Cenit

Política de seguridad

Sistema de Gestión de la Seguridad de la Información

Versión 06.00

1 Introducción

La empresa **Consultoría Estratégica de Negocio IT**[1] depende de los sistemas TIC para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El **objetivo** de la seguridad de la información es **garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes**.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que las distintas áreas de la empresa deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad[2], así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

La empresa debe cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación.

La empresa debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el artículo 8 del ENS.

1.1 Prevención

La empresa debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, las áreas afectadas deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, la organización debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.

[1] En adelante, CENIT.

[2] En adelante, ENS. Definido en el Real Decreto 311/2022, de 3 de mayo.

- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

1.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios se monitorizan de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.

La monitorización es especialmente relevante en las líneas de defensa establecidas. Se establecen mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

1.3 Respuesta

La empresa dispone de:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Un punto de contacto para las comunicaciones con respecto a incidentes detectados de manera interna o en otros organismos.
- Protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias[3].

1.4 Conservación

Para garantizar la disponibilidad de los servicios críticos, la organización dispone de un plan de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

2 Alcance

Esta política de seguridad de la información[4] se aplica a los alcances establecidos para cada uno de los sistemas de gestión internos de la empresa relacionados con la prestación de servicios a los clientes.

- Sistema de Gestión de la Calidad y Medio Ambiente:
  - Diseño, desarrollo y mantenimiento de sistemas de información
  - Oficinas técnicas de proyecto TIC
- Sistema de Gestión de Servicios: ídem.

[3] En adelante, CERT.

[4] También denominada política de seguridad o PSI en el resto del documento.

- Sistema de Gestión de la seguridad de la Información: los sistemas de información que soportan las actividades de los servicios de gestión interna de proyectos.

La política de seguridad afecta a todas las personas de la empresa involucradas en estas gestiones.

3 Misión, visión y valores

3.1 Misión

"Potenciar el proceso de transformación digital de las entidades públicas mediante la aportación de servicios profesionalizados, confiables y cercanos".

3.2 Visión

"Ser la consultora TI de referencia en el Sector, por su aportación de valor, por la gestión del talento, y por su compromiso social".

3.3 Valores

- Honestidad. "Hacemos lo que decimos y decimos lo que hacemos".
- Cercanía. "Empatizamos con las inquietudes de clientes y empleados".
- Profesionalidad. "Hacemos nuestra la aplicación de buenas prácticas y metodologías".
- Compromiso. "Los objetivos de nuestros clientes son también nuestros objetivos".
- Pasión. "Nuestra actividad nos entusiasma y disfrutamos de nuestros logros".
- Conciencia social. "Nos solidarizamos con las realidades sociales que requieren apoyo y atención".

4 Marco normativo

Para la construcción del **Sistema de Gestión de la Seguridad de la Información**[5] se tendrán en cuenta los requisitos aplicables de las normativa vigente. Para ello se dispone de un responsable normativo y un procedimiento para su revisión y actualización periódica. El cuadro adjunto es parte del listado completo que se recoge en el Registro de Disposiciones legales.

Título	Fecha
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	12/04/1996

[5] En adelante, SGSI.

Título	Fecha
Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico	11/07/2002
Ley 59/2003 de firma electrónica	19/12/2003
Ley 39/2015 del Procedimiento Administrativo Común de las Administraciones Públicas	01/10/2015
Ley 40/2015 de Régimen Jurídico del Sector Público	01/10/2015
REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)	26/04/2016
Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales	05/12/2018
Real Decreto 311/2022por el que se regula el Esquema Nacional de Seguridad	03/05/2022
XVIII Convenio colectivo estatal de empresas de consultoría y estudios de mercado y de la opinión pública	13/07/2023

Otras normas / guías utilizadas:

- UNE-ISO/IEC 17799, que contiene las mejores prácticas para la Gestión de la Seguridad de la Información.
- UNE-ISO/IEC 27001, que contiene las mejores prácticas recomendadas en Seguridad de la Información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información.
- UNE-ISO/IEC 31000, que proporciona directrices para gestionar el riesgo al que se enfrentan las organizaciones.
- MAGERIT. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

5 Organización de la seguridad

Teniendo en cuenta las características de la empresa, se constituyen los órganos descritos en los apartados siguientes.

