POLÍTICA DE GRUPO AL S.A.

INTRODUCCIÓN

GRUPO AL depende de los sistemas de información para alcanzar sus objetivos, Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas, en función del riesgo, para protegerlos frente a daños accidentales o deliberados que puedan afectar a la autenticidad, trazabilidad, integridad o confidencialidad de la información tratada o la disponibilidad de los servicios prestados. El objetivo último de la seguridad de la información es garantizar que la entidad pueda cumplir con sus objetivos, desarrollar sus funciones o competencias y prestar los servicios para la cual se ha sido constituida 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 exigidas por el Esquema Nacional 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. La 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. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos donde se traten datos personales, se adquieran servicios TIC o se presten servicios que afecten a los sistemas de información.

ALCANCE

La presente Política de Seguridad es aplicable a todo el Grupo AL, y de forma específica a los alcances de las certificaciones de ISO/IEC 27001:2022 y ENS que se describen a continuación:

CONSULTORIA:

AUDIFILM CONSULTING S.L.U.

En el caso de la norma ISO/IEC 27001 y Esquema Nacional de Seguridad, esta política se aplica a: “sistemas de información que dan soporte al diseño y desarrollo de sistemas de información para la administración pública. prestación de servicios de consultoría, implantación, puesta en marcha, soporte y formación para la administración pública”.

AL TRÁFICO Y MOVILIDAD SEGURA, S.L.

En el caso de la norma ISO/IEC 27001 y Esquema Nacional de Seguridad, esta política se aplica a: “sistemas de información que dan soporte al diseño y desarrollo de sistemas de información para la administración pública. prestación de servicios de consultoría, implantación, puesta en marcha, soporte y formación para la administración pública”.

ASESORES LOCALES CONSULTORÍA, S.A

En el caso de la norma ISO/IEC 27001 y Esquema Nacional de Seguridad, esta política se aplica a: “sistemas de información que dan soporte al diseño y desarrollo de sistemas de información para la administración pública. prestación de servicios de consultoría, implantación, puesta en marcha, soporte y formación para la administración pública”.

COLABORUM, S.L.

En el caso de la norma ISO/IEC 27001 y Esquema Nacional de Seguridad, esta política se aplica a: “sistemas de información que dan soporte al diseño y desarrollo de sistemas de información para la administración

pública. prestación de servicios de consultoría, implantación, puesta en marcha, soporte y formación para la administración pública".

CIVIC BRIDGE, S.L.

En el caso de la norma ISO/IEC 27001 y Esquema Nacional de Seguridad, esta política se aplica a: "sistemas de información que dan soporte al diseño y desarrollo de sistemas de información para la administración pública. prestación de servicios de consultoría, implantación, puesta en marcha, soporte y formación para la administración pública".

POSTALES:

La presente Política de Seguridad es aplicable a todo el Grupo AL, y de forma específica a los alcances de las certificaciones de ISO/IEC 27001, ENS y NIS2 que se describen a continuación:

RD POST COMUNICACIÓN CERTIFICADA, S.L.

En cuanto a la norma ISO/IEC 27001 y Esquema Nacional de Seguridad, esta política aplica a los sistemas de información que dan soporte a la gestión integral y backoffice del proceso postal. recogida, admisión, clasificación, tratamiento, transporte, distribución y entrega a domicilios de los envíos de cartas, ordinarias, cartas certificadas, notificaciones administrativas y otros servicios postales.

SMS91

En cuanto a la norma ISO/IEC 27001 y Esquema Nacional de Seguridad, esta política aplica a los sistemas de información que dan soporte a la gestión integral y backoffice del proceso postal. recogida, admisión, clasificación, tratamiento, transporte, distribución y entrega a domicilios de los envíos de cartas, ordinarias, cartas certificadas, notificaciones administrativas y otros servicios postales.

MISIÓN

La misión de GRUPO AL es proveer a sus clientes las soluciones y servicios que se encuentran en su catálogo de productos.

La empresa tiene como objetivo proveer soluciones aptas para que sus clientes dispongan de unos productos y servicios eficaces y de alta calidad, ofreciéndose también como el socio ideal para hacer frente a la ejecución del ciclo total de un proyecto. En definitiva, proporcionar servicios profesionales con la máxima calidad posible, por lo que exige a sus empleados que tomen todas las medidas necesarias parar garantizar la integridad de la información de la compañía y sus sistemas de comunicaciones, siguiendo los procedimientos y guías implantados en su SGSI.

