Recursos técnicos y logísticos para garantizar la seguridad de la red y la integridad del servicio y prevención de fraudes al interior de la red

SISTELEC SAS , como proveedor de redes y servicios de telecomunicaciones garantiza la seguridad de la red y la integridad del servicio, para evitar la interceptación, interrupción e interferencia del mismo y hemos tomado las respectivas medidas de seguridad de conformidad con las normas aplicables y de acuerdo a los siguientes aspectos:

1. **Principio de Autenticación**: Es la verificación de la identidad tanto de usuarios, dispositivos, servicios y aplicaciones. La información utilizada para la identificación, la autenticación y la autorización debe estar protegida. El acceso a la red está restringido a los usuarios de acuerdo con una contraseña y una clave. Además se autentica el equipo del cliente mediante la MAC.

2. **Principio de Acceso**: Es prevenir la utilización no autorizada de un recurso, por eso el control de acceso debe garantizar que sólo los usuarios o los dispositivos autorizados puedan acceder a los elementos de la red, la información almacenada, los flujos de información, los servicios y aplicaciones. El acceso a la red está restringido a los usuarios de acuerdo con una contraseña y una clave. Además se autentica el equipo del cliente mediante la MAC. Estas funciones se llevan a cabo en el enrutador de borde.

3. **Servicio de No repudio:** Tiene como objeto recolectar, mantener, poner a disposición y validar evidencia irrefutable sobre la identidad de los remitentes y destinatarios de transferencias de datos. Cuando sea solicitado, se puede monitorear y almacenar la información que permite la trazabilidad de una comunicación entre un remitente y un destinatario.

4**. Principio de Confidencialidad de datos**: SISTELEC SAS asegura la protección y la garantía que la información no se divulgará ni se pondrá a disposición de individuos, entidades o procesos no autorizados.

La confidencialidad de datos se garantiza por procesos técnicos y operativos:

PROCESOS TECNICOS: El acceso a los equipos del cliente están protegidos por usuario y contraseña y el acceso a la red por validación de la dirección MAC.

PROCESOS OPERATIVOS: Los técnicos que operan y mantienen la red les está prohibido el monitoreo de paquetes de datos de los clientes. Cualquier violación a este principio es causal de despido de acuerdo a las normas laborales vigentes. Por otra parte, la interceptación de las telecomunicaciones solo puede ser realizada por entidades competentes de acuerdo con el proceso adoptado para tal fin.

5. **Principio de Integridad de datos**: SISTELEC SAS garantiza en su red la exactitud y la veracidad de los datos, protegiéndolos contra acciones no autorizadas de modificación, supresión, creación o reactuación, e informará de las acciones no autorizadas, cuando tenga conocimiento, incluso a las autoridades competentes.

Existen barreras contra accesos no autorizados a la red como FIREWALLS y programas residentes en el ENRUTADOR DE BORDE para filtro de PHISHING, MALWARE y VIRUS.

6. **Principio de Disponibilidad**: Es garantizar que las circunstancias de la red no impidan el acceso autorizado a los elementos de la red, la información almacenada, los flujos de información, los servicios y las aplicaciones.

SISTELEC SAS no BLOQUEARÁ el acceso a páginas Web o el uso de aplicaciones en la red, sin el consentimiento expreso del usuario, salvo en aquéllos casos en que por disposición legal o reglamentaria estén prohibidas o su acceso sea restringido.

Neutralidad del Servicio

SISTELEC SAS, como proveedor de redes y servicios de telecomunicaciones, en desarrollo de la neutralidad del servicio, CUMPLE con los siguientes principios:

1. **Principio de libre elección**. El usuario podrá en forma libre utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio a través de Internet, salvo en los casos que por disposición legal u orden judicial estén prohibidos o su uso se encuentre restringido. Además, el usuario podrá utilizar en forma libre cualquier clase de instrumento, dispositivos o aparatos en la red, siempre que sean legales y que los mismos no dañen o perjudiquen la seguridad de la red o la calidad del servicio.

   SISTELEC SAS de ninguna manera restringe el acceso de sus usuarios para usar, enviar, recibir, ofrecer cualquier contenido legal, aplicación o servicio a través de Internet.

2. **Principio de no discriminación**. Brindará 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, sin embargo, podrán hacer ofertas según las necesidades de los segmentos de mercado o de sus usuarios de acuerdo con sus perfiles de uso y consumo, lo cual no se entenderá como discriminación.

