SEGURIDAD DE LA RED DE REDCON REDES Y CONEXIONES SAS

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

1. **RIESGOS RELATIVOS AL SERVICIO DE INTERNET:**
    - 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. La diferencia entre estas variantes radica en la forma en que se distribuyen: algunas veces se aprovechan de sistemas vulnerables y otras de usuarios no precavidos.
    - Spam: El spam es el famoso "correo basura". Son aquellos mensajes que no fueron solicitados por el usuario y que llegan a la bandeja de entrada. Normalmente, este tipo de correos contienen propagandas – muchas veces engañosas – que incitan al usuario a ingresar a páginas, con ofertas "milagrosas", cuyo contenido es potencialmente dañino para el usuario.
    - Scam: Los scam son engaños o estafas, que se llevan a cabo a través de Internet. Se realizan de diversas formas como, por ejemplo, a través de correos no solicitados (spam), así como también a través de técnicas de Ingeniería Social. Estas últimas, intentan convencer al usuario de la prestación de un servicio cuando en realidad sólo quieren acceder a información confidencial. Un ejemplo son los mensajes falsos solicitando nuestra contraseña y clave de redes sociales a través de Internet.
    - Ciberacoso: Es una conducta hostil que puede ser practicada hacia los niños. La víctima de este tipo de acosos es sometida a amenazas y humillaciones de parte de sus pares en la web, cuyas intenciones son atormentar a la persona y llevarla a un quiebre emocional. Estas prácticas pueden ser realizadas a través de Internet, así como también, teléfonos celulares y videoconsolas. También denominado en inglés, cyberbullying, no siempre son realizadas por adultos, sino también son frecuentes entre adolescentes.
    - Grooming: Se trata de la persuasión de un adulto hacia un niño, con la finalidad de obtener una conexión emocional y generar un ambiente de confianza para que el niño realice actividades sexuales. Muchas veces los adultos se hacen pasar por niños de su edad e intentan entablar una relación para, luego, buscar realizar encuentros personales.
    - Sexting: Proviene del acrónimo formado entre Sex y Texting. Inicialmente, y como lo indica su nombre, se trataba del envío de mensajes con contenidos eróticos. Posteriormente, dado el avance tecnológico, esta modalidad evolucionó hacia el intercambio de imágenes y videos convirtiéndose en una práctica habitual entre adolescentes y niños.

- Robo de información: Toda la información que viaja por la web, sin las medidas de precaución necesarias, corre el riesgo de ser interceptada por un tercero. De igual modo, existen también ataques con esta finalidad. La información buscada, normalmente apunta a los datos personales. Un paso en falso ante este tipo de incidentes, puede exponer al menor de edad a la pérdida de dinero familiar o al robo de identidad. Igualmente, el usuario podrá encontrar otras disposiciones referentes a este tipo de temas en los links que se indican a continuación, alojados en la página oficial de **REDCON REDES Y CONEXIONES SAS**.

2. MEDIDAS ADOPTADAS POR REDCON REDES Y CONEXIONES SAS

Se ha implementado medidas para garantizar la seguridad de la red, así:

2.1 Seguridad de la red física.

- Sistemas de protección (Sigar) contra intrusión no autorizada en sus elementos de red (armarios), que permiten monitorear en tiempo real cualquier intento de acceso a la red física de un abonado asociado a dicho elemento. El aseguramiento y la gestión se encuentran soportados mediante procesos establecidos al interior de la Compañía.
- Registrar los técnicos de campo que requieran ingresar a realizar trabajos dentro del domicilio de los quienes puede llamar al número de celular **3112551234** con el fin de confirmar la identidad de los empleados y constatar si efectivamente laboran con **REDCON REDES Y CONEXIONES SAS**.
- Sistemas de protección física de su infraestructura que impiden intrusiones no autorizadas e interrupción del servicio de sus líneas de abonado, tales como las tapas de seguridad en sus cámaras y el atraque de concreto en sus canalizaciones y sistemas antiescalatorios a nivel de postería entre otros.
- **REDCON REDES Y CONEXIONES SAS** dispone de sistemas de seguridad que monitorean y controlan el acceso a sus instalaciones y áreas críticas de sus edificios, haciendo uso tarjetas de seguridad entre otros.
- Centro de operaciones de red NOC (Network Operation Center) los siete (7) días de la semana las 24 horas, encargado de monitorear e informar sobre actividades físicas y lógicas en los equipos que ponen la red de internet y datos de la misma.

