Recomendaciones de seguridad para uso de Internet

COLOMBIANET como proveedor del servicio de conectividad a Internet está convencido de que las relaciones con nuestros clientes se deben fortalecer desde una comunicación asertiva, sana y orientada a proporcionar las herramientas y consejos prácticos necesarios para la protección adecuada de los elementos de cómputo y los servicios asociados a la Internet.

Por esta razón COLOMBIANET pone a disposición de todos nuestros clientes y de la comunidad en general, las siguientes recomendaciones, prácticas y conceptos teóricos que permitan evitar o reducir los riesgos a los que se exponen cuando se interactúa con la Internet y sus elementos asociados.

Glosario de términos de Seguridad Informática.

- **Activo.** Recurso, procedimiento, sistema u otra cosa que tenga valor para la organización y por lo tanto debe ser protegida, los activos pueden ser bienes físicos tales como equipos de cómputo y maquinaria, como también puede ser información y propiedad intelectual.

- **Amenaza.** Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada, si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad.

- **Anti-spam.** Programa capaz de detectar, controlar y eliminar correos spam.

- **Antivirus.** Es un programa informático específicamente diseñado para detectar, bloquear y eliminar código malicioso (virus, troyanos, gusanos, etc.), así como proteger los equipos de otros programas peligrosos conocidos genéricamente como malware. La forma de actuar del antivirus parte de una base de datos que contiene parte de los códigos utilizados en la creación de virus conocidos. El programa antivirus compara el código binario de cada archivo ejecutable con esta base de datos, además de esta técnica, se valen también de procesos de monitorización de los programas para detectar si éstos se comportan como programas maliciosos.

- **Backup.** Copia de seguridad que se realiza sobre ficheros o aplicaciones contenidas en un dispositivo con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados. Los dispositivos más empleados para llevar a cabo la técnica de Backup pueden ser discos duros, discos ópticos, USB o DVD. También es común la realización de copias de seguridad mediante servicios de copia basados en la nube,

es de suma importancia mantener actualizada la copia de seguridad, así como tener la máxima diligencia de su resguardo, para evitar pérdidas de información que pueden llegar a ser vitales para el funcionamiento ya sea de una empresa, institución o de un contenido de tipo personal; además, cada cierto tiempo es conveniente comprobar que la copia de seguridad puede restaurarse con garantías.

- **Bomba lógica.** Porción de código insertado intencionalmente en un programa informático que permanece oculto hasta cumplirse una o más condiciones pre programadas, momento en el que se ejecuta una acción maliciosa. La característica general de una bomba lógica y que lo diferencia de un virus es que este código insertado se ejecuta cuando una determinada condición se produce, por ejemplo, tras encender el dispositivo una serie de veces, o pasados una serie de días desde el momento en que la bomba lógica se instaló en nuestro dispositivo.

- **Cartas nigerianas.** Se trata de una comunicación inesperada mediante correo electrónico carta o mensajería instantánea en las que el remitente promete negocios muy rentables, la expectativa de poder ganar mucho dinero mediante unas sencillas gestiones, es el gancho utilizado por los estafadores para involucrar a las potenciales víctimas en cualquier otra situación engañosa, procurando que finalmente transfiera una fuerte cantidad de dinero para llevar a cabo la operación. El funcionamiento es muy variado, pero a grandes rasgos se podría resumir así: Un remitente desconocido contacta con la potencial victima haciéndose pasar por un abogado, familiar o amigo cercano de un miembro del gobierno o de un importante hombre de negocios que ha perdido la vida en un accidente o similar. Según esta comunicación, antes de morir esa persona, depositó una gran cantidad de dinero en una cuenta bancaria. El remitente asegura que tiene acceso legal a esa cuenta y pretende transferir el dinero a una cuenta en el extranjero. El remitente ha encontrado el nombre y la dirección de la víctima por recomendación de otra persona o por casualidad y la víctima es la única persona de confianza que puede ayudarle a realizar la transferencia del dinero. Por su asistencia, promete a la víctima, un porcentaje de la cantidad total de dinero y solicita discreción para llevar a cabo el negocio. La víctima debe abrir una cuenta en un banco determinado para que pueda remitirle el dinero y generalmente pagar por adelantado unos gastos para la transferencia del dinero. La siguiente fase del fraude consiste en convencer a la víctima de que la transferencia de dinero está en proceso. Para ello, mandan a la víctima documentos aparentemente oficiales, al igual que cartas y movimientos bancarios falsos. Sin embargo, esta transferencia del dinero por parte de los estafadores nunca llega a tener lugar.