   Todos los usuarios tienen igual acceso a contenidos y aplicaciones presentes en la red sin ningún tipo de discriminación. Sin embargo, se reserva el derecho de ofrecer planes que puedan restringir la velocidad o el acceso a algún tipo de aplicaciones tales como OTT (video o audio streaming) u otras cuyo consumo de ancho de banda sea intenso.

3. **Principio de transparencia**. Presentará periódicamente sus políticas de gestión de tráfico a los usuarios y a otros proveedores que tengan acceso a su red.

   Las políticas de gestión de tráfico que SISTELEC SAS emplea están encaminadas a garantizar una excelente calidad de servicio y cumplir con el ancho de banda contratado. Para ello en el servidor de Gestión de Tráfico establece reglas de administración de ancho de banda según cada plan contratado y restricción de acceso de acuerdo a la calidad de la señal de radio recibida, por lo que antes de viabilizar un servicio hace un análisis de propagación y determina cual es el equipo del cliente más adecuado y las condiciones de instalación. Este estudio establece en parte el costo de instalación que deberá pagar el cliente.

4. **Principio de Información**. Informará al usuario de toda la información asociada a las condiciones de prestación del servicio incluida velocidad, calidad, prácticas de gestión de tráfico relativas a cada plan ofrecido o acordado, en los términos dispuestos en la Resolución 5078 de 2016, de la Comisión de Regulación de Comunicaciones.

   En la página WEB y en el contrato que se suscribe con el cliente se establecen claramente las condiciones de prestación del servicio como la velocidad, QoS, y las prácticas de gestión de tráfico ya antes señaladas.

PRÁCTICAS DE GESTIÓN DE TRÁFICO

SISTELEC SAS podrá implementar medidas de gestión de tráfico razonables y no discriminatorias respecto de algún proveedor, servicio, contenido o protocolo específico.

Las prácticas de gestión de tráfico están destinadas a:

Aplicar medidas para reducir o mitigar los efectos de la congestión sobre la red, por ejemplo balanceo de carga, incremento del ancho de banda disponible, entre otras.

Asegurar la seguridad e integridad de las redes, introduciendo y actualizando permanentemente equipos y/o programas como FIREWALLs, ANTIVIRUS;

Asegurar la calidad del servicio a los usuarios, revisando constantemente el flujo de tráfico de cada nodo de la red en nuestro Centro de Gestión y Soporte Técnico.

En caso de ser necesario, priorizar tipos o clases genéricas de tráfico en función de los requisitos de calidad de servicio (QoS) propias de dicho tráfico, tales como latencia y retardo de estos. Entre otras aplicaciones tales como vídeo y voz.

Para proporcionar servicios o capacidades de acuerdo con la elección de los usuarios, que atiendan los requisitos técnicos, estándares o mejores prácticas adoptadas por iniciativas de

gobernanza de Internet u organizaciones de estandarización. Ejemplo plataformas de vídeo, video-conferencia, voz sobre IP, aplicaciones educativas, etc.

En todo caso, SISTELEC SAS solo aplica prácticas de gestión de red cumpliendo con lo previsto en la recomendación UIT-T X.700 y aquéllas que la complementen, modifiquen o sustituyan.

Los proveedores de redes y servicios de acceso a Internet durante la ocurrencia de pandemias declaradas por la Organización Mundial de la Salud con incidencia en Colombia, en los términos de lo previsto en el parágrafo segundo del artículo 56 de la Ley 1450 de 2011, adicionado por el Decreto 555 de 2020, concordado con el Decreto 417 de 2020, podrán priorizar el tráfico, para garantizar el acceso del usuario a contenidos o aplicaciones relacionados con los servicios de salud, las páginas gubernamentales y el sector público, el desarrollo de actividades laborales, de educación y el ejercicio de derechos fundamentales, con arreglo a lo dispuesto en el el ANEXO 2.9 DEL TÍTULO DE ANEXOS DE LA RESOLUCIÓN CRC 5050 DE 2016.

PRIORIZACION DE TRÁFICO

SISTELEC SAS no lleva a cabo conductas de priorización, degradación o bloqueo que contravengan las normas regulatorias relativas a la neutralidad de la red neutralidad de la red, gestión y priorización de tráfico y en especial con los establecido en la Resolución 3502 del 2011, compilada en la resolución CRC5050 del 2016, TITULO II, capítulo 9.