permisso

Política de Seguridad de la Información

CLASIFICACIÓN	PÚBLICO
ÁMBITO DE DIFUSIÓN	Sin restricciones

TÍTULO	Política de Seguridad de la información
RESPONSABLE	Responsable de Seguridad
CÓDIGO	POL.1

CONTROL DE VERSIONES		
Versión	Fecha	Descripción
1.0	25/06/2024	Edición de partida
2.0	28/11/2024	Referencias a la normativa existente
3.0	20/08/2025	Revisión anual, cambio de nombre a Permisso, inclusión de la normativa aplicable como QTSP y fusión con la Política de Seguridad de QTSP

REFERENCIAS	
Código	Título
A	CCN STIC 805-ENS Política de seguridad
B	CCN STIC 801-ENS Responsabilidades y funciones

ABREVIATURAS	
Abreviatura	Descripción
ENS	Esquema Nacional de Seguridad
SGSI	Sistema de Gestión de la Seguridad de la Información
QTSP	Qualified Trust Service Provider

CONTROL DE FIRMAS		
Elaborado por:	Revisado por:	Aprobado por:
Responsable de Seguridad	Comité de Seguridad de la Información	Dirección
Gabriel Esteban Gullón Digitally signed by Gabriel Esteban Gullón Date: 2025.10.04 17:27:20 +02'00'	MARIN GARCIA HONORIO - 47996647V Firmado digitalmente por MARIN GARCIA HONORIO - 47996647V Fecha: 2025.10.06 09:29:33 +02'00'	74883955A ALVARO MANCILLA MORENO (R: B04948766) Firmado digitalmente por 74883955A ALVARO MANCILLA MORENO (R: B04948766) Fecha: 2025.10.06 21:14:07 +02'00'

ÍNDICE

1 OBJETO

PERMISSO depende de los sistemas de Tecnologías de Información y Comunicaciones (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 los departamentos deben aplicar las medidas mínimas de seguridad, 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.

Los diferentes departamentos deben 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. Los requisitos de seguridad, y los recursos necesarios para atenderlos, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Los departamentos de PERMISSO, y aquellos proveedores a los que se subcontraten servicios de información en su beneficio, deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes de seguridad de la información.

Adicionalmente, esta política establece el marco de actuación para garantizar la seguridad en la prestación de servicios de certificación y confianza, en cumplimiento con los requisitos exigidos a PERMISSO como Prestador de Servicios de Confianza Cualificado.

2 MISIÓN

La misión de PERMISSO es ofrecer un servicio que permita a los usuarios de este servicio la obtención de una imagen financiera completa de sus clientes para tomar decisiones más informadas, agilizando el acceso basado en permisos a los datos financieros de las fuentes de datos más relevantes con una sola integración.

3 ALCANCE

Esta Política se aplicará al sistema de información de PERMISSO, que gestiona la información y los servicios empleados en la gestión de la entidad, y a todos aquellos que, de una forma u otra, interactúan con él.

En consecuencia, esta política será de cumplimiento obligatorio para todo el personal de PERMISSO y para cualquier tercero que participe en sus actividades. De forma específica, el alcance del SGSI cubre la ejecución de las actividades relacionadas con los servicios de confianza y de certificación de PERMISSO, esto es, la gestión del ciclo de vida de los certificados electrónicos (emisión, validación, mantenimiento y revocación).

4 MARCO NORMATIVO

Ver Anexo I.

5 PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

Los principios fundamentales que regirán la protección de la seguridad de la información y datos personales serán los siguientes:

5.1 SEGURIDAD COMO UN PROCESO INTEGRAL Y SEGURIDAD POR DEFECTO

La seguridad constituye un proceso integrado por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema.

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

Los sistemas se diseñarán de forma que garanticen la seguridad por defecto, del siguiente modo:

- El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.
- Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos autorizados, pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.
- En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés sean innecesarias e incluso aquellas que sean inadecuadas al fin que se persigue.
- El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

5.2 REEVALUACIÓN PERIÓDICA E INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA

PERMISSO ha implementado controles y evaluaciones regulares de la seguridad (incluyendo evaluaciones de los cambios de configuración de forma rutinaria) para conocer, en todo momento, el estado de la seguridad de los sistemas en relación con las especificaciones de los fabricantes, con las vulnerabilidades y con las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de estos. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos requerirán de una autorización formal.

