centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 825

ESQUEMA NACIONAL DE SEGURIDAD
CERTIFICACIONES 27001

Julio 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
2023.07.10 13:31:06 +02'00'

Pº de la Castellana 109, 28046 Madrid

Fecha de Edición: julio de 2023
NIPO: 083-23-187-8

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

Los retos que en la actualidad presenta el uso de los medios tecnológicos, así como la incesante evolución de las denominadas tecnologías disruptivas vienen suponiendo un enorme desafío para las estrategias globales en ciberseguridad. La velocidad de la evolución tecnológica y la creciente dependencia de las sociedades en tales medios es paralela al incremento de los riesgos y amenazas que comporta su uso, requiriendo respuestas más sofisticadas, adaptadas a la realidad y coordinadas entre los diferentes agentes implicados.

Ha sido en este escenario donde los más significativos marcos de ciberseguridad[1] han evolucionado, gracias al esfuerzo de las diferentes entidades y autoridades responsables, que, en muchos casos, han derivado en normas de naturaleza legal, con el objetivo de impulsar y homogeneizar la seguridad en los estados.

Como decimos, en el contexto actual, las amenazas representan un grave problema para el funcionamiento de las actividades sociales, políticas y económicas de los estados, lo que ha propiciado que, en el ámbito internacional, europeo y nacional, hayan surgido normas que tienen como objetivo dar adecuada respuesta a estos retos.

El esfuerzo por incrementar los niveles de ciberseguridad, mediante la evolución de las regulaciones y normativas en materia de seguridad de la información, ha dado como resultado la actualización de dos normas clave para la ciberseguridad en nuestro país: el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) y la norma ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements[2]. Ambos textos han experimentado modificaciones significativas para afrontar los desafíos derivados de las nuevas amenazas, fortaleciendo los programas e iniciativas de seguridad, y facilitando la compatibilidad entre ambas y sus medidas y controles de seguridad.

El CCN, consciente de la existencia de diferentes marcos normativos, tanto a nivel europeo como internacional, ha desarrollado el presente documento para facilitar la integración e implantación de las normas citadas, señalando lo que de común tienen´.,.

Como marco [legal] de ciberseguridad, el Esquema Nacional de Seguridad[3], requiere el cumplimiento de los principios y requisitos mínimos establecidos[4], adoptando las medidas y refuerzos de seguridad correspondientes, establecidas en su Anexo II. Para implementar estas medidas, se hace necesario considerar previamente la categoría del sistema, tal y como se prevé en el artículo 40 y se detalla en el Anexo I, los activos que forman parte del sistema de información y la propia gestión de los riesgos de seguridad de la información.

El propio Esquema Nacional de Seguridad, reconoce la posibilidad de desplegar medidas de seguridad adicionales, a criterio del Responsable de Seguridad. Es más, dentro de esta flexibilidad para adaptarse a las necesidades del sistema de información y de los riesgos detectados, las propias medidas, pueden ser “moduladas” o “reemplazadas” por medidas compensatorias o

[1] Como es el caso del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).
[2] UNE-ISO/IEC 27001:2023 “Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos”
3 Artículo 28. Cumplimiento de los requisitos mínimos.
[4] Ver Capitulo II y Capitulo III del Real Decreto 311/2022, de 3 de mayo. BOE núm. 106, de 4 de mayo de 2022. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191

complementarias, que cumpliendo el mismo fin que las sustituidas, puedan lograr una seguridad y protección, al menos, equivalente.

Marco de [ciber]seguridad.

En el actual entorno tecnológico y de interconexiones, coexisten diferentes marcos de [ciber] seguridad, que se esfuerzan en desarrollar pautas para la gestión integral de los riesgos, y para reducir, detectar, reaccionar y recuperarse de cualquier ataque en [ciber]seguridad. Estos marcos, sin duda, coexisten y se interrelacionan con el Esquema Nacional de Seguridad, y permiten una visión holística de la seguridad en todo el entorno actual de ciber-tecnología.

Esquema Nacional de Seguridad presenta una estrecha relación con la norma ISO/IEC 27001:2022, pero existen otros marcos que con gran relevancia:

Organización	Marco de [ciber]seguridad
NIST National Institute of Standards and Technology https://www.nist.gov	**Cybersecurity Framework (CSF)** Marco de ciberseguridad voluntario desarrollado por NIST[5], que permite a las entidades desarrollar sus programas ciberseguridad y gestión de riesgos, con la característica de la adaptabilidad y flexibilidad. Así es un estándar que puede ser empleado en entidades de cualquier tamaño y sector. Su adhesión es voluntaria. Este marco despliega todo el programa sobre cinco funciones diferenciadas; identificar, proteger, detectar, responder y recuperar y una escala diferenciada de madurez.
	NIST SP 800-53 Marco de seguridad y privacidad para sistemas de información y organizaciones, que incluye un catálogo de controles para proteger las operaciones y los activos de la organización. Pueden encontrarse equivalencias entre diferentes marcos, como la ISO 27001. NIST 800-53 proporciona controles de seguridad que ayudan a desplegar NIST CSF[6]. .
National Cyber Security Centre https://www.ncsc.gov.uk/	El Centro Nacional de Ciberseguridad del Reino Unido, ha desarrollado un proceso de certificación[7] con similitudes al Esquema Nacional de Seguridad, encaminado a evaluar la experiencia, los productos y los servicios de ciberseguridad, de forma independiente según sus propios estándares. Existen diferentes esquemas de acreditación, bien para productos o para servicios.
Cloud Security Alliance (CSA) https://cloudsecurityalliance.org/	**Cloud Controls Matrix - CMM v4.**[8] Marco de control desarrollado por CSA, que se compone de 197 objetivos de controles distribuidos en 17 dominios, relacionado con elementos clave de la seguridad en la nube. Este marco se orienta a la mejora de la seguridad e implementación de controles de los diferentes servicios cloud. Pueden resultar útiles sus matrices de equivalencia con otros estándares de seguridad, como la ISO 27001/27002/27017/27018, NIST SP 800-53, AICPA TSC, German BSI C5, PCI DSS, ISACA COBIT, NERC CIP, FedRamp, CIS.
Center for Internet Security [CIS] https://www.cisecurity.org	CIS, es una organización sin ánimo de lucro, que trabaja en ciberseguridad. Ha desarrollado los estándares de seguridad; CIS Controls y CIS Benchmarks. También desarrolla otros trabajos en seguridad basados en las mejores prácticas globales. **CIS Controls** Incluye un conjunto de controles[9] que han sido priorizados y que, bajo las mejores prácticas de ciberseguridad, presenta bloques de acciones de prevención, protección, respuesta y recuperación. Estos controles están

[5] Agencia gubernamental de los EEUU. https://www.nist.gov/
[6] https://csrc.nist.gov/CSRC/media/Publications/sp/800-53/rev-5/final/documents/csf-pf-to-sp800-53r5-mappings.xlsx
[7] https://www.ncsc.gov.uk/section/products-services/introduction
[8] https://cloudsecurityalliance.org/research/cloud-controls-matrix/
[9] https://www.cisecurity.org/controls

	distribuidos en requisitos de seguridad organizados en 3 categorías, controles básicos, controles fundamentales, y controles organizativos. Entre los puntos de control que ha incorporado CIS se encuentran PCI DSS[10], HIPAA[11] y RGPD[12].
ISACA https://www.isaca.org	COBIT[13] Marco de seguridad desarrollado por ISACA para el gobierno y gestión de TI, modulable y adaptable a las organizaciones. Trabaja sobre 5 bloques de dominio en los que despliegan 40 procesos.

A los que hay que añadir la norma ISO/IEC 27001:2022. ISO [14]27001, es una norma de carácter voluntario que emplea la estructura de alto nivel de las normas ISO, Anexo (L), para mantener la compatibilidad con otras normas ISO. Dispone de un conjunto de cláusulas generales y un Anexo (A) que contiene el listado de controles de seguridad que las organizaciones deben desplegar en los sistemas.

2. OBJETO

El presente documento muestra las medidas compatibles entre el Esquema Nacional de Seguridad con el estándar ISO/ IEC 27001:2022.

Dicha compatibilidad no debe ser interpretada como una relación aritmética de equivalencia, sino una interpretación bajo un análisis general de los contenidos de ambas normas. Este análisis incluye los requisitos mínimos desplegados en el articulado del Real Decreto 311/2022, de 3 de mayo, y cláusulas [requisitos] de la ISO.

Esta guía pretende ofrecer una herramienta ágil para aquellas entidades que pretenden enriquecer su marco de seguridad asociado al cumplimiento del Esquema Nacional de Seguridad, mediante el despliegue de un sistema de gestión de seguridad de la información, con fuentes complementarias de la ISO 27002:2022 e incluso, capaz de soportar una certificación de la ISO 27001. Para la integración de sistemas de gestión, es recomendable realizar siempre un análisis de convergencias, por lo que la labor iniciada en esta guía solo es una aproximación general que deben ser particularizada para cada organización.

Esta guía también puede ser empleada a la inversa, es decir para aquellas entidades que ya disponiendo de sistemas de gestión de seguridad de la información bajo la ISO 27001, pretendan validar la conformidad de sus sistemas con el Real Decreto 311/2022 de 3 de mayo.

3. ALCANCE

Esta guía establece unas pautas de carácter general que son aplicables a entidades de distinta naturaleza, dimensión y sensibilidad sin entrar en casuísticas particulares. Se espera que cada organización las particularice para adaptarlas a su entorno singular.

[10] Payment Card Industry Data Security Standard
[11] Health Insurance Portability and Accountability Act
[12] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
[13] https://www.isaca.org/resources/cobit
[14] ISO (Organización Internacional de Normalización) e IEC (la Comisión Electrotécnica Internacional)constituyen el sistema especializado para la normalización a nivel mundial.

4. NORMAS ISO

ISO[15] es la Organización Internacional para la estandarización, que desarrolla mediante diferentes grupos de expertos [16], normas internacionales como marcos de reconocido prestigio y que permiten evidenciar la conformidad de procesos, productos o servicios, a unos requisitos previamente establecidos.

ISO goza de reconocimiento y prestigio internacional, por lo que a nivel global un sistema acreditado bajo este estándar otorga confiabilidad. Así, para una organización, presentar una acreditación relacionada con un estándar ISO supone poder evidenciar ante cualquier tercero, que de manera independiente se ha revisado y comprobado, el cumplimiento efectivo de los requisitos ISO. Un estándar ISO supone confiabilidad, por lo que en ocasiones son adoptadas por los gobiernos y autoridades de control, como referente de solidez y refuerzo normativo[17] lo que ayuda a ahorrar tiempo, costes y reducir las barreras en el ámbito internacional.

Y es aquí, donde destaca la importancia de esta Guía, como herramienta de análisis de las medidas de seguridad compatibles del estándar ISO/IEC 2700:2022 y el marco [legal] Real Decreto 311/2022, de 3 de mayo. De tal forma, que permita a entidades que así lo consideren, aprovechar las sinergias de un sistema de gestión de seguridad de la información bajo el paraguas de ambas[18].

Es importante en este punto resaltar que del mero hecho de disponer de un certificado de una norma ISO no se deviene automáticamente la equivalencia con otras normas o marcos. Las entidades han de someter a sus sistemas de gestión a los procesos de acreditación y conformidad que cada marco o norma requiere.

4.1. LA SAGA ISO/IEC 27000

A nivel general existe un conjunto completo de normas ISO 27000, que engloban diferentes prácticas, elementos o requerimientos de seguridad de la información y que servirán de ayuda para desplegar un sistema de seguridad de la información adecuado, y bajo las dimensiones de confidencialidad, integridad y disponibilidad.

Dentro de la familia ISO 27000[19], podemos pararnos en la propia ISO 27000 que nos describe la visión general de los sistemas de seguridad y nos aporta vocabulario y definiciones clave de los sistemas de gestión de seguridad de la información

También pueden ser buenas referencias de la familia de sistemas de gestión de seguridad de la información;

[15] https://www.iso.org/
[16] Los comités de expertos cuentan además con acuerdos de desarrollo con otras organizaciones como IEC- International Electrotechnical Comisión / Comisión Internacional Electrotécnica-.
[17] Puede considerarse por ejemplo, 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 (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).*"
[18] Liderado bajo marco [legal] de referencia, como norma de obligado cumplimiento para los sujetos que se encuentren bajo su ámbito de aplicación.
[19] https://www.iso.org/search.html?q=27000

ISO/IEC 27003 (norma que aporta pautas para desplegar un sistema de gestión de seguridad de la información con el ciclo de mejora ““Plan, Do, Check, Act”)

ISO/IEC 27004 (norma que desarrolla técnicas relacionadas con métricas e indicadores para medir la eficacia de un sistema de gestión de seguridad de la información)

ISO/IEC 27005 (norma que incluye metodologías para desarrollar el proceso de gestión de riesgos de seguridad de la información)

ISO /IEC 27017 (norma que despliega controles para la seguridad de la información en la nube)

ISO /IEC 27018 (norma que despliega controles de privacidad para servicios en la nube)

ISO /IEC 27019 (norma relacionada con los sistemas de control de procesos relacionados con la energía)

ISO/IEC 27701 (norma que desarrolla en paralelo a la ISO 27001, un Sistema de Gestión de Privacidad).

4.1.1. ISO/ IEC 27001:2022

La norma ISO/IEC 27001 es una norma de seguridad de la información internacional, certificable, que puede ser acogida por las organizaciones [públicas y privadas] de manera voluntaria. La norma en sí es flexible y modulable, dado que sus requisitos son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de tipo, tamaño o naturaleza.

El hecho de que la norma ISO, establezca sus” requisitos”[20] supone que el sistema de gestión desarrollado bajo su paraguas es auditable y certificable. Por eso, las entidades de certificación acreditadas, tras un proceso de auditoria sistemático y metódico, podrán considerar la conformidad con la norma.

No olvidemos que la finalidad de la ISO es proporcionar los *requisitos* para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de seguridad de la información, que será el que se someta al proceso de certificación.

Los sistemas de gestión de seguridad de la información desplegados bajo esta norma buscan mantener la confidencialidad, integridad y disponibilidad de la información mediante un proceso de gestión de riesgos.

Para la elaboración de esta guía se ha tenido en cuenta la **ISO/ IEC 27001:2022 “Seguridad de la Información, ciberseguridad y protección de la Privacidad – Sistemas de gestión de la Seguridad de la Información -Requisitos** ”.[21]. Heredera de la ISO /IEC 27001:2013, ha sido revisada en toda su extensión, considerando ciertas adaptaciones y actualizaciones en su conjunto de Clausulas[22] y en el anexo A de controles

[20] En el marco de normas ISO, solo aquellas que consideran requisitos pueden ser certificables. La ISO / IEC 27001:2022 es una norma de requisitos “*Information security, cybersecurity and privacy protection — Information security management systems —**Requirements***”

[21] Considérese la norma UNE-ISO/IEC 27001:2023 “Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos”

[22] Se ha incluido una subcláusula nueva, 6.3 Planificación de cambios.

En relación con las cláusulas, han tenido pequeñas modificaciones, que afectan más a la parte de redacción o separación en subcláusulas, que a cambios significativos.

Si bien es cierto que se han puntualizado aspectos concretos, como la monitorización y seguimiento de los objetivos de seguridad, en general, se mantienen los requisitos del estándar del año 2013, con pequeños cambios.

CLAUSULA		CAMBIOS	
4 Contexto de la organización	4.1 Comprensión de la organización y su contexto	Sin Cambios	
	4.2 Comprensión de las necesidades y expectativas de las partes interesadas	Cambios menores	Se debe actualizar las necesidades y expectativas de las partes interesadas de forma que la organización sea capaz de demostrar que requisitos relevantes van a ser abordados a través del SGSI
	4.3 Determinación del alcance del sistema de gestión de seguridad de la información	Sin Cambios	
	4.4 Información seguridad gestión sistema	Cambios menores	Se centra en sus procesos y como interactúan en el SGSI
5 Liderazgo	5.1 Liderazgo y compromiso	Sin Cambios	
	5.2 Política	Sin Cambios	
	5.3 Funciones, responsabilidades y autoridades de la organización	Sin Cambios	
6 Planificación	6.1 Acciones para tratar los riesgos y oportunidades	Sin Cambios	
		Sin Cambios	Es necesario tener en cuenta que los controles son nuevos por lo que deben tenerse en cuenta y actualizarse.
		Cambios menores	Debe actualizarse la Declaración de Aplicabilidad [SOA] haciendo el cambio de los 114 controles a los 93 que se consideran en la norma versión 2022.
	6.2 Objetivos de seguridad de la Información y planificación para su consecución	Sin Cambios	
	6.3 Planificación de cambios	Nueva	Se ha de incluir un proceso de cambio, que permitirá el control, planificación, aprobación y seguimiento de los cambios asociados al sistema.
7 Soporte	7.1 Recursos	Sin Cambios	
	7.2 Competencia	Sin Cambios	
	7.3 Conciencia	Sin Cambios	
	7.4 Comunicación	Cambios menores	Se debe considerar el plan de comunicaciones como elemento documentado con clara determinación de medios. Se ha eliminado el "quien" y se ha añadido un "como". El responsable ya no requiere estar documentado.

CLAUSULA		CAMBIOS	
			Se elimina e) procesos por los que se debe efectuar la comunicación. Ya no es necesario documentarlos.
	7.5 Información documentada	Sin Cambios	
		Sin Cambios	
		Sin Cambios	
8 Operación	8.1 Planificación y control operacional	Cambios menores	Se da mayor relevancia al control, y especialmente cuando hay terceros implicados.
	8.2 Evaluación de riesgo de seguridad de la información	Sin Cambios	
	8.3 Tratamiento de riesgo de seguridad de la información	Sin Cambios	
9 Evaluación del desempeño	9.1 Seguimiento, medición, análisis y evaluación	Cambios menores	Se ha trabajado la mejora en la redacción.
	9.2 Auditoría Interna	Cambios menores	Se ha separado la cláusula en dos subpuntos con un contenido muy similar. La cláusula ahora dispone de dos subcláusulas.
		Cambios menores	Se ha separado la cláusula en dos subpuntos con un contenido muy similar. La cláusula ahora dispone de dos subcláusulas.
	9.3 Revisión por la dirección	Cambios menores	Se ha separado la cláusula en tres subpuntos con un contenido muy similar. La cláusula ahora dispone de tres subcláusulas.
		Cambios menores	Se ha separado la cláusula en tres subpuntos con un contenido muy similar. La cláusula ahora dispone de tres subcláusulas. Se añade un nuevo punto relacionado con las partes interesadas.
		Cambios menores	Se ha separado la cláusula en tres subpuntos con un contenido muy similar. La cláusula ahora dispone de tres subcláusulas.
10 Mejora	10.1 Mejora continua	Sin Cambios	Se alerta el orden de las cláusulas.
	10.2 No conformidad y acción correctiva	Sin Cambios	Se alerta el orden de las cláusulas.

Tabla. Análisis de cambios realizados en las cláusulas [requisitos] norma 2022. Tras la correspondiente revisión y evolución en su clausulado, la norma sufrió un cambio significativo en la estructura del Anexo A. Así se han reagrupado los objetivos de control de su Anexo A, en cuatro grandes bloques; *controles organizacionales; controles de personas; controles físicos, controles tecnológicos*.

Núm. Controles	Capítulo	Contenido	Observaciones
37	Capítulo 5	Controles organizacionales	Bloque general de seguridad

8	Capítulo 6	Controles de personas	Se refiere a individuos
14	Capítulo 7	Controles de infraestructura	Se refiere a objetos físicos
34	Capítulo 8	Controles de tecnología	Se refiere a tecnología

Tabla. Bloque de controles Anexo A ISO 27001:2022

Además de esta nueva distribución de controles bajo 4 capítulos, el número de controles ha pasado de 113 en su versión 2013 a 93, en su versión 2022. No obstante, esta reducción no supone una merma en la seguridad, sino una reestructuración donde se han incluido controles nuevos, otros han sido fusionados o integrados con otros controles, y algunos han sido modificados, mientras que solo uno de ellos, ha sido eliminado[23].

Como nuevos controles se han considerado:

Nuevo Control			Punto clave
Capítulo 5 Controles organizacionales	5.7	Inteligencia de amenazas	Logs
	5.23	Seguridad de la información para el uso de servicios en la nube	Proveedor Cloud
	5.30	Preparación para las TIC para la continuidad del negocio	Continuidad
Capítulo 7 Controles físicos	7.4	Monitorización de la seguridad física	Monitorización y seguimiento
Capítulo 8 Controles tecnológicos	8.9	Gestión de la configuración	Bastionados
	8.10	Eliminación de la información	Proceso eliminación
	8.11	Enmascaramiento de datos	Enmascaramiento
	8.12	Prevención de fugas de datos	Prevención
	8.16	Seguimiento de actividades	Monitorización
	8.23	Filtrado de Webs	Web
	8.28	Codificación segura	Código

Tabla. Nuevos controles Anexo A ISO 27001:2022

Como se verá más adelante, el nuevo sistema de controles del Anexo A, presenta una mejor comparación de los controles compatibles con el Anexo II del Real Decreto 311/2022, de 3 mayo, dado que ambas normas han tenido muy presente la evolución en ciberseguridad que se requiere para afrontar nuevos riesgos y desafíos.

4.1.2. ISO/IEC 27002

La **ISO/IEC 27002 Seguridad de la Información, ciberseguridad y Protección de la Privacidad — Control de la seguridad de la Información** no es una norma de requisitos por tanto no es certificable. Sin embargo, esta norma es un código de buenas prácticas para la gestión de la seguridad de la información y que, sin duda, resulta de gran ayuda para desplegar sistemas de gestión de seguridad de la información.

[23] A.11.2.5 Retirada de activos (materiales propiedad de la empresa)

Su finalidad es servir como guía de orientación para desplegar los controles contenidos en el Anexo A de la ISO 27001. También puede usarse como un documento de orientación e implementación de los controles de seguridad de la información comúnmente aceptados,

En la norma se incluye un Anexo A, [24] en el que se presentan cinco bloques de características, con diferentes atributos que se han asignado a cada uno de los 93 controles del Anexo A de la ISO 27001:2022.

Estos atributos deben servir para diferenciar y separar los controles, en base a sus usos y fines prioritarios. Permite búsquedas concretas y trazar los controles con sus finalidades, puntos clave o dimensiones asociadas.

