Política 1

Política de seguridad de la información de Grupo GP

CONTROL DE REVISIONES EFECTUADAS

Revisión	Fecha	Descripción
1	23/10/2023	Elaboración del documento
2	31/01/2024	Actualización compromiso de cumplimiento y objetivos específicos
3	01/10/2025	Conversión de la Política de GPartners a la Política para todo el Grupo GP, incluyéndose ACATIA
4	02/06/2026	Integración de los requisitos del Esquema Nacional de Seguridad (ENS). Revisión y ampliación de la estructura

ELABORADO	REVISADO	APROBADO
Responsables del Sistema	Responsable de Seguridad	Alta Dirección

ÍNDICE

CAPÍTULO 1. Objeto

GRUPO GP, y en particular, GPartners como empresa proveedora de servicios de Forensic y Corporate Finance y Acatia como proveedora de servicios de Compliance, HSQE y Cibercompliance a clientes de todos los sectores, así como ámbitos privados y públicos, asume su compromiso con la seguridad de la información y protección de los datos de carácter personal, comprometiéndose a la adecuada gestión de la misma, con el fin de ofrecer a todos sus grupos de interés las mayores garantías de confidencialidad en torno a la información utilizada y los datos tratados.

La Dirección de Grupo GP considera la seguridad de la información un aspecto fundamental para garantizar la consecución de los objetivos de la organización y la adecuación a la legislación vigente. Por ello, se compromete a mantener un nivel de seguridad adecuado y alineado al negocio, en los procesos asociados a los servicios prestados por la organización, con objeto de ofrecer a sus clientes internos y externos las mayores garantías en cuanto a la calidad de dichos servicios.

La Dirección de Grupo GP se compromete a gestionar y proteger su información y sus servicios de forma adecuada mediante la implementación, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI) que cumpla los requisitos del Esquema Nacional de Seguridad (ENS en adelante), así como de sus partes interesadas, y dentro del marco regulatorio legal y vigente del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

El presente documento constituye la Política de Seguridad de la Información de Grupo GP que establece las directrices y principios que regirán el modo en que el Grupo GP gestionará y protegerá su información y sus servicios a través de su Sistema de Gestión interno.

Por todo lo anteriormente expuesto, la Dirección se compromete al estricto cumplimiento de las siguientes premisas relativas al Sistema de seguridad de la información:

- Proporcionar un marco operacional en aras de aumentar la capacidad de resistencia y resiliencia para dar una respuesta eficaz.
- Asegurar la recuperación rápida y eficiente de los servicios, frente a cualquier desastre físico o contingencia que pudiera ocurrir y que pusiera en riesgo la continuidad de las operaciones.
- Prevenir incidentes de seguridad de la información en la medida que sea técnica y económicamente viable, así como mitigar los riesgos de seguridad de la información generados por nuestras actividades.
- Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

CAPÍTULO 2. Ámbito de aplicación

El alcance de esta política abarca la totalidad de las actividades desarrolladas y servicios prestados por Grupo GP, pudiendo resumirse de la siguiente manera: "Sistemas de información que apoyan la prestación de servicios de realización de informes periciales e investigaciones de fraude, cumplimiento normativo y consultoría", en la sede C/ Carpinteros 12, 1º, Of. S1, Villaviciosa de Odón – Madrid, conforme a la categorización del sistema vigente, a fecha de emisión del certificado.

El alcance de esta política incluye a todo el personal perteneciente al Grupo GP (GPartners y ACATIA), así como al personal subcontratado o los suministradores que están ubicados en las instalaciones del Grupo, o que utilizan o se conectan a cualquier sistema perteneciente al Grupo GP.

El alcance de esta política comprende el conjunto de servicios relacionados con informes periciales e investigaciones de fraude, cumplimiento normativo y consultoría que se prestan por los departamentos o áreas de Grupo GP, a los clientes externos.

