	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 1 de 31	
		Revisión núm. 5	14/02/2025

POLÍTICA DE SEGURIDAD

IDM Sistemas de Comunicación mantiene un compromiso firme con la seguridad de la información, garantizando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los datos y servicios que gestiona, conforme al Esquema Nacional de Seguridad (ENS).

La política se apoya en los siguientes pilares:

Marco Normativo

La seguridad se rige por el Real Decreto 311/2022 (ENS) y su normativa complementaria, además de la legislación vigente en materia de protección de datos, administración digital, contratación pública y otros marcos regulatorios aplicables.

Gobernanza y Gestión

La organización establece funciones y responsabilidades específicas para coordinar la seguridad, fomentar la mejora continua y garantizar el cumplimiento de las obligaciones legales y contractuales.

Gestión del Riesgo

La seguridad se gestiona mediante metodologías reconocidas de análisis y tratamiento de riesgos, evaluando vulnerabilidades y amenazas para mantener niveles adecuados de protección en función de la criticidad de la información y los servicios.

Medidas de Seguridad

Se implantan medidas técnicas, organizativas y procedimentales para:

- Controlar accesos.
- Proteger datos almacenados y en tránsito.
- Garantizar continuidad del servicio.
- Prevenir, detectar y gestionar incidentes.
- Supervisar proveedores y servicios de terceros.
- Proteger infraestructuras y activos tecnológicos.

Compromiso con Usuarios y Clientes


IDM asegura que todo el personal implicado —propio y externo— cumple las obligaciones en materia de seguridad y confidencialidad, con formación, procedimientos y controles adecuados.

Objetivo

Mantener servicios fiables y seguros, protegiendo la información y generando confianza en clientes, administraciones y terceros mediante una gestión responsable y conforme al ENS.

Este documento es propiedad de IDM SISTEMAS DE COMUNICACIÓN no puede ser utilizado para propósitos diferentes de aquellos para el que ha sido creado.

Reproducido, total o parcialmente, o transmitido o comunicarlo a cualquier persona sin la autorización del propietario

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 2 de 31	
		Revisión núm. 5	14/02/2025

1. ARTICULADO.

Esta Política desarrolla el artículo 12 del Real Decreto 311/2022 (ENS) ubicado el en Capítulo III “Política de seguridad y requisitos mínimos de seguridad” y el Anexo II “Medidas de seguridad” (medidas org.1–org.4).

La Política es aprobada por el órgano competente y se revisa, como mínimo, anualmente o tras cambios significativos. Su ámbito cubre los sistemas en alcance del ENS de categoría MEDIA definidos por la organización.

3. Marco organizativo [ORG]: El marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad.

3.1 Política de seguridad [org.1], en cumplimiento de lo dispuesto en el citado artículo 12 del Real Decreto 311/2022, tendrá como requisitos la regulación de al menos:

- [org.1.1] *Los objetivos o misión de la organización.*
- [org.1.2] *El marco legal y regulatorio en el que se desarrollarán las actividades.*
- [org.1.3] *Los roles o funciones de seguridad, definiendo para cada uno los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.*
- [org.1.4] *La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, las personas integrantes y la relación con otros elementos de la organización.*
- [org.1.5] *Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.*

La estructura del sistema documental del SGSI del ENS se describe en el documento ‘NI-ENS-20 - Sistema documental’. La lista maestra y vigente de documentos aplicables al ENS (procedimientos, instrucciones, normativa interna, plantillas, formatos y registros) se mantiene en el registro F-PRENS02-06 Lista de documentación en vigor, incluyendo la trazabilidad de versión y revisión”


3.2 Normativa de seguridad [org.2].

Requisitos. Se dispondrá de una serie de documentos que describan:

- [org.2.1] *El uso correcto de equipos, servicios e instalaciones, así como lo que se considerará uso indebido.*
- [org.2.2] *La responsabilidad del personal con respecto al cumplimiento o violación de la normativa: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.*

Se ha revisado todos los documentos relativos a medidas disciplinarias principalmente para:

- 1) Mejorar la disuasión y concienciación:

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 3 de 31	
		Revisión núm. 5	14/02/2025

- Si los empleados, usuarios y terceros entienden fácilmente qué acciones constituyen una falta de seguridad y cuál es la sanción asociada, el documento se convierte en una herramienta de disuasión mucho más efectiva.
 - Ayuda a concienciar al personal sobre la gravedad de las faltas de seguridad (como el uso indebido de contraseñas, la fuga de información, o la instalación de software no autorizado).
- 2) Facilitar la aplicación consistente:
- Un texto claro y simplificado asegura que los responsables de aplicar las medidas disciplinarias (Recursos Humanos, Dirección) puedan hacerlo de forma consistente, justa y sin ambigüedades.
 - Evita interpretaciones erróneas que podrían llevar a aplicar sanciones desproporcionadas o, por el contrario, a no aplicar ninguna cuando correspondería.
- 3) Promover el Cumplimiento:
- Los documentos disciplinarios suelen estar relacionados con el convenio colectivo, el régimen de personal o la legislación vigente. Una relación sencilla y clara permite a la organización asegurarse de que su normativa interna de seguridad se alinea correctamente con el marco legal superior.

La normativa disciplinaria es una herramienta práctica y comprensible que fortalece la seguridad al establecer consecuencias claras para la conducta negligente o maliciosa.

3.3 Procedimientos de seguridad [org.3].


Requisitos. Se dispondrá de una serie de documentos que detallen de forma clara y precisa cómo operar los elementos del sistema de información:

- [org.3.1] *Cómo llevar a cabo las tareas habituales.*
- [org.3.2] *Quién debe hacer cada tarea.*
- [org.3.3] *Cómo identificar y reportar comportamientos anómalos.*
- [org.3.4.] *La forma en que se ha de tratar la información en consideración al nivel de seguridad que requiere, precisando cómo efectuar:*
 - a) *Su control de acceso.*
 - b) *Su almacenamiento.*
 - c) *La realización de copias.*
 - d) *El etiquetado de soportes.*
 - e) *Su transmisión telemática.*
 - f) *Cualquier otra actividad relacionada con dicha información.*

3.4 Proceso de autorización.

Se establecerá un proceso formal de autorizaciones que cubra todos los elementos del sistema de información concernidos:

- [org.4.1] *Utilización de instalaciones, habituales y alternativas.*

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 4 de 31	
		Revisión núm. 5	14/02/2025

- [org.4.2] *Entrada de equipos en producción, en particular, equipos que involucren criptografía.*
- [org.4.3] *Entrada de aplicaciones en producción.*
- [org.4.4] *Establecimiento de enlaces de comunicaciones con otros sistemas.*
- [org.4.5] *Utilización de medios de comunicación, habituales y alternativos.*
- [org.4.6] *Utilización de soportes de información.*
- [org.4.7] *Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, tabletas, teléfonos móviles u otros de naturaleza análoga.*
- [org.4.8] *Utilización de servicios de terceros, bajo contrato o convenio, concesión, encargo, etc.*

2. OBJETO.

El objeto de este documento es definir la Política de Seguridad de la Información de IDM SISTEMAS DE COMUNICACIÓN en relación con el Esquema Nacional de Seguridad (ENS), estableciendo el marco común para gestionar y proteger la información que tratamos y los servicios que prestamos, de acuerdo con los principios del ENS y la normativa aplicable, en concreto en cumplimiento del artículo 12 del Real Decreto 311/2022 y del Anexo II. Esta Política establece y desarrolla los principios, objetivos, responsabilidades y requisitos mínimos para proteger la información que tratamos y los servicios que prestamos.


