (por ejemplo, ausencias o la oficina está desocupada). Esta medida debe ponerse en consonancia con [org.2] y 5.10 Uso aceptable de la información y otros activos asociados y 5.36 Cumplimiento de políticas y estándares para la seguridad de la información. Las acciones de sensibilización deben trabajar esta medida.
mp.eq. 2	**Bloqueo de puesto de trabajo**	**ALTA ***	**MEDIA**	**SI**	7.7 Escritorio despejado y pantalla limpia	Deben definirse y aplicarse reglas claras de escritorio, papeles y medios de almacenamiento y/o extraíbles, así como reglas claras para pantallas limpias en las instalaciones del organismo.	70%		0%	30%	HERRAMIENTAS GOBERNANZA (INES) CLARA	Esto implica necesariamente que los equipos y dispositivos y servicios, deben desconectarse o protegerse con un mecanismo de bloqueo controlado por una contraseña, token o mecanismo de autenticación de usuario. Todos los equipos y dispositivos y servicios deben configurarse con una función de tiempo de espera o cierre de sesión automático. El OOPP debería al menos, desplegar esta política en el directorio y desplegarlo desde el bastionado, elaborar una Instrucción Técnica que lo desarrolle en otros elementos del sistema / dispositivos, y comprobar la efectividad cada cierto tiempo. Por ejemplo, se puede proceder cada cierto tiempo a comprobar mediante CLARA la aplicación en los equipos. Los servicios SaaS deben desplegar esta medida en idénticos términos, por lo que debe requerirse a los proveedores su presencia y comprobar su aplicabilidad. Los usuarios en todo caso, deben ser conocedores de la necesidad de bloquear las sesiones de los equipos, dispositivos y servicios cuando procedan a abandonar el puesto, aunque sea por un tiempo limitado.
mp.eq. 3	**Protección de dispositivos portátiles**	**ALTA**	**BASICA (+R2)**	**PARCIAL**	7.9 Seguridad de los activos fuera de las instalaciones 8.1 Dispositivos de usuario	Los activos fuera de las instalaciones deben protegerse teniendo en cuenta los diferentes riesgos. La información almacenada, procesada o accesible a través de los dispositivos de los usuarios debe protegerse.	70%		0%	30%	HERRAMIENTAS GOBERNANZA (INES) CLARA CCN-STIC-105 Catálogo de Productos y Servicios de Seguridad de las TIC	Esta medida conecta directamente con los controles [op.exp.1]. Es posible que el inventario operativo completo este gestionado o compartido por otro organismo gestor de patrimonio público. Además, debe considerarse especialmente la gestión de incidentes de seguridad [op.exp.7], (5.24, 5.26) junto con el control de acceso desde fuera de zonas controladas [op.acc.6]. [op.acc.6.r8.1] Para el acceso desde o a través de zonas no controladas se requerirá un doble factor de autenticación. Refuerzo R9-Acceso remoto (todos los niveles). [op.acc.6.r9.1] Será de aplicación la ITS de Interconexión de sistemas de información. [op.acc.6.r 9.2] El acceso remoto deberá considerar los siguientes aspectos: a) Ser autorizado por la autoridad correspondiente. b) El tráfico deberá ser cifrado. c) Si la utilización no se produce de manera constante, el acceso remoto deberá encontrarse inhabilitado y habilitarse únicamente cuando sea necesario. d) Deberán recogerse registros de auditoría de este tipo de conexiones. Debe considerarse, el cifrado del mismo como indica el Refuerzo R1 – Cifrado del disco, si del inventario de información se contempla que la

ENS				Nivel de equivalencia ISO	Control asociado de la ISO	Puntualizaciones ISO	Responsabilidades				CCN	CONCLUSIONES
Control		Cat. Aplicable PG	Cat. Aplicable PP				OOPP	OODD	Entidad Pública superior /CA / OOCC	Proveedor	Herramienta / GUIA	
												misma tiene un nivel MEDIO. En tal caso se considerara CCN-STIC-105 Catálogo de Productos y Servicios de Seguridad de las TIC 7.5.1 FAMILIA: ALMACENAMIENTO CIFRADO DE DATOS Igualmente, cuando el equipo contenga información que por razones de las funciones que desarrolla el OOPP pueda considerase crítica y ALTA, se mantendrá Refuerzo R2 – Entornos protegidos [mp.eq.3.r1.1] El uso de equipos portátiles fuera de las instalaciones de la organización se restringirá a entornos protegidos, donde el acceso sea controlado, a salvo de hurtos y miradas indiscretas. Son interesantes las buenas prácticas de seguridad contenidas en la ISO 27002 y especialmente: a) Disponer de un registro de dispositivos de usuario con identificación de los requisitos de protección física y lógica que requiere cada uno. b) Restricción de la instalación de software (por ejemplo, controlado de forma remota por los administradores del sistema); c) Requisitos para versiones de software del dispositivo y para aplicar actualizaciones (por ejemplo, actualización automática activa); d) Identificación y aprobación previa de reglas para la conexión a servicios , redes públicas o cualquier otra red fuera de las instalaciones (por ejemplo, que requiera el uso de un cortafuegos personales); e) Cifrado de dispositivos de almacenamiento; f) Protección, detección y respuesta contra malware (por ejemplo, uso de antimalware específico); g) Desactivación, eliminación o bloqueo remoto; h) Copias de seguridad del equipo completo, incluyendo configuración; i) Fomentar el uso de servicios y aplicaciones SaaS; j) Análisis del comportamiento del usuario final; k) Uso controlado de dispositivos extraíbles y posibilidad de desactivar los puertos USB; i) Uso de capacidades de partición, si es compatible con el dispositivo, que puede separar de forma segura la información de la organización y otros activos asociados (por ejemplo, software) de otra información y otros activos asociados en el dispositivo.