Asimismo, solicitará la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

5.3 GESTIÓN DE PERSONAL Y PROFESIONALIDAD

Todos los miembros del PERMISSO asistirán, como mínimo, a una sesión de concienciación en materia de seguridad una vez al año. Asimismo, se establecerá un programa de concienciación continua dirigida a todo el personal y, en particular, al de nueva incorporación.

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.

5.4 GESTIÓN DE LA SEGURIDAD BASADA EN LOS RIESGOS Y ANÁLISIS Y GESTIÓN DE RIESGOS

Todos los sistemas afectados por esta Política de Seguridad deberán ser objeto de un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos, una vez al año.
- Cuando cambien la información utilizada y/o los servicios prestados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de Seguridad será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades.

5.5 INCIDENTES DE SEGURIDAD, PREVENCIÓN, REACCIÓN Y RECUPERACIÓN

PERMISSO ha implementado un proceso integral de detección, reacción y recuperación frente a código dañino mediante el desarrollo de procedimientos que cubren los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, PERMISSO implementa medidas de seguridad, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales, se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

El PERMISSO establecerá las siguientes medidas de reacción ante incidentes de seguridad:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT), si es necesario.
- Para garantizar la disponibilidad de los servicios, el PERMISSO dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

5.6 LÍNEAS DE DEFENSA Y PREVENCIÓN ANTE OTROS SISTEMAS INTERCONECTADOS

PERMISSO ha implementado una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falle, el sistema implementado permita:

- Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
- Minimizar el impacto final sobre el mismo.

Esta estrategia de protección ha de proteger el perímetro, en particular, si se conecta a redes públicas. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

5.7 FUNCIÓN DIFERENCIADA Y ORGANIZACIÓN E IMPLANTACIÓN DEL PROCESO DE SEGURIDAD

PERMISSO ha organizado su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en la Política de Roles y Responsabilidades, que complementa esta política

5.8 AUTORIZACIÓN Y CONTROL DE LOS ACCESOS

PERMISSO ha implementado mecanismos de control de acceso al sistema de información, limitándose a los estrictamente necesarios y debidamente autorizados.

5.9 PROTECCIÓN DE LAS INSTALACIONES

PERMISSO ha implementado 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.

5.10 ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD Y CONTRATACIÓN DE SERVICIOS DE SEGURIDAD

Para la adquisición de productos, PERMISSO tendrá en cuenta que dichos productos tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen, a juicio del Responsable de Seguridad.

5.11 PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO Y CONTINUIDAD DE LA ACTIVIDAD

PERMISSO ha implementado mecanismos para proteger la información almacenada o en tránsito, especialmente cuando esta se encuentra en entornos inseguros (portátiles, tablets, soportes de información, redes abiertas, etc.).

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

Se han desarrollado procedimientos que aseguran la recuperación y conservación a largo plazo de los documentos electrónicos producidos por PERMISSO. De igual modo, se han implementado mecanismos de seguridad en base a la naturaleza del soporte en el que se encuentren los documentos, para garantizar que toda información relacionada en soporte no electrónico esté protegida con el mismo grado de seguridad que la electrónica.

5.12 REGISTROS DE ACTIVIDAD

PERMISSO ha habilitado registros de la actividad de los usuarios reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Todo ello con la finalidad exclusiva de garantizar la seguridad del sistema de información, 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, de función pública o laboral, y demás disposiciones que resulten de aplicación.

5.13 DATOS DE CARÁCTER PERSONAL

PERMISSO cumplirá la normativa existente sobre la protección de datos de carácter personal y solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso.

5.14 CUMPLIMIENTO DE LOS REQUISITOS DE SEGURIDAD

Con el fin de hacer cumplir los preceptos de esta política general, PERMISSO desarrollará un cuerpo normativo, accesible a aquellos a los que aplique, estructurado en políticas, procedimientos y registros, cuya gestión, denominación, numeración y revisión se recogerán en una política específica.