La Dirección de IDM, impulsa un Sistema de Gestión Integrado (SGI) alineado con el ENS, orientado a comprender y atender las necesidades de nuestros clientes y partes interesadas, prestando servicios conformes y fomentando la mejora continua. Esta Política fija los principios y responsabilidades necesarias para salvaguardar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, guiando la implantación proporcional de controles y buenas prácticas en los sistemas y servicios en alcance.

Manifiesta expresamente su compromiso de potenciar la Seguridad de la Información del servicio prestado, y se compromete a satisfacer las necesidades y expectativas de las partes interesadas, a mantener alta nuestra competitividad en los servicios y productos.

3. MISIÓN Y OBJETIVOS.

[org.1.1] Los objetivos o misión de la organización.

En cumplimiento del artículo 12.1.a) del ENS, la misión de IDM SISTEMAS DE COMUNICACIÓN es prestar servicios y soluciones de software fiables y seguros, orientados a transformar datos en información útil para la toma de decisiones de nuestros

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 5 de 31	
		Revisión núm. 5	14/02/2025

clientes, fomentando la mejora continua del servicio y del soporte y consolidando el posicionamiento de IDM como referente en el sector. La seguridad de la información y la ciberseguridad constituyen un pilar por defecto en la prestación de nuestros servicios y en el diseño y operación de nuestros sistemas.

Para alcanzar estos objetivos, IDM impulsa un Sistema de Gestión Integrado alineado con el ENS y con la normativa aplicable. Mantenemos un sistema de metas, métricas e indicadores para el seguimiento y la medición de nuestros procesos internos y de la satisfacción de clientes y partes interesadas, velando por el cumplimiento de los requisitos contractuales y por una mejora continua basada en evidencias. Contamos con un equipo profesional y especializado, al que proporcionamos formación y concienciación continuas, y con infraestructuras adecuadas y acordes a las necesidades de los servicios.


Nuestro enfoque operativo se fundamenta en la gestión de riesgos con metodologías de análisis y gestión de estos reconocidas, basada en estándares, en la protección de la información almacenada y en tránsito, en la gestión segura de adquisiciones, en la interconexión controlada con otros sistemas de información y en la monitorización y registro de actividad para la detección oportuna de anomalías. Prestamos especial atención a la gestión de incidentes, así como a la continuidad y disponibilidad del negocio y de los servicios, manteniendo planes y pruebas acorde a las necesidades del servicio. Cumplimos la legislación vigente, en particular el RGPD/LOPDGDD, y aplicamos nuestra Documentación de Seguridad.

Estos principios se aplican de forma proporcional y coherente en los ámbitos físico, lógico y político-corporativo: desde la protección de dependencias, instalaciones, hardware y soportes (físico); pasando por aplicaciones, redes y comunicaciones (lógico); hasta la organización interna, normas y requisitos legales y regulatorios (político-corporativo) (org.1.2). Todo ello se rige por los **principios básicos del ENS: seguridad como proceso integral, gestión basada en riesgos, prevención, detección, respuesta y conservación, líneas de defensa, vigilancia continua, reevaluación periódica y diferenciación de responsabilidades.**

El alcance de estos objetivos comprende los sistemas de información que dan soporte a los servicios de instalación y mantenimiento del sistema inteligente de gestión de esperas, de acuerdo con la categorización vigente. Para dichos sistemas, la organización vela por el cumplimiento de las medidas del ENS en nivel MEDIO en las cinco dimensiones de seguridad (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad), aplicando controles acordes al riesgo y a la naturaleza del servicio.

4. LEGISLACIÓN. MARCO LEGAL Y REGULATORIO.


[org.1.2] El marco legal y regulatorio en el que se desarrollarán las actividades

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 6 de 31	
		Revisión núm. 5	14/02/2025

El marco legal y regulatorio que rige las actividades de IDM SISTEMAS DE COMUNICACIÓN en materia de seguridad de la información está encabezado por el Real Decreto 311/2022 (ENS) y sus Instrucciones Técnicas de Seguridad (ITS), junto con la normativa de administración digital, protección de datos, servicios electrónicos de confianza, contratación pública y demás reglas sectoriales aplicables. A todos los efectos, se considerará vigente la redacción consolidada del BOE y, en caso de derogación o sustitución, será aplicable la norma sucesora.

Con carácter principal, resultan de aplicación:


- **Esquema Nacional de Seguridad:** Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. **Instrucciones Técnicas de Seguridad:**
 - o Resolución de 13 de octubre de 2016, la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Plan Nacional de Seguridad.
 - o Resolución de 7 de octubre de 2016, la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad del Estado de la Seguridad.
 - o Resolución de 27 de marzo de 2018, de la Oficina de Estado de Función Pública, mediante la cual se aprueba la Instrucción Técnica de Seguridad de auditoría de la seguridad de los sistemas de información.
 - o Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- **Administración digital / procedimiento e interoperabilidad:**
 - o Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
 - o Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
 - o Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
 - o Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
 - o Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
 - o Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
 - o **Esquema Nacional de Interoperabilidad** – Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- **Protección de datos:**
 - o 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

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 7 de 31	
		Revisión núm. 5	14/02/2025

respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- **Servicios electrónicos de confianza y firma:**
 - Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
 - Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. (que deroga la Ley 59/2003 de firma electrónica).
 - Se mantiene el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.
- **Contratación pública:** Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- **Servicios de la sociedad de la información:** Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- **Telecomunicaciones:** Ley 11/2022, de 28 de junio, General de Telecomunicaciones, que sustituye a la Ley 9/2014.
- **Transparencia y reutilización:**
 - Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
 - Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público. Modificada por RDL 24/2021.
 - Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, para el ámbito del sector público estatal.
- **Otras:**
 - Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
 - Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.
 - Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido del Estatuto Básico del Empleado Público.

El mantenimiento del marco legal y regulatorio será responsabilidad de IDM SISTEMAS DE COMUNICACIÓN y se conservará en un anexo vivo a esta Política, que incluirá la normativa vigente y sus referencias oficiales. En caso de discrepancia o

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 8 de 31	
		Revisión núm. 5	14/02/2025


actualización posterior, prevalecerá lo recogido en el citado Anexo I por ser el registro vivo de mantenimiento. Dicho anexo se actualizará para reflejar cualquier modificación normativa que afecte al ENS, a la protección de datos, a la administración digital, a la contratación pública o a otras obligaciones sectoriales aplicables. A efectos de interpretación, prevalecerá siempre la redacción oficial vigente publicada por los organismos competentes.