mp.eq.4	**Otros dispositivos conectados a la red**	**MEDIA**	**BASICA ***	**PARCIAL**	8.1 Dispositivos de usuario	Considerar el proceso de configuración y el manejo seguro por los usuarios	60%		40%	0%	HERRAMIENTAS GOBERNANZA (INES) CCN-STIC-105 Catálogo de Productos y Servicios de Seguridad de las TIC	Este control implica necesariamente considerar estos dispositivos en [op.exp.2] y [op.exp.3] y mantener las comprobaciones precisas. Se excluirá el R1 por no ser contemplado en la ISO, pero cuando se inicien procesos de renovación y licitación competencia del OOPP, se procederá a analizar la adecuación del dispositivo al mismo.

ENS				Nivel de equivalencia ISO	Control asociado de la ISO	Puntualizaciones ISO	Responsabilidades				CCN	CONCLUSIONES
Control		Cat. Aplicable PG	Cat. Aplicable PP				OOPP	OODD	Entidad Pública superior /CA / OOCC	Proveedor	Herramienta / GUIA	
mp.com.1	Perímetro seguro	MEDIA	MEDIA	PARCIAL	8.20 Controles de red 8.21 Seguridad de los servicios de red	Los mecanismos de seguridad, los niveles de servicio y los requisitos de los servicios de red, deben identificarse, implementarse y monitorizarse.	10%		20%	70%	ROCIO EMMA HERRAMIENTAS GOBERNANZA (INES) CCN-STIC 816 Seguridad en Redes Inalámbricas en el ENS CCN-STIC-811 Interconexión en el ENS	Los servicios de red incluyen la provisión de conexiones, servicios de red privada y soluciones de seguridad de red administrada, como firewalls y sistemas de detección de intrusos. Estos servicios pueden variar desde ancho de banda simple no administrado, hasta servicios complejos . Es posible que dependa a nivel de red de una entidad pública y no pueda gestionar este control. Se recuerda que todos los dispositivos de red están implicados en el proceso de bastionado [op.exp.2][op.exp.3]. A nivel de servicios SaaS / IaaS (y Cloud en general) debe considerarse al proveedor responsable del cumplimiento. A nivel de equipo, se desplegará el firewall en modo local de los equipos de usuario.
mp.com.2	Protección de la confidencialidad	MEDIA	MEDIA	PARCIAL	8.20 Controles de red 8.21 Seguridad de los servicios de red	Los mecanismos de seguridad, los niveles de servicio y los requisitos de los servicios de red, deben identificarse, implementarse y monitorizarse.	10%		20%	70%	EMMA HERRAMIENTAS GOBERNANZA (INES) CCN-STIC-836 ENS - Seguridad en VPN CCN-STIC-807 Criptología de empleo en el ENS	La organización debe garantizar que se apliquen los controles de seguridad adecuados al uso de redes virtualizadas, incluidas las redes SDN, SD-WAN. Se deben considerar diferentes modalidades, VPN TLS, IPSEC, MACSEC, WIREGUARD. Recomendación de algoritmo de cifrado 128 cifrado simétrico. AES Todas las redes estarán inventariadas y las VPN deberán ser controladas, gestionadas e inhabilitadas cuando cesen en su necesidad. Se tendrá en cuenta lo dispuesto en [op.acc.6]. Refuerzo R9-Acceso remoto (todos los niveles). [op.acc.6.r9.1] Será de aplicación la ITS de Interconexión de sistemas de información. [op.acc.6.r 9.2] El acceso remoto deberá considerar los siguientes aspectos: a) Ser autorizado por la autoridad correspondiente. b) El tráfico deberá ser cifrado. c) Si la utilización no se produce de manera constante, el acceso remoto deberá encontrarse inhabilitado y habilitarse únicamente cuando sea necesario. d) Deberán recogerse registros de auditoría de este tipo de conexiones.
