PROTECCION AL CONSUMIDOR

SOPORTE REGULATORIO

Ley 1450 2001

Resolución 3502 de 2011.
Resolución 5050 de 2016, artículos 2.9.1.3.2 y 5.1.2.2.
Resolución 5078 de 2016, artículo 5.1.1.3

Protección al consumidor es el conjunto de normas que regulan las relaciones de consumo que nacen en la cadena de comercialización de bienes y servicios entre productores, proveedores y expendedores.

- **Neutralidad en Internet -No Limitación al Acceso**

Artículo 56. Neutralidad en Internet

Los prestadores del servicio de Internet:

1. Sin perjuicio de lo establecido en la Ley 1336 de 2006 (sic), no podrán 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.
2. Deberán ofrecer 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.
3. Los prestadores del servicio de Internet 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.
4. Bloquearán el acceso a determinados contenidos, aplicaciones o servicios, sólo ha pedido expreso del usuario.
5. Artículo 5.1.1.3.3. Suministrar las mismas condiciones de calidad que ofrecen a sus usuarios, tanto a otros PRST que accedan a su red, como a los respectivos usuarios de éstos.

- Artículo 5.1.2.2. Limitaciones al acceso: Los proveedores de redes y servicios de telecomunicaciones que presten el servicio de acceso a Internet no podrán bloquear el acceso a páginas Web o el uso de aplicaciones en la red, sin el consentimiento expreso del usuario, salvo en aquellos casos en que por disposición legal o reglamentaria estén prohibidas o su acceso sea restringido.
- Artículo 2.9.1.3.1. Libre Elección. El usuario podrá libremente utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio a través de Internet, salvo en los casos en que por disposición legal u orden judicial estén prohibidos o su uso se encuentre restringido. Adicionalmente, el usuario podrá libremente utilizar cualquier clase de instrumentos, 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.
- Artículo 2.9.1.3.2. No Discriminación. En todo momento, los proveedores de redes y servicios de telecomunicaciones que prestan el servicio de acceso a Internet brindarán 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.
- De acuerdo a lo previsto en el artículo 56 de la Ley 1450 de 2011, los proveedores de redes y servicios de telecomunicaciones que prestan el servicio de acceso a Internet 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.

- Artículo 2.9.1.3.3. Transparencia. Los proveedores de redes y servicios de telecomunicaciones que prestan el servicio de acceso a Internet deben revelar sus políticas de gestión de tráfico a los usuarios y a otros proveedores que tengan acceso a su red.

Articulo2.9.1.3.4. Información. Los proveedores de redes y servicios de telecomunicaciones que prestan el servicio de acceso a Internet deben suministrar al usuario 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.

Neutralidad en Internet

Unotel, como proveedor de redes y servicios de telecomunicaciones, en desarrollo de la neutralidad del servicio, cumple con los siguientes servicios:

Principio de Libre Eleccion: El usuario podrá libremente utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio a través de Internet, salvo en los casos en que por disposición legal u orden judicial estén prohibidos o su uso se encuentre restringido.

El usuario podrá libremente utilizar cualquier clase de instrumentos, 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.

Unotel; no restringe el acceso de sus usuarios para usar, enviar, recibir , ofrecer cualquier contenido legal, aplicación o servicio a través de internet.

Principio de no Discriminación: Se brinda 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.

En este sentido, se hacen ofertas según las necesidades de los segmentos de mercado o de los usuarios de acuerdo con sus perfiles de uso y consumo, lo cual no se entenderá como discriminación.

Garantía de Seguridad de la Red e Integridad del Servicio

Permanentemente monitoreamos cada uno de los elementos que forman parte técnica de la prestación de los servicios, permitiendo la identificación oportuna de cualquier evento o anomalía en la red. Para ello, utiliza equipos estratégicamente ubicados que monitorean aspectos como:

- Estado de los equipos de red
- Logs de actividades en los equipos
- Comportamiento del tráfico en distintos sectores de la red (puntos de interconexión, peering y nodos)
- Informes de control de Firewall, detallando tráfico en puntos críticos, firmas de ataques, y análisis de vulnerabilidades
- Backups de dispositivos de red, protegidos bajo estructuras de mínima exposición pública
- Evaluación de Seguridad para exponer vulnerabilidades y establecer medidas correctivas

Modelos de Seguridad Adaptados a la Red

Cumpliendo con las normativas de vigilancia y control, hemos implementado modelos de seguridad específicos para la protección de redes y usuarios.

1. Autenticación:

- Basada en las normas UIT X.805 y X.811, la autenticación verifica la identidad de entidades (personas, servicios, aplicaciones). Los servicios de autenticación de la empresa, utiliza un modelo descentralizado que permite garantizar el acceso individual a equipos específicos con privilegios definidos y evitar riesgos de seguridad masivos que pongan en peligro la integridad completa de la plataforma tecnológica que presta los servicios a nuestros usuarios.

2. Control de Acceso:

- Este control asegura que solo personas y dispositivos autorizados accedan a la red y sus recursos, basándose en las recomendaciones UIT X.810 y X.812. Aplica medidas de seguridad física y lógica:

Seguridad Física: Mesa de Servicios con vigilancia 24/7, control de acceso con autenticación múltiple y monitoreo continuo. Seguridad Lógica: Acceso controlado a plataformas de enrutamiento y acceso, con autenticación de protocolo seguro

3. Registros de Auditoría

- Mantenemos registros de acceso y actividades en la infraestructura de ACCESO, con periodos de retención definidos en cada equipo

4. Confidencialidad de Datos

- Asegura la privacidad y protección contra accesos no autorizados, usando cifrado y controles de acceso

5. Privacidad

- Las políticas de Seguridad de la Información y Protección de Datos, garantizan que la información de usuarios no se divulga sin autorización

6. Integridad de Datos

- Protege contra modificaciones no autorizadas, aplicando actualizaciones de software que mitiguen vulnerabilidades en la infraestructura de red

7. Disponibilidad

- Garantizamos alta disponibilidad mediante infraestructuras redundantes y sistemas de respaldo que aseguran continuidad de servicios ante fallos

Medidas de Seguridad para Garantizar Confidencialidad, Integridad y Disponibilidad

Las actividades y métodos descritos garantizan la autenticación, protección y cifrado, así como el monitoreo continuo para identificar amenazas y problemas en la red.

- Medidas contra Interceptación y Violación de Comunicaciones, implementando controles de acceso y sistemas de detección para monitorear eventos en la red, asegurando acciones ejecutadas y denegadas a usuarios y terceros

- Tratamiento de Incidentes de Seguridad realiza análisis forense en situaciones de desastre, con equipos capaces de recuperar información y rastrear eventos.

- Mecanismos para Garantizar Confidencialidad, Integridad y Disponibilidad, cumplimos con regulaciones gubernamentales para el manejo de información de usuarios, garantizando la confidencialidad y prevención de fraudes en telecomunicaciones

POLITICA DE SEGURIDAD DE LA INFORMACION haga clic aquí

Objetivo

Definir e implementar los lineamientos y política de Seguridad y Privacidad de la información de la empresa 02 Online "Unotel" , que permita preservar la integridad, confidencialidad, disponibilidad y privacidad de la información alineado al Modelo de Seguridad y Privacidad de la información y la Norma NTC-ISO-IEC 27001:2013.

Controles:

- 5.1.1 Políticas para la seguridad de la información
- 5.1.2 Revisión de las políticas de seguridad de la información

Se definen las políticas de la seguridad de la información, fueron aprobadas por la gerencia y se comunicaron a los empleados y demás partes interesadas. La comunicación de las políticas se realiza a todos los niveles de la empresa, no solo al nivel de los directivos y responsables, se adaptan continuamente a las necesidades y cambios de la empresa por lo que no pueden permanecer estáticas y se mantiene actualizada.

¿Qué es la seguridad en Internet?

La seguridad en Internet se refiere a las prácticas y medidas que ayudan a proteger a los usuarios, sus datos y dispositivos contra amenazas en línea. Esto incluye la protección contra ataques cibernéticos, el robo de información personal, el acceso no autorizado a cuentas y la prevención de fraudes. Algunos aspectos clave de la seguridad en Internet incluyen:

- Uso de contraseñas seguras: Elegir contraseñas complejas y únicas para cada cuenta.
- Autenticación de dos factores: Agregar una capa adicional de seguridad al iniciar sesión.
- Protección contra malware: Instalar software antivirus y evitar descargas sospechosas.
- Cuidado con el phishing: No hacer clic en enlaces dudosos ni proporcionar información a fuentes no verificadas.
- Privacidad en redes sociales: Configurar correctamente los permisos para evitar el acceso no deseado.
- Uso de redes seguras: Evitar redes Wi-Fi públicas sin protección y usar conexiones VPN cuando sea necesario.

Principales riesgos en internet

Algunas de las cosas que los cibercriminales buscan conseguir por medio de internet son:

- Robo de información
- Daño de información
- Ataques a sistemas o equipos
- Suplantación de identidad
- Venta de datos personales
- Robo de dinero

RECOMENDACIONES PARA MEJORAR LA SEGURIDAD DE WINDOWS

Para mejorar la seguridad de Windows, es fundamental mantener el sistema operativo y el software actualizados, usar un software antivirus confiable y activo, y configurar correctamente el firewall de Windows. Además, se recomienda utilizar contraseñas seguras y evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos o mensajes.

Recomendaciones específicas:

Mantener el sistema operativo y el software actualizados:

Las actualizaciones incluyen parches de seguridad que corrigen vulnerabilidades y mejoran la seguridad del sistema.

Usar un software antivirus confiable:

Un software antivirus fiable debe ofrecer protección en tiempo real, actualizaciones periódicas y análisis frecuentes.

Configurar correctamente el firewall de Windows:

El firewall ayuda a bloquear el tráfico de red no autorizado y a proteger el sistema contra ataques.

Utilizar contraseñas seguras:

Las contraseñas deben ser largas, únicas y difíciles de adivinar para cada cuenta.

Evitar abrir archivos adjuntos o enlaces sospechosos:

Estos pueden contener malware o virus que pueden comprometer la seguridad del sistema.

Desactivar el acceso remoto si no lo necesita:

Si no utiliza la función de escritorio remoto, es mejor desactivarla para evitar posibles vulnerabilidades.

Considerar la descarga de aplicaciones de fuentes confiables:

Evitar la descarga de aplicaciones de fuentes no oficiales, ya que pueden contener malware.

Ejecutar escaneos de malware regularmente:

Esto ayuda a detectar y eliminar cualquier software malicioso que pueda estar presente en el sistema.

Utilizar el servicio de Protección de Windows para obtener consejos de seguridad:

Microsoft Defender ofrece recomendaciones de seguridad específicas para tu dispositivo.

RECOMENDACIONES PARA MEJORAR LA SEGURIDAD DE MAC

Para mejorar la seguridad de tu Mac, se recomienda utilizar contraseñas seguras y únicas, activar Face ID o Touch ID, realizar actualizaciones de software regularmente, y considerar opciones de privacidad como el firewall y la navegación privada. También es importante proteger tu información con FileVault, realizar respaldos regularmente, y estar atento a posibles amenazas de malware.

Recomendaciones detalladas:

- **Contraseñas seguras y únicas:**

Utiliza contraseñas largas, complejas y únicas para cada cuenta, y considera usar un administrador de contraseñas para generar y almacenar contraseñas seguras.

- **Face ID o Touch ID:**

Activa estas opciones para una autenticación más segura al iniciar sesión y realizar compras.

- **Actualizaciones de software:**

Mantén tu Mac y todos los programas actualizados para beneficiarte de las últimas correcciones de seguridad.

- **Firewall y privacidad:**

Configura el firewall para bloquear comunicaciones no deseadas y utiliza la navegación privada en tu navegador.

- **FileVault:**

Asegúrate de que FileVault esté activado para encriptar tus datos en el disco duro.

- **Respaldos regulares:**

Realiza respaldos regulares de tus archivos con Time Machine, para poder recuperarlos en caso de pérdida o daño.

- **Malware:**

Ten cuidado con los enlaces y archivos adjuntos sospechosos, y considera usar software antivirus si es necesario.

- **Privacidad:**

Controla qué aplicaciones pueden acceder a tu cámara, micrófono y ubicación, y considera desactivar los anuncios personalizados.

- **Buscar mi Mac:**

Activa la opción “Buscar mi Mac” para poder ubicar tu Mac si la pierdes o te la roban.

- **Seguridad de correo electrónico:**

Implementa buenas prácticas de seguridad del correo electrónico para evitar el acceso no autorizado a tus datos.

- **Bloquear inicios de sesión automáticos:**

Asegúrate de que los inicios de sesión automáticos estén desactivados para mayor seguridad.

- **Limitando acceso a aplicaciones:**

Limita el acceso a las aplicaciones a través de la opción “Permitir aplicaciones descargadas solo de la App Store”, o “Permitir aplicaciones de la App Store y de desarrolladores identificados” en Privacidad y Seguridad, para mayor seguridad.

- **Verifica la seguridad de las actualizaciones:**

Antes de instalar cualquier actualización de software, asegúrate de que la fuente sea confiable y oficial.

- **Considera la seguridad en la nube:**

Si utilizas servicios en la nube, asegúrate de que tus datos estén protegidos con contraseñas seguras y que el servicio tenga buenas prácticas de seguridad.