centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 825

Anexo Independiente
Mapeo entre la Norma ISO 27001:2022 y el RD 311/2022 (ENS)

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
2023.07.19 08:39:34 +02'00'

Pº de la Castellana 109, 28046 Madrid

Fecha de Edición: julio de 2023

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

ÍNDICE

1. MAPEO ENTRE LA NORMA ISO 27001:2022 Y EL RD 311/2022 (ENS)

Referencia ISO 27001	Control ISO 27001:2022	Descripción resumida del control de la norma ISO 27001:2022	Referencia ENS	Medida de seguridad RD 311/2022
5				
5.1	Políticas para la seguridad de la información	Se definirá la PSI y otra normativa interna específica, se aprobarán por la dirección, se comunicarán al personal y demás partes interesadas, revisándose a intervalos planificados y ante cambios significantes	[org.1] [org.2]	Política de Seguridad Normativa de Seguridad
5.2	Roles y responsabilidades en seguridad de la información	Los roles y responsabilidades de seguridad de la información se definirán y asignarán de acuerdo a las necesidades de la organización.	[org.4]	Proceso de Autorización
5.3	Segregación de tareas	Los conflictos de funciones y de áreas de responsabilidad deben segregarse.	[op.acc.3]	Segregación de funciones y tareas
5.4	Responsabilidades de la dirección	La alta dirección requerirá a todo el personal que aplique la seguridad de la información de acuerdo con la PSI, normativa específica y procedimientos de la organización.	[org.1] Art.13	Política de Seguridad Organización e implantación del proceso de seguridad.
5.5	Contacto con las autoridades	La organización establecerá y mantendrá contacto con las autoridades relevantes.	Art. 25 [op.exp.7]	Incidentes de seguridad Gestión de incidentes
5.6	Contacto con grupos de interés especial	La organización establecerá y mantendrá contacto con grupos de especial interés u otros foros de seguridad especializados y asociaciones profesionales.	Artículo 13 [org.1]	Organización e implantación del proceso de seguridad Política de Seguridad
5.7	Inteligencia de amenazas	La información relacionada con amenazas a la seguridad de la información será recabada y analizada para obtener inteligencia de amenazas.	[op.mon.3]	Vigilancia
5.8	Seguridad de la información en la gestión de proyectos	La seguridad de la información debe integrarse en la gestión de proyectos.	[op.pl.3]	Adquisición de nuevos componentes
5.9	Inventario de información y otros activos asociados	Debe elaborarse y mantenerse un inventario de información y otros activos asociados, que incluya sus propietarios.	[op.exp.1] [op.pl.2]	Inventario de activos Arquitectura de Seguridad
5.10	Uso aceptable de la información y activos asociados	Se deben identificar, documentar e implementar normas para el uso aceptable y procedimientos para el manejo e información y otros activos asociados.	[org.2] [org.3] [mp.si.3]	Normativa de seguridad Procedimientos de seguridad Custodia
5.11	Devolución de activos	El personal y otras terceras partes, según corresponda, devolverán	[org.2]	Normativa de seguridad

Referencia ISO 27001	Control ISO 27001:2022	Descripción resumida del control de la norma ISO 27001:2022	Referencia ENS	Medida de seguridad RD 311/2022
		todos los activos de la organización que estén en su posesión en el momento en que cambie o finalice su empleo, contrato o acuerdo.		
5.12	Clasificación de la información	La información debe ser clasificada de acuerdo a las necesidades de seguridad de la información de la organización, basadas en confidencialidad, integridad, disponibilidad y requisitos relevantes de las partes interesadas.	[mp.info.2]	Calificación de la información
5.13	Etiquetado de la información	Debe ser elaborado e implementado 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.	[mp.si.1]	Marcado de soportes
5.14	Transferencia de la información	Debe disponerse de normas, procedimientos o acuerdos de transferencia de información para todo tipo de servicios de transferencia dentro de la organización y entre la organización y terceros.	[org.2] [org.3] [op.ext.1] [mp.s.1]	Normativa de seguridad Procedimientos de Seguridad Contratación y ANS Protección del correo electrónico
5.15	Control de acceso	Se establecerán e implementarán normas de control de acceso físico y lógico a la información y a otros activos asociados, basadas en requisitos de la organización y de seguridad de la información.	[op.acc.2]	Requisitos de Acceso
5.16	Gestión de identidad	Debe gestionarse el ciclo de vida completo de las identidades.	[op.acc.1]	Identificación
5.17	Información de autenticación	La asignación y gestión de la información de autenticación debe controlarse por un proceso de gestión, incluyendo el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.	[op.acc.1] [op.acc.2]	Identificación Requisitos de acceso
5.18	Derechos de acceso	Los derechos de acceso a la información y a otros activos asociados deben ser provisionados, revisados, modificados y suprimidos de acuerdo con la política específica de la organización y las reglas sobre el control de accesos.	[op.acc.4]	Proceso de gestión de derechos acceso
5.19	Seguridad de la información en las relaciones con proveedores	Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el empleo de productos o servicios de proveedores.	[op.ext.1]	Contratación y acuerdos de nivel de servicio
5.20	Abordar la seguridad de la información dentro de los acuerdos de proveedores	Los requisitos relevantes de seguridad de la información deben establecerse y acordarse con cada proveedor según el tipo de relación establecida con ellos.	[op.ext.1]	Contratación y acuerdos de nivel de servicio
5.21	Gestión de la Seguridad de la información en la cadena de suministro de las TIC	Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios TIC.	[op.ext.3]	Protección de la cadena de suministro

