Prevención CiberViolencia

Guia de mediación parental para el acompañamiento a menores en el uso de internet.

Índice.

Guía de mediación parental para el acompañamiento a menores en el uso de internet.

Aviso de descargo de responsabilidad:

Tanto en las redes sociales, página web y publicaciones que se llevan a cabo en los distintos canales de comunicación por medio de internet del proyecto social sin fines de lucro “Prevención Ciberviolencia” se busca realizar una difusión oportuna y novedosa de información que le sea de utilidad a las personas usuarias de internet y seguidoras de nuestros post, publicaciones y rede sociales, dicha información muchas veces es proveniente de otras fuentes ajenas a “Prevención Ciberviolencia, el objetivo del presente documento es meramente informativo.

Texto: Dania Bejarano Morales.

Facebook: Prevención Ciberviolencia.

Instagram: Ciberviolencia.

LinkedIn: Prevención Ciberviolencia.

TikTok: @preven.Ciberviolencia

https://www.prevencionciberviolencia.org

GUÍA DE MEDIACIÓN PARENTAL Y ACOMPAÑAMIENTO A MENORES EN EL USO DE INTERNET.

Las personas menores de edad están creciendo