Super TV Electronic Ltda.

Neutralidad en Internet -No Limitación al Acceso

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.

ARTÍCULO 56. Neutralidad en Internet.

Los prestadores del servicio de Internet: (Ley 1450 de 2011)

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. En este sentido, 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. 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.
6. Bloquearán el acceso a determinados contenidos, aplicaciones o servicios, sólo a pedido expreso del usuario.

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.

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.

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. En todo caso, conforme 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.

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.

2.9.1.3.4. 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, en los términos dispuestos en el CAPÍTULO 1 del TÍTULO II.

SOPORTE REGULATORIO

Ley 1450 2001 – PND, artículo 56, cuyas condiciones regulatorias se establecen en la Resolución 3502 de 2011.
Resolución 5050 de 2016, artículos 2.9.1.3.2 y 5.1.2.2.
Resolución 5078 de 2016, articulo 5.1.1.3

PERIODICIDAD DE PRESENTACIÓN: PERMANENTE
TIPO DE SERVICIO AL QUE APLICA: INTERNET

VERIFICACIÓN DOCUMENTAL Y DE BASES DE DATOS
Verificación o Visita por Aspecto IN SITU o Verificación o Visita IN SITU Integral 3

DOCUMENTOS Y/O REPORTES A VERIFICAR
Bases de datos de Peticiones, quejas, reclamos y denuncias.

ACTIVIDAD DE VERIFICACIÓN
Verificar que en la base de datos de peticiones, quejas, reclamos y denuncias no se haya denunciado por parte de usuarios informado sobre conductas contrarias a los principios de neutralidad en internet de que trata esta obligación.

CRITERIO DE ACEPTACIÓN
Que no existan denuncias por parte de usuarios informado sobre conductas contrarias a los principios de neutralidad en internet de que trata esta obligación.

IC-003 -002 Neutralidad en Internet

Super TV Electronic Ltda, como proveedor de redes y servicios de telecomunicaciones, en desarrollo de la neutralidad del servicio, cumple con los siguientes servicios:

PRINCIPIO 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 perjudiquen la seguridad de la red o la calidad del servicio.

Super TV Electronic Ltda; de ninguna manera restringe el acceso de sus usuarios para usar, enviar, recibir , ofrecer cualquier contenido legal, aplicación o servicio a través de internet.

PRINCIPIO DE NO DISCRIMINACION; 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. En todo caso, conforme 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.

Control Parental,Resoluciones Y Decreto

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.

Protección Al Consumidor

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.

REGIMEN DE PROTECCIÓN AL USUARIO
https://drive.google.com/file/d/1aeI_JouTKNaoFjsxND8IwCOzqfmWvATP/view
LEY 1480 DE 2011
https://drive.google.com/file/d/1Fe9IKL9gBr5G0GLSXhn1y7jUKxT4fDmu/view
ACUERDO 011 DE 2006
https://drive.google.com/file/d/12sbW6g4kaCpQj_as1GTpCAI4qI8012si/view
HABEAS DATA
https://drive.google.com/file/d/1l62O_7gGpWqxfJ-OxleA8BSOR5u5kUTU/view
LEY 679 DE 2001
https://drive.google.com/file/d/1ZO_laUUWCLwBm-KKS6Vb2f8TvCfSR4fW/view
CONTRATO DE PRESTACIÓN DE SERVICIOS

Control Parental

Actualmente los dispositivos electrónicos cuentan con aplicaciones y sistemas de control parental, los cuales son de gran utilidad durante las vacaciones, pues les permiten a los padres de familia conocer sobre las actividades que realizan los niños, niñas y adolescentes mientras están en Internet.

Link De La Herramienta
https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/53254:Usa-las-herramientas-de-control-parental-en-estas-vacaciones

Las siguientes son algunas aplicaciones que puede utilizar para el control del uso del internet por parte de sus hijos.

https://www.netnanny.com
https://www.opendns.com/home-internet-security/

Como Denunciar

Conozca como proteger a sus hijos para no ser victimas de la Pornografía e Infórmese Infantil acerca de nuestra gestión contra este delito y como denunciar.

En los siguientes lugares se pueden realizar denuncias relacionadas con sitios y contenidos de pornografía infantil, así como páginas web que ofrezcan servicios sexuales con niños:

Ministerio de las tecnologías de la información y las comunicaciones.
https://ciberpaz.gov.co/portal/

Instituto colombiano de bienestar familiar ICBF
Línea gratuita nacional icbf:(57 1) 01 8000 91 80 80. Disponible de lunes a domingo las 24 horas.

Línea de prevención abuso sexual:(57 1) 01 8000 11 24 40. Disponible de lunes a domingo las 24 horas.

Canales de atención en línea:
chat icbf y llamada en línea disponibles de lunes a domingo las 24 horas.

Videollamada disponible de lunes a viernes de 7:00 am a 7:00 pm en jornada continua.
Correo de atención al ciudadano.

https://www.icbf.gov.co

Te Protejo
https://teprotejocolombia.org
o descarga el app en las tiendas iOS o Android.

Fiscalia General de la Nacion
Línea nacional gratuita (01 8000 9197 48)
desde su celular marque gratis al 122.
https://www.fiscalia.gov.co/colombia/

Dirección central de policía judicial – DIJIN
Grupo investigativo delitos informáticos
carrera 77a # 45-61 barrio modelia
teléfonos: pbx: 426 6900 ext. 6301-6302
directo: 4266300
https://www.policia.gov.co
https://caivirtual.policia.gov.co

Resoluciones Y Decretos

Conozca las resoluciones y normativas para no vulnerar los derechos de los usuarios.

RESOLUCIÓN NO. 5397 DE 2018
https://drive.google.com/file/d/1Ses8cYuhALQT37c_UoJ2jGnfTgBPjq-h/view
RESOLUCIÓN NO.5344 DE 2018
https://drive.google.com/file/d/1T7VkFZGI5hw50xbukCakUi7ks8JlHxVm/view
RESOLUCIÓN NO. 5337 DE 2018
https://drive.google.com/file/d/16t3dP8MW5BzhTAWQOJr5O4Xunk8P6LUO/view
RESOLUCIÓN NO. 5322 DE 2018
https://drive.google.com/file/d/1P9KWDoFB_BXtv-NTZBCQdnnLn_T_l5PA/view
DECRETO 90 DEL 18 DE ENERO DE 2018
https://drive.google.com/file/d/1iGhv67fl7KBlpLDNKqf2VRw4NqOChb7s/view
RESOLUCIÓN 5321 DE 2018
https://drive.google.com/file/d/1qqDAR0RfNFZNmxe-c1i-E_2JNM8KVe5X/view
RESOLUCIÓN NO. 5299 DE 2018
https://drive.google.com/file/d/1yZU-B53ySe_Z0ehid_TJkbCW9vg5_sjh/view
RESOLUCIÓN NO. 5300 DE 2018
https://drive.google.com/file/d/1JxeVWjvm__Xo2GE5qoLjPb1cDI3gW0HR/view

Políticas de Seguridad de la Información

MONITOR CON BASE A LA NORMA ISO 27001 DISPONE:

Objetivo 1:

Proporcionar orientación y apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes

Controles:

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

Se definen las políticas de la seguridad de la información:

Fueron aprobadas por la gerencia
Se comunicaron a los empleados y partes externas pertinentes
Más información:
https://www.normaiso27001.es/fase-3-elaboracion-de-la-politica-objetivos-del-sgsi/

La comunicación de las políticas se realizan a todos los niveles, no solo al nivel de los directivos y responsables. El objetivo de la Seguridad de la información pasa por involucrar a toda la empresa Super TV Electronic Ltda.

Revisión **PERMANENTE** de las políticas de seguridad de la información

Las políticas de la Seguridad de la información en Super TV Electronic Ltda se adaptan continuamente a las necesidades y cambios de la organización por lo que no pueden permanecer estáticas. Se mantiene actualizada la política de la seguridad de la información. Para ello es interesante tener en cuenta algunas recomendaciones.

Qué es la seguridad en Internet?

La seguridad en internet son todas aquellas precauciones que se toman para proteger todos los elementos que hacen parte de la red como infraestructura e información, la más afectada por delincuentes cibernéticos.

La seguridad informática se encarga de crear métodos, procedimientos y normas que logren identificar y eliminar vulnerabilidades en la información y equipos físicos, como los computadores.

Una de las mejores formas de mantenerse protegido en internet es por medio de un antivirus, como usuario se pueden tomar varias medidas preventivas como mantener activados y actualizados los antivirus en nuestros dispositivos con conexión a internet, evitar realizar operaciones financieras en redes abiertas o computadores públicos y verificar los archivos adjuntos de mensajes de desconocidos y evitar descargarlos si no se tiene plena seguridad de su contenido.

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.