Para la gestión del sistema se han considerado tres grandes bloques de responsabilidad:

1. La responsabilidad legal y la especificación de las necesidades o requisitos, que corresponde a la Dirección de la entidad y al responsable de la información y del servicio[6].

[6] En adelante, RIS.

2. La supervisión, que corresponde al responsable de la seguridad[7].
3. La operación del sistema de información, que corresponde al responsable del sistema[8].

5.1 Comité de seguridad corporativa

El comité de seguridad corporativa[9] estará compuesto por los miembros del comité de dirección de la empresa y por el RSG.

Sus funciones son:

- Aprobar la política de seguridad, las normas y los procedimientos que enmarcan el uso del servicio.
- Respaldar explícita y notoriamente las actividades de seguridad TIC en la organización.
- Aprobar los presupuestos presentados por el RSG cuando sobrepasen una cantidad determinada.
- Coordinar todas las funciones de seguridad de la empresa.
- Velar por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial.
- Velar por el alineamiento de las actividades de seguridad y los objetivos de la organización.
- Coordinar y aprobar las propuestas recibidas de los diferentes ámbitos de seguridad.
- Recabar informes regulares sobre el estado de seguridad de la organización y de los posibles incidentes del RSG.
- Coordinar y dar respuesta a las inquietudes transmitidas a través del RSG.
- Definir, dentro de la PSI, la asignación de roles y los criterios para alcanzar las garantías que estime pertinentes en lo relativo a segregación de tareas.
- Aprobar los requisitos de formación y calificación de los distintos tipos de usuario del servicio desde el punto de vista de la seguridad.
- Actuar como Comité de Crisis en caso de desastre.

5.2 Responsable de la información y del servicio

Las figuras de responsable de la información y responsable del servicio recaerán en la misma persona. Sus funciones son las enumeradas a continuación.

- Determinar los requisitos de seguridad de la información tratada y de los servicios prestados.
- Valorar las consecuencias de un impacto negativo sobre la seguridad de la información y de los servicios, atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los interesados.

[7] En adelante, RSG.

[8] En adelante, RST.

[9] En adelante, CSC.

- Incluir las especificaciones de seguridad en el ciclo de vida de los sistemas, acompañadas de los correspondientes procedimientos de control.
- Encargarse de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el RSG.
- Cerciorarse de que las medidas de seguridad se integran adecuadamente en el marco general de seguridad.
- Proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. La decisión final, que será tomada por la Dirección de la entidad, debe ser acordada con el RSG.

Es el responsable último del uso que se haga de la información manejada en los servicios incluidos en el alcance de la política de seguridad y, por tanto, de su protección.

Es el responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad, de integridad (en materia de protección de datos) o de disponibilidad (en materia de seguridad de la información).

Esta figura será asumida por la persona que ocupe la Dirección de Producción y reporta directamente al CSC.

5.3 Responsable de seguridad

Las funciones del RSG son las siguientes.

- Estar al tanto de cambios normativos (leyes, reglamentos o prácticas sectoriales) que afecten a la organización, debiendo informarse de las consecuencias para las actividades de la empresa, alertando al CSC y proponiendo las medidas oportunas de adecuación al nuevo marco.
- Tomar las decisiones del día a día entre las reuniones del CSC, en especial en caso de incidencias que tengan repercusión fuera de la organización y en caso de desastres.
- Coordinar todas las actuaciones relacionadas con cualquier aspecto de la seguridad de la empresa en caso de desastre.
- Redactar la política de seguridad de la información, las normas y los procedimientos relativos a la seguridad de la empresa.
- Elaborar un análisis de riesgos de los sistemas, análisis que será presentado al CSC para su aprobación. Este análisis debe actualizarse al menos una vez al año.
- Ejecutar regularmente verificaciones de seguridad según un plan determinado y aprobado por el CSC. Los resultados de estas inspecciones se presentarán al CSC para su conocimiento y aprobación. Si como resultado de la inspección aparecen incumplimientos, propondrá medidas correctoras que presentará al CSC para su aprobación, responsabilizándose de que sean llevadas a cabo.
- Elaborar los requisitos de formación y calificación de los distintos tipos de usuario del servicio desde el punto de vista de la seguridad.
- Identificar las tareas de administración y operación que garanticen la satisfacción de los criterios y requisitos de segregación de tareas impuestos por el CSC.