2.2 Seguridad en el acceso a internet.

- Para los usuarios se cuenta con sistemas de protección antivirus y antispam, los cuales previenen la perdida de información y garantizan la integridad de la información almacenada en sus cuentas de correo previamente suministrada por **REDCON REDES Y CONEXIONES SAS**
- Frente a la autenticación de los usuarios del servicio de acceso a internet, **REDCON REDES Y CONEXIONES SAS** dispone de plataformas y procesos, que permiten en tiempo real, asegurar la autorización de acceso a la navegación vía la verificación de identidad (información residente en el equipo lado usuario – CPE) del usuario que

intenta conectarse. Lo anterior asegura que solo usuarios autorizados puedan hacer uso de los servicios contratados con la compañía. La plataforma usada corresponde a un servicio de RADIUS implementado en configuración de alta disponibilidad, como también se cuenta con un sistema de administración de dispositivos de usuario final CPE, para la protección estos dispositivos contra vulnerabilidades que pudieran afectar el servicio de nuestros usuarios.

- La plataforma en operación de **REDCON REDES Y CONEXIONES SAS** cuenta con funcionalidades de Accounting (Servicio de no repudio), esto es, que genera logs para cada una de las sesiones de usuario, donde se relaciona una dirección IP dinámica con la cuenta única asociada para cada cliente (asegura la identidad), fecha de inicio y duración de la sesión. Estos datos son almacenados mes a mes y guardados por un periodo de dos (2) años.

- Frente a la Confidencialidad de los datos, **REDCON REDES Y CONEXIONES SAS**, dispone de sistemas que almacenan la información (almacenamiento masivo de datos) con protecciones que evitan la intrusión indebida a éstos. A su vez frente a los datos biográficos de sus usuarios, tiene establecidos procesos que garantizan la recepción y trámite de los requerimientos allegados solo desde los entes de seguridad mediante los cuales, se realiza la solicitud de información confidencial asociada a los usuarios de línea básica y datos (Pej. direcciones IP). Dicha solicitud debe estar soportada mediante orden judicial. (Artículo 22 Resolución CRT 1732 de 2007).
- Mecanismos de protección del CORE de la Red, como son: Firewalls y filtrado perimetral, lo cual, evita y elimina todo riesgo de acceso no autorizado a la data correspondiente al servicio de correo masivo de sus usuarios.
- Plataforma especializada en el bloqueo de páginas y redirección a portales cautivos, dando cumplimiento a lo establecido por la normatividad vigente, se filtran las páginas de pornografía infantil publicadas por el ministerio de Comunicaciones Ley 679 (Esto se hace a través de los URLs reportados en la página).

- **REDCON REDES Y CONEXIONES SAS** cuenta con una red de alta disponibilidad, la cual opera basada en un modelo de operación que contempla la redundancia en los diferentes elementos que constituyen el CORE sobre el que se soporta el servicio de Internet. Consagra y cumple la normatividad de ARIN (American Register Internet Numbers), en la cual exige que como service provider tengamos esquemas de conectividad multihoming hacia el CORE de Internet.

- La Disponibilidad se garantiza, sobre la base de una topología de red en esquema 1+1, para todos los elementos que componen el CORE de la red, a saber: Red MPLS; múltiples puntos de acceso a Internet redundantes; redundancia en la conectividad hacia los proveedores de salida Internacional y sobre las Plataformas de servicio (DNS, RADIUS, LDAP, Firewall). Configuraciones redundantes en sus elementos de operación crítica y una topología basada en un esquema full mesh.

