SEGURIDAD DE LA RED Y CONTROLES PARENTALES

En cumplimiento a lo establecido en la **Resolución CRC 5050 de 2016**, **DIGITVNET S.A.S.** ha implementado sistemas para garantizar la seguridad de su red y la integridad del servicio prestado a sus usuarios, evitando así la interceptación, interrupción e interferencia del mismo; igualmente, sobre otros aspectos importantes relacionados en la citada regulación como son:
i) Información del Servicio de Acceso a Internet,
ii) Acceso a Contenidos, entre otros, los cuales se describen a continuación:

I. RIESGOS RELATIVOS AL SERVICIO DE INTERNET

Dentro de dichos riesgos se tienen:

- **Malware:** Es el acrónimo en inglés de *software malicioso (malicious software)*. El objetivo de este tipo de aplicaciones es dañar la computadora. En la mayoría de los casos, la infección ocurre por "errores" realizados por los usuarios al ser engañados por el atacante. Existen muchas herramientas (antivirus, antispyware) y buenas prácticas que reducen el riesgo de infección ante todas las variantes de códigos maliciosos: virus, gusanos, troyanos, spyware, etc.

- **Spam:** Es el famoso "correo basura". Son mensajes no solicitados que llegan a la bandeja de entrada. Normalmente contienen propaganda —muchas veces engañosa— que incita al usuario a ingresar a páginas con ofertas "milagrosas", cuyo contenido puede ser dañino.

- **Scam:** Son engaños o estafas realizadas a través de Internet. Pueden ser por correos no solicitados o por técnicas de ingeniería social que buscan obtener información confidencial (como contraseñas o datos bancarios).

- **Ciberacoso (Cyberbullying):** Conducta hostil hacia menores, practicada usualmente por pares en la web, que busca humillar o afectar emocionalmente a la víctima. Puede darse a través de Internet, celulares o videoconsolas.

- **Grooming:** Persuasión de un adulto hacia un niño para crear una conexión emocional y generar confianza con fines sexuales. El adulto suele hacerse pasar por un menor para entablar relación y luego intentar encuentros personales.
- **Sexting:** Acrónimo de *Sex* y *Texting*. Consiste en el envío o intercambio de mensajes, imágenes o videos con contenido erótico o sexual, práctica que se ha extendido entre adolescentes.
- **Robo de información:** La información transmitida por la web sin medidas de seguridad puede ser interceptada. Los ataques suelen buscar datos personales o financieros, exponiendo a las víctimas a robo de identidad o pérdidas económicas.

El usuario podrá encontrar más información y disposiciones sobre estos temas en los enlaces alojados en la página oficial de **DIGITVNET S.A.S.**

II. MEDIDAS ADOPTADAS POR DIGITVNET S.A.S.

DIGITVNET S.A.S. ha implementado múltiples medidas para garantizar la seguridad de la red:

- Sistemas de protección (*SIGAR*) contra intrusiones no autorizadas en sus elementos de red, que permiten monitorear en tiempo real cualquier intento de acceso a la red física de un abonado.
- Registro y control de técnicos de campo. Los usuarios pueden llamar al número **300 835 0887**para confirmar la identidad del personal técnico.
- Sistemas de protección física (tapas de seguridad, canalizaciones en concreto, sistemas antiescalatorios, etc.) que impiden el acceso no autorizado.
- **Centro de Operaciones de Red (NOC)** disponible los 7 días de la semana, 24 horas, encargado de monitorear la infraestructura de Internet y datos.
- **Sistemas de protección antivirus y antispam** para usuarios de banda ancha, garantizando la integridad de la información.

- Plataformas de autenticación seguras (*RADIUS*, alta disponibilidad) que aseguran que solo usuarios autorizados accedan a los servicios.
- **Accounting (servicio de no repudio):** registro de logs de conexión con IP dinámica, usuario y duración de sesión, almacenados por dos (2) años.
- **Protección de datos confidenciales:** sistemas de almacenamiento masivo con mecanismos de seguridad y acceso solo mediante orden judicial (Artículo 22 de la Resolución CRT 1732 de 2007).
- **Mecanismos de protección del CORE de red:** Firewalls, filtrado perimetral, y bloqueo de URLs de pornografía infantil reportadas por el Ministerio de Comunicaciones según la Ley 679.
- Red redundante con esquema **1+1**, conectividad *multihoming* hacia el CORE de Internet, cumplimiento de normatividad **ARIN**, y plataformas redundantes (DNS, RADIUS, LDAP, Firewall).
- Procedimientos de seguridad en bases de datos corporativas con accesos limitados por perfil y control de usuarios.
- Políticas de confidencialidad firmadas por empleados con acceso a información privada de clientes.
- Validación documental (cédula, huella) para prevenir suplantación de identidad en procesos comerciales.

III. ACCIONES QUE DEBE TOMAR EL USUARIO PARA GARANTIZAR LA SEGURIDAD EN LA RED

1. Proteger los dispositivos:

- Descargar aplicaciones solo desde tiendas oficiales.
- Revisar valoraciones y comentarios de otros usuarios.
- Instalar herramientas antivirus y mantenerlas actualizadas.

2. Cuidado con las redes Wi-Fi públicas:

- Evitar ingresar datos personales o bancarios.

- No usar banca en línea desde redes públicas.

3. Uso de contraseñas seguras:

- Mínimo 8 caracteres, combinando mayúsculas, minúsculas, números y símbolos.
- No usar contraseñas obvias (“123456”, “qwerty”, nombres personales, etc.).
- No reutilizar contraseñas ni compartirlas.

4. Mantener el sistema actualizado:

- Actualizar software, antivirus y navegadores.
- Verificar sitios seguros (https:// y candado visible).

5. Configuración de privacidad:

- Revisar la configuración de redes sociales.
- Controlar quién puede ver publicaciones, etiquetar o acceder al perfil.
- Evitar publicar datos personales, planes o comportamientos inapropiados.

6. Verificar fuentes de información:

- Evitar difundir o abrir enlaces de noticias falsas o correos sospechosos.

CONTROLES PARENTALES

Los controles parentales permiten limitar el tiempo de navegación, bloquear contenido inapropiado y proteger la privacidad de los menores. Sin embargo, son herramientas complementarias: la supervisión de los padres es fundamental.

Windows 7 / 8 / 8.1

1. Inicio → Panel de control → Cuentas de usuario y protección infantil.
2. Configurar el Control Parental → Activar → Seleccionar cuenta del menor.
3. Establecer límites: tiempo, juegos o programas específicos.

Windows 10

1. Configuración → Cuentas → Familia y otros usuarios.
2. Agregar familiar → Agregar hijo → Administrar configuración familiar en línea.
3. Personalizar control parental (actividad, exploración web, apps, tiempo en pantalla).

macOS

1. Preferencias del sistema → Controles parentales → Desbloquear con contraseña de administrador.
2. Activar para el usuario del niño.
3. Definir restricciones: apps, sitios web, contactos, límites de tiempo y privacidad.