En cumplimiento a lo establecido en la **Resolución CRC 5050 de 2016, INFOTIC S.A** se permite compartir los Riesgos de seguridad relativos al servicio de internet y las acciones necesarias que los usuarios deben tomar para garantizar la seguridad en la red, los cuales se describen a continuación:

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. 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 e dad 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 INFOTIC S.A.

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

Proteger adecuadamente los dispositivos y descargas, 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 diez (10) caracteres y compuestas por mayúsculas, minúsculas, números y caracteres especiales. NO utilizar contraseñas fáciles de adivinar como: "12345678", "qwerty", "aaaaa", nombres de familiares o 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.

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, descárgarlos 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.

Habilite siempre que la aplicación lo permite la autenticación Multifactor(MFA). Por ejemplo la validación a través de mensaje de texto o alguna aplicación como Authy, Google.

Utilizar un gestor de contraseñas para almacenar y custodiar las claves de acceso y evitar así utilizar los navegadores como gestores de contraseñas. Existen opciones gratuitas como Keepass, AuthPass, o puede hacer uso de las versiones de pago que permiten en algunos casos la autenticación Multifactor.

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 veraz, En la Red circula un sinfín de falsas noticias que a menudo generan inquietud sin ningún fundamento en aquellas personas que las reciben. Con frecuencia estas falsas noticias se utilizan para realizar engaños haciendo que el usuario acceda a un sitio web infectado, que está siendo utilizado para propagar software malicioso. Por tanto, se debe tener en cuenta que: Detrás de estos mensajes pueden esconderse campañas de estos.

Utilizar programas de control parental: Son programas que realizan una función de análisis detallado de las palabras claves definidas y de los listados con sitios web autorizados o prohibidos. Además, permiten limitar la cantidad de tiempo de navegación y determinar horarios para permitir el acceso a Internet, también impiden el acceso a sus datos personales, bloquean el acceso a ciertas informaciones, etc. Lo más importante es tener en cuenta que estas herramientas son solo una ayuda, no nos garantizan la seguridad de nuestros hijos en Internet, son los padres los que mejor asistiremos a nuestros niños.

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 tales como:

Límites de tiempo, acceso a juegos, permitir o bloquear programas específicos.

Como activar el control Parental en Sistema Operativo Windows:

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 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:

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.

Para teléfonos celulares puede utilizar la aplicación Family Link para Android o control parental para Iphone.