Referencia ISO 27001	Control ISO 27001:2022	Descripción resumida del control de la norma ISO 27001:2022	Referencia ENS	Medida de seguridad RD 311/2022
5.22	Seguimiento, revisión y gestión del cambio de los servicios de proveedores	La organización debe regularmente supervisar, revisar, evaluar y gestionar cambios en las prácticas de seguridad de la información del proveedor y en la prestación de los servicios.	[op.ext.2]	Gestión diaria
5.23	Seguridad de la información para el uso de servicios en la Nube	Los procesos para adquisición, uso, gestión y finalización de los servicios en la Nube, deben ser establecidos de acuerdo con los requisitos de seguridad de la información de la organización.	[op.nub.1]	Protección de Servicios en la Nube
5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información.	La organización debe planificar y prepararse para gestionar incidentes de seguridad de la información mediante la definición, elaboración y comunicación de procesos para la gestión de incidentes de seguridad de la información, roles y responsabilidades.	[op.exp.7]	Gestión de Incidentes
5.25	Evaluación y decisión sobre los eventos de seguridad de la información	La organización evaluará los eventos de seguridad de la información y decidir si deben ser catalogados como incidentes de seguridad de la información.	[op.exp.7]	Gestión de Incidentes
5.26	Respuesta a incidentes de seguridad de la información	La respuesta a los incidentes de seguridad de la información debe realizarse de acuerdo a procedimientos documentados.	[op.exp.9]	Registro de la Gestión de Incidentes
5.27	Aprender de los incidentes de seguridad de la información	El conocimiento obtenido a partir de los incidentes de seguridad de la información debe emplearse para fortalecer y mejorar los controles de seguridad de la información.	[op.exp.7] [op.exp.9]	Gestión de Incidentes Registro de la Gestión de Incidentes
5.28	Recopilación de evidencias	La organización debe establecer e implementar procedimientos para la identificación, recogida, clasificación y preservación de evidencias relacionadas con eventos de seguridad de la información.	[op.exp.7] [op.exp.9]	Gestión de Incidentes Registro de la Gestión de Incidentes
5.29	Seguridad de la información durante la interrupción	La organización debe planificar como mantener la seguridad de la información en un nivel apropiado durante una interrupción.	[op.cont.1] [op.cont.2]	Análisis de impacto Plan de Continuidad
5.30	Preparación para las TIC para la continuidad del negocio	La resiliencia de las TIC debe planificarse, implementarse, mantenerse y verificarse en base a los objetivos de continuidad del negocio y de los requisitos de continuidad de las TIC.	[op.cont.3]	Pruebas Periódicas
5.31	Identificación de requisitos legales, reglamentarios y contractuales	Los requisitos legales, estatutarios, regulatorios y contractuales relevantes para la seguridad de la información, junto a la forma de abordar el cumplimiento de dichos requisitos por la organización, deben identificarse, documentarse y mantenerse actualizados.	[org.1] [mp.info.3]	Política de seguridad Firma electrónica
5.32	Derechos de propiedad intelectual	La organización debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual.	[org.1] [org.2] [op.exp.1]	Política de seguridad Normativa de seguridad Inventario de activos
5.33	Protección de los registros	Los registros deben protegerse ante su pérdida, destrucción, falsificación, acceso y divulgación no autorizada.	[op.exp.8] [op.mon.3]	Registro de la actividad Vigilancia