Como respuesta a un nuevo entorno tecnológico donde la convergencia entre la informática y las comunicaciones están facilitando un nuevo paradigma de productividad para las empresas, donde el desarrollo de buenas prácticas en Seguridad de la Información es fundamental para conseguir los objetivos de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de toda la información gestionada.

Se ha diseñado una Política de Seguridad de la Información cuyos objetivos principales son:

- Proteger, mediante controles/medidas, los activos frente a amenazas que puedan derivar en incidentes de seguridad.
- Paliar los efectos de los incidentes de seguridad.
- Establecer un sistema de clasificación de la información y los datos con el fin de proteger los activos críticos de información.
- Definir las responsabilidades en materia de seguridad de la información generando la estructura organizativa correspondiente.
- Elaborar un conjunto de reglas, estándares y procedimientos aplicables a los órganos de dirección, empleados, socios, proveedores de servicios externos, etc.
- Especificar los efectos que conlleva el incumplimiento de la Política de Seguridad en el ámbito laboral.

- Evaluar los riesgos que afectan a los activos con el objeto de adoptar las medidas/controles de seguridad oportunos.
- Verificar el funcionamiento de las medidas/controles de seguridad mediante auditorías de seguridad internas realizadas por auditores independientes.
- Formar a los usuarios en la gestión de la seguridad y en tecnologías de la información y las comunicaciones.
- Controlar el tráfico de información y de datos a través de infraestructuras de comunicaciones o mediante el envío de soportes de datos ópticos, magnéticos, en papel, etc.
- Observar y cumplir la legislación en materia de protección de datos, propiedad intelectual, laboral, de servicios de la sociedad de la información, penal, etc., que afecte a los activos de la entidad.
- Proteger el capital intelectual de la organización para que no se divulgue ni se utilice ilícitamente.
- Reducir las posibilidades de indisponibilidad a través del uso adecuado de los activos de la organización.
- Defender los activos ante ataques internos o externos para que no se transformen en incidentes de seguridad.
- Controlar el funcionamiento de las medidas de seguridad averiguando el número de incidencias, su naturaleza y efectos.

PRINCIPIOS RECTORES DE LA POLÍTICA

- **Alcance estratégico:** la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles de la entidad y deberá coordinarse e integrarse con el resto de las iniciativas estratégicas de forma coherente
- **Seguridad integral:** la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de la información, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.
- **Gestión de la seguridad basada en el riesgo:** la gestión de la seguridad basada en los riesgos identificados permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Las medidas de seguridad se establecerán en función de los riesgos a que esté sujeta la información y sus sistemas. y serán proporcionales al riesgo que tratan, debiendo estar justificadas. Se tendrán también en cuenta los riesgos identificados en el tratamiento de datos personales.
- **Prevención, detección, respuesta y conservación:** con la implementación de acciones preventivas de incidentes, minimizando las vulnerabilidades detectadas, evitando la materialización de las amenazas y, cuando estas se produzcan, danto una respuesta ágil para restaurar la información o servicios prestados, garantizando una conservación segura de la información.
- **Existencia de líneas de defensa:** la estrategia de seguridad de la entidad se diseña e implementa en capas de seguridad.
- **Vigilancia continua y reevaluación periódica:** la entidad implementa medios la detección y respuesta a actividades o comportamientos anómalos. Además, de otros que permitan una evaluación continuada del estado de seguridad de los activos, Existirá, también, un proceso de mejora continua para la revisión y actualización de las medidas de seguridad, de manera periódica, conforme a su eficacia y la evolución de los riesgos y sistemas de protección.
- **Seguridad por defecto y desde el diseño**: los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto. Los sistemas proporcionarán la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados.
- **Diferenciación de responsabilidades:** en aplicación de este principio las funciones del Responsable de la Seguridad y del Responsable del Sistema estarán diferenciadas.

MARCO NORMATIVO

Las principales normas que afectan a esta Política son:

- ENS, Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- ENI, 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.
- NIS2, Directiva (UE) 2022/2555 del Parlamento Europeo.
- Ley SIIF, Sistema interno de información
- ISO/IEC 27001:2022, Sistemas de Gestión de la Seguridad de la Información.

- ISO/IEC 9001:2015, Gestión de Calidad.
- ISO/IEC 14001:2015, Sistemas de gestión ambiental.
- ISO/IEC 39001:2013, Sistemas de gestión de la seguridad vial.
- ISO/IEC 45001:2023, Sistemas de gestión de la seguridad y salud en el trabajo.

