POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Septiembre 2021

ÍNDICE

1. COMPROMISO DE LA DIRECCIÓN 3

2. OBJETIVOS 3

3. LINEAMIENTO DE LA POLÍTICA DE SEGURIDAD 4

4. ÁMBITO DE APLICACIÓN 4

5. DOCUMENTOS DE REFERENCIA 4

6. ORGANIZACIÓN Y RESPONSABILIDADES 5

6.1. Comité de Seguridad 5

6.2. Atribuciones y mecanismos de resolución de conflictos 6

7. NORMAS DE SEGURIDAD DE LA INFORMACIÓN 6

8. CLASIFICACIÓN DE LA INFORMACIÓN 6

9. ANÁLISIS DE SEGURIDAD 6

10. AUDITORÍA 7

11. PLANES DE SEGURIDAD ESPECÍFICOS 7

12. PROVEEDORES Y TERCERAS PARTES 7

13. LEGISLACIÓN APLICABLE 7

14. CRIPTOGRAFÍA 7

15. EFECTO 7

16. PROCESO DE APROBACIÓN Y REVISIÓN 8

1. COMPROMISO DE LA DIRECCIÓN

La Dirección del **GRUPO INV**, dentro de la estrategia global definida para el desarrollo del negocio, considera la seguridad de la información y la de los datos personales como un aspecto vital para garantizar la consecución de forma eficiente y eficaz de los objetivos de negocio definidos. "*Estamos obligados a garantizar la máxima seguridad de los servicios que prestamos, es decir, la integridad, confidencialidad, autenticidad, trazabilidad y disponibilidad de los datos, sistemas y/o conexiones al* ***GRUPO INV***".

La Dirección se compromete a liderar y fomentar a todos los niveles la seguridad de acuerdo a la Política de Seguridad y los objetivos que en ella se definen, creando un Sistema de Gestión para la Seguridad de la Información (SGSI) que se articule en las normas y reglas de gestión, protección y distribución que emanan de la ISO 27001 y del Esquema Nacional de Seguridad (ENS).

2. OBJETIVOS

La Política de Seguridad de la Información del GRUPO INV supone el compromiso expreso de la empresa en determinar y establecer las directivas y el soporte adecuado para la administración de la seguridad de la información que maneja, de acuerdo con los requerimientos propios y con las leyes y regulaciones vigentes.

Se asumen de este modo los siguientes objetivos:

- Considerar la información y los sistemas que la soportan como activos estratégicos. Así pues, GRUPO INV manifiesta su determinación de alcanzar los niveles de seguridad necesarios que garanticen los requisitos de confidencialidad, integridad, autenticidad, trazabilidad y disponibilidad de la información procesada en la organización y de los recursos de los sistemas de información que la procesan, almacenan o distribuyen.
- Garantizar la difusión de la normativa definida como soporte de esta Política, con el objetivo de conseguir infundir entre el personal que preste sus servicios en el GRUPO INV un nivel de concienciación y formación en materia de seguridad de la información que garantice la aplicación de prácticas adecuadas en esta materia, como elemento inherente al desarrollo de sus funciones.
- Promover que la consecución de los niveles de seguridad de la información requeridos se desarrolle como un proceso continuo de mejora y progreso constante, sustentado en la definición de los objetivos y requisitos a cumplir, la implantación de los procesos y medidas oportunos, la comprobación constante de su efectividad, eficacia y eficiencia, y la adopción de las correcciones y modificaciones que resulten adecuadas.
- Adoptar la Política de Seguridad de la Información como la principal herramienta para garantizar adecuadamente la Seguridad de la Información, promoviendo y asegurando su cumplimiento dentro de los diferentes servicios.

- Velar por la existencia de los mecanismos necesarios que aseguren la continuidad de las actividades críticas de la empresa que estén sustentadas en los sistemas de información, permitiendo la recuperación de los mismos en un periodo de tiempo aceptable.
- Maximizar la calidad de los servicios prestados.
- Reducir o eliminar los peligros y riesgos en nuestros activos, procesos y servicios.

3. LINEAMIENTO DE LA POLÍTICA DE SEGURIDAD

El conjunto de políticas y procedimientos de seguridad resultado de la implantación de la presente será definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.

Éstas serán revisadas anualmente o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Estarán en todo momento alineadas con los requerimientos legales y contractuales con clientes, proveedores y trabajadores, garantizándose el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual, RGPD, LOPDGDD y prevención de riesgos laborales.

4. ÁMBITO DE APLICACIÓN

Esta política afecta a todos los activos de información y de soporte a los procesos de negocio definidos por el GRUPO INV para el desarrollo de sus actividades y es de aplicación obligatoria para todos los empleados de la organización y terceros implicados en el uso de la información y los sistemas.

5. DOCUMENTOS DE REFERENCIA

- 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 (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Norma UNE-ISO/IEC 27001:2014.

- Norma UNE-ISO/IEC 27002:2015.

6. ORGANIZACIÓN Y RESPONSABILIDADES

La función de la seguridad es responsabilidad de la Dirección General, que delegará estas facultades en el delegado de Protección de Datos para los asuntos relacionados con la protección de datos de carácter personal y el responsable de Seguridad para el resto de asuntos relacionados con la seguridad del GRUPO INV.