Referencia ISO 27001	Control ISO 27001:2022	Descripción resumida del control de la norma ISO 27001:2022	Referencia ENS	Medida de seguridad RD 311/2022
5.34	Privacidad y protección de datos de carácter personal (DCP)	La organización debe identificar y cumplir con los requisitos relativos a la preservación de la privacidad y la protección de datos de carácter personal (DCP) de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales.	[mp.info.1]	Datos personales
5.35	Revisión independiente de la seguridad de la información	El enfoque de la organización para gestionar la seguridad de la información y su implementación incluyendo personas procesos y tecnología, debe ser revisado de forma independiente a intervalos planificados, o tras producirse cambios significativos.	Art. 31 Anexo III [mp.s.2]	Auditoría de la Seguridad Auditoría de la Seguridad Protección de los servicios y aplicaciones Web
5.36	Cumplimiento de las políticas, y normas de seguridad de la información	El cumplimiento de la política de seguridad de la información de la organización, otras políticas, normas y estándares, debe ser regularmente revisado.	Art. 31 Anexo III [org.4] [op.exp.3] [op.exp.4]	Auditoría de la Seguridad Auditoría de la Seguridad Proceso de Autorización Gestión de la configuración de la seguridad Mantenimiento y actualizaciones de seguridad
5.37	Documentación de procedimientos operacionales	Deben documentarse los procedimientos operacionales de los medios de tratamiento de la información y ponerse a disposición de todos los usuarios que los necesiten.	[org.3]	Procedimientos de Seguridad
6				
6.1	Comprobación	Debe realizarse de forma continuada la verificación de antecedentes, comprobando que a todos los candidatos antes de que se incorporen a la organización, de acuerdo con la legislación aplicable, regulaciones y principios éticos, de forma proporcional a los requerimientos del negocio, la clasificación de la información a la que se accederá y los riesgos percibidos.	[mp.per.1]	Caracterización del puesto de trabajo
6.2	Términos y condiciones de contratación	Los acuerdos contractuales del empleo deberán indicar las responsabilidades de seguridad de la información del personal y de la organización.	[mp.per.2]	Deberes y obligaciones
6.3	Concienciación, educación y formación en seguridad de la información	El personal de la organización y las partes interesadas relevantes deben recibir la apropiada concienciación, educación y formación sobre seguridad de la información, así como actualizaciones regulares de la PSI de la organización, otras normas internas y procedimientos, relevantes para su puesto de trabajo.	[mp.per.3] [mp.per.4]	Concienciación Formación

Referencia ISO 27001	Control ISO 27001:2022	Descripción resumida del control de la norma ISO 27001:2022	Referencia ENS	Medida de seguridad RD 311/2022
6.4	Proceso disciplinario	Debe existir un proceso disciplinario formal que haya sido comunicado a los empleados y partes interesadas pertinentes, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad.	[org.1]	Política de Seguridad
6.5	Responsabilidades ante la finalización o cambio	Las responsabilidades y deberes de seguridad de la información, que siguen vigentes tras la finalización o el cambio de empleo, deben definirse, comunicarse y hacerse cumplir al personal relevante y a otras partes interesadas.	[mp.per.2]	Deberes y obligaciones
6.6	Acuerdos de confidencialidad o no divulgación	Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de protección de la información de la organización deben ser identificados, documentados, revisados regularmente y firmados por el personal y otras partes interesadas pertinente	[org.2] [mp.per.2] [op.ext.1]	Normativa de seguridad Deberes y obligaciones Contratación y acuerdos de nivel de servicio.
6.7	Teletrabajo	Deben ser implementadas medidas de seguridad cuando el personal se encuentre trabajando remotamente, para proteger la información accedida, tratada o almacenada fuera de las instalaciones de la organización.	[org.2] [mp.per.2]	Normativa de seguridad Deberes y obligaciones
6.8	Notificación de los eventos de seguridad de la información	La organización debe proporcionar un mecanismo para que el personal reporte eventos de seguridad de la información, observados o sospechosos, a través de los canales apropiados.	[op.exp.7]	Gestión de Incidentes
7				
7.1	Perímetro de seguridad física	Deben ser definidos y empleados perímetros de seguridad, para proteger áreas que contengan información y otros activos asociados.	[mp.if.1]	Áreas separadas con control de acceso
7.2	Controles físicos de entrada	Las áreas seguras deben protegerse mediante controles de entrada apropiados y puntos de acceso.	[mp.if.2] [mp.if.7]	Identificación de las personas Registro de entrada y salida de equipamiento
7.3	Seguridad de oficinas, despachos y recursos	Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física	[mp.if.1] [mp.if.3]	Áreas separadas con control de acceso Acondicionamiento de los locales
7.4	Monitorización de la seguridad física	Las instalaciones deben ser continuamente monitorizadas para detectar accesos físicos no autorizados.	[mp.if.1] [mp.info.1]	Áreas separadas y con control de acceso Datos personales
7.5	Protección contra las amenazas externas y ambientales	Deben ser diseñadas e implementadas protecciones frente a amenazas físicas y ambientales, como son los desastres naturales, u otras amenazas físicas a la infraestructura, ya sean intencionadas o no.	[mp.if.3] [mp.if.5] [mp.if.6]	Áreas separadas con control de acceso Protección frente a incendios Protección frente a inundaciones
7.6	El trabajo en áreas seguras	Se debe diseñar e implementar procedimientos para trabajar en las	[mp.if.1]	Acondicionamiento de los locales

