GRAFENO COMUNICACIONES S.A.S.

NIT 901.048.229-5 | Registro TIC 96005786

SEGURIDAD DE LA RED Y CONTROLES PARENTALES

Documento técnico-informativo sobre las medidas de seguridad de la red, protección a NNA y herramientas de control parental disponibles para los usuarios.

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

Conforme a: Resolución CRC 5050 de 2016, Ley 679 de 2001, Decreto 1524 de 2002, Ley 1336 de 2009 y Ley 1581 de 2012

1. PRESENTACIÓN

GRAFENO COMUNICACIONES S.A.S. (en adelante, GRAFENO), Proveedor de Redes y Servicios de Telecomunicaciones (PRST) inscrito en el Registro TIC con número 96005786, presenta este documento técnico e informativo en cumplimiento de lo establecido en la Resolución CRC 5050 de 2016 y demás normas que la modifican, complementan o adicionan, en particular las Resoluciones CRC 5111 de 2017, CRC 7811 de 2025 y CRC 8171 de 2026.

Este documento expone las acciones, controles y mecanismos que GRAFENO ha adoptado para: (i) garantizar la seguridad de la red de transporte (radioenlaces WiMAX propios y enlaces de fibra con aliados) y de los servicios de acceso a Internet; (ii) proteger a las niñas, niños y adolescentes (NNA) frente a contenidos inapropiados o ilícitos; y (iii) ofrecer al usuario información clara sobre las herramientas de control parental disponibles, así como las medidas de autoprotección que puede aplicar en sus equipos terminales.

2. IDENTIFICACIÓN DEL PROVEEDOR

Campo	Información
Razón social	GRAFENO COMUNICACIONES S.A.S.
NIT	901.048.229-5
Registro TIC (RUTIC)	96005786
Representante legal	María Marcela Duarte Pérez
Domicilio	Villa de Leyva — Boyacá
Servicio al cliente	+57 313 432 2994
Correo electrónico	grafenocomunicaciones@gmail.com
Sitio web	https://grafenocomunicaciones.com
Tecnología	WiMAX (radioenlaces propios) + Fibra óptica (con aliados)
Área responsable	Administrativa

3. MARCO NORMATIVO APLICABLE

- Constitución Política de Colombia, artículos 15, 20 y 44.
- Ley 679 de 2001 — Estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores de edad.
- Decreto 1524 de 2002 — Reglamenta el artículo 5 de la Ley 679 de 2001 (deberes de los ISP).
- Ley 1098 de 2006 — Código de la Infancia y la Adolescencia.
- Ley 1336 de 2009 — Robustece la lucha contra la explotación, pornografía y turismo sexual con NNA.
- Ley 1273 de 2009 — De la protección de la información y de los datos (delitos informáticos).
- Ley 1341 de 2009 — Marco general del sector TIC.
- Ley 1581 de 2012 y Decretos 1377 de 2013 y 1074 de 2015 — Protección de datos personales.
- Resolución CRC 5050 de 2016 — Resolución compilatoria de la CRC.
- Resolución CRC 5111 de 2017 — Régimen de Protección de los Derechos de los Usuarios de Servicios de Comunicaciones (RPU).

- Resolución CRC 7811 de 2025 y Resolución CRC 8171 de 2026 — Modificaciones al RPU vigentes desde el 1 de enero de 2026.

4. DEFINICIONES

Término	Definición
Control parental	Conjunto de herramientas y mecanismos que permiten a padres, madres o representantes legales restringir, supervisar o filtrar el acceso de NNA a contenidos en Internet.
Filtro de contenido	Solución técnica que bloquea el acceso a sitios o categorías de contenidos previamente definidos.
URL	Localizador uniforme de recursos. Identifica una página o recurso en Internet.
DNS	Sistema de nombres de dominio que traduce nombres a direcciones IP.
Phishing	Técnica fraudulenta para obtener información personal o financiera mediante suplantación de identidad.
Malware	Programa malicioso diseñado para dañar, robar o controlar dispositivos.
MFA	Autenticación multifactor; mecanismo de seguridad que combina dos o más factores de verificación.
DDoS	Ataque distribuido de denegación de servicio, que busca saturar la red o un servicio para hacerlo inaccesible.
NNA	Niñas, niños y adolescentes (toda persona menor de 18 años).

5. MEDIDAS DE SEGURIDAD ADOPTADAS POR GRAFENO

GRAFENO ha implementado un conjunto integral de medidas técnicas, administrativas y humanas para proteger la red, los servicios y la información de sus suscriptores, alineado con la Política de Seguridad de la Información (PO-SEG-001) y el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC.