- De igual manera, en relación con la seguridad de los datos e informaciones de nuestros usuarios **REDCON REDES Y CONEXIONES SAS** ha implementado los siguientes mecanismos: Se han enviado cartas a los empleados de la compañía que

manejan datos e información de nuestros usuarios, en donde se les manifiesta que tienen opciones con acceso a información y datos privados de los clientes (confidencial), con el objetivo de comprometerlos a manejar de forma prudente dicha información. Se consolidó la información enviada como respuesta de los subgerentes y directores al administrador de la base de datos para la permanente actualización de los perfiles de usuarios.

- Por otra parte, se crearon esquemas de seguridad a nivel de base de datos para cada uno de los sistemas de información y sistema de red corporativo, mediante procedimientos documentados, en donde se garantiza el acceso sólo a las opciones que se tienen autorizadas por los jefes inmediatos.

- En relación con la prevención de fraudes por suplantación de identidad, **REDCON REDES Y CONEXIONES SAS** cuenta con las siguientes herramientas de verificación y control: Para las ventas se debe solicitar fotocopia de la cédula ampliada al 150% y huella. Se constituyó un grupo de operaciones comerciales encargado de realizar validación previa a los contratos y sus anexos antes de la instalación de los servicios.

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

- Proteger adecuadamente los Dispositivos Descárgalas únicamente a través de las tiendas de apps oficiales.
- Revisar previamente la valoración y los comentarios que los usuarios han hecho sobre una determinada app. Cuando se comporta mal o de manera sospechosa, los propios usuarios se encargan de reflejarlo en los comentarios.
- Instala una herramienta antivirus para que detecte posibles apps maliciosas que intenten colarse en el dispositivo. Se debe tener Cuidado con las redes wifi públicas a las que se conecta. Si son usadas: No intercambiar información privada o confidencial. No conectarse al servicio de banca online. Utilizar contraseñas fuertes y protegerlas Elegir contraseñas fuertes o robustas de al menos ocho (8) caracteres y compuestas por mayúsculas, minúsculas, números y caracteres especiales. NO utilizar contraseñas fáciles de adivinar como: “12345678”, “qwerty”, ”aaaaa”, nombres de familiares, matrículas de vehículos NO compartir las contraseñas: Si se hace, dejará de ser secreta y se estará dando acceso a otras personas a tu privacidad.
- NO utilizar la misma contraseña en varios servicios.
- Mantener protegido el dispositivo de acceso a la red de manera adecuada Instalar en el dispositivo un antivirus y mantenerlo actualizado para que detecte las últimas amenazas que circulan por la red. Los programas del equipo y el/los navegador(es) se deben mantener actualizados y correctamente configurados.

- Crear una cuenta de usuario para cada persona que vaya a utilizar el dispositivo de acceso a la red. Cuando se visite un sitio, comprobar que realmente es al que se quiere acceder. La URL, empezará por https y mostrará un candado en la barra de direcciones. Cuando se haga clic sobre dicho candado, la URL también deberá estar bien escrita. Saber qué información manejan los navegadores Mantener el navegador actualizado a la última versión.

- Elegir complementos y plugins de confianza, descárgalos solo de sitios conocidos y con buena reputación como son las páginas oficiales de los navegadores. Instalar un verificador de páginas web, normalmente proporcionado por los principales antivirus. Revisar las opciones de configuración del navegador y habilitar aquellas que se consideren más interesantes para proteger la privacidad.