Referencia ISO 27001	Control ISO 27001:2022	Descripción resumida del control de la norma ISO 27001:2022	Referencia ENS	Medida de seguridad RD 311/2022
		áreas seguras.	[org.2]	Normativa de seguridad
7.7	Puesto de trabajo despejado y pantalla limpia	Deben definirse y hacerse cumplir reglas de puesto de trabajo despejado de papeles y de medios de almacenamiento removibles, así como reglas de pantalla limpia para los recursos de tratamiento de la información.	[mp.eq.1] [mp.eq.2]	Puesto de trabajo despejado Bloqueo del puesto de trabajo
7.8	Emplazamiento y protección de los equipos	Los equipos deben ser situados de forma segura y protegidos.	[mp.if.1] [mp.eq.3]	Áreas separadas con control de acceso Protección de dispositivos portátiles
7.9	Seguridad de los equipos fuera de las instalaciones	Los activos fuera de las instalaciones deben ser protegidos.	[mp.eq.3]	Protección de dispositivos portátiles
7.10	Soportes de almacenamiento	Los soportes de almacenamiento deben ser gestionados a lo largo de su ciclo de vida, incluyendo su adquisición, uso, transporte y desechos, de acuerdo con el esquema de clasificación de la organización y los requisitos de manipulación.	[mp.si.1] [mp.si.2] [mp.si.3] [mp.si.4] [mp.si.5]	Marcado de soportes Criptografía Custodia Transporte Borrado y destrucción
7.11	Instalaciones de suministro	El equipamiento de tratamiento de la información debe protegerse frente a falta de suministro eléctrico, y otras alteraciones causadas por fallos en las instalaciones de suministro.	[mp.if.4]	Energía eléctrica
7.12	Seguridad del cableado	El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.	[mp.if.3]	Acondicionamiento de los locales
7.13	Mantenimiento de los equipos	Los equipos deben recibir u mantenimiento correcto para asegurar la disponibilidad, integridad y confidencialidad de la información.	[op.exp.4]	Mantenimiento y actualizaciones
7.14	Eliminación o reutilización segura de los equipos	Todos los soportes de almacenamiento, deben ser verificados para asegurar que ninguna información sensible y/o licencia de software ha sido eliminada o sobrescrita de forma segura antes de su desechado o reutilización.	[mp.si.5]	Borrado y destrucción
8				
8.1	Dispositivos finales de usuario	La información almacenada, procesada o accesible a través de dispositivos finales de usuario debe protegerse.	[mp.eq.3] [mp.eq.4]	Protección de dispositivos portátiles Otros dispositivos conectados a la red
8.2	Gestión de privilegios de acceso	La asignación y uso de derechos de acceso privilegiados deben ser restringidos y gestionados.	[op.acc.1]	Identificación
8.3	Restricción del acceso a la información	El acceso a la información y a otros activos asociados debe restringirse de acuerdo con la normativa de control de acceso.	[op.acc.2] [op.acc.3] [op.acc.4]	Requisitos de acceso Segregación de funciones y tareas Proceso de gestión de derechos de acceso