Cada control se asocia con todos aquellos atributos que le corresponden y/o describen:

a) Tipo de Control El tipo de control es un atributo para ver los controles desde la perspectiva de cuándo y cómo el control modifica el riesgo con respecto a la ocurrencia de un incidente de seguridad de la información. Los valores del atributo consisten en Preventivo (el control que pretende evitar la ocurrencia de un incidente de seguridad de la información), Detectivo (el control actúa cuando se produce un incidente de seguridad de la información) y Correctivo (el control actúa después de que se produzca un incidente de seguridad de la información)

b) Propiedades o dimensiones de seguridad [25]

Las dimensiones de seguridad de la información son un atributo para ver los controles desde la perspectiva de que características de la información contribuirá a preservar. Los valores del atributo son Confidencialidad, Integridad y Disponibilidad.

c)Ciberseguridad

Los conceptos de ciberseguridad son un atributo para ver los controles desde la perspectiva de la asociación de controles a conceptos de la ciberseguridad definidos en el marco de la ciberseguridad descrito en la Norma ISO/IEC TS 27110. Los valores del atributo consisten en Identificar, Proteger, Detectar, Responder y Recuperar

d)Capacidades operativas

Las capacidades operativas son un atributo para ver los controles desde la perspectiva del profesional de las capacidades de seguridad de la información. Los valores del atributo consisten en Gobernanza, Gestión de activos, Protección de la Información, Seguridad de los recursos humanos, Seguridad física, Seguridad de los sistemas y de las redes, Seguridad de las aplicaciones, Configuración segura, Gestión de la identidad y del acceso, Gestión de las amenazas y de la vulnerabilidad, Continuidad, Seguridad de las relaciones con los proveedores, Legalidad y Cumplimiento normativo, Gestión de eventos de seguridad de la información y Garantía de seguridad de la información.

e) Dominios de seguridad

[24] Table A.1 — Matrix of controls and attribute values

[25] Este bloque se puede asimilar a los del Esquema Nacional de Seguridad que también detalla la(s) dimensión(es) en las que se desenvuelve un control de seguridad. No obstante, debe considerarse que, para esta norma, hay 5 dimensiones frente a las tres dimensiones clásicas de seguridad que considera la ISO 27001.

Dominios de seguridad es un atributo para ver los controles desde la perspectiva de cuatro dominios de seguridad de la información: "Gobernanza y ecosistema" incluye "Gobernanza de la seguridad de los sistemas de información y gestión de riesgos" y "Gestión de la ciberseguridad del ecosistema" (incluidas las partes interesadas interna y externas); "Protección" incluye "Arquitectura de la seguridad informática", "Administración de la seguridad informática", "Gestión de la identidad y el acceso", "Mantenimiento de la seguridad informativa" y "Seguridad física y del entorno"; "Defensa" incluye "Detección" y "Gestión de incidentes de seguridad informática"; "Resiliencia" incluye "Continuidad de las operaciones" y "Gestión de crisis". Los valores de los atributos consisten en "Gobernanza y ecosistema", "Protección", "Defensa" y "Resiliencia".

4.2 DIFERENCIAS ENTRE ISO 27001 Y ENS

Ya se ha puesto de manifiesto la buena sinergia y reciprocidad entre el Esquema Nacional de Seguridad [Real Decreto 311/2022 de 3 de mayo] y la ISO/IEC 27001:2022, y la posibilidad de desplegar sistemas de gestión, considerando lo establecido por ambos marcos. Pero también hay que canalizar las particularidades y diferencias existentes entre ambos sin las cuales, no se podrá optar a mantener un sistema capaz de afrontar la conformidad de ambos.

A nivel nacional, no podemos obviar que conforme al artículo 2 del Real Decreto 311/2022, las entidades sometidas al cumplimiento del Esquema Nacional de Seguridad[26], deben desplegar sistemas de gestión conforme a la misma. No obstante, estos sistemas pueden contemplar los requisitos complementarios contenidos en la ISO, y superar con solvencia sus requisitos.

A nivel global, podemos analizar ambos marcos y extraer las siguientes conclusiones:

	ISO/IEC 27001	**Esquema Nacional de Seguridad (RD 311/2022)**
Autoridad responsable	International Organization of Standardization.(ISO)	Centro Criptológico Nacional (CCN)[27]
Naturaleza	Estándar de seguridad internacional de seguridad	Marco[legal] estatal, derivado de la Ley 40/2015.
Carácter	Adhesión voluntaria	Sujetos sometidos obligatoriamente
Ámbito de aplicación	Sistema de gestión de seguridad de la información de cualquier organización.	Sistemas de información sector público. Sistemas de información sector privado (*)
Función	Confiabilidad ante terceros, evidenciando procesos para la seguridad de la información.	Requisito legal para impulsar la protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación
Modulación de las medidas	Según contexto, partes interesadas y organización, conforme al análisis de riesgos.	A criterio del Responsable de Seguridad, conforme a los riesgos, estado de la tecnología y servicios / información. Determinadas entidades o sectores de actividad concretos podrán implementar perfiles de cumplimiento específicos[28], con modulación de las medidas de seguridad.

[26] Todo el sector público, en los términos en que este se define por el artículo 2 de la Ley 40/2015, de 1 de octubre, y de acuerdo con lo previsto en el artículo 156.2 de la misma, así como entidades del sector privado presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.
[27] Adscrito al Centro Nacional de Inteligencia. -Ministerio de Defensa
[28] Ver artículo 30 del Real Decreto 311/2022, de 3 de mayo.

Dimensiones	Considera las tres dimensiones clásicas de seguridad: Disponibilidad, Integridad y Confidencialidad	Considera cinco dimensiones de seguridad. Disponibilidad, Integridad, Confidencialidad, Trazabilidad y Autenticidad.
Sistema de fuentes	Mínimo Anexo A de la ISO N.º total de controles: 93	Mínimo Anexo II del Real Decreto N.º total de controles: 73
Gestión de riesgos	Se puede emplear cualquier metodología, pero se orienta hacia la metodología de la ISO 31000. Referencias en la ISO/IEC 27005.	Se puede emplear cualquier metodología, pero se orienta hacia MAGERIT[29].
Evidencia de cumplimiento o conformidad	Mediante certificación, expedida por entidad de certificación acreditada, previa auditoría con resultado satisfactorio.	Mediante declaración de conformidad legal, expedida por entidad de certificación acreditada, previa auditoría con resultado satisfactorio.
Ciclo de vigencia	Ciclo de 3 años, sometido a un proceso de revisiones o seguimientos anuales, interno y externo.	Ciclo de 2 años, sometido a un proceso de revisiones o seguimiento anual interno.
Referencias	Cualquier marco de seguridad puede ser un marco de referencia.	Existen Instrucciones, Abstract, Guías[30], y Buenas Prácticas. Cualquier marco de seguridad puede aportar mejoras al sistema.
Certificación	Por medio de entidades acreditadas.	Por medio de entidades acreditadas. [31]

Tabla. Resumen de las características de ambas normas

Aunque como puede observarse, ambas normas tienen diferencias, las dos comparten su objetivo clave; la gestión de los riesgos asociados a la [ciber]seguridad y considerando no solo a la propia organización propietaria del sistema, sino que extienden sus requisitos a proveedores y cadenas de suministro, incluidos aquellos que participan en los servicios cloud, tan habituales en nuestro entorno actual.

El despliegue de un sistema de gestión, bajo las directrices de sendas normas, permitirá generar confianza frente a terceros, mejorar de manera muy significativa la seguridad y resiliencia del sistema y mantendrá el reconocimiento de los servicios y productos que se encuentren incluidos bajo el alcance de estas.

Por último, es conveniente recordar que a nivel internacional la ISO puede servir como vehículo "unificador" de requisitos de seguridad, funcionando como un "traductor" de normas o estándares de seguridad. Así se refleja, por ejemplo, en los requerimientos impuestos en la PAC [Política Agraria Común], o en las normas asociadas al sector financiero, donde es habitual hacer equivalencias entre la ISO/IEC 27001 y las propias directrices de las autoridades.

Por ello, trabajar con unas medidas de seguridad compatibles del Esquema Nacional de Seguridad y la ISO 27001, puede ser enriquecedor y servir para evidenciar los requisitos impuestos de manera uniforme y bajo un "lenguaje" común.

[29] Metodología desarrollada por Consejo Superior de Administración Electrónica y actualmente mantenida por la Secretaría General de Administración Digital (Ministerio de Asuntos Económicos y Transformación Digital) y CCN. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

[30] Disposición adicional segunda.
(…) Las instrucciones técnicas de seguridad tendrán en cuenta las normas armonizadas por la Unión Europea aplicables.
Para el mejor cumplimiento de lo establecido en este real decreto, el CCN, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC), particularmente de la serie 800, que se incorporarán al conjunto documental utilizado para la realización de las auditorías de seguridad.

[31] https://ens.ccn.cni.es/es/certificacion/entidades-de-certificacion

5. CUMPLIMIENTO DEL ENS A TRAVÉS DE UNA CERTIFICACIÓN 27001

Un Sistema de Gestión de Seguridad de la Información, es un conjunto de políticas, procedimientos y directrices, que se establecen en una organización, junto con los recursos y procesos necesarios para proteger los activos y especialmente, el activo información. Y esto es precisamente el objetivo del Esquema Nacional de Seguridad, que busca aumentar la seguridad de los servicios y la información, en el entorno público, de manera organizada y en la que se puedan conjugar principios básicos y requisitos mínimos, con las medidas tecnológicas y la necesaria gobernanza de la seguridad.

Establecer y mantener un sistema de gestión es una decisión estratégica que beneficia sin duda a las entidades. Seleccionar el estándar o marco apropiado dependerá de la normativa aplicable y en muchas ocasiones de las necesidades de la organización, de sus objetivos, de los procesos internos y el tamaño y estructura de esta.

El Esquema Nacional de Seguridad es un marco [legal] que se adapta al medio, y que ha considerado los puntos clave de la [ciber]seguridad, y que permite alinearse con otros marcos de seguridad, y entre ellos la ISO 27001. Hay que considerar, no obstante, ciertas diferencias entre ambos, que obligarán a hacer adaptaciones en el sistema de gestión de la organización.

Si una entidad desarrolla los procesos requeridos por las normas, logrará beneficiarse de las ventajas de disponer de un Sistema de Gestión de Seguridad de la Información bajo los requerimientos legales, completo, capaz de evidenciar seguridad, y que fomenta las capacidades de detección, reacción, recuperación y aprendizaje frente a incidentes y eventos de seguridad.

Una de las ventajas que aporta el marco [legal] del Esquema Nacional de Seguridad, son los esfuerzos desarrollados por la Autoridad de Control garante del mismo [CCN]. Si bien es cierto que ISO tiende a publicar diferentes normas de apoyo, como la ISO/IEC 27002, es necesario un análisis más detallado y rápido, capaz de adaptarse a las necesidades del momento, como se desarrolla en el ámbito del Esquema Nacional de Seguridad. Y es precisamente el interés por mejorar la promoción y desarrollo de la seguridad, que se mantiene un trabajo constante con la constante publicación de Abstract, Informes, Buenas Prácticas, Guías[32] de cumplimiento y soluciones de ciberseguridad[33], que permiten gestionar puntos clave, tales como vigilancia tecnológica, trazabilidad del dato o visibilidad de la red, de manera más ágil y rápida que el estándar ISO.

Otra mejora que podrá obtenerse al integrar los requerimientos del Esquema Nacional de Seguridad es la consideración de las cinco dimensiones de seguridad, lo que permite desplegar controles enfocados en las dos dimensiones no consideradas inicialmente por la ISO.

A nivel general, cuando una entidad se encuentra incluida en el ámbito de aplicación del Esquema Nacional de Seguridad, debe desplegarse esta debe incluir en el sistema de gestión las condiciones establecidas en el mismo. No obsta a que en el mismo se integren el resto de los puntos que la norma ISO establece y que permiten un enriquecimiento de la seguridad.

---

[32] Disposición adicional segunda. Desarrollo del Esquema Nacional de Seguridad.
"(…)
Para el mejor cumplimiento de lo establecido en este real decreto, el CCN, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC), particularmente de la serie 800, que se incorporarán al conjunto documental utilizado para la realización de las auditorías de seguridad."

[33] https://www.ccn-cert.cni.es/soluciones-seguridad.html

Trabajando sobre la base de una estrategia en la que el sistema de gestión integre los puntos comunes de ambos marcos y a su vez, considere aquellos en los que habiendo diferencias pueden ser incluidos sin obstaculizar la seguridad, podemos desplegar un Sistema de Gestión de Seguridad de la Información que soporte ambas normas. Para ello deberemos considerar:

A) Trabajar con las cinco dimensiones de seguridad. Se deben incluir dos dimensiones más que las tres clásicas contempladas por la ISO. Esto no supone un problema de seguridad, sino que puede enriquecer el proceso de atributos que el Anexo A de la ISO/IEC 27002 ha incluido en su versión 2022.
B) Analizar el alcance de cada norma y describir documentalmente cada uno de ellos. Una buena estrategia será, intentar unificar los alcances cuando sea posible, para que el sistema pueda abarcar de manera integral ambos.
C) Unificar las declaraciones de aplicabilidad, incluyendo y describiendo todos los controles aplicados, y motivando las excepciones. Las normas en su versión 2022, han evolucionado y permiten una buena compatibilidad de las medidas de seguridad.
D) Desarrollar una metodología de riesgos única, que permita cubrir la gestión de estos y realizar el seguimiento pertinente. Ambas normas son permisivas en cuanto a la metodología de riesgos, por lo que la entidad deberá adoptar aquella que encaje mejor en su sistema y con sus activos.
E) Integrar los roles de seguridad y las revisiones de dirección. Para incluir los requisitos de ambas normas, se puede establecer un informe anual de revisión [por la dirección], supeditado a su presentación al Comité de Seguridad de la Información, con el contenido requerido por la ISO y que además contemple aquellos aspectos que el Esquema Nacional de Seguridad establece.
F) Considerar un sistema de gestión integrado, que incluya todos los procesos necesarios, con los registros y las evidencias documentales que ambas normas exigen.
G) Analizar la eficacia y eficiencia del sistema de gestión, empleando métricas e indicadores que permitan satisfacer los requisitos de análisis y monitorización de ambos marcos. A nivel de la ISO será necesario considerar los objetivos de seguridad de la organización y a nivel del Esquema, deberá tenerse en cuenta los indicadores clave requeridos[34].
H) Establecer un proceso de revisión, que incluya auditorias anuales con los requisitos de ambas normas. En el proceso se incluirán las revisiones periódicas de seguridad que se deben realizar.
I) Superar los procesos de certificación[35], teniendo en cuenta el esquema de certificación diferenciado de cada una de las dos normas, incluyendo los correspondientes seguimientos, bajo el ciclo completo que cada norma exige. .

Una de las particularidades que tiene la ISO, es que solo la ISO /IEC 27001 es certificable al ser la norma que incluye los requisitos. No obstante, la entidad puede considerar no lanzarse a la certificación de la misma o desplegar la ISO/IEC 27002, y enriquecer el sistema gracias a los

[34] Artículo 32. Informe del estado de la seguridad.
[35] 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, 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"

aportes de seguridad que otorgan. En todo caso, la organización debería realizar un análisis coste beneficio y adoptar la decisión más adecuada a sus necesidades.

5.1. ESTRATEGIA DE DESPLIEGUE DE ENS CON ADAPTACIONES

El Esquema Nacional de Seguridad, es un marco [legal], fruto de la regulación nacional que es de obligado cumplimiento para el sector público y sistemas de información de las entidades del sector privado cuando presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas, conforme al ordenamiento jurídico.[36]

El ENS requiere un proceso de categorización (Anexo I) y el despliegue de una serie mínima de medidas de seguridad (Anexo II) en base a la misma. El Real Decreto 311/2002 de 3 de mayo, ha introducido novedades en relación con la aplicabilidad de las medidas de seguridad contenidas en el Anexo II, desde la posibilidad dada por el artículo 30 relacionada con la publicación de perfiles de cumplimiento especifico, a refuerzos obligatorios u opcionales diferenciados por el nivel y categoría declarada.

A nivel general, las dos normas [ISO/IEC 27001:2022 y Real Decreto 311/2022], tienen un buen Nivel Compatible, habiendo seguido una evolución muy similar en relación a nuevos riesgos, considerando el entorno cloud y la posible dependencia de proveedores.

Por eso, para lograr un sistema integrado con ambas normas, se debe partir de la **categoría MEDIA del ENS, con una modulación concreta** basada en:

A) Aplicación de algunos controles de categoría ALTA para despliegue mejorado del proceso de cambios y continuidad de negocio.
B) Aplicación de controles de categoría MEDIA en toda su extensión, aun no siendo previstos por la ISO 27001:2022.

Es importante que se mantenga como estrategia, el cumplimiento del ENS bajo el alcance dado por la Ley 40/2015, tanto desde el punto de vista de los activos esenciales (Anexo I) como de los componentes implicados[37]. Por ello el alcance debe estar alineado con el cumplimiento legal.

Además, hay que destacar que el Anexo II modula los requisitos en función de la categorización del sistema, mientras que en la ISO/IEC 27001 el nivel de exigencia queda limitado al alcance seleccionado y motivación de la entidad. Por ello será necesario considerar el principio de proporcionalidad consagrado por el ENS, y desplegar los controles que, bajo la aplicación de este, sean necesarios.

A continuación, se presenta un mapa inicial de requisitos compatibles, que pretende ayudar a desplegar un sistema integrado para ambos marcos.

Hay que tener en cuenta que la estructuración de las medidas no es la misma en el ENS que en las normas 27001 y 27002. Algunos aspectos están contemplados parcialmente en algún control,

[36] Considerar las disposiciones derivadas de la Ley 40/2015.
[37] Nótese que una certificación 27001 tiene el alcance que la organización decida. Basta que quede claramente delimitado qué parte del sistema de gestión está siendo certificado.

y en la mayoría de los casos, los controles del ENS requieren de varios controles de la ISO 27001, para cumplirlos en toda su magnitud.

Aunque ya se ha mencionado, es importante tener presente que ni el Esquema Nacional de Seguridad ni la ISO/IEC 27001:2022, tienen como objetivo la continuidad de negocio, sino que esta forma parte del bloque de medidas de seguridad que se "pueden llegar" a desplegar. No obstante ISO ha trabajado un conjunto de normas de continuidad, que recogen los requisitos de un Sistema de Gestión de Continuidad de Negocio[38].

5.2. CUADRO RESUMEN

Se ha realizado un análisis de medidas global de ambos marcos, tanto de su parte general (articulado del Esquema Nacional de Seguridad y Anexo L de la ISO) como de las medidas o controles del Anexo A de la ISO 27001:2022 y del Anexo II Real Decreto 311/2022, de 3 de mayo.

Debe recordarse que la ISO/IEC 27001 es maleable[39], mientras que el ENS requiere el cumplimiento exigido para las dimensiones y categorías que corresponda, por lo que deberá verificarse siempre, este extremo. 5.2.2. Análisis de requisitos compatibles parte general:

A continuación, se muestra un detalle de la comparativa y análisis de las cláusulas de la ISO/IEC 27001:2022 y el Real Decreto 311/2022 de 3 de mayo, que debe considerarse para poder incluir en el sistema de gestión, los requerimientos dados.

CLAUSULA		Artículo / Medida ENS	Análisis de requisitos compatibles y diferencias.
4 Contexto de la organización	4.1 Comprensión de la organización y su contexto	**Real Decreto 311/2022** INTRODUCCIÓN Artículo 30 Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras Artículo 40 Categorías de seguridad **Anexo I** **Anexo II** o [org.1] Política de seguridad	Para la ISO, las organizaciones determinen los aspectos externos e internos que son relevantes para su propósito y que condicionan el logro de los resultados previstos de su SGSI. Algunas de estas cuestiones pueden ser la situación política y económica, la regulación existente, el estado de la tecnología, las relaciones con los ciudadanos y con los proveedores, las funciones de cara área o departamento afectado por el SGSI, la misión, visión y funciones de la organización, y en general, cualquier factor que tenga impacto sobre sus objetivos y funcionamiento. El actual ENS ha considerado las particularidades de las entidades públicas y ha considerado en su Artículo 30, los Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras. De tal forma 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 idóneas para una concreta categoría de seguridad. Para el ENS al valorarse en la fase de categorización de los sistemas estos posibles perjuicios, las organizaciones están realizando un ejercicio de comprensión de su contexto. Esta categorización es obligatoria para todos los sistemas de información dentro del alcance del ENS. No obstante, la organización debe revisar si dispone de una estrategia donde se analicen de forma periódica las cuestiones internas y externas relevantes para el SGSI, con el fin de cumplir su misión y objetivos y lograr una mayor alineación con la norma ISO 27001.
	4.2 Comprensión de las necesidades y expectativas de las partes interesadas	**Real Decreto 311/2022** INTRODUCCIÓN Artículo 30 Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras Artículo 40 Categorías de seguridad Anexo I	Para la ISO, requiere que se determinen los requisitos de las partes interesadas (ciudadanos, proveedores, personal, otras administraciones públicas, etc.) que son relevantes para la seguridad de la información: requisitos legales y regulatorios, obligaciones contractuales, etc. La organización debe considerar las partes relevantes y los requisitos asociados a la seguridad. Esto a su vez encuentra su correspondencia en el ámbito del ENS en su introducción y en los artículos referenciados, enfocando las principales partes interesadas; entidades del sector público y sector privado, derechos y libertades y el bienestar de los ciudadanos y para garantizar el suministro de los servicios y recursos esenciales. La organización debe revisar si dispone de un listado de partes interesadas internas y externas relevantes para el SGSI y de aquellas que dependen de su correcta operación y de manera muy significativa cuando analiza impactos y dependencias.

