SEGURIDAD DE LA RED, RIESGOS DEL SERVICIO DE INTERNET Y CONTROLES PARENTALES

I. INFRAESTRUCTURA Y SEGURIDAD DE LA RED

UNIMOS S.A. ESP ha implementado una infraestructura de vanguardia para garantizar la integridad y continuidad del servicio, bajo los siguientes pilares técnicos:

1. **Seguridad Perimetral Lógica:** Implementación de Firewalls y sistemas de filtrado perimetral que mitigan accesos no autorizados y ataques DDoS, protegiendo el núcleo (CORE) de la red.
    - **Firewalls de Capa 7:** Filtrado inteligente de tráfico en el Core de la red para mitigar ataques DDoS y accesos no autorizados.
    - **Trazabilidad de Sesión:** Sistema que vincula cada dirección IP con el abonado, garantizando el "no repudio" y la seguridad jurídica.
    - **Redundancia N+1:** Equipamiento MikroTik/GPON configurado en alta disponibilidad para evitar interrupciones del servicio
2. **Autenticación y Control de Acceso:** Uso de plataformas de alta disponibilidad que aseguran la identidad del usuario en tiempo real mediante protocolos de autenticación y registro (Accounting).
3. **Trazabilidad y No Repudio:** Generación automatizada de logs de sesión que vinculan direcciones IP con cuentas específicas, garantizando la identidad y la duración de cada conexión.
4. **Protección de Infraestructura Física:** Control de acceso a nodos y armarios mediante llaves de seguridad exclusivas y vigilancia por CCTV las 24/7 en áreas críticas.
5. **Centro de Operaciones de Red (NOC):** Monitoreo activo los 7 días de la semana para la detección de anomalías físicas o lógicas en la red.

II. RIESGOS DEL SERVICIO DE INTERNET

El uso de internet moderno presenta desafíos que escalan más allá del entorno físico. Los principales vectores de riesgo identificados son:

- **Amenazas Tecnológicas:** Proliferación de malware, ransomware, troyanos y spyware que

aprovechan vulnerabilidades en sistemas no actualizados.

- **Riesgos de Información:** Exposición a contenidos falsos (Fake News), material nocivo, ilícito o inapropiado.
- **Ingeniería Social y Comunicación:** Recepción de phishing, spam masivo, pérdida de intimidad en foros y contacto con identidades falsas.
- **Delitos Económicos:** Estafas financieras, robo de identidad y violaciones a la propiedad intelectual.
- **Riesgos Críticos para Menores:**
    - **Ciberacoso (Cyberbullying):** Hostigamiento a través de medios digitales.
    - **Grooming:** Acercamiento de adultos a menores con fines ilícitos.
    - **Sexting y Extorsión:** Riesgos derivados del intercambio de contenido íntimo.

III. Protocolos de Seguridad para el Usuario Final

Para garantizar una navegación segura, UNIMOS S.A. ESP exige y recomienda a sus usuarios adoptar las siguientes medidas técnicas:

1. **Protección de Endpoints:** Instalación de soluciones de seguridad (Antivirus/Antispyware) con licencias vigentes de fabricantes reconocidos.
2. **Higiene Digital:**
    - **Actualización Constante:** Mantener el sistema operativo y aplicaciones con los últimos parches de seguridad para cerrar brechas de vulnerabilidad.
    - **Gestión de Credenciales:** Uso de contraseñas robustas (mínimo 8 caracteres, combinación alfanumérica y símbolos).
    - **Validación de Sitios:** Verificar el uso de protocolos seguros (**HTTPS**) y la legitimidad de los dominios antes de ingresar datos sensibles.
    - Evitar transacciones bancarias en redes WiFi abiertas. Se recomienda el uso de **VPN** para cifrar datos en entornos públicos.
3. **Prevención de Malware:** Evitar la ejecución de archivos sospechosos de fuentes no confiables (P2P, correos desconocidos) y descargas desde sitios no oficiales.
4. **Gestión de Credenciales:** Uso de autenticación de dos factores (2FA) y contraseñas de alta complejidad (alfanuméricas + símbolos).
5. **Verificación de Dominios:** Ingresar datos solo en sitios con certificados **SSL (HTTPS)** válidos.

IV. MECANISMOS DE CONTROL PARENTAL

Los controles parentales son herramientas esenciales para limitar el tiempo de exposición y filtrar contenidos inapropiados según la edad.

1. **Controles Nativos por Plataforma**
   - **Windows 10 y 11:** Acceda a *Configuración* > *Cuentas* > *Familia y otros usuarios*. Permite administrar el tiempo de pantalla, filtros web y restricciones de aplicaciones a través de la cuenta de Microsoft.
     - Video Instructivo habilitar control parental en Windows 10 https://www.youtube.com/watch?v=ROzX3GlIUh4
     - Video Instructivo habilitar control parental en Windows 11 https://www.youtube.com/watch?v=NMDaYgQiZVk
   - **Sistemas de Escritorio Anteriores:** En Windows 7 y 8, la configuración se realiza a través del *Panel de Control* > *Cuentas de usuario y protección infantil*.
   - **MacOS / iOS:** Uso de *Screen Time* para restringir contenido y comunicaciones.
   - **Android:** Gestión mediante *Google Family Link* (aprobación de apps y ubicación en tiempo real).
2. **Software Especializado Recomendado**