ORGANIZACIÓN DE LA SEGURIDAD

5.1. COMITÉS: FUNCIONES Y RESPONSABILIDADES

La composición del Comité de Calidad y Seguridad de la Información del GRUPO AL es la siguiente:

- La Dirección.
- Responsable de la Información.
- Responsable del Servicio.
- Responsable del Sistema.
- Responsable de Seguridad.
- Administrador de Sistemas
- Responsable Desarrollo
- Responsable Calidad
- Responsable Seguridad Fisica
- Delegado de Protección de Datos.
- Secretario del Comité de Calidad y Seguridad de la Información.

Dentro de esta estructura, el Secretario del Comité de Calidad y Seguridad de la Información tendrá como funciones de los hitos a tratar, la difusión de sus resultados y el seguimiento de los acuerdos alcanzados bajo la supervisión del Responsable del Sistema

El Comité de Calidad y Seguridad de la Información reportará a través del Responsable del Sistema, al Comité de Dirección.

El Comité de Calidad y Seguridad de la Información, por lo que se refiere al SGSI de GRUPO AL y al cumplimiento de lo dispuesto en el ENS, tendrá las siguientes funciones:

- Atender las inquietudes de la Dirección de la entidad y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, evitando duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación por la Dirección.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la gestión de incidentes de seguridad.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la organización. En particular velará por la coordinación de distintos planes que puedan realizarse en diferentes áreas.
- Priorizar 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 TIC 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.

- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Todas las propuestas elevadas por cada miembro del Comité u otros acuerdos, serán aprobadas previamente por el Responsable del Sistema antes de proceder a su implantación y/o acción del proceso, excepto cuando venga del propio Responsable del Sistema la iniciativa, lo tendrá que elevar para su aprobación al Comité de Dirección y ser conocedor el propio comité de seguridad.

Asimismo, cabe señalar que GRUPO AL dispone de otros comités específicos en diferentes ámbitos de gestión (como son Comité de Seguridad y Salud en el Trabajo, Comité de Ética, Órgano de Cumplimiento, Gestor de movilidad y el mencionado Comité de Dirección), que actúan de manera coordinada con el Comité de Calidad y Seguridad de la Información cuando las materias tratadas tienen relación con la seguridad de la información o con el cumplimiento del ENS. Esta coordinación asegura la coherencia de las decisiones corporativas, evita solapamientos de funciones y refuerza el modelo de gobernanza de la organización.

5.2. ROLES: FUNCIONES Y RESPONSABILIDADES

Las funciones del Responsable de la Información son las siguientes:

- Define y aprueba los requisitos de seguridad de la información.
- . Determina el nivel de seguridad y su clasificación (categorías ENS).
- . Supervisa el uso adecuado de la información.

Las funciones del Responsable del Servicio son las siguientes:

- . Define y aprueba los requisitos de seguridad del servicio.
- . Determina el nivel de seguridad de los servicios prestados.
- . Informa y coordina actuaciones en caso de incidentes.

Las funciones del Responsable del Sistema son las siguientes:

- . Desarrolla, opera y mantiene el sistema de información durante todo su ciclo de vida.
- . Implementar las medidas técnicas de seguridad incluidas en el SOA.
- . Adopta medidas correctoras derivadas de auditorías.
- . Supervisa incidencias técnicas y de explotación a su vez reporta los Responsable de Información y Servicio.

Las funciones del Responsable de Seguridad son las siguientes:

- Determina e impulsa las medidas de seguridad de la información y servicios.
- . Supervisa su implantación y efectividad.
- . Participa en la categorización de sistemas y en la Declaración de Aplicabilidad.
- . Coordina la gestión de incidentes de seguridad.

Las funciones del Administrador de Sistemas son las siguiente:

- . Ejecuta tareas delegadas del Responsable del Sistema o de Seguridad.
- . Configura y mantiene sistemas, redes y aplicaciones.
- . Gestiona usuarios, accesos y privilegios.
- . Informa sobre anomalías y colabora en la resolución de incidente

Las funciones del Responsable de Desarrollo son las siguientes:

- Supervisa el ciclo de vida del software y aplicaciones.
- Garantiza la aplicación de prácticas seguras de desarrollo.
- Controla cambios y versiones (gestión de la configuración).
- Colabora con Seguridad en pruebas y despliegues.