[38] ISO/IEC 27031, ISO 22313 e ISO 22301

[39] Limitado al alcance seleccionado y a la motivación de la entidad

CLAUSULA				Artículo / Medida ENS	Análisis de requisitos compatibles y diferencias.
	4.3 Determinación del alcance del sistema de gestión de seguridad de la información			**Ley 40/2015:** o Artículo 2 o Artículo 156 **Real Decreto 311/2022:** Artículo 1 Objeto Artículo 2 Ámbito de aplicación	La norma ISO permite acotar los alcances, según las necesidades de la organización y los objetivos que defina. En todo caso constara documentado. En el ENS, el alcance está acotado a los medios electrónicos utilizados y gestionados por a todo el sector público, para la prestación de servicios a los ciudadanos en el ejercicio de sus competencias y en su relación con otras Administraciones Públicas, todo ello en el ámbito de la Ley 40/2015, a los sistemas de información de las entidades del sector privado, de acuerdo con la normativa aplicable y en virtud de una relación contractual, cuando presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.
	4.4 Sistema de gestión de seguridad de la información			**Real Decreto 311/2022** Artículo 6 La seguridad como un proceso integral **Anexo II** [org.1] Política de seguridad [op.pl.2] Arquitectura de seguridad - *Refuerzo R1-Sistema de gestión. Refuerzo R2-Sistema de gestión de la seguridad con mejora continua.* [op.ext.3]. protección de la cadena de suministro Refuerzo R2-Sistema de gestión de la seguridad. [op.mon.2] - *Refuerzo R2-Eficiencia del sistema de gestión de la seguridad.* **Anexo III** Auditoría de la seguridad	Para la ISO, la organización debe establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información. Para el ENS, la seguridad es entendida como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información (artículo 5) y por ello deberá acreditarse la existencia de un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección, tomando como base la Declaración de Aplicabilidad regulada en el artículo 28, mediante procesos de auditoría.
5 Liderazgo	5.1 Liderazgo y compromiso			**Real Decreto 311/2022** Artículo 11 Diferenciación de responsabilidades Artículo 13 Organización e implantación del proceso de seguridad **Anexo II** [org.1] Política de seguridad	Para la ISO, la alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información, mediante una serie de elementos, tales como dotar de recursos al sistema, aprobar una política de seguridad, promoviendo la mejora continua... Para el ENS, la seguridad de los sistemas de información deberá comprometer a todos los miembros de la organización (artículo 13), conforme a los diferentes roles (artículo 11)
	5.2 Política			**Real Decreto 311/2022** Artículo 11 Diferenciación de responsabilidades Artículo 12 Política de seguridad y requisitos mínimos de seguridad Artículo 13 Organización e implantación del proceso de seguridad **Anexo II** [org.1] Política de seguridad	Para la ISO, la dirección debe establecer una política de seguridad de la información, la cual debe estar disponible como información documentada, comunicada y accesible. Para el ENS, debe desarrollarse y aprobarse una política de seguridad que considerará el contenido trazado (especialmente por artículo 11 y por el control del Anexo II [org.1]) y que articulará la gestión continuada de la seguridad, y será aprobada por el titular del órgano superior correspondiente.
	5.3 Roles, responsabilidades y autoridades de la organización			**Real Decreto 311/2022** Artículo 11 Diferenciación de responsabilidades **Anexo II** [org.1] Política de seguridad	Para la ISO, la dirección debe asegurarse de que las responsabilidades para los roles de seguridad de la información se asignen y comuniquen dentro de la organización. Para el ENS, se establecen roles diferenciados que son detallados en la Política de Seguridad, definiendo para cada uno, los deberes y responsabilidades de cada rol, así como el procedimiento para su designación y renovación y los mecanismos de coordinación y resolución de conflictos.
6 Planificación	6.1 Acciones para tratar los riesgos y oportunidades	6.1.1	Consideraciones generales	**Real Decreto 311/2022** Artículo 7 Gestión de la seguridad basada en los riesgos Artículo 8 Prevención, detección, respuesta y conservación Artículo 14 Análisis y gestión de los riesgos **Anexo II** [op.pl.1] Análisis de riesgos	Para la ISO, debe existir una planificación para gestionar los riesgos y oportunidades, prevenir y reducir impactos y lograr una mejora continua. Para el ENS, la planificación, gestión de riesgos, acciones preventivas y reactivas, así como la mejora continua está desplegada en varios artículos y controles, por cuanto se detalla en mayor medida

CLAUSULA				Artículo / Medida ENS	Análisis de requisitos compatibles y diferencias.
		6.1.2	Apreciación de riesgos de seguridad de la información	**Real Decreto 311/2022** Artículo 7 Gestión de la seguridad basada en los riesgos Artículo 8 Prevención, detección, respuesta y conservación Artículo 14 Análisis y gestión de los riesgos **Anexo II** [op.pl.1] Análisis de riesgos	Para la ISO, la organización debe definir y aplicar un proceso documentado de apreciación de riesgos de seguridad de la información, definiendo los criterios del proceso, una sistemática objetiva, determine los riesgos (analice y evalúa) y los propietarios de estos, y gestione un plan de tratamiento . Para el ENS, el mandato es claro y deriva en un proceso global del proceso de seguridad, de manera que el análisis y la gestión de los riesgos es parte esencial de la seguridad, debiendo constituir una actividad continua y permanentemente actualizada. Cada organización que desarrolle e implante sistemas para el tratamiento de la información o la prestación de servicios realizará su propia gestión de riesgo.
		6.1.3	Tratamiento de los riesgos de seguridad de la información	**Real Decreto 311/2022** Artículo 7 Gestión de la seguridad basada en los riesgos Artículo 14 Análisis y gestión de los riesgos Artículo 28 Cumplimiento de los requisitos mínimos Artículo 30 Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones segura **Anexo II** apartado 2.1.3 [op.pl.1] Análisis de riesgos	Para la ISO, La organización debe definir y efectuar un proceso de tratamiento de los riesgos de seguridad de la información, que será documentado. La organización debe elaborar una "Declaración de Aplicabilidad" que contendrá, los controles necesarios, la justificación de las inclusiones, si los controles necesarios están implementados o no; y la justificación de las exclusiones de cualquiera de los controles del anexo A de la ISO. Para el ENS, Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos. Para ENS la criticidad de la declaración de los controles del Anexo II, se establece en el artículo 28, al establecer que la relación de medidas de seguridad seleccionadas se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de la seguridad. Debe tenerse en cuenta que para el ENS puede desplegarse modulaciones de las medidas de seguridad, mediante perfiles de cumplimiento, por cuanto se podrán establecer perfiles de cumplimiento específicos, según el artículo 30, 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.
	6.2 Objetivos de seguridad de la Información y planificación para su consecución			**Real Decreto 311/2022** Artículo 2 Objeto Artículo 5 Principios básicos del Esquema Nacional de Seguridad **Anexo II** [org.1] Política de seguridad	Para la ISO, La organización debe establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes, que serán coherentes, medibles, alineados con la seguridad y los riesgos, actualizados y comunicados. Para el ENS, los objetivos están integrados en el propio mandato del legislador y específicamente desplegar los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, 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 utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias. A su vez, el control [org.1] establece que la política de seguridad debe precisar los objetivos o misión de la organización. No obstante, no se especifica que los objetivos de seguridad de la información deben estar documentados, ni ser medibles, comunicados y actualizados a intervalos periódicos. Por tanto, las organizaciones deben disponer de información documentada sobre los objetivos de seguridad de la información, derivados de los objetivos de la organización, y soportados por controles y métricas de seguridad, así como cumplir con en el resto de los aspectos indicados en este requisito de ISO 27001.
	6.3 Planificación de cambios			**Real Decreto 311/2022** Artículo 21. Integridad y actualización del sistema Artículo 27. Mejora continua del proceso de seguridad. **Anexo II** [op.exp.5] Gestión de Cambios	Para la ISO hasta la versión 2022, cambios era un control contenido en el objetivo de control A.12 Seguridad de las operaciones [A.12.1.2. Gestión de Cambios]. Ahora pasa a formar parte del bloque de cláusulas que el sistema debe considerar, y debe considerarse a nivel global para el sistema de gestión de seguridad de la información, por lo que los cambios serán planificados. Para el ENS, cambios se mantiene en su versión 2022, como control de explotación [op.exp.5], considerando no solo la planificación, sino el registro, análisis de riesgos, aprobación, pruebas, actualizaciones del sistema y en su caso, posible marcha atrás.
7 Soporte	7.1 Recursos			**Real Decreto 311/2022** Artículo 6 La seguridad como un proceso integral Artículo 13 Organización e implantación del proceso de seguridad **Anexo II** [op.pl.2] Arquitectura de seguridad [op.mon.2] Sistema de métricas [op.pl.4] Dimensionamiento /gestión de la capacidad	Para la ISO, estipula que las organizaciones deben determinar y proporcionar los recursos necesarios (de personal y económicos, generalmente) para el SGSI. Para el ENS, a lo largo de su articulado recoge referencias a los recursos que pueden ser necesarios para el despliegue de la seguridad en el sistema, como se puede observar por ejemplo en el artículo 13. También se pueden observar las referencias en Refuerzo R1. [op.pl.2.r1.1] Sistema de gestión, relativo a la planificación, organización y control de los recursos relativos a la seguridad de la información, o [op.exp.7.r2.2] Asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente. En general el sistema desplegado por ENS requiere que se detalle el sistema de gestión, relativo a la planificación, organización y control de los recursos relativos a la seguridad de la información y de manera muy clara, en [op.pl.4] Dimensionamiento/gestión de la capacidad. En base a ello es necesario considerar una previsión de los recursos necesarios para dar correspondencia a las dos normas y asociados a

CLAUSULA				Artículo / Medida ENS	Análisis de requisitos compatibles y diferencias.
					mediciones o monitorizaciones que permitan comprobar su eficacia, tal y como se plantea Refuerzo R1 – Efectividad del sistema de gestión de incidentes [op.mon.2.r1.1] y Refuerzo R2 – Eficiencia del sistema de gestión de la seguridad [op.mon.2.r2.1].
	7.2 Competencia			**Real Decreto 311/2022** Artículo 15 Gestión de personal Artículo 16 Profesionalidad **Anexo II** [mp.per.4] Formación	Para la ISO, las organizaciones deben asegurar que las personas que realizan trabajos que afectan a su desempeño en seguridad de la información sean competentes, basándose en la educación, formación o experiencia adecuadas. Para el ENS, este requisito está presente y forma parte del articulado, en su parte inicial "profesionalidad" como en su evolución desde el punto de vista de formaciones periódicas y específicas, especialmente en perfiles críticos para funciones de seguridad. Cabe destacar que la cualificación del personal no solamente se exige a nivel interno, sino también al personal de los proveedores que prestan servicios de seguridad a la organización. Específicamente el ENS considera en el control [mp.per.4] formaciones concretas a personas y funciones críticas, pero además se despliegan más requisitos de formación en otros controles. Además, se evaluará la eficacia de las acciones formativas llevadas a cabo. Por ejemplo, se recoge en [op.pl.3.3] Contemplará las necesidades técnicas, de formación y de financiación, de forma conjunta, [op.cont.2.4] Las personas afectadas por el plan recibirán formación específica relativa a su papel en dicho plan, [mp.per.1.2], ...
	7.3 Conciencia			**Real Decreto 311/2022** Artículo 6 La seguridad como un proceso integral **Anexo II** [mp.per.3] Concienciación	Para la ISO, indica que las personas deben ser conscientes de la política de seguridad de la información, de su contribución a la eficacia del SGSI, así como a las implicaciones de no cumplir con los requisitos del SGSI. Para el ENS, la concienciación es un principio básico de seguridad. *Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y la de los responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y de coordinación o de instrucciones adecuadas, constituyan fuentes de riesgo para la seguridad. Asimismo, la medida de seguridad [mp.per.3] requiere de nuevo la realización de acciones periódicas de concienciación, en particular sobre la normativa de seguridad y sobre la identificación y reporte de incidentes de seguridad.*
	7.4 Comunicación			**Real Decreto 311/2022** Artículo 25 Incidentes de seguridad **Anexo II** [org.1] Política de seguridad [org.2] Normativa de seguridad [op.exp.7] Gestión de incidentes [op.cont.2] Plan de continuidad	Para la ISO, las organizaciones deben determinar la necesidad de realizar las comunicaciones internas y externas relacionadas con el SGSI. Para el ENS, las comunicaciones están asociadas a puntos de control del sistema, empezando por la propia política, comunicaciones a usuarios y partes interesadas, normativa, procedimientos.... y terminando por el punto de contacto asociado a incidentes o contingencia. Esto asegura que el sistema se concentre en las comunicaciones claves. Por ello, ambas normas deben alinearse y será preciso disponer de un árbol de comunicaciones asociado a cada punto requerido de la norma ENS y que es plenamente integrable en la ISO, así como mantener las evidencias necesarias sobre las comunicaciones efectuadas relativas al SGSI.
	7.5 Información documentada	7.5.1	Consideraciones generales	**Real Decreto 311/2022** Artículo 12 Política de seguridad y requisitos mínimos de seguridad Artículo 28 Cumplimiento de los requisitos mínimos **Anexo II** [org.1] Política de seguridad [org.2] Normativa de seguridad [org.3] Procedimientos de seguridad [op.pl.2] Arquitectura de seguridad	Para la ISO, debe incluir la información documentada requerida por la norma, y aquella que se determine necesaria para la eficacia de dicho SGSI. También debe existir un control sobre dicha documentación. Para el ENS, gestionar las evidencias y desplegar el sistema de manera documental es importante y se refleja en varios puntos. Por ejemplo, el propio articulo 12 o la política [org.1] declara que se incluyen las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso o el artículo 28 cuando referencia las medidas a documental. La documentación requerida por arquitectura de seguridad [op.pl.2], la documentación de seguridad asociada a [op.acc], documentos de configuración [op.exp.2], interconexiones de sistemas [op.ext.4]... Sin embargo, no especifica claramente el control del proceso global de información documental por cuanto debería seguirse las pautas de la norma ISO para ambos sistemas.
		7.5.2	Creación y actualización	**Real Decreto 311/2022** Artículo 12 Política de seguridad y requisitos mínimos de seguridad Artículo 28 Cumplimiento de los requisitos mínimos **Anexo II** [org.1] Política de seguridad [org.2] Normativa de seguridad [org.3] Procedimientos de	Para la ISO, es más restrictivo el proceso de creación y control de documentos, así establece puntos asociados al formato y descripción. No obstante, comparte con ENS la aprobación. Para el ENS, la información asociada a seguridad considera puntos precisos de creación y aprobación, dispersos a lo largo del articulado y de los controles, como puede ser [org.1] u [org.4].

CLAUSULA				Artículo / Medida ENS	Análisis de requisitos compatibles y diferencias.
				seguridad [op.pl.2] Arquitectura de seguridad	
		7.5.3	Control de la información documentada	**Real Decreto 311/2022** Artículo 12 Política de seguridad y requisitos mínimos de seguridad Artículo 28 Cumplimiento de los requisitos mínimos **Anexo II** [org.3] Procedimientos de seguridad [op.pl.2] Arquitectura de seguridad	Para la ISO, la información del sistema estará controlada y protegida. No obstante, para el ENS, esta preocupación es compartida y así se puede observar el control [org.3] de manera directa, al referir puntos asociados los accesos, almacenamiento, realización de copias, etiquetado de soportes, transmisión telemática, ...
8 operación	8.1 Planificación y control operacional			**Real Decreto 311/2022** Artículo 6 Artículo 7 Artículo 8 Artículo 37 **Anexo II** [op.pl.1] Análisis de riesgos [op.pl.2] Arquitectura de seguridad	Para la ISO, requiere a nivel general que se disponga de información de control sobre el SGSI en grado suficiente para poder asegurar que los procesos se llevan a cabo según lo planificado. Esto implica la existencia de políticas, procedimientos y buenas prácticas en seguridad de la información, gestión de riesgos, gestión de incidentes, métricas de seguimiento de los objetivos de seguridad, gestión de la contratación externa, etc.. Para el ENS, la seguridad del sistema será objeto de un planteamiento integral, contando con un sistema de gestión actualizado y aprobado, y un proceso de gestión de riesgos global. Esto es así porque el análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada, y la reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.
	8.2 Evaluación de riesgo de seguridad de la información			**Real Decreto 311/2022** Artículo 7 Artículo 14 **Anexo II** [op.pl.1] Análisis de riesgos	Para la ISO, en este punto, la norma ISO 27001 requiere la existencia de información documentada sobre los resultados de las apreciaciones de riesgos de seguridad de la información. Para el ENS, los requisitos del ENS en cuanto al análisis de riesgos son análogos a los de la norma ISO 27001.Para el ENS la gestión de riesgos, se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema, sin perjuicio de lo dispuesto en el anexo II, se empleará alguna metodología reconocida internacionalmente, y las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos. Considérese igualmente el Anexo III, el cual menciona que las auditorías deben verificar que existe un SGSI documentado y con un proceso regular de aprobación por la dirección.
	8.3 Tratamiento de riesgo de seguridad de la información			**Real Decreto 311/2022** Artículo 7 Artículo 14 **Anexo II** [op.pl.1] Análisis de riesgos	Para la ISO, la organización debe conservar información documentada de los resultados del tratamiento de los riesgos de seguridad de la información. Para el ENS, con carácter general los riesgos deben ser gestionados y las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos. Además, forma parte de la responsabilidad del comité o comités la gestión y coordinación de la seguridad, por canto se deriva la responsabilidad de los riesgos.
9 Evaluación del desempeño	9.1 Seguimiento, medición, análisis y evaluación			**Real Decreto 311/2022** Artículo 10 Artículo 21 Artículo 27 **Anexo II** [op.mon.2] Sistema de métricas	Para la ISO, la organización debe evaluar el desempeño de la seguridad de la información y la eficacia del SGSI mediante la implantación de métricas de seguridad, debiéndose disponer de evidencias documentadas sobre los resultados de dicha supervisión y medición. Para ISO además debe considerarse el seguimiento de los objetivos de seguridad. Para el ENS, esto se corresponde con el principio básico de reevaluación periódica, el cual dispone que las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario. No olvidemos que la evaluación y monitorización permanente forman parte del proceso global de seguridad y están integrados en todo el ciclo de seguridad de ENS, y se hace necesario la recopilación de los datos necesarios para conocer el grado de implantación de las medidas de seguridad que resulten aplicables. Es importante, además, tener en cuenta la previsión del Artículo 27. Mejora continua del proceso de seguridad; "*El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.*". Si bien es cierto que a nivel global el sistema debe ser "monitorizado" para

CLAUSULA				Artículo / Medida ENS	Análisis de requisitos compatibles y diferencias.
					analizar posibles evoluciones y mejoras, no olvidemos la previsión del artículo 110, cuando dispone en su apartado 3 "*Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.*"
	9.2 Auditoría Interna	9.2.1	Generalidades	**Real Decreto 311/2022** Artículo 31**Anexo III**	Para la ISO, implica la realización de auditorías internas a intervalos planificados, para conocer si el SGSI cumple con los requerimientos de las organizaciones para su SGSI y los de la propia norma, está implementado, y se mantiene de forma eficaz. En la práctica, para renovar la certificación de ISO 27001, esto supone la realización de una auditoría de seguimiento anual durante los dos primeros años, y de una auditoría de renovación al tercer año. Para el ENS, y fruto de seguir un esquema de certificación diferente, el ciclo de auditorías conlleva dos años, y se requiere anualmente una auditoría interna. los sistemas de información serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos de este marco legislativo. Además, especifica que, con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales en el sistema de información que puedan repercutir en las medidas de seguridad requeridas. Con carácter general ambos sistemas requieren el proceso de auditoria si bien cada sistema deriva a un proceso temporal diferenciado. La entidad deberá disponer de un plan de auditoria en la que incluirá todas las revisiones internas y externas. En este plan debe considerarse la ejecución de la auditoría interna, que será considerada también para ENS (Ver Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información, cuando requiere el análisis de "El grado de confianza en las revisiones de la Dirección y auditorías internas del auditado.").
		9.2.2	Programa de auditoría Interna		
	9.3 Revisión por la dirección	9.3.1	Generalidades	**Real Decreto 311/2022** **Anexo III**	Para la ISO, la dirección debe revisar el SGSI a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia continua. En la práctica, esto supone la celebración de revisiones por la dirección al menos con una periodicidad anual. Para el ENS, en su Anexo III, el cual menciona que las auditorías deben verificar que existe un SGSI documentado y con un proceso regular de aprobación por la dirección. Además, se debe acudir Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información, cuando requiere el análisis de "El grado de confianza en las revisiones de la Dirección y auditorías internas del auditado."
		9.3.2	Entradas de la revisión por la dirección		
		9.3.3	Resultados de la revisión por la dirección		
11 Mejora	10.1 Mejora continua			**Real Decreto 311/2022** Artículo 12 Artículo 25 Artículo 27 **Anexo II** [op.pl.2] Arquitectura de seguridad	Para la ISO la organización debe mejorar de manera continua la idoneidad, adecuación y eficacia del sistema de gestión de la seguridad de la información. Para el ENS, la política de seguridad de la información incluye como principio transversal de seguridad la mejora continua del proceso de seguridad. Así la seguridad implantada deberá ser actualizada y mejorada de forma continua, y para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad. Además de manera particular, la gestión de incidentes de seguridad contemplará el preceptivo registro que servirá, además, para la mejora continua, junto con el resto de los procesos de seguridad el sistema. Para el ENS este principio es fundamental y a tal efecto se puede comprobar como 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.
	10.2 No conformidad y acción correctiva			**Real Decreto 311/2022** Artículo 8 Artículo 31 **Anexo III**	Para la ISO, cuando ocurra una no conformidad, las organizaciones deben reaccionar ante la misma, llevar a cabo acciones para controlarla, corregirla y eliminar sus causas, y revisar la eficacia de dichas acciones, manteniéndose información documentada al respecto. Para el ENS, tras un proceso de auditoría, serán presentados al responsable del sistema y al responsable de la seguridad, quien los analizará y presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas. En el ENS no se detalla de forma explícita el contenido que debe incluir un registro o documento similar de no conformidades y la gestión de las acciones correctivas asociadas, por lo que se recomienda integrar el requisito del registro de la ISO en el sistema para lograr el nivel compatible.

5.2.3. ANÁLISIS DE MEDIDAS COMPATIBLES / CONTROLES DE SEGURIDAD.

Se ha incluido una columna relacionada con el nivel compatible de los controles de seguridad:

Identificación	Nivel Compatible	Detalle
	Análogo	En el análisis de requisitos del control analizado, se ha concluido que existe plena compatibilidad. Ambas normas exigen idénticos requisitos o las medidas detalladas resultan asimilables. Las finalidades de seguridad para el control analizado son análogos en ambas normas.
	Parcialmente análogo	En el análisis de requisitos del control analizado, se ha concluido que no existe plena compatibilidad. Las normas no son igual de exigentes en los requisitos descritos. Parte de los requisitos del control analizado resulta análogo, 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 compatibilidad. 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.

Tabla. Matriz de nivel de medidas compatibles.

DIMENSIONES Y CATEGORIA			Cod.	Control	ISO/IEC 27001:2022[40]	Nivel compatible control ISO 27001:2022 - RD 311/2022.	
Básico	Medio	Alta			[Control Principal]	Categoría ENS	Nivel compatible
			org	Marco organizativo			
aplica	aplica	aplica	org.1	Política de seguridad	5.1 Políticas para la seguridad de la información 5.36 Cumplimiento de las políticas y normas de seguridad de la información	MEDIA	
aplica	aplica	aplica	org.2	Normativa de seguridad	5.10 Uso aceptable de la información y activos asociados	MEDIA	
aplica	aplica	aplica	org.3	Procedimientos de seguridad	5.37 Documentación de procedimientos operacionales	MEDIA	
aplica	aplica	aplica	org.4	Proceso de autorización	5.2 Roles y responsabilidades en seguridad de la información	MEDIA	
			op	Marco operacional			
			op.pl	Planificación			

[40] Código de colores:
a) Azul: Controles organizacionales
b) Amarillo: Controles técnicos.
c) Verdes: Controles de personas
d) Naranja: Controles físico.

