NEUTRALIDAD Y SEGURIDAD DE LA RED
CONETWORK

Compunetwork Renting S.A.S. Como Proveedor de Redes y Servicio de Telecomunicaciones (PRST) y Proveedor de Servicio de Internet (ISP) habilitado mediante Registro Único de TIC N° 96005445 del 08 de Julio de 2020, se acoge al cumplimiento normativo en lo relacionado a la Ley 1450 de 2011 artículo 56 y la Ley 1341; como también a lo dispuesto en la Resolución CRC 3502 de 2011. Por lo cual valiéndose de la responsabilidad inherente al actuar de su objeto social, da cumplimiento a la Neutralidad y Seguridad de la Red, así:

PRINCIPIOS

Libertad: *Nuestros usuarios de Internet tendrán completa libertad, bajo propia responsabilidad, para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio lícito a través de la red. Nosotros nos abstenemos de realizar cualquier distinción arbitraria de contenidos, aplicaciones o servicios, basados en la fuente de origen o propiedad de estos.*
No obstante realizaremos ofertas según las necesidades que identifiquemos y puedan ser de interés para nuestros usuarios de acuerdo con sus perfiles de uso y consumo.
Igualmente no limitaremos el derecho de nuestros usuarios a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos en la red, siempre que sean legales y que los mismos no dañen o perjudiquen la red o la calidad del servicio.

No Discrimiación: *Nos comprometemos y garantizamos un trato igualitario a los contenidos, aplicaciones y servicios, sin ningún tipo de discriminación arbitraria, en especial en razón al origen o propiedad de los mismos.*
No obstante realizaremos ofertas según las necesidades que identifiquemos y puedan ser de interés para nuestros usuarios de acuerdo con sus perfiles de uso y consumo lo cual no se entenderá como discriminación.

Transparencia: *Como PRST que prestamos servicios de acceso a Internet, publicamos nuestras políticas de gestión de tráfico, las cuales pueden ser consultadas en nuestro documento "Políticas de gestión de tráfico". Clic Aquí*

Información: *Al adquirir un plan de servicio de internet fijo, el cliente/suscriptor recibe de nuestra parte: el acta de entrega del servicio donde se especifica datos del servicio y equipamiento, así mismo, un contrato donde se consigna los datos del suscriptor, cláusulas del servicio y detalles mismo (velocidad del plan, calidad del servicio, entre otros aspectos). En todo caso los documentos deberán ir firmados debidamente por el operador y el cliente/suscriptor y ambas partes conservarán copia de este documento.*

COMPROMISOS

Así mismo, dando cumplimiento a la normativa vigente y sin perjuicio de lo establecido en la Ley 1336 de 2006, nos comprometemos a:

1. No bloquear, interferir, discriminar, ni restringir el derecho de cualquier usuario de Internet, para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio lícito a través de Internet. Ofreciendo a cada usuario un servicio de acceso a Internet o de conectividad, que no distinga arbitrariamente contenidos, aplicaciones o servicios, basados en la fuente de origen o propiedad de estos.

2. No limitar el derecho del usuario/suscriptor a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos en la red, siempre que sea legal y que no dañe o perjudique la red o la calidad del servicio.

3. Ofrecer servicio de control parental para contenidos que atenten contra la ley, para lo cual, desde los nodos y cabeceras de la red de acceso, implementaremos las políticas de gestión de tráfico. Así mismo brindaremos consejos aplicables a nivel local para que el usuario final pueda configurar estos servicios en sus máquinas. Ejemplo el control parental para computadores con sistema operativo Microsoft.

4. Brindar información relevante, desde nuestro sitio web, de nuestros servicios como son sus características, alcance y cobertura.

5. Implementar mecanismos para preservar la privacidad del usuario/suscriptor, contra virus y la seguridad de la red.

6. Bloquear el acceso a determinados contenidos, aplicaciones o servicios, sólo a pedido expreso del usuario.

CALIDAD DEL SERVICIO

Nuestros clientes/suscriptores actuales podrán hacer revisión de la calidad del servicio de acceso a internet realizando un test de velocidad, donde podrán apreciar la tasa efectiva del Ancho de Banda contrato.
Hacer test de velocidad: https://www.speedtest.net/es
Debido a que nuestro segmento de mercado es corporativo y nuestra base de suscriptores está por debajo del 1% de la tasa nacional, nos acogemos a lo indicado en la *Resolución CRC 5050 de 2016, artículo 5.1.4.4. y, al Anexo 5.1-B, Parte 2, literal A* donde quedamos por fuera de medir y reportar algún indicador de calidad del servicio. No obstante, los indicadores de disponibilidad de nuestros nodos son reportados a MinTIC mes tras mes y pueden ser consultados Aquí.

