POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

GAUSS CONTROL

1. **Introducción:** Gauss Control aprueba la adopción de un Sistema de Gestión de Seguridad de la Información (SGSI), un conjunto de medidas destinadas a preservar la confidencialidad, integridad y disponibilidad de la información, que constituyen los tres componentes básicos de la seguridad de la información, y tiene como objetivo establecer los requisitos para proteger la información, los equipos y servicios tecnológicos que sirven de soporte para la mayoría de los procesos de negocio de Gauss Control.

La presente Política de Seguridad de la Información (en adelante "la Política") es la pieza angular por la que se rige el Cuerpo Normativo de Seguridad de Gauss Control, que es un conjunto de documentos a diferentes niveles que conforman los requerimientos, directrices y protocolos que se deben seguir en materia de seguridad. El **Documento de Seguridad (en adelante DS)** deberá ser desarrollado mediante un conjunto de documentos (normas de uso, estándares normativos, procedimientos, manuales, guías, buenas prácticas, etc.) de tal manera que cubran todos los aspectos que se presentan en la Política, llegando a nivel de proceso operativo. En la actualidad, las tecnologías de la información se enfrentan a un creciente número de amenazas, lo cual requiere de un esfuerzo constante por adaptarse y gestionar los riesgos introducidos por estas.

1.1. **Objetivo**: El objetivo principal de la presente Política de alto nivel es definir los principios y las reglas básicas para la gestión de la seguridad de la información. El fin último es lograr que Gauss Control garantice la seguridad de la información, su integridad, confidencialidad y disponibilidad, y minimice los riesgos de naturaleza no financiera derivados de un impacto provocado por una gestión ineficaz de la misma.

1.2. **Alcance**: La Política deberá cumplir este mínimo requisito sin perjuicio de tener políticas más restrictivas y mejorar la seguridad en la medida de lo posible. Gauss Control deberá adaptar y desarrollar esta Política y deberá reportar la adecuación de dicha Política. El alcance de la presente Política abarca toda la información relativa a los procesos, servicios y productos de Gauss Control, con independencia de la forma en la que se procese, quién acceda a ella, el medio que la contenga o el lugar en el que se encuentre, ya se trate de información impresa o almacenada electrónicamente. La presente política aplicará a:

- Los colaboradores de Gauss Control, proveedores de bienes o servicios; y en general, a todos aquellos con quienes de manera directa o indirecta Gauss Control establezca alguna relación contractual o de cooperación.
- Los activos de información que almacenen, gestionen y/o transporten datos.

La Política deberá estar disponible en la página web corporativa www.gausscontrol.com y en un repositorio común de DS, de forma que sea accesible por todas las personas de la compañía.

1.3. **Adaptación y desarrollo de la Política de Seguridad de la información:** La Política deberá ser adaptada y desarrollada continuamente en la compañía. Se decidirá la manera en la que adapta la Política a su operativa mediante documentación concreta de DS, que siempre deberá estar alineada con las directrices que se marcan en el presente documento.

2. Principios de la Política de la Seguridad de la Información

La presente Política responde a las mejores prácticas de Seguridad de la Información recogidas en el Estándar Internacional ISO/IEC 27001, así como al cumplimiento de la legislación vigente en materia de protección de datos personales y de las normativas que, en el ámbito de la Seguridad de la Información, puedan afectar a Gauss Control. Además, se establecen los siguientes principios básicos como directrices fundamentales de seguridad de la información que han de tenerse siempre presentes en cualquier actividad relacionada con el tratamiento de información:

- **Alcance estratégico**: La seguridad de la información contará con el compromiso y apoyo de todos los niveles directivos de Gauss Control, de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas para conformar un marco de trabajo completamente coherente y eficaz. Puesto que la Seguridad de la Información incumbe a todo el personal de Gauss Control, esta Política deberá ser conocida, comprendida y asumida por todos sus empleados.
- **Seguridad integral**: La seguridad de la información se entenderá como un proceso integral constituido por elementos técnicos, humanos, materiales y organizativos, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información deberá considerarse como parte de la operativa habitual, estando presente y aplicándose durante todo el proceso de diseño, desarrollo y mantenimiento de los sistemas de información.
- **Gestión de riesgos**: Gauss Control define un proceso de identificación y evaluación de riesgos, para implementar controles de mitigación y estableciendo procedimientos regulares para su reevaluación. El análisis y gestión de riesgos será parte esencial del proceso de seguridad de la información. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que están expuestos y la eficacia y el coste de las medidas de seguridad.
- **Proporcionalidad:** El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos, a la criticidad, valor de la información y de los servicios afectados.