Con el fin de asegurar la vigencia del marco legal y regulatorio, la organización mantiene un seguimiento continuo de la normativa aplicable mediante la suscripción a boletines de actualización normativa de su proveedor de protección de datos y de su asesoría jurídica laboral, que remiten las novedades que resultan de aplicación. Adicionalmente, se consultan de forma periódica fuentes oficiales (Boletín Oficial del Estado y organismos competentes) y comunicaciones de asesoría especializada en ENS. Las novedades identificadas se analizan por el Responsable de Seguridad y/o el Responsable de Información para determinar su aplicabilidad e impacto, registrándose en el “Registro marco legal en materia de seguridad” junto con las acciones de adecuación necesarias. Cuando corresponda, las modificaciones se elevan al Comité de Seguridad para su aprobación y se actualizan la Política de Seguridad y el resto de documentación de seguridad, manteniendo trazabilidad y evidencias de la revisión.

Instrucciones Técnicas de Seguridad (ITS) y guías CCN-STIC. Forman parte del marco regulatorio las Instrucciones Técnicas de Seguridad de obligado cumplimiento y las guías CCN-STIC que, conforme prevé el ENS, precisan criterios y buenas prácticas para su implantación. IDM mantiene un documento vivo que identifica las ITS y las guías CCN-STIC.

En relación con las revisiones del marco legal y regulatorio que constituye la Política, se distinguirán tres tipos de actividades:

- Revisiones periódicas, que se realizarán, al menos, con una periodicidad anual.
- Revisiones sistemáticas: Deberán realizarse cuando se detecten incidencias o cambios en el marco legal que puedan cuestionar la validez de dicha Política. [org.1.2] El marco legal y regulatorio en el que se desarrollarán las actividades. IDM dispone de asesoría externa con especialización en ENS que realiza un seguimiento continuo de novedades legales y técnicas (BOE y fuentes oficiales) y comunica los cambios relevantes al Responsable de Seguridad, a fin de evaluar su alcance y proponer las modificaciones oportunas en la documentación y controles.
- Revisiones no planificadas: Estas revisiones deberán realizarse en respuesta a cualquier evento o incidente de seguridad que pudiera suponer un incremento significativo del nivel de riesgo actual o que haya causado un impacto en la seguridad de la información IDM.

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 9 de 31	
		Revisión núm. 5	14/02/2025

5. MODELO DE GOBERNANZA

Para garantizar el cumplimiento del Esquema Nacional de Seguridad y establecer la organización de la seguridad de la información en IDM SISTEMAS DE COMUNICACIÓN, designará roles de seguridad y constituirá un Comité de Seguridad de la información.

5.1 Roles o perfiles de seguridad.

[org.1.3] Los roles o funciones de seguridad, definiendo para cada uno los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.

Para garantizar el cumplimiento y la adaptación de las medidas exigidas reglamentariamente, se han creado roles o perfiles de seguridad, los nombramientos constan en el Registro de Nombramientos a efectos de trazabilidad se reflejan a continuación y se han designado los cargos u órganos que los ocuparán, del siguiente modo:

- Responsable de Información (RI):
- Responsable de los Servicios (RSv):
- Responsable de Seguridad (RS):
- Responsable del Sistema (RSis):
- Responsable de contacto con proveedores (POC):

5.2 Funciones de cada uno de los roles.


[org.1.3] Los roles o funciones de seguridad, definiendo para cada uno los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.

A continuación, se detallan las funciones y responsabilidades de cada uno de los roles de seguridad del ENS. Los aspectos relativos a nombramiento, vigencia, suplencias y cese se rigen por el Procedimiento de designación y renovación de roles.

RESPONSABLE DE LA INFORMACIÓN.

El responsable de la Información será designado por gerencia por un periodo de 2 años. A tal efecto:

- Determinará los requisitos de seguridad que deban ser garantizados en el tratamiento de la información de la que él es responsable.
- Valorará, para cada información contemplada en el análisis de riesgos, las diferentes dimensiones de la seguridad.
- Aceptará los riesgos residuales, calculados en el análisis de riesgos respecto de la información.
- Realizará el seguimiento y control de los riesgos con la ayuda del responsable de Seguridad.

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 10 de 31	
		Revisión núm. 5	14/02/2025

RESPONSABLE DEL SERVICIO.


El responsable del Servicio será designado por gerencia por un periodo de 2 años. A tal efecto:

- Realizará, junto a los responsables de la Información y el responsable de Seguridad, los preceptivos análisis de riesgos y seleccionarán las salvaguardas que se han de implantar.
- Realizará el seguimiento y control de los riesgos, con la participación del responsable de Seguridad.
- Suspenderá, de acuerdo con el responsable de la Información y el responsable de Seguridad, la prestación de un servicio electrónico o el manejo de una determinada información, si es informado de deficiencias graves de seguridad.

RESPONSABLE DE SEGURIDAD.

El responsable de Seguridad será designado por gerencia por un periodo de 2 años. Tendrá las siguientes funciones:

- Mantener la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.
- Impulsar el cumplimiento normativo definido en, así como velar por el mantenimiento de la documentación de seguridad y la gestión de mecanismos de acceso a la misma.
- Mantener un inventario actualizado de las normas de primer y segundo nivel detalladas, de los nombramientos derivados del procedimiento, así como de los informes de auditorías, autoevaluaciones y análisis de riesgos realizados y de las declaraciones y certificaciones de seguridad.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes de cada período.
- Promover la mejora continua en la gestión de la seguridad de la información.
- Impulsar la formación y concienciación en materia de seguridad de la información.
- Aprobar la declaración de aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema.
- Realizar los preceptivos análisis de riesgos y mantenerlos actualizados según la legislación vigente.
- Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información, y analizar los informes de auditoría, elaborando las conclusiones a presentar a los responsables del Servicio y los responsables de la Información para que adopten las medidas correctoras adecuadas bajo su responsabilidad.

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 11 de 31	
		Revisión núm. 5	14/02/2025

Cualesquiera otras funciones que el Real Decreto 311/2022, de 3 de mayo, asigne a los responsables de seguridad.

Cuando lo justifique la complejidad, la separación física de sus elementos o el número de usuarios de la información en soporte electrónico, o de los sistemas que la manejen, podrán designarse “responsables de seguridad delegados”, dependientes funcionalmente del responsable principal, que serán responsables de las actuaciones que se les deleguen.

RESPONSABLE DEL SISTEMA.

El responsable del Sistema será designado por gerencia por un periodo de 2 años. Será el titular del órgano con competencias en materia de sistemas y tecnologías de la información, y tiene las siguientes funciones:


- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad.
- Suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informado de deficiencias graves de seguridad, previo acuerdo con el responsable de dicha información o servicio, según proceda, y con el responsable de seguridad.

Cuando lo justifique la complejidad, la separación física de sus elementos o el número de usuarios de la información en soporte electrónico, o de los sistemas que la manejen, el responsable del Sistema podrá designar «responsables de sistema delegados», dependientes funcionalmente del responsable principal, que se harán cargo, en su ámbito competencial, de todas aquellas acciones delegadas por el Responsable del Sistema relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del sistema de información. El responsable principal seguirá siendo el responsable final.

RESPONSABLE CONTACTO CON PROVEEDORES.