5.1 Controles de acceso

- Autenticación multifactor (MFA) obligatoria para el acceso a sistemas críticos: gestión de la red, plataforma de facturación, base de datos de suscriptores y herramientas de bloqueo Ley 679.
- Cuentas individuales por usuario, principio de mínimo privilegio y revisión semestral de privilegios.
- Contraseñas con longitud mínima de 12 caracteres, complejidad mixta y vigencia máxima de 90 días.
- Acceso físico restringido a las áreas de equipos de red mediante control por tarjeta o llave, bitácora y videovigilancia.

5.2 Protección perimetral

- Firewalls de nueva generación en los puntos de borde, con reglas restrictivas por defecto.
- Sistemas de detección y prevención de intrusiones (IDS/IPS) con firmas actualizadas.
- Mitigación de ataques DDoS mediante filtrado en el operador de tránsito y políticas de rate-limiting en los equipos de borde.
- Segmentación lógica de red entre la red de gestión, la red corporativa y la red de clientes.

5.3 Cifrado y comunicaciones seguras

- Toda administración remota se realiza únicamente sobre canales cifrados (SSH, HTTPS, VPN AES-256).
- Se prohíben los protocolos en texto plano (Telnet, FTP, HTTP) para administración.

- Las bases de datos con información personal se almacenan cifradas en reposo (AES-256).
- Se promueve el uso de TLS/SSL para los servicios web y las aplicaciones expuestas a usuarios.

5.4 Protección del core de red

El core de red, encargado de gestionar el tráfico y las conexiones de los radioenlaces WiMAX y enlaces de fibra óptica, cuenta con redundancia y alta disponibilidad para garantizar continuidad ante fallas. El acceso al core está restringido a personal autorizado y capacitado, con controles físicos y lógicos. El monitoreo es continuo (24/7) mediante NOC propio o tercerizado, con alertas tempranas, registros sincronizados por NTP y conservación de logs por mínimo seis (6) meses.

5.5 Gestión de vulnerabilidades y parches

- Escaneos periódicos de vulnerabilidades en infraestructura interna y externa.
- Aplicación de parches críticos dentro de 30 días desde su publicación; parches altos en 60 días.
- Pruebas de penetración (pentest) con periodicidad anual o ante cambios significativos.

5.6 Gestión de incidentes

GRAFENO cuenta con un procedimiento documentado de gestión de incidentes, descrito en la Política de Seguridad de la Información, con flujo de detección, contención, erradicación, recuperación y lecciones aprendidas. Cuando un incidente involucre datos personales, se reporta a la Superintendencia de Industria y Comercio (SIC) dentro de los 15 días hábiles siguientes a su detección, a través del Registro Nacional de Bases de Datos.

5.7 Capacitación y auditorías

- Capacitación obligatoria anual al personal en seguridad cibernética, manejo de datos personales y Ley 679.
- Auditorías internas anuales y, cuando aplique, externas, para verificar el cumplimiento normativo.
- Indicadores de gestión revisados mensualmente por la Representación Legal.

6. PROTECCIÓN DE NIÑAS, NIÑOS Y ADOLESCENTES (LEY 679 DE 2001)

En cumplimiento de la Ley 679 de 2001, el Decreto 1524 de 2002 y la Ley 1336 de 2009, GRAFENO implementa un mecanismo permanente de bloqueo, en su red de acceso, de las URL identificadas por el Ministerio TIC, la Dijín de la Policía Nacional, el ICBF y demás autoridades competentes como contenedoras de material de explotación sexual de NNA. El procedimiento detallado se encuentra en el documento PR-VCM-001 "Procedimiento de Bloqueo MinTIC".

6.1 Mecanismos disponibles para el usuario

- Página de aviso visible cuando un usuario intenta acceder a una URL bloqueada, indicando el fundamento legal.
- Enlace permanente en https://grafenocomunicaciones.com para denunciar páginas con material de explotación sexual de NNA.
- Información sobre los alcances de la Ley 679 de 2001 publicada en el sitio web de GRAFENO.
- Difusión a los suscriptores de los canales oficiales de denuncia: línea 141 del ICBF y plataforma MASI del MinTIC.

6.2 Cláusulas en los contratos con suscriptores

De conformidad con el artículo 7 del Decreto 1524 de 2002, los contratos de prestación del servicio de Internet de GRAFENO incluyen una cláusula que prohíbe al usuario alojar, distribuir, almacenar o acceder a través de la red a material de explotación sexual de NNA, advirtiendo que el incumplimiento acarrea las sanciones administrativas y penales previstas en la Ley 679 de 2001.

7. CONTROLES PARENTALES DISPONIBLES PARA EL USUARIO

GRAFENO informa a sus usuarios, conforme al numeral 4 del artículo 5 del Decreto 1524 de 2002, sobre la existencia de mecanismos de filtrado y control parental que pueden ser activados por el padre, madre o representante legal en los equipos terminales y en la red doméstica. A continuación se describen las opciones más utilizadas y los criterios de clasificación que las soportan.