Esta versión de la Política de Seguridad de la Información es efectiva desde el 2 de junio de 2026, fecha de su aprobación por la Alta Dirección de Grupo GP, hasta que sea reemplazada por una nueva versión. Su cumplimiento es obligatorio a partir de dicha fecha, de forma indefinida, para todo el personal dentro del alcance.

CAPÍTULO 3. Objetivos de la política de seguridad de la información

Grupo GP opera en el mercado español desde 2011, especializado en la prestación de servicios de Disputas y Compliance, liderado por socios y un equipo de profesionales (economistas, peritos, abogados, auditores, etc.) con amplia experiencia prestando este tipo de servicios a clientes de todos los sectores y tamaños.

Para el cumplimiento de su Propósito, la prestación de los servicios y el cumplimiento de sus objetivos, el Grupo GP depende de sistemas TIC. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la confidencialidad, disponibilidad, integridad, autenticidad y trazabilidad de la información tratada o los servicios prestados.

Con la implementación del ENS se fortalece la seguridad de los servicios, así como de la información y datos que incluyen dichos servicios, mejorando notablemente la gestión de la seguridad necesaria para el Grupo GP como parte del cumplimiento satisfactorio de su misión.

Así como se compromete al cumplimiento de los siguientes objetivos específicos relativos al sistema:

- Contar con expertos externos que certifiquen que nuestro sistema de gestión se alinea con las mejores prácticas internacionales.
- Crear un equipo interno con conocimientos sólidos en el ámbito de la seguridad de la información que permita operar con total autonomía y bajo los más altos niveles de seguridad.

Para poder lograr estos objetivos, desde nuestra Organización trabajamos cada día en:

- Mejorar continuamente nuestro Sistema de Gestión de la Seguridad de la Información (SGSI).
- Cumplir con los requisitos legales aplicables vigentes y con cualesquiera otros requisitos que suscribamos, además de los compromisos adquiridos con los clientes.
- Identificar las amenazas potenciales, así como el impacto en las operaciones de negocio que dichas amenazas, caso de materializarse, puedan causar.
- Preservar los intereses, expectativas y necesidades de nuestras principales partes interesadas (clientes, usuarios, accionistas, empleados, proveedores, etc.), la reputación, la marca y las actividades de creación de valor.
- Trabajar de forma conjunta con nuestros proveedores y subcontratistas con el fin de mejorar la prestación de servicios, la continuidad de los mismos y la seguridad de la información / confidencialidad / protección de datos de carácter personal.
- Evaluar y garantizar la competencia técnica del personal, así como asegurar la motivación adecuada de éste para su participación en la mejora continua de nuestros procesos, proporcionando la formación y la comunicación interna adecuada para que desarrollen buenas prácticas definidas en el sistema.
- Garantizar el correcto estado de las instalaciones y el equipamiento adecuado, de forma tal que estén en correspondencia con la actividad, objetivos y metas de la empresa.
- Garantizar un análisis de manera continua de todos los procesos relevantes, estableciéndose las mejoras pertinentes en cada caso, en función de los resultados obtenidos y de los objetivos establecidos.

Dentro de este contexto, los objetivos específicos de la presente Política de Seguridad de la Información son:

- Garantizar los aspectos de confidencialidad, disponibilidad, integridad, autenticidad y trazabilidad de la información.
- Gestionar el riesgo de seguridad existente hasta los umbrales establecidos por la Dirección, en base a la prestación del servicio a clientes.
- Implantar un Sistema de Gestión que permita gestionar y proteger la información y servicios que presta la compañía.
- Implantar un conjunto de medidas o controles de seguridad adecuados, determinados por el ENS, así como cualquier control adicional identificado, como parte del Sistema de Gestión para asegurar la protección ante amenazas que puedan incidir en la autenticidad, trazabilidad, confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios.
- Nombrar a los responsables de la implementación y gestión de la seguridad de la información, que incluya un Responsable del Sistema, encargado de gestionarlo y velar por el desarrollo, mantenimiento y mejora del mismo.
- Nombrar un Responsable de Seguridad y asegurar que dispone de los recursos necesarios para llevar a cabo los controles de seguridad de la información necesarios.
- Gestionar la prestación y continuidad de los servicios realizados a los clientes de forma eficaz y eficiente, dentro de un ciclo de vida que permita la mejora continua de los procesos implantados y del Sistema en general.
- Establecer periódicamente un conjunto de objetivos e indicadores en materia de gestión de seguridad de la información, que permitan a la Dirección llevar a cabo un adecuado seguimiento del nivel de seguridad y cumplimiento de los objetivos.
- Formar y concienciar a todos los empleados en materia de seguridad de la información, garantizando que el personal dispone del suficiente conocimiento sobre las políticas y los controles de seguridad.
- Garantizar servicio ininterrumpido, alta satisfacción del cliente y rápida resolución de incidencias, asegurando que los incidentes de seguridad de la información son correctamente identificados, gestionados y resueltos.
- Cumplir con todos los requisitos legales, normativos, reglamentarios aplicables y obligaciones contractuales relacionados con la seguridad de la información.
- Asegurar la continuidad de los procesos de negocio incluidos dentro del alcance.

CAPÍTULO 4. Marco normativo

Grupo GP se esfuerza en cumplir con toda la legislación aplicable a su actividad, ya sea de carácter general o específico. Por todo ello, Grupo GP podrá ser requerida por los órganos administrativos pertinentes a proporcionar los registros electrónicos o cualquier otra información relativa al uso de los sistemas de información.

Esta política se sitúa dentro del marco jurídico definido por las leyes y reales decretos siguientes:

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI-CE).
- Real Decreto 13/2012, de 30 de marzo, por el que se modifica el texto correspondiente al apartado segundo del artículo 22 de la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones y Ley 11/2022, de 28 de junio, General de Telecomunicaciones en España.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

Grupo GP trata datos de carácter personal que se encuentran incorporados en los registros de actividades del tratamiento (RAT) correspondientes. Todos los sistemas de información de Grupo GP se ajustarán a los niveles de seguridad requeridos por la normativa relacionada:

- Reglamento Europeo de Protección de Datos 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) que adapta el ordenamiento jurídico español al RGPD.

Al comprometerse el Grupo GP a implantar los requisitos del ENS y establecer un Sistema de Gestión basado en dichos requisitos, la siguiente legislación también le es de aplicabilidad:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

La implantación de dichas leyes y decretos se completa en los documentos del Sistema de Gestión que cumplen los requisitos requeridos por el ENS.

CAPÍTULO 5. Sistema de Gestión

La Dirección de Grupo GP se compromete a destinar los recursos y medios necesarios para establecer, implantar, mantener y mejorar el Sistema de Gestión y los controles de seguridad necesarios, manteniendo un adecuado balance entre coste y beneficio, así como a demostrar liderazgo y compromiso respecto a éste.

Mejorar continuamente nuestro Sistema de Gestión de la Seguridad de la Información (SGSI). Todos los elementos de nuestro SGSI se nutren de los respectivos registros y evidencias que garantizan su cumplimiento.

La gestión de nuestro sistema se encomienda al Comité de Seguridad y el sistema estará disponible en nuestro Share Point corporativo, al cual se puede acceder según los perfiles de acceso concedidos según nuestro procedimiento en vigor de gestión de los accesos.

Por su parte, la Dirección dispone los medios necesarios y dota a sus empleados de los recursos suficientes para su cumplimiento, plasmándose y poniéndolos en público conocimiento a través de la presente Política disponible en nuestra web corporativa.

5.1. Objetivos y su planificación

Los objetivos de seguridad de la información se establecerán en las funciones y niveles pertinentes, enfocados a la mejora y utilizando como marco de referencia:

- Cambios en las necesidades de las partes interesadas que lleven a una mejora del alcance del sistema.
- Requisitos de seguridad de la información y los resultados de la apreciación y del tratamiento de los riesgos para garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información.
- Factores internos y externos.
- La mejora de la eficacia de la formación y concienciación del personal que trabaja en la entidad y afecta a su desempeño en seguridad de la información.