El Punto de Contacto de Proveedores (POC) será designado por gerencia por un periodo de 2 años, actuará como canal único con terceros en materia de seguridad y tiene las siguientes funciones:

- Actuar como punto único de contacto con proveedores (incl. subcontratas).
- Mantener canal de comunicaciones con los proveedores.
- Mantener el Registro de Proveedores y evidencias asociadas.
- Recabar declaraciones/certificaciones ENS y sus renovaciones, si fuese necesario.

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 12 de 31	
		Revisión núm. 5	14/02/2025

- Verificar cláusulas de seguridad y privacidad en contratos (con Legal).
- Inventariar interconexiones y servicios cloud en alcance.
- Coordinar due diligence y evaluación de riesgos de terceros.
- Proponer criticidad y medidas compensatorias; no aceptar riesgos (elevar a RS/Comité).
- Recibir y canalizar notificaciones de incidentes; coordinar respuesta y evidencias.
- Controlar cambios del proveedor (infra, personal, ubicación, subprocesadores).
- Coordinar pruebas relevantes (DRP/restauración, pentest/escaneos) y recopilar resultados.
- Gestionar offboarding: revocación de accesos y devolución/destrucción certificada de datos.
- Reportar periódicamente al Comité (estado riesgos e incidentes)

5.3 Procedimientos de designación.

*[org.1.3] Los roles o funciones de seguridad, definiendo para cada uno los deberes y responsabilidades del cargo, así como el **procedimiento para su designación y renovación.***

La constitución del Comité de Seguridad de la Información será llevada a cabo por el comité de dirección de IDM Sistemas de Comunicación, y comunicada a los responsables designados. Igualmente la designación de éstos, los responsables de Información, Servicios, Seguridad, Sistemas y Contacto con proveedores será realizada por gerencia de IDM Sistemas de Comunicación, y comunicada a éstos para su aceptación.


Los roles de seguridad serán revisados cada dos años, en el caso de que exista una vacante la misma deberá ser cubierta en el plazo de un mes, siguiendo el mismo procedimiento.

5.4 Resolución de conflictos.

Los conflictos que surjan entre los responsables (RI, RSv, RS, RSis y, en su caso, POC) en relación con requisitos, riesgos, medidas de seguridad, continuidad del servicio, acceso o tratamiento de la información serán tratados y resueltos por el Comité de Seguridad de la Información.

Cuando el asunto lo requiera, la Presidencia (asumida por la gerencia de IDM) podrá convocar sesión extraordinaria. El Comité deliberará sobre alternativas y riesgos y adoptará acuerdo por mayoría simple; en caso de empate, dirime la Presidencia. En situaciones urgentes, la Presidencia, junto con el Responsable de Seguridad y el Responsable de Sistemas cuando proceda, podrá acordar medidas provisionales de contención hasta la resolución formal del Comité.

Las decisiones de resolución de conflictos se documentarán en acta, incluyendo responsables de ejecución, plazos, medidas provisionales (si las hubiera) y, cuando corresponda, su traslado a la declaración de aplicabilidad, Plan de Tratamiento de Riesgos y normativa interna.

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 13 de 31	
		Revisión núm. 5	14/02/2025

Si el sistema o el conflicto afecta al tratamiento de datos personales, se actuará conforme al Reglamento (UE) 2016/679 y a la LO 3/2018, recabando el criterio de la función de privacidad/asesoría legal. En caso de colisión, prevalecerá la normativa de protección de datos sin perjuicio de las obligaciones del ENS.

En conflictos que involucren a proveedores o terceros, el POC coordinará la gestión y se estará a lo pactado en contratos suscritos, elevando al Comité las decisiones que impliquen aceptación de riesgo o medidas compensatorias.

5.5 Estructura del comité.

[org.1.4] La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, las personas integrantes y la relación con otros elementos de la organización.

Composición

1. Responsable de la Información (RI):
2. Responsable del Servicio (RSv):.
3. Responsable de Seguridad (RS):.
4. Responsable del Sistema (RSis):.
5. Punto de Contacto de Proveedores (POC):. *(Figura complementaria para coordinación con terceros).*


En servicios externalizados, salvo causa justificada y documentada, el proveedor deberá designar un POC de seguridad con respaldo de su dirección, responsable de canalizar requisitos de seguridad, evidencias y comunicaciones de incidentes del ámbito del servicio.

Participación adicional. Podrán incorporarse grupos de trabajo especializados (internos, externos o mixtos) y, cuando proceda, Privacidad/Legal para materias RGPD/LOPDGDD.

Funciones del Comité.

El Comité de Seguridad de la Información es el órgano colegiado que coordina, impulsa y supervisa la seguridad de la información en IDM. Entre sus funciones destacan:

1. Promover la mejora continua del sistema de gestión de la seguridad de la información.
2. Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, evitando duplicidades.
3. Elaborar y revisar regularmente la Política y Organización de la Seguridad de la Información, para que sea aprobada por IDM SISTEMAS DE COMUNICACIÓN.
4. Proponer la aprobación de la normativa de seguridad de la información.
5. Promover la realización de las auditorías periódicas, que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
6. Proponer planes de mejora de la seguridad de la información de la organización.
7. Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos de tecnologías de la información, desde su especificación inicial hasta

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 14 de 31	
		Revisión núm. 5	14/02/2025

su puesta en operación y posterior mantenimiento, así como en la preservación de la información, que sea requerida tras el cese en la utilización del mismo.

8. Divulgar la Política de Seguridad de la Información y normativas e instrucciones de seguridad de la información aprobadas.

Funcionamiento.

El Comité de Seguridad de la Información se reunirá, al menos, con periodicidad trimestral en sesión ordinaria y, con carácter extraordinario, cuando lo convoque la Presidencia o ante incidentes o necesidades urgentes.

Los acuerdos se adoptarán por mayoría simple de los asistentes con derecho a voto; en caso de empate, decidirá la Presidencia.

Toda sesión generará acta con puntos tratados, acuerdos, responsables, plazos y evidencias, y se dará seguimiento en la sesión posterior.

5.6 Instrumentos de desarrollo.

[org.1.5] Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.


El cumplimiento de los objetivos de esta Política se materializa en un cuerpo documental coherente con el ENS, integrado por Política de Seguridad → Normativa de primer y segundo nivel → procedimientos e instrucciones técnicas → guías/estándares de configuración → registros/evidencias.

Cada documento establecerá:

- Jerarquía y codificación documental (PSI → normativa → procedimientos/instrucciones → registros/evidencias) y su ámbito.
- Propiedad, elaboración, revisión y aprobación de cada documento (roles responsables).
- Control de cambios y versionado.
- Datos mínimos (código, título, propietario, aprobador, estado).
- Gestión de acceso bajo mínimo privilegio y difusión controlada (autorizaciones, registros de acceso y prohibición de copias no autorizadas).
- Integridad (firmas/aprobaciones) y recuperación (copias y restauraciones verificadas).

La revisión anual de la presente Política corresponde al Comité de Seguridad de la Información, que propondrá, cuando proceda, mejoras para su aprobación por el mismo órgano que la aprobó inicialmente. La normativa y procedimientos vinculados se revisarán al menos una vez al año o antes si existen cambios normativos, técnicos o de riesgo que lo aconsejen.