- **Ciberbullying.** Es un tipo de agresión psicológica que ocurre a través de las redes sociales. Se generan insultos, rechazos, humillaciones y exclusiones constantes entre los contactos de la red social hacia alguno de sus miembros. Normalmente los menores de edad, en etapa escolar, son los más afectados.

- **Cifrado.** Proceso de transformar texto plano a texto cifrado.

- **Confidencialidad**. Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad de la información constituye la piedra angular de la seguridad de la información.

- **Control parental.** Conjunto de herramientas o medidas que se pueden tomar para evitar que los menores de edad hagan un uso indebido del ordenador, accedan a contenidos inapropiados o se expongan a riesgos a través de Internet. Estas herramientas tienen la capacidad de bloquear, restringir o filtrar el acceso a determinados contenidos o programas, accesibles a través de un dispositivo o de la red, y de dotar de un control sobre el equipo y las actividades que se realizan con él, a la persona que sea el administrador del mismo, que normalmente deberá ser el padre o tutor del menor.

- **Criptografía.** Es el arte de cifrar y descifrar información con claves secretas, donde los mensajes o archivos sólo puedan ser leídos por las personas a quienes van dirigidos, evitando la interceptación de éstos.

- **DNS.** El término DNS, del inglés *Domain Name Service*, se refiere tanto al servicio de Nombres de Dominio, como al servidor que ofrece dicho servicio. El servicio DNS asocia un nombre de dominio con información variada relacionada con ese dominio, su función más importante es traducir nombres inteligibles para las personas en direcciones IP asociados con los sistemas conectados a la red con el propósito de poder localizar y direccionar estos sistemas de una forma mucho más simple.

- **Disponibilidad.** Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.

- **Exploit.** Secuencia de comandos utilizados para aprovechar fallos o vulnerabilidades en un sistema, provocar un comportamiento no deseado o imprevisto. Mediante la ejecución de Exploit se suele perseguir el acceso a un sistema de forma ilegítima, obtención de permisos de administración en un sistema ya accedido o un ataque de denegación de servicio a un sistema.

- **Firewall.** Sistema de seguridad compuesto o bien de programas (software) o de dispositivos hardware situados en los puntos limítrofes de una red que tienen el objetivo de permitir y limitar, el flujo de tráfico entre los diferentes ámbitos que protege sobre la base de un conjunto de normas y otros criterios. La funcionalidad básica de un firewall es asegurar que todas las comunicaciones entre la red e Internet se realicen conforme a las políticas de seguridad de la organización o

corporación. Estos sistemas suelen poseer características de privacidad y autentificación.

- **Grooming.** Ocurre cuando una persona adulta se hace pasar por un menor de edad para entablar una relación y ganarse la confianza de otro, con el fin de manipularlo y lograr que éste realice acciones que no son propias de su edad, normalmente de tipo sexual.

- **Gusano.** Es un programa malicioso (o malware) que tiene como característica principal su alto grado de «dispersabilidad», es decir, lo rápidamente que se propaga, mientras que los troyanos dependen de que un usuario acceda a una web maliciosa o ejecute un fichero infectado, los gusanos realizan copias de sí mismos, infectan a otros dispositivos y se propagan automáticamente en una red independientemente de la acción humana. Su fin es replicarse a nuevos sistemas para infectarlos y seguir replicándose a otros equipos informáticos, aprovechándose de todo tipo de medios como el correo electrónico, IRC, FTP, P2P y otros protocolos específicos o ampliamente utilizados.