Referencia ISO 27001	Control ISO 27001:2022	Descripción resumida del control de la norma ISO 27001:2022	Referencia ENS	Medida de seguridad RD 311/2022
8.4	Acceso al código fuente	Se debe gestionar adecuadamente el acceso de lectura y escritura al código fuente, a las herramientas de desarrollo y a las bibliotecas de software.	[op.acc.2] [mp.sw.1]	Requisitos de acceso Desarrollo de aplicaciones
8.5	Autenticación segura	Las Tecnologías y procedimientos de autenticación segura deben implementarse en base a las restricciones de acceso a la información y la normativa de control de acceso.	[op.acc.6]	Mecanismos de autenticación (usuarios de la organización)
8.6	Gestión de capacidades	El uso de los recursos debe ser monitorizado y ajustado en base a los requisitos de capacidad actuales y previstos.	[op.pl.4] [mp.s.4]	Gestión de la Capacidad Protección frente a la denegación del servicio
8.7	Controles contra el código malicioso	La protección frente al código malicioso debe ser implementada y apoyada mediante la concienciación apropiada de los usuarios.	[op.exp.6]	Protección frente a código dañino
8.8	Gestión de vulnerabilidades técnicas	Debe obtenerse información sobre las vulnerabilidades técnicas de los sistemas de información en uso, evaluar la exposición de la organización a dichas vulnerabilidades, y adoptar las medidas adecuadas.	[op.mon.3] [op.exp.4]	Vigilancia Mantenimiento y actualizaciones
8.9	Gestión de la configuración	Las configuraciones, incluidas las de seguridad, de hardware, software, servicios y redes, deben establecerse, documentarse, implementarse, monitorizarse y revisarse.	[op.exp.2] [op.exp.3]	Configuración de Seguridad Gestión de la Configuración
8.10	Eliminación de la información	La información almacenada en sistemas de información, dispositivos o en cualquier otro soporte de información, debe ser borrada cuando ya no se requiera.	[mp.si.5]	Borrado y destrucción
8.11	Enmascaramiento de datos	El enmascaramiento de datos debe emplearse de acuerdo a la normativa de control de acceso de la organización y otras normativas, así como con los requisitos del negocio y teniendo en cuenta la legislación aplicable.	[mp.info.1]	Datos personales
8.12	Prevención de fugas de datos	Deben aplicarse medidas para la prevención de fugas de datos a los sistemas, redes y cualquier otro dispositivo que trate, almacene o transmita información sensible.	[mp.com.1] [mp.com.2] [mp.si.2] [mp.eq.3]	Perímetro seguro Protección de la confidencialidad Criptografía Protección de equipos portátiles
8.13	Copias de seguridad de la información	Las copias de seguridad de la información, el software y los sistemas deben mantenerse y comprobarse regularmente de acuerdo con la política de copias de seguridad específica acordada.	[mp.info.6]	Copias de seguridad
8.14	Redundancia de los recursos de tratamiento de la información	El equipamiento de tratamiento de la información debe implementarse con las redundancias suficientes para satisfacer con los requisitos de disponibilidad.	[op.cont.4]	Medios alternativos