7.1 Criterios y categorías de clasificación de contenido

Las herramientas de control parental se basan en la clasificación de contenidos por categorías, entre las que típicamente se encuentran: (i) violencia explícita; (ii) contenido sexual o pornográfico; (iii) sustancias psicoactivas y juegos de azar; (iv) lenguaje ofensivo; (v) redes sociales; (vi) videojuegos por edades (PEGI/ESRB); (vii) sitios de phishing y malware. Estas clasificaciones permiten al adulto responsable habilitar o restringir contenidos según la edad y el grado de madurez del menor.

7.2 Control parental en el router del hogar

La mayoría de routers domésticos permiten configurar reglas de filtrado por dirección, por dispositivo o por horario. GRAFENO recomienda al usuario revisar la documentación del fabricante y, en caso de requerir asistencia, comunicarse con el canal de soporte técnico al teléfono +57 313 432 2994 o al correo grafenocomunicaciones@gmail.com. Las acciones recomendadas en el router son:

- Cambiar las credenciales de administración predeterminadas y la contraseña del Wi-Fi por contraseñas fuertes.
- Activar el cifrado WPA2 o, preferentemente, WPA3.
- Configurar la función de control parental que ofrezca el equipo (filtrado de URL, listas negras, horarios).
- Configurar servidores DNS con filtrado familiar (por ejemplo, soluciones públicas como CleanBrowsing Family, OpenDNS FamilyShield o Cloudflare for Families 1.1.1.3) que bloquean contenido para adultos a nivel de resolución de nombres.
- Crear una red Wi-Fi separada para invitados o dispositivos de NNA, con políticas más restrictivas.

7.3 Control parental por sistema operativo

7.3.1 Windows 10 y Windows 11 — Microsoft Family Safety

1. Abrir Configuración > Cuentas > Familia y otros usuarios.
2. Hacer clic en "Agregar a alguien", seleccionar "Crear una para un menor" o ingresar el correo electrónico Microsoft del NNA.
3. Aceptar la invitación desde la cuenta del menor para vincularla.
4. Acceder al portal https://family.microsoft.com para gestionar: filtros web, límites de tiempo por dispositivo y aplicación, restricciones de juegos por edad, historial de actividad y control de compras.
5. Guardar la configuración y realizar seguimiento periódico.

7.3.2 Windows 8 y 8.1 — Seguridad Familiar

6. Ir a Panel de control > Cuentas de usuario y protección infantil > Configurar Seguridad Familiar para cualquier usuario.
7. Elegir o crear una cuenta estándar para el menor.
8. Activar la función Seguridad Familiar.
9. Vincular la cuenta del menor a una cuenta Microsoft.
10. Configurar desde https://family.microsoft.com los filtros, límites y reportes.

7.3.3 Windows 7 — Control parental clásico

11 Ir a Inicio > Panel de control > Cuentas de usuario y protección infantil > Control parental.

12 Elegir una cuenta estándar existente o crear una para el menor.

13 Activar la opción "Activado, aplicar la configuración actual".

14 Establecer límites de tiempo, restricciones de juegos por clasificación y selección de programas permitidos.

15 Guardar los cambios.

7.3.4 macOS — Tiempo en Pantalla

16 Ir a Preferencias del Sistema > Tiempo en Pantalla.

17 Activar "Tiempo en Pantalla" para el usuario del menor.

18 Configurar Tiempo de inactividad, Límites de aplicaciones, Restricciones de Contenido y Privacidad.

19 Activar la restricción de contenido web para adultos.

7.3.5 iOS / iPadOS — Tiempo en Pantalla

20 Ir a Ajustes > Tiempo en Pantalla > Activar Tiempo en Pantalla.

21 Configurar "Este es el iPhone de mi hijo/a".

22 Establecer un código de Tiempo en Pantalla diferente al del desbloqueo.

23 En "Restricciones de contenido y privacidad" activar y limitar contenido web, aplicaciones, compras y privacidad.

7.3.6 Android — Family Link

24 Descargar la aplicación Google Family Link en el dispositivo del padre/madre/representante legal.

25 Crear o vincular una cuenta de Google del menor (para menores de 13 años se requiere supervisión parental).

26 Configurar filtros de Google Play, SafeSearch en Chrome, límites de tiempo de uso y aprobación de aplicaciones.

27 Revisar periódicamente los reportes de actividad.

7.4 Filtros adicionales

- Activar SafeSearch en motores de búsqueda (Google, Bing, YouTube Modo Restringido).
- Configurar perfiles infantiles en plataformas de streaming (YouTube Kids, Netflix Niños, Disney+, etc.).
- Instalar soluciones complementarias de seguridad familiar (control parental de fabricantes de antivirus reconocidos).