- **Incidente de seguridad.** Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

- **Ingeniería social.** Tácticas utilizadas para obtener información de naturaleza sensible, en muchas ocasiones claves o códigos, de una persona, estas técnicas de persuasión suelen valerse de la buena voluntad y falta de precaución de la víctima, entregando al atacante la información necesaria para superar las barreras de seguridad.

- **Integridad.** La Integridad es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales. La integridad, la disponibilidad y la confidencialidad constituyen las dimensiones claves en la seguridad de la información, ya que, de un lado, se pretende evitar los accesos no autorizados a los datos, y de otro, se garantiza la no alteración de los mismos.

- **Malware.** Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de software malintencionado: *malicious software*. Dentro de esta definición tiene cabida un amplio elenco de programas maliciosos: virus, gusanos, troyanos, backdoors, spyware, etc. La nota común a todos estos programas es su carácter dañino o lesivo.

- **No repudio.** El no repudio en el envío de información a través de las redes es la capacidad de demostrar la identidad del emisor de esa información. El objetivo que se pretende es certificar que los datos, o la información, provienen realmente de la fuente que dice ser.

- **P2P.** (del inglés *Peer-to-Peer*) es un modelo de comunicaciones entre sistemas o servicios en el cual todos los nodos/extremos son iguales, tienen las mismas capacidades y cualquiera de ellas puede iniciar la comunicación. Se trata de un modelo opuesto al cliente/servidor en donde el servidor se encuentra a la espera de una comunicación por parte del cliente. El modelo P2P se basa en que todos los nodos actúan como servidores y clientes a la vez. Una red P2P es por tanto una red de sistemas o servicios que utiliza un modelo P2P. Todos los sistemas/servicios conectados entre sí y que se comportan como iguales con un objetivo en común. Por ejemplo, las botnets P2P utilizan este modelo para evitar que haya un servidor central único fácilmente detectable.

- **Phishing.** Es la capacidad de duplicar una página Web para hacer creer al visitante que se encuentra en la página original en lugar de la copiada, este delito consiste en obtener información sensible de la víctima tales como contraseñas, información de cuentas, números de tarjetas de crédito o débito por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes. En esta modalidad de fraude, el usuario malintencionado envía millones de mensajes falsos que parecen provenir de sitios Web reconocidos o de su confianza, como un banco o la empresa de su tarjeta de crédito. Dado que los mensajes y los sitios Web que envían estos usuarios parecen oficiales, logran engañar a muchas personas haciéndoles creer que son legítimos, la gente confiada normalmente responde a estas solicitudes de correo electrónico con sus números de tarjeta de crédito, contraseñas, información de cuentas u otros datos personales. Para que estos mensajes parezcan aún más reales, el estafador suele incluir un vínculo (link) falso que parece dirigir al sitio Web legítimo, pero en realidad lleva a un sitio falso o incluso a una ventana emergente que tiene exactamente el mismo aspecto que el sitio Web oficial. Estas copias se denominan "sitios Web piratas". Una vez que el usuario está en uno de estos sitios Web, introduce información personal sin saber que se transmitirá directamente al delincuente, que la utilizará para realizar compras, solicitar una nueva tarjeta de crédito o robar su identidad.

- **Pornografía Infantil.** Es la representación de actividades sexuales, mediante fotos o videos que involucran a menores de edad.

- **Ransomware.** El ciber-delincuente, toma control del equipo infectado y «secuestra» la información del usuario cifrándola, de tal forma que permanece ilegible si no se cuenta con la contraseña de descifrado. De esta manera extorsiona al usuario pidiendo un rescate económico a cambio de esta contraseña para que,

supuestamente, pueda recuperar sus datos, la seguridad del sistema está basada en la dificultad de factorización de grandes números. Su funcionamiento se basa en el envío de un mensaje cifrado mediante la clave pública del destinatario, y una vez que el mensaje cifrado llega, éste se encarga de descifrarlo con su clave privada.

