SEGURIDAD DE LA RED Y CONTROLES PARENTALES.

En cumplimiento de las normativas vigentes y con el propósito de garantizar la seguridad de la red y la integridad de los servicios ofrecidos, **Standard Connection S.A.S.** ha desarrollado sistemas y procesos que previenen la interceptación, interrupción e interferencia del servicio, protegiendo así a sus usuarios. A continuación, presentamos información clave relacionada con la seguridad del servicio de acceso a Internet y controles parentales.

Guía para Controlar el Acceso de sus Hijos a Sitios Web

I. RIESGOS RELATIVOS AL SERVICIO DE INTERNET

El acceso a Internet se ha convertido en una herramienta esencial para los usuarios, quienes interactúan, comparten información, realizan compras y consumen contenido digital. Sin embargo, también representa riesgos para la seguridad y privacidad. Por esta razón, **Standard Connection S.A.S.** busca concientizar a sus usuarios sobre estos riesgos y promover el uso seguro de Internet. Los principales riesgos incluyen:

1. Malware

Software malicioso diseñado para dañar dispositivos. Este puede infectar sistemas a través de vulnerabilidades o errores de los usuarios. Para minimizar el riesgo, recomendamos:

- Instalar antivirus y antispyware actualizados.
- Evitar descargar software de fuentes desconocidas.

2. Spam

Correos electrónicos no solicitados que pueden contener enlaces dañinos. Es importante:

- Configurar filtros de correo.
- No abrir correos sospechosos.

3. Estafas en Línea (Scam)

Técnicas como phishing buscan engañar a los usuarios para obtener información confidencial. Sugerimos verificar la autenticidad de los correos y no proporcionar datos sensibles sin confirmación previa.

4. Ciberacoso (Cyberbullying)

Conducta hostil que afecta principalmente a niños y adolescentes. Padres y tutores deben supervisar el uso de dispositivos y redes sociales.

5. Grooming

Interacción de adultos con menores con fines inapropiados. Supervisar las redes sociales y limitar la información compartida por los niños es fundamental.

6. Sexting

Intercambio de contenido sexual entre usuarios. Se recomienda educar a los menores sobre los riesgos asociados.

7. Robo de Información

Información enviada sin cifrado o medidas de seguridad puede ser interceptada. Para evitarlo:

- Utilice conexiones seguras (https).
- Evite redes Wi-Fi públicas para transacciones sensibles.

II. MEDIDAS ADOPTADAS POR STANDARD CONNECTION S.A.S. PARA GARANTIZAR LA SEGURIDAD DE LA RED

Standard Connection S.A.S. ha implementado diversas medidas de seguridad para proteger su red y a sus usuarios, destacando las siguientes:

1. Infraestructura de Red y Protección Física

- Uso de radioenlaces PTP (Point-to-Point) y PTMP ((Point-to-Multipoint) para garantizar conexiones seguras y estables.
- Protección física de los equipos con sistemas antiescalatorios, canalizaciones seguras y monitoreo continuo.
- Sistemas de acceso controlado a instalaciones críticas mediante tarjetas y tecnologías biométricas.

2. Centro de Operaciones de Red (NOC)

El NOC opera 24/7 monitoreando y gestionando la actividad en los equipos que soportan la red. Esto incluye la identificación y resolución de posibles incidentes de seguridad.

3. Seguridad de Datos

- Los datos de los usuarios se almacenan en sistemas protegidos, garantizando su confidencialidad.
- Cualquier solicitud de datos personales debe estar respaldada por una orden judicial.

4. Prevención de Fraudes

- Validación estricta de documentos de identidad al momento de la contratación.
- Supervisión de contratos antes de la activación de los servicios.

5. Bloqueo de Contenidos Inadecuados

- Bloqueo de páginas reportadas relacionadas con pornografía infantil, en cumplimiento de la Ley 679.
- Monitoreo constante para garantizar la seguridad en el acceso a Internet.

III. ACCIONES RECOMENDADAS PARA LOS USUARIOS

Los usuarios pueden implementar las siguientes medidas para garantizar su seguridad al usar Internet:

1. Proteger Dispositivos

- Descargar aplicaciones únicamente de tiendas oficiales.
- Instalar herramientas antivirus y mantenerlas actualizadas.
- Evitar el uso de redes Wi-Fi públicas para transacciones sensibles.

2. Contraseñas Seguras

- Crear contraseñas robustas con combinaciones de letras, números y caracteres especiales.
- No reutilizar contraseñas en diferentes servicios.
- No compartir contraseñas.

3. Configuración del Navegador

- Utilizar navegadores actualizados con complementos confiables.
- Borrar el historial de navegación y cookies regularmente.
- Verificar que los sitios visitados usen protocolos seguros (https).

IV. CONTROLES PARENTALES

Pasos para Activar el Control Parental en Windows

1. Ir a *Inicio* > *Configuración* > *Cuentas* > *Familia y otros usuarios*.

2. Crear una cuenta de menor y personalizar configuraciones como:
    - Límites de tiempo.
    - Bloqueo de juegos inapropiados.
    - Restricciones de aplicaciones.

Pasos para Activar el Control Parental en Mac

1. Ir a *Preferencias del Sistema* > *Controles Parentales*.
2. Definir restricciones en:
    - Acceso a aplicaciones y sitios web.
    - Límites de tiempo.
    - Comunicación con terceros.

Standard Connection S.A.S. se compromete a proteger la seguridad de su red y a brindar información educativa a sus usuarios para el uso responsable y seguro de Internet.