DIMENSIONES Y CATEGORIA			Cod.	Control	ISO/IEC 27001:2022[40]	Nivel compatible control ISO 27001:2022 - RD 311/2022.	
Básico	Medio	Alta			[Control Principal]	Categoría ENS	Nivel compatible
aplica	+ R1	+ R2	op.pl.1	Análisis de riesgos	6.1 – Acciones para tratar los riesgos y oportunidades	ALTA *	
aplica	+ R1	+ R1 + R2 + R3	op.pl.2	Arquitectura de seguridad	Clausula 4.4 Sistema de gestión de la seguridad de la información 8.27 Arquitectura segura de sistemas y principios de ingeniería	MEDIA (+R2*)	
aplica	aplica	aplica	op.pl.3	Adquisición de nuevos componentes	5.8 Seguridad de la información en la gestión de proyectos	MEDIA	
aplica	+ R1	+ R1	op.pl.4	Dimensionamiento/ Gestión de capacidades	8.6 Gestión de capacidades	MEDIA	
n.a.	aplica	aplica	op.pl.5	Componentes certificados	Nivel de medidas compatibles: No se contempla expresamente	MEDIA	
			op.acc	Control de acceso			
aplica	+ R1	+ R1	op.acc.1	Identificación	5.16 Gestión de identidad	MEDIA	
aplica	aplica	+ R1	op.acc.2	Requisitos de acceso	5.15 Control de acceso	ALTA *	
n.a.	aplica	+ R1	op.acc.3	Segregación de funciones y tareas	5.3 Segregación de tareas	MEDIA*	
aplica	aplica	aplica	op.acc.4	Proceso de gestión de derechos de acceso	5.18 Derechos de acceso 8.2 Gestión de privilegios de acceso	MEDIA	
+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] +R5	+ [R2 o R3 o R4] +R5	op.acc.5	Mecanismo de autenticación (usuarios externos)	5.18 Derechos de acceso 8.5 Autenticación segura	MEDIA	
+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 +	op.acc.6	Mecanismo de autenticación (usuarios de la organización)	8.5 Autenticación segura	MEDIA	
			op.exp	Explotación			
aplica	aplica	aplica	op.exp.1	Inventario de activos	5.9 Inventario de información y otros activos asociados	MEDIA (+R4)	
aplica	aplica	aplica	op.exp.2	Configuración de seguridad	8.9 Gestión de la configuración	MEDIA	
aplica	+ R1	+ R1 + R2 + R3	op.exp.3	Gestión de la configuración	8.9 Gestión de la configuración	ALTA *	
aplica	+ R1	+ R1 + R2	op.exp.4	Mantenimiento y actualizaciones de seguridad	7.13 Mantenimiento de equipos 8.8 Gestión de Vulnerabilidades técnicas	ALTA*	
n.a.	aplica	+ R1	op.exp.5	Gestión de cambios	8.32 Gestión de cambios	ALTA *	
aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	op.exp.6	Protección frente a código dañino	8.7 Controles contra el código malicioso	MEDIA	
aplica	+ R1 + R2	+ R1 + R2 + R3	op.exp.7	Gestión de incidentes	5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información	MEDIA	

DIMENSIONES Y CATEGORIA			Cod.	Control	ISO/IEC 27001:2022[40]	Nivel compatible control ISO 27001:2022 - RD 311/2022.	
Básico	Medio	Alta			[Control Principal]	Categoría ENS	Nivel compatible
					5.25Evaluación y decisión sobre los eventos de seguridad de la información		
aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5	op.exp.8	Registro de la actividad	8.15 Registros de eventos 8.17 Sincronización de reloj	MEDIA	
aplica	aplica	aplica	op.exp.9	Registro de la gestión de incidentes	5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información 5.28 Recolección de evidencia	MEDIA	
aplica	+ R1	+ R1	op.exp.10	Protección de claves criptográficas	8.24 Uso de la criptografía	MEDIA	
			op.ext	Servicios externos			
n.a.	aplica	aplica	op.ext.1	Contratación y acuerdos de nivel de servicio	5.19 Seguridad de la información en las relaciones con los proveedores 5.20 Abordar la seguridad de la información dentro de los acuerdos con los proveedores	MEDIA	
n.a.	aplica	aplica	op.ext.2	Gestión diaria	5.22 Seguimiento, revisión y gestión del cambio de los servicios de los proveedores	MEDIA	
n.a.	n.a.	aplica	op.ext.3	Protección de la cadena de suministro	5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC	ALTA *	
n.a.	aplica	+ R1	op.ext.4	Interconexión de sistemas	8.22 Segregación en redes	MEDIA	
			op.nub	Servicio en la nube			
aplica	+ R1	+ R1 + R2	op.nub.1	Protección de servicios en la nube	5.23 Seguridad de la información para el uso de servicios en la nube	MEDIA	
			op.cont	Continuidad del servicio			
n.a.	aplica	aplica	op.cont.1	Análisis de impacto	5.29 Seguridad de la información durante la interrupción 5.30 Preparación para las TIC para la continuidad del negocio	MEDIA	
n.a.	n.a.	aplica	op.cont.2	Plan de continuidad	5.29 Seguridad de la información durante la interrupción 5.30 Preparación para las TIC para la continuidad del negocio	ALTA *	
n.a.	n.a.	aplica	op.cont.3	Pruebas periódicas	5.30 Preparación para las TIC para la continuidad del negocio	ALTA *	
n.a.	n.a.	aplica	op.cont.4	Medios alternativos	8.14 Redundancia de los recursos de tratamiento de la información	ALTA *	
			op.mon	Monitorización del sistema			
aplica	+ R1	+ R1 + R2	op.mon.1	Detección de intrusión	8.21 Seguridad de los servicios de red	MEDIA	

DIMENSIONES Y CATEGORIA			Cod.	Control	ISO/IEC 27001:2022[40]	Nivel compatible control ISO 27001:2022 - RD 311/2022.	
Básico	Medio	Alta			[Control Principal]	Categoría ENS	Nivel compatible
aplica	+ R1+ R2	+ R1+ R2	op.mon.2	Sistema de Métricas	9 – Evaluación del desempeño 9.1 – Seguimiento, medición, análisis y evaluación	MEDIA	
aplica	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 +R6	op.mon.3	Vigilancia	5.7 Inteligencia de amenazas 8.16 Seguimiento de actividades	MEDIA	
			mp	Medidas de protección			
			mp.if	Protección de las instalaciones e infraestructuras			
aplica	aplica	aplica	mp.if.1	Áreas separadas y con control de acceso	7.1 Perímetro de seguridad física	MEDIA	
aplica	aplica	aplica	mp.if.2	Identificación de las personas	7.2 Controles físicos de entrada	MEDIA	
aplica	aplica	aplica	mp.if.3	Acondicionamiento de los locales	7.5 Protección contra las amenazas externas y ambientales 7.8 Emplazamiento y protección de equipos	MEDIA	
aplica	+ R1	+ R1	mp.if.4	Energía eléctrica	7.11 Instalaciones de suministro	MEDIA	
aplica	aplica	aplica	mp.if.5	Protección frente a incendios	7.5 Protección contra las amenazas externas y ambientales	MEDIA	
n.a.	aplica	aplica	mp.if.6	Protección frente a inundaciones	7.5 Protección contra las amenazas externas y ambientales	MEDIA	
aplica	aplica	aplica	mp.if.7	Registro de entrada y salida de equipamiento	7.2 Controles físicos de entrada	MEDIA	
			mp.per	Gestión del personal			
n.a.	aplica	aplica	mp.per.1	Caracterización del puesto de trabajo	6.1 Comprobación	MEDIA	
aplica	+ R1	+ R1	mp.per.2	Deberes y obligaciones	6.2 Términos y condiciones de contratación	MEDIA	
aplica	aplica	aplica	mp.per.3	Concienciación	6.3 Concienciación, educación y formación en seguridad de la información	MEDIA	
aplica	aplica	aplica	mp.per.4	Formación	6.3 Concienciación, educación y formación en seguridad de la información	MEDIA	
			mp.eq	Protección de los equipos			
aplica	+ R1	+ R1	mp.eq.1	Puesto de trabajo despejado	7.7 Puesto de trabajo despejado y pantalla limpia	MEDIA	
n.a.	aplica	+ R1	mp.eq.2	Bloqueo de puesto de trabajo	7.7 Puesto de trabajo despejado y pantalla limpia	MEDIA	
aplica	aplica	+R1 + R2	mp.eq.3	Protección de dispositivos portátiles	7.9 Seguridad de los equipos fuera de las instalaciones 8.1 Dispositivos finales de usuario	ALTA *	
aplica	+ R1	+ R1	mp.eq.4	Otros dispositivos conectados a la red	8.1 Dispositivos finales de usuario	MEDIA	
			mp.com	Protección de las comunicaciones			

DIMENSIONES Y CATEGORIA			Cod.	Control	ISO/IEC 27001:2022[40]	Nivel compatible control ISO 27001:2022 - RD 311/2022.	
Básico	Medio	Alta			[Control Principal]	Categoría ENS	Nivel compatible
aplica	aplica	aplica	mp.com.1	Perímetro seguro	8.20 Seguridad de redes 8.21 Seguridad de los servicios de red	MEDIA	
aplica	+ R1	+ R1 + R2 + R3	mp.com.2	Protección de la confidencialidad	8.20 Seguridad de redes 8.21 Seguridad de los servicios de red	MEDIA	
aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	mp.com.3	Protección de la autenticidad y de la integridad	8.20 Seguridad de redes 8.21 Seguridad de los servicios de red	MEDIA	
n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4	mp.com.4	Separación de flujos de información en la red	8.22 Segregación en redes	MEDIA	
			mp.si	Protección de los soportes de información			
aplica	aplica	aplica	mp.si.1	Marcado de soportes	5.13 Etiquetado de la información	MEDIA	
n.a.	aplica	+ R1 +R2	mp.si.2	Criptografía	8.24 Uso de la criptografía	MEDIA (+R2)*	
aplica	aplica	aplica	mp.si.3	Custodia	7.10 Soportes de almacenamiento	MEDIA	
aplica	aplica	aplica	mp.si.4	Transporte	7.10 Soportes de almacenamiento	MEDIA	
aplica	aplica	aplica	mp.si.5	Borrado y destrucción	7.14 Eliminación o reutilización segura de los equipos 8.10 Eliminación de información	MEDIA	
			mp.sw	Protección de las aplicaciones informáticas			
n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4	mp.sw.1	Desarrollo de aplicaciones	8.25 Seguridad en el ciclo de vida del desarrollo	MEDIA	
aplica	+ R1	+ R1	mp.sw.2	Aceptación y puesta en servicio	8.29 Pruebas de seguridad en desarrollo y aceptación	MEDIA	
			mp.info	Protección de la información			
aplica	+ R1 + R2	+ R1 + R2	mp.info.1	Datos personales	5.34Privacidad y protección de datos de carácter personal (DCP)	MEDIA	
n.a.	aplica	aplica	mp.info.2	Calificación de la información	5.12 Clasificación de la información	MEDIA	
aplica	+ R1 + R2 +R3	+ R1 + R2+R3 +R4	mp.info.3	Firma electrónica	8.24 Uso de la criptografía	MEDIA	
n.a.	n.a.	aplica	mp.info.4	Sellos de tiempo	8.24 Uso de la criptografía 8.26 Requisitos de seguridad de las aplicaciones	ALTA*	
aplica	aplica	aplica	mp.info.5	Limpieza de documentos	5.13 Etiquetado de la información	MEDIA	
aplica	+R1	+ R1 + R2	mp.info.6	Copias de seguridad	8.13 Copias de seguridad de la información	MEDIA (+R2) *	
			mp.s	Protección de los servicios			

DIMENSIONES Y CATEGORIA			Cod.	Control	ISO/IEC 27001:2022[40]	Nivel compatible control ISO 27001:2022 - RD 311/2022.	
Básico	Medio	Alta			[Control Principal]	Categoría ENS	Nivel compatible
aplica	aplica	aplica	mp.s.1	Protección del correo electrónico	5.14 Transferencia de la información	MEDIA	
+[R1 o R2]	+[R1 o R2]	+ R2+R3	mp.s.2	Protección de servicios y aplicaciones web	8.26 Requisitos de seguridad de las aplicaciones	MEDIA	
aplica	aplica	+ R1	mp.s.3	Protección de la navegación web	8.2 Filtrado de Webs	MEDIA	
n.a.	aplica	+ R1	mp.s.4	Protección frente a la denegación de servicio	8.6 Gestión de capacidades	MEDIA	

6. DESARROLLO DE MEDIDAS DE SEGURIDAD COMPATIBLES

6.1. [ORG] MARCO ORGANIZATIVO

[org.1] Política de Seguridad

- **Control Principal ISO/IEC 27001:2022**
  - 5.1 Políticas para la seguridad de la información
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.2 Roles y responsabilidades en seguridad de la información
  - 6.4 Proceso disciplinario
  - 5.31 Identificación de requisitos legales, reglamentarios y contractuales

Categoría: MEDIA
Nivel de medidas Compatible: **Análogo**
Particularidades de la ISO:

Será aprobada por la alta dirección y debe establecer el enfoque de la organización para gestionar la seguridad de la información.

Se deben considerar otras políticas que complementaran ésta, y en su caso la responsabilidad del desarrollo, revisión y aprobación de las políticas específicas por parte del personal pertinente en función de su nivel de autoridad y competencia técnica.

Recomendación Implantación:

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 de la organización, su estructura funcional y clara separación, lo que facilita el despliegue de controles de seguridad.

Se elaborará una Política de seguridad común, que será aprobada por el Comité y se publicará en el Boletín oficial.

[org.1.5] Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso deben alinearse con la cláusula 7.5 Información Documentada de la ISO 27001.

Es recomendable que se revisen los requerimientos de información documentada que se han incluido en las cláusulas expresamente.

[org.2] Normativa de seguridad

- **Control Principal ISO/IEC 27001:2022**
  - 5.1 Políticas para la seguridad de la información
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.6 Contacto con grupos de interés especial
  - 5.10 Uso aceptable de la información y activos asociados
  - 5.11 Devolución de activos
  - 5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información
  - 5.36 Cumplimiento de las políticas y normas de seguridad de la información
  - 6.7 Teletrabajo
  - 7.7 Puesto de trabajo despejado y pantalla limpia
  - 7.9 Seguridad de los equipos fuera de las instalaciones
  - 8.1 Dispositivos finales de usuario

Categoría: MEDIA
Nivel de medidas Compatible: Análogo
Particularidades de la ISO:

El cumplimiento de la política de seguridad de la información de la organización, las políticas y los estándares específicos debe revisarse periódicamente.

Recomendación Implantación:

Con carácter general se dispondrá de una normativa sobre el uso de equipos, servicios e instalaciones, y muy específicamente, los usos indebidos y en su caso, la responsabilidad ante el cumplimiento o violación de la normativa: (medidas disciplinarias).

Para lograr la sinergia es necesario incluir los mandatos de ambas normas, con 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].

Se dispondrá de documentación de seguridad, según las guías CCN-STIC que resulten de aplicación.

La normativa deberá ser aprobada por el Comité de Seguridad y debe darse a conocer a los usuarios afectados, incluyendo acciones de sensibilización [mp.per.4] que ayuden a una mejor comprensión.

[org.3] Procedimientos de seguridad

- **Control Principal ISO/IEC 27001:2022**
  - 5.37 Documentación de procedimientos operacionales
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.5 Contacto con las autoridades
  - 5.37 Documentación de procedimientos operacionales
  - 5.14 Transferencia de la información
  - 5.36 Cumplimiento de políticas y normas de seguridad de la información

Categoría: MEDIA
Nivel de medidas Compatible: Análogo
Particularidades de la ISO:

Los procedimientos operativos para las acciones de tratamiento de la información deben documentarse y ponerse a disposición del personal que los necesite.

Recomendación Implantación:

Será necesario mantener un mínimo de procedimientos operativos. La organización debe desarrollar los procedimientos necesarios, asociados con el sistema, especificando qué, quién y cómo hacer las operaciones, gestionar las actividades anómalas y la información.

Las organizaciones pueden disponer de proveedores encargados de la elaboración de los procedimientos en los que pudieran estar interviniendo, por lo que estos pueden ser los encargados de la elaboración de instrucciones específicas, bajo la supervisión del Responsable de Seguridad de la entidad.

Se gestionará la información de acuerdo al punto 7.5 Información documentada de la ISO 27001:2022.

[org.4] Proceso de autorización

- **Control Principal ISO/IEC 27001:2022**
  - 5.2 Roles y responsabilidades en seguridad de la información
- **Controles Complementarios ISO/IEC 27001:2022**
  - Clausula 5.3 Roles, responsabilidades y autoridades en seguridad de la información
  - 8.1 Dispositivos finales de usuario
  - 5.10 Uso aceptable de la información y activos asociados
  - 7.10 Soportes de almacenamiento
  - 8.19 Instalación del software en sistemas de producción
  - 8.20 Seguridad de redes
  - 8.21 Seguridad de los servicios de red
  - 8.32 Gestión de cambios

Categoría: MEDIA
Nivel de medidas Compatible: Parcialmente análogo

Particularidades de la ISO:

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.

Recomendación Implantación:

Si bien la ISO no es tan específica, permite desplegar un proceso particularizado de autorización.

La entidad debe mantener un proceso de autorizaciones, que identifique los diferentes roles y responsabilidades, para acciones clave, y entre ellas al menos para el uso de instalaciones, entrada de equipos y aplicaciones en producción, interconexiones y enlaces de comunicaciones, uso de medios de comunicación y de soportes de información.

También debe considerarse la responsabilidad, relacionada con los accesos al sistema, accesos remotos y desde dispositivo portátil.

Debe alinearse con el proceso de cambios. Se debe considerar no solo el control de la ISO sino la Cláusula 6.3 Planificación de cambios, *"Cuando la organización determine la necesidad de cambios en el sistema de gestión de seguridad de la información, estos cambios deberán ser llevados a cabo de forma planificada."*

Se recomienda desplegar una matriz de responsabilidades para identificar claramente los roles existentes y sus posibles funciones en relación con los activos y en el sistema.

6.2. [OP] MARCO OPERACIONAL

[OP.PL] PLANIFICACIÓN

[op.pl.1] Análisis de riesgos

- **Control Principal ISO/IEC 27001:2022**
  - 6.1 – Acciones para tratar los riesgos y oportunidades
- **Controles Complementarios ISO/IEC 27001:2022**
  - 6.1.1 – Consideraciones Generales
  - 6.1.2 – Evaluación de los riesgos de seguridad de la información
  - 6.1.3 – Tratamiento de los riesgos de seguridad de la información
  - 8.2 – Evaluación de los riesgos de seguridad de la información
  - 8.3 – Tratamiento de los riesgos de seguridad de la información

Categoría: MEDIA
Nivel de medidas Compatible: Análogo
Particularidades de la ISO:

Se debe documentar el criterio seguido para la aceptación del riesgo, identificar propietarios de estos, priorizando los tratamientos y asumiendo los riesgos residuales.

Recomendación Implantación:

Ambas normas convergen y puede emplearse la misma metodología de riesgos para desplegar este control. Al menos será necesario realizar un análisis de riesgos semiformal, usando un lenguaje específico, con un catálogo básico de amenazas y una presentación con tablas, considerando valoraciones cualitativas de los activos más valiosos del sistema, cuantitativas de las amenazas más probables, valoración de las salvaguardas y valoración del riesgo residual.

Se recomienda la metodología MAGERIT empleando la herramienta PILAR. No obstante, puede emplearse la metodología de la ISO 31000.

Debe considerarse una declaración de aplicabilidad compartida de ambas normas

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

- **Control Principal ISO/IEC 27001:2022**
  - 5.9 Inventario de información y otros activos asociados
- **Controles Complementarios ISO/IEC 27001:2022**
  - 8.20 Seguridad de redes
  - 8.27 Arquitectura segura de sistemas y principios de ingeniería

Categoría: MEDIA (+R2*)
Nivel de medidas Compatible: Análogo
Particularidades de la ISO:

La organización debe establecer, implementar, mantener y mejorar de manera continua un Sistema de Gestión de Seguridad de la Información, de acuerdo con los requisitos de la norma.

Los principios para diseñar sistemas seguros deben establecerse, documentarse, mantenerse y aplicarse a cualquier actividad de desarrollo de sistemas de información.

Recomendación Implantación:

Ambos sistemas se apoyan en un Sistema de Gestión y de Seguridad de la Información, con un ciclo de mejora (PDCA). 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.

Es importante considerar la parte de información documentada que la ISO recuerda a lo largo de sus cláusulas.

[op.pl.3] Adquisición de nuevos componentes

- **Control Principal ISO/IEC 27001:2022**
  - 5.8 Seguridad de la información en la gestión de proyectos

- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.19 Seguridad de la información en las relaciones con los proveedores
  - 5.20 Abordar la seguridad de la información dentro de los acuerdos con proveedores

Categoría: MEDIA
Nivel de medidas Compatible: Parcialmente análogo

Particularidades de la ISO:

Los procesos de adquisición se integrarán en proyectos completos y globales, que contemplarán muchos elementos y entre ellos debería incluirse, la adquisición de componentes, arquitectura y necesidades. La seguridad de la información debe integrarse en las actividades de gestión de proyectos de la organización.

Recomendación Implantación:

Es importante considerar el proceso global, y de manera transversal. Así se documentará y se incluirán requisitos de seguridad en los procesos de contratación de la entidad. Y se deberá alinear con capacidad; proceso formal para planificar la adquisición de nuevos componentes del sistema, considerando la capacidad [op.pl.4], los riesgos del sistema [op.pl.1], la arquitectura[op.pl.2] y las necesidades técnicas, de formación y de financiación.

Este plan anual de capacidad considerará las previsiones, las necesidades de crecimiento y de seguridad y los recursos necesarios. Será aprobado por el Comité de Seguridad de la Información.

En todo caso, las entidades deben considerar la integración en sus procesos de contratación y el pleno sometimiento a la normativa específica de contratación pública.

[op.pl.4] Dimensionamiento / Gestión de capacidades

- **Control Principal ISO/IEC 27001:2022**
  - 8.6 Gestión de capacidades
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.23 Seguridad de la información para el uso de servicios en la nube

Categoría: MEDIA
Nivel de medidas Compatible: Análogo
Particularidades de la ISO:

Planificación, monitorización y ajuste. Esta gestión implica una dual estrategia; aumentando la capacidad y/o reduciendo la demanda.

Recomendación Implantación:

Ambas normas pueden converger perfectamente. Con carácter general se dispondrá de un estudio al menos anual, actualizado y monitorizado periódicamente. Se pueden emplear diferentes herramientas que permitan conocer en tiempo real el estado de la capacidad y alertas, ver las tendencias de periodos determinados y generar alertas, bajo umbrales definidos. Es recomendable la automatización, que puede ser mediante un proveedor TICS que ayude a gestionar las mediciones, alertas y planificaciones.