- **Red Privada Virtual**. También conocida por sus siglas VPN (*Virtual Private Network*) es una tecnología de red que permite una extensión segura de una red local (LAN) sobre una red pública o no controlada como Internet. Al establecerlas, la integridad de los datos y la confidencialidad se protegen mediante la autentificación y el cifrado. Se trata realmente de una conexión virtual punto a punto entre dos redes LAN usando para la conexión una red pública como es Internet y consiguiendo que esta conexión sea segura gracias al cifrado de la comunicación.

- **Riesgo.** Es un hecho potencial, que en el evento de ocurrir puede impactar negativamente la seguridad, los costos, la programación o el alcance de un proceso de negocio o de un proyecto. Correo electrónico: El correo electrónico es un servicio de red que permite que los usuarios envíen y reciban mensajes incluyendo textos, imágenes, videos, audio, programas, etc., mediante sistemas de comunicación electrónicos.

- **Seguridad de la Información.** Son aquellas acciones que están encaminadas al establecimiento de directrices que permitan alcanzar la confidencialidad, integridad y disponibilidad de la información, así como la continuidad de las operaciones ante un evento que las interrumpa.

- **Sexting.** Es una práctica común entre jóvenes y parejas que incluye el envío de imágenes y videos personales con contenido erótico. En este tipo de prácticas existe el riesgo de que quien recibe el material haga un uso indebido de éste y la información sea expuesta de forma pública en la red. La manipulación también es uno de los riesgos de practicar Sexting, ya que, para evitar que su información privada sea difundida, la víctima debe acceder a las exigencias del agresor.

- **Smishing.** Utilización de técnicas de Phishing en los mensajes de texto de teléfonos móviles.

- **Spam.** Envío de cualquier correo electrónico, masivo o no, a personas a través de este medio que incluyen temas tales como pornografía, bromas, publicidad, venta de productos, entre otros, los cuales no han sido solicitados por el(los) destinatario(s).

- **Troyano.** Se trata de un tipo de malware o software malicioso que se caracteriza por carecer de capacidad de auto replicación. Generalmente, este tipo de malware requiere del uso de la ingeniería social para su propagación. Una de las

características de los troyanos es que al ejecutarse no se evidencian señales de un mal funcionamiento; sin embargo, mientras el usuario realiza tareas habituales en su dispositivo, el programa puede abrir diversos canales de comunicación con un equipo malicioso remoto que permitirán al atacante controlar nuestro sistema de una forma absoluta.

- **Vishing.** Utilización de técnicas de Phishing para servicios asociados con voz sobre IP (VoIP).

- **Virus.** Es un programa que se copia automáticamente y que tiene por objeto alterar el normal funcionamiento del dispositivo, sin el permiso o el conocimiento del usuario. Los virus pueden destruir, de manera intencionada, los datos almacenados en un dispositivo, aunque también existen otros más "benignos", que solo se caracterizan por ser molestos. Los virus informáticos tienen, básicamente, la función de propagarse, replicándose, pero algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

- **Vulnerabilidad.** Fallos o deficiencias de un programa que pueden permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota. Los agujeros de seguridad pueden ser aprovechadas por atacantes mediante Exploit, para acceder a los sistemas con fines maliciosos. Las empresas deben ser conscientes de estos riesgos y mantener una actitud preventiva, así como llevar un control de sus sistemas mediante actualizaciones periódicas.

Recomendaciones de seguridad

- Si no se reconoce un remitente de un correo, no abrir los archivos adjuntos del mensaje, incluso si usted tiene un software antivirus y/o filtro de aplicación ejecutándose en su dispositivo, los archivos adjuntos a menudo incluyen software o aplicaciones malintencionadas que pueden tener efectos muy negativos sobre su dispositivo. Evite caer en técnicas conocidas como de Ingeniería social en la cual llega un correo electrónico con un mensaje del estilo "ejecute este programa y gane un premio". Evitar la instalación de software pirata o de baja calidad, mediante la utilización de redes P2P, ya que muchas veces, existen ciertos sitios que "prometen" la descarga de un aplicativo en particular, pero en realidad lo que el usuario descarga es un programa malicioso.
- No publique su cuenta de correo en sitios no confiables.
- No preste su cuenta de correo ya que cualquier acción será su responsabilidad.
- No divulgue información confidencial o personal a través del correo.
- Si un usuario recibe un correo con una advertencia sobre su cuenta bancaria, no debe contestarlo.

