Grenergy
renovables

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

JUNIO 2023

ÍNDICE

1. OBJETIVO

El objetivo de esta política es establecer los principios básicos y el marco general para el control y la gestión de los riesgos de Seguridad de la Información a los que está expuesta Grenergy.

El marco de Seguridad de la Información de Grenergy, contiene las normas y regulaciones que establecen los requisitos organizativos, de procedimiento y técnicos para proteger los activos de información y los productos, soluciones y servicios de Grenergy frente a las amenazas internas y externas.

2. ALCANCE

El presente documento resulta de aplicación a todos los empleados de GRENERGY, así como a todas las sociedades del Grupo, incluyendo las sociedades participadas en las que cuenta con un control efectivo o con posibilidad de este.

Es responsabilidad de las personas físicas y jurídicas más arriba mencionadas, cualquiera que sea la función desempeñada en el seno de la organización o sociedades del Grupo a la que pertenezcan, conocer, hacer respetar y cumplir el presente documento.

El cuerpo normativo interno del grupo forma parte de las obligaciones contractuales del trabajador y por tanto cualquier incumplimiento de este, conllevará las sanciones disciplinarias que procedan.

3. POLÍTICA DE SEGURIDAD DE LA INFORMA

3.1. La Seguridad de la Información

A menudo se consideran como activos de la empresa únicamente los bienes tangibles como mobiliario, maquinaria, servidores, etc. Sin embargo, también existen bienes intangibles como la cartera de clientes, las tarifas, el conocimiento comercial, la propiedad intelectual o la reputación entre otros. **Todos estos elementos forman parte de la información de nuestra empresa y constituyen uno de los activos más importantes de nuestra organización y que por tanto deben ser protegidos.**

La seguridad de la información es un término más general que abarca tanto el ámbito digital (ciberseguridad) como el físico. Son conceptos similares pero el de seguridad de la información es más amplio e incluye la ciberseguridad.

3.2.- Principios básicos para la Seguridad de la Información

1. Proteger los activos de información y tecnológicos críticos de la compañía frente a posibles amenazas de ciberseguridad y físicas.
2. Sensibilizar a todos los empleados acerca de los riesgos de seguridad y garantizar que disponen de la formación y capacidades tecnológicas

necesarias para proteger la seguridad de los sistemas de información del grupo.

3. Desarrollar la implantación de mecanismos de seguridad adecuados siguiendo un enfoque basado en los riesgos específicos de la compañía.
4. Promover las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación que permitan reaccionar con agilidad ante posibles amenazas.
5. Mantener un proceso de revisión y mejora continua del modelo de gestión de la seguridad para que se mantenga actualizado frente a las condiciones cambiantes del entorno tecnológico y las nuevas amenazas.
6. Garantizar el cumplimiento normativo aprobado relativo a la seguridad de la información.

3.3.- Riesgos en la Seguridad de la Información

Es necesario establecer los controles que nos permitan prevenir y mitigar los riesgos en la Seguridad de la Información en la medida de lo posible. A continuación, y a modo ilustrativo se recoge una clasificación de los riesgos más comunes en seguridad de la información.

Riesgos digitales

El riesgo digital se refiere a todas las consecuencias inesperadas que provienen de los sistemas digitales. Algunos ejemplos en donde se puede materializar los riesgos digitales son:

- Riesgo de ciberataques, Malware, phishing, ataques de denegación de servicio o ransomware son algunos de los métodos que los ciberdelincuentes utilizan para tratar de obtener acceso a un sistema y utilizarlo contra los intereses de la compañía.
- Falta de habilidades digitales y concienciación sobre la materia.
- Problemas de compatibilidad entre sistemas IT y riesgos derivados de la falta de actualización de los mismos.
- Riesgos de adopción durante la implantación de una nueva tecnología cómo por ejemplo pérdida de información.
- Riesgos derivados de una mala calidad del dato, como errores y toma de malas decisiones basadas en información imprecisa.
- Riesgos sobre la privacidad de datos gestionados por la empresa (bases de datos, cookies de la página web, etc.).

Riesgos físicos

Son los riesgos que se refieren a consecuencias indeseadas que pueden impactar en los equipos físicos o a su uso indebido.

- Irregularidades en el control de accesos: Manipulación de vigilantes, de controles de acceso y/o biométricos.

- Fallos en los dispositivos provocados por el deterioro o antigüedad de los sistemas que pueden hacer que la información no esté accesible, no sea fiable e incluso causar la caída total de un sistema.
- Deterioro o destrucción de activos con información sensible por un uso inadecuado.
- Robo y pérdida de activos corporativos con información confidencial.
- Catástrofes naturales como terremotos, inundaciones o huracanes. Especialmente relevantes en zonas proclives a sufrir este tipo de desastres.

3.4.- Modelo Organizativo

3.4.1 Compromiso de la Dirección

La Dirección de Grenergy, consciente de la importancia de la seguridad de la información, se compromete a:

- Impulsar la divulgación y la concienciación de la Política de Seguridad de la Información entre los empleados del grupo.
- Facilitar los recursos adecuados para alcanzar los objetivos de seguridad de la información.
- Considerar los riesgos de seguridad de la información en la toma de decisiones.

3.4.2 Comité de seguridad de la información en Grenergy

Grenergy decide crear un comité de seguridad cuyo objetivo principal es velar por que todos los empleados conozcan y cumplan la política de ciberseguridad y normas internas que la desarrollan.

El Comité de Seguridad de la Información estará formado por el CHRO, el responsable de IT & Digital de Grenergy y el responsable de Compliance.

El Comité debe ser un órgano adaptable y con un enfoque práctico, por lo que si todos sus integrantes están de acuerdo se podrán incluir miembros adicionales que complementen el conocimiento y capacidades del Comité. Asimismo, el Comité podrá contar con el asesoramiento de expertos externos para asegurar su correcto y eficaz funcionamiento.

3.4.3 Gestión del riesgo

A) Evaluación e identificación de los riesgos

En Grenergy, el Comité de Seguridad de la Información identificará y evaluará los riesgos relativos a la seguridad de la información, emitiendo un informe anual o cuando sea necesario a petición de los Órganos de Administración.

La identificación y evaluación se realizará:

- Regularmente, una vez al año.

- Cuando haya cambios significativos en la estructura y Sistemas de Información (IT).
- Cuando ocurra un incidente de seguridad grave.

B) Gestión de riesgos

Una vez identificados y evaluados los riesgos, se establecerá por el Comité de Seguridad las medidas oportunas para mitigarlos en la medida en que sea necesario, de forma que los valores de riesgo residual se consideren valores aceptables.

4. CLÁUSULA DE RESERVA

GRENERGY se reserva expresamente el derecho de modificar, actualizar y/o eliminar unilateralmente, cualquier cuestión regulada en el/la presente política/norma/procedimiento.

5. MAYORES CAMBIOS COMPARADOS CON LA ÚLTIMA REVISIÓN

Versión:	Descripción del cambio
1.0	Versión inicial