MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

CONECTIC TELECOMUNICACIONES S.A.S.

1. Objetivo

Establecer los lineamientos, controles y responsabilidades para proteger la confidencialidad, integridad y disponibilidad de la información administrada por Conectic Telecomunicaciones S.A.S., garantizando el cumplimiento de la normatividad vigente, en especial la Resolución CRC 5050 de 2016 y sus modificaciones.

2. Alcance

El presente Sistema de Gestión de Seguridad de la Información aplica a todos los procesos, empleados, contratistas, proveedores, sistemas de información, equipos tecnológicos, redes de comunicaciones y activos de información utilizados por Conectic Telecomunicaciones S.A.S. para la prestación de sus servicios.

3. Marco normativo

- Resolución CRC 5050 de 2016.
- Resolución CRC 5569 de 2018.
- Anexo 5.8 de la CRC.
- Ley 1581 de 2012 (Protección de Datos Personales).
- Demás normas aplicables en materia de seguridad de la información y telecomunicaciones.

4. Política de seguridad de la información

Conectic Telecomunicaciones S.A.S. se compromete a proteger la información de sus clientes, usuarios, colaboradores y demás partes interesadas mediante la implementación de controles administrativos, técnicos y físicos orientados a prevenir accesos no autorizados, pérdidas, alteraciones, destrucción o divulgación indebida de la información.

La organización promoverá una cultura de seguridad basada en la gestión de riesgos, la mejora continua, la concientización del personal y el cumplimiento de los requisitos legales, regulatorios y contractuales aplicables.

Conectic Telecomunicaciones S.A.S. garantiza la disponibilidad, integridad y confidencialidad de sus servicios de telecomunicaciones mediante las siguientes acciones:

- Implementación de controles de acceso lógico y físico a la infraestructura tecnológica, incluyendo routers, switches, OLT, servidores, sistemas de gestión, redes VPN, credenciales de acceso, puertos de comunicación y direccionamiento IP privado.
- Aplicación del principio de mínimo privilegio para la asignación de permisos y accesos a sistemas críticos.
- Monitoreo continuo de la infraestructura tecnológica y de telecomunicaciones las 24 horas del día, los 7 días de la semana (24/7), a través del Centro de Operaciones de Red (NOC), permitiendo la detección temprana y atención oportuna de incidentes.
- Ejecución de actividades de mantenimiento preventivo, correctivo y de mejora continua sobre la infraestructura tecnológica y de red.
- Actualización periódica de firmware, sistemas operativos y plataformas tecnológicas para corregir vulnerabilidades y mantener niveles adecuados de seguridad.
- Implementación de prácticas de ingeniería y redundancia en el backbone de la red para garantizar la continuidad operativa, resiliencia y tolerancia ante fallas.
- Gestión y evaluación permanente de riesgos de seguridad de la información que puedan afectar los activos tecnológicos y la prestación de los servicios.
- Protección de la red mediante mecanismos de filtrado, detección y mitigación de ataques de denegación de servicio distribuido (DoS), malware, accesos no autorizados y demás amenazas cibernéticas.
- Implementación de procedimientos para la gestión, reporte, análisis y tratamiento de incidentes de seguridad de la información.
- Realización de copias de seguridad de la información crítica y verificación periódica de los procedimientos de recuperación.

- Protección de los datos personales de clientes, empleados, proveedores y demás titulares de información, en cumplimiento de la normativa vigente sobre protección de datos personales.
- Capacitación y sensibilización periódica del personal en temas de seguridad de la información, ciberseguridad y buenas prácticas operativas.
- Cumplimiento de las obligaciones regulatorias, técnicas y de seguridad establecidas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), la Comisión de Regulación de Comunicaciones (CRC) y demás autoridades competentes.
- Revisión periódica de esta política para asegurar su vigencia, eficacia y alineación con los objetivos estratégicos de la organización.

Todos los colaboradores, contratistas y terceros que tengan acceso a los activos de información de Conectic Telecomunicaciones S.A.S. deberán cumplir las disposiciones establecidas en esta política y reportar cualquier situación que pueda comprometer la seguridad de la información o la continuidad de los servicios.