mp.com.3	Protección de la integridad y de la autenticidad	MEDIA	MEDIA	PARCIAL	8.20 Controles de red 8.21 Seguridad de los servicios de red	Los mecanismos de seguridad, los niveles de servicio y los requisitos de los servicios de red, deben identificarse, implementarse y monitorizarse.	10%		20%	70%	EMMA HERRAMIENTAS GOBERNANZA (INES) CCN-STIC-836 ENS - Seguridad en VPN CCN-STIC-807 Criptología de empleo en el ENS	La organización debe garantizar que se apliquen los controles de seguridad adecuados al uso de redes virtualizadas, incluidas las redes SDN, SD-WAN. Se deben considerar diferentes modalidades, VPN TLS, IPSEC, MACSEC, WIREGUARD. Dado que la ISO es flexible a la hora de incorporar requerimiento de regulaciones nacionales, se derivan los requisitos a las Guías del CCN-STIC 836 y 807. Recomendación de algoritmo de cifrado 128 cifrado simétrico. AES Todas las redes estarán inventariadas y las VPN deberán ser controladas, gestionadas e inhabilitadas cuando cesen en su necesidad. Se tendrá en cuenta lo dispuesto en [op.acc.6].

ENS				Nivel de equivalencia ISO	Control asociado de la ISO	Puntualizaciones ISO	Responsabilidades				CCN	CONCLUSIONES
Control		Cat. Aplicable PG	Cat. Aplicable PP				OOPP	OODD	Entidad Pública superior /CA / OOCC	Proveedor	Herramienta / GUIA	
												Refuerzo R9-Acceso remoto (todos los niveles). [op.acc.6.r9.1] Será de aplicación la ITS de Interconexión de sistemas de información. [op.acc.6.r 9.2] El acceso remoto deberá considerar los siguientes aspectos: a) Ser autorizado por la autoridad correspondiente. b) El tráfico deberá ser cifrado. c) Si la utilización no se produce de manera constante, el acceso remoto deberá encontrarse inhabilitado y habilitarse únicamente cuando sea necesario. d) Deberán recogerse registros de auditoría de este tipo de conexiones.
mp.com.4	**Separación de flujos de información en la red**	**MEDIA**	**MEDIA**	**PARCIAL**	8.23 Segregación en redes	Mismo criterio de seguridad para la ISO que ENS, por cuanto las redes deben dividirse en dominios de red separados y separándolas de la red pública (es decir, Internet). Las agrupaciones pueden hacerse por confianza, criticidad, sensibilidad, organización...y mediante red física o lógica	10%		20%	70%	EMMA HERRAMIENTAS GOBERNANZA (INES) CCN-STIC-836 ENS - Seguridad en VPN CCN-STIC-807 Criptología de empleo en el ENS CCN-STIC-811 Interconexión en el ENS	Es posible que las operaciones y gestiones dependan a nivel de red, de una entidad pública jerárquicamente superior y/o otra entidad pública y no pueda gestionarse este control por el OOPP. Por ello deberá constar la petición de segmentación y la información precisa y actualizada en el diagrama de red del OOPP [op.pl.2] Cuando por razones de tamaño y capacidad, no pueda gestionarse una segregación a los efectos del control, será suficiente con VLAN para una red de administración y una de usuarios internos del OOPP La red wifi debe ser segregada o anulada. Ver requisitos en la Guía CCN STIC 836
mp.si.1	**Marcado de soportes**	**MEDIA**	**MEDIA**	**SI**	5.13 Etiquetado de la información	Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de la información adoptado por la organización	100%		0%	0%	HERRAMIENTAS GOBERNANZA (INES)	La entidad debe desplegar un proceso asociado a [mp.info.2] y considerar los procedimientos operativos correspondientes [org.3]. El personal afectado (propio o externo) recibirá formación al efecto [mp.per.4] Se considerará el etiquetado necesario y cómo colocarlo en documentos papel y digital (metadatos). Este control se conectará con el control [mp.info.5]. Ambas normas cohesionan perfectamente y podrán enlazarse los controles para dar cumplimiento a las dos.
