1. Declaración de adopción

Cable Fácil SAS adopta formalmente la presente Política de Seguridad de la Información, aplicable al dominio de seguridad de red, con el propósito de proteger la Confidencialidad, Integridad y Disponibilidad (C/I/D) de la información y de los servicios de acceso a Internet fijo-provistos mediante tecnología FTTH.

Esta política consolida y documenta los controles técnicos y operativos implementados en la infraestructura de red de la compañía, conforme a lo establecido en el documento IC-004 – Seguridad de la Red – Protocolo Técnico, sirviendo como referencia oficial para auditorías internas, revisiones regulatorias y procesos de mejora continua.

2. Propósito, Alcance y Marco normativo

- ✓ **Propósito:**
  Proteger C/I/D del servicio de Internet fijo, garantizar la inviolabilidad de las comunicaciones y la integridad del servicio, así como informar a los usuarios sobre riesgos y acciones de protección.

- ✓ **Alcance:**
  Esta política aplica a toda la infraestructura de red FTTH de Cable Fácil SAS, incluyendo:
  - Equipos de acceso y transporte de la red.
  - Elementos de gestión, monitoreo y supervisión.
  - Procedimientos técnicos asociados a la operación y mantenimiento de la red.

- ✓ **Marco normativo:**
  La presente política se fundamenta en la Resolución CRC 5050 de 2016 (Título II, Capítulo 9, Sección 2, Art. 2.9.2.3), que establece la obligación de preservar la seguridad de la red, la inviolabilidad de las comunicaciones y la integridad del servicio.

  Se adoptan modelos y herramientas de seguridad alineados con las recomendaciones de la UIT, serie X.800, en lo referente a autenticación, control de acceso, no repudio, confidencialidad, integridad y disponibilidad.

Para el caso de redes móviles, se consideran las recomendaciones UIT X.1121 y X.1122, aclarando que no aplican a la prestación de servicios de Internet fijo de la compañía.

"Cable Fácil SAS mantiene esta política en revisión continua para garantizar su alineación con la normativa vigente y con los cambios regulatorios que pudieran emitirse por la CRC."

3. Compromiso con el SGSI (ISO/IEC 27000)

Cable Fácil SAS adopta un sistema de políticas de seguridad de la información alineado con las mejores prácticas de la familia de normas ISO/IEC 27000, asegurando que sus procesos de seguridad de red se desarrollen bajo un enfoque sistemático y medible.

La compañía se encuentra en proceso de implementación progresiva de un Sistema de Gestión de Seguridad de la Información (SGSI) para el dominio de seguridad de red, priorizando:

- ✓ La identificación y gestión de riesgos asociados a la infraestructura de red.
- ✓ La documentación, monitoreo y mejora continua de los controles técnicos y operativos descritos en esta política.
- ✓ La trazabilidad de decisiones y cambios mediante control de versiones y revisión periódica.

Esta política no constituye una declaración de certificación ISO/IEC 27001, pero establece la base documental y operativa que permitirá su integración en un SGSI corporativo completo de forma planificada, gradual y conforme a los recursos y prioridades de la organización.

4. Principios de Seguridad Exigidos por la Regulación

En concordancia con la Resolución CRC 5050 de 2016 (Título II, Capítulo 9, Sección 2, Art. 2.9.2.3) y con las recomendaciones de la UIT, serie X.800, Cable Fácil SAS gestiona la seguridad de su red garantizando los siguientes principios:

- **Autenticación**: Verificación de identidad de usuarios, dispositivos, servicios y aplicaciones. La información utilizada para autenticación y autorización es protegida de acuerdo con las recomendaciones UIT X.805 y X.811.

- **Control de acceso:** Prevención de la utilización no autorizada de recursos de red, asegurando que únicamente usuarios, dispositivos y servicios autorizados tengan acceso a elementos de red, información almacenada, flujos de datos y aplicaciones (UIT X.805 y X.812).
- **No repudio**: Disponibilidad de evidencia irrefutable de remitentes y destinatarios en las transferencias de datos, garantizando la trazabilidad de las acciones (UIT X.805 y X.813).
- **Confidencialidad de datos**: Protección de la información frente a accesos, divulgaciones o uso no autorizado, asegurando que solo los sujetos autorizados puedan conocerla (UIT X.805 y X.814).
- **Integridad de datos**: Garantía de exactitud y veracidad de la información, previniendo su modificación, eliminación o creación no autorizada y generando alertas ante eventos sospechosos (UIT X.805 y X.815).
- **Disponibilidad**: Garantía de que los elementos de red, servicios y aplicaciones estén accesibles para los usuarios autorizados cuando se requiera, evitando interrupciones no planificadas (UIT X.805).