Los servicios en la nube pueden ser ayuda, dada la escalabilidad de estos. Considérese el control [op.nub.1].

[op.pl.5] Componentes certificados

- **Control Principal ISO/IEC 27001:2022**
  - No hay medidas compatibles
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.19 Seguridad de la información en la relación con los proveedores
  - 5.20 Abordar la seguridad de la información dentro de los acuerdos con proveedores

Categoría: MEDIA
Nivel de medidas Compatible: Nula
Particularidades de la ISO:

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. Es necesario que se trate de productos y servicios acreditados, bajo la premisa de mejorar la seguridad.

Recomendación Implantación:

Este control no está contemplado en la ISO. Es necesario incluir un inventario de los componentes afectados, analizando si los mismos cumplen las exigencias establecidas, las particularidades previstas en el artículo 19 del Real Decreto y específicamente son componentes incluidos en el Catálogo STIC CCN 105. En su caso, debe considerarse acreditaciones europeas análogos, tales como Common Criteria (EU).

Se recomienda integrar como requisitos en los procesos de adquisición y contratación, como previsiones futuras de adquisición de nuevos componentes, estos requisitos.

Cuando los componentes no se encuentran en el catálogo correspondiente, pueden asociarse otras certificaciones de producto o de servicio, por ejemplo, de la familia ISO 27000.

[OP.ACC] CONTROL DE ACCESO

[op.acc.1] Identificación

- **Control Principal ISO/IEC 27001:2022**
  - 5.16 Gestión de identidad
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.15 Control de acceso

Categoría: MEDIA
Nivel de medidas Compatible: Análogo
Particularidades de la ISO:

Se debe administrar el ciclo de vida completo de las identidades.

Recomendación Implantación:

Ambas normas permiten la gestión de las identidades de manera completa. Para ello, se deberá identificar a los usuarios con un identificador único, pudiendo estar alineados con las premisas de la normativa.

Cuando un usuario deba tener diferentes roles frente al sistema, recibirá identificadores diferentes. Es importante que toda entidad (entidad, usuario o proceso) disponga de un identificador singular que permita conocer quien actúa [id] y las acciones realizadas por cada entidad. Además, las cuentas deben ser inhabilitadas por pérdida de necesidad y se asociaran a las retenciones necesarias. Las retenciones deben considerarse en base a los requerimientos legales.

Se considerará el Refuerzo R1 – Identificación avanzada; se podrá singularizar a la persona, los privilegios asociados y se mantendrá una lista de usuarios.

Es recomendable que la entidad mantenga un inventario de servicios (incluyendo aquellos que son proporcionados por servicios en la nube) y asocie los permisos concedidos. 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

- **Control Principal ISO/IEC 27001:2022**
  - 5.15 Control de acceso
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.18 Derechos de acceso
  - 8.2 Gestión de privilegios de acceso
  - 8.3 Restricción de acceso a la información
  - 8.18 Uso de los programas de utilidad con privilegios
  - 8.4 Acceso al código fuente

Categoría: ALTA *
Nivel de medidas Compatible: Análogo
Particularidades de la ISO:

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.

Se pueden emplear varios métodos para el control de acceso, pudiendo desplegar elementos dinámicos.

Recomendación Implantación:

Los derechos de acceso de cada recurso se establecerán según las decisiones del responsable del recurso, ateniéndose a la política y normativa de seguridad del sistema. 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).

Particularmente, se controlará el acceso a los componentes del sistema operativo y a sus ficheros o registros de configuración.

Es necesario considerar el Refuerzo R1 – Privilegios de acceso, alinear ambos marcos y específicamente el control 8.2. Derechos de acceso privilegiados.

- [op.acc.2.r1.1] Todos los usuarios autorizados deben tener un conjunto de atributos de seguridad (privilegios) que puedan ser mantenidos individualmente.

- [op.acc.2.r1.2] Los privilegios de acceso se implementarán para restringir el tipo de acceso que un usuario puede tener (lectura, escritura, modificación, borrado, etc.).

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

- **Control Principal ISO/IEC 27001:2022**
  - 5.3 Segregación de tareas
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.18 Derechos de acceso
  - 8.2 Gestión de Privilegios de acceso

Categoría: MEDIA*
Nivel de medidas Compatible: **Análogo**
Particularidades de la ISO:

Deben segregarse los deberes y las áreas de responsabilidad en conflicto.

Recomendación Implantación:

Será de aplicación los requisitos de categoría MEDIA. Excepcionalmente cuando las entidades se encuentren limitadas en cuanto a personal ""cualificado"", podrá considerar medidas compensatorias para el requisito, [op.acc.3.1] Siempre que sea posible, las capacidades de desarrollo y operación no recaerán en la misma persona. así, siempre que sea difícil segregar, se podrán considerar otros controles, como el seguimiento de las actividades, pistas de auditoría y la supervisión de la gestión.

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, ...

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

- **Control Principal ISO/IEC 27001:2022**
  - 5.18 Derechos de acceso
- **Controles Complementarios ISO/IEC 27001:2022**

- 8.2 Gestión de Privilegios de acceso

Categoría: MEDIA
Nivel de medidas Compatible: Análogo
Particularidades de la ISO:

Concesión y revocación de los derechos de acceso. Se deben realizar acciones de revisión ante cambios o terminación del empleo.

La asignación y el uso de derechos de acceso privilegiado deben restringirse y administrarse.

Recomendación Implantación:

"Ambas normas convergen, si bien en el caso de la ISO deben considerarse previsiones contenidas en varios controles.

Se documentará el cumplimiento de los principios de; "*todo acceso estará prohibido, salvo autorización expresa.", "capacidad de autorizar, con una revisión de permisos periódica."; [org.4]"Mínimo privilegio para cumplir sus obligaciones o funciones.", "Necesidad de conocer y responsabilidad de compartir", y "política específica de acceso remoto, requiriéndose autorización expresa."*

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)

- **Control Principal ISO/IEC 27001:2022**
  - 5.18 Derechos de acceso
- **Controles Complementarios ISO/IEC 27001:2022**
  - 8.5 Autenticación segura

Categoría: MEDIA
Nivel de medidas Compatible: Parcialmente análogo
Particularidades de la ISO:

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.

Recomendación Implantación:

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.

Es importante considerar el Refuerzo R5 Registro

[op.acc.5.r5.1] Se registrarán los accesos con éxito y los fallidos.

[op.acc.5.r5.2] Se informará al usuario del último acceso efectuado con su identidad.

Es posible que intervengan terceros por lo que se deberían considerar las responsabilidades del proveedor (desarrollador y mantenedor de servicios) y el titular de estos.

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

- **Control Principal ISO/IEC 27001:2022**
  - 8.5 Autenticación segura
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.15 Control de acceso

Categoría: MEDIA
Nivel de medidas Compatible: Análogo
Particularidades de la ISO:

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.

Recomendación Implantación:

El control de la ISO permite adaptar a los requisitos del ENS las autenticaciones, modulándose con las particularidades que requiere el control ENS.

Antes de proporcionar las credenciales, los usuarios conocerán y aceptarán la política de seguridad y reconocerán que han recibido las credenciales de acceso y que conocen y aceptan las obligaciones que implica; así como el deber de custodia diligente, la protección de su confidencialidad y el deber de notificación inmediata en caso de pérdida.

El sistema solo dará la información imprescindible, para que el usuario se autentique, y si se rechaza, no se informará del motivo del mismo.

El número de intentos permitidos será limitado, y se informará al usuario de sus derechos u obligaciones inmediatamente después de obtener el acceso, así como del último acceso efectuado con su identificador. Los accesos e intentos serán registrados.

Los accesos físicos a las instalaciones, se podrán considerar accesos a zonas controladas siempre que se cumpla el requisito dispuesto en el control [op.acc.6]. Se considerará la zona de controlada, como elemento diferenciador para requerir mayor robustez en la autenticación:

a) Zona controlada; considerada como una zona que no es de acceso público y el usuario, antes de tener acceso al equipo, se ha autenticado de alguna forma (control de acceso a las instalaciones), pero con un mecanismo diferente al de autenticación lógica frente al sistema.

b) Zona no controlada; por ejemplo, Internet. Se requiere refuerzo en el proceso de autenticación.

Como mecanismos de autenticación en zonas controladas, podrá elegir entre:

a) Contraseña cuando el acceso se realiza desde zonas controladas y sin atravesar zonas no controladas

b) Contraseña y Otro factor

c) Certificado

Doble factor para acceso desde o a través de zonas no controladas.

a) Contraseña y Otro factor

b) Certificado

Por defecto, se documentará una política de acceso remoto los usuarios y situaciones autorizadas. Acceso remoto deberá:

a) Ser autorizado.

b) Su tráfico deberá ser cifrado.

c)Ser inhabilitado cuando no sea necesario, si la utilización no es constante.

d)Disponer de los registros de auditoría de este tipo de conexiones.

Los refuerzos (+R6) y (+ R7) pueden ser interesantes en base a la criticidad de la información que puede procesar y se alinea con las practicas recogidas en la ISO 27002

Accesos de un proveedor se podrá autorizar, acceso mediante túneles, con IP de origen y un control de accesos previo por parte del proveedor.

Por último, se pueden considerar los refuerzos contenidos en la categoría Alta, dado que los mismos pueden mejorar la seguridad del acceso y son contemplados por la ISO 27002:

- finalizar sesiones inactivas después de un período definido de inactividad,

- 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] EXPLOTACIÓN

[op.exp.1] Inventario de activos

- **Control Principal ISO/IEC 27001:2022**
  - 5.9 Inventario de información y otros activos asociados
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.11 Devolución de activos
  - 7.8 Emplazamiento y protección de equipos
  - 7.9 Seguridad de los activos fuera de las instalaciones

Categoría: MEDIA (+R4)
Nivel de medidas Compatible: **Análogo**
Particularidades de la ISO:

Se debe desarrollar y mantener un inventario de información y otros activos asociados, y se incluirán los propietarios de los mismos.

Recomendación Implantación:

Será de aplicación los requisitos de categoría BASICA. Se debe recomendar el considerar los refuerzos presentes en este control, que si bien no son directamente aplicables pueden ayudar a gestionar los activos de manera más completa. Como ejemplo se puede ver 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 análogo a lo requerido en [mp.sw.1.r5].

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 de la entidad. No obstante, lo ideal será un inventario que permita realizar trazas con puntos clave como incidentes de seguridad o gestión del cambio.

Debe considerarse al 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.

Por último, puede enriquecer la información del inventario el incluir la información correspondiente con el control [op.pl.5].

[op.exp.2] Configuración de seguridad

- **Control Principal ISO/IEC 27001:2022**
  - 8.9 Gestión de la configuración
- **Controles Complementarios ISO/IEC 27001:2022**
  - 8.8 Gestión de vulnerabilidades técnicas
  - 8.12 Prevención de fuga de datos
  - 8.19 Instalación de software en sistemas de producción
  - 8.20 Seguridad de redes
  - 8.21 Seguridad de los servicios de red.

Categoría: MEDIA
Nivel de medidas Compatible: Parcialmente análogo
Particularidades de la ISO:

Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, monitorizarse y revisarse.

Recomendación Implantación:

Se configurarán los equipos previamente a su entrada en operación, de forma que:

- Se retiren cuentas y contraseñas estándar.

- Se aplicará la regla de "mínima funcionalidad "al, será un uso seguro.

Las máquinas virtuales estarán configuradas y gestionadas de un modo seguro tal y como se gestionan las máquinas físicas.

Muchas funciones pueden estar gestionadas por el proveedor de servicios, que considerará los requisitos de seguridad necesarios y específicamente, aquellas guías del CCN- STIC[41] y/o herramientas del CCN que pudieran ser útiles. 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.

Por razón de la superficie de exposición, aquellos activos que estén solo en el ámbito interno y que no presenten riesgos significativos, podrán ser configurados con una plantilla genérica de seguridad, rebajando ciertos requisitos de seguridad.

[op.exp.3] Gestión de la configuración

- **Control Principal ISO/IEC 27001:2022**
  - 8.9 Gestión de la configuración
- **Controles Complementarios ISO/IEC 27001:2022**
  - 8.8 Gestión de vulnerabilidades técnicas
  - 8.12 Prevención de fuga de datos
  - 8.13 Copias de seguridad de la información
  - 8.19 Instalación de software en sistemas de producción
  - 8.20 Seguridad de redes
  - 8.21 Seguridad de los servicios de red.

Categoría: ALTA*
Nivel de medidas Compatible: **Parcialmente análogo**

Particularidades de la ISO:

Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, monitorizarse y revisarse.

Recomendación Implantación:

La organización debe definir e implementar procesos y herramientas para hacer cumplir la configuración. Además de mantener una serie de plantillas estándar para la configuración de seguridad de hardware, software, servicios y redes, deben ser revisadas periódicamente y cuando sea necesario, actualizarse. Se debe definir e implementar en los procesos y herramientas, la necesidad de cumplir la configuración de seguridad.

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

[41] https://www.ccn-cert.cni.es/guias.html

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 y, además, en los procesos se considerarán las copias de las configuraciones lo que nos permitirá alinear ambas normas; 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.

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 y la documentación de aquellas herramientas que ayudan a gestionar posibles desviaciones o vulnerabilidades.

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

- **Control Principal ISO/IEC 27001:2022**
  - 7.13 Mantenimiento de equipos

Controles Complementarios ISO/IEC 27001:2022

- 8.8 Gestión de vulnerabilidades técnicas
- 8.31 Separación de los entornos de desarrollo, prueba y producción
- 8.32 Gestión de cambios

Categoría: ALTA*
Nivel de medidas Compatible: **Parcialmente análogo**

Particularidades de la ISO:

El equipo debe mantenerse correctamente. Lo que conlleva un proceso y registro de mantenimientos.

Recomendación Implantación:

En el caso del ENS es más estricto en sus requisitos, siendo recomendable la aplicación de este control en su categoría ALTA, si bien puede considerarse en su categoría MEDIA. Pueden lograrse la compatibilidad 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 para la 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 en 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.

5.- No puede aislarse en ninguna de las dos normas, la gestión de cambios y, puede aprovecharse el propio ciclo de gestión 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

- **Control Principal ISO/IEC 27001:2022**
  - 8.32 Gestión de cambios
- **Controles Complementarios ISO/IEC 27001:2022**
  - 7.13 Mantenimiento de los equipos
  - 8.8 Gestión de Vulnerabilidades técnicas
  - 8.31 Separación de los entornos de desarrollo, prueba y producción

Categoría: ALTA*
Nivel de medidas Compatible: **Análogo**
Particularidades de la ISO:

Los cambios en la organización, procesos, instalaciones y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios.

Recomendación Implantación:

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 controlados) y aceptación de pruebas funcionales y de seguridad y la autorización de cambios.

Será de aplicación los requisitos de categoría ALTA. Es necesario asociar el “Refuerzo R1-Prevención de fallos” con el control [op.exp.4]

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

- **Control Principal ISO/IEC 27001:2022**
  - 8.7 Controles contra el código malicioso
- **Controles Complementarios ISO/IEC 27001:2022**
  - 8.8 Gestión de vulnerabilidades técnicas
  - 8.9 Gestión de la configuración

Categoría: MEDIA
Nivel de medidas Compatible: Análogo
Particularidades de la ISO:

Se debe implementar la protección contra el malware, incluyendo acciones de concienciación del usuario.

Recomendación Implantación:

Ambas normas convergen perfectamente si bien es necesario que el control sea liderado por los requisitos del ENS para categoría MEDIA. Así se dispondrá de soluciones de detección de código dañino, en todos los equipos y dispositivos del sistema, actualizándose las bases de datos y analizando cualquier fichero externo. La solución analizará los sistemas en sus arranques.

Debemos considerar el impacto de este control en el control [op.exp.4] Mantenimiento y controles de continuidad [op.cont] y considerar el control [mp.per. 3].

.. op.exp.7 Gestión de incidentes

- **Control Principal ISO/IEC 27001:2022**
  - 5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información
  - 5.25 Evaluación y decisión sobre los eventos de seguridad de la información
  - 5.26 Respuesta a incidentes de seguridad de la información
  - 5.27 Aprender de los incidentes de seguridad de la información
  - 5.28 Recopilación de evidencias
  - 6.8 Notificación de los eventos de Seguridad de la Información

Categoría: MEDIA
Nivel de medidas Compatible: Parcialmente análogo

Particularidades de la ISO:

Se realizará una gestión de incidentes de seguridad, definiendo y establecimiento un proceso, con los roles implicados y las responsabilidades.

Recomendación Implantación:

En el caso de la ISO son varios los controles que debemos considerar para poder cubrir los requisitos del ENS den su categoría MEDIA. 5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información, 5.25 Evaluación y decisión sobre los eventos de seguridad de la información, 5.26 Respuesta a incidentes de seguridad de la información, 5.27 Aprender de los incidentes de seguridad de la información.

Es conveniente que las entidades tiendan a cumplir los requerimientos tal y como detalla el ENS, dado que el Real Decreto está alineado con la normativa europea y traza la estrategia de ciberseguridad. Debe considerarse desplegar un proceso que estará alineado con la Guía CCN-STIC 817 y con la Guía de Ciberincidentes Nacional y trabajar bajo la ventanilla única, la plataforma LUCIA (Refuerzo R1 – Notificación [op.exp.7.r1.1] entidades sector público).

La entidad desarrollará un proceso integral frente a incidentes de seguridad, incluyendo los criterios de clasificación y el escalado de la notificación. Se incluirá necesariamente un proceso para la comunicación de pérdida o sustracción de dispositivos y portátiles [mp.eq.3.2] y se desplegarán las medidas precisas y recursos suficientes para la gestión de los incidentes.

[op.exp.8] Registro de la actividad de los usuarios

- **Control Principal ISO/IEC 27001:2022**
  - 8.15 Registro de eventos
- **Controles Complementarios ISO/IEC 27001:2022**
  - 8.17 Sincronización del reloj

Categoría: MEDIA
Nivel de medidas Compatible: **Parcialmente análogo**

Particularidades de la ISO:

Se deben activar, proteger, almacenar y analizar registros de actividades, excepciones, fallos y otros eventos relevantes.

Recomendación Implantación:

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. Así se mantendrá operativo un registro de auditoría, que incluirá al menos el identificador del usuario o entidad, fecha y hora, qué información se ve afectada, tipo de evento (*) y su resultado (fallo o éxito). Es necesario activar los registros en los servidores.

Se mantendrá un proceso de revisión informal, manteniendo un estricto control sobre el acceso a los registros y a su configuración; se mantendrá una sincronización de relojes, para la evidencia del registro y se preparará un registro o inventario con los registros operativos, terceros implicados y tiempos de retención establecidos.

Con respecto a los eventos (*), deberían considerarse [es recomendable]:

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 (incluidos 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).

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 análogo 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.

Es recomendable que, si se 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 incidencias

- **Control Principal ISO/IEC 27001:2022**
  - 5.26 Respuesta a incidentes de seguridad de la información
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información
  - 5.25 Evaluación y decisión sobre los eventos de seguridad de la información
  - 5.26 Respuesta a incidentes de seguridad de la información
  - 5.27 Aprender de los incidentes de seguridad de la información
  - 5.28 Recopilación de evidencias
  - 6.8 Notificación de los eventos de seguridad de la información

Categoría: MEDIA
Nivel de medidas Compatible: **Análogo**
Particularidades de la ISO:

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 mortem.

Recomendación Implantación:

A nivel general la ISO es flexible a la hora de desplegar los requisitos de ENS. Se deben documentar todas las acciones derivadas de [op.exp.7]. El Registro podrá ser gestionado mediante un archivo manual, pero debe estar trazado con los requisitos establecidos en la Guía CCN STIC 817 y cuando disponga del acceso, la propia solución LUCIA.

Se gestionarán las evidencias para su utilidad en cualquier ámbito jurisdiccional, (fines disciplinarios y/o desviaciones de proveedores externos y/o persecución de delitos).

Existirán análisis de los incidentes y la determinación de los eventos auditables [op.exp.8]

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.

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. Es interesante que la entidad reciba información periódicamente sobre la tendencia global y acotada al ámbito de actuación de la misma, sobre incidentes y ataques. Esto puede ayudar a la entidad a calibrar medidas de prevención e incluso formar y concienciar a sus usuarios.

[op.exp.10] Protección de claves criptográficas

- **Control Principal ISO/IEC 27001:2022**
  - 8.24 Uso de criptografía
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.17 Información de Autenticación

Categoría: MEDIA
Nivel de medidas Compatible: **Parcialmente análogo**

Particularidades de la ISO:

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). Se tendrá en cuenta la Guía de Seguridad de las TIC CCN-STIC 807

Recomendación Implantación:

La propia ISO deriva a los requerimientos legales, en el cumplimiento de este control. 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 los requerimientos.

Las claves criptográficas se protegerán durante todo su ciclo de vida, por lo que la entidad mantendrá procesos y herramientas para ello. Deben inventariarse y mantenerse un análisis de los algoritmos empleados.

Los medios de generación y explotación estarán aislados.

Existirá una retención de las claves que deban ser archivadas y se controlará la retención de estas.

Se considera la gestión de las claves, los requerimientos de los algoritmos (ver Guía CCN STIC 807 y Guía CCN STIC 221), los correspondientes certificados y firma cualificados.

Los servicios gestionados por terceros y especialmente aquellos en la nube deben considerar los requisitos de este control. No obstante, la entidad debe comprobar el cumplimiento de este control.

A los efectos de los gestores de claves, debe considerarse CCN-STIC-105 Catálogo de Productos y Servicios de Seguridad de las TIC, 7.2.7 FAMILIA: DISPOSITIVOS PARA GESTIÓN DE CLAVES CRIPTOGRÁFICAS".

[OP.EXT] SERVICIOS EXTERNOS

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

- **Control Principal ISO/IEC 27001:2022**
  - 5.19 Seguridad en la información en las relaciones con los proveedores
- **Controles Complementarios ISO/IEC 27001:2022**
  - 6.6 Acuerdos de confidencialidad o no divulgación
  - 5.19 Seguridad de la Información en las relaciones con los proveedores
  - 5.20 Abordar la seguridad de la información dentro de los acuerdos con los proveedores
  - 5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC

Categoría: MEDIA
Nivel de medidas Compatible: **Análogo**
Particularidades de la ISO:

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.

Recomendación Implantación:

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. Se deberá incluir como requisitos en los contratos (y específicamente en las licitaciones) Acuerdos de Nivel de Servicio, así como las características del "servicio mínimo admisible", la responsabilidad y consecuencias del incumplimiento. Se tendrán en cuenta otros controles afectados [op.cont] y [op.pl.3] [op.pl.4] y muy especialmente aquellos servicios derivados de un tercero. Se considerarán en este punto los servicios en la nube [op.nub].

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.

