GRAFENO COMUNICACIONES S.A.S.

NIT 901.048.229-5 | Registro TIC 96005786

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Sistema de gestión de seguridad de la información para proteger la confidencialidad, integridad y disponibilidad de los activos de información de la empresa.

Código del documento:	PO-SEG-001
Versión:	1.0
Fecha de emisión:	08 de mayo de 2026
Ciudad:	Villa de Leyva — Boyacá

Conforme a: ISO/IEC 27001:2022, Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC y Ley 1581 de 2012

1. CONTROL DEL DOCUMENTO

Versión	Fecha	Elaboró / Aprobó	Descripción del cambio
1.0	08 de mayo de 2026	Área Administrativa / Representante Legal	Versión inicial.

2. DECLARACIÓN DE LA ALTA DIRECCIÓN

La Representación Legal de GRAFENO COMUNICACIONES S.A.S. (en adelante, GRAFENO) declara su compromiso con la protección de la información propia, de sus suscriptores, empleados, proveedores y terceros, garantizando la confidencialidad, integridad y disponibilidad de los activos de información, así como el cumplimiento de las obligaciones legales, regulatorias y contractuales que le aplican como Proveedor de Redes y Servicios de Telecomunicaciones (PRST) inscrito en el Registro TIC con número 96005786.

3. OBJETIVO

Establecer los principios, lineamientos y controles que rigen la gestión de la seguridad de la información en GRAFENO, alineados con la norma ISO/IEC 27001, el Modelo de Seguridad y Privacidad de la Información (MSPI) promovido por el MinTIC, la Ley 1581 de 2012 y demás normatividad aplicable.

4. ALCANCE

Esta política aplica a toda la información que GRAFENO genera, recibe, almacena, transmite o procesa en cualquier medio (físico o digital), a su infraestructura de red y sistemas de información (WiMAX y fibra óptica), a todo el personal vinculado mediante contrato laboral, de prestación de servicios u otra modalidad, y a los terceros (proveedores, contratistas, aliados) que tengan acceso a información o sistemas de la empresa.

5. MARCO NORMATIVO Y DE REFERENCIA

- Constitución Política de Colombia, artículo 15.
- Ley 1273 de 2009 — Delitos informáticos.
- Ley 1341 de 2009 — Marco general TIC.
- Ley 1581 de 2012 y Decretos 1377 de 2013 y 1074 de 2015 — Protección de datos personales.
- Ley 679 de 2001, Decreto 1524 de 2002 y Ley 1336 de 2009 — Protección de NNA frente a contenidos en redes globales.
- Resolución CRC 5050 de 2016 (régimen unificado) y demás resoluciones de la CRC sobre régimen de protección al usuario y obligaciones técnicas de los PRST.
- Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC.
- Norma ISO/IEC 27001:2022 — Sistema de Gestión de Seguridad de la Información (referencia).
- Norma ISO/IEC 27002:2022 — Buenas prácticas de controles.

6. PRINCIPIOS DE SEGURIDAD

Principio	Descripción
Confidencialidad	Sólo accede a la información quien está autorizado.
Integridad	La información se mantiene exacta y completa, libre de modificaciones no autorizadas.
Disponibilidad	La información y los servicios están accesibles cuando son requeridos por usuarios autorizados.

Legalidad	Todo tratamiento se ajusta a la normativa aplicable.
Responsabilidad demostrada	GRAFENO puede demostrar el cumplimiento de los controles ante autoridades.
Mejora continua	La seguridad se gestiona bajo el ciclo Planear–Hacer–Verificar–Actuar.

7. ESTRUCTURA ORGANIZACIONAL DE LA SEGURIDAD

Rol	Responsabilidades
Representación Legal	Aprobar la política, asignar recursos, asumir la responsabilidad última en seguridad.
Comité de Seguridad de la Información	Revisar trimestralmente el estado de la seguridad, aprobar el tratamiento de riesgos y los planes de remediación.
Oficial de Seguridad de la Información (OSI)	Coordinar el sistema de gestión, gestionar riesgos e incidentes, mantener los indicadores.
Responsable de Datos Personales	Articular la política con la Política de Datos Personales y atender la relación con la SIC.
Líder Técnico / NOC	Operar y monitorear los controles técnicos en la infraestructura WiMAX y fibra óptica.
Talento Humano / Administrativa	Verificar antecedentes, gestionar acuerdos de confidencialidad, ejecutar el plan de capacitación.
Todos los colaboradores y terceros	Cumplir la política, reportar incidentes y proteger los activos asignados.

8. GESTIÓN DE ACTIVOS DE INFORMACIÓN

GRAFENO mantiene un inventario actualizado de activos de información (datos, software, hardware, servicios e instalaciones, incluyendo los radioenlaces propios y enlaces de fibra contratados con aliados), con su responsable, clasificación y nivel de criticidad. Los activos se clasifican en: Pública, Interna, Confidencial y Restringida. La clasificación determina los controles de manejo, almacenamiento, transmisión y destrucción aplicables.