- Actuar como interlocutor oficial con otras organizaciones.
- Coordinar la respuesta ante incidentes que desborden los casos previstos y procedimentados.
- Coordinar la investigación forense relacionada con los incidentes que considere relevantes.

5.4 Responsable normativo

Sus funciones serán desarrolladas por el RSG:

- Mantenimiento actualizado del Registro de Disposiciones Legales.
- Comunicación a toda la organización de los cambios legales significativos en la materia a través de los canales establecidos.

5.5 Delegado de Protección de Datos

Sus funciones son las establecidas en la legislación vigente.

5.6 Procedimiento de designación

Las personas que ocupen los roles anteriores serán designadas por el comité de dirección de la empresa a propuesta del CSC, debiendo acreditarse la comunicación y aceptación del rol por cada una de ellas

El nombramiento se revisará cada dos (2) años o cuando el puesto quede vacante.

Para el nombramiento de las personas, se tomará en cuenta los aspectos siguientes:

- Experiencia mínima de dos años en la materia.
- Formación en seguridad (acreditada mediante la asistencia a cursos, charlas, jornadas).

5.7 Política de seguridad de la información

Será misión del CSC la revisión anual de esta política de seguridad de la información y la propuesta de revisión o mantenimiento de esta.

La Dirección de la empresa muestra su compromiso con la política de seguridad y para ello, de forma anual, se procederá a la revisión completa del sistema y se fomentará la comunicación e información de esta a la totalidad de la organización.

5.8 Resolución de conflictos entre los diversos intervinientes

Los conflictos que puedan surgir entre los diversos roles serán tratados en el CSC, que adoptará las medidas oportunas.

La persona que detecte o considere que existe un conflicto, enviará comunicación al CSC con la descripción del conflicto y las medidas que se podrían tomar para resolverlo. El CSC pedirá

información al resto de miembros implicados en el conflicto y tras el análisis correspondiente adoptará las decisiones correspondientes para su resolución.

6 Análisis y gestión de riesgos

Se considera el análisis de riesgos fundamental para la gestión de la seguridad de los sistemas de información, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el CSC establece como referencia un **nivel de riesgo medio** para los diferentes tipos de información manejados y los diferentes servicios prestados, incluyendo los sistemas y la infraestructura que los soportan.

El CSC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

Se adopta la **Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica** (Magerit v3) para analizar los riesgos que soportan los Sistemas de Información, y para recomendar las medidas apropiadas que deban adoptarse en la mejora de su control.

En el análisis de riesgos se valorarán las salvaguardas presentes en la fecha de aprobación del plan de adecuación.

7 Gestión de personas

La formación e información de todas las personas de la organización en materia de seguridad, así como, en los deberes y obligaciones que se derivan de su puesto de trabajo es un elemento básico del sistema.

El plan de formación tiene como finalidad asegurar el conocimiento de todas las personas tanto en los procesos, procedimientos y normas de seguridad del sistema, como en las mejores prácticas en materia de seguridad.

El plan de comunicación mantendrá informado a todas las personas trabajadoras acerca de las actualizaciones del sistema.

Tanto el plan de formación como la comunicación se llevarán a cabo utilizando los sistemas de Microsoft 365.

8 Profesionalidad

En la definición de los roles y el nombramiento de las personas se ha tomado en cuenta la formación previa de cada uno de los responsables.

El plan de formación y concienciación establecerá un programa de formación continua para los responsables que permita estar adaptado a la cambiante realidad en esta materia.