[op.ext.2] Gestión diaria

- **Control Principal ISO/IEC 27001:2022**
  - 5.22 Seguimiento, revisión y gestión del cambio de los servicios de proveedores
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.19 Seguridad de la Información en las relaciones con los proveedores
  - 5.20 Abordar la seguridad de la información dentro de los acuerdos con los proveedores
  - 5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC

Categoría: MEDIA
Nivel de medidas Compatible: **Parcialmente análogo**

Particularidades de la ISO:

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.

Recomendación Implantación:

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. Se recomienda requerir a los proveedores, que emitan informes (con cierta periodicidad y al menos anuales) de cumplimiento y/o desviaciones, y especialmente para servicios en la nube. Las entidades públicas deben considerar las mediciones requeridas anualmente en la encuesta nacional- INES.

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

- **Control Principal ISO/IEC 27001:2022**
  - 5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC
- **Controles Complementarios ISO/IEC 27001:2022**

- 5.29 Seguridad de la información durante la interrupción

Categoría: ALTA *
Nivel de medidas Compatible: **Análogo**
Particularidades de la ISO:

Debe gestionarse 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.

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.

Recomendación Implantación:

Se debe considerar este control para alinear ambas normas, de manera que será de aplicación la categoría ALTA, relacionados con los controles del bloque de controles [op.cont].

Es conveniente considerar el requerimiento de la previsión contenida en el artículo 2 del Real Decreto 311/2022, de 3 de mayo;

"Los pliegos de prescripciones administrativas o técnicas de los contratos que celebren las entidades del sector público (...) contemplarán todos aquellos requisitos necesarios para asegurar la conformidad con el ENS (...)."

Esta cautela se extenderá también a la cadena de suministro de dichos contratistas, en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos.

En el análisis de riesgos de la entidad, deberían considerarse los servicios y las subcontrataciones, con independencia de la metodología empleada.

Se deben considerar los requerimientos legales implicados.

Se debería exigir que los proveedores propaguen los requisitos de seguridad a lo largo de la cadena de suministro si mantienen subcontrataciones 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

- **Control Principal ISO/IEC 27001:2022**
  - 8.22 Segregación en redes
- **Controles Complementarios ISO/IEC 27001:2022**
  - 8.20 Seguridad de redes
  - 8.21 Seguridad de los servicios de red.

Categoría: MEDIA
Nivel de medidas Compatible: **Nula**

Particularidades de la ISO:

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.

Recomendación Implantación:

Este control es requisito directo del ENS, se tendrá en cuenta la Guía de Seguridad de las TIC CCN-STIC 811.

A efectos de la ISO se percibe en algunos controles. Será de aplicación la categoría MEDIA, debiendo prestar atención al 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 asociadas a requisitos públicos (por ejemplo, RED SARA o RED IRIS), se debe considerar la previsión contenida en el 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."

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] SERVICIO EN LA NUBE

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

- **Control Principal ISO/IEC 27001:2022**
  - 5.23 Seguridad de la información para el uso de servicios en la nube
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.19 Seguridad de la Información en las relaciones con los proveedores
  - 5.20 Abordar la seguridad de la información dentro de los acuerdos con los proveedores
  - 5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC
  - 5.22 Seguimiento, revisión y gestión de cambios de los servicios de proveedores

Categoría: MEDIA
Nivel de medidas Compatible: **Parcialmente análogo**

Particularidades de la ISO:

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.

Recomendación Implantación:

Los requisitos de la ISO están muy alineados con el ENS. Los servicios requerirán un cumplimiento de las medidas del ENS y se mantendrán durante el servicio.

Se requerirá la certificación correspondiente en la categoría MEDIA. No obstante, la entidad debería considerar el Refuerzo R2 – Guías de Configuración de Seguridad Específicas y asociar este, al control relacionado con [org.3] y [op.exp.2]

En relación con [op.nub.1.r1.2]; si el servicio en la nube es un servicio de seguridad deberá cumplir con los requisitos establecidos en [op.pl.5].

Cuando existan proveedores o servicios carentes de ello, se podrá desplegar una medida complementaria en la que se identifiquen los controles aplicables. Podrá aceptarse una certificación en ISO 27001 como medida complementaria. Es posible en su caso, considerar una medida derivada de la Guía CCN STIC 819.

[OP.CONT] CONTINUIDAD DEL SERVICIO

[op.cont.1] Análisis de impacto

- **Control Principal ISO/IEC 27001:2022**
  - 5.29 Seguridad de la información durante la interrupción
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.30 Preparación de las TIC para la continuidad del negocio

Categoría: MEDIA
Nivel de medidas Compatible: **Análogo**
Particularidades de la ISO:

La organización debe planificar cómo mantener la seguridad de la información en un nivel adecuado durante la interrupción.

Recomendación Implantación:

En ambos marcos se resalta el elemento clave en tema de resiliencia y contingencia: planificación. La planificación debe considerar el alcance, el impacto de las interrupciones y priorizar las consecuencias de la pérdida de confidencialidad e integridad de la información, además de la necesidad de mantener la disponibilidad. Se deben considerar los servicios y las criticidades, permitiendo detectar RTO y RPO.

Se recomienda que se analicen riesgos detectados (salida del análisis de riesgos [op.pl.1]), que tengan la particularidad de disponer de un alto impactos y baja probabilidad. Estos riesgos pueden ser considerados como escenarios asociados a disrupciones y deberían servir para ayudar a la preparación de las situaciones de contingencia. ".

[op.cont.2] Plan de continuidad

- **Control Principal ISO/IEC 27001:2022**
  - 5.29 Seguridad de la información durante la interrupción
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.30 Preparación de las TIC para la continuidad del negocio
  - 8.14 Redundancia de los recursos de tratamiento de la información

Categoría: ALTA *
Nivel de medidas Compatible: Análogo
Particularidades de la ISO:

La organización debe planificar cómo mantener la seguridad de la información en un nivel adecuado durante la interrupción.

Recomendación Implantación:

"La entidad debe considerar el despliegue del control en su categoría ALTA. Existen situaciones en las que las dependencias y las necesidades asociadas a las disponibilidades de los servicios exigen desplegar estrategias de continuidad. Pero además cuando realizamos un proceso de integración del Esquema Nacional de Seguridad y la ISO 27001, debe impulsarse los controles asociados a continuidad y alternatividad.

Se debe diseñar un plan global que incluya necesariamente la estrategia de contingencia de la entidad, información, sistemas, activos, personal, instalaciones, colaboradores y herramientas de apoyo. Es necesario planificar y mantener una preparación ante la hipotética materialización de un evento catastrófico.

Dentro de la estrategia de la organización, debe estudiarse aquellos controles de seguridad que no operaran durante una caída total o paralización de la organización, y en su caso, proponer controles de compensación para estos controles de seguridad de la información que no se pueden mantener durante la interrupción. Una buena estrategia para ello puede ser considerar una declaración de aplicabilidad con fuentes complementarias a la ISO 27001 y el ENS, y que identifique aquellos controles que resultarán inhabilitados temporalmente y aquellos que se habilitaran temporalmente como medida alternativa o compensatoria. ".

[op.cont.3] Pruebas periódicas

- **Control Principal ISO/IEC 27001:2022**
  - 5.30 Preparación de las TIC para la continuidad del negocio
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.29 Seguridad de la información durante la interrupción
  - 8.13 Copias de seguridad de la información

Categoría: MEDIA
Nivel de medidas Compatible: Análogo
Particularidades de la ISO:

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.

Recomendación Implantación:

Se incluirá este control de categoría ALTA. Como parte de la estrategia de continuidad, la entidad debe analizar las pruebas más adecuadas para comprobar que su planificación es correcta y que los recursos estimados son suficientes. La necesidad de preparación de las TIC para la continuidad del negocio se puede enriquecer al considerar también los riesgos detectados con alto impacto y baja probabilidad.

La entidad debería establecer un plan de pruebas, con calendarios y responsables y documentar los resultados, para su análisis y estudio detallado. Para la realización de las pruebas se pueden considerar diferentes modalidades y diferentes perspectivas, tanto simulacros como pruebas de papel.

La planificación 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 con mayor criticidad, trazar los tiempos y analizar desviaciones.

[op.cont.4] Medios alternativos

- **Control Principal ISO/IEC 27001:2022**
  - 8.14 Redundancia de los recursos de tratamiento de la información
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.29 Seguridad de la información durante la interrupción
  - 8.13 Copias de seguridad de la información

Categoría: ALTA *
Nivel de medidas Compatible: **Parcialmente análogo**

Particularidades de la ISO:

Las instalaciones de procesamiento de información deben implementarse con suficiente redundancia para cumplir con los requisitos de disponibilidad.

Recomendación Implantación:

Para tener un sistema de gestión alineado con las dos normas, se incluirá este control de categoría ALTA. Se puede perfilar el alcance del control al requerimiento principal de la ISO, pero en todo caso, la organización debe alinear su plan de capacidad [op.pl.4] con este control, dado que existen escenarios (clásicos) de contingencia asociados con "indisponibilidades" de recursos clave en el día a día.

Se recomienda que la organización diseñe e implemente una arquitectura de sistemas con la redundancia adecuada para cumplir con estos requisitos.

Los servicios en la nube permiten el cumplimiento de este control, siempre y cuando se consideren como alternatividad o se contraten con el servicio de redundancias clave.

[OP.MON] MONITORIZACIÓN DEL SISTEMA

[op.mon.1] Detección de intrusión

- **Control Principal ISO/IEC 27001:2022**
  - 8.20 Seguridad de redes
- **Controles Complementarios ISO/IEC 27001:2022**
  - 8.21 Seguridad de los servicios de red.

- 8.23 Filtrado de Webs

Categoría: MEDIA
Nivel de medidas Compatible: **Parcialmente análogo**

Particularidades de la ISO:

Las redes y los dispositivos de red se asegurarán, administrarán y controlarán para proteger la información en los sistemas y aplicaciones. 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.

Recomendación Implantación:

Aunque el control de la ISO incluye la propia protección de los servicios IDS / IPS, se debe considerar específicamente el despliegue de herramientas y/o funcionalidades de detección y/o prevención de intrusiones basadas en reglas, siendo suficiente contar con dispositivos de red configurados para poder realizar una monitorización. Lo servicios SaaS incluirán necesariamente estas medidas como parte del servicio.

[op.mon.2] Sistema de métricas

- **Control Principal ISO/IEC 27001:2022**
  - 9 – Evaluación del desempeño
- **Controles Complementarios ISO/IEC 27001:2022**
  - 9.1 Seguimiento, medición, análisis y evaluación

Categoría: MEDIA
Nivel de medidas Compatible: **Parcialmente análogo**

Particularidades de la ISO:

La organización deberá evaluar el desempeño de seguridad de la información y la eficacia del sistema de gestión de seguridad de la información. La organización debe determinar, quien, cuando, que y como, debe monitorizarse.

Las métricas pueden servir para ambos sistemas, pero a efectos de la ISO, deben incluirse el seguimiento de los objetivos de seguridad.

Recomendación Implantación:

Se debe imponer el criterio de ENS para recopilar las métricas requeridas, se deberá tener en cuenta lo indicado en la Guía de Seguridad de las TIC CCN-STIC 817. La entidad debe mantener una medición relacionada con el grado de implantación de las medidas de seguridad y, en su caso, en aquellas entidades públicas deberá realizar el informe anual de estado de seguridad, mediante la plataforma INES. Además, es conveniente tener en cuenta las mediciones de niveles de madurez y niveles de implantación conforme a la Guía CCN-STIC 808.

Se consideran las mediciones derivadas de [op.exp.9] y análisis de los recursos, horas y presupuesto para la seguridad.

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, considerando la Cláusula 6.2 Objetivos de seguridad de la Información y planificación para su consecución; estos han de ser medibles (si es posible). Para lograr las medidas compatibles deben considerarse los objetivos de seguridad y métricas apropiadas.

[op.mon.3] Vigilancia

- **Control Principal ISO/IEC 27001:2022**
  - 5.7 Inteligencia de amenazas
- **Controles Complementarios ISO/IEC 27001:2022**
  - 8.8 Gestión de vulnerabilidades técnicas
  - 8.16 Seguimiento de actividades

Categoría: MEDIA
Nivel de medidas Compatible: **Análogo**
Particularidades de la ISO:

Se recopilará información relacionada con las amenazas a la seguridad y se analizaran para generar información.

Recomendación Implantación:

Se dispondrá de un sistema automático de recolección y correlación de eventos de seguridad, servicios / arquitectura. Este servicio puede ser desarrollado directamente por la entidad o puede ser contratado a un tercero. Es algunas ocasiones los servicios en la nube incluirán este servicio como elemento añadido.

La entidad además deberá disponer de soluciones de vigilancia que permitan determinar la superficie de exposición con relación a vulnerabilidades y deficiencias de configuración. Esta funcionalidad de seguridad puede ser también un servicio externalizado y gestionado por un tercero. Estas soluciones de vigilancia permitirán determinar la superficie de exposición en relación con vulnerabilidades y deficiencias de configuración. Es conveniente consultar las soluciones del CCN y en todo caso, considerar los análisis de CVE mediante fuentes y listas oficiales. La organización podría considerar los avisos de vulnerabilidades, y considerarlo para los análisis de riesgos y analizar los impactos derivados. En todo caso es recomendable mantener un sistema de fuentes amplio, mediante información suministrada por diferentes agentes, tales como proveedores o asesores independientes, autoridades de control o grupos de expertos de inteligencia de amenazas.

Un elemento significativo para tener en cuenta es el formato disponible para los logs y eventos del sistema, para que éstos puedan ser almacenados con un formato estandarizado, susceptible de ser explotados por correladores o syslog.

Las entidades pueden consultar las diferentes herramientas disponibles en el CCN para la gestión de este control.

Para la ISO hablamos de inteligencia de amenazas y requiere conexión con los controles 5.25 Evaluación y decisión sobre los eventos de seguridad de la información, 8.7 Controles contra el

código malicioso, 8.8 Gestión de vulnerabilidades técnicas; 8.16 Seguimiento de actividades o 8.23 Filtrado web, para mantener la calidad de la información sobre amenazas.

6.3 [MP] MEDIDAS DE PROTECCIÓN

[MP.IF] PROTECCIÓN DE LAS INSTALACIONES E INFRAESTRUCTURAS

[mp.if.1] Áreas separadas y con control de acceso

- **Control Principal ISO/IEC 27001:2022**
  - 7.1 Perímetro de seguridad física
- **Controles Complementarios ISO/IEC 27001:2022**
  - 7.3 Seguridad de oficinas, despachos y recursos
  - 7.6 El trabajo en áreas seguras

Categoría: MEDIA
Nivel de medidas Compatible: **Análogo**
Particularidades de la ISO:

Existirán perímetros de seguridad, en las zonas con protección según la información y/o activos que contienen.

Recomendación Implantación:

"Centro de Proceso de Datos (CPD) se instalará, en la medida de lo posible, en áreas separadas específicas, y los accesos serán controlados. Es posible que no exista esta instalación a nivel de infraestructura, bien porque la entidad haya externalizado a un tercero los servicios de alojamiento (housing / hosting), bien porque se esté trabajando con servicios cloud (IaaS, PaaS, SaaS) o bien por que la propia infraestructura dependa de otra entidad. Las entidades deben analizar el impacto del control y mantener los requerimientos de ambas normas. En todo caso, las medidas de seguridad deben considerarse extendidas a los centros de procesamiento de datos y a las salas de comunicaciones o de interconexión. Se debe considerar el cumplimiento para la infraestructura propia y en su caso, requerir a los proveedores y servicios en la nube el cumplimiento de estos. 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 de las 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

- **Control Principal ISO/IEC 27001:2022**
  - 7.2 Controles físicos de entrada
- **Controles Complementarios ISO/IEC 27001:2022**
  - 7.1 Perímetro físico de seguridad
  - 7.6 El trabajo en áreas seguras

Categoría: MEDIA
Nivel de medidas Compatible: Análogo
Particularidades de la ISO:

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.".

Recomendación Implantación:

Se identificará a las personas que accedan a las infraestructuras de procesamiento de datos y comunicaciones, registrando las correspondientes entradas y salidas.

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

- **Control Principal ISO/IEC 27001:2022**
  - 7.5 Protección contra las amenazas externas y ambientales.
- **Controles Complementarios ISO/IEC 27001:2022**
  - 7.3 Seguridad de oficinas, despachos y recursos
  - 7.6 El trabajo en áreas seguras
  - 7.8 Emplazamiento y protección de equipos
  - 7.12 Seguridad del cableado

Categoría: MEDIA
Nivel de medidas Compatible: Parcialmente análogo

Particularidades de la ISO:

Para obtener una compatibilidad total se debe considerar el mismo, junto a otros controles.

La protección contra las amenazas externas y ambientales, intencionales o no intencionales, deberá ser diseñada e implementada.

Recomendación Implantación:

Se considerarán las propias condiciones de las oficinas y específicamente, acondicionamientos derivados de prevención, del AARR y problemas derivados de cableados y armarios de comunicaciones. Se realizarán revisiones y controles respecto a:

[mp.if.3.1] Las condiciones de temperatura y humedad.

[mp.if.3.2] La protección frente a las amenazas identificadas en el análisis de riesgos.

[mp.if.3.3] La protección del cableado frente a incidentes fortuitos o deliberados.

El cumplimiento de este control mediante la ISO recae en varios controles. Seguridad de oficinas, despachos y recursos; 7.8 Emplazamiento y protección de equipos; 7.12 Seguridad del cableado

Así el control 7.8 Emplazamiento 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, 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

- **Control Principal ISO/IEC 27001:2022**
  - 7.11 Instalaciones de suministro
- **Controles Complementarios ISO/IEC 27001:2022**
  - 7.12 Seguridad del cableado
  - 5.30 Preparación de las TIC para la continuidad del negocio

Categoría: MEDIA
Nivel de medidas Compatible: **Análogo**
Particularidades de la ISO:

Las instalaciones de procesamiento de información deben estar protegidas contra cortes de energía y otras interrupciones causadas por fallos en los servicios de soporte.

Recomendación Implantación:

Se dispondrá de tomas de energía eléctrica suficiente y se podrá garantizar el suministro y el funcionamiento de las luces de emergencia. Se considerarán regletas preparadas frente a picos de tensión o SAI a nivel de equipos instalados en las oficinas.

Con la información disponible deberemos desplegar el análisis de riesgos y contemplar los impactos.

Es una buena estrategia contemplar pruebas asociadas a [op.cont] para poder evidenciar la redundancia y robustez del sistema de apoyo. Es conveniente que se asocie al mantenimiento [op.exp.4] y en su caso cambios [op.exp.5], elementos claves como baterías, reparaciones... ".

[mp.if.5] Protección frente a incendios

- **Control Principal ISO/IEC 27001:2022**
  - 7.5 Protección contra las externas y ambientales
- **Controles Complementarios ISO/IEC 27001:2022**
  - 7.3 Seguridad de oficinas, despachos y recursos
  - 7.6 El trabajo en áreas seguras

Categoría: MEDIA
Nivel de medidas Compatible: **Análogo**
Particularidades de la ISO:

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.

Recomendación Implantación:

Se considerarán las propias condiciones de las oficinas y específicamente, acondicionamientos derivados de prevención de riesgos. Tales medidas suelen estar documentadas y "testeadas" por el proceso de prevención de riesgos.

La información disponible debe enriquecer el análisis de riesgos y contemplar los impactos.

[mp.if.6] Protección frente a inundaciones

- **Control Principal ISO/IEC 27001:2022**
  - 7.5 Protección contra las externas y ambientales
- **Controles Complementarios ISO/IEC 27001:2022**
  - 7.3 Seguridad de oficinas, despachos y recursos
  - 7.6 El trabajo en áreas seguras

Categoría: MEDIA
Nivel de medidas Compatible: **Análogo**
Particularidades de la ISO:

Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso apropiados.

Recomendación Implantación:

Ambas normas exigen en paralelo las mismas obligaciones y en este sentido se debe requerir a un registro que permita la trazabilidad [de entrada y salida] del equipamiento esencial (para centros de procesamiento de datos). Se incluirá la identificación de la persona que autoriza el movimiento. 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 implementar un proceso de cotejo, de manera que las entregas se contrasten contra el albarán, se analice si hay evidencia de manipulación del paquete y en su caso inspeccione en busca de materiales peligrosos o manipulación no permitida.

Las entradas deben estar trazadas con la gestión de activos [op.exp.1] y control 5.9 y control 7.10 de la ISO.

[mp.if.7] Registro de entrada y salida de equipamiento

- **Control Principal ISO/IEC 27001:2022**
  - 7.2 Controles físicos de entrada
- **Controles Complementarios ISO/IEC 27001:2022**
  - 7.3 Seguridad de oficinas, despachos y recursos

- 7.6 El trabajo en áreas seguras

Categoría: MEDIA
Nivel de medidas Compatible: Análogo
Particularidades de la ISO:

Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso apropiados.

Recomendación Implantación:

Ambas normas exigen en paralelo las mismas obligaciones y en este sentido se debe requerir a un registro que permita la trazabilidad [de entrada y salida] del equipamiento esencial (para centros de procesamiento de datos). Se incluirá la identificación de la persona que autoriza el movimiento. 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 implementar un proceso de cotejo, de manera que las entregas se contrasten contra el albarán, se analice si hay evidencia de manipulación del paquete y en su caso inspeccione en busca de materiales peligrosos o manipulación no permitida.

Las entradas deben estar trazadas con la gestión de activos [op.exp.1] y control 5.9 y control 7.10 de la ISO.

[MP.PER] GESTIÓN DEL PERSONAL

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

- **Control Principal ISO/IEC 27001:2022**
  - 6.1 Comprobación
- **Controles Complementarios ISO/IEC 27001:2022**
  - 6.2 Términos y condiciones de contratación
  - 5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información

Categoría: MEDIA
Nivel de medidas Compatible: Análogo
Particularidades de la ISO:

Es necesario realizar verificaciones previas de los antecedentes de todos los candidatos para convertirse en personal, 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 información a la que se accede y los riesgos percibidos.

Este control debe complementarse con Términos y condiciones de contratación.

Recomendación Implantación:

Ambas normas trabajan en sintonía, teniendo en cuenta que la necesidad ISO puede no ser aplicable en toda su magnitud cuando existan procesos de personal previos [provisiones de

puestos en el sector público] que ya haya cotejado previamente la información a verificar. Si se deben considerar las verificaciones de idoneidad en el puesto y competencia en relación con la necesaria para desempeñar la función de seguridad que pueda llevar aparejada y muy especialmente la confidencialidad.

A nivel del ENS, no entra a valorar los antecedentes de los usuarios al sistema, más allá de aquellos que hagan referencia a las necesidades de seguridad. Es importante establecer una asignación de recursos humanos (apropiados y capacitados) en consideración con [op.pl.4], con una clara separación de funciones (considerar los controles [org.4] y [op.acc.3]), así como la definición de las atribuciones (y especialmente para el sector público, mediante los correspondientes procesos administrativos RPT).