6 IMPLANTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Con el fin de atender a los principios anteriores, PERMISSO ha decidido implantar un Sistema de Gestión de la Seguridad de la Información (SGSI) que, analizando los riesgos pertinentes a la seguridad de la información y la privacidad, determine qué tratamientos son necesarios para limitar el impacto y la probabilidad de que puedan materializarse, mediante la aplicación de las salvaguardas adecuadas.

Este proceso de análisis de riesgos integrará los riesgos a los derechos y libertades de las personas que pudiera producirse al tratar sus datos personales y, si estos riesgos fueran relevantes, incluirá una evaluación específica del impacto, tal y como determina la legislación vigente. El análisis de riesgos de datos personales se integrará en el análisis de riesgos del conjunto del sistema de información.

Estos procesos de análisis y tratamiento de riesgos se adaptarán al contexto interno y externo de PERMISSO, y al marco legal al que está sujeta la empresa por la naturaleza de sus actividades.

El conjunto de procesos que desarrollen el Sistema de Gestión de la Seguridad de la Información se documentará adecuadamente.

En el proceso de desarrollar documentalmente los procesos del Sistema de Gestión de Seguridad de la información, se tomarán en consideración las recomendaciones contenidas en las Guías STIC, Buenas prácticas y abstracts publicados por el Centro Criptológico Nacional. En la redacción de esta política se han tomado en consideración las recomendaciones de la Guía CCN STIC 805-ENS Política de seguridad (Ref. A).

En el Anexo III figura el conjunto de normativa de seguridad redactada para el desarrollo de las directrices de esta política.

7 ORGANIZACIÓN DE LA SEGURIDAD

La organización de la seguridad de la información en PERMISSO se establece según las recomendaciones del CCN STIC 801 Esquema Nacional de Seguridad – Responsabilidades y Funciones (Ref. B):

- Funciones de Gobierno: Un Comité de Seguridad de la Información
- Funciones de Supervisión: Una figura, reportando a dirección y desarrollando las funciones de Responsable de Seguridad
- Funciones de Operación: Una figura, reportando a Dirección, e integrando las siguientes funciones:
    - Responsable del Sistema
    - Administrador de Seguridad
- Delegado de Protección de Datos
- Responsables de información
- Responsables de los servicios

Estos roles se consideran primordiales y por ello figuran en esta política general. Se redactará una política de roles y responsabilidades específica en la que figurarán otros roles relevantes para el cumplimiento del ENS, así como para el cumplimiento de las obligaciones como Prestador de Servicios de Confianza Cualificado

7.1 Funciones, composición y régimen de trabajo del Comité de Seguridad de la Información

Ver Anexo II

7.2 Funciones del Responsable de Seguridad

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad; identificar medidas de seguridad; determinar configuraciones necesarias; elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la categoría del sistema en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información de la Información.

- Participar en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.

7.3 Funciones del Responsable del Sistema

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
- Elaborar los procedimientos operativos necesarios.
- 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 específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Prestar al Responsable de Seguridad de la Información asesoramiento para la determinación de la Categoría del Sistema.
- Colaborar, si así se le requiere, en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad.
- Llevar a cabo las funciones del administrador de la seguridad del sistema:
    - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
    - La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
    - Aprobar los cambios en la configuración vigente del Sistema de Información.
    - Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
    - Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
    - Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
    - Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

7.4 Funciones del Delegado de Protección de Datos

Las que les corresponden por la legislación vigente.

7.5 Funciones del responsable de información

- Definir los criterios de clasificación de seguridad para proteger la información que se gestiona en su departamento (según los criterios generales establecidos en la Política de Clasificación y Tratamiento de la Información.
- Asegurarse de que la información que se gestiona en su departamento/sección está clasificada adecuadamente.
- Definir quién puede acceder a todo tipo de información de su departamento y con qué permisos, aplicando los principios de privilegio mínimo y necesidad de conocer.
- Con el apoyo del Asesor Legal, establecer los criterios de retención de la información que se gestiona en su departamento.
- Con el apoyo del Responsable de Seguridad, establecer el Objetivo de Punto de Recuperación (RPO) para la información que se gestiona en su departamento

7.6 Funciones del responsable de servicios

- Establecer los requisitos de seguridad de los servicios que se gestionan en cada departamento.
- Definir quién puede hacer uso de los servicios y con qué permisos.
- Con el apoyo del Responsable de Seguridad, establecer el Objetivo de Tiempo de Recuperación (RTO) para los servicios que se gestiona en su departamento

7.7 Procedimientos de designación

El nombramiento y la designación de los Responsables identificados en esta Política ha sido realizada por la dirección de PERMISSO y comunicada a las partes afectadas.