La documentación de seguridad se custodia en repositorios corporativos autorizados; su acceso se concede por rol/función y queda trazado. La publicación externa (si la

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 15 de 31	
		Revisión núm. 5	14/02/2025

hubiese) se limitará a lo exigido contractual o legalmente, garantizando que no se expone información sensible.

Se siguen las directrices y recomendaciones de CCN-STIC 808 (verificación del cumplimiento ENS) y las guías aplicables que precise la organización en su anexo legal y en el mapa documental.

6. NORMATIVA DE SEGURIDAD.

6.1 Objeto y alcance.

Esta normativa de seguridad establece los principios y reglas de obligado cumplimiento aplicables a las personas, activos y servicios en el alcance ENS de IDM. Su desarrollo operativo se detalla en los **procedimientos (org.3)** y en las guías técnicas vinculadas.

6.2 Uso correcto de equipos, servicios e instalaciones (y uso indebido).

[org.2.1] El uso correcto de equipos, servicios e instalaciones, así como lo que se considerará uso indebido.

Queda definido el **uso aceptable** de los medios puestos a disposición por IDM: puestos de trabajo, portátiles y móviles corporativos, redes, correo, herramientas colaborativas, repositorios, impresoras y accesos remotos.

Se **prohíben** usos indebidos (instalación de software no autorizado, elusión de controles, uso personal intensivo, custodia negligente de credenciales, conexión de dispositivos no autorizados, extracción no autorizada de información, entre otros).

6.3 Responsabilidad del personal: derechos, deberes y medidas disciplinarias.


[org.2.2] La responsabilidad del personal con respecto al cumplimiento o violación de la normativa: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

Todo el personal es responsable del cumplimiento de la Política de Seguridad y de la normativa derivada. IDM garantiza los derechos de información y confidencialidad y exige el cumplimiento de las obligaciones de seguridad, pudiendo aplicar medidas disciplinarias y contractuales según la normativa laboral/mercantil aplicable. La formación y concienciación es obligatoria y periódica; la aceptación de la normativa quedará documentada.

6.4 Principios aplicables (art. 6 y 20 RD 311/2022).

Art. 6. La seguridad como proceso integral.

La seguridad se gestiona como proceso integral, constituido por todos los elementos técnicos, humanos, materiales, jurídicos y organizativos, relacionados con el

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 16 de 31	
		Revisión núm. 5	14/02/2025

sistema. La aplicación del Esquema Nacional de Seguridad a IDM SISTEMAS DE COMUNICACIÓN, estará presidida por este principio.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y coordinación, o de instrucciones inadecuadas, constituyan fuentes de riesgo para la seguridad.

Art. 20. Mínimo privilegio.

Así como el sistema de información de IDM está guiado por el principio de mínimo privilegio necesario para su correcto desempeño, que implica incorporar los siguientes aspectos:

- El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.
- Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.

En resumen, los sistemas se configuran para reducir superficie de exposición; se deshabilita funcionalidad innecesaria y se aplican guías de configuración adecuadas a la categoría ENS.

Vigilancia continua, reevaluación periódica e integridad, actualización del sistema y mejora continua del proceso de seguridad.


La vigilancia continua por parte de IDM SISTEMAS DE COMUNICACIÓN, permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

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.

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 17 de 31	
		Revisión núm. 5	14/02/2025

vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

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

7. PROCEDIMIENTOS DE SEGURIDAD.

Éste apartado concreta cómo se ejecutan las tareas habituales de seguridad, quién las realiza, cómo se identifican y comunican anomalías y cómo se trata la información según su nivel de seguridad.

7.1 Como llevar a cabo las tareas habituales.

[org.3.1] Cómo llevar a cabo las tareas habituales.

Gestión de Equipos y Activos

- Se identificarán y registrarán todos los equipos que contienen activos esenciales, como el NAS y el servidor, en un inventario de activos de la organización.
- Se asignarán roles y permisos de acceso limitados a los usuarios según las necesidades operativas de la organización y el principio de mínimos privilegios.


Tareas Habituales

- Los usuarios realizarán tareas habituales a nivel de uso general, como acceso a la información almacenada en el NAS y el servidor, de acuerdo con los roles y permisos asignados.
- Los administradores recibirán actualizaciones periódicas sobre el estado, la memoria, la seguridad y la salud general de los equipos revisiones semestrales.
- Los administradores realizan tareas de mantenimiento y soporte de forma periódica sobre los equipos asignados de la organización; así como revisiones de los sistemas de información.

7.2 Quien debe hacer cada tarea.

[org.3.2] Quién debe hacer cada tarea.

- Responsable de Seguridad (RS): supervisa implantación, evidencia y cumplimiento de los procedimientos; coordina incidentes.
- Responsable del Sistema (RSis): opera y mantiene plataformas; aplica bastionado, parches, cambios y copias.
- Responsable del Servicio (RSv): vela por la continuidad y calidad del servicio; coordina con terceros (POC).

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 18 de 31	
		Revisión núm. 5	14/02/2025

- Responsable de la Información (RI): clasifica información y valida accesos y riesgos residuales.
- POC (proveedores): coordina requisitos ENS, evidencias y ANS/SLA con terceros.
- Usuarios: Cumplir con las medidas de seguridad establecidas y reportar cualquier comportamiento anómalo.

7.3 Como identificar y reportar comportamientos anómalos.

[org.3.3] Cómo identificar y reportar comportamientos anómalos.

- Se establecerá un procedimiento de notificación en caso de mal funcionamiento o comportamientos anómalos tanto en los equipos de trabajo individuales como en los terminales de uso general.
- Los usuarios estarán capacitados para identificar y reportar cualquier anomalía o incidente de seguridad a través de un canal de comunicación establecido.

7.4 La forma en que se ha de tratar la información en consideración al nivel de seguridad que requiere.

[org.3.4.] La forma en que se ha de tratar la información en consideración al nivel de seguridad que requiere, precisando cómo efectuar:

- a) ***Su control de acceso.***
- b) ***Su almacenamiento.***
- c) ***La realización de copias.***
- d) ***El etiquetado de soportes.***
- e) ***Su transmisión telemática.***
- f) ***Cualquier otra actividad relacionada con dicha información.***


8. PROCESOS DE AUTORIZACIÓN.

Se establece un proceso formal de autorizaciones que cubra todos los elementos del sistema de información concernidos.

8.1 Utilización de instalaciones, habituales y alternativas.

[org.4.1] Utilización de instalaciones, habituales y alternativas.

- Descripción: Autorización para utilizar las instalaciones físicas y virtuales.
- Responsable: responsable de seguridad.
- Procedimiento:
 1. El solicitante completa un formulario de solicitud de uso de instalaciones.
 2. El Gerente de Infraestructura verifica la disponibilidad y asigna el recurso.
 3. Se emite una autorización formal para el uso de las instalaciones.

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 19 de 31	
		Revisión núm. 5	14/02/2025

8.2 Entrada de equipos en producción, en particular, equipos que involucren criptografía.

[org.4.2] Entrada de equipos en producción, en particular, equipos que involucren criptografía.

- Descripción: Autorización para incorporar equipos al entorno de producción.
- Responsable: responsable de seguridad.
- Procedimiento:
 1. El equipo correspondiente en cada caso solicita la entrada de un nuevo servidor.
 2. Se verifica que el equipo cumpla con los estándares de seguridad y criptografía.
 3. Se emite una autorización formal para su entrada en producción.