Además, se han de considerar otras medidas como las acciones de formación (mp.per.4), problemas relacionados con la [alta] rotación [op.pl.1].

[mp.per.2] Deberes y obligaciones

- **Control Principal ISO/IEC 27001:2022**
  - Términos y condiciones de contratación
- **Controles Complementarios ISO/IEC 27001:2022**
  - 6.4 Proceso disciplinario
  - 6.5 Responsabilidades ante la finalización o el cambio
  - 5.11 Devolución de activos
  - 6.6 Acuerdos de confidencialidad o no divulgación

Categoría: MEDIA
Nivel de medidas Compatible: **Parcialmente análogo**

Particularidades de la ISO:

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.

Recomendación Implantación:

Aunque el ENS es más estricto en este control, ambas normas pueden alinearse claramente. Se informará a cada persona con acceso al sistema, de los deberes y responsabilidades derivados de su puesto y funciones, en materia de seguridad.

Se gestionará el reporte con la información precisa y se evidenciará la recepción y el acceso a los procedimientos asociados a sus funciones y accesos. Se dará a conocer la responsabilidad en caso de desviación de las instrucciones o incumplimiento.

Se deben considerar las previsiones derivadas de la normativa sectorial asociada a personal de una entidad pública y la debida confidencialidad. Es recomendable que se trabajen los procesos de acogida de las personas usuarias [Bienvenida, Onboarding o Welcome], teniendo en cuenta a los usuarios "externos" (personal de proveedores) en el que se incluya toda la información requerida para el acceso y manejo del sistema, y de la información / servicios.

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

- **Control Principal ISO/IEC 27001:2022**
  - 6.3 Concienciación, educación y formación en seguridad de la información
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información.

Categoría: MEDIA
Nivel de medidas Compatible: **Análogo**
Particularidades de la ISO:

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.

Recomendación Implantación:

Se realizarán acciones para concienciar regularmente, sobre la normativa de seguridad, el procedimiento de incidentes y técnicas de ingeniería social.

Las organizaciones deben disponer de un plan, en el que incluyan las previsiones de 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. Para estas evaluaciones se debería considerar, no solo la visión del usuario, sino de los responsables y personas con relevancia en la seguridad. Se debería considerar la evolución de la concienciación, mediante ciertas métricas e indicadores.

Periódicamente el CCN actualiza documentos y seminarios, e incluye sus herramientas (por ejemplo, ELENA y ATENEA) que pueden ayudar en este proceso. Existen más entidades y autoridades de seguridad que también pueden ayudar en la concienciación (INCIBE, ENISA...) y efectividad de este control.

[mp.per.4] Formación

- **Control Principal ISO/IEC 27001:2022**

- 6.3 Concienciación, educación y formación en seguridad de la información

- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información

Categoría: MEDIA
Nivel de medidas Compatible: Análogo
Particularidades de la ISO:

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.

Recomendación Implantación:

El personal con funciones críticas en seguridad debería mantener una capacitación actualizada en materia de configuración de sistemas.

Las personas con acceso al sistema deben conocer y estar formados en la detección y reacción ante incidentes, así como en la gestión de la información (almacenamiento, transferencia, copias, distribución y destrucción).

Se evaluará la eficacia de las acciones formativas llevadas a cabo.

Se debe desarrollar un plan de formación anual, que incluya las acciones previstas. Las acciones de formación pueden tener diferentes modalidades, y tener temarios diferenciados. El CCN dispone de herramientas que pueden ayudar a ello y otras autoridades de seguridad también (INCIBE, ENISA...). Pueden aprovecharse acciones de formación, presentes en las plataformas del CCN, como por ejemplo VANESA.

Por último, no se debe olvidar la responsabilidad de formación para el personal de terceros con acceso al sistema de la entidad, por lo que se deberá acordar y vigilar, la correspondiente acción de formación en seguridad.

[MP.EQ] PROTECCIÓN DE LOS EQUIPOS

[mp.eq.1] Puesto de trabajo despejado

- **Control Principal ISO/IEC 27001:2022**
  - 7.7 Puesto de trabajo despejado y pantalla limpia

- **Controles Complementarios ISO/IEC 27001:2022**
  - 7.3 Seguridad de oficinas, despachos y recursos
  - 7.8 Emplazamiento y protección de equipos
  - 5.10 Uso aceptable de información y activos asociados

Categoría: MEDIA
Nivel de medidas Compatible: Análogo
Particularidades de la ISO:

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 de la organización

Recomendación Implantación:

Ambas normas están en clara sinergia por lo que se debe considerar la protección de la información (especialmente aquella que por las funciones desarrolladas deba someterse a confidencialidad o se considere sensible o crítica, considerando en todo caso el control [mp.info.2]).

Los puestos de trabajo permanecerán despejados, manteniendo en uso, exclusivamente de aquella información necesaria en cada momento, y que será almacenada en un lugar seguro siempre que se pueda.

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 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 información y activos asociados y 5.36 Cumplimiento de las políticas y normas de seguridad de la seguridad de la información.

Las acciones de sensibilización deben trabajar esta medida.

[mp.eq.2] Bloqueo del puesto de trabajo

- **Control Principal ISO/IEC 27001:2022**
  - 7.7 Puesto de trabajo despejado y pantalla limpia
- **Controles Complementarios ISO/IEC 27001:2022**
  - 8.9 Gestión de la configuración
  - Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deberán ser establecidas, documentadas, implementadas, monitorizadas y revisadas.

Categoría: MEDIA
Nivel de medidas Compatible: Análogo
Particularidades de la ISO:

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 de la organización.

Recomendación Implantación:

A nivel de ambas normas, al menos se considerará la categoría MEDIA. Esto implica necesariamente trazar medidas técnicas para que los equipos y dispositivos y servicios, se desconecten o protejan 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.

Se debería al menos, desplegar esta política en el directorio y desplegarlo desde el bastionado inicial del componente [op.exp.2], elaborando una Instrucción Técnica [org.3] que lo desarrolle, y se comprobará la efectividad cada cierto tiempo [op.exp.3].

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.

En base a los riesgos detectados, puede ser recomendable desplegar el 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.

[mp.eq.3] Protección de equipos portátiles

- **Control Principal ISO/IEC 27001:2022**
  - 8.1 Dispositivos finales de usuario
- **Controles Complementarios ISO/IEC 27001:2022**
  - 7.9 Seguridad de los equipos fuera de las instalaciones
  - 5.9 Inventario de información y otros activos asociados.
  - 5.12 Clasificación de información
  - 5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información
  - 5.25 Evaluación y decisión sobre los eventos de seguridad de la información

Categoría: ALTA *
Nivel de medidas Compatible: **Parcialmente análogo**

Particularidades de la ISO:

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.

Recomendación Implantación:

Ambas normas convergen en la seguridad de este tipo de dispositivos, si bien se debería considera la categoría ALTA, en base a la derivación del control [mp.info.2] 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. Este punto debe ser asociado al control [mp.info.2]. Asimismo, se deberá tener en cuenta los riesgos detectados [op.pl.1].

Refuerzo R1 – Cifrado del disco, [mp.eq.3.r2.1]; si del inventario de información se contempla que la misma tiene un nivel MEDIO. Se debe considerar de manera muy precisa, la valoración de la información con sus responsables de información.

Además, debe considerarse especialmente la gestión de incidentes de seguridad [op.exp.7], controles ISO 5.24, 5.26 y el control de acceso desde fuera de zonas confiables [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. En el caso de accesos remotos, se deberá considerar el 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.

Para el proceso de cifrado se debe considerar, el cifrado del mismo como indica el Refuerzo R1 – Cifrado del disco, si del inventario de información se contempla que la misma tiene un nivel MEDIO. En tal caso se considerará CCN-STIC-105 Catálogo de Productos y Servicios de Seguridad de las TIC 7.5.1 FAMILIA: ALMACENAMIENTO CIFRADO DE DATOS

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 personal);

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

- **Control Principal ISO/IEC 27001:2022**
  - 8.1 Dispositivos finales de usuario
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.9 Inventario de información y otros activos asociados.
  - 5.12 Clasificación de información
  - 8.9 Gestión de la configuración

Categoría: MEDIA
Nivel de medidas Compatible: **Parcialmente análogo**

Particularidades de la ISO:

Considerar el proceso de configuración y el manejo seguro por los usuarios.

Recomendación Implantación:

Este control implica necesariamente considerar estos dispositivos en [op.exp.2] y [op.exp.3] y mantener las comprobaciones precisas. Se incluirán como componentes configurados de manera segura, los dispositivos conectados a la red y que puedan tener el algún momento acceso a la información (dispositivos multifunción y multimedia, y los dispositivos [IoT], BYOD, etc.) conforme a los citados [op.exp.2 y 3] y cuando permitan el almacenamiento de información, proporcionarán la funcionalidad para eliminar, de manera segura [mp.si.5] Borrado y destrucción.

A medida que se inicien procesos de renovación del parque de dispositivos afectados por este control, se adquirirán productos contenidos en el catálogo CCN STIC 105 o en su caso, certificación de seguridad análogo.

Debe incluirse el R1 que, si bien no está contemplado en la ISO, debe ser aplicado para el ENS. Se deberán realizar verificaciones por pliegos de los componentes [op.pl.5].

[MP.COM] PROTECCIÓN DE LAS COMUNICACIONES

[mp.com.1] Perímetro seguro

- **Control Principal ISO/IEC 27001:2022**
  - 8.20 Seguridad de redes
- **Controles Complementarios ISO/IEC 27001:2022**
  - 8.21 Seguridad de los servicios de red
  - 8.9 Gestión de la configuración

Categoría: MEDIA
Nivel de medidas Compatible: **Parcialmente análogo**

Particularidades de la ISO:

Las redes deben administrarse y controlarse para proteger la información en los sistemas y aplicaciones.

Recomendación Implantación:

Se dispondrá de un sistema de protección mediante Firewall [ver op.pl.5], autorizándose los flujos [org.4] y tomando en consideración los requisitos contenidos en la Instrucción Técnica de Seguridad de Interconexión de Sistemas de Información [op.ext.4]. 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 importante 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

- **Control Principal ISO/IEC 27001:2022**
  - 8.21 Seguridad de los servicios de red
- **Controles Complementarios ISO/IEC 27001:2022**
  - 8.20 Seguridad de redes
  - 8.24 Uso de la criptografía
  - 8.9 Gestión de la configuración
  - 8.26 Requisitos de seguridad de las aplicaciones

Categoría: MEDIA
Nivel de medidas Compatible: **Parcialmente análogo**
Particularidades de la ISO:

Los mecanismos de seguridad, los niveles de servicio y los requisitos de los servicios de red, deben identificarse, implementarse y monitorizarse.

Recomendación Implantación:

Se emplearán redes VPN con algoritmos y parámetros autorizados por el CCN (Ver Guía CCN STIC 807 y Guía CCN STIC 221). La organización debe garantizar que se apliquen los controles de seguridad adecuados al uso de redes virtualizadas, incluidas las redes SDN, SD-WAN. Se pueden considerar diferentes modalidades, VPN TLS, IPSEC, MACSEC, WIREGUARD. Todas las redes estarán inventariadas y las VPN deberán ser controladas, gestionadas e inhabilitadas cuando cesen en su necesidad.

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 y la recomendación de algoritmo de cifrado 128 cifrado simétrico. AES

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.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.

Pueden considerarse los requisitos en la Guía CCN-STIC-836 ENS - Seguridad en VPN.

[mp.com.3] Protección de la autenticidad y de la integridad

- **Control Principal ISO/IEC 27001:2022**
  - 8.21 Seguridad de los servicios de red
- **Controles Complementarios ISO/IEC 27001:2022**
  - 8.20 Seguridad de redes
  - 8.24 Uso de la criptografía
  - 8.9 Gestión de la configuración
  - 8.26 Requisitos de seguridad de las aplicaciones

Categoría: MEDIA
Nivel de medidas Compatible: **Parcialmente análogo**
Particularidades de la ISO:

Los mecanismos de seguridad, los niveles de servicio y los requisitos de los servicios de red, deben identificarse, implementarse y monitorizarse.

Recomendación Implantación:

En comunicaciones con puntos exteriores al dominio propio de seguridad, se asegurará la autenticidad del otro extremo, [op.acc.5] e incluirá mecanismo de autenticación (usuarios externos), lo que conlleva emplear contraseñas y otro elemento (OTP /certificado) y mantener el registro operativo. Se emplearán redes VPN conforme algoritmos y parámetros autorizados por el CCN (Ver Guía CCN STIC 807 y Guía CCN STIC 221). La organización debe garantizar que se apliquen los controles de seguridad adecuados al uso de redes virtualizadas, incluidas las redes SDN, SD-WAN. Se pueden 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 y la 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. Es conveniente que se revisen periódicamente, se compruebe su necesidad y se restrinja en todo caso cuando dejen de ser necesarias.

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.

Pueden considerarse los requisitos en la Guía CCN-STIC-836 ENS - Seguridad en VPN".

[mp.com.4] Separación de flujos de información en la red

- **Control Principal ISO/IEC 27001:2022**
  - 8.22 Segregación en redes
- **Controles Complementarios ISO/IEC 27001:2022**
  - 8.20 Seguridad de redes
  - 8.27 Arquitectura segura de sistemas y principios de ingeniería
  - 5.9 Inventario de información y otros activos asociados

Categoría: MEDIA
Nivel de medidas Compatible: **Análogo**
Particularidades de la ISO:

Las redes deben dividirse en dominios y ""separarse"" de la red pública (es decir, Internet).

Las agrupaciones pueden hacerse por confianza, criticidad, sensibilidad, organización, etc., y mediante red física o lógica.

Recomendación Implantación:

Se realizarán segmentaciones de la red, acotando accesos y limitando riesgos de propagación, mediante medios lógicos, área local virtuales (Virtual Local Area Network VLAN), redes privadas virtuales (Virtual Private Network VPN) o medios físicos separados.

Las redes inalámbricas, será en un segmento separado. La red del sistema deberá segregarse al menos, en red de usuarios, red de servicios y red de administración.

El diagrama que permita visualizar la segmentación y la información precisa de la red constará documentada y actualizada en la información de la arquitectura [op.pl.2]

Cuando por razones de tamaño y capacidad, no pueda gestionarse una segregación a los efectos del control, podrá estudiarse la viabilidad de segregar las redes en menos puntos, por ejemplo, VLAN para una red de administración y una VLAN de usuarios internos.

La red wifi debe ser segregada o anulada.

Pueden considerarse los requisitos en la Guía CCN-STIC-836 ENS - Seguridad en VPN y CCN-STIC-816 Seguridad en Redes Inalámbricas en el ENS.

[MP.SI] PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN

[mp.si.1] Marcado de soportes

- **Control Principal ISO/IEC 27001:2022**
  - 5.13 Etiquetado de la información
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.12 Clasificación de información
  - 7.10 Soportes de almacenamiento
  - 8.12 Prevención de fuga de datos

Categoría: MEDIA
Nivel de medidas Compatible: **Análogo**
Particularidades de la ISO:

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.

Recomendación Implantación:

Dada la flexibilidad que otorga la ISO, se debe adoptar las premisas dadas por el ENS, desplegando el esquema derivado de la información y valoración efectuada. Se considerará el etiquetado necesario y cómo colocarlo en documentos papel y digital (metadatos). Este control se conectará con el control limpieza de metadatos [mp.info.5]. Se colocarán marcas de agua en la documentación, referente a la calificación de estos como USO OFICIAL [mp.info.2]. La entidad debe desplegar un proceso asociado a [mp.info.2] y considerar los procedimientos operativos correspondientes [org.3].

El personal y otras partes interesadas deben conocer los procedimientos de etiquetado, por lo que todo el personal debe recibir la capacitación necesaria para garantizar que la información se etiquete correctamente y se manipule, en consecuencia. Esto debe estar conectado con la concienciación [mp.per.3] y formación [mp.per.4].

[mp.si.2] Criptografía

- **Control Principal ISO/IEC 27001:2022**
  - 8.24 Uso de criptografía
- **Controles Complementarios ISO/IEC 27001:2022**

- 8.13 Copias de seguridad de la información
- 8.12 Prevención de fugas de datos
- 7.9 Seguridad de los equipos fuera de las instalaciones
- 7.10 Soportes de almacenamiento

Categoría: MEDIA (+R2) *
Nivel de medidas Compatible: **Parcialmente análogo**

Particularidades de la ISO:

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.

Recomendación Implantación:

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 (Ver Guía CCN STIC 807 y Guía CCN STIC 221). Se deberá cifrar aquellos dispositivos que salgan de las instalaciones, especialmente si son copias.

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 debe considerar el control [op.pl.5] que derivará hacia una aplicación colateral del Refuerzo R1– Productos certificados [mp.si.2.r1.1] Se emplearán productos certificados conforme a lo establecido en [op.pl.5].

[mp.si.3] Custodia

- **Control Principal ISO/IEC 27001:2022**
  - 7.10 Soportes de almacenamiento
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.9 Inventario de información y otros activos asociados
  - 5.10 Uso aceptable de la información y activos asociados
  - 5.11 Devolución de activos
  - 6.3 Concienciación, educación y formación en seguridad de la información
  - 8.12 Prevención de fugas de datos

Categoría: MEDIA
Nivel de medidas Compatible: **Análogo**
Particularidades de la ISO:

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.

Recomendación Implantación:

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. Los medios deben almacenarse en un entorno seguro y protegido de acuerdo con la calificación de la información y, protegidos contra amenazas ambientales (como calor, humedad, campo electrónico o envejecimiento), de acuerdo con las especificaciones de los fabricantes.

Se desplegarán medidas físicas y lógicas para evitar usos indebidos.

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] y 7.13 Mantenimiento de equipo (El equipamiento deberá ser mantenido adecuadamente para garantizar la disponibilidad, integridad y confidencialidad de la información.)

Es recomendable tener en cuenta las buenas prácticas que se describen en la ISO 27002, ya que pueden enriquecer el cumplimiento de este control. 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

- **Control Principal ISO/IEC 27001:2022**
  - 7.10 Soportes de almacenamiento
- **Controles Complementarios ISO/IEC 27001:2022**
  - 8.24 Uso de criptografía
  - 8.12 Prevención de fugas de datos
  - 7.2 Controles físicos de entrada

Categoría: MEDIA
Nivel de medidas Compatible: **Análogo**
Particularidades de la ISO:

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.

Recomendación Implantación:

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.

Se considerará este procedimiento de gestión, bajo la tutela del Responsable del Sistema, y se considerará un registro de entradas y salidas, donde se cotejará el movimiento de elementos. Este registro tiene especial conexión con el asociado a [mp.if.7]

Cuando por razón de la información que contenga sea preciso [mp.si.2] se emplearán cifrados y se gestionarán las claves [op.exp.10].

Este punto tendrá muy en cuenta 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. La información considerada confidencial por la normativa europea gozará de esta presunción.

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 con 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 o campos electromagnéticos;

d) utilizar controles a prueba de manipulaciones o a prueba de manipulaciones.

[mp.si.5] Borrado y destrucción

- **Control Principal ISO/IEC 27001:2022**
  - 7.10 Soportes de almacenamiento
- **Controles Complementarios ISO/IEC 27001:2022**
  - 8.10 Eliminación de información
  - 8.12 Prevención de fugas de datos
  - 7.10 Soportes de almacenamiento

Categoría: MEDIA
Nivel de medidas Compatible: Análogo
Particularidades de la ISO:

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.

Recomendación Implantación:

Ambas normas convergen y requieren a nivel general, que la organización establezca 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.

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 trituración. Se deben registrar los resultados de la eliminación y borrado como prueba y evidencia.

[MP.SW] PROTECCIÓN DE LAS APLICACIONES INFORMÁTICAS (SW)

[mp.sw.1] Desarrollo de aplicaciones

- **Control Principal ISO/IEC 27001:2022**
  - 8.25 Seguridad en el ciclo de vida del desarrollo
- **Controles Complementarios ISO/IEC 27001:2022**
  - 8.28 Codificación segura
  - 8.29 Pruebas de seguridad en desarrollo y aceptación.
  - 8.31 Separación de los entornos de desarrollo, prueba y producción
  - 8.32 Gestión del cambio
  - 8.4 Acceso al código fuente
  - 8.30 Externalización del desarrollo
  - 8.27 Arquitectura segura de sistemas y principios de ingeniería
  - 5.8 Seguridad de la información en la gestión de proyectos

Categoría: MEDIA
Nivel de medidas Compatible: **Análogo**

Particularidades de la ISO:

Deben establecerse y aplicarse reglas para el desarrollo seguro de software y sistemas.

Recomendación Implantación:

Se deben mantener los entornos de desarrollo y producción separados y cumplir con el principio de mínimo privilegio y evitar el uso de datos reales para pruebas.

Cuando una entidad no realice directamente desarrollo debe considerar requerir a proveedores de software, su cumplimiento y en su caso, las pruebas que puedan realizarse.

Las pruebas previas a implantación o modificación de sistemas de información, preferentemente no se realizarán con datos reales; en caso de que fuese necesario recurrir a datos reales, se garantizará el nivel de seguridad correspondiente. Es posible que ciertos servicios electrónicos sean en modo SaaS por lo que se debe considerar como proveedor. [ver op.nub.1].

Para el enriquecimiento de este control se considerarán;

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 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

- **Control Principal ISO/IEC 27001:2022**
  - 8.29 Pruebas de seguridad en desarrollo y aceptación
- **Controles Complementarios ISO/IEC 27001:2022**
  - 8.31 Separación de los entornos de desarrollo, prueba y producción
  - 8.32 Gestión del cambio
  - 8.33 Datos de Prueba
  - 8.11 Enmascaramiento de datos
  - 8.30 Externalización del desarrollo

- 8.27 Arquitectura segura de sistemas y principios de ingeniería
- 5.8 Seguridad de la información en la gestión de proyectos

Categoría: MEDIA
Nivel de medidas Compatible: **Parcialmente análogo**

Particularidades de la ISO:

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.

Recomendación Implantación:

Ambas normas requieren entornos de pruebas, desarrollo y [pre]producción diferenciados. Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación y de otros elementos, manteniéndose los criterios de seguridad.

Para ello se pueden considerar pruebas básicas mediante una lista de validación, presentando al Responsable de Seguridad los resultados y asociado a Gestión del Cambio [op.exp.5]. Se considerarán pruebas para versionados y parches, que serán probados en un entorno controlado. Deben considerarse 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 a nivel de entidad pública o filiales dependan de otra entidad, por cuanto, en ambos casos, el control derivará en su cumplimiento a los mismos.

Además, se debe realizar la codificación y configuraciones seguras, incluida la de los sistemas operativos, firewalls y otros componentes de seguridad.