BLOQUEO DE CONTENIDOS

Nos acogemos al principio de libre elección del cual trata la Resolución CRC 3502 de 2011, artículo 3, numeral 3.1. Sin embargo, aplicamos las *"Políticas de gestión de tráfico". Conózcalas Aquí* por las cuales restringimos el acceso a contenidos de pornografía infantil de acuerdo a la Ley 679 de 2001, así como a las URL informadas por las autoridades competentes que estén prohibidas o restringidas.

SEGURIDAD DE LA RED

De conformidad al artículo 2.9.2.3. de la Resolución 5050 de 2016 COMPUNETWORK dispondrá "...los recursos técnicos y logísticos tendientes a garantizar y preservar la seguridad de la red, la inviolabilidad de las comunicaciones, la protección contra virus y la integridad del servicio, utilizando las herramientas tecnológicas disponibles y modelos de seguridad, de acuerdo con las características y necesidades propias de su red de acceso, de conformidad con lo definido por la UIT en las recomendaciones de la serie X.700 y X.800, en relación con la autenticación, acceso, no repudio, confidencialidad de datos, integridad de datos y disponibilidad…", así mismo "...implementará modelos de seguridad que eviten el acceso no autorizado, la interrupción, el repudio o la interferencia deliberada de la comunicación, utilizando modelos cifrados, firmas digitales y controles de acceso…" En este sentido las acciones implementadas que nos permiten dar cumplimiento y garantizar la Seguridad de la red son mediante:

- **Filtrado de DNS.** Nos referimos a bloquear el acceso a determinados contenidos web para impedir que aparezcan en los resultados de búsqueda o que se puedan descargar. Filtrar por DNS es una manera de prevenir el acceso a contenidos específicos, como, por ejemplo, a sitios web que contienen pornografía infantil u otros tipos de materiales ilegales o prohibidos.
El filtrado de DNS, por tanto, protege a los usuarios y sus dispositivos y a los propietarios de redes, ya que permite y garantiza el cumplimiento de las normativas nacionales.

- **Filtrado de contenidos.** Internet ha invadido cada aspecto de nuestra vida. En Internet es donde trabajamos, aprendemos, escuchamos música, vemos vídeos, encontramos soluciones a problemas de salud y hacemos compras en tiendas online. El Internet es nuestro todo. Si es verdad que tiene muchas ventajas, en términos de comodidad y eficiencia, también es verdad que plantea riesgos.
Sabemos perfectamente que Internet tiene un lado oscuro-la dark web o red oscura-, donde encontramos imágenes sórdidas, armas ilegales, identidades robadas y muchísimo más. El problema es que no hace falta ir tan a fondo para dar con contenidos inapropiados. En realidad, incluso cuando buscamos los contenidos más inofensivos corremos el riesgo de toparnos con resultados

desagradables. Aquí es donde entra en juego el filtrado de contenidos lo cual también está en paralelo y concordancia con el bloqueo de contenidos.
Igualmente establecemos preferencias para las CDN -Red de distribución de contenidos (Content delivery network)- y fortalecer las medidas.

- **Protección contra el malware.** El malware es un problema universal, y la protección contra el malware un ámbito técnico altamente especializado. En esta sección aplicamos la tecnología proporcionada por FlashStart para encarar el problema, pues incluye funciones de seguridad y de buenas prácticas para uso y administración de la red.

- **Tecnología de filtrado de URL.** En concomitancia con los diferentes elementos de seguridad de nuestra red, empleamos la tecnología del servicio de FlashStart para filtrar la red basándose en las URL.

- **Lista negra normativa.** Restricción de acceso a sitios web específicos indicados por las autoridades competentes, por ejemplo los que contienen contenido de pornografía infantil. Esto con el propósito de prevenir y combatir la pornografía infantil en Internet. Además se restringe otras URL identificadas e informadas por las autoridades competentes consideradas ilegales como son las de juegos de azar.

- **Redundancia.** Redundancia mediante la tecnología -Red Anycast-**.** La nube de FlashStart cuenta con muchos puntos de conexión en todo el mundo. Cada punto de conexión se apoya en hardware de redundancia. Si se pierde un punto de conexión, se recurre automáticamente a la red de DNS ANYCAST para transferir el tráfico a un punto de conexión cloud alternativo, sin que se produzca una interrupción del servicio.

- **Privacidad de datos.** Damos cumplimiento a la Ley 1581 de 2012 y a la Resolución MinTIC 1377 de 2013, mediante procesos administrativos integrales para garantizar la Protección de Datos personales de nuestros clientes/suscriptores.

- **HTTPS.** Aplicamos certificados de seguridad nativos los cuales se integran con el protocolo HTTP. Y mediante la tecnología de FlashStart, bloqueamos contenido sin confundir al usuario con un mensaje de error 404.