9 Autorización y control de los accesos

El acceso al sistema de información de gestión de proyectos, así como el acceso a los datos y demás documentación está sometido al proceso de autorización establecido en el procedimiento vigente.

10 Protección de las instalaciones

El acceso al CPD está debidamente protegido. Asimismo, el acceso a las oficinas se efectúa mediante llave entregada a los usuarios.

Los documentos en papel se encuentran en armarios bajo llave.

11 Adquisición de productos

Las compras se realizarán siguiendo el procedimiento vigente, todos los equipos y compras se ajustarán al nivel medio de seguridad fijado por esta política.

12 Seguridad por defecto

El sistema está diseñado para que los usuarios tengan los mínimos privilegios necesarios para el uso de las aplicaciones. El acceso se realiza mediante usuario y contraseña con doble factor de autenticación.

Los usuarios tienen acceso sólo a los sitios, carpetas y documentos que necesitan para su uso.

La documentación relativa al sistema está disponible para todos los usuarios en modo solo lectura en la página del SGSI publicada en la intranet de la empresa.

13 Integridad y actualización del sistema

Las actualizaciones del sistema requerirán de la autorización formal previa antes de su instalación. Para ello, se seguirá lo indicado en el procedimiento de gestión de tareas e incidencias.

14 Protección de la información almacenada y en tránsito

Toda la información debe estar almacenada en la estructura establecida en la nube de Microsoft. La descarga de información en los equipos portátiles estará limitada al mínimo tiempo necesario para llevar a cabo la actividad concreta que se esté realizando con dichos documentos.

15 Prevención ante otros sistemas de información interconectados

No se dispone de sistemas de información interconectados.

16 Registro de la actividad

Toda la actividad que afecte a derechos personales quedará registrada y se efectuará un seguimiento periódico de la misma a fin de garantizar su fiel cumplimiento.

17 Incidentes de seguridad

El procedimiento de gestión de tareas e incidencias establecerá la forma en la que se llevan a cabo la gestión de los incidentes, estableciendo su análisis y puesta en marcha de las medidas para su resolución.

18 Continuidad de la actividad

Al disponer de sistemas en la nube, las copias de seguridad están automatizadas por el proveedor.

19 Mejora continua

Para la mejora continua se establece una revisión periódica del sistema, de forma que cada procedimiento indica en qué fechas deben ser obligatoriamente revisados con objeto de analizar su adecuación a las mejores prácticas existentes y a la realidad del funcionamiento de la organización.

Asimismo, todo incidente deberá ser utilizado para obtener lecciones aprendidas y modificar los procesos y procedimientos que se vean afectados.

20 Datos de carácter personal

Los principios establecidos por la legislación vigente en materia de protección de datos de carácter personal, de forma que se garantice el cumplimiento de dicha normativa son los enumerados a continuación.

- **Principio de licitud**. Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento explícito del interesado o sobre otra base o fundamento jurídico.
- **Principio de lealtad**. No pueden recabarse datos personales por medios fraudulentos (esto es, no podrán utilizase medios o métodos engañosos) desleales (que den lugar a una discriminación injusta o arbitraria contra los titulares) e ilícitos (es decir, que sean ilegales, estén fuera o al margen de la Ley).
- **Principio de transparencia**. Exige que toda información y comunicación relativa al tratamiento de datos personales sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro.
- **Principio de limitación de la finalidad**. Los datos personales deben ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados, posteriormente, de manera incompatible o distinta con dichos fines.
- **Principio de minimización de datos**. Los datos personales deben ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados, posteriormente, de manera incompatible o distinta con dichos fines.
- **Principio de exactitud**. Los datos deben ser exactos y, si fuera necesario, actualizados. Deben adoptarse todas las medidas razonables para corregir errores, modificar los datos que resulten ser inexactos o incompletos y garantizar la certeza de la información objeto de tratamiento.
- **Principio de limitación del plazo de conservación**. No podrán conservarse o mantenerse los datos durante más tiempo del necesario para los fines del tratamiento. Deben establecerse plazos para la supresión o revisión periódica.
- **Principio de integridad y confidencialidad**. Debe garantizarse una seguridad adecuada para preservar la integridad de los datos e impedir el acceso o uso no autorizado. Todas las personas que intervengan en cualquier fase del tratamiento están sujetas a guardar secreto o confidencialidad con carácter indefinido.
- **Principio de responsabilidad proactiva**. Se establece que son los responsables del tratamiento de datos personales quienes, además de aplicar las medidas para cumplir la normativa, deben preocuparse por garantizar y demostrar que, en efecto, las aplican y cumplen.