7.8 Resolución de conflictos

El Comité de Seguridad de la Información se encargará de la resolución de los conflictos y/o diferencias de opiniones, que pudieran surgir entre los roles de seguridad. Las partes discrepantes llevarán sus argumentos al Comité que, en reunión extraordinaria, o mediante correo electrónico, conocerá del conflicto, y, por mayoría simple, tomará una decisión al respecto. En la toma de decisiones, se valorará primordialmente que la solución elegida minimice los riesgos a la seguridad de la información, evite que el conflicto existente se prolongue o enquiste, y que dicha solución cuente con el menor ratio coste/beneficio.

Este mecanismo servirá como medida compensatoria para mitigar la circunstancia de que la particular estructura orgánica de PERMISSO dado su pequeño tamaño, dificultará que el Responsable de Seguridad y el Responsable de Sistema se encuentren separados jerárquicamente.

8 TERCERAS PARTES

Se considera Tercera Parte a proveedores externos que proporcionan servicios a PERMISSO relacionados directa o indirectamente con su sistema de información; a dichos proveedores, si también gestionan información de PERMISSO; y a otras organizaciones o empresas a las que se les ceda información por cualquier motivo, como pueden ser datos personales.

PERMISSO hará partícipe a las terceras partes 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. En la medida en que sea aplicable, la normativa de seguridad será incluida dentro de los planes de formación del personal y de los terceros vinculados. De igual modo, PERMISSO exigirá a terceros que le presten servicios que estén en condiciones de exhibir la correspondiente Declaración de Conformidad con estándares de Seguridad de la Información (ENS, ISO 27001).

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. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

El detalle de los servicios críticos provisionados por terceros se recogerá en un documento específico, donde se relacionarán los proveedores de servicios del sistema de información de PERMISSO.

9 REVISIÓN Y MEJORA CONTÍNUA

PERMISSO se compromete a arbitrar mecanismos de revisión del adecuado funcionamiento del Sistema de Gestión de la Seguridad de la Información y a establecer objetivos de seguridad y privacidad cuya consecución plasmará el principio de mejora continua de la seguridad.

Estos objetivos constarán de las propias revisiones que se llevan a cabo con regularidad para evaluar los procesos del sistema, de las no conformidades provenientes de auditorías internas y externas que se programen, así como de la propia iniciativa de todos los actores implicados cuando perciban disfuncionalidades u oportunidades de mejora.

Los objetivos de seguridad y cumplimiento contarán con responsables designados, recursos suficientes y plazos de consecución plausibles. Su desarrollo y ejecución se revisarán, al menos, con periodicidad anual.

Los objetivos podrán agruparse entorno a los siguientes bloques de trabajo:

- Protección del conocimiento, la información y los datos.
- Protección de las tecnologías de la información y las comunicaciones.
- Protección de las instalaciones, edificios y estancias.
- Protección de los activos de la compañía.
- Protección de la continuidad del negocio.
- Cumplimiento con los estándares legales y normativos.

La revisión del funcionamiento de los controles y requisitos de seguridad se desarrollará estableciendo un marco de métricas cuyos indicadores se revisarán con periodicidad ajustada a su naturaleza cuyo detalle se incluirá en un documento específico de métricas.