Las funciones del Responsable de Calidad son las siguientes:

- Supervisa la correcta implantación del SGC (ISO 9001).
- Asegura la integración de procesos de calidad con el SGSI.
- Participa en auditorías internas y externas.
- Colabora en la mejora continua de los procesos.

Las funciones del Responsable de Seguridad Física son las siguientes:

- Define e implementa medidas de protección física de instalaciones, equipos y accesos.
- Coordina con el Responsable de Seguridad ENS la protección integral (física y lógica).
- Supervisa controles de acceso, videovigilancia y servicios de seguridad.
- Gestiona incidentes relacionados con seguridad física.

Las funciones del Secretario son las siguientes:

- Organiza las sesiones del Comité de Calidad y Seguridad de la Información.
- Levanta actas y da seguimiento a acuerdos adoptados.
- Facilita la comunicación entre los miembros y la Dirección.

Las funciones del Delegado de Protección de Datos son las siguientes:

- Asesora en el cumplimiento del RGPD y LOPDGDD.
- Supervisa la aplicación de medidas de protección de datos personales.
- Colabora en la gestión de evaluaciones de impacto y brechas de datos.
- Actúa como punto de contacto con la AEPD.

La descripción concreta de todas las responsabilidades puede consultarse en el documento: **PS01_SEGURIDAD DE LA INFORMACIÓN**.

Por su parte, el personal de la empresa tiene identificadas y comunicadas sus responsabilidades en relación con la seguridad de la información entre las que se destacan:

- Comunicar las incidencias de seguridad mediante los canales establecidos.

- Aplicar los mecanismos establecidos para el intercambio de información entre el personal, clientes y proveedores.

Cualquier asignación de tareas y responsabilidades de seguridad de la información será aprobada por el Comité de Calidad y Seguridad de la Información.

PROCEDIMIENTOS DE DESIGNACIÓN

Los miembros del Comité de Calidad y Seguridad de la Información serán designados por: Responsable del Servicio.
El Responsable de la Información y del Servicio serán designados a propuesta del Comité de Calidad y Seguridad de la Información.

El Responsable del Sistema será designado a propuesta del Responsable de Información y Comité de Dirección.

Los nombramientos podrán ser revisados cada dos años, pudiendo realizarse antes cuando el puesto quede vacante o por un incumplimiento reiterado de sus funciones, previo apercibimiento. GRUPO AL debe disponer de un mecanismo que permita la sustitución de los responsables designados en caso de ausencias de larga duración o aquellas de menor duración pero que puedan provocar ineficiencias en las funciones de cada uno de ellos que afecten al sistema.

RESOLUCIÓN DE CONFLICTOS

Se han implementado medidas compensatorias para la resolución de conflictos entre los diferentes responsables, el Comité de Calidad y Seguridad de la Información podrá dirimir las discrepancias, en el caso que se den.

GESTIÓN DE INCIDENTES DE SEGURIDAD

GRUPO AL dispondrá de un procedimiento para la gestión ágil de los eventos e incidentes de seguridad que supongan una amenaza para la información y los servicios. Este procedimiento se integrará con otros relacionados con los incidentes de seguridad de otras normas sectoriales como la de protección de datos personales u otra que afecte al organismo para coordinar la respuesta desde los diferentes Centro Criptológico Nacional 20 CCN-STIC-805 Esquema Nacional de Seguridad - Política de Seguridad de la Información enfoques y comunicar a los diferentes organismos de control sin dilaciones indebidas y, cuando sea preciso, a las Fuerzas y Cuerpos de Seguridad el Estado o los juzgados.

GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política de Seguridad realizarán 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 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 Comité de Calidad y Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información gestionados, los tratamientos de datos personales y los diferentes servicios prestados.

CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS PERSONALES

La Organización desarrolla su actividad conforme a la normativa vigente en materia de protección de datos personales, en particular, el Reglamento (UE) 2016/679, General de Protección de Datos (RGPD), y la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). En el tratamiento de los datos personales, la Organización aplica y respeta los **principios de licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad**.

La Organización integra la **privacidad desde el diseño y por defecto** en todos aquellos procesos, productos y servicios que impliquen tratamiento de datos personales, valorando desde el inicio el impacto en la privacidad y estableciendo las medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo sean objeto de tratamiento los datos personales necesarios en cada caso, en función de los fines legítimos perseguidos.

