POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

ENVIAMOS COMUNICACIONES S.A.S.

1. Objetivo

Establecer los lineamientos generales para la implementación, mantenimiento y mejora continua de la gestión de la seguridad de la información y la ciberseguridad en **ENVIAMOS COMUNICACIONES S.A.S.,** con el propósito de proteger los activos de información frente a riesgos o amenazas que puedan afectar su confidencialidad, integridad, disponibilidad o trazabilidad.

Esta política tiene como finalidad resguardar los procesos operativos, tecnológicos, logísticos y administrativos, así como los activos de información físicos y digitales de la organización, contribuyendo a la continuidad del negocio y al fortalecimiento de la confianza de los clientes, aliados y demás partes interesadas.

2. Alcance

Esta política aplica a todos los colaboradores, contratistas, proveedores y terceros que accedan, administren o procesen información propiedad de **ENVIAMOS COMUNICACIONES S.A.S.,** independientemente de su forma o medio de almacenamiento.

Su aplicación comprende todas las áreas, procesos, sistemas, plataformas tecnológicas, infraestructuras y ubicaciones físicas o remotas desde las cuales se gestione información de la organización o de sus partes interesadas.

3. Compromiso de la alta dirección

La alta dirección de **ENVIAMOS COMUNICACIONES S.A.S.** demuestra su compromiso con la seguridad de la información y la ciberseguridad mediante la asignación de recursos, liderazgo y apoyo a todas las iniciativas relacionadas con esta materia.

En cumplimiento de este compromiso, la dirección se responsabiliza de:

- Proveer los recursos humanos, tecnológicos y financieros necesarios para implementar, mantener y fortalecer la seguridad de la información y la ciberseguridad.
- Cumplir los requisitos legales, regulatorios, normativos y contractuales aplicables en materia de seguridad de la información y protección de datos.
- Identificar, evaluar y tratar proactivamente los riesgos asociados.
- Promover la mejora continua y fomentar una cultura organizacional orientada a la protección de la información y a la gestión responsable del riesgo.

4. Principios generales

Todos los colaboradores, contratistas y terceros que gestionen información de **ENVIAMOS COMUNICACIONES S.A.S.** deben cumplir con los siguientes principios:

- **Confidencialidad**: Resguardar la información conforme a su nivel de clasificación, evitando su divulgación no autorizada.
- **Integridad**: Proteger los datos y sistemas de información, previniendo alteraciones o manipulaciones indebidas.
- **Disponibilidad**: Asegurar que la información, los sistemas y los servicios estén accesibles para los usuarios autorizados cuando se requiera.
- **Reporte oportuno**: Informar de manera inmediata cualquier incidente, anomalía o sospecha que pueda afectar la seguridad de la información o los activos tecnológicos.
- **Cumplimiento**: Observar las políticas, procedimientos, normas y controles establecidos por la organización en materia de seguridad de la información y ciberseguridad.

5. Roles y responsabilidades

Para garantizar la adecuada gestión de la seguridad de la información y la ciberseguridad, se establecen los siguientes roles y responsabilidades:

- **Comité de Riesgos:** Dirige y supervisa la implementación de la política, define estrategias y prioriza acciones para la gestión de riesgos, incidentes y mejora continua.
- **Responsable de Seguridad de la Información y Ciberseguridad:** Coordina las actividades de identificación, evaluación y tratamiento de riesgos, ejecución de auditorías internas, capacitación y concientización del personal.
- **Usuarios finales (colaboradores, contratistas y terceros):** Cumplen las políticas, procedimientos y controles definidos por la organización, utilizan los recursos tecnológicos de manera responsable y reportan de inmediato cualquier anomalía, incidente o vulnerabilidad detectada.

6. Lineamientos

Los activos de información de la organización están conformados por los sistemas de información, aplicativos de software, bases de datos, archivos físicos y digitales, así como por cualquier otro elemento o recurso asociado a los procesos internos.

Por tal motivo, se establecen los siguientes lineamientos, los cuales deberán ser observados y cumplidos por todo el personal de la organización, con el propósito de proteger y asegurar el uso adecuado de la información.

- Todo el personal debe aplicar las políticas institucionales y utilizar los procedimientos y herramientas autorizadas para acceder a la información de la organización.

- Se prohíbe el ingreso a módulos, sistemas o aplicaciones no autorizadas, así como la extracción, modificación, alteración o eliminación de información de manera no permitida.

- La información contenida en los sistemas de la organización solo podrá ser utilizada para el desarrollo de las actividades laborales asignadas, quedando estrictamente prohibido su uso con fines personales o ajenos a la operación.
- Se prohíbe el uso de equipos de cómputo personales dentro de las instalaciones de la organización, salvo autorización expresa de la gerencia.
- No se permite conectar a los equipos institucionales dispositivos de almacenamiento externo, como memorias USB u otras unidades portátiles, sin la autorización correspondiente.
- Está prohibido retirar equipos de cómputo o dispositivos de las oficinas de la organización sin la aprobación previa de la gerencia.
- Cada empleado es responsable del adecuado uso, custodia y conservación de su estación de trabajo y del equipo de cómputo asignado.
- Los equipos institucionales deben ser utilizados exclusivamente para las funciones propias del cargo; no está permitido su uso para actividades personales o ajenas al ámbito laboral.
- No se permite el préstamo de estaciones de trabajo o equipos de cómputo a terceros.
- Las actividades de mantenimiento, reparación o soporte técnico de los equipos de cómputo deberán ser realizadas únicamente por la persona o proveedor designado por la gerencia.

7. Incumplimiento

El incumplimiento de lo establecido en esta política, así como de los procedimientos, lineamientos o controles derivados de ella, podrá generar acciones disciplinarias, contractuales o legales, de acuerdo con el reglamento interno de trabajo, los contratos suscritos y la normativa vigente.

Dichos incumplimientos podrán ser considerados como faltas que comprometen la seguridad de la información, la ciberseguridad y la continuidad del negocio, por lo que serán tratados con la severidad que corresponda según su impacto.

8. Revisión

Esta política será revisada y actualizada al menos una vez al año, o cuando se presenten cambios significativos en el entorno tecnológico, organizacional o normativo, o ante la detección de nuevas amenazas o vulnerabilidades que puedan afectar la seguridad de la información y la ciberseguridad.

La responsabilidad de su revisión y actualización recae en el responsable de Seguridad de la Información y Ciberseguridad, con la aprobación del Comité de Riesgos o de la alta dirección, según corresponda.

9. Marco normativo y de referencia

Esta política se fundamenta en el cumplimiento de la Ley 1581 de 2012 y sus decretos reglamentarios, los cuales establecen las disposiciones generales para la protección de los datos personales en Colombia.

Asimismo, se alinea con los principios, requisitos y controles definidos en la Norma Internacional ISO/IEC 27001, orientada al establecimiento, implementación, mantenimiento y mejora continua de la seguridad de la información en la organización.

Cualquier cambio en la legislación o actualización de las normas de referencia será considerado en las revisiones periódicas de esta política.

Publíquese y Cúmplase.

Firma Gerente General

Revisado 27 octubre de 2025