- **DNS sobre HTTPS (DoH).** DoH es un importante estándar de cifrado de alta intensidad computacional y amenaza con ralentizar el funcionamiento de la nube, si no se maneja adecuadamente. FlashStart usa una tecnología de vanguardia para un desempeño eficiente del cifrado DoH.

PROTECCIÓN CONTRA ATAQUES:

- **Protección ARP Spoofing.** Esta medida de protección evita la suplantación del gateway de la red para capturar todo el tráfico. Se

bloquea el ataque cuando se detecta el envío de mensajes ARP falsos a la red con el objetivo de vincular su dirección MAC con la IP de un equipo legítimo en dicha red.

- **Protección MAC Flooding.** El ataque por inundación de direcciones MAC (MAC Flooding) consiste en enviar miles de direcciones MAC falsas hacia el switch para llenar su tabla CAM y que colapse al no poder almacenar más registros.

- **Protección DHCP Spoofing.** El ataque de suplantación de DHCP consiste en implementar un servidor DHCP falso el cual va a ofertar direcciones a los usuarios de la red para espiar el tráfico generado por dichos usuarios, el éxito del ataque depende de que se envíen tantas peticiones al servidor válido, hasta que esté sature el rango de asignación de direcciones y pueda entrar en acción el servidor atacante.

MEDIDAS DE PREVENCIÓN FRENTE A LAS DoS Y DDos:

- Los ataques de denegación de servicio, ya sea distribuido o no, causan graves consecuencias en los sistemas atacados. Implementar medidas preventivas será imprescindible ya que, en caso contrario, solamente sabremos que hemos sido víctimas de este ataque cuando el servicio deje de funcionar.
  Para minimizar las consecuencias de estos ataques sobre nuestros sistemas incorporan distintas medidas de seguridad:
  - Soluciones adoptadas: Bloqueo de tráfico por tres escalas de seguridad donde al primer intento de ataque se penaliza por 2 minutos, el segundo ataque lo agrega en lista para con penalización de 15 minutos y el tercer ataque es bloqueado por 15 días. De repetir el ataque pasados 15 días la dirección IP pública es agregada en lista negra y no podrá volver a conectarse.
  - La protección se encuentra sobre telnet, ssh, ftp, Dns, Proxy Cache, nmap, SYN, PSH, RST.

MECANISMOS DE PROTECCIÓN

- **Firewall (Corta fuegos):** Filtra los accesos entre autorizado y no, en la transmisión de paquetes entrantes como salientes. Aplicable a nivel de hardware y/o software, puede filtrar y bloquear puertos, protocolos, direcciones URL, entre otros.

- **Antimalware:** Los software malintencionados abundan en sitios web de dudosa procedencia y publicidad maliciosa. Por eso los computadores deben estar protegidos frente a estos. La mayoría de Sistemas Operativos tienen herramientas para contrarrestar este tipo de software malicioso, sin embargo se recomienda la instalación de un antivirus que incluya este módulo de protección.

- **Antivirus:** Software especializado en identificar, neutralizar, controlar y eliminar una amenaza de virus informático o códigos maliciosos como: gusanos, virus, troyanos, spyware, keyloggers, virus de macros, bots maliciosos, etc. Es imprescindible que los computadores tengan instalado y actualizado al menos un antivirus.

- **Antispam:** Igual que el antivirus, el Antispam descubre, controla y dispone para la eliminación de correos electrónicos, que puedan contener software y códigos maliciosos.

IDENTIFICACIÓN DE AMENAZAS A LA SEGURIDAD INFORMÁTICA

- **Código Malicioso:** Cargado en un software, hardware o firmware es introducido en el sistema operativo del equipo para destruir, secuestrar, sustraer, modificar y realizar otras acciones no autorizadas. Algunos de estos códigos son: gusanos, troyanos, works, hijacker, spyware, rootkits, pornware, adware, backdoor, dialers, exploit, keyloggers, etc.

- **Spam:** Correo electrónico masivo o directo, que puede llegar a contener información o contenidos no solicitados por el destinatario o cuya finalidad es generar afectación.

- **Hoax:** Este tipo de correo electrónico divulga cadenas e información fraudulenta y engañosa. Su finalidad es adquirir las cuentas de correo para diferentes fines posteriores.

- **Phishing:** Supla un sitio web y engaña al usuario haciéndole creer que está seguro. Por lo general este tipo de amenaza se da para robar información confidencial del usuario y propicia así fraudes.

- **Engaño social:** La utilización de artilugios mediante la manipulación de la persona para sustraer información personal y confidencial, así como para incitar a tomar acciones que le presentan un riesgo a su integridad y patrimonio. Este tipo de engaños se presenta comúnmente por teléfono o mediante correo electrónico.