   Se sugiere la implementación de soluciones que permitan la gestión integral en dispositivos móviles y computadoras:
   - **Qustodio:** Bloqueo de apps y sitios peligrosos con notificaciones en tiempo real. https://www.qustodio.com/es/
   - **Norton Family:** Especializado en el filtrado de contenido inapropiado. https://family.norton.com/web/
   - **Wondershare FamiSafe:** Filtrado avanzado de contenido para adultos y detección de palabras clave en redes sociales. https://famisafe.wondershare.com/es/
   - **Bark:** Especializado en detectar señales de acoso o depresión en mensajes y redes sociales.
3. **Configuración en el Router/CPE:**
   - El usuario puede solicitar o configurar en su router suspensión del servicio

V. Confidencialidad y Marco Legal

- **Ley 679 de 2001:** UNIMOS S.A. ESP bloquea activamente el acceso a sitios de pornografía infantil reportados por las autoridades.
- **Privacidad:** Los datos de navegación son confidenciales y solo se entregarán a autoridades competentes previa **orden judicial**, conforme a la Ley de Protección de Datos Personales (Habeas Data).

ESTRATEGIA DE SEGURIDAD DE RED, GESTIÓN DE RIESGOS Y CONTROL PARENTAL 2026

I. INFRAESTRUCTURA Y SEGURIDAD DE LA RED (Art. 9.2.1.1)

UNIMOS S.A. ESP garantiza la integridad y continuidad del servicio mediante una arquitectura blindada:

1. **Seguridad Física y Prevención de Sabotaje:**
    - Protección de infraestructura externa (canalizaciones y postería) con sistemas antiescalatorios y tapas de seguridad.
    - Control de acceso estricto a nodos y armarios mediante llaves de seguridad y monitoreo por CCTV 24/7.
2. **Seguridad Lógica Multicapa:**
    - **Firewalls de Capa 7:** Filtrado inteligente de tráfico en el Core de la red para mitigar ataques DDoS y accesos no autorizados.
    - **Trazabilidad de Sesión:** Sistema que vincula cada dirección IP con el abonado, garantizando el "no repudio" y la seguridad jurídica.
    - **Redundancia N+1:** Equipamiento MikroTik/GPON configurado en alta disponibilidad para evitar interrupciones del servicio.

II. RIESGOS DEL SERVICIO DE INTERNET (Art. 9.2.1.2)

La navegación moderna implica riesgos que evolucionan constantemente. Clasificamos las amenazas en:

- **Amenazas a la Integridad Técnica:** Malware, Ransomware (secuestro de datos) y Spyware.

- **Amenazas de Ingeniería Social:** Phishing (suplantación de bancos), Spam masivo y estafas en redes sociales.
- **Riesgos Críticos para Menores:**
    - **Ciberacoso (Cyberbullying):** Hostigamiento a través de medios digitales.
    - **Grooming:** Acercamiento de adultos a menores con fines ilícitos.
    - **Sexting y Extorsión:** Riesgos derivados del intercambio de contenido íntimo.

III. GUÍA DE AUTOPROTECCIÓN PARA EL USUARIO

Para una navegación segura, es imperativo seguir estos protocolos técnicos:

1. **Seguridad del Endpoint:** Uso obligatorio de Antivirus y Firewalls personales actualizados.
2. **Higiene de Red:** Evitar transacciones bancarias en redes WiFi abiertas. Se recomienda el uso de **VPN** para cifrar datos en entornos públicos.
3. **Gestión de Credenciales:** Uso de autenticación de dos factores (2FA) y contraseñas de alta complejidad (alfanuméricas + símbolos).
4. **Verificación de Dominios:** Ingresar datos solo en sitios con certificados **SSL (HTTPS)** válidos.

IV. MECANISMOS DE CONTROL PARENTAL 2.0 (Art. 9.2.1.3)

Más allá del bloqueo básico, UNIMOS S.A. ESP promueve el uso de herramientas de **Seguridad Familiar Integral**:

1. Controles Nativos por Plataforma:

- **Windows 11:** Configuración a través de *Microsoft Family Safety* (límites de tiempo y filtrado web).
- **MacOS / iOS:** Uso de *Screen Time* para restringir contenido y comunicaciones.
- **Android:** Gestión mediante *Google Family Link* (aprobación de apps y ubicación en tiempo real).

2. Software Especializado Recomendado (Top 2026):

- **Qustodio / Norton Family:** Líderes en filtrado de contenido por categorías y reportes de actividad.
- **Bark:** Especializado en detectar señales de acoso o depresión en mensajes y redes sociales.
- **FamiSafe:** Bloqueo integral de contenido pornográfico y detección de imágenes sospechosas.

3. Configuración en el Router/CPE:

El usuario puede solicitar o configurar en su router límites de horario para dispositivos específicos (p.ej., desconexión automática de consolas a las 9:00 PM).

V. COMPROMISO LEGAL Y CONFIDENCIALIDAD

- **Ley 679 de 2001:** UNIMOS S.A. ESP bloquea activamente el acceso a sitios de pornografía infantil reportados por las autoridades.
- **Privacidad:** Los datos de navegación son confidenciales y solo se entregarán a autoridades competentes previa **orden judicial**, conforme a la Ley de Protección de Datos Personales (Habeas Data).