"Estos principios son aplicados mediante los controles técnicos descritos en esta política (segmentación, firewall, monitoreo, backups y gestión de incidentes), con el fin de garantizar que no solo se declaren, sino que se ejecuten en la operación diaria."

5. Controles Técnicos Implementados (Defensa en Capas)

La seguridad de la red se implementa mediante un enfoque de defensa en capas, combinando segmentación, filtrado de tráfico, exposición controlada de servicios y procedimientos de operación y monitoreo continuo.

✓ **Segmentación y Control de Acceso**

- **Autenticación PPPoE** en OLT Huawei MA5800, asegurando que solo usuarios registrados puedan acceder al servicio.
- **Aislamiento de clientes en capa 2** para evitar tráfico cruzado entre abonados.
- Segmentación por VLAN diferenciando backbone, usuarios y red de gestión.
- **Listas de control de acceso** que restringen el acceso administrativo al router y a la OLT únicamente desde redes de gestión autorizadas.

✓ **Firewall Perimetral (RouterOS – CCR2216)**

Tabla filter – Reglas base y mitigación de DDoS:

- **Política base**: aceptación únicamente de conexiones established y related; uso de lista blanca MGMT_ALLOWED para administración segura.
- **Mitigación de DDoS básica:**
  - Bloqueo de estados inválidos.
  - Descarte de paquetes TCP NEW sin bandera SYN (handshake inválido).
  - Limitación de tráfico ICMP: permite pings con tasa razonable y descarta excesos (protección ante ICMP flood).
  - Control de abuso: límite de conexiones concurrentes por IP (connection-limit), excluyendo redes de gestión autorizadas.
- **Ajuste de sistema**: activación de tcp-syncookies para resistencia ante ataques SYN flood en capa 4.

Tabla raw – Filtro de alto rendimiento:

- Aplicación de reglas notrack a flujos de alto volumen para optimizar el rendimiento.
- Aceptación directa de tráfico de subredes internas confiables.
- Bloqueo preventivo de puertos sensibles y comúnmente atacados (ej.: 22, 23, 25, 445, 8080 en TCP/UDP), de acuerdo con las mejores prácticas y evidencia operativa.

✓ **Exposición Controlada de Servicios del Router**

- **FTP**: Deshabilitado.
- **HTTP/WWW**: Habilitado en puerto no estándar (180).
- **Winbox:** Habilitado en puerto 2891.
- **SSH**: Habilitado en puerto 6800, restringido por IP.
- **API**: Disponible únicamente para subredes internas 172.29.64.0/19 y 172.29.224.0/24.
- **Telnet**: Identificado como activo en puerto alterno; considerado inseguro y sujeto a plan de deshabilitación para cumplir con buenas prácticas.

- ✓ **Bloqueo de Contenidos**
  - Bloqueo puntual de dominios específicos por capa 7.
  - Estrategia principal de filtrado basada en DNS propio, desplegado en centro de datos (Equinix), lo que reduce la carga del router y mejora la eficiencia del filtrado.
- ✓ **Operación, Respaldo y Gestión de Cambios**
  - Respaldo previo a cambios críticos mediante export de configuración para trazabilidad “antes y después”.
  - Verificación de reglas a través de comentarios y estadísticas, con posibilidad de deshabilitación selectiva de reglas para mantenimiento.
  - Monitoreo 24/7 por NOC, incluyendo correlación de eventos y procedimientos documentados de respuesta a incidentes, garantizando continuidad de servicio y rápida detección de anomalías.

6. Deber de Información al Usuario

Cable Fácil SAS cumple con el deber de información establecido en el Artículo 2.9.2.3 de la Resolución CRC 5050 de 2016, comunicando a los usuarios:

- ✓ Los riesgos relativos a la seguridad de la red asociados al servicio de acceso a Internet.
- ✓ Las acciones recomendadas para preservar la seguridad de la red y de su propia información.