La Dirección establecerá los órganos de organización y control necesarios para velar por el correcto cumplimiento de las normas establecidas por la empresa y la legislación a la que está sujeta.

Con las facultades delegadas, los responsables de Seguridad supervisarán la implantación, con el apoyo de la organización de seguridad, de los controles de seguridad y aplicación del cuerpo normativo en las diferentes áreas de la empresa.

Todo usuario de sistemas es responsable del uso que se haga de los mismos y del cumplimiento de los controles establecidos.

Los roles y responsabilidades se encuentran detallados en el documento “SG-P-005 Roles y responsabilidades”.

6.1. Comité de Seguridad

Con el objetivo de hacer consultas regulares y periódicas de las actuaciones de la organización en materia de la seguridad de la información, se ha nombrado un Comité de Seguridad, formado por los siguientes representantes:

- Presidente del Comité: Según nombramiento en “SG-R-101 Acta de Reunión CS 001 v1.0”.
- Responsable de Seguridad: Según nombramiento en “SG-R-101 Acta de Reunión CS 001 v1.0”.
- Delegado de Protección de Datos: Según nombramiento en “SG-R-118 BIS Acta de Reunión DPD-RGPD”.
- Secretario del Comité: Según nombramiento en “SG-R-101 Acta de Reunión CS 001 v1.0”.

Sus responsabilidades son, entre otras, las siguientes:

- Mantenimiento de la presente Política de Seguridad de la Información.
- Creación y aprobación de las normas y procedimientos sobre el uso de las TICs.

- Definición de requisitos de formación y concienciación a los usuarios en materia de seguridad.

6.2. Atribuciones y mecanismos de resolución de conflictos

Las atribuciones de cada responsable y los mecanismos de resolución de conflictos se han detallado en el procedimiento “SG-P-005 Roles y Responsabilidades”.

7. NORMAS DE SEGURIDAD DE LA INFORMACIÓN

La presente Política de Seguridad de la Información será soportada y complementada por un conjunto de documentos específicos. Estos documentos son las denominadas Normas de Seguridad de la Información y estarán basadas en las mejores prácticas de mercado y alineadas con las necesidades específicas del GRUPO INV.

8. CLASIFICACIÓN DE LA INFORMACIÓN

Toda la información debe ser clasificada, de acuerdo con su importancia para la organización y debe ser tratada de conformidad con dicha clasificación, cumpliendo con las disposiciones de la norma en materia de clasificación y tratamiento de información clasificada.

Deben seguirse las pautas reflejadas en el documento: CS-P-003 Procedimiento de clasificación y tratamiento de la información clasificada.

9. ANÁLISIS DE SEGURIDAD

Ante implantación de nuevos procesos o cambios importantes en los mismos o en la infraestructura que los soportan, se realizarán los oportunos análisis de riesgos que permitan su correcta gestión y tratamiento.

Para estas actividades se definirá una metodología acorde con las necesidades del negocio, el entorno de las operaciones y los servicios y las buenas prácticas reconocidas internacionalmente.

La metodología que se sigue para llevar a cabo los análisis de riesgos se recoge en el siguiente documento: GR-P-001 Metodología de análisis de riesgos.

10. AUDITORÍA

Los sistemas de información se someterán periódicamente a auditorías internas y externas con el fin de comprobar la correcta aplicación de la normativa de seguridad, determinar el grado de cumplimiento y recomendar medidas correctoras.

11. PLANES DE SEGURIDAD ESPECÍFICOS

Cualquier plan de seguridad de la información específico de un proceso o servicio debe cumplir con todas las disposiciones contempladas en esta norma.

12. PROVEEDORES Y TERCERAS PARTES

Todas las adquisiciones relevantes de bienes o servicios o que supongan un impacto en los servicios o sistemas de la empresa, serán sometidos a un proceso de análisis de riesgos.

Los requisitos de seguridad de la información para la mitigación de los riesgos asociados al proveedor deben acordarse con este y quedar documentados, y debe seguirse lo establecido en el documento: CS-P-017 Normativa de buenas prácticas con terceros.

13. LEGISLACIÓN APLICABLE

Para los aspectos de legislación aplicable en materia de seguridad de la información, se encuentran reflejados en el documento: SG-P-007: Requisitos legales, normativos y contractuales del SGSI.

14. CRIPTOGRAFÍA

En los casos que sea requerido contractualmente por los clientes y siempre dentro de la ley y las buenas prácticas de seguridad, se utilizarán los controles criptográficos que se acuerden con estos.

15. EFECTO

La Política de Seguridad de la Información surtirá efecto a partir el mismo día de su publicación en la intranet y web de la empresa.

16. PROCESO DE APROBACIÓN Y REVISIÓN

Este documento está sujeto a un proceso de revisión regular que lo adapte a nuevas circunstancias, técnicas u organizativas, marcos de referencia, etc. y evitar que quede obsoleto.

Para ello se establecerá un proceso organizativo que asegure que regularmente se revisa la oportunidad, idoneidad, completitud y precisión de lo que la presente Política establece y será sometido a la aprobación formal por parte de la Dirección del GRUPO INV.

LA DIRECCIÓN

Mayo 2022