Referencia ISO 27001	Control ISO 27001:2022	Descripción resumida del control de la norma ISO 27001:2022	Referencia ENS	Medida de seguridad RD 311/2022
8.15	Registro de eventos	Se deben generar, proteger, almacenar y analizar los registros de las actividades, excepciones, fallos y otros eventos relevantes	[op.exp.8]	Registro de la actividad
8.16	Seguimiento de actividades	Las redes, sistemas y aplicaciones deben ser monitorizados en busca de comportamientos anómalos, adoptando acciones apropiadas para evaluar posibles incidentes de seguridad de la información.	[op.mon.3] [mp.s.4]	Vigilancia Protección frente a DoS
8.17	Sincronización del reloj	Los relojes de los sistemas de tratamiento de información empleados por la organización deben sincronizarse con fuentes de tiempos apropiadas.	[op.exp.8]	Registro de la actividad
8.18	Uso de los programas de utilidad con privilegios	Se debe restringir y controlar rigurosamente el uso de programas de utilidad que puedan ser capaces de invalidar los controles del sistema y de la aplicación.	[op.acc.2]	Requisitos de Acceso
8.19	Instalación del software en sistemas de producción	Deben implementarse procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas de producción.	[op.exp.2] [op.acc.3] [mp.sw.2]	Configuración de seguridad Segregación de funciones y tareas Aceptación y puesta en servicio
8.20	Seguridad de redes	Las redes y los dispositivos de red deben ser asegurados, gestionados y controlados para proteger la información en sistemas y aplicaciones.	[mp.com.1]	Perímetro seguro
8.21	Seguridad de los servicios de red	Se deben identificar, implementar y monitorizar los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de todos los servicios de red.	[mp.com.2] [mp.com.3]	Protección de la confidencialidad Protección Integridad/Autenticidad
8.22	Segregación en redes	Los grupos de servicios de información, de usuarios y de sistemas de información deben ser segregados en las redes de la organización.	[op.ext.4] [mp.com.4]	Interconexión de sistemas Separación de flujos de información en la red
8.23	Filtrado de Webs	El acceso a sitios webs externos debe ser gestionado para reducir la exposición a contenido malicioso.	[mp.s.3]	Protección de la navegación Web
8.24	Uso de la criptografía	Deben definirse e implementarse normas para el uso efectivo de criptografía, incluyendo la gestión de claves criptográficas.	[op.exp.10] [mp.si.2] [mp.info.3]	Protección de claves criptográficas Criptografía Firma electrónica
8.25	Seguridad en el ciclo de vida del desarrollo	Deben establecerse y aplicarse normas para el desarrollo seguro de software y sistemas.	[mp.sw.1]	Desarrollo de aplicaciones
8.26	Requisitos de seguridad en las aplicaciones	Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones.	[mp.sw.1] [mp.s.2]	Desarrollo de aplicaciones Protección de servicios y aplicaciones web

Referencia ISO 27001	Control ISO 27001:2022	Descripción resumida del control de la norma ISO 27001:2022	Referencia ENS	Medida de seguridad RD 311/2022
			[mp.com.3] [mp.sw.2] [mp.info.4]	Protección Integridad/Autenticidad Aceptación y puesta en servicio Sellos de tiempo
8.27	Arquitectura segura de sistemas y principios de ingeniería	Los principios de ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicar a todas las actividades de desarrollo de sistemas de información.	[op.pl.2] [mp.sw.1]	Arquitectura de Seguridad Desarrollo de aplicaciones
8.28	Codificación segura	Principios de codificación segura deben aplicarse al desarrollo de software.	[mp.sw.1]	Desarrollo de aplicaciones
8.29	Pruebas de seguridad en desarrollo y aceptación	Deben definirse e implementarse, en todo el ciclo de vida del desarrollo, procesos de prueba de la seguridad.	[mp.sw.2]	Aceptación y puesta en servicio
8.30	Externalización del desarrollo	La organización debe controlar, monitorizar y revisar las actividades relacionadas con el desarrollo de sistemas externalizados.	[op.ext.1] [mp.sw.1] [mp.sw.2] [op.ext.3]	Contratación y acuerdos de nivel de servicio Desarrollo de aplicaciones Aceptación y puesta en servicio Protección de la cadena de suministro
8.31	Separación de los entornos de desarrollo, prueba y producción	Los entornos de desarrollo, pruebas y producción deben estar separados y protegidos.	[mp.sw.2]	Aceptación y puesta en servicio
8.32	Gestión de cambios	Los cambios en las instalaciones de tratamiento de la información y en los sistemas de información, deben estar sujetos a procedimientos de gestión de cambios.	[op.exp.5]	Gestión de Cambios
8.33	Datos de prueba	Los datos de prueba deben ser seleccionados, protegidos y gestionados apropiadamente.	[mp.sw.1] [mp.sw.2]	Desarrollo de aplicaciones Aceptación y puesta en servicio
8.34	Protección de los sistemas de información durante las pruebas de auditoría	Las pruebas de auditoría y otras actividades de aseguramiento en la evaluación de los sistemas en producción deben ser cuidadosamente planificadas y acordadas entre el evaluador y los gestores adecuados.	[op.exp.2] [op.exp.3] [op.exp.4] [mp.s.2] Artículo 31	Configuración de seguridad Gestión de la configuración de seguridad Mantenimiento y actualizaciones de seguridad Protección de servicios y aplicaciones web Auditoría de seguridad

PUBLICACIONES DE DEFENSA

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