Esta información es entregada antes de la contratación y durante la vigencia del servicio, a través de:

- ✓ Esta información es entregada antes de la contratación y durante la vigencia del servicio, a través de:
- ✓ Documentación técnica y manuales de uso publicados en la página web oficial de la compañía.
- ✓ Comunicaciones directas en los procesos de instalación y soporte técnico.
- ✓ Notificaciones cuando se realizan cambios relevantes en la política de seguridad de la red.

Con estas acciones, la compañía asegura que el usuario pueda tomar decisiones informadas y adoptar medidas preventivas para proteger sus equipos y su información personal.

7. Roles y responsabilidades

Para garantizar el cumplimiento de esta política, Cable Fácil SAS define los siguientes roles y responsabilidades dentro del dominio de seguridad de red:

- ✓ **Personal de Administración de Red:**
  - Aplica, revisa y actualiza las reglas de firewall, listas de control de acceso y configuraciones de seguridad.
  - Realiza respaldos periódicos de configuración antes de cualquier cambio crítico.
  - Documenta las modificaciones y mantiene trazabilidad de cambios para auditoría.
- ✓ **Centro de Operaciones de Red (NOC) – 24/7:**
  - Realiza monitoreo continuo de la red, alertas y métricas de desempeño.
  - Ejecuta procedimientos de detección, contención y escalamiento de incidentes de seguridad.
  - Genera reportes de eventos y mantiene bitácoras para análisis forense y mejora continua.
- ✓ **Gerencia de Operaciones / Comité de Seguridad (cuando aplique):**
  - Revisa y aprueba las actualizaciones de la política.
  - Garantiza la asignación de recursos (personal, herramientas de monitoreo y capacitación) para su cumplimiento.
  - Supervisa la correcta implementación de las acciones correctivas derivadas de incidentes o auditorías.

8. Revisión y Vigencia

Esta política entra en vigor a partir de su aprobación por la Gerencia de Operaciones y se mantendrá vigente mientras los controles descritos permanezcan operativos.

La política será revisada al menos una vez al año, o de forma inmediata cuando:

- ✓ Existan cambios significativos en la infraestructura de red o en los controles de seguridad.
- ✓ Se presenten nuevas disposiciones regulatorias emitidas por la CRC u otras autoridades.
- ✓ Se detecten hallazgos en auditorías internas o externas que requieran actualización de esta política.

Los ajustes técnicos (por ejemplo, cambios en reglas de firewall, listas de control o servicios expuestos) serán incorporados a la política una vez implementados y verificados, manteniendo registro en el control de versiones para garantizar trazabilidad y evidencia documental ante auditoría.

9. Anexo A – Referente Normativo Citado

Resolución CRC 5050 de 2016

- ✓ **Título II, Capítulo 9, Sección 2, Artículo 2.9.2.3 – Seguridad de la Red**
  - Obliga a los proveedores de redes y servicios de telecomunicaciones que prestan servicio de acceso a Internet a informar a los usuarios, antes de la contratación y durante la vigencia del servicio, los riesgos relativos a la seguridad de la red y las acciones que deben adelantar para su protección.
  - Exige el uso de recursos técnicos y logísticos para garantizar y preservar la seguridad de la red, la inviolabilidad de las comunicaciones, la protección contra virus y la integridad del servicio.
  - Indica la adopción de modelos de seguridad conforme a las recomendaciones UIT serie X.800, en relación con autenticación, control de acceso, no repudio, confidencialidad de datos, integridad de datos y disponibilidad.

Recomendaciones UIT serie X.800

- ✓ Establecen el marco de referencia para implementar controles de seguridad en redes de telecomunicaciones, abordando los siguientes principios:
  - Autenticación
  - Control de acceso
  - No repudio
  - Confidencialidad de datos
  - Integridad de datos

- Disponibilidad

Recomendaciones UIT X.1121 y X.1122

- ✓ Modelos de seguridad aplicables a redes móviles, que establecen el uso de cifrado, firmas digitales y controles de acceso para prevenir acceso no autorizado, interrupción o interferencia deliberada de la comunicación.
- ✓ No aplican a los servicios de Internet fijo provistos por Cable Fácil SAS, pero se mantienen como referencia normativa para futuros casos en que se amplíe la oferta de servicios.