mp.si.2	**Criptografía**	**MEDIA (+R2)***	**BASICA***	**PARCIAL**	7.10 Medios de almacenamiento	Los medios de almacenamiento deben ser gestionados a lo largo de su ciclo de vida; e adquisición, uso, transporte y eliminación, de acuerdo con el esquema de clasificación y los requisitos de uso de la organización.	50%	10%	0%	40%	HERRAMIENTAS GOBERNANZA (INES) CCN-STIC-105 Catálogo de Productos y Servicios de Seguridad de las TIC CCN-STIC-807 Criptología de empleo en el ENS	La organización debe establecer una política específica sobre la gestión de medios extraíbles y comunicar dicha política a cualquier persona que use o manipule, medios extraíbles. Con carácter general se considerará como medida, que los puertos de medios extraíbles, por ejemplo, las ranuras para tarjetas SD y los puertos USB, solo deben habilitarse si existe una razón organizativa para su uso. Se deberá cifrar aquellos dispositivos que salgan de las instalaciones, especialmente si son copias. Dado que pueden depender de una entidad jerárquica superior y/o entidad pública, se puede delegar este control a la misma o al proveedor que gestione esta actividad en el CPD. Esta medida es susceptible de excluirse si no existen dispositivos

ENS				Nivel de equivalencia ISO	Control asociado de la ISO	Puntualizaciones ISO	Responsabilidades				CCN	CONCLUSIONES
Control		Cat. Aplicable PG	Cat. Aplicable PP				OOPP	OODD	Entidad Pública superior /CA / OOCC	Proveedor	Herramienta / GUIA	
												afectados y el OOPP emplea servicios de almacenamiento Cloud que eviten almacenamientos en local. Se debe considerar el requerimiento dado por la Guía CCN-STIC 807 Criptología de empleo en el ENS y/o Guía CCN-STIC 221.
mp.si.3	Custodia	MEDIA	MEDIA	SI	7.10 Medios de almacenamiento	Los medios de almacenamiento deben ser gestionados a lo largo de su ciclo de vida, adquisición, uso, transporte y eliminación, de acuerdo con el esquema de clasificación y los requisitos de uso de la organización.	70%		20%	10%	HERRAMIENTAS GOBERNANZA (INES)	La organización debe establecer una política específica sobre la gestión de medios extraíbles y comunicar dicha política a cualquier persona que use o manipule, medios extraíbles, exigir autorización para los medios y mantener un registro. Es posible que se establezcan almacenamientos en cajas ignifugas, por lo que se debe trazar con las indicaciones de los fabricantes y el punto de conservación que permite la misma ante el fuego. Se deben tener en consideración, las instrucciones fabricantes con la temperatura y humedad, por lo que formará parte de la documentación del sistema las fichas técnicas correspondientes [org.3] Se desplegaran aquellas buenas prácticas que se describen en la ISO 27002 que puedan enriquecer este control para los OOPP. Por ejemplo; todos los medios deben almacenarse en un entorno seguro y protegido de acuerdo con su clasificación de información y protegidos contra amenazas ambientales (como calor, humedad, campo electrónico o envejecimiento), de acuerdo con las especificaciones de los fabricantes; para mitigar el riesgo de que los medios se degraden mientras aún se necesita la información almacenada, la información debe transferirse a medios nuevos antes de que se vuelva ilegible.
mp.si.4	Transporte	MEDIA	MEDIA	SI	7.10 Medios de almacenamiento	Los medios de almacenamiento deben ser gestionados a lo largo de su ciclo de vida, adquisición, uso, transporte y eliminación, de acuerdo con el esquema de clasificación y los requisitos de uso de la organización	70%		20%	10%	HERRAMIENTAS GOBERNANZA (INES)	La organización debe establecer una política específica sobre la gestión de medios extraíbles y comunicar dicha política a cualquier persona que use o manipule medios extraíbles, exigiendo la autorización y supervisándose por el Responsable de Sistemas, quien controlará el registro de entradas y salidas y analizará la coherencia de sus anotaciones. Con carácter general, los elementos con información catalogada como USO OFICIAL, serán protegidos y sometidos a un cifrado si así lo determina la sensibilidad de la información. Se pueden agrupar requisitos del ENS y buenas prácticas de la ISO, bajo un proceso único. Así podremos considerar cuando corresponda en el OOPP, las siguientes pautas; a) utilizar transporte o mensajeros de confianza o debidamente acreditados, creando una lista de mensajeros autorizados; b) desarrollar procedimientos para verificar la identificación de los mensajeros; c) el embalaje debe ser suficiente para proteger el contenido de cualquier daño físico que pueda surgir durante el tránsito, protegiendo contra cualquier factor ambiental, como la exposición al calor, humedad

ENS				Nivel de equivalencia ISO	Control asociado de la ISO	Puntualizaciones ISO	Responsabilidades				CCN	CONCLUSIONES
Control		Cat. Aplicable PG	Cat. Aplicable PP				OOPP	OODD	Entidad Pública superior /CA / OOCC	Proveedor	Herramienta / GUIA	
												o campos electromagnéticos ; d) utilizar controles a prueba de manipulaciones o a prueba de manipulaciones.