8. ACCIONES RECOMENDADAS AL USUARIO PARA SU SEGURIDAD

La seguridad en la red es una responsabilidad compartida entre GRAFENO y el usuario final. A continuación se presentan recomendaciones para que el usuario fortalezca la seguridad en su entorno digital.

8.1 Contraseñas y autenticación

- Usar contraseñas robustas y únicas por servicio, combinando mayúsculas, minúsculas, números y símbolos.
- Activar autenticación multifactor (MFA) en correo electrónico, banca, redes sociales y servicios sensibles.
- Utilizar un gestor de contraseñas confiable.

8.2 Red Wi-Fi doméstica

- Cambiar el nombre y contraseña predeterminados del router.
- Habilitar cifrado WPA2 o WPA3.
- Mantener actualizado el firmware del router.

- Crear una red de invitados separada de la red principal.

8.3 Dispositivos y software

- Mantener actualizados los sistemas operativos y aplicaciones de computadores, móviles, tabletas y dispositivos IoT (cámaras, asistentes virtuales, televisores inteligentes).
- Instalar software antivirus o antimalware confiable.
- Realizar copias de seguridad periódicas, cifradas y con acceso restringido.
- Deshabilitar funciones innecesarias como compartir archivos, Bluetooth o conexiones remotas cuando no se usen.

8.4 Comportamiento digital

- Desconfiar de correos, mensajes y enlaces sospechosos (phishing).
- Verificar la autenticidad de las páginas antes de ingresar datos personales o financieros.
- Nunca compartir credenciales por canales no oficiales.
- Usar VPN cuando se conecte a redes Wi-Fi públicas.

8.5 Educación y acompañamiento a NNA

- Conversar con los NNA sobre los riesgos en línea (grooming, ciberacoso, sexting, retos peligrosos).
- Acompañar la actividad digital, especialmente en menores de 13 años.
- Reportar contenidos ilegales y conductas de riesgo en https://grafenocomunicaciones.com, en la línea 141 del ICBF y en la plataforma MASI del MinTIC.

9. CANALES DE DENUNCIA Y APOYO

Entidad / Canal	Medio de contacto	Para qué sirve
GRAFENO — denuncia interna	grafenocomunicaciones@gmail.com | +57 313 432 2994 | https://grafenocomunicaciones.com	Reportar URL con contenido ilegal, fallas en el bloqueo o solicitar apoyo en control parental.
MinTIC — Plataforma MASI	https://mintic.gov.co (sección Promoción y Prevención — Denuncias MASI)	Denunciar sitios con material de abuso sexual infantil.
ICBF — Línea 141	Línea telefónica nacional 141	Reportar maltrato infantil, violencia sexual, ciberacoso, trabajo infantil y otras situaciones que afecten a NNA.
Policía Nacional — CAI Virtual	https://caivirtual.policia.gov.co | Línea 123	Reportar delitos informáticos, ciberacoso o material de explotación sexual.
Fiscalía General de la Nación	https://www.fiscalia.gov.co	Denuncia formal de delitos.
Te Protejo — Red PaPaz	https://www.teprotejo.org	Reporte ciudadano de situaciones que vulneren derechos de NNA en internet.

10. INFORMACIÓN INCORPORADA EN EL CONTRATO DE SERVICIO

De acuerdo con la Resolución CRC 5050 de 2016 y el Decreto 1524 de 2002, los contratos de prestación del servicio celebrados entre GRAFENO y sus suscriptores incluyen, entre otras, las siguientes obligaciones e informaciones relacionadas con este documento:

- Prohibición expresa de utilizar el servicio para acceder, alojar o distribuir material de explotación sexual de NNA, con la advertencia de las sanciones de la Ley 679 de 2001.

- Información al usuario sobre las consecuencias legales del acceso a contenidos ilícitos o violación de derechos de autor.
- Información sobre los mecanismos de filtrado y control parental disponibles.
- Información sobre los canales de denuncia, atención al usuario y régimen de protección al usuario.

11. VIGENCIA Y ACTUALIZACIÓN

Este documento entra en vigor el 08 de mayo de 2026 y será revisado, como mínimo, una vez al año, o ante cambios normativos, tecnológicos u operativos relevantes. Las versiones actualizadas serán publicadas en https://grafenocomunicaciones.com y comunicadas a los suscriptores por los canales habituales.

APROBACIÓN

María Marcela Duarte Pérez	**Área Administrativa** **Responsable del documento**
Representante Legal	GRAFENO COMUNICACIONES S.A.S.
GRAFENO COMUNICACIONES S.A.S.	