Asimismo, la planificación para la consecución de los objetivos de seguridad de la información establecidos se realizará considerando las acciones a realizar y su responsable, los recursos y plazos necesarios y los indicadores para evaluar el resultado/cumplimiento.

5.2. Establecimiento, despliegue y mejora del Sistema de Gestión

El establecimiento y despliegue del Sistema de Gestión de Grupo GP se iniciará a partir del Análisis de Riesgos, que permitirá determinar el nivel de riesgo de seguridad de la información en que se encuentra Grupo GP e identificar los controles de seguridad necesarios para el tratamiento del riesgo y llevarlo a un nivel aceptable, así como las oportunidades de mejora, considerando las cuestiones internas y externas y los requisitos de las partes interesadas.

Los controles de seguridad deberán implantarse, mantenerse y mejorarse continuamente, y estar disponibles como información documentada, mediante procedimientos, normativas, instrucciones técnicas, y cualquier otra documentación que así se considere, revisados y aprobados por el Comité de Seguridad de Grupo GP.

Se deberá comunicar la información documentada de los controles de seguridad al personal que trabaja en Grupo GP (empleados y proveedores), que tendrá la obligación de aplicarla en la realización de sus actividades laborales, comprometiéndose de ese modo al cumplimiento de los requisitos del Sistema de Gestión.

5.3. Evaluación

Se realizarán auditorías periódicamente que revisen y verifiquen el cumplimiento del Sistema de Gestión con los requisitos aplicables dentro del marco regulatorio del ENS, de la ISO 27001 y de la legislación vigente, por lo que, en caso necesario, el personal afectado por el alcance deberá colaborar en éstas, así como en la aplicación de las acciones correctivas que se deriven para el mejoramiento continuo. Se definirán criterios de cualificación para las personas que realicen dichas auditorías en los diferentes procedimientos que conforman el Sistema.

CAPÍTULO 6. Organización de la seguridad

6.1. Comités: funciones y responsabilidades

Con objeto de garantizar el cumplimiento de los intereses de la Dirección y asegurar una correcta gestión de la seguridad de la Información, se ha constituido el Comité de Seguridad, que responde a la Dirección.

El Comité de Seguridad es el órgano con mayor responsabilidad en la gestión de la seguridad de la información dentro del SGSI implementado, de forma que todas las decisiones más importantes relacionadas con la seguridad de la información se acuerdan por este Comité, levantando acta y actuando y decidiendo por mayorías. Es un órgano autónomo, ejecutivo y con autonomía para la toma de decisiones y que no tiene que subordinar su actividad a ningún otro elemento de Grupo GP. El Comité de Seguridad mediará y resolverá cualquier conflicto que pudiera surgir garantizando la seguridad de la información y el correcto funcionamiento del sistema de gestión implementado.

Los miembros del Comité de Seguridad de la información son:

- Responsable de Información y Servicio: Eduardo Gómez García
- Responsable de Seguridad: César Huerta, a través de NIMBUSTECH, delegando la gestión a Chema Gómez
- Responsable del Sistema: Ana Isabel Pérez Aparicio
- Delegado de Protección de Datos: José Antonio Torrado

La Alta Dirección a efectos del Sistema está representada por Gonzalo Vega y Antonio Gómez, pudiendo actuar en este ámbito de forma solidaria.

Estos miembros son designados por el órgano de gobierno de la Organización, único órgano que puede nombrarlos, renovarlos y cesarlos.

Las competencias del Comité de Seguridad y los miembros que forman parte de él se encuentran detallados en la documentación de funciones y responsabilidades del personal de Grupo GP.