mp.si.5	Borrado y destrucción	MEDIA	MEDIA	SI	7.14 Eliminación segura o reutilización de equipos 8.10 Eliminación de información	Los elementos susceptibles de ser medios de almacenamiento, deben revisarse para garantizar que todos los datos confidenciales y el software con licencia, se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización. La información almacenada en los sistemas y dispositivos de información debe eliminarse cuando ya no se necesite	80%		10%	10%	HERRAMIENTAS GOBERNANZA (INES) OLVIDO CCN-STIC-105 Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación CCN-STIC-140 Taxonomía de referencia para productos de Seguridad TIC (Anexo E3 y E3M)	La organización debe establecer una política específica sobre la gestión de medios extraíbles y comunicar dicha política a cualquier persona que use o manipule medios extraíbles. Para el uso de elementos de borrado se deberá considerar las recomendaciones del CCN y las herramientas contenidas en el Catálogo CCN STIC 105. Se podrán emplear propuestas derivadas de la ISO 27040 En su caso puede ser importante tener presente medidas complementarias considerando las amenazas y requisitos de seguridad presentes en el CCN-STIC-140 Taxonomía de referencia para productos de Seguridad TIC - Anexo E.3: Herramientas de Borrado Seguro y Anexo E.3M: Herramientas de Borrado Seguro. En los servicios SaaS (y Cloud en general) se procederá a requerir el uso de procesos de borrado seguro y acreditaciones al efecto. Si se contrata a proveedores para realizar procesos de borrado y eliminación, se deberá requerir evidencias de la seguridad en el servicio y certificación de la efectividad al efecto. Cuando se proceda a reutilizar el medio, deberá procederse a un borrado efectivo que impida acceder a la información. Para la eliminación de los medios de manera segura, se podrá optar por incineración o trituración. Se deben registrar los resultados de la eliminación y borrado como prueba y evidencia.
mp.sw.1	Desarrollo de aplicaciones	MEDIA	MEDIA	SI	8.25 Ciclo de vida de desarrollo seguro	Deben establecerse y aplicarse reglas para el desarrollo seguro de software y sistemas.	20%	20%	20%	40%	HERRAMIENTAS GOBERNANZA (INES) CCN STIC 422 Desarrollo seguro de aplicaciones web	A nivel del ENS debe considerarse el control solo en el caso de que el OOPP proceda a realizar desarrollo para los servicios propios derivados de su naturaleza. En caso contrario no aplicara. Es posible que ciertos servicios electrónicos sean en modo SaaS o el responsable sea una entidad jerárquica superior y/o entidad pública, por cuanto, en ambos casos, el control derivará en su cumplimiento a los mismos. A efectos de la ISO, este control debe complementarse con otros controles más detenidamente. a) separación de los entornos de desarrollo, prueba y producción (ver 8.31); b) orientación sobre la seguridad en el ciclo de vida del desarrollo de software: metodología de desarrollo de software (ver 8.28 y 8.27);pautas de codificación segura (ver 8.28); c) requisitos de seguridad en la fase de especificación y diseño (ver 5.8); d) puntos de control de seguridad dentro de los hitos del proyecto (ver 5.8); e) pruebas de sistema y seguridad, como pruebas de regresión, escaneo de código y pruebas de penetración (ver 8.29); f) repositorios seguros para el código fuente y la configuración (ver 8.4 y

ENS				Nivel de equivalencia ISO	Control asociado de la ISO	Puntualizaciones ISO	Responsabilidades				CCN	CONCLUSIONES
Control		Cat. Aplicable PG	Cat. Aplicable PP				OOPP	OODD	Entidad Pública superior /CA / OOCC	Proveedor	Herramienta / GUIA	
												8.9); g) seguridad en el control de versiones (ver 8.32); h) conocimiento y capacitación en seguridad de aplicaciones requeridos (ver 8.28); i) la capacidad de los desarrolladores para prevenir, encontrar y reparar vulnerabilidades (ver 8.28); j) requisitos de licencia y alternativas para garantizar soluciones rentables y evitar futuros problemas de licencia (ver 5.32).
