El **control parental** es una herramienta destinada a asegurar la navegación de los niños por Internet por parte de los adultos. No se debe confundir con los software espías. Según la UNICEF, contenidos violentos, información errónea o directamente mentiras forman parte de muchos sitios y juegos infantiles. Los controles parentales son muy útiles, pero al mismo tiempo se deben inculcar hábitos de navegación segura. De hecho, los niños tienen cada vez más acceso a dispositivos móviles que se han transformado en un objeto personal ligado a su intimidad y privacidad, cada vez más lejos de la supervisión de los padres.

Control parental: definición y tipos de controles parentales

Los controles parentales son aplicaciones que los adultos pueden configurar en los dispositivos que utilizan los niños. Su objetivo es limitar el acceso a contenidos inapropiados. También, planificar y administrar el tiempo frente a la pantalla.

Hay diferentes tipos de aplicaciones. Sin embargo, el **control parental** no se debe confundir con los software espías. De hecho, no lo son. En cambio, el control parental debe instalarse con total transparencia y explicando a los niños los motivos, con palabras que ellos puedan comprender.

La mayoría de los controles parentales permiten:

- Crear diferentes tipos de perfil. Así, se pueden adaptar las restricciones de acuerdo a la edad y hábitos de los niños. Por ejemplo, para los más pequeños conviene permitir el acceso a una selección de sitios predefinidos y sin espacios de diálogo.
- Prohibir el acceso a contenidos inapropiados.
- Limitar el tiempo de conexión estableciendo horarios de acceso o cuotas de horas por período.
- Limitar el acceso a juegos, software y aplicaciones.
- Controlar los usos digitales consultando el historial de navegación.

En tanto, hay diferentes tipos de software de control parental:

- Según el dispositivo en que se activan: celulares, computadoras o tabletas. Incluso televisores inteligentes y consolas de videojuegos.
- De acuerdo al servicio: se puede instalar el control parental en servicios de streaming, redes sociales o videojuegos.

Activación de los controles parentales en videojuegos y consolas

Los videojuegos pueden ocultar peligros muy grandes para los niños. Desde la ONG Mamá en Línea, dedicado a combatir el grooming, advierten los riesgos de distintos juegos, redes sociales y servicios de mensajería como Whatsapp. Al mismo tiempo, brindan orientación acerca de cómo utilizarlos de manera segura.

Algunos juegos como Fortnite incluyen la posibilidad de activar el control parental. Se debe vincular una cuenta de correo electrónico a la cuenta del juego. Una vez asociadas, se genera un PIN para configurar las opciones.

Por ejemplo en Fortnite se puede realizar ajustes para:

- No visibilizar lenguaje adulto.

- Bloquear solicitudes de amistad.
- Ocultar el nombre.
- Desactivar el chat de voz y de texto.
- Obener informes semanales de tiempo de juego.

También se puede activar el control parental en consolas de videojuegos. Por ejemplo:

- Playstation. Se debe inicir sesión e ir a la opción de Administración de familia. Se debe seleccionar al niño para el que se establecerá el control parental y editar cada función para ajustarla. Para que el control parental sea efectivo se debe verificar el correo electrónico e iniciar sesión en la plataforma. Para evitar que el niño inhabilite el control parental, se debe establecer quién puede realizar estos cambios en la configuración.
- Nintendo. El control parental se realiza a través de una aplicación que se descarga de App Store o Google Play. La aplicación permite controlar el tiempo de juego, qué juegos se jugaron y con quién o quiénes.También, restringir el acceso a juegos que se considera que no son apropiados para su edad. Para poder utilizar la aplicación se debe contar con una cuenta Nintendo.

Aplicación del control parental a computadoras personales, portátiles y tabletas

Al igual que los teléfonos móviles, muchas marcas de tablets tienen una función de control parental integrado. Se debe activar desde la configuración o descargando una aplicación.

- El sistema operativo Windows cuenta con su propio control parental. Permite establecer restricciones y controlar el tiempo que se pasa frente a la computadora. Para comenzar se debe crear una cuenta independiente para el niño, la cual se agrega a la cuenta familiar de Microsoft. A continuación, se debe autorizar a esta cuenta para que inicie sesión en Windows. Para que los controles parentales funcionen, los niños deben ingresar siempre con esta cuenta.
- Google. El más popular de los buscadores cuenta con Family Link, un conjunto de herramientas diseñadas para establecer los controles parentales. También puede descargarse como aplicación para smartphones. Permite una mayor protección en línea y herramientas para entender cómo los niños utilizan los dispositivos. También, compartir ubicación, administrar la configuración de la privacidad y mucho más. La configuración de la supervisión puede llevar unos 10 minutos y tanto el adulto como el niño deben tener su propia cuenta en Google.
- Linux. El sistema operativo Linux también permite el control parental. Para habilitarlo, se deben crear cuentas para los niños sin derechos de administrador. También, establecer los horarios y limitar las aplicaciones que pueden usar.

Buenos hábitos de seguridad en Internet, aliados clave

Los buenos hábitos para una navegación segura en Internet son los mejores aliados del control parental. Como decíamos anteriormente, al instalar los filtros y controles parentales es importante informar al niño cómo funcionan y por qué se habilitan. Todo de manera sencilla para que lo entienda. No recomendamos, de ninguna manera, instalar software espías.

La ONG Mamá en Línea brinda valiosos consejos para una navegación segura en Internet y dispositivos móviles.

Uso seguro de Whatsapp

- Habilitar la verificación en dos pasos.
- Hacer privada la foto del perfil.
- Asignar un PIN seguro al buzón de voz.
- Siempre, verificar la identidad de quien llame o realice un pedido inusual.
- Prestar atención para saber si ha sido víctima de un robo de identidad.
- No compartir códigos de verificación.

Evitar ser víctima de acosadores sexuales

La pornografía infantil y el acoso sexual a niños, niñas y adolescentes es uno de los mayores riesgos de Internet. Además del **control parental**, los niños deben saber reconocer cuándo están en peligro.

- No hablar con extraños.
- No brindar datos personales ni compartir públicamente fotografías personales, de la familia, compañeros o amigos, la casa o la escuela.
- Evitar los seudónimos que pueden revelar sexo o edad, por ejemplo Carlita2010.
- No encontrarse con supuestos amigos de Internet en lugares privados. Si se establece un encuentro, debe ser siempre en un lugar público, como una plaza o un centro comercial. Además, se debe avisar a los padres que se está por producir un encuentro. Detrás de un supuesto nuevo amigo se puede estar ocultando un adulto con las peores intenciones.