Política de Seguridad Informática

SERVISYSTEN S.A.S. | NIT 901.196.026-0 | Registro TIC 96004327

Calle 6 #7-65, barrio Páez, La Plata, Huila

Fecha de entrada en vigor: 1 de enero de 2026

Política propuesta para aprobación: antes de publicarla oficialmente, SERVISYSTEN debe confirmar que los controles y procesos descritos están implementados y asignar responsables internos.

1. Propósito y alcance

Establecer principios generales de protección de la infraestructura de telecomunicaciones, los sistemas administrativos y la información utilizada por SERVISYSTEN S.A.S. Se dirige al personal, contratistas y terceros autorizados que intervengan en los sistemas de la organización.

2. Principios de seguridad

Aplicación de controles proporcionales para preservar la confidencialidad, integridad y disponibilidad de la información; mínimo privilegio en accesos; gestión responsable de activos; actualización de equipos; trazabilidad de cambios; y tratamiento adecuado de incidentes.

3. Control de accesos y credenciales

Los accesos a plataformas, routers, concentradores y sistemas internos deberán estar asignados según funciones autorizadas. Se deberán aplicar contraseñas robustas, revocación de permisos al finalizar vínculos y mecanismos adicionales de autenticación cuando estén disponibles. Se prohíbe compartir credenciales.

4. Gestión de infraestructura y redes

La empresa definirá medidas técnicas acordes con sus riesgos: segmentación de redes, configuración segura, copia y respaldo de configuraciones, actualizaciones controladas, monitoreo, protección frente a accesos no autorizados y evaluación de tráfico anómalo.

Las medidas específicas que se implementen deberán estar documentadas y verificadas por el equipo técnico; esta política no certifica por sí sola la existencia de tecnologías concretas ni garantiza la eliminación total de ataques.

5. Tratamiento de incidentes

Ante un incidente se deberán activar los procesos internos para identificar, contener, analizar, recuperar y documentar la situación. Cuando corresponda, se realizarán las notificaciones a titulares o autoridades dentro del marco legal aplicable. Se conservarán evidencias pertinentes de forma segura.

6. Protección de datos y confidencialidad

La seguridad informática se articula con la Política de Tratamiento de Datos Personales de SERVISYSTEN. El personal debe acceder únicamente a la información necesaria para sus funciones, mantener reserva y utilizar

canales autorizados para transferir datos.

7. Proveedores y terceros

Los proveedores con acceso a sistemas deberán cumplir controles de seguridad acordes con el acceso concedido, así como compromisos de confidencialidad y devolución o eliminación segura de información cuando aplique.

8. Responsabilidades, revisión y canales

La administración de SERVISYSTEN debe definir responsables, evidencias de implementación y periodicidad de revisión de esta política. Los incidentes o consultas pueden reportarse a contactenos@servisysten.com o al 310 864 1960.