mp.sw.2	**Aceptación y puesta en servicio**	**MEDIA**	**MEDIA**	**PARCIAL**	8.29 Pruebas de seguridad en desarrollo y aceptación	Los procesos de prueba de seguridad deben definirse e implementarse en el ciclo de vida del desarrollo. Se debe complementar este control con el 8.31 Separación de los entornos de desarrollo, prueba y producción	50%		20%	30%	HERRAMIENTAS GOBERNANZA (INES) CCN STIC 422 Desarrollo seguro de aplicaciones web	Importante mantener los entornos de pruebas, desarrollo y [pre]producción diferenciados. Se deben realizar pruebas funcionales y de seguridad, por ejemplo, autenticación de usuario y restricción de acceso y uso de criptografía. Es posible que ciertos servicios electrónicos sean en modo SaaS o el responsable sea una entidad jerárquica superior y/o entidad pública, por cuanto, en ambos casos, el control derivará en su cumplimiento a los mismos. Además, se debe realizar la codificación segura y configuraciones seguras, incluida la de los sistemas operativos, firewalls y otros componentes de seguridad. actividades de revisión de código para probar fallas de seguridad, realizar análisis de vulnerabilidades para identificar configuraciones inseguras y vulnerabilidades del sistema y realizar pruebas de penetración para identificar código y diseño inseguros.
mp.info.1	**Datos personales**	**MEDIA**	**MEDIA**	**SI**	5.34 Privacidad y protección de la información de identificación personal (PII)	La organización debe identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la información personal de acuerdo con las leyes y normas aplicables y los requisitos contractuales.	50%	30%	10%	10%	HERRAMIENTAS GOBERNANZA (INES)	Debe considerarse las obligaciones derivadas del legislador europeo y la necesidad de dar cumplimiento. Es posible que parte de estas obligaciones sean compartidas con una entidad pública jerárquicamente superior y/o entidad pública o que asuma ciertos roles. Asimismo, es necesario que se contemplen los encargos de tratamiento y corresponsabilidades y estén reguladas las obligaciones correctamente.
mp.info.2	**Calificación de la información**	**MEDIA**	**MEDIA**	**SI**	5.12 Clasificación de la información	Se puede trazar con los requisitos concretos del ENS y derivar el cumplimiento de las dos normas a esta.	80%	10%	10%	0%	HERRAMIENTAS GOBERNANZA (INES)	La política de calificación determinará los criterios que, determinarán el nivel de seguridad requerido, dentro del marco regulador operativo en OOPP y en su caso, considerando con carácter general lo criterios descritos en el Anexo I del Real Decreto 311/2022. Se considerará la sensibilidad de la información y en base a la misma, se asignará el USO OFICIAL. Será el responsable de cada información, el encargado de asignar a cada información el nivel de seguridad requerido, y de su documentación y aprobación formal. Este tendrá en cada momento la exclusiva potestad de modificar el nivel de seguridad. Es importante considerar que la entidad va a generar intercambios con otras entidades y debe incluir el esquema de calificación en los acuerdos, implicando las medidas de seguridad que se derivan de ello. En el caso de la ISO se integra perfectamente con los requerimientos

ENS				Nivel de equivalencia ISO	Control asociado de la ISO	Puntualizaciones ISO	Responsabilidades				CCN	CONCLUSIONES
Control		Cat. Aplicable PG	Cat. Aplicable PP				OOPP	OODD	Entidad Pública superior /CA / OOCC	Proveedor	Herramienta / GUIA	
												legales desplegados por el ENS por lo que se pueden unificar requerimientos.
mp.info.3	Firma electrónica	MEDIA	MEDIA	No	8.24 Uso de criptografía 8.26 Requisitos de seguridad de la aplicación	Este no es un control especifico de la ISO, pero lo asociamos a ciertos controles Consideramos los elementos criptográficos. Cuando se utiliza una autoridad de confianza (p. ej., con el fin de emitir y mantener firmas o certificados digitales), la seguridad está integrada en todo el proceso de gestión de firmas o certificados de extremo a extremo	20%	10%	70%	10%	HERRAMIENTAS GOBERNANZA (INES) LORETO CCN-STIC-807 Criptología de empleo en el ENS CCN-STIC-140 Taxonomía de referencia para productos de Seguridad TIC	La ISO no considera este control, pero puede asociarse a los controles 8.26 y 8.24. Es importante, que el OOPP despliegue una política o se adscriba a la de la entidad administrativa superior. Es importante que se gestione la custodia y uso de la firma. En este entorno tendrá especial consideración los servicios en la nube por lo que puede que sea necesario desplegar acuerdos concretos con otras entidades públicas o con terceros. Es posible que se desplieguen servicios HSM, que deberán ser conforme al ENS. Dentro de la misma se deberá considerar los procesos en los que debe mantenerse la verificación de la firma y por ello desplegar entornos de conservación, que permitan dicha verificación. Estos entornos pueden ser en un servicio propio o de un tercero. Si bien no es aplicable, el OOPP puede desplegar componentes certificados conforme al [op.pl.5]
mp.info.4	Sellos de tiempo	ALTA	NA	No	8.24 Uso de criptografía 8.26 Requisitos de seguridad de la aplicación	Este no es un control especifico de la ISO, pero lo asociamos a ciertos controles Consideramos los elementos criptográficos y específicamente la sincronización de relojes y acreditación temporal de los actos.	50%		40%	10%	HERRAMIENTAS GOBERNANZA (INES)	La ISO no considera este control, pero puede asociarse a los referenciados. Este control solo aplica a los OOPP que gestionan ayudas superiores a 400 millones, por su implicación y criticidad. Se emplearán "sellos cualificados de tiempo electrónicos" atendiendo a lo dispuesto en el Reglamento (UE) nº 910/2014
mp.info.5	Limpieza de documentos	MEDIA	MEDIA	No	5.13 Etiquetado de la información	Este control no está contemplado expresamente por la norma, pero puede considerarse en el control derivado de etiquetado de documentos digitales y el uso de metadatos para ello.	80%		0%	20%	HERRAMIENTAS GOBERNANZA (INES) Guía CCN-STIC 835 Borrado de metadatos en el marco del ENS	Este control está conectado con el control [org.2] y [mp.si.1] y [mp.info.2]. Se deben mantener acciones de formación y concienciación a los efectos de lo dispuesto en el [mp.per.3] y [mp.per.4] Aunque la ISO no contempla expresamente control si se aprecian referencias a la gestión de metadatos en el control 5.13 y como buenas prácticas pueden completar lo dispuesto por ENS.