8.3 Entrada de aplicaciones en producción.

[org.4.3] Entrada de aplicaciones en producción.

- Descripción: Autorización para implementar aplicaciones en el entorno de producción.
- Responsable: responsable de sistemas.
- Procedimiento:
 1. El equipo de desarrollo presenta la aplicación para su revisión.
 2. Se realizan pruebas de seguridad y rendimiento.
 3. Se emite una autorización formal para su entrada en producción.

8.4 Establecimiento de enlaces de comunicaciones con otros sistemas.

[org.4.4] Establecimiento de enlaces de comunicaciones con otros sistemas.

- Descripción: Autorización para conectar sistemas internos y externos.
- Responsable: responsable de seguridad.
- Procedimiento:
 1. Se evalúa la seguridad de los enlaces propuestos.
 2. Se verifica la autenticidad de los sistemas remotos.
 3. Se emite una autorización formal para establecer los enlaces.

8.5 Utilización de medios de comunicación, habituales y alternativos.


[org.4.5] Utilización de medios de comunicación, habituales y alternativos.

- Descripción: Autorización para utilizar medios de comunicación (correo electrónico, mensajería, etc.).
- Responsable: responsable de seguridad.
- Procedimiento:
 1. Se establecen políticas de uso seguro de los medios de comunicación.
 2. Se capacita al personal sobre las mejores prácticas.
 3. Se emite una autorización formal para su uso.

8.6 Utilización de soportes de información.

[org.4.6] Utilización de soportes de información.

- Descripción: Autorización para utilizar medios físicos (discos duros, USB, etc.).

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 20 de 31	
		Revisión núm. 5	14/02/2025

- Responsable: responsable de seguridad.
- Procedimiento:
 1. Se establecen políticas de seguridad para el uso de soportes físicos.
 2. Se verifica la encriptación de datos sensibles.
 3. Se emite una autorización formal para su uso.

8.7 Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, tabletas, teléfonos móviles u otros de naturaleza análoga.

[org.4.7] Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, tabletas, teléfonos móviles u otros de naturaleza análoga

- Descripción: Autorización para utilizar dispositivos móviles.
- Responsable: responsable de seguridad.
- Procedimiento:
 1. Se establecen políticas de seguridad para dispositivos móviles.
 2. Se verifica la instalación de software de seguridad.
 3. Se emite una autorización formal para su uso.

8.8 Utilización de servicios de terceros, bajo contrato o convenio, concesión, encargo, etc.

[org.4.8] Utilización de servicios de terceros, bajo contrato o convenio, concesión, encargo, etc.

- Descripción: Autorización para utilizar servicios proporcionados por terceros.
- Responsable: responsable de seguridad.
- Procedimiento:
 1. Se evalúa la seguridad y confiabilidad de los servicios.
 2. Se revisan los contratos y acuerdos.
 3. Se emite una autorización formal para su uso.


9. CUMPLIMIENTO DE LOS REQUISITOS MÍNIMOS DE SEGURIDAD.

IDM SISTEMAS DE COMUNICACIÓN aplica los requisitos mínimos del Esquema Nacional de Seguridad conforme al Real Decreto 311/2022, de 3 de mayo. Las medidas de seguridad se seleccionan e implantan de forma proporcional a la naturaleza de la información, a los servicios a proteger y a la categoría ENS del sistema, siguiendo el principio de proporcionalidad y la gestión basada en riesgos.

Las medidas y su eficacia se revisan con carácter periódico y ante cambios relevantes (tecnológicos, normativos o de riesgo), garantizando la mejora continua del proceso de seguridad y la adecuación permanente al ENS.

10. GESTIÓN DE PERSONAL Y PROFESIONALIDAD.

Art. 15. Gestión del personal. Art. 16. Profesionalidad. [org.2.2] Responsabilidad del personal.

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 21 de 31	
		Revisión núm. 5	14/02/2025

Todo el personal, propio y de terceros, que intervenga en los sistemas y servicios en alcance ENS de IDM SISTEMAS DE COMUNICACIÓN será informado y formado en sus deberes, obligaciones y responsabilidades en materia de seguridad. El uso de los sistemas está supervisado para verificar el cumplimiento de los procedimientos y para detectar desviaciones, bajo los principios de proporcionalidad y necesidad de conocer.

La responsabilidad del personal respecto del cumplimiento o violación de la normativa se rige por esta Política y por la legislación vigente. Los derechos y deberes se concretan en las normas internas de IDM y, cuando proceda, en la normativa laboral y de protección de datos. El uso indebido de los sistemas, la inobservancia de medidas de seguridad o la vulneración de confidencialidad podrán conllevar medidas disciplinarias conforme al régimen interno y/o contractual aplicable, sin perjuicio de otras responsabilidades que pudieran derivarse.

IDM define y mantiene los requisitos de competencia y experiencia para cada puesto con impacto en la seguridad (extracto de RPT y fichas de puesto), asegurando que las funciones se desempeñan por personal competente (art. 16). Se implantan planes de concienciación y formación continua adecuados a la categoría ENS de los sistemas y a los riesgos existentes, con registro de asistencia y evaluación de eficacia. La capacitación incluye, entre otros, protección de la información, control de accesos, gestión de incidentes, uso aceptable, teletrabajo y movilidad, y tratamiento de datos personales cuando aplique.

El personal de terceros (proveedores, subcontratas) deberá asumir obligaciones equivalentes a las del personal propio: confidencialidad, observancia de la normativa de seguridad y formación específica cuando proceda. Estas obligaciones se reflejan en los contratos y se gestionan a través del POC y del Responsable del Servicio, pudiendo requerirse evidencias (declaraciones, certificaciones o formación impartida).


11. GESTIÓN DE LA SEGURIDAD BASADA EN LOS RIESGOS, ANÁLISIS Y GESTIÓN DE RIESGOS.

Artículo 14. Análisis y gestión de los riesgos.

El análisis y la gestión de los riesgos será parte esencial del proceso de seguridad y será una actividad continua y permanentemente actualizada.

La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. 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.

Esta gestión 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 del Real Decreto

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 22 de 31	
		Revisión núm. 5	14/02/2025

311/2022, de 3 de mayo, se empleará alguna metodología reconocida internacionalmente. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

12. INCIDENTES DE SEGURIDAD, PREVENCIÓN, DETECCIÓN, REACCIÓN Y RECUPERACIÓN.

El IDM SISTEMAS DE COMUNICACIÓN, dispondrá de procedimiento de gestión de incidentes de seguridad de acuerdo con lo previsto en el artículo 33 del Real Decreto 311/2022, de 3 de mayo, y de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas.

La seguridad del sistema contemplará las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

Las medidas de prevención podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

Las medidas de respuesta se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

El sistema de información garantizará la conservación de los datos e información en soporte electrónico.


De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación de todos los activos.

IDM, hemos desarrollado un procedimiento de quejas.

La principal utilidad de un procedimiento de quejas en el contexto del ENS de categoría media (o cualquier categoría) es establecer un **mecanismo formal y accesible** para que los usuarios (internos y externos), clientes o terceros puedan **notificar, expresar su disconformidad o alertar** sobre aspectos relacionados con la seguridad de los servicios y sistemas de información de la organización.