6.2. Roles: funciones y responsabilidades

Los roles o funciones de seguridad definidos en la organización son:

Función	Deberes y responsabilidades
Responsable de la información y servicio	Tomar las decisiones relativas a la información tratada. Coordinar la implantación del sistema. Mejorar el sistema de forma continua.
Delegado de Protección de Datos	Velar por el cumplimiento de la normativa de protección de datos de carácter personal.
Responsable de la seguridad	Determinar la idoneidad de las medidas técnicas. Proporcionar la mejor tecnología para el servicio.
Responsable del sistema	Coordinar la implantación del sistema. Mejorar el sistema de forma continua.
Alta Dirección	Proporcionar los recursos necesarios para el sistema. Liderar el sistema.

(*) Todos los roles anteriores son coincidentes en ambas sociedades del Grupo GP, orquestándose todo el entorno de seguridad de forma unánime.

Esta definición se completa en los perfiles de puesto y en los documentos del sistema. El procedimiento para su designación y renovación será la ratificación en el Comité de Seguridad.

Los roles establecidos en la organización relacionados con la seguridad de la información se describen en los correspondientes documentos del Sistema de Gestión de la organización.

6.3. Resolución de conflictos

En caso de conflicto entre los diferentes responsables de Grupo GP, éste será resuelto por el superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Comité de Seguridad, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

CAPÍTULO 7. Gestión de riesgos de seguridad

Todos los sistemas sujetos a esta Política deberán realizar 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 o los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Responsable de Seguridad, con el apoyo, cuando sea necesario, del Comité de Seguridad, establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. Los criterios de evaluación de riesgos detallados se especificarán en la metodología de evaluación de riesgos, basándose en estándares y buenas prácticas reconocidas.

El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar, además de las requeridas como mínimo por parte del ENS, la ISO 27000 y restante legislación vigente. Aquellos controles que no sean de aplicación obligada por motivos legales, normativos o de negocio se aplicarán en base a la gestión de riesgos de la organización y los umbrales definidos y aprobados por el Responsable de Seguridad.

El Responsable de Seguridad realizará el análisis de los riesgos, así como el plan de tratamiento de los mismos, para generar el documento de aplicabilidad de los controles y medidas de seguridad. El Comité de Seguridad aprobará el análisis y tratamiento de los riesgos, así como la declaración de aplicabilidad. Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la organización de forma grave.

Los riesgos residuales esperados sobre cada información o servicio tras la implementación de las medidas de seguridad previstas serán determinados por el Responsable de Seguridad y presentados al Comité de Seguridad, para que éste proceda, en su caso, a evaluar, aprobar o rectificar las opciones de tratamiento propuestas. Dichos riesgos residuales deberán ser aceptados previamente por los responsables correspondientes.

CAPÍTULO 8. Incidencias de seguridad

8.1. Detección

Los departamentos de Grupo GP deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad.

8.2. Prevención

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una disminución hasta el cese del nivel de prestación, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.

8.3. Respuesta

Se han establecido mecanismos de detección, análisis y reporte para que se pueda informar a los responsables tanto regularmente como cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

8.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, se han desarrollado planes de restauración de los sistemas como parte de su plan de recuperación que pueden verse en los diferentes procedimientos que conforman el Sistema.

CAPÍTULO 9. Concienciación y formación

Se ha establecido un Plan de Formación y Concienciación en materia de Seguridad de la Información, que ayuda a todo el personal implicado a conocer y cumplir las actividades de gestión definidas, y a participar de manera activa en asegurar la seguridad de la organización.

CAPÍTULO 10. Desarrollo de la política

La Política de Seguridad de la Información se desarrolla por medio de manuales, restantes políticas, normativas o procedimientos detallados que afronten aspectos específicos de seguridad en general, cuya estructura, gestión y acceso están descritos en la documentación del Sistema y en concreto en el procedimiento de gestión de la información documentada y con los registros de actividades del tratamiento y tratamientos automatizados que contengan datos de carácter personal. Dicha documentación detallada estará 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.