mp.info.6	Copias de seguridad	MEDIA (+R2) *	BASICA*	SI	8.13 Copia de seguridad de la información	Las copias de seguridad abarcarán la información, el software, configuración y en general los sistemas deben mantenerse y probarse regularmente de acuerdo con la política de respaldo específica del tema acordada.	30%		10%	60%	HERRAMIENTAS GOBERNANZA (INES) CCN-STIC-822 Procedimientos de Seguridad ENS. Anexo III .PR 30 Procedimiento de generación de copias de respaldo y recuperación de la información	A efectos de la ISO existe una equivalencia adecuada por cuanto el control operativo 8.13, se alinea con el [mp.info.6] Es importante tener en cuenta que este control se asocia a continuidad y para la ISO esto es significativo, por cuanto los OOPP deberán tenerlo presente para cumplir con los requisitos de la norma. Es necesario el establecimiento de una política de respaldo que considere los requisitos de seguridad de la información y retención de datos de la organización. Se deben considerar instalaciones de respaldo para la información y el software. El proceso de copias y sus plazos y retenciones estarán alineadas con los requerimientos legales, específicamente aquellos propios de la naturaleza del OOPP y de la información personal que contiene. Se tiene que controlar la información relacionada con todo el proceso de copias, incluido el software empleado, los procesos, revisiones… Se

ENS				Nivel de equivalencia ISO	Control asociado de la ISO	Puntualizaciones ISO	Responsabilidades				CCN	CONCLUSIONES
Control		Cat. Aplicable PG	Cat. Aplicable PP				OOPP	OODD	Entidad Pública superior /CA / OOCC	Proveedor	Herramienta / GUIA	
												debería disponer de un protocolo para realizar restauraciones sencillas y se podrá alinear con el control [op.cont.3], y considerarlo como pruebas de continuidad Debe considerarse dentro del proceso, la eliminación segura de las copias y de los soportes de estas. Es posible que este control se delegue a un proveedor o a una entidad pública cuando existan elementos o servicios responsabilidad de estos. Determinados procesos de copias asociados a elementos de la infraestructura/ arquitectura, pueden ser responsabilidad de una entidad pública jerárquicamente superior y/o entidad pública o incluso un prestador. Los servicios en la nube deben asumir y evidenciar los procesos de copias y restauraciones, manteniendo los acuerdos correspondientes. Con carácter general, se recomienda no permitir el proceso de almacenamiento en local, evitando que información y determinados servicios estén excluidos de la política de copias.