10 COMPROMISO CORPORATIVO

La consecución de los objetivos del sistema de gestión de la seguridad de la información y cumplimiento requiere de un compromiso total de PERMISSO para garantizar su ejecución y la mejora de los procesos y actividades que conlleva. Este compromiso se plasmará con la difusión y comunicación de estas directrices al conjunto de los empleados de PERMISSO y a aquellas personas y organizaciones externas que requieran de su conocimiento. Este documento se publicará en un medio accesible a todos los implicados. Esta comunicación,

se complementará con acciones de concienciación interna que faciliten la integración de este sistema en los objetivos de negocio de PERMISSO.

ANEXO I. MARCO NORMATIVO

La base normativa que afecta al desarrollo de las actividades de PERMISSO en lo que afecta a la gestión de la información, y que implica la implantación de forma explícita de medidas de seguridad en los sistemas de información, está constituida por la siguiente legislación:

- 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 (RGPD)).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- 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.
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE).
- Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Reglamento Europeo 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (eIDAS). Asimismo, se incluyen todas las normas técnicas asociadas a la prestación de servicios de confianza:
    - ETSI EN 319 401 General Policy Requirements for Trust Service Providers.
    - ETSI EN 319 411-2 Policy and security requirements for Trust Service Providers issuing certificates: Requirements for trust service providers issuing EU qualified certificates [QCP-n, QCP-n-qcsd, QCP-l, QCP-l-qscd, [QCP-n].
    - ETSI EN 319 421 Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.

- Orden ETD/743/2022, de 26 de julio, por la que se modifica la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.

ANEXO II. COMPOSICIÓN Y FUNCIONES DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

II.1 Composición

PERMISSO ha constituido un Comité de Seguridad de la Información, como órgano colegiado, y está formado por los siguientes miembros:

- Presidente: Responsable del Sistema
- Secretario/a: Responsable de Seguridad
- Miembros:
    - Delegado de Protección de Datos.
    - Responsable de Seguridad.
    - Responsable del Sistema.
    - Asesor legal
    - Responsable de RRHH

El Delegado de Protección de Datos participará con voz, pero sin voto en las reuniones del Comité de seguridad de la información cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación. En todo caso, si un asunto se sometiera a votación, se hará constar siempre en acta la opinión del Delegado de Protección de Datos.

Los jefes de otros departamentos de PERMISSO, a efectos de desarrollar responsabilidades asociadas a los roles de Responsables de la Información y los Servicios serán convocados en función de los asuntos a tratar.

II.2 Régimen de trabajo

El Comité de Seguridad de la Información celebrará sus sesiones en las dependencias de PERMISSO, con periodicidad mínima anual, previa convocatoria al efecto realizada por el Presidente de dicho Comité.

II.3 Funciones

El Comité de Seguridad tendrá las siguientes funciones:

- Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:

- Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración y recomendar posibles actuaciones respecto de ellos.
- Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
- Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.
- Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con Dirección.
- Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
- Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
- Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

ANEXO III. NORMATIVA DE DESARROLLO DE LA POLÍTICA DE SEGURIDAD

Código	Título
POL.01	Política de Seguridad de la Información
POL.02	Política de Roles y Responsabilidades
POL.03	Política de Uso Apropiado del Sistema de Información
POL.04	Política de Gestión Documental
POL.05	Política de Clasificación y Tratamiento de la Información
POL.06	Política de Concienciación y Formación
POL.07	Política de Seguridad de la Información con Proveedores y Nube
POL.08	Política de Monitorización y Protección Anti-Malware
POL.09	Política de Desarrollo Seguro de Aplicaciones
POL.10	Política de Copias de Seguridad
POL.11	Política de Gestión Criptográfica, Firma Electrónica y Sellado de Tiempo
POL.12	Política de Gestión de Inventario
POL.13	Política de Gestión de Software, Capacidad y Configuración Técnica
POL.14	Política de Gestión de la Seguridad de la Red y Comunicaciones
POL.15	Política de diseño y funcionamiento del SGSI
POL.16	Política de Seguridad de RRHH
POL.17	Política de Control de Accesos
POL.18	Política de Seguridad Física
POL.19	Política de Gestión de Cambios, Autorizaciones y Adquisiciones
POL.20	Política de Programa de Auditoría
POL.25	Política de Régimen Disciplinario
PRO.02	Procedimiento de Gestión de Incidentes
PRO.03	Plan de Respuesta ante Desastres en el Sistema de Información