- Nunca responda a un correo HTML con formularios embebidos.
- Asegurarse que su dispositivo cuente con las últimas actualizaciones a nivel de seguridad tanto a nivel de sistema operativo como de los aplicativos instalados, dadas por el fabricante. Existen algunos tipos de virus que se propagan sin la intervención de los clientes y que aprovechan debilidades de seguridad de los diferentes sistemas y aplicaciones, por ejemplo, los virus Blaster y Sasser.
- Instalar software antivirus en el dispositivo, que esté actualizado con las últimas firmas dadas por el fabricante respectivo, además de tener en su equipo elementos como anti-spyware y bloqueadores de pop-up (ventanas emergentes).
- Nunca responda a solicitudes de información personal a través de correo electrónico, si tiene alguna duda, póngase en contacto con la entidad que supuestamente le ha enviado el mensaje. Tener especial cuidado en correos que supuestamente han sido enviados por entidades financieras y compras por Internet, como eBay, PayPal, bancos, etc. Solicitando actualizar datos de cuentas y/o accesos, ya que ninguna de estas entidades solicita este tipo de información por este medio. Asegúrese que su dispositivo cuente con las últimas actualizaciones a nivel de seguridad dadas por los fabricantes.
- Asegúrese de que el sitio Web utiliza cifrado.
- Si tiene instalado servidores Web, asegúrese que tanto el aplicativo como el sistema operativo cuenten con las últimas actualizaciones a nivel de seguridad dadas por los fabricantes correspondientes. Muchas veces los atacantes buscan en la red servidores Web vulnerables que puedan ser utilizados para montar páginas que intentan suplantar la identidad de una entidad financiera, sin que el usuario se dé cuenta. Para el cliente, esto tiene como repercusión la afectación directa en su servicio de Internet, ya que la IP donde se encuentra alojada la página fraude es reportada por entidades internacionales pidiendo al ISP (COLOMBIANET) el bloqueo de la misma.
- Comunique los posibles delitos relacionados con su información personal a las autoridades competentes.
- Evite el envío de mensajes cadena, pornografía, mensajes no solicitados, bromas a otros remitentes de correo.
- Si usted es un usuario frecuente portales donde se ingresan datos personales, manténgase actualizado, consultando en la página de la policía nacional http://www.policia.gov.co/, CAI virtual, los últimos eventos, recomendaciones y consultas en línea.
- Para visitar sitios Web, ingrese directamente al sitio oficial desde el navegador, nunca desde el enlace enunciado en el correo, ni ingresar a dicho enlace. Cuando ingrese al sitio, valide que la seguridad que se indica a través de certificados digitales, si estén respaldados. Conozca de antemano cual es la dirección o URL del sitio real y valide este nombre cada que ingrese a realizar un proceso donde deba ingresar sus datos, recuerde que el atacante utiliza técnicas que pueden engañar la percepción del sitio cuando se lee.
- Evite alojar, publicar o trasmitir información, mensajes, gráficos, dibujos, archivos de sonido, imágenes, fotografías, grabaciones o software que en forma indirecta o

directa se encuentren actividades sexuales con menores de edad, en los términos de la legislación internacional o nacional, tales como la Ley 679 de 2001 y el Decreto 1524 de 2002 o aquella que la aclare, modifique o adicione o todas las leyes que lo prohíban.