La documentación de seguridad estará disponible en el sistema de información de Grupo GP en un repositorio en nuestro SharePoint corporativo, al cual se puede acceder según los perfiles de acceso concedidos según el procedimiento en vigor de gestión de los accesos.

La Política de Seguridad de la Información se desarrolla aplicando los siguientes principios mínimos:

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal.
- Profesionalidad.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos de seguridad y contratación de servicios de seguridad.
- Mínimo privilegio.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de actividad.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

CAPÍTULO 11. Obligaciones del personal

Los directores y responsables de las direcciones, áreas y departamentos de Grupo GP incluidos dentro del alcance de esta política serán los responsables de asegurar su cumplimiento dentro de sus departamentos.

Todos los trabajadores de Grupo GP tienen la obligación de conocer esta Política de Seguridad de la Información y la normativa y políticas de seguridad que la desarrollan, que son de obligado cumplimiento dentro del alcance identificado, siendo responsabilidad del Comité de Seguridad y de la Dirección de la empresa disponer los medios necesarios para que la información llegue a los afectados.

Todo el personal contratado deberá recibir y firmar un compromiso de cumplimiento de la Política de Seguridad de la Información y de la normativa de seguridad, y deberá recibir formación o concienciación relativa a la seguridad de la Información, en función de cuál sea su puesto de trabajo.

CAPÍTULO 12. Terceras partes

Cuando Grupo GP preste servicios a otras organizaciones o maneje información de otras organizaciones, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación del Comité de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando Grupo GP utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad de la Información y de la normativa de seguridad para que estén informados acerca de lo que aplica a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla o asumiendo los procedimientos de Grupo GP para la gestión. 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 Política 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.

Trabajar de forma conjunta con nuestros proveedores y subcontratistas con el fin de mejorar la prestación de servicios, la continuidad de los mismos y la seguridad de la información / confidencialidad / protección de datos de carácter personal, que repercutan en una mayor eficiencia de nuestra actividad para con los clientes.

CAPÍTULO 13. Aceptación de la Política de Seguridad de la Información

Este documento y cualesquiera otras normas, procedimientos, estándares o documentos relacionados con la seguridad de los sistemas de información y los datos que tratan, son propiedad de Grupo GP y, por lo tanto, tienen carácter confidencial estando únicamente permitida su utilización y difusión con carácter interno o externamente cuando así sea decidido por la Dirección de la empresa.

El incumplimiento de cualquiera de los principios recogidos en esta Política, dará lugar a una falta, que atendiendo a su importancia, reincidencia e intención se clasificará como leve, grave o muy grave, pudiendo ser sancionado según la legislación vigente, y pudiendo Grupo GP ejercitar tantas acciones como sean necesarias para la reclamación de daños y perjuicios.

CAPÍTULO 14. Difusión

La presente Política de Seguridad de la Información, aprobada por la Dirección, es conocida y suscrita por todo el personal de la organización, así como por los proveedores o las terceras partes que interactúen con la organización, conforme a las exigencias de la Dirección. Tras cada revisión, la Política será nuevamente publicada y comunicada al personal dentro del alcance y a otras partes interesadas, cuando aplique.

La presente Política se mantendrá publicada en el servidor de Grupo GP y será difundida externamente a través de la página web de Grupo GP.

CAPÍTULO 15. Revisión

Esta Política de Seguridad de la Información será revisada como mínimo anualmente o cada vez que se produzcan cambios importantes organizativos o en la infraestructura.

Será misión del Comité de Seguridad la revisión de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la Alta Dirección de Grupo GP y difundida para que la conozcan todas las partes afectadas.

D. Antonio Gómez López, como representante de la Alta Dirección de GRUPO GP

Fecha: 2 de junio de 2026

Esta política se complementa con el resto de las políticas, procedimientos, anexos y documentos en vigor para desarrollar nuestro SGSI.