Sirve para:

1. Identificar y corregir fallos: Permite a la organización tomar conocimiento de debilidades, deficiencias, incumplimientos o incidentes que podrían no haber sido

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 23 de 31	
		Revisión núm. 5	14/02/2025

- detectados por los mecanismos internos habituales (como auditorías o monitorización).
2. Gestión de no conformidades: Proporciona una vía estructurada para registrar y gestionar las no conformidades o las percepciones de riesgo por parte de los afectados.
 3. Mejora Continua: Las quejas y sus resoluciones son una fuente de información valiosa para el ciclo de mejora continua del sistema de gestión de seguridad, ayudando a reforzar las medidas de seguridad deficientes.
 4. Transparencia y confianza: Demuestra el compromiso de la organización con la seguridad y con la atención a los usuarios. Ofrecer un canal de quejas aumenta la confianza de los ciudadanos y clientes en los servicios prestados, especialmente en el ámbito de la administración Electrónica.
 5. Cumplimiento Normativo: Contar con un procedimiento documentado y operativo es parte de las medidas de seguridad de carácter organizativo que el ENS exige para demostrar un nivel adecuado de protección de la información.

“La gestión de quejas y reclamaciones formales se realiza conforme al procedimiento PE-004 ‘Gestión de reclamaciones y medición de satisfacción del cliente’. Cuando una queja implique o pueda implicar un incidente de seguridad, se tramitará además conforme al PR06 (Gestión de Incidentes), manteniendo trazabilidad entre registros.”

13. EXISTENCIA DE LÍNEAS DE DEFENSA Y PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS.


IDM SISTEMAS DE COMUNICACIÓN, mantendrá actualizada una estrategia de protección del sistema de información constituida por múltiples capas de seguridad, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una capa sea comprometida permita desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto y minimizar el impacto final sobre el mismo.

Se protegerá el perímetro del sistema de información, especialmente, cuando el sistema de la empresa se conecta a redes públicas, tal y como se definen en la legislación vigente en materia de telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

14. DIFERENCIACIÓN DE RESPONSABILIDADES, ORGANIZACIÓN E IMPLANTACIÓN DEL PROCESO DE SEGURIDAD.

Artículo 11. Diferenciación de responsabilidades.

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 24 de 31	
		Revisión núm. 5	14/02/2025

IDM SISTEMAS DE COMUNICACIÓN, organizará su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas. [org.1.3].

Es importante puntualizar que la responsabilidad de seguridad recae en el Responsable de la Información mientras que la explotación de sistemas es responsabilidad del proveedor de servicios. Ambos roles trabajan en conjunto para garantizar la seguridad y el funcionamiento adecuado de los sistemas de información.

15. AUTORIZACIÓN Y CONTROL DE LOS ACCESOS.

Artículo 17. Autorización y control de los accesos.

IDM SISTEMAS DE COMUNICACIÓN, implementará mecanismos de control de acceso al sistema de información, limitándolo a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

16. PROTECCIÓN DE LAS INSTALACIONES.

Artículo 18. Protección de las instalaciones.

IDM SISTEMAS DE COMUNICACIÓN, implementará mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

17. ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD Y CONTRATACIÓN DE SERVICIOS DE SEGURIDAD.


Artículo 19. Adquisición de productos de seguridad y contratación de servicios de seguridad.

Para la adquisición de productos o contratación de servicios de seguridad IDM SISTEMAS DE COMUNICACIÓN, tendrá en cuenta la utilización de forma proporcionada a la categoría del sistema y el nivel de seguridad determinado, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

Para la contratación de servicios de seguridad se atenderá a lo señalado en cuanto a la profesionalidad.

18. PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO Y CONTINUIDAD DE LA ACTIVIDAD.

IDM SISTEMAS DE COMUNICACIÓN, prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección. Se

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 25 de 31	
		Revisión núm. 5	14/02/2025

aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

19. REGISTRO DE ACTIVIDAD Y DETECCIÓN DE CÓDIGO DAÑINO.


IDM SISTEMAS DE COMUNICACIÓN, con el propósito de satisfacer el objeto de este real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, y demás disposiciones que resulten de aplicación, registrará las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de la empresa, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, el IDM SISTEMAS DE COMUNICACIÓN, podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

20. INFRAESTRUCTURAS Y SERVICIOS COMUNES.

IDM SISTEMAS DE COMUNICACIÓN, tendrá en cuenta que la utilización de infraestructuras y servicios comunes de la empresa, incluidos los compartidos o transversales, facilitará el cumplimiento de lo dispuesto en este real decreto.

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 26 de 31	
		Revisión núm. 5	14/02/2025

21. PERFILES DE CUMPLIMIENTO ESPECÍFICOS Y ACREDITACIÓN DE ENTIDADES DE IMPLEMENTACIÓN DE CONFIGURACIONES SEGURAS

IDM SISTEMAS DE COMUNICACIÓN, tendrá en cuenta la aplicación de aquellos perfiles de cumplimiento específicos para empresas que sean de aplicación.

Revisión de la política. La revisión de la Política deberá garantizar que ésta se encuentra alineada con la estrategia, la misión y visión IDM SISTEMAS DE COMUNICACIÓN, en materia de seguridad de la información y que asegura el cumplimiento de los objetivos de control establecidos.

En relación a las revisiones que puedan realizarse sobre la redacción del texto que constituye la Política, se distinguirán tres tipos de actividades:

- Revisiones periódicas, que se realizarán, al menos, con una periodicidad anual.
- Revisiones sistemáticas: Deberán realizarse cuando se detecten incidencias o cambios en el marco legal que puedan cuestionar la validez de dicha Política. *[org.1.2] El marco legal y regulatorio en el que se desarrollarán las actividades.*
- Revisiones no planificadas: Estas revisiones deberán realizarse en respuesta a cualquier evento o incidente de seguridad que pudiera suponer un incremento significativo del nivel de riesgo actual o que haya causado un impacto en la seguridad de la información IDM SISTEMAS DE COMUNICACIÓN.


22. TERCERAS PARTES.

Cuando IDM SISTEMAS DE COMUNICACIÓN, preste servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. IDM, definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad, así como el resto de las actuaciones que IDM, lleve a cabo en materia de Seguridad en relación con otros organismos.

Cuando IDM, utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad existente que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias.

Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

De igual modo, teniendo en cuenta la obligación de cumplir con lo dispuesto en las Instrucciones Técnicas de Seguridad recogida en la Disposición adicional segunda

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 27 de 31	
		Revisión núm. 5	14/02/2025

(Desarrollo del Esquema Nacional de Seguridad) del Real Decreto Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y en consideración a la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, donde se establece que los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA.

Cuando algún aspecto de esta Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Dicho informe deberá ser aprobado por los responsables de información y los servicios, con carácter previo al inicio de la relación con la tercera parte.

23. CATEGORIA DE SEGURIDAD.

Artículo 40. Categorías de seguridad.

1. La categoría de seguridad de un sistema de información modulará el equilibrio entre la importancia de la información que maneja y los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el principio de proporcionalidad.

