RECOMENDACIÓN PARA EL CONTROL DE CONTENIDO DE USO DE INTERNET EN EL HOGAR

Ahora que los niños pasan más tiempo conectados al **internet,** ya sea por clases virtuales, deberes y tiempo de ocio; están más expuestos a contenido peligroso. En este contexto, iniciar o reforzar el control parental se vuelve una necesidad imperante. ¿Cómo hacerlo, existen herramientas de apoyo, qué contenido puede ser nocivo para los estudiantes?

"Si bien, internet ha sido clave para la teleeducación en tiempos de pandemia, el acceso a las miles de posibilidades que permite, tales como: visualización de vídeos de todo tipo (musicales, tutoriales, películas…), recorridos virtuales, juegos en línea, libros digitales, bibliotecas virtuales, entre otros… exige tener un mayor control sobre su uso, sobre todo para los más pequeños de la casa. Sin querer podrían terminar en un sitio con contenido para adultos, ingresar información personal para favorecer un ataque cibernético, entre otros peligros", explica **John Holguin**, experto de HughesNet.

Recomendaciones para el uso seguro de internet:

Existen varias pautas básicas para realizar una navegación segura:

1. **Filtrar y bloquear contenido violento o pornográfico:** Este proceso es fácil de realizar, ya que en los buscadores (Google Chrome, Firefox, Kiddle) y navegadores (Teen Browser, Kidoz, Zoddles) existen opciones para elegir la información permitida para búsquedas. Por ejemplo, en la configuración de Google Chrome se debe seleccionar "aplicar controles de filtro" y activar el ítem "permitir solo algunos sitios".
2. **Minimizar el seguimiento de anunciantes:** Es importante enseñar a los niños cómo eliminar las cookies en cada tipo de navegador o navegar en privado para que no tengan anunciantes que los sigan en toda la web. Esto debido a que las cookies pueden ser un punto de entrada para algunos ataques cibernéticos, por lo que es necesario eliminarlas con regularidad. También se debe indicar a los pequeños que, al dar click en anuncios o ventanas emergentes se corre el riesgo de introducir malware en el sistema o algún otro virus informático.
3. **Actualización de navegadores y software:** Las actualizaciones para navegadores o sistemas operativos tienen parches de seguridad que pueden evitar daños, por lo que aceptar las actualizaciones es lo mejor, ya que incluyen el mantenimiento actualizado de antivirus y firewalls.

3. **Actualización de navegadores y software:** Las actualizaciones para navegadores o sistemas operativos tienen parches de seguridad que pueden evitar daños, por lo que aceptar las actualizaciones es lo mejor, ya que incluyen el mantenimiento actualizado de antivirus y firewalls.
4. **Establecer límites de tiempo de uso:** Para menores de dos años, lo más recomendable es establecer el uso ocasional de pantallas con acompañamiento de sus padres en horas adecuadas. De dos a cinco años, fijar un máximo de una hora al día y; de cinco años en adelante (hasta la adolescencia), lo ideal es no exceder las 4 horas, sin contar con el tiempo de clases virtuales. De igual manera, se aconseja distribuir los horarios (mañana, tarde o noche) de acuerdo a las necesidades del hogar.
5. **Monitoreo de redes sociales:** En muchos casos, el contenido peligroso puede encontrarse directamente en las redes sociales de los niños. Para filtrar palabras prohibidas y contenido indebido, también existen aplicaciones móviles especializadas: Mamabear, Qustodio, Net Nany, Teen Safe y Circle.
6. **Establecer perfiles para cada usuario:** Otra alternativa es crear cuentas para cada usuario del computador, con el fin de establecer el acceso a contenido determinado para cada uno. Este proceso es sencillo, ya que el sistema operativo de Windows cuenta con esta alternativa, solo se necesita ir a configuración, seleccionar "Cambiar configuración de PC", después ir a "Cuentas" y, a continuación, pulsar "Agregar una cuenta" e ingresar la información respectiva conforme las instrucciones y listo. Al terminar este procedimiento, se debe configurar el control parental en los buscadores de cada perfil (punto 1). Es importante que los usuarios de los adultos tengan clave privada, a fin de evitar el acceso de los niños.

Algunas herramientas digitales de control parental:

Además, existen otras **herramientas** prácticas para controlar o bloquear el acceso a contenidos. Las más comunes son:

1. **Control web:** Este tipo de herramientas permiten limitar las páginas web a las cuales acceden los niños. La forma más sencilla es habilitando "Google SafeSearch" en cualquier navegador que usen. Para esto se debe configurar a Google como motor de búsqueda predeterminado y activar esta opción.

2. **Acceso a aplicaciones:** Limitar el acceso a Google Play o App Store evitará que los niños accedan a APPs indebidas e incluso evitará que realicen algún tipo de compra online.
3. **Bloqueo de llamadas:** Esta opción permite evitar la entrada de llamadas de números desconocidos o internacionales. Su función garantiza que los usuarios no tengan contacto de este tipo con desconocidos.
4. **Geolocalización:** Actualmente los celulares y computadoras permiten tener acceso a la ubicación del dispositivo en tiempo real, esta herramienta ayuda a conocer el lugar exacto de la persona y se puede usar como una medida de seguridad preventiva.
5. **Google Family Link:** Es una aplicación gratuita que permite conocer la información que ven los niños en internet y en sus dispositivos.
6. **Windows Live Family Safety:** Es gratuita y viene incluida en todos los dispositivos Windows, de igual manera permite verificar el contenido al cual están expuestos los niños.