mp.s.1	**Protección del correo electrónico**	**MEDIA**	**MEDIA**	**PARCIAL**	5.14 Transferencia de información	Deben existir reglas, procedimientos o acuerdos de transferencia de información, tanto dentro de la organización como entre la organización y otras partes, para todos los tipos de transferencia.	40%	10%	0%	50%	HERRAMIENTAS GOBERNANZA (INES) Guía CCN- STIC 814 Seguridad en correo CCN-STIC-821 Normas de Seguridad en el ENS - ENS. Apéndice III. NP 20 Normas de acceso al correo Electrónico (E-Mail)	Para ISO se trata sobre todo de intercambio o transferencia de información, además de medios electrónicos que es donde se incluye el servicio de correo, Deberá incluir el OOPP pautas relacionadas a medios de transmisión de información (no solo correo electrónico, sino otros medios, incluidos medios físicos y transmisión verbal) que enriquecerán las pautas de seguridad de ENS. Considerar acciones de ingeniería social que pueden ayudar a concienciar [mp.per.3]
mp.s.2	**Protección de servicios y aplicaciones web**	**MEDIA**	**MEDIA**	**PARCIAL**	8.26 Requisitos de seguridad de la aplicación	Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones.	40%		20%	40%	ANA HERRAMIENTAS GOBERNANZA (INES) CCN-STIC-812 Seguridad en servicios web CCN-STIC-823 Utilización de servicios en la nube	Este control se podrá delegar a una entidad jerárquicamente superior y/o entidad pública o a un prestador con servicios específicos o incluso al prestador de servicios web. Se recomienda incluir en los contratos y condiciones de los pliegos, el requerimiento de la ejecución del análisis y de los planes de acción resultantes de dichos análisis. Los servicios contratados a terceros deberán contener las medidas requeridas en este control y específicamente la obligación de corregir las vulnerabilidades detectadas en las plataformas mediante los análisis de seguridad. EL OOPP dispondrá de un plan de auditoria en el que reflejará las fechas estimadas de ejecución de las auditorias y la referencia de la entidad (pública o privada) encargada de la misma.

ENS				Nivel de equivalencia ISO	Control asociado de la ISO	Puntualizaciones ISO	Responsabilidades				CCN	CONCLUSIONES
Control		Cat. Aplicable PG	Cat. Aplicable PP				OOPP	OODD	Entidad Pública superior /CA / OOCC	Proveedor	Herramienta / GUIA	
												No existe un nivel de equivalencia con respecto a los requisitos establecidos por las normas dado que el ENS es riguroso y especifico. No obstante, la ISO, permite desplegar estos requisitos y ajustar el sistema y la declaración de aplicabilidad para su armonía. Se trazará con el plan de auditorías y revisiones y se enlazará con la gestión de los planes de acción derivados de la seguridad de las aplicaciones web / elementos publicados. Las aplicaciones accesibles a través de las redes están sujetas a una variedad de amenazas, por lo que se considerarán los requisitos de seguridad que se encuentran dispersos por la ISO, como la gestión de la accesos mediante la autenticación (ver 5.17 , 8.2 , 8.5); la resiliencia contra ataques maliciosos o interrupciones no intencionales (por ejemplo, protección contra desbordamiento de búfer o inyecciones de SQL);
mp.s.3	**Protección de la navegación web**	**MEDIA**	**MEDIA**	**SI**	8.22 Filtrado Web	El acceso a sitios web externos debe administrarse para reducir la exposición a contenido malicioso.	30%	10%	10%	50%	CLAUDIA MARTA HERRAMIENTAS GOBERNANZA (INES) VANESA ATENEA ELENA CCN-STIC-821 Normas de Seguridad en el ENS. Apéndice II. NP 10 Normas de acceso a Internet	Las dos normas se encuentran en este control muy alineadas. El filtrado web puede incluir una variedad de técnicas que incluyen firmas, lista de sitios web o dominios aceptables, lista de sitios web o dominios prohibidos y configuración personalizada para ayudar a evitar que el software y otras actividades maliciosas, afecten a la red y los sistemas de la organización. Se deben considerar acciones como bloqueo automáticos y formación y sensibilización, alineadas siempre con otros controles. No obstante, es posible que el OOPP no gestione los servicios de red por lo que podría ser responsabilidad de una entidad diferente o un proveedor la gestión y despliegue de algunas de las medidas descritas. Es cierto que el organismo puede gestionar parte del control mediante herramientas de seguridad, como un software preventivo frente al malware y que controle las acciones del usuario en la red. Se deben considerar las configuraciones de los navegadores conforme a [op.exp.2] y [op.exp.3].
mp.s.4	**Protección frente a denegación de servicio**	**MEDIA**	**MEDIA***	**PARCIAL**	8.6 Gestión de capacidad	El uso de los recursos debe monitorizarse y ajustarse de acuerdo con los requisitos de capacidad actuales y esperados.	10%			90%	GLORIA REYES HERRAMIENTAS GOBERNANZA (INES) CCN-STIC-820 Protección contra Denegación de Servicio	Los servicios Cloud llevan embebidos estas medidas, por cuanto sus servicios serán correctamente protegidos y balanceados en caso de necesidad. Deben establecerse controles de detección para indicar los problemas a su debido tiempo. Sería una buena medida considerar servicios en la nube con despliegue de medidas asociadas a la capacidad y disponibilidad (Los servicios en la nube se caracterizan por la elasticidad y escalabilidad que permiten una rápida expansión y reducción bajo demanda de los recursos disponibles para aplicaciones y servicios particulares, lo que es útil para reducir la demanda de los recursos de la organización)

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