5. **Análisis de riesgo**

Nombre	Tipo	Valor	Observación
Routers y switches	Hardware	Alto	Equipos esenciales para el enrutamiento, conmutación y transporte del tráfico de datos de la red.
OLT	Hardware	Alto	Equipos críticos para la provisión de servicios FTTH y la conexión de los clientes a la red.
Servidores	Hardware	Alto	Soportan servicios de autenticación, monitoreo, aprovisionamiento, gestión de usuarios y aplicaciones corporativas.
NOC	Instalación	Alto	Instalación destinada al monitoreo, supervisión y gestión de la infraestructura y los servicios de telecomunicaciones.
Personal técnico	Humano	Alto	Responsable de la operación, mantenimiento, soporte y atención de incidentes de la red.

Sistema de facturación y gestión de clientes	Software	Alto	Gestiona la información comercial, contratos, facturación y cartera de clientes.
Enlaces de Internet y backbone	Servicio	Alto	Garantizan la conectividad y disponibilidad de los servicios ofrecidos a los clientes.
Sistema eléctrico, UPS y respaldo energético	Infraestructura	Alto	Mantiene la continuidad operativa de los equipos y servicios ante fallas de energía.

6. Matriz de riesgo

Activo	Amenaza	Probabilidad	Impacto	Riesgo	Control
Rourters	Ataques DoS, accesos no autorizados, explotación de vulnerabilidades	Alta	Alto	Critico	Firewall perimetral, listas de control de acceso (ACL), gestión segura de credenciales, VPN, monitoreo continuo y respaldos de configuración.
Servidor Radius DMA	Interrupción del servicio, accesos no autorizados, fallas de configuración o interferencia	Media	Alto	Alto	Autenticación de usuarios, monitoreo permanente y respaldos de configuración.
Servidor U2000	Ransomware, secuestro de cuentas, malware y explotación de vulnerabilidades	Media	Alto	Alto	Firewall, VPN, copias de seguridad y control de accesos.
OLT	Acceso no autorizado,	Alta	Alto	Alto	VPN, control de privilegios, monitoreo

	alteración de configuraciones y afectación de los servicios				continuo y respaldos de configuración.
Red de Fibra Óptica	Corte accidental o intencional de fibra, daños físicos o vandalismo	Alta	Alto	Critico	Redundancia de enlaces, rutas alternas, monitoreo de la red y mantenimiento preventivo.
DNS	Ataques DoS, envenenamiento de caché, accesos no autorizados y fallas del servicio	Medio	Alto	Alto	ACL, monitoreo de tráfico y restricciones de acceso.
Usuarios finales	Malware, phishing, robo de credenciales e ingeniería social	Alta	Medio	Alto	Filtrado DNS, firewall, políticas de seguridad y mantener informado a los usuarios de los riesgos en la red.
Sistema de monitoreo y gestión de red	Acceso no autorizado, indisponibilidad o manipulación de registros	Medio	Alto	Alto	Control de acceso, VPN, y monitoreo de eventos.
Sistema de facturación y gestión de clientes	Fuga de información, acceso no autorizado o corrupción de datos	Medio	Alto	Alto	Control de acceso y copias de seguridad.
Información de clientes	Divulgación no autorizada, pérdida o alteración de datos	Media	Alto	Alto	Políticas de protección de datos, control de acceso, respaldos y cifrado de información sensible.
Cabecera de	Acceso físico no autorizado,	Baja	Alto	Medio	Control de acceso físico, videovigilancia, monitoreo ambiental y

telecomunicaciones	interrupción operativa o fallas de infraestructura				procedimientos de continuidad operativa.
Personal técnico	Error humano, uso indebido de privilegios o fuga de información	Media	Alto	Alto	Capacitación periódica, segregación de funciones, políticas de seguridad y acuerdos de confidencialidad.

Escala sugerida para futuras evaluaciones:

- **Probabilidad:** Baja, Media, Alta.
- **Impacto:** Bajo, Medio, Alto.
- **Nivel de Riesgo:** Bajo, Medio, Alto, Crítico.