- Borrar el historial de navegación cuando no se necesita. Eliminar las cookies, ficheros que guardan información de los sitios que son visitados. Utilizar un gestor de contraseñas para almacenar y custodiar las claves de acceso y evitar así utilizar los navegadores como gestores de contraseñas. Cerrar siempre la sesión cuando salgas de una página en la que se haya autenticado con usuario y contraseña. Con esta acción se evita que si una persona utiliza el ordenador o un dispositivo móvil pueda acceder a la información personal usando la sesión que se ha dejado abierta. No publicar más información de la necesaria, hay cierto tipo de información que no debería ser publicada en los perfiles para que no comprometa la privacidad ni sea utilizada en contra de quien la pública, acarreando problemas o conflictos personales o laborales: Datos personales, Contraseñas, Datos bancarios, Teléfono móvil, Planes para las vacaciones, Comportamientos inapropiados Insultos, palabras malsonantes, Ideologías, Datos médicos o relativos a tu salud. Solo quien esté autorizado pueda acceder a la información.

- Se debe revisar las opciones de configuración de cada red social para tener controlados los principales aspectos de privacidad y seguridad: Conocer quién tiene acceso a las publicaciones efectuadas. Saber quién te puede etiquetar en una red social. Saber si el perfil está visible a los buscadores de Internet Conocer la geolocalización de las publicaciones, entre otros. Validar si la información publicada es veras.

4. CONTROL PARENTAL

- Pasos para activar el Control Parental en Sistema Operativo Windows 7, Windows 8 y Windows 8.1: a). Vamos a: Inicio -> Panel de control -> Cuentas de usuario y protección infantil. b) Pulsar sobre la opción Configurar el Control parental para todos los usuarios. (Se debe que confirmar la petición y, en algunos casos, escribir la contraseña de administrador). c) Se debe indicar la cuenta sobre la que se quiere establecer el Control Parental y dar click sobre la opción Activado, aplicar configuración actual. (Es conveniente que nuestros hijos tengan una cuenta personalizada, sin permisos de administrador para utilizar el computador personal, que no puedan utilizar la misma cuenta de los padres). d) Definidos estos parámetros podrá establecer los controles requeridos para su servicio: Límites de tiempo. Acceso a juegos. Permitir o bloquear programas específicos. Como activar el control Parental en Sistema Operativo Windows 10 PASOS: a). Hay que ir a la

opción: Configuración > Cuentas > Familia y otros usuarios. En Tu familia hay que pulsar sobre Agregar familiar. b). Se puede agregar un menor, por ejemplo, un Hijo, e indicar si puede o no iniciar sesión, entre otras opciones. c). Se debe que pulsar la opción, a continuación, sobre Administrar la configuración de la familia en línea con el fin de configurar el control parental. d). El último paso consiste en la personalización del control parental verificando los siguientes parámetros: Actividad reciente, Exploración web, Aplicaciones, juegos y multimedia, o Tiempo en pantalla. Configurar el Control Parental Computadoras Mac PASOS: a). Abrir el panel de preferencias Controles parentales, haz clic en el icono del candado para desbloquearlo y, a continuación, introduce un nombre y una contraseña de administrador. Selecciona el nombre de usuario del niño y, a continuación, haz clic en Activar controles parentales. b). Definir restricciones: Abre el panel de preferencias Controles parentales, haz clic en el icono del candado para desbloquearlo y, a continuación, introduce un nombre y una contraseña de administrador. Selecciona un usuario y, a continuación, haz clic en las pestañas de la parte superior. c). Apps: Especifica las apps a las que puedan acceder los niños. Si permites que el niño acceda a la tienda App Store, puedes especificar una clasificación de apps permitidas, de modo que el niño solo vea las apps adecuadas para su edad. d) Web: Limita el acceso a los sitios web o permite el acceso ilimitado. e) Personas: Limita los contactos del niño con otras personas a través de Game Center, del correo electrónico y de Mensajes. f). Límites de tiempo: Establece límites de tiempo para los días de entre semana, los fines de semana y las horas de acostarse. g). Otra: Oculta las palabrotas del diccionario y de otras fuentes, y bloquea el uso de la cámara integrada, Dictado, la grabación de discos CD y DVD, o el cambio de contraseña o de los ajustes de la impresora.