Se considerarán actividades de revisión de código para detectar fallos 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. Debe considerarse planes [anuales] para la realización de auditorías y revisiones en este sentido.

[MP.INFO] PROTECCIÓN DE LA INFORMACIÓN

[mp.info.1] Datos personales

- **Control Principal ISO/IEC 27001:2022**
  - 5.34 Privacidad y protección de datos de carácter personal (DCP)
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.31 Identificación de requisitos legales, reglamentarios y contractuales

Categoría: MEDIA
Nivel de medidas Compatible: **Análogo**
Particularidades de la ISO:

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.

Recomendación Implantación:

Debe considerarse las obligaciones derivadas del legislador europeo y la necesidad de dar cumplimiento. Debe considerarse la figura del Delegado de Protección de Datos que puede ser compartida con otras entidades públicas.

Es posible que, en los procesamientos u operaciones de tratamiento de datos, participen terceros que deberán acreditar el cumplimiento de la normativa de referencia. 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

- **Control Principal ISO/IEC 27001:2022**
  - 5.12 Clasificación de la información
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.13 Etiquetado de información
  - 5.14 Transferencia de información
  - 5.15 Control de acceso
  - 5.9 Inventario de información y otros activos asociados.
  - 5.10 Uso aceptable de información y activos asociados
  - 8.12 Prevención de fugas de datos

Categoría: MEDIA
Nivel de medidas Compatible: **Análogo**
Particularidades de la ISO:

La información deberá ser clasificada de acuerdo con las necesidades de seguridad de la información de la organización, en función en confidencialidad, integridad, disponibilidad y requisitos de las partes interesadas.

Recomendación Implantación:

Dada la flexibilidad de la ISO se impondrá el criterio del ENS. La política de calificación determinará los criterios que, determinarán el nivel de seguridad requerido, dentro del marco regulador 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.

Es importante designar responsable de información y trazar en la política los criterios de valoración conforme a la normativa implicada. 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.

Debe considerarse el Marcado de soportes [mp.si.1] y el impacto que este control implica.

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.

[mp.info.3] Firma electrónica

- **Control Principal ISO/IEC 27001:2022**
  - 8.24 Uso de la criptografía
- **Controles Complementarios ISO/IEC 27001:2022**
  - 8.26 Requisitos de seguridad de las aplicaciones
  - 5.31 Identificación de requisitos legales, reglamentarios y contractuales

Categoría: MEDIA
Nivel de medidas Compatible: **Nula**
Particularidades de la ISO:

Este no es un control especifico de la ISO, pero lo asociamos a ciertos controles, considerando 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.

Recomendación Implantación:

La ISO no considera este control, pero puede asociarse a los controles 8.26 y 8.24. Se considerará cumplida la medida cuando se emplee cualquier firma válida en la normativa vigente. Se deben gestionar controles sobre la misma y el uso aceptable.

Es importante considerar los siguientes refuerzos:

Refuerzo R1 – Certificados cualificados: Cuando se use firma electrónica avanzada basada en certificados, estos serán cualificados. Serán prestadores cualificados quienes emitan las mismas, conforme a la normativa europea en vigor.

Refuerzo R2 – Algoritmos y parámetros autorizados: El CCN determinará los algoritmos criptográficos que hayan sido autorizado.

Refuerzo R3 – Verificación y validación de firma: Se garantizará la verificación y validación de la firma durante el tiempo requerido.

Se debe desplegar una política o adscribirse a la de la entidad administrativa superior. Es importante que se gestione la custodia y uso de la firma. En este sentido 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.

Pueden tenerse en cuenta por aplicación directa del control [op.pl.5] componentes certificados.

[mp.info.4] Sellos de tiempo

- **Control Principal ISO/IEC 27001:2022**
  - 8.26 Requisitos de seguridad de las aplicaciones
- **Controles Complementarios ISO/IEC 27001:2022**
  - 8.17 Sincronización del reloj
  - 8.24 Uso de la criptografía

Categoría: ALTA*
Nivel de medidas Compatible: **Nula**
Particularidades de la ISO:

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.

Recomendación Implantación:

Este control tiene la particularidad de no estar presente en el caso de la ISO y de no ser requerido en aquellas entidades cuya categoría sea MEDIA. No obstante, en el caso que la entidad tenga declarada una categoría ALTA o bien por que se haya considerado la aplicación del control (especialmente a efectos de procedimiento administrativos implicados), se considerará este control.

Se renovarán regularmente los sellos de tiempo hasta que la información protegida ya no sea requerida por el proceso administrativo al que da soporte.

- [mp.info.4.4] Se emplearán ""sellos cualificados de tiempo electrónicos"" atendiendo a lo dispuesto en el Reglamento (UE) nº 910/2014

Con carácter complementario se considerarán los certificados de sede / sitio web, que deberán ser emitidos por entidades cualificadas conforme al Reglamento (UE) nº 910/2014.

[mp.info.5] Limpieza de documentos

- **Control Principal ISO/IEC 27001:2022**
  - No se contempla
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.13 Etiquetado de información
  - 8.12 Prevención de fugas de datos

Categoría: MEDIA
Nivel de medidas Compatible: **Nula**
Particularidades de la ISO:

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.

Recomendación Implantación:

Este control está conectado con el control [org.2] y [mp.si.1] y [mp.info.2]. Es importante desplegar una política de metadatos para el control de la información que se incorporará de manera activa a los procesos de la entidad. Aquella información que debe ser eliminada, antes de su publicación / difusión, deberá ser ""procesada"" para eliminar aquellos metadatos innecesarios.

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

- **Control Principal ISO/IEC 27001:2022**
  - 8.13 Copias de seguridad de la información
- **Controles Complementarios ISO/IEC 27001:2022**
  - 8.14 Redundancia de los recursos de tratamiento de la información
  - 7.14 Eliminación o reutilización segura o de equipos
  - 7.10 Soportes de almacenamiento
  - 5.37 Documentación de procedimientos operacionales
  - 5.29 Seguridad de la información durante la interrupción
  - 5.30 Preparación para las TIC para continuidad de negocio
  - 5.31 Identificación de requisitos legales, reglamentarios y contractuales

Categoría: MEDIA (+R2) *
Nivel de medidas Compatible: **Análogo**
Particularidades de la ISO:

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.

Recomendación Implantación:

A efectos de la ISO existe un nivel de medidas de seguridad compatible por cuanto el control operativo 8.13, se alinea con el [mp.info.6]

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.

- Se considera Refuerzo R2-Protección de las copias de seguridad, para elementos críticos que requieran su almacenamiento en lugar diferente. 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] y la consideración a 8.14 Redundancia de las instalaciones de procesamiento de información y 5.31 Identificación de requisitos legales, reglamentarios y contractuales

.

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.

Es importante tener en cuenta que este control se asocia a continuidad y para la ISO esto es significativo, por cuanto deberá tenerse presente para cumplir con los requisitos de la misma. 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 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 debería disponer de un protocolo [org.3] para realizar restauraciones sencillas y se podrá alinear con el control [op.cont.3], y considerarlo como pruebas de continuidad.

Deben considerarse los soportes empleados en su caso, y las indicaciones dadas por el fabricante, así como aquellas especificaciones de almacenamiento. Debe considerarse dentro del proceso, la eliminación segura de las copias y de los soportes de estas. [mp.si.5].

[MP.S] PROTECCIÓN DE LOS SERVICIOS

[mp.s.1] Protección del correo electrónico

- **Control Principal ISO/IEC 27001:2022**
  - 5.14 Transferencia de la información
- **Controles Complementarios ISO/IEC 27001:2022**
  - 8.12 Prevención de fugas de datos
  - 5.10 Uso aceptable de la información y activos asociados
  - 5.23 Seguridad de la información para el uso de servicios en la nube
  - 6.2 Términos y condiciones de contratación
  - 6.3 Concienciación, educación y formación en seguridad de la información

Categoría: MEDIA
Nivel de medidas Compatible: **Parcialmente análogo**

Particularidades de la ISO:

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

Recomendación Implantación:

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. Este control se podrá delegar al proveedor de correo y se considerará el control [org.2] para la especificación de las instrucciones de uso.

Este control considerará las pautas relacionadas con más 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

- **Control Principal ISO/IEC 27001:2022**
  - 8.26 Requisitos de seguridad de las aplicaciones
- **Controles Complementarios ISO/IEC 27001:2022**
  - 5.35 Revisión independiente de la seguridad de la información.
  - 5.8 Seguridad de la información en la gestión de proyectos
  - 5.17 Información de Autenticación
  - 8.2 Gestión de privilegios de acceso
  - 8.5 Autenticación segura

Categoría: MEDIA
Nivel de medidas Compatible: **Parcialmente análogo**

Particularidades de la ISO:

Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones.

Recomendación Implantación:

Por defecto todos los servicios publicados considerarán controles de acceso (cuando sea preciso), protecciones frente a ataques de manipulación y de inyección de código, escalado de privilegios y cross site scripting.

Debe disponerse de un plan de auditoría que contemple las acciones de revisiones automáticas de vulnerabilidades, herramientas similares y auditorías de caja negra / caja blanca.

Es habitual desplegar servicios mediante un prestador (de servicios específicos o servicios web). Se recomienda incluir en los contratos y condiciones de 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.

Se exigirá al menos, una prueba anual de caja negra con un informe y plan de acción. El plan de auditoria reflejará las fechas estimadas de ejecución de las auditorías y la referencia de la entidad (pública o privada) encargada de la misma.

No existe un nivel de medidas compatibles 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 los 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

- **Control Principal ISO/IEC 27001:2022**
  - 8.23 Filtrado Web
- **Controles Complementarios ISO/IEC 27001:2022**
  - 8.9 Gestión de la configuración
  - 8.12 Prevención de fugas de datos
  - 6.3 Concienciación, educación y formación en seguridad de la información

Categoría: MEDIA
Nivel de medidas Compatible: **Análogo**
Particularidades de la ISO:

El acceso a sitios web externos debe administrarse para reducir la exposición a contenido malicioso.

Recomendación Implantación:

Las dos normas se encuentran en este control muy alineadas.

Se establecerá una normativa de uso y las limitaciones de uso personal [org.2]. Se llevarán a cabo regularmente actividades de concienciación [mp.per.3], sobre higiene en la navegación web, fomentando el uso seguro y alertando de usos incorrectos, mediante correos o poster informativos o banner de sesión.

Se realizarán acciones de formación [mp.per.4] al personal de administración del sistema, en monitorización del servicio y de respuesta a incidentes.

Se desplegarán medidas para proteger la información de resolución de direcciones web y de establecimiento de conexiones, contra la actuación de programas dañinos, y se establecerá una política de control de cookies, en particular para evitar la contaminación entre uso personal y uso organizativo que será dada a conocer a los usuarios mediante acciones de concienciación [mp.per.3]. 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 bloqueos automáticos.

Se deben considerar las configuraciones de los navegadores conforme a [op.exp.2] y [op.exp.3].

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

- **Control Principal ISO/IEC 27001:2022**
  - 8.6 Gestión de capacidades
- **Controles Complementarios ISO/IEC 27001:2022**
  - 8.16 Seguimiento de actividades

Categoría: MEDIA
Nivel de medidas Compatible: **Parcialmente análogo**

Particularidades de la ISO:

El uso de los recursos debe monitorizarse y ajustarse de acuerdo con los requisitos de capacidad actuales y esperados.

Recomendación Implantación:

Se realizarán análisis de previsión en el plan de capacidad anual [op.pl4], con un especial énfasis en el análisis de necesidades y se desplegarán herramientas para un seguimiento del comportamiento del sistema, mediante las que se podrán extraer tendencias y realizar adaptaciones por las necesidades presentadas. Deben establecerse controles de detección para indicar los problemas a su debido tiempo.

Se considerarán los servicios de la gestión de la red, mediante servicios del firewall y la configuración adecuada para considerar este tipo de incidentes DoS. Se considerarán herramientas que ayuden a la prevención de los mismos además de servicios gestionados.

Es conveniente revisar e incluir como requisito en contratos de suministro / soluciones y la gestión de la denegación de servicio.

Los servicios Cloud llevan embebidos estas medidas, por cuanto sus servicios serán correctamente protegidos y balanceados en caso de necesidad. [op.nub.1]

Sería una buena medida alternativa 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)

7. OTROS CONTROLES DE LA ISO

Como se ha podido observar, se hace necesario en algunos casos, desplegar varios controles de la ISO para poder dar cobertura completa al requisito establecido en el ENS. No obstante, existen algunos de ellos, que no se ha incluido por tener menor impacto.

Se han destacado algunos controles de la ISO en este punto, como ejemplificación de su consideración dentro de algún aspecto del Real Decreto 311/2022.

5.4 Responsabilidades de la Dirección

La alta dirección debe asegurarse de que todos los empleados y contratistas conozcan y sigan la política de seguridad de la información de la organización.

Consideración en el ENS:

Artículo 13. Organización e implantación del proceso de seguridad.

org.1 Política de seguridad

5.5 Contacto con las autoridades

Debe quedar claro quién es responsable de contactar a las autoridades (p. ej., organismos encargados de hacer cumplir la ley, organismos reguladores, autoridades de supervisión), qué autoridades deben contactarse (p. ej., qué región/país) y en qué casos es necesario hacerlo. Una respuesta rápida y adecuada a los incidentes puede disminuir en gran medida el impacto, e incluso puede ser obligatoria por ley.

Consideración en el ENS:

Artículo 25. Incidentes de seguridad.

op.exp.7 Gestión de incidentes

5.6 Contacto con grupos de interés especial

Para asegurarse de que se mantengan las últimas tendencias y mejores prácticas de seguridad de la información, el personal con tareas de SGSI debe mantener un buen contacto con los grupos de interés especial. A estos grupos se les puede pedir consejo de expertos en ciertos casos, y ser una gran fuente para mejorar el propio conocimiento.

Consideración en el ENS:

Artículo 13. Organización e implantación del proceso de seguridad.

org.1 Política de seguridad

5.11 Devolución de activos

Cuando un empleado o un externo ya no puede acceder a un activo, por ejemplo, finalizado el contrato, debe devolver el activo a la organización. Debe haber una política clara para esto, que debe ser conocida por todos los implicados.

Consideración en el ENS:

org.2 Normativa de seguridad

5.17 Información de autenticación

La autenticación secreta, como contraseñas y claves de acceso, debe gestionarse en un proceso formal. Además, entre otras acciones de seguridad se debe, prohibir a los usuarios compartir información de autenticación secreta.

Consideración en el ENS:

op.acc.1 Identificación

op.acc.2 Requisitos de acceso

5.32 Derechos de propiedad intelectual (DPI)

Los derechos de propiedad intelectual también son parte del cumplimiento legal. La propiedad intelectual puede ser de gran valor. El uso incorrecto puede dar lugar a grandes perjuicios y perdidas.

Consideración en el ENS:

org.1 Política de seguridad

op.exp.1 Inventario de activos

org.2 Normativa de seguridad

5.33 Protección de registros

Todos los registros, deben protegerse. Los registros tienen el riesgo añadido de pérdida, compromiso o acceso sin autorización. Los requisitos para la protección de registros pueden provenir de la propia organización o de otras fuentes, como la legislación. Para esto, se deben crear y seguir pautas estrictas.

Consideración en el ENS

op.exp.8 Registro de la actividad

op.mon.3 Vigilancia

5.35 Revisión independiente de la seguridad de la información

No es recomendable que las organizaciones revisen su propio sistema de seguridad de la información. Por ello es conveniente que se hagan revisiones independientes, de manera que se audite la seguridad de su información periódicamente o cuando se produzcan cambios significativos. Esto mantiene la visión objetiva y transparente de la seguridad de la información.

Consideración en el ENS

Artículo 31. Auditoría de la seguridad.

Anexo III. Auditoría de la seguridad.

mp.s.2 Protección de servicios y aplicaciones web.

5.36 Cumplimiento de políticas y normas de la seguridad de la información

En relación con las políticas, estándares y procedimientos de seguridad, es importante que se revise periódicamente si las actividades y/o procesos de la organización las respetan y cumplen en su totalidad.

Los sistemas de información también deben revisarse periódicamente para verificar su cumplimiento. Se pueden considerar herramientas automatizadas.

Consideración en el ENS

Artículo 31. Auditoría de la seguridad.

Anexo III. Auditoría de la seguridad.

org.4 Proceso de autorización

op.exp.3 Gestión de la configuración de seguridad

op.exp.4 Mantenimiento y actualizaciones de seguridad

6.4 Proceso disciplinario

Debe existir un proceso disciplinario frente a incumplimientos de la política de seguridad de la. El procedimiento disciplinario debe ser proporcional y gradual, en base a la gravedad, la intencionalidad, reincidencia y, lo que es más importante, si se recibió una formación adecuada.

Consideración en el ENS

org.1 Política de seguridad

6.5 Responsabilidades ante la finalización o cambio

Las responsabilidades de seguridad no terminan cuando se cambia o termina la relación profesional. Deben incluirse acuerdos de confidencialidad, que requieran que se respete la confidencialidad de la información tras dejar la organización.

Consideración en el ENS

mp.per.2 Deberes y obligaciones

6.6 Acuerdos de confidencialidad o no divulgación

Se deben utilizar acuerdos de confidencialidad, que establecen la información cubierta, las responsabilidades de todas las partes, la duración del acuerdo y las sanciones en caso de incumplimiento del acuerdo.

Consideración en el ENS

org.2 Normativa de seguridad

mp.per.2 Deberes y obligaciones

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

6.7 Teletrabajo

El trabajo en remoto se ha convertido en algo común y habitual. Sin embargo, existen implicaciones de seguridad de la información, que deben considerarse y documentarse. La política de trabajo remoto debe describir dónde y cuándo se permite, la provisión de dispositivos y equipos, el acceso autorizado y a qué información se puede acceder de forma remota.

Consideración en el ENS

org.2 Normativa de seguridad

mp.per.2 Deberes y obligaciones

7.4 Monitorización de la seguridad física

La vigilancia puede disuadir de acceso no autorizados y detectar la intrusión. El personal de vigilancia, las cámaras de seguridad y las alarmas, monitorizan y alertan ante accesos no autorizados.

El diseño de cualquier sistema de seguridad y vigilancia debe considerarse confidencial.

Se requieren pruebas periódicas para garantizar que el sistema diseñado e implementado funciona correctamente. Los sistemas de vigilancia con cámaras y otros, que recopilen información

personal o pueden usarse para rastrear y/o geolocalizar a una persona, pueden requerir una consideración especial en materia de protección de datos.

Consideración en el ENS

mp.if Protección de las instalaciones e infraestructuras

mp.info.1 Datos personales

7.9 Seguridad de los equipos fuera de las instalaciones

Los dispositivos, incluidos los dispositivos personales autorizados para el acceso, uso y tratamiento de información de la organización, necesitan protección cuando salen de las instalaciones. La organización debe saber qué dispositivos se utilizan fuera de las instalaciones, por quién y a qué información se accede o se utiliza fuera de las instalaciones.

Consideración en el ENS

mp.eq.3Protección de dispositivos portátiles

8.3 Restricción de acceso a la información

El acceso a la información y otros activos debe basarse en las necesidades de cada usuario, reduciéndose el acceso al mínimo imprescindible y a usuarios particulares. La información no debe ser accesible a usuarios anónimos para evitar el acceso no trazable y no autorizado. Esto es importante para preservar la confidencialidad de la información, monitorizar su uso y evitar su modificación y distribución no autorizada.

Consideración en el ENS

op.acc.2 Requisitos de acceso

op.acc.3 Segregación de funciones y tareas

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

8.11 Enmascaramiento[42] de datos

Solo la cantidad mínima de datos necesarios estará disponible para la función específica ejecutada en los resultados de búsqueda. Para lograr esto, los datos personales deben enmascararse (o anonimizarse o seudonimizar) para ocultar la identidad de los sujetos. Esto puede ser requerido no solo por seguridad, sino por la legislación vigente como puede ser el RGPD.

Consideración en el ENS

mp.info.1 Datos personales

8.19 Instalación de software en sistemas de producción

La instalación de software puede introducir vulnerabilidades en los sistemas operativos. Para minimizar este riesgo, el software solo debe ser instalado por personal autorizado.

El software debe provenir de fuentes confiables y estar mantenido o completamente probado si se desarrolló internamente. Las versiones anteriores deben conservarse y todos los cambios registrados para que sea posible revertirlos si es necesario.

[42] Entendido como sinónimo de ofuscación o anonimización

Consideración en el ENS

op.exp.2 Configuración de seguridad

op.acc.3 Segregación de funciones y tareas

mp.sw.2 Aceptación y puesta en servicio

8.30 Externalización del desarrollo

Cuando el desarrollo se subcontrata, los requisitos de seguridad de la información deben ser comunicados y aceptados por el desarrollador. La concesión de licencias y la propiedad intelectual, las pruebas y la evidencia de las pruebas, y los derechos contractuales para auditar el proceso de desarrollo son ejemplos de consideraciones de seguridad que deben acordarse entre las partes.

Consideración en el ENS

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

mp.sw.1 Desarrollo de aplicaciones

mp.sw.2 Aceptación y puesta en servicio

op.ext.3 Protección de la cadena de suministro

8.34 Protección de los sistemas de información durante las pruebas de Auditoría

Los sistemas operativos no deben verse afectados indebidamente por auditorías o revisiones técnicas. Para evitar perturbaciones excesivas, las auditorías deben planificarse, acordándose el tiempo y el alcance. Los accesos exclusivamente en modo lectura evitarán cambios accidentales en los sistemas durante una auditoría. Todos los accesos deben ser monitorizados.

Consideración en el ENS

op.exp.2 Configuración de seguridad

op.exp.3Gestión de la configuración de seguridad

op.exp.4 Mantenimiento y actualizaciones de seguridad

mp.s.2 Protección de servicios y aplicaciones web

Artículo 31. Auditoría de la seguridad.

ANEXO A. GLOSARIO Y ABREVIATURAS

Ver guía CCN-STIC 800 Glosario de Términos y Abreviaturas del ENS.

ANEXO B. REFERENCIAS

- [ENS] Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. BOE de 4 de mayo de 2022
- ISO/ IEC 27001:2022 Information security, cybersecurity, and privacy protection — Information security management systems — Requirements-.
- ISO/IEC 27002:2022 Information security, cybersecurity, and privacy protection — Information security controls.
- ISO/IEC 27004, Tecnología de la información. Técnicas de seguridad. Gestión de la seguridad de la información. Seguimiento, medición, análisis y evaluación.
- ISO/IEC 27005, Seguridad de la información, ciberseguridad y protección de la privacidad. Orientación sobre la gestión de riesgos de seguridad de la información.
- ISO 31000:2018, Gestión de riesgos— Directrices
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- CCN-STIC. Serie 800. Esquema Nacional de Seguridad.

PUBLICACIONES DE DEFENSA

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