2. La determinación de la categoría de seguridad se efectuará en función de la valoración del impacto que tendría un incidente que afectase a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, siguiendo el procedimiento descrito en el anexo I.


ANEXO I. Categorías de seguridad de los sistemas de información

1. Fundamentos para la determinación de la categoría de seguridad de un sistema de información.

La determinación de la categoría de seguridad de un sistema de información se basará en la valoración del impacto que tendría sobre la organización un incidente que afectase a la seguridad de la información tratada o de los servicios prestados para:

- a) Alcanzar sus objetivos.*
- b) Proteger los activos a su cargo.*
- c) Garantizar la conformidad con el ordenamiento jurídico.*

Anualmente, o siempre que se produzcan modificaciones significativas en los citados criterios de determinación, deberá re-evaluarse la categoría de seguridad de los sistemas de información concernidos.

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 28 de 31	
		Revisión núm. 5	14/02/2025

2. Dimensiones de la seguridad

A fin de determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información tratada o de los servicios prestados y, en su consecuencia, establecer la categoría de seguridad del sistema de información en cuestión, se tendrán en cuenta las siguientes dimensiones de la seguridad, que se identificarán por sus correspondientes iniciales en mayúsculas:

- a) Confidencialidad [C].*
- b) Integridad [I].*
- c) Trazabilidad [T].*
- d) Autenticidad [A].*
- e) Disponibilidad [D].*

3. Determinación del nivel de seguridad requerido en una dimensión de seguridad

Una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles de seguridad: BAJO, MEDIO o ALTO. Si una dimensión de seguridad no se ve afectada, no se adscribirá a ningún nivel.

b) Nivel MEDIO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio grave:


- 1.º La reducción significativa de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias, aunque estas sigan desempeñándose.*
- 2.º Causar un daño significativo en los activos de la organización.*
- 3.º El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.*
- 4.º Causar un perjuicio significativo a algún individuo, de difícil reparación.*
- 5.º Otros de naturaleza análoga.*

Cuando un sistema de información trate diferentes informaciones y preste diferentes servicios, el nivel de seguridad del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio.

4. Determinación de la categoría de seguridad de un sistema de información

1. Se definen tres categorías de seguridad: BÁSICA, MEDIA y ALTA.

- a) Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad ALTO.*
- b) Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad MEDIO, y ninguna alcanza un nivel de seguridad superior.*

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 29 de 31	
		Revisión núm. 5	14/02/2025

c) Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

2. La determinación de la categoría de seguridad de un sistema de información sobre la base de lo indicado en el apartado anterior, no implicará que se altere, por este hecho, el nivel de seguridad de las dimensiones de seguridad que no han influido en la determinación de la categoría de seguridad del mismo.

5. Secuencia de actuaciones para determinar la categoría de seguridad de un sistema

1. Identificación del nivel de seguridad correspondiente a cada información y servicio, en función de las dimensiones de seguridad, teniendo en cuenta lo establecido en el apartado 3 anterior.


2. Determinación de la categoría de seguridad del sistema, según lo establecido en el apartado 4 anterior.

Las guías CCN-STIC, del CCN, precisarán los criterios necesarios para una adecuada categorización de seguridad de los sistemas de información

24. PROCESO DE APROBACIÓN Y REVISIÓN.


La Política de Seguridad de la Información (PSI) ENS de IDM SISTEMAS DE COMUNICACIÓN es propuesta por el Comité de Seguridad y aprobada por Gerencia (órgano competente), quedando vigente desde la fecha indicada en su portada y sustituyendo a cualquier versión anterior.

La PSI se revisa al menos anualmente y, adicionalmente, cuando las circunstancias técnicas u organizativas lo requieran, Las actualizaciones mantienen trazabilidad mediante control de cambios (versión, motivo, aprobaciones, fecha de entrada en vigor) y registro de difusión.

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 30 de 31	
		Revisión núm. 5	14/02/2025

25. REGISTROS.

CODIGO	REGISTRO	NORMA	RESPONSABLE	VIGENCIA
F-PRENS02-1	Registro marco legal en materia de seguridad	<i>Org Marco organizativo</i>	Responsable de la información.	2 años, salvo modificaciones normativas
F-PRENS02-2	Registro de ITS y las guías CCN-STIC aplicables	<i>Refuerzo R1- Documentos específicos. [org.2.r1.1]</i>	Responsable de la información	2 años.
F-PRENS02-3	Registro de nombramientos	<i>Org Marco organizativo</i>	Responsable de la información	2 años
F-PRENS02-4	Documento donde se desarrolla org.3.4.	<i>Org Marco organizativo</i>	Responsable de la información	2 años
F-PRENS02-5	Acta de reuniones del comité	<i>Org Marco organizativo</i>	Responsable de la información.	2 años.
F-PRENS02-6	Lista de documentación en vigor	<i>Refuerzo R1- Documentos específicos. [org.2.r1.1]</i>	Responsable de la información	2 años.
F-PRENS02-7	Jornada de formación	<i>Org Marco organizativo</i>	Responsable de la información	2 años.

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD	PR-ENS-02	
	TITULO POLÍTICA DE SEGURIDAD	Página 31 de 31	
		Revisión núm. 5	14/02/2025

ANEXO I.

Se ha generado una lista de documentos con enlace al buscador en lugar de un repositorio con los documentos.

El ENS no solo se compone del Real Decreto 311/2022, sino que se desarrolla a través de un amplio conjunto de Instrucciones Técnicas de Seguridad (ITS) y Guías de Seguridad publicadas por el CCN-CERT (Centro Criptológico Nacional).

La propuesta de cambiar un "repositorio con los documentos" por una "lista de documentos con enlace al buscador" sirve para mejorar la usabilidad y la eficiencia en el proceso de cumplimiento del ENS:

Elemento	Repositorio (Método Actual/Anterior)	Lista con Enlace al Buscador (OM Propuesta)
Búsqueda	El usuario debe descargar o examinar el documento completo para encontrar la información.	Permite buscar directamente por palabras clave dentro del contenido de todos los documentos o en la lista descriptiva.
Contexto	Se ven muchos documentos juntos, lo que puede ser abrumador.	La lista puede ofrecer una descripción concisa y un enlace directo a la sección relevante o al documento completo, facilitando la comprensión del propósito.
Actualización	Si un documento se actualiza, es posible que el usuario tenga una versión antigua descargada localmente.	Al usar el buscador y enlazar siempre al sitio oficial, el usuario siempre accede a la última versión oficial de la Guía o ITS.
Implementación	Dificulta la tarea del Responsable de Seguridad o Auditor para localizar rápidamente la Guía específica que aborda un control o medida del ENS.	Acelera la identificación de la documentación de apoyo necesaria para implementar una medida de seguridad concreta.

En resumen, esta oportunidad de mejora implementada está orientada a la gestión del conocimiento y busca agilizar el cumplimiento del ENS, haciendo que las ITS y Guías de Seguridad sean más accesibles, localizables y siempre actualizadas para los responsables de seguridad y auditores.


Juan Carlos Manresa Vila

Alta dirección/Gerencia de IDM Sistemas de Comunicación S.L
Aprueba la Política de Seguridad