7. Principios de seguridad

- Confidencialidad.
- Integridad.
- Disponibilidad.
- Autenticidad.
- Trazabilidad.

8. Roles y responsabilidades

Gerencia

- Aprobar la política de seguridad.
- Proveer recursos para el SGSI.
- Revisar periódicamente el desempeño del sistema.

Responsable de Tecnología

- Implementar los controles de seguridad.
- Gestionar incidentes de seguridad.
- Mantener actualizados los registros.

Colaboradores

- Cumplir las políticas y procedimientos establecidos.
- Reportar incidentes o eventos de seguridad.

9. Gestión de activos de información

La empresa mantendrá un inventario actualizado de los activos de información, incluyendo:

- Equipos de cómputo.
- Servidores.
- Equipos de red.
- Aplicaciones.
- Bases de datos.
- Documentación física y digital.

Cada activo deberá tener un responsable designado.

10. Gestión de riesgos

Conectic Telecomunicaciones S.A.S. identificará, evaluará y tratará periódicamente los riesgos que puedan afectar la seguridad de la información.

Los riesgos serán clasificados según su probabilidad e impacto, definiendo controles apropiados para su mitigación.

11. Gestión de incidentes

Incidente	Controles / Mitigación
Caída de OLT	Restauración desde respaldos de configuración, redundancia y monitoreo del equipo.
Saturación de CPU	Balanceo de carga, optimización de recursos y monitoreo de rendimiento.
Corte de fibra	Redundancia mediante bonding o rutas alternas, monitoreo de enlaces y planes de contingencia.

Ataques DoS	Protección mediante firewall, filtrado de tráfico y sistemas de mitigación.
Problemas de energía	Uso de UPS, fuentes de poder redundantes y sistemas de energía regulada.
Detección del incidente	Sistemas de monitoreo, alarmas y alertas automáticas del NOC.
Respuestas	Atención por ingenieros y técnicos especializados según el tipo de incidente.
Responsables	Ingenieros de red y personal técnico del área de telecomunicaciones.

12. Control de accesos

- Cada usuario contará con credenciales individuales.
- Se aplicará el principio de mínimo privilegio.
- Los accesos serán retirados cuando finalice la relación laboral o contractual.
- Las contraseñas deberán cumplir criterios mínimos de complejidad.

❖ Registro

Todo incidente deberá registrarse indicando:

- Fecha y hora.
- Descripción.
- Responsable.
- Impacto.
- Acciones ejecutadas.

❖ Tratamiento

Los incidentes serán analizados, contenidos, corregidos y documentados.

❖ Reporte

Los incidentes relevantes serán reportados a la Gerencia y, cuando aplique, a las autoridades competentes.

13. Copias de seguridad

Se realizarán respaldos periódicos de la información crítica de la organización.

Las copias deberán almacenarse en medios seguros y verificarse periódicamente para garantizar su recuperación.

14. Continuidad del negocio

La organización establecerá medidas para garantizar la continuidad de los servicios ante eventos que afecten la operación normal.

Se contemplarán procedimientos de recuperación de información y restablecimiento de servicios críticos.

15. Capacitación y concientización

Todos los colaboradores recibirán capacitación periódica sobre:

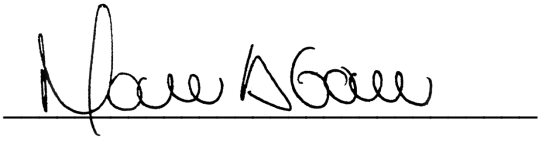
- Seguridad de la información.
- Protección de datos.
- Gestión de incidentes.
- Buenas prácticas de seguridad.

16. Auditoría y mejora continua

La organización realizará revisiones periódicas del SGSI para verificar su eficacia y establecer acciones de mejora cuando sea necesario.

17. Aprobación

El presente documento entra en vigencia a partir de su aprobación por la Gerencia de Conectic Telecomunicaciones S.A.S. y será revisado al menos una vez al año o cuando se presenten cambios significativos en la organización o en la normatividad aplicable.



Gerencia Conectic Telecomunicaciones S.A.S.