RECOMENDACIONES DE SEGURIDAD PARA CLIENTES/SUSCRIPTORES

Nuestros clientes/suscriptores deberán seguir al menos las siguiente recomendaciones para garantizar una seguridad más fuerte:

1. Al momento de conectarse a una URL, deberá comprobar la seguridad de la página web. Esto es revisar que sea segura y cuente con los certificados SSL. Una mirada rápida establece que inicie como https://... Igualmente y antes de la URL también podrá visualizar un ícono de

"candado" el cual funciona como marcador e indica que la dicha página web es un sitio seguro.

2. Tenga siempre actualizado su navegador web y antivirus. Esta protección se hace con el fin de evitar daño, robo o cualquier vulneración que le implique un acceso a sus equipos no autorizados.

3. No abra o acepte correos electrónicos de dudosa procedencia o de contenidos maliciosos. Ni tampoco de clic en los íconos u URL que le indiquen en el correo.

4. Cerciórese siempre que el sitio web que visite sea el oficial, preferiblemente digitando usted directamente la dirección web.

5. Actualice regularmente las aplicaciones y el sistema operativo de su equipo. Con esto logra que se instalen parches de seguridad.

6. Aceptar y/o estar de acuerdo con los Términos y Condiciones expuestos en los sitios a los que se conecta. Tanto para el acceso a la red como para las aplicaciones y software que utilizará siempre y cuando esté seguro(a).

7. Nunca suministre datos personales, financieros u otros datos que le comprometan si desconfía o no está seguro(a) de quién se los solicita y para qué los solicita. Igualmente, no acepte ayuda de desconocidos o personal con quien apenas ha hablado y realmente no le conoce. Así como no acepte regalos, correos o contenidos de dudosa procedencia o con información cuestionable. Recuerda ser cauteloso con cada acción que realiza en la red.

8. Asegurar sus datos personales y la aceptación de "cookies", pues esto implica que su información sea guardada y luego usada. Los navegadores ofrecen opciones de privacidad que el usuario/suscriptor podrá modificar según su propio criterio.

9. Procurar prácticas seguras para sus credenciales de acceso. Esto significa que deberá implementar usuarios y contraseñas diferentes para cada cuenta, con nivel alto de seguridad (claves seguras: letras, símbolos, números).

10. Siempre que realice una descarga, asegúrese que sea del sitio oficial y/o de una fuente confiable. Evite descargar archivos o software de dudosa procedencia.

11. Blinde sus compras online mediante procesos de doble comprobación para aprobar la transacción, revise detenidamente la transacción y cargos asociados, y lo más importante realice compras en lugares que

sean de su confianza y cuente con los elementos de seguridad de un sitio web seguro.

12. Active herramientas de control de acceso y autorización para ciertos contenidos. Por ejemplo, haga uso del control parental configurando los contenidos a los cuales sus hijos tienen acceso cuando buscan algún contenido específico, así como limite el tiempo en que este lo utilice.

13. Instruya a sus familiares e hijos en el uso correcto del internet. Los niños son más vulnerables al ser presas de los delincuentes e inescrupulosos, por tal razón enseñale sobre los tips vistos aquí, sobre los riesgos que puede correr y cómo pueden evitar situaciones de peligro.

RECUERDE (peligros y consecuencias)

- Los delincuentes están al acecho y harán todo lo posible por hacer daño. Esto implica creación de cuentas, sitio web, llamadas telefónicas, envío de mensajes de texto, entre otras acciones que le faciliten su objetivo. Siempre esté atento(a).
- No corra ningún riesgo ni se exponga ante alguna amenaza, pues cualquiera puede ser vulnerable siempre y cuando tenga un smartphone, acceso a internet o correo electrónico.
- Tome todas las precauciones necesarias como:
    - Visitar sólo páginas web que conozca y sean oficiales.
    - No divulgar información personal ni confidencial por ningún medio desconocido o que le genere duda.
    - No acceda a los enlaces o descargue archivos que lleguen a su correo electrónico y cuyo remitente no conozca o le genere sospechas.
- Los delincuentes quieren sus datos personales para guardarlos en bases de datos que luego le permitan sacar un beneficio: robo de su dinero, realizar estafas, suplantaciones, entre otras.
- Instale y use hardware (dispositivos electrónicos: tabletas, computadores, smartphone) y software confiables.
- Ante alguna vulneración, informe inmediatamente a las autoridades y entidades implicadas: policía nacional, fiscalía general de la nación, bancos y corporaciones, entre las demás que le permitan bloquear, suspender, cambiar claves, restringir accesos o realizar cualquier tipo de operación que considere necesaria.