POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
SISTEMAS AVANZADOS EN TELECOMUNICACIONES S.A.S.
NIT: 900381389-8

Norma base: ISO/IEC 27001:2022
Responsable de cumplimiento: Dirección Técnica y Representante Legal

Esta política de seguridad de la información describe las medidas y lineamientos que se deben tener en consideración para gestionar los riesgos de seguridad de la información sobre los activos de información.

OBJETIVO

Esta política tiene como objetivo establecer las directrices para proteger los activos de información de SISTEMAS AVANZADOS EN TELECOMUNICACIONES S.A.S., garantizando su **confidencialidad, integridad y disponibilidad**, al tiempo que se da cumplimiento a la **normativa legal nacional (Ley 1581 de 2012, Ley 1341 de 2009, Ley 1273 de 2009, Ley 679 de 2001)** y estándares internacionales como **ISO 27001**.

ALCANCE

La política aplica a:

- Todos los **empleados**, **contratistas**, **terceros**, **clientes** y **usuarios** con acceso a la infraestructura o a los servicios gestionados por SISTEMAS AVANZADOS EN TELECOMUNICACIONES S.A.S.
- Todos los **activos de información**, incluyendo datos, redes, sistemas, bases de datos, dispositivos y comunicaciones.
- Las actividades técnicas y administrativas involucradas en la **prestación del servicio de telecomunicaciones**, tanto fijas como inalámbricas.

DEFINICIONES

- **Activos de información:** Todos los elementos que contienen o gestionan información: bases de datos, documentos, redes, servidores, routers, sistemas, etc.

- **Autenticación:** Proceso mediante el cual un sistema verifica la identidad de un usuario antes de permitir el acceso a un recurso (ej: usuario y contraseña)
- **Confidencialidad:** Propiedad que asegura que la información solo sea accesible por personal autorizado.
- **Disponibilidad:** Capacidad de los sistemas y servicios para estar operativos y accesibles cuando se necesiten.
- **Integridad:** Propiedad que garantiza que la información no ha sido alterada de forma no autorizada.
- **SGSI (Sistema de Gestión de Seguridad de la Información):** Conjunto de políticas, procesos y controles que permiten gestionar de forma sistemática la seguridad de la información según ISO/IEC 27001.
- **Incidente de Seguridad de la Información:** Cualquier evento que afecte o pueda afectar la confidencialidad, integridad o disponibilidad de la información (ej: virus, acceso no autorizado, pérdida de datos).
- **Evaluación de riesgos:** Proceso de identificación, análisis y valoración de amenazas y vulnerabilidades que pueden afectar la seguridad de la información.
- **Tratamiento de riesgos:** Acciones para mitigar, transferir, aceptar o evitar los riesgos detectados en la evaluación.
- **Controles de seguridad:** Medidas (técnicas, físicas o administrativas) que se aplican para reducir los riesgos a un nivel aceptable.
- **Clasificación de la información:** Proceso mediante el cual se asigna una categoría a la información según su sensibilidad (Ej: pública, interna, confidencial, crítica).
- **Firewall:** Dispositivo o software que controla el tráfico de red entre diferentes zonas de seguridad.
- **Backup (Copia de seguridad):** Proceso mediante el cual se guarda una copia de la información para poder restaurarla en caso de pérdida o daño.
- **Normatividad TIC aplicable:** Conjunto de leyes y resoluciones que regulan el tratamiento de datos, neutralidad en la red, filtrado de contenidos, protección de menores, etc. (Ej: Ley 1581 de 2012, Ley 1341 de 2009, Ley 679 de 2001).
- **Política de Seguridad de la Información:** Documento formal aprobado por la alta direcciónque define el compromiso, objetivos, principios y directrices de seguridad de la información en la organización.
- **Usuarios autorizados:** Personas a las que se les ha concedido acceso formal a sistemas, datos o dispositivos, conforme a su rol o función.

OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

1. Proteger la información de accesos no autorizados.
2. Evitar alteraciones indebidas o pérdida de datos.
3. Garantizar la disponibilidad del servicio incluso ante incidentes.
4. Asegurar el cumplimiento de la legislación TIC y la protección de datos personales.
5. Gestionar los riesgos de ciberseguridad de forma proactiva.

PRINCIPIOS FUNDAMENTALES

- **Confidencialidad:** Solo el personal autorizado puede acceder a la información.
- **Integridad:** La información no debe ser modificada de manera accidental o maliciosa.
- **Disponibilidad:** Los datos y sistemas deben estar disponibles cuando se necesiten.
- **Transparencia:** Los usuarios deben conocer las políticas y prácticas aplicadas.
- **Legalidad:** Toda acción debe enmarcarse en la legislación vigente.
- **Mejora continua:** Se revisarán y ajustarán los controles periódicamente.

GESTIÓN DE RIESGOS

- SISTEMAS AVANZADOS EN TELECOMUNICACIONES S.A.S. adopta un enfoque basado en **evaluación y tratamiento de riesgos**, conforme a la metodología de ISO 27005.
- Se identifican vulnerabilidades y amenazas en procesos, tecnologías y personas.
- Se aplican controles preventivos, detectivos y correctivos según el nivel de criticidad.

Controles típicos aplicados:

Categoría	Control
Técnico	Firewalls, antivirus, backups, cambio de contraseñas de manera de periódica
Físico	Cámaras.
Administrativo	Cláusulas contractuales, roles definidos.

CLASIFICACIÓN DE LA INFORMACIÓN

Toda la información manejada por SISTEMAS AVANZADOS EN TELECOMUNICACIONES S.A.S. se clasifica en:

- **Pública:** Información institucional sin restricciones.
- **Interna:** Uso exclusivo del personal de la empresa.
- **Confidencial:** Datos de clientes, configuraciones de red, accesos, etc.
- **Crítica:** Infraestructura técnica, direcciones IP públicas, datos de seguridad.

Cada tipo de información tendrá **niveles de protección distintos**, según su sensibilidad.

GESTIÓN DE INCIDENTES

SISTEMAS AVANZADOS EN TELECOMUNICACIONES S.A.S. contará con un **procedimiento de gestión de incidentes**, que incluye:

- Escalamiento automático según criticidad.
- Contención, análisis forense y recuperación.
- Notificación a las autoridades cuando corresponda.

Se contemplan incidentes como:

- Accesos no autorizados.
- Interrupciones de servicio.
- Malware.
- Fugas de información.

RESPONSABILIDADES

- **Alta dirección:** Aprobar y promover esta política.
- **Dirección técnica:** Aplicar los controles, liderar el SGSI y atender auditorías.
- **Todos los usuarios:** Cumplir con las normas internas y reportar anomalías.

COMPROMISO LEGAL

SAT S.A.S garantiza el cumplimiento de:

- **Ley 1581 de 2012:** Protección de datos personales.
- **Ley 1341 de 2009:** Neutralidad en la red y deberes del operador.
- **Ley 679 de 2001:** Protección de menores frente a contenido ilegal.
- **Ley 1273 de 2009:** Delitos informáticos.
- **Resoluciones y requerimientos MINTIC.**

REVISIÓN Y VIGENCIA

Esta política se revisará anualmente o cuando:

- Se presente un incidente de seguridad grave.
- Cambie la legislación TIC.
- Existan auditorías con hallazgos relevantes.

Aprobado por

Edwin Alexander Gómez Ortega
Representante Legal
SISTEMAS AVANZADOS EN TELECOMUNICACIONES S.A.S.
NIT 900381389-8