En el marco del **principio de responsabilidad proactiva**, la Organización adopta las políticas, procedimientos y medidas de control interno necesarios para poder demostrar en todo momento el cumplimiento de la normativa de protección de datos. Ello incluye, entre otras actuaciones, el mantenimiento del registro de actividades de tratamiento, la realización de evaluaciones de impacto en protección de datos cuando resulte exigible, la suscripción de los correspondientes contratos de encargo del tratamiento con proveedores que acceden a datos personales y la implantación de medidas de seguridad adecuadas al riesgo.

Asimismo, la Organización promueve la **sensibilización y la formación periódica** de su personal con acceso a datos personales, con el fin de asegurar que conocen y aplican las obligaciones derivadas de la normativa de protección de datos y de las políticas internas aprobadas en esta materia.

OBLIGACIONES DEL PERSONAL

Todos los trabajadores de GRUPO AL tienen la obligación de conocer esta Política de Seguridad de la Información, que es de obligado cumplimiento dentro del alcance identificado, siendo responsabilidad del Comité de Calidad y Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados.

Se establecerá un programa de concienciación continua para atender a todos los miembros de GRUPO AL, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC dentro del alcance 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.

DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El cumplimiento de los objetivos marcados en esta Política de Seguridad se lleva a cabo mediante el desarrollo de documentación que componen las normas (Normativa de Seguridad) y procedimientos de Seguridad asociados al cumplimiento del Esquema Nacional de Seguridad e ISO/IEC 27001. Para GRUPO AL se ha definido una Norma para la Gestión de la Documentación que establece las directrices para la organización, gestión y acceso.

MANTENIMIENTO, APROBACIÓN Y REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Periódicamente, y en todo caso no superando el plazo de un año, el Comité de Calidad y Seguridad de la Información revisará la vigencia y razonabilidad de la presente política y se llevarán a cabo las mejoras, adaptaciones o modificaciones requeridas en función de los cambios organizativos, técnicos o regulatorios aplicables.

Cualquier cambio o evolución que afecte o pudiera afectar al contenido de la Política de Seguridad de la Información quedará registrado en una nueva firma del documento de aprobación. De esta forma se concreta y confirma el compromiso de estas entidades por la seguridad de la información.

TERCERAS PARTES

Las terceras partes relacionadas con GRUPO AL, dentro del alcance, firman con la empresa un acuerdo que protege la información intercambiada.

Cuando GRUPO AL utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha Política, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Esta Política será revisada para su continua adecuación anualmente por la dirección, así como los objetivos y metas de la empresa, y comunicada a todo el personal de la organización.

PROCEDIMIENTO PARA EL TRATAMIENTO DE EXENCIONES Y EXCEPCIONES

De manera excepcional, podrán autorizarse exenciones o excepciones al cumplimiento de políticas, normas o controles de seguridad cuando existan razones operativas, técnicas o justificadas por el análisis de riesgos que impidan su aplicación completa o inmediata.

Toda solicitud de exención o excepción deberá:

- Presentarse por escrito, indicando el control o requisito afectado, la justificación y los riesgos asociados.
- Ser evaluada por el Responsable del Sistema en coordinación con el resto del comité de seguridad según proceda, donde se valorará su impacto y se propondrá las medidas compensatorias necesarias.

- Ser aprobada por el Comité de Seguridad previa autorización del Responsable del Sistema, según el nivel de criticidad del riesgo identificado.

Las exenciones o excepciones aprobadas serán documentadas y registradas en el Registro de Exenciones y Excepciones del SGSI, indicando su fecha de autorización, duración prevista y condiciones de revisión.

Una vez superadas las causas que motivaron la excepción, el Responsable del Sistema revisará su vigencia y promoverá su cierre, restituyendo el cumplimiento pleno del control afectado.

Ninguna exención o excepción podrá considerarse indefinida ni implicar la anulación de los principios de confidencialidad, integridad y disponibilidad definidos en esta política.

CONTROL DE VERSIONES

Registro de versiones		
Descripción	**Versión**	**Fecha**
Versión inicial del documento.	V1	6/11/2025

ENTRADA EN VIGOR

La presente Política de Seguridad de la Información es efectiva desde el día siguiente al de su fecha de aprobación por la Dirección de GRUPO AL y hasta que sea reemplazada por una nueva Política.

APROBADO POR: LA DIRECCIÓN
Fecha: 6/11/2025 Diego Cambló Giménez CEO/Responsable de la Información/ Responsable de Servicios

En Málaga a 6 de noviembre de 2025