Todas las personas trabajadoras de Cenit tienen la obligación de respetar y aplicar estos principios en su ámbito de responsabilidad, de acuerdo con lo detallado en el código de conducta de la empresa.

Se establece un procedimiento específico en materia de protección de datos.

21 Documentación del sistema

Tanto la presente política como los diversos documentos, procesos, procedimientos, guías e instrucciones están ubicados en la intranet.

El procedimiento de gestión documental establece las diversas tipologías de documentos, la forma de aprobación, revisión y la ubicación de dichos documentos.

Esta política se desarrolla por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad está a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones incluidos en el alcance.

22Obligación de todas las personas que trabajan en la organización

Todas las personas que trabajan en la organización tienen la obligación de conocer y cumplir esta política de seguridad de la información y la normativa de seguridad.

Se desarrollarán sesiones de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de la empresa, en particular a los de nueva incorporación. La asistencia es obligatoria.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

El plan anual de formación de la empresa incluirá cursos y charlas periódicas en materia de seguridad.

23Terceras partes

Cuando la prestación de servicios implique a otros organismos, o maneje información de otros organismos, se les hará partícipes de esta PSI, se establecerán canales para el reporte y la coordinación de los respectivos RSG y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando se utilicen servicios de terceros o se ceda información a terceros, se les hará partícipes de esta política de seguridad y de la normativa de seguridad que ataña a dichos servicios o información. Esta tercera parte quedará sujeta a las obligaciones establecidas en esta normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará

que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la PSI no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del RSG que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

24 Firma y aprobación

BERMEJO OROZ MIGUEL - 52260458L
2025.11.10 17:06:52 +01'00'

25Anexos

25.1 Glosario de términos

Término	Descripción
CERT	Equipos de Respuesta a Emergencias, del inglés *Computer Emergency Response Team*
CSC	Comité de Seguridad Corporativa
ENS	Esquema Nacional de Seguridad
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
PSI	Política de Seguridad de la Información
SGCMA	Sistema de Gestión de la Calidad y Medio Ambiente
SGS	Sistema de Gestión de Servicios
SGSI	Sistema de Gestión de la Seguridad de la Información
RIS	Responsable de la Información y del Servicio
RSG	Responsable de Seguridad
RST	Responsable de Sistemas
RNOR	Responsable Normativo

25.2Bibliografía y referencias

Bibliografía y referencias

Hoja de control

Documento	
Título	Política de seguridad Sistema de Gestión de la Seguridad de la Información
Versión	06.00
Realizado por	Miguel Bermejo
Fecha de creación	10 de noviembre de 2025
Aprobado por	
Fecha de aprobación	

Control de versiones		
Versión	**Descripción / Motivo de la versión**	**Fecha**
01.00	Versión inicial	14/06/2021
02.00	Inclusión de los enlaces al BOE en el marco normativo. Inclusión del apartado de profesionalidad. Inclusión del apartado de Seguridad por defecto.	17/09/2021
02.01	Modificación del formato a la identidad corporativa.	25/11/2021
03.00	Actualización del marco normativo con la inclusión del RD 311/2022. Revisión anual de contenidos.	05/05/2022
04.00	Revisión anual de contenidos, con adaptación al nuevo ENS.	13/07/2023
05.00	Inclusión del SGCMA y del SGS dentro del alcance.	07/07/2024
06.00	Revisión anual de contenidos, sin cambios	10/11/2025

BERMEJO OROZ MIGUEL - 52260458L
2025.12.01 16:48:35 +01'00'