- **Mejora continua**: Las medidas de seguridad se evaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado. En el transcurso de este ciclo de mejora continua, Gauss Control mantendrá la definición tanto del nivel de riesgo residual aceptado (apetito al riesgo) como de sus umbrales de tolerancia.

3. **Compromiso de la Dirección:** La Dirección de Gauss Control se compromete a:

- Promover en la organización las funciones y responsabilidades en el ámbito de seguridad de la información.
- Disponer los recursos adecuados para alcanzar los objetivos de seguridad de la información.
- Impulsar la divulgación y la concienciación de la Política de Seguridad de la Información entre los empleados de Gauss Control.
- Exigir el cumplimiento de la Política, de la legislación vigente y de los requisitos de los reguladores en el ámbito de la seguridad de la información.
- Considerar los riesgos de seguridad de la información en la toma de decisiones.

4. Roles y responsabilidades

Gauss Control, a través de su alta dirección y de su Comité de Seguridad de la Información,se compromete a velar por la Seguridad de todos los activos bajo su responsabilidad, siempre garantizando el cumplimiento de las distintas normativas y leyes aplicables. Gauss Control, nombrará una figura responsable de definir, implementar y monitorear las medidas de ciberseguridad y seguridad de la información, responsables de la gestión, mantenimiento y aplicación del SGSI.

Las responsabilidades específicas por cargo se describen a continuación:

Cargo	Responsabilidades
Gerente General/Gerente de Finanzas	- Revisar y aprobar la Política General de Seguridad de la Información con base en una evaluación de riesgos de ciberseguridad, al menos una vez al año. - Autorizar la provisión de recursos para la correcta implementación de la Política de Seguridad de la Información.
Encargado de Seguridad de la Información y Gobierno de Datos	- Realizar un análisis de riesgo de manera anual y actualizar el documento de Política de Seguridad de la Información en base al resultado del análisis. - Tomar acciones correctivas en base a un proceso de mejora continua. - Ejecutar un plan de mitigación de tales riesgos.
Comité de Ciberseguridad	- Gestionar las respuestas a situaciones de crisis e incidentes.- Realizar ensayos de respuesta frente a situaciones de contingencia mayor. - Establecer una política de comunicación de incidentes.
Data Owners	- Velar por la implementación del Sistema de Gestión de Seguridad de la Información. - Asegurar la capacitación y concientización de las personas. - Establecer un plan de trabajo sobre los resultados de las auditorías internas.

21. Gestión de Excepciones

Cualquier excepción a la presente Política de Seguridad de la Información, o a otra que emane desde el SGSI regido por la presente Política, deberá ser registrada e informada al responsable de la Seguridad de la Información de Gauss Control. Estas excepciones serán analizadas para evaluar el riesgo que podrían introducir a la sociedad y, en base a la categorización de estos riesgos, estos deberán ser asumidos por el peticionario de la excepción junto con los responsables del negocio.

22. Sanciones disciplinarias

Cualquier violación de la presente Política de Seguridad de la Información, o a otra que emane desde el SGSI regido por la presente Política, puede resultar en la toma de las acciones disciplinarias correspondientes de acuerdo con el proceso interno de Gauss Control. Es responsabilidad de todos los empleados de Gauss Control notificar al responsable de Seguridad de la Información de la sociedad afectada ante cualquier evento o situación que pudiera suponer el incumplimiento de alguna de las directrices definidas por la presente Política.

23. Revisión de la Política

La aprobación de esta Política implica que su implantación contará con el apoyo de la Dirección para lograr todos los objetivos establecidos en la misma, como también para cumplir con todos sus requisitos. La presente Política de Seguridad de la Información, será revisada y aprobada anualmente por el Consejo de Administración. No obstante, si tuvieran lugar cambios relevantes en la sociedad o se identificaran cambios significativos en el entorno de amenazas y riesgos, ya sean estos de tipo operativo, legal, regulatorio o contractual, se procederá a su revisión siempre que se considere necesario, asegurando así que la Política permanece adaptada en todo momento a la realidad de Gauss Control.