SEGURIDAD DE LA RED, RIESGOS DEL SERVICIO DE INTERNET Y CONTROLES PARENTALES

I. Seguridad de la red

UNIMOS S.A ESP ha adoptado medidas para garantizar la seguridad de la red y la integridad del servicio prestado a sus usuarios evitando la interceptación, interrupción e interferencia del mismo, las cuales se describen a continuación:

1. UNIMOS S.A ESP cuenta con un sistema de seguridad, operado a través de llave de seguridad contra intrusión no autorizada de sus elementos de red (Armarios), que permite que estos solo sean operados por el personal exclusivo de la empresa, evitando que sean manipulados por personal ajeno.

2. UNIMOS S.A ESP cuenta con un esquema de vigilancia que permite identificar personal que ingresa a la empresa, a fin de brindar protección contra intrusos o personal no autorizado.

3. Contamos con un centro de operaciones de red los siete (7) días de la semana las 24 horas encargado de monitorear e informar sobre actividades físicas y lógicas en los equipos e instalaciones que hace parte vital del servicio de banda ancha.

4. UNIMOS S.A ESP; cuenta con sistemas de seguridad que monitorean y controlan el acceso a sus instalaciones y áreas críticas de sus edificios, haciendo uso de cámaras de seguridad.

II. Riesgos relativos al servicio de internet

El uso de Internet también conlleva riesgos, algunos de estos son:

a) Relacionados con la información Las personas frecuentemente necesitamos información para realizar nuestras actividades, y muchas veces la podemos obtener en Internet de manera más rápida, cómoda y económica que en el "mundo físico". No obstante, hemos de considerar posibles riesgos:

- Acceso a información poco fiable y falsa. Existe mucha información errónea y poco actualizada en Internet, ya que cualquiera puede poner información en la red.

- Acceso a información inapropiada y nociva. Existen webs que, aunque contengan información científica, pueden resultar inapropiadas y hasta nocivas por el modo en el que se abordan los temas o la crudeza de las imágenes.
- Acceso a información peligrosa, inmoral, ilícita. Existe información poco recomendable y con contenidos considerados delictivos.

b) Riesgos relacionados con la comunicación Las personas muchas veces necesitamos comunicarnos. Internet nos ofrece infinidad de canales (e-mail, chats, weblogs...) y oportunidades, aunque conllevan algunos riesgos:

- Bloqueo del buzón de correo. El adjuntar grandes archivos a los correos sin pedir previamente autorización al receptor del mensaje puede bloquear temporalmente su buzón de correo.

- Recepción de "mensajes basura". Ante la carencia de una legislación adecuada, por e-mail se reciben muchos mensajes de propaganda no deseada (spam) o con virus.

- Recepción de mensajes personales ofensivos. Al comunicarse en los foros virtuales, como los mensajes escritos (a menudo mal redactados y siempre privados del contacto visual y la interacción inmediata con el emisor) se prestan más a malentendidos que pueden resultar ofensivos para algunos de sus receptores.

- Pérdida de intimidad. En ocasiones, hasta de manera inconsciente al participar en los foros, se puede proporcionar información personal, familiar o de terceras personas a gente desconocida.

- Acciones ilegales. Difundir determinadas opiniones o contenidos, insultar o amenazar a través de Internet... puede acarrear responsabilidades judiciales.

- Malas compañías. Especialmente en los chats, se puede entrar en contacto con personas que utilizan identidades falsas con oscuras intenciones.

c) Riesgos relacionados con actividades económicas. En internet se pueden llevar a cabo operaciones con repercusión económica, pudiendo suponer estos algunos riesgos como estafas, robos, negocios ilegales, delitos de propiedad intelectual, compras inducidas por publicidad abusiva o a menores sin autorización paterna.

d) Riesgos relacionados con la tecnología A veces por limitaciones tecnológicas, a veces por actos de sabotaje y piratería, y que aún resultan incontrolables: virus, spam, troyanos, spyware, etc. A pesar de que la mayoría de estos riesgos son los mismos que nos podemos encontrar en el mundo real, internet los potencia al:

- Facilitar el acceso a la información
- Favorecer el anonimato
- Conceder accesibilidad permanente
- Facilitar comunicación interpersonal

III. Medidas adoptadas por UNIMOS S.A. ESP. para garantizar la seguridad de la red.

Frente a las acciones tomadas en relación a servicios prestados a sus usuarios de internet en banda ancha, UNIMOS S.A ESP; les informa que es necesario que ellos adquieran sistemas de seguridad como:

- Los usuarios del servicio de banda ancha deben adquirir sistemas de protección ANTIVIRUS y ANTISPAM, los cuales previenen la pérdida de información y garantizan la integridad de la información almacenada en sus equipos.

- Frente a la autenticación de usuarios del servicio de acceso a internet UNIMOS S.A ESP; dispone de plataformas de procesos, que permiten en tiempo real, asegurar la autorización de acceso a la navegación. Lo anterior asegura que solo usuarios autorizados puedan hacer al uso de los servicios contratados por la compañía. La plataforma usada corresponde a un servicio de autenticación, autorización y registro implementado en configuración de alta disponibilidad.

- La plataforma en operación de UNIMOS S.A ESP; cuenta con funcionalidades de accounting (Servicio de no repudio) generando logs para cada una de las sesiones de usuario, donde se relaciona una dirección IP dinámica con la cuenta asociada para cada cliente (asegura la identidad), fecha de inicio y duración de la sesión.

- Frente a la confidencialidad de los datos UNIMOS S.A ESP; dispone de sistemas que almacenan la información (almacenamiento masivo de datos) con protección que evitan la intrusión indebida a éstos. A su vez frente a los datos biográficos de sus usuarios, tiene establecidos procesos que garantizan la recepción y trámite de los requisitos allegados solo desde los entes de seguridad mediante los cuales, se realizan la solicitud de información confidencial asociada a los usuarios de línea básica y datos (Ej: direcciones IP). Dicha solicitud debe estar soportada mediante orden judicial.

- Complementado lo anteriormente expresado, y específicamente en lo que compete al principio de Integridad de Datos, UNIMOS S.A ESP; cuenta con mecanismos de protección del CORE de la Red, como son: Firewalls y filtrado perimetral, lo cual evita riesgo de acceso no autorizado.

IV. Acciones que debe tomar el usuario para garantizar la seguridad en la Red.

Como un complemento a lo anteriormente enunciado, UNIMOS S.A ESP, recomienda a los clientes de Internet Banda Ancha que para garantizar una conexión y navegación segura por la red debe obtener e instalar, en sus equipos de cómputo, licencias de protección informática que contengan: control parental, antivirus y antispyware de casas de antivirus reconocidas. Además, tener en cuenta lo siguiente:

- Evitar los enlaces sospechosos: uno de los medios más utilizados para direccionar a las víctimas a sitios maliciosos son los hipervínculos o enlaces. Evitar hacer clic en éstos previene el acceso a páginas web que posean amenazas capaces de infectar al usuario. Los enlaces pueden estar presentes en un correo electrónico, una ventana de chat o un mensaje en una red social: la clave está en analizar si son ofrecidos en alguna situación sospechosa (una invitación a ver una foto en un idioma distinto al propio, por ejemplo), provienen de un remitente desconocido o remiten a un sitio web poco confiable.

- No acceder a sitios web de dudosa reputación: a través de técnicas de Ingeniería Social, muchos sitios web suelen promocionarse con datos que pueden llamar la atención del usuario – como descuentos en la compra de productos (o incluso ofrecimientos gratuitos), primicias o materiales exclusivos de noticias de actualidad, material multimedia, etc. Es recomendable para una navegación segura que el usuario esté atento a estos mensajes y evite acceder a páginas web con estas características.
- Actualizar el sistema operativo y aplicaciones: el usuario debe mantener actualizados con los últimos parches de seguridad no sólo el sistema operativo, sino también el software instalado en el sistema a fin de evitar la propagación de amenazas a través de las vulnerabilidades que posea el sistema.

- Descargar aplicaciones desde sitios web oficiales: muchos sitios simulan ofrecer programas populares que son alterados, modificados o suplantados por versiones que contienen algún tipo de malware y descargan el código malicioso al momento que el usuario lo instala en el sistema. Por eso, es recomendable que al momento de descargar aplicaciones lo haga siempre desde las páginas web oficiales.

- Utilizar tecnologías de seguridad: las soluciones antivirus, firewall y antispam representan las aplicaciones más importantes para la protección del equipo ante las principales amenazas que se propagan por Internet. Utilizar estas tecnologías disminuye el riesgo y exposición ante amenazas.

- Evitar el ingreso de información personal en formularios dudosos: cuando el usuario se enfrente a un formulario web que contenga campos con información sensible (por ejemplo, usuario y contraseña), es recomendable verificar la legitimidad del sitio. Una buena estrategia es corroborar el dominio y la utilización del protocolo HTTPS para garantizar la confidencialidad de la información. De esta forma, se pueden prevenir ataques de phishing que intentan obtener información sensible a través de la simulación de una entidad de confianza.

- Tener precaución con los resultados arrojados por buscadores web: a través de técnicas de Black Hat SEO , los atacantes suelen posicionar sus sitios web entre los primeros lugares en los resultados de los buscadores, especialmente en los casos de búsquedas de palabras clave muy utilizadas por el público, como temas de actualidad, noticias extravagantes o temáticas populares (como por ejemplo, el deporte y el sexo). Ante

cualquiera de estas búsquedas, el usuario debe estar atento a los resultados y verificar a qué sitios web está siendo enlazado.

- Aceptar sólo contactos conocidos: tanto en los clientes de mensajería instantánea como en redes sociales, es recomendable aceptar e interactuar sólo con contactos conocidos. De esta manera se evita acceder a los perfiles creados por los atacantes para comunicarse con las víctimas y exponerlas a diversas amenazas como malware, phishing, cyberbullying u otras.

- Evitar la ejecución de archivos sospechosos: la propagación de malware suele realizarse a través de archivos ejecutables. Es recomendable evitar la ejecución de archivos a menos que se conozca la seguridad del mismo y su procedencia sea confiable (tanto si proviene de un contacto en la mensajería instantánea, un correo electrónico o un sitio web). Cuando se descargan archivos de redes P2P, se sugiere analizarlos de modo previo a su ejecución con una solución de seguridad.

- Utilizar contraseñas fuertes: muchos servicios en Internet están protegidos con una clave de acceso, de forma de resguardar la privacidad de la información. Si esta contraseña fuera sencilla o común (muy utilizada entre los usuarios) un atacante podría adivinarla y por lo tanto acceder indebidamente como si fuera el usuario verdadero. Por este motivo se recomienda la utilización de contraseñas fuertes, con distintos tipos de caracteres y una longitud de al menos 8 caracteres. Como siempre, las buenas prácticas sirven para aumentar el nivel de protección y son el mejor acompañamiento para las tecnologías de seguridad. Mientras estas últimas se encargan de prevenir ante la probabilidad de algún tipo de incidente, la educación del usuario logrará que este se exponga menos a las amenazas existentes, algo que de seguro cualquier lector deseará en su uso cotidiano de Internet.

MECANISMOS DE FILTRADO

Controles parentales

Los controles parentales son programas que realizan una función de análisis detallado de las palabras claves definidas y de los listados con sitios web autorizados o prohibidos. Además, permiten limitar la cantidad de tiempo de navegación y determinar horarios para permitir el acceso a Internet, también impiden el acceso a sus datos personales, bloquean el acceso a ciertas informaciones, etc. Estas herramientas son solo una ayuda, no nos garantizan la seguridad de nuestros hijos en Internet, son los padres los que mejor asistiremos a nuestros niños.

Como activar el control Parental en Windows 7, 8 y 8.1

PASOS:
1. Vamos a Inicio -> Panel de control -> Cuentas de usuario y protección infantil.

2. Pulsa sobre Configurar el Control parental para todos los usuarios. (Tenemos que confirmar la petición y, en algunos casos, escribir la contraseña de administrador).

3. Indica la cuenta sobre la que quieres establecer el Control Parental y pulsa sobre Activado, aplicar configuración actual. (Es conveniente que nuestros hijos tengan una cuenta personalizada, sin permisos de administrador para utilizar el computador personal, que no puedan utilizar la misma cuenta de los padres).

4. Definidos estos parámetros podrá establecer los controles requeridos para su servicio: – Límites de tiempo. – Acceso a juegos. – Permitir o bloquear programas específicos.

Como activar el control Parental en Windows 10

PASOS:
1. Hay que ir a Configuración > Cuentas > Familia y otros usuarios. En Tu familia hay que pulsar sobre Agregar familiar.

2. Se puede agregar un menor, por ejemplo, un Hijo, e indicar si puede o no iniciar sesión, entre otras opciones.

3. Hay que pulsar, a continuación, sobre Administrar la configuración de la familia en línea con el fin de configurar el control parental.

4. El último paso consiste en la personalización del control parental verificando los siguientes parámetros: Actividad reciente, Exploración web, Aplicaciones, juegos y multimedia, o Tiempo en pantalla.

Video Instructivo habilitar control parental en Windows 10

https://www.youtube.com/watch?v=ROzX3GlIUh4

Video Instructivo habilitar control parental en Windows 11

https://www.youtube.com/watch?v=NMDaYgQiZVk

Además, en las siguientes direcciones encontrarán mecanismos de filtrado o control parental que puedan ser instalados en sus equipos o teléfonos.

Qustodio

https://www.qustodio.com/es/

Bloquea las aplicaciones, los juegos y los sitios web que consideres inapropiados. Podrás permitir que tus hijos naveguen por páginas apropiadas para su edad y bloquear automáticamente los sitios potencialmente peligrosos para protegerles del contenido para adultos, los juegos de azar, la violencia y otro tipo de amenazas. Te enviaremos una notificación cada vez que intenten acceder al contenido bloqueado.

secureKids

https://securekids.es/

https://family.norton.com/web/

La herramienta de control parental tiene una función dedicada a bloquear todo tipo de contenido que sea inapropiado para tus hijos.

https://famisafe.wondershare.com/es/

FamiSafe Porn Blocker.

La aplicación de bloqueo de porno FamiSafe es sin duda la mejor aplicación de bloqueo de porno que puedes utilizar. Dado que es extremadamente fácil de usar y puede bloquear el contenido porno de forma integral, no tendrás ningún problema aprender a bloquear las aplicaciones porno o los sitios para adultos en el teléfono de tu hijo. Además, los padres también pueden controlar los textos de las redes sociales que contengan palabras clave pornográficas o detectar imágenes pornográficas. La aplicación del filtro porno es compatible con todos los principales dispositivos Android, iOS, Windows, Mac y Kindle Fire.