9. CONTROL DE ACCESOS

9.1 Acceso lógico

- Cada usuario cuenta con un identificador único e intransferible.
- Se aplica el principio de mínimo privilegio y necesidad de conocer.
- Las contraseñas tienen una longitud mínima de 12 caracteres, combinando mayúsculas, minúsculas, números y símbolos, con vigencia máxima de 90 días.
- Se exige doble factor de autenticación (MFA) para el acceso a sistemas críticos: facturación, base de datos de suscriptores, gestión de red, herramientas de bloqueo Ley 679 y administración del sitio web.
- Las cuentas inactivas durante 60 días se deshabilitan automáticamente.
- Se realiza revisión semestral de privilegios.

9.2 Acceso físico

- Las áreas con servidores y equipos de red operan con acceso restringido por tarjeta o llave, bitácora de ingreso y videovigilancia.
- Los visitantes son acompañados en todo momento por personal autorizado.

10. SEGURIDAD EN LAS OPERACIONES

- Antivirus / EDR actualizado en estaciones de trabajo y servidores con políticas centralizadas.
- Gestión de parches: parches críticos aplicados dentro de 30 días desde su publicación; parches de seguridad altos en 60 días.
- Segmentación de red: separación lógica entre la red de gestión, la red corporativa y la red de clientes.
- Hardening de routers, switches y servidores conforme a guías CIS Benchmark.
- Sincronización horaria mediante NTP confiable para todos los equipos.
- Registros (logs) de seguridad centralizados, con retención mínima de seis (6) meses, sin perjuicio de los términos mayores que disponga la regulación CRC o las autoridades competentes para fines probatorios.

11. SEGURIDAD EN LAS COMUNICACIONES

- Las comunicaciones administrativas remotas se realizan exclusivamente por canales cifrados (SSH, HTTPS, VPN con cifrado AES-256).
- Se prohíbe el uso de protocolos en texto plano (Telnet, FTP, HTTP) para administración de equipos.
- Las VPN de acceso remoto requieren MFA.
- Las comunicaciones con autoridades (MinTIC, SIC, Fiscalía, Dijín) se realizan por canales oficiales y se conservan los acuses de recibo.

12. CRIPTOGRAFÍA Y PROTECCIÓN DE DATOS EN REPOSO

Las bases de datos que contienen datos personales y la información clasificada como Confidencial o Restringida se almacenan cifradas (AES-256). Las llaves criptográficas se gestionan en un repositorio de secretos con acceso registrado y rotación al menos anual o ante incidentes.

13. COPIAS DE RESPALDO

Sistema	Frecuencia	Retención	Tipo
Base de datos de suscriptores y facturación	Diaria	30 días en línea / 1 año en frío	Incremental + completa semanal
Configuración de equipos de red (radioenlaces, routers, switches)	Tras cada cambio y semanal	12 versiones	Completa
Sitio web y CMS	Semanal	8 semanas	Completa
Logs y evidencias de bloqueo Ley 679	Diaria	Mínimo 5 años	Cifrada y replicada

Se ejecutan pruebas de restauración trimestrales documentadas en el formato FR-SEG-002. Las copias se almacenan en sitio diferente al principal y permanecen cifradas.

14. GESTIÓN DE INCIDENTES DE SEGURIDAD

GRAFENO define el siguiente flujo para la gestión de incidentes de seguridad de la información:

1. **Detección y reporte:** cualquier colaborador o tercero que identifique un evento sospechoso lo reporta al correo grafenocomunicaciones@gmail.com o a la mesa de servicio dentro de la primera hora siguiente.
2. **Clasificación:** el OSI clasifica el incidente como bajo, medio, alto o crítico, según impacto en confidencialidad, integridad y disponibilidad.
3. **Contención:** se aíslan los sistemas afectados, se revocan accesos comprometidos y se preservan evidencias forenses.

4. **Erradicación y recuperación:** se elimina la causa raíz y se restauran los servicios desde copias verificadas.
5. **Notificación:** cuando el incidente involucre datos personales, se reporta a la SIC dentro de los 15 días hábiles siguientes a su detección, a través del Registro Nacional de Bases de Datos. Cuando comprometa la prestación del servicio, se atiende lo dispuesto por la CRC.
6. **Lecciones aprendidas:** se documenta el análisis post-incidente y se actualizan los controles.

15. CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN

GRAFENO mantiene un Plan de Continuidad del Negocio (BCP) y un Plan de Recuperación ante Desastres (DRP) para los procesos críticos: prestación del servicio de Internet (WiMAX y fibra), atención de PQR, facturación y bloqueo Ley 679. Los objetivos definidos son:

Indicador	Definición	Objetivo
RTO	Tiempo objetivo de recuperación	≤ 4 horas para servicios críticos
RPO	Punto objetivo de recuperación (pérdida máxima de datos)	≤ 24 horas

El BCP y el DRP se prueban como mínimo una vez al año, con simulacros documentados.

16. SEGURIDAD EN RECURSOS HUMANOS

- Verificación de antecedentes y referencias antes de la contratación.
- Firma obligatoria de acuerdo de confidencialidad y aceptación de las políticas de seguridad y de datos personales.
- Inducción dentro de los 15 días siguientes al ingreso, con cobertura de Ley 1581, Ley 679, uso aceptable de recursos y manejo de incidentes.
- Capacitación anual obligatoria, con prueba de evaluación y registro de asistencia.
- Procedimiento de retiro: revocación de accesos en menos de 24 horas, devolución de activos y firma del acta de paz y salvo de información.

17. SEGURIDAD EN LA RELACIÓN CON PROVEEDORES

Los contratos con proveedores que accedan a información o sistemas de GRAFENO (incluyendo aliados de fibra óptica) incluyen cláusulas de confidencialidad, niveles de servicio (SLA) en seguridad, derecho de auditoría, obligación de reportar incidentes en menos de 24 horas y devolución o destrucción certificada de información al término del contrato. Se realiza evaluación de seguridad antes de la contratación y revaluación anual para proveedores críticos.

18. USO ACEPTABLE DE RECURSOS

- Está prohibido instalar software no autorizado en equipos de la empresa.
- Está prohibido conectar dispositivos externos no aprobados a las redes de gestión.
- Está prohibido compartir credenciales o dejar sesiones abiertas sin bloqueo de pantalla.
- Está prohibido el uso de los recursos de GRAFENO para acceder, almacenar o distribuir contenido ilegal, en particular el material señalado por la Ley 679 de 2001. La detección de cualquier actividad de este tipo se reporta inmediatamente al Oficial de Cumplimiento Ley 679 y a las autoridades competentes.
- El correo electrónico corporativo se utiliza exclusivamente para fines laborales.

19. ARTICULACIÓN CON LA PROTECCIÓN DE NNA (LEY 679 DE 2001)

Los controles de esta política soportan la operación del Procedimiento de Bloqueo de URL (PR-VCM-001), garantizando la integridad de los listados oficiales recibidos de MinTIC y la Dijín, la disponibilidad de los servicios de filtrado y la confidencialidad de las evidencias de bloqueo, las cuales se conservan por un mínimo de cinco (5) años.

20. GESTIÓN DEL RIESGO

GRAFENO realiza, al menos una vez al año, un análisis formal de riesgos de seguridad de la información, identificando activos, amenazas, vulnerabilidades, probabilidad e impacto. El tratamiento del riesgo se ejecuta mediante mitigación, transferencia, aceptación o evitación, según corresponda. Los riesgos residuales son aprobados por la Representación Legal y monitoreados trimestralmente por el Comité de Seguridad.

21. AUDITORÍA INTERNA Y CUMPLIMIENTO

Anualmente se ejecuta una auditoría interna al sistema de gestión de seguridad de la información. Los hallazgos se documentan, se asignan responsables y se monitorean hasta su cierre. La política se revisa al menos una vez al año o ante cambios normativos sustanciales, incidentes mayores o modificaciones organizacionales.

22. INDICADORES DE SEGURIDAD

Indicador	Meta	Frecuencia
Disponibilidad de la red	≥ 99,5 %	Mensual
Tiempo de detección de incidentes (MTTD)	≤ 4 horas	Mensual
Tiempo de resolución de incidentes críticos (MTTR)	≤ 8 horas	Mensual
Cobertura de capacitación anual	≥ 95 % del personal	Anual
Pruebas de restauración exitosas	100 %	Trimestral
Cumplimiento del plan de parches	≥ 95 %	Mensual

23. INCUMPLIMIENTOS Y SANCIONES

El incumplimiento de esta política por parte de un colaborador será considerado falta grave y dará lugar a las medidas disciplinarias previstas en el Reglamento Interno de Trabajo, sin perjuicio de las acciones civiles, penales o administrativas a que haya lugar, particularmente las contempladas en la Ley 1273 de 2009, la Ley 1581 de 2012 y la Ley 679 de 2001.

24. VIGENCIA

Esta política rige desde el 08 de mayo de 2026 y permanecerá vigente hasta su reemplazo por una versión posterior. Las modificaciones serán comunicadas a todo el personal y publicadas en los canales internos.

APROBACIÓN

María Marcela Duarte Pérez	**Oficial de Seguridad de la Información (OSI)**
Representante Legal	GRAFENO COMUNICACIONES S.A.S.

GRAFENO COMUNICACIONES S.A.S.