

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

RJC ECOGESTIONES SAS, en aplicación de las disposiciones establecidas en la Ley 1581 de 2012 y el Decreto 1074 de 2015 y entendiendo la importancia de una adecuada gestión de la información para prevenir los riesgos existentes en el que es considerado su principal activo empresarial; ha implementado un sistema de gestión para garantizar su seguridad, basados en un marco de confianza para el desarrollo de su operaciones así como el relacionamiento con sus grupos de interés y valor, en concordancia con la misión y visión de la empresa.

1. Objetivos y Principios Generales

La gobernanza de la información en la organización se regirá por los siguientes pilares estructurales:

- Gestión del Riesgo: Identificar, valorar y minimizar de forma sistemática las vulnerabilidades en todos los procesos, clasificándolos de acuerdo con su nivel de riesgo.
- Tríada de la Seguridad: Integridad, Confidencialidad y Disponibilidad de la información, como ejes fundamentales de la gestión organizacional.
- Cultura Organizacional: Fortalecer la conciencia sobre seguridad en todos los niveles organizacionales, incluyendo aprendices, clientes y proveedores.
- Resiliencia Operativa: Garantizar la continuidad del negocio ante incidentes de seguridad.

2. Recomendaciones sobre uso seguro de herramientas informáticas y lineamientos de responsabilidad.

La seguridad de la información es un compromiso compartido. Los usuarios deben seguir estas pautas en el uso de las herramientas asignadas:

- Toda la información catalogada por las áreas como importante debe contar con copias de respaldo para garantizar su seguridad.



EcoGestiones

- Los equipos de cómputo y procesamiento de información son áreas de acceso restringido por tal motivo el ingreso y retiro de información o equipos debe ser controlado y supervisado.
- No responda ni dé clic a enlaces que reciba de remitentes desconocidos; primero asegúrese de que se trata de una fuente confiable. Se recomienda escribir el enlace directamente en el navegador.
- Compruebe que la URL o enlace estén aseguradas con certificado SSL, que significa que esté incluido el **https**.
- Cambie sus contraseñas de forma regular (por lo menos 1 vez al mes), evitando usar la misma en todas las cuentas que tenga, así como datos evidentes como su nombre, teléfono o fecha de nacimiento. Como sugerencia se recomienda usar una contraseña mínima de 12 a 16 caracteres.
- Las contraseñas que no sean de fácil acceso para los criminales, permitirán un resguardo efectivo de la información y son la primera línea para la prevención de riesgos.
- No comparta inmediatamente todo lo que recibe, analice y verifique la veracidad de la información antes de difundirla entre sus compañeros.
- Evite aceptar personas que no conoce en sus redes sociales, así tengan muchos amigos en común.
- No publique todo lo que hace, ni todos los lugares a los que va. Tenga en cuenta que esa es información que los delincuentes pueden usar.
- Evite tener encuentros con personas que haya conocido en los entornos digitales; tenga en cuenta que siempre existe la posibilidad de que sea un perfil falso.
- Evite compartir sus cuentas personales y contraseñas de aplicativos con personas ajenas a su entorno familiar.
- Evite poner la misma clave de seguridad en más de una cuenta.

3. El traslado de activos

- El colaborador que tenga bajo su responsabilidad o asignado algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.
- Los equipos de comunicación y/o computación que sean propiedad de la empresa RJC ECOGESTIONES SAS no deben abandonar las instalaciones en las que fueron asignadas a menos que esté acompañado por la autorización respectiva según el formato FT-SG-



301 669 8128



contactenos@ecogestiones.com
www.ecogestiones.com



Planta: Vereda la Florida, Predio San Javier. Funza-Cundinamarca



EcoGestiones

OPE-071 FORMATO CONTROL DE ENTRADA Y SALIDA DE HERRAMIENTAS y la validación de la alta gerencia.

- Está estrictamente prohibido el uso del equipo informático perteneciente a los compañeros de trabajo sin la debida autorización. Cualquier utilización no autorizada de los recursos informáticos de otros empleados constituye una violación de las políticas de seguridad de la información de la empresa y puede resultar en medidas disciplinarias.

4. Sanciones

- El incumplimiento de las políticas de seguridad de la información descritas en este documento se trata mediante el procedimiento de incidentes de seguridad de la información, de acuerdo con la naturaleza del incidente y los resultados de su tratamiento e investigación y los responsables de los procesos institucionales evalúan la necesidad de adelantar procesos disciplinarios o legales.
- Se consideran violaciones graves el robo, daño, duplicación, extracción y divulgación de información reservada o confidencial de la Institución, o de que se le declare culpable de un delito informático.

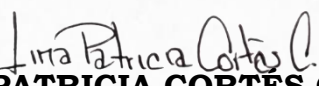
La presente política involucra toda la información manejada por la organización en cualquier formato o medio, generada internamente o proporcionada por terceros.

Su alcance implica a todos los empleados, contratistas, proveedores y otras partes que tengan acceso a nuestra información.

Con la presente se aprueba la política de seguridad de la información de la empresa RJC ECOGESTIONES SAS a los 8 días del mes de Mayo de 2026.



EcoGestiones


LINA PATRICIA CORTÉS CORTÉS
Gerente General
RJC ECOGESTIONES SAS



301 669 8128



contactenos@ecogestiones.com
www.ecogestiones.com



Planta: Vereda la Florida, Predio San Javier. Funza-Cundinamarca