- Se debe tener en cuenta según la Sentencia SP-9792 (42307), Jul. 29/15, M. P. Patricia Salazar) los padres pueden tener acceso a los correos y redes sociales de sus hijos menores de edad.
- Generar espacios de diálogo y conversación que sirvan para conocer los intereses y comportamientos de los niños y adolescentes frente al uso de la tecnología.
- Comunicar a la familia, personas de confianza o autoridades, situaciones negativas que se generan a través de los medios tecnológicos.
- Pensar antes de publicar: enseñarle a los niños y adolescentes a pensar en el mundo virtual como una prolongación de su vida real, por lo que es importante tener prudencia a la hora de publicar contenidos de su vida privada.
- Respetar a los demás y cuidar las palabras que se utilizan en las redes sociales.
- Mantener en secreto las contraseñas y no utilizar nombres ni fechas de nacimiento en ellas, es clave para evitar riesgos. Además, cuando se ingrese desde un computador diferente al personal, siempre se debe cerrar sesión.
- Verificar qué información personal aparece en Internet: para esto se puede usar un buscador como Google y poner el nombre de la persona que se desea encontrar; aparecerá toda la información pública que se encuentra en la red sobre esta persona.
- Utilizar los sistemas de protección como bloqueo de páginas, programas y software que permiten alertar y monitorear sobre lo que los niños están viendo y haciendo en Internet.
- Asegúrese que se aplican las actualizaciones en sistemas operativos y navegadores Web de manera regular.
- Si sus programas o el trabajo que realiza en su computador no requieren de pop-up, Java support, ActiveX, Multimedia Autoplay o auto ejecución de programas, deshabilite estos.
- Si así lo requiere, obtenga y configure el firewall personal, esto reducirá el riesgo de exposición.
- Si ingresa la clave en un sitio no confiable, procure cambiarla en forma inmediata para su seguridad y en cumplimiento del deber de diligencia que le asiste como titular de la misma.
- No reenvíe los correos cadenas, esto evita congestiones en las redes y el correo, además el robo de información contenidos en los encabezados.
- No divulgue información confidencial suya o de las personas que lo rodean.
- No hable con personas extrañas de asuntos laborales o personales que puedan comprometer información.
- Utilice los canales de comunicación adecuados para divulgar la información.

- Si un usuario recibe un correo, llamada o mensaje de texto con una advertencia sobre su cuenta bancaria, no debe contestarlo.
- Para los sitios que indican ser seguros, revise su certificado SSL.
- Valide con la entidad con quien posee un servicio, si el mensaje recibido por correo es válido.
- Cambie sus contraseñas frecuentemente, mínimo cada 30 días.
- Use contraseñas fuertes: fácil de recordar y difícil de adivinar.
- Evite fijar contraseñas muy pequeñas, se recomienda que sea mínimo de una longitud de 12 caracteres alfanuméricos y caracteres especiales.
- No envíe información de claves a través del correo u otro medio que no esté encriptado.
- Si recibe un correo spam, nunca haga clic en el vínculo "Quitar spam", ya que lo que buscan los atacantes es que el cliente verifique que esta dirección de correo está activa, añadiendo posiblemente su cuenta de correo a más y más listas de spam, lo cual ocasionará que usted reciba mayor cantidad de correo no deseado.
- Si tiene instalado servidores de correo, asegúrese que tanto el aplicativo como el sistema operativo cuenten con las últimas actualizaciones a nivel de seguridad dadas por los fabricantes correspondientes. En muchos casos, los servidores de correo, debido a configuraciones deficientes, permiten que cualquier persona, desde Internet, utilice estos servidores para enviar correos (conocido como Open Relay), afectando el servicio de correo del cliente y muy posiblemente será bloqueado en listas negras de Spam mantenidas a nivel mundial.
- En caso que usted como cliente tenga problemas en el envío de correos, para verificar que su IP pública no se encuentra reportada en listas negras de spam, puede revisar los siguientes enlaces para realizar la consulta: https://mxtoolbox.com/.
- Se debe tener en cuenta el tiempo de desbloqueo de parte del sitio Web que realizó el reporte, entre los mas frecuentes están los siguientes:
    - www.aol.com: tiempo de desbloqueo aproximado 48 horas.
    - www.lashback.com: tiempo de desbloqueo aproximado 1 hora.
    - www.spamcop.net: tiempo de desbloqueo aproximado 24 horas.
    - www.dsbl.org: tiempo de desbloqueo aproximado 1 hora.
    - www.uceprotect.net: tiempo de desbloqueo aproximado 7 días.
    - www.spamhaus.org: tiempo de desbloqueo aproximado 24 horas.
    - www.abuso.cantv.net: tiempo de desbloqueo aproximado 48 horas.
    - www.comcast.com: tiempo de desbloqueo aproximado 48 horas.
    - www.moensted.dk: tiempo de desbloqueo aproximado 1 hora.
    - www.wpbl.info: tiempo de desbloqueo aproximado 1 hora.

Mecanismos de seguridad

COLOMBIANET ha implementado configuraciones de seguridad de la red en sus equipos perimetrales, reduciendo el nivel de impacto ante los riesgos potenciales, adicional a ello los clientes pueden realizar el filtrado de URLs través de sus navegadores Web debido a

que Internet es vasto y sin censura, este puede ser una fuente de material peligroso para los niños y jóvenes, por lo cual los padres deben desempeñar un papel activo para asegurarse que el contenido visitado sea seguro y confiable para ellos; existen diferentes herramientas de control parental que permiten limitar el acceso de los menores a contenidos inapropiados; a continuación se describen los pasos para el filtrado de URL y se sugiere la utilización de los siguientes programas para control parental, las cuales pueden descargarse de los links adjuntos.

Para realizar el control parental en cada uno de los navegadores se debe seguir los siguientes pasos:

- Para Chrome, abra las preferencias () y active el "Filtros SafeSearch".
- Para internet Explorer, abra la pestaña de "herramientas" de la parte superior derecha. De clic en "opciones de Internet" -> contenidos -> clic en habilitar.
- Para el navegador Mozilla Firefox, se puede descargar el complemento "BlockSite" y "Anti-Porn Pro".
- Para el navegador Safari, ingrese a Preferencias del sistema> Usuarios y grupos>Limitar acceso a sitios de adultos.
- Para el navegador Opera, active la extensión Adult Blocker.

COLOMBIANET no se hace responsable por el uso de software en los dispositivos del cliente, se sugiere las siguientes herramientas para control parental:

- https://www.spyrix.com
- https://kidlogger.net
- https://family.norton.com/web
- https://www.netnanny.com
- https://www.cyberpatrol.com
- http://www.qustodio.com

Adicionalmente de los programas mencionados anteriormente, otra solución es el uso de DNS, además de los más usados como los de Google o Cloudfire, existen algunos DNS que sirven para proteger la red de ingreso a páginas no deseadas, los cuales son:

- DNS de OpenDNS FamilyShield, los cuales permiten filtrar automáticamente todas las páginas que no sean consideradas aptas para menores, estos son:

- 208.67.222.123
- 208.67.220.123

- DNS de Norton ConnectSafe también permite proteger a los menores de contenido no apropiado:
  - 199.85.126.30
  - 199.85.127.30

- Por último, los DNS Family que al igual que los anteriores, permiten filtras todo tipo de contenido inapropiado.
  - 77.88.8.7
  - 77.88.8.3

Limitaciones de acceso

Si bien se cuenta con mecanismos de seguridad, filtrado y se hace un control de navegación acorde a los estipulado en la ley (en especial la ley 679 de 2001 y sus decretos reglamentarios), en ningún caso COLOMBIANET restringe, bloquea o hace uso de software o programas que eviten la libre navegación y acceso a Internet (salvo lo estipulado en la ley), por consiguiente, COLOMBIANET no tiene limitaciones en el acceso hacia Internet para sus clientes y usuarios, dando cumplimiento a lo estipulado por el ministerio de las TIC.

Atentamente;

Área de prevención de riesgos en internet de **COLOMBIANET Y SEPCOM S.A.S.**