¿Tienes niños en casa?

¿Estas preocupado por el contenido de información que pueden adquirir en sus navegadores?

¡Protégelos!
Con mecanismos de filtrado a contenido.

MECANISMOS DE FILTRADO

Existen aplicaciones y herramientas que impiden a un usuario acceder a diferentes tipos de contenido de cualquier índole como Sitios web, aplicaciones, plataformas, servicios sobre Internet, entre otros; para ello existen varias categorías, desde los que se instalan a propósito en una terminal que solo afectan el tráfico de red local, (computadora, teléfono móvil), hasta los que se imponen a gran escala, como los filtros a nivel de servidor, dirección IP, nombre de dominio, entre otros.

En nuestra infraestructura contamos con la protección que nos brinda la plataforma **WISPRO**; En la cual se bloquean más de 30.000 sitios por medio de listados que se actualizan mensualmente para proteger el con contenido inapropiado, violento, *pornográfico* y que atenta *contra la niñez*.

Dicho proceso se realiza de la siguiente forma: Con un filtro de Pornografía infantil **(PO)** y se implementa a través de redirección por **DNS,** Así:

1. Sobre el BMU se carga un archivo que contiene todas las páginas bloqueadas por el MINTIC.
2. Cuando un usuario intenta acceder al dominio que se encuentra bloqueado, este es redirigido al BMU, a la interfaz LOOPBACK (127.0.0.1).
3. Esto mostrara un error de conexión en la pantalla de los usuarios negando su acceso e intentos.

Esto implica que cada vez que un usuario de la red quiera ingresar a alguno de los URL de esos dominios, el BMU automáticamente realizara una redirección a la IP 127.0.0.1. Y en caso de que el cliente realice un cambio en su DNS locales, quitando la IP del BMU como DNS, el bloqueo continuara funcionando ya que cuando el pedido llegue al BMU se realizara el redireccionamiento automático.

A demás sugerimos a nuestros clientes, tomar en cuenta las algunas recomendaciones que se deben hacer de manera individual e instalar de forma local, para reforzar la seguridad de nuestro servicio de internet de amenazas que existen en la web.

CONTROL PARENTAL:

El control parental es un mecanismo usado por adultos para controlar en diferentes sitios web, sistemas operativos o equipos el acceso y uso que los menores de edad le dan a internet.

A través del control parental podemos monitorear la navegación, restringir contenidos no aptos para menores y bloquear páginas o usuarios que puedan ser una amenaza para los niños.

El funcionamiento suele ser muy sencillo e intuitivo, se instala la aplicación en el móvil o tableta, y se crea una cuenta en la web con la que se conecta al móvil, con ello ya se puede disfrutar de las ventajas que tienen estas herramientas y de la tranquilidad que ofrecen a sus usuarios.

Las características que pueden tener disponibles este tipo de herramientas son las siguientes:

Control Web: El control parental permitirá bloquear sitios web en función de las diferentes categorías que existen, o si lo prefieres puedes poner páginas web concretas las cuales se pueden bloquear.

Control de aplicaciones: De este modo podemos hacer que nuestros hijos no puedan tener acceso a ciertas aplicaciones como por ejemplo programas de mensajería instantánea, aplicaciones de redes sociales, acceso a navegadores web, acceder al Google Play o Apple Store para realizar compras, etc.

Bloqueo de llamadas: Con esta herramienta podrás bloquear los teléfonos a los que no se podrán emitir o recibir llamadas, además de definir el funcionamiento ante llamadas internacionales o números desconocidos.

Tiempo de uso: Con lo que se podrá controlar la cantidad de tiempo de uso que tu hijo pueda tener acceso a las diferentes categorías como por ejemplo juegos o navegadores.

Alarmas: Con esto podrás determinar alarmas para el dispositivo de tu hijo, avisándole de cualquier cosa.

Geolocalización: Te permite conocer la localización en la que está situado tu hijo conociendo donde se encuentra en tiempo real.

Botón de Emergencias: Añade un "Botón del Pánico" al teléfono de tu hijo con el que te envía una alerta de emergencia avisando de una situación excepcional.

ANTIVIRUS:

Debemos preguntarnos **¿Qué es un antivirus? y ¿para qué sirve?**

Al navegar por internet, descargar archivos o recibir mails entre otras tareas online generando inseguridad para tu ordenador, además de generar lentitud en la navegación. El antivirus informático ayuda a proteger el equipo y evitar que se pueda perder información importante.

Un antivirus es un tipo de software que se utiliza para evitar, buscar, detectar y eliminar virus de una computadora o equipo electrónico de navegación. Una vez instalados, la mayoría de los software antivirus se ejecutan automáticamente en segundo plano para brindar protección en tiempo real contra ataques de virus.

EL PHISHING (suplantación de identidad):

PHISHING es el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito.

Como ocurre en la pesca, existe más de una forma de atrapar a una víctima, pero hay una táctica de PHISHING que es la más común.

Si un usuario pica el anzuelo y hace clic en el enlace, se le envía a un sitio web que es una imitación del legítimo. A partir de aquí, se le pide que se registre con sus credenciales de nombre de usuario y contraseña.

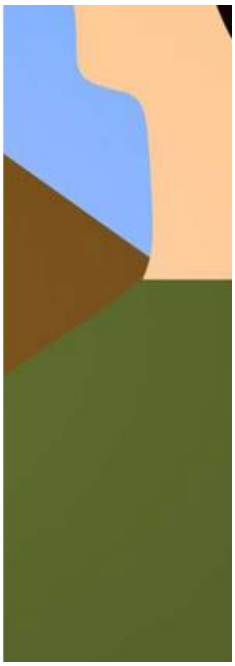
Las víctimas reciben un mensaje de correo electrónico o un mensaje de texto que imita o "suplanta la identidad" de una persona u organización de confianza, como un compañero de trabajo, un banco o una oficina gubernamental; Cuando la víctima abre el correo electrónico o el mensaje de texto, encuentra un mensaje pensado para asustarle, con la intención de debilitar su buen juicio al infundirle miedo. El mensaje exige que la víctima vaya a un sitio web y actúe de inmediato o tendrá que afrontar alguna consecuencia.

Si es lo suficientemente ingenuo y lo hace, la información de inicio de sesión llega al atacante, que la utiliza para robar identidades, saquear cuentas bancarias, y vender información personal en el mercado negro.

GROUP
NIT: 901.175.142-7

MALWARE: ¿Cómo evitarlo?

Se llama **malware** a cualquier tipo de programa que realiza Acciones dañinas en un sistema sin que la persona se dé Cuenta y de forma intencionada, estas actividades dañinas Incluyen robo de información, mal funcionamiento del sistema, chantajear al dueño del equipo solicitando dinero para que pueda volver a recuperar la información, Acceso a clientes no autorizados.



Prevención contra el malware:

- Tener navegador y sistema operativo actualizado.
- Tener contraseñas de alta seguridad.
- Evitar descargar software de redes P2P ya que no se sabe de donde provienen.
- Tener precaución al ejecutar software procedente de internet o por medio extraíble como CD, memorias USB.
- Tener instalado un antivirus y un firewall y tener activado las actualizaciones automáticas.
- Se recomienda hacer copias de respaldo sobre la información que hay en el equipo, para que en caso de un ataque la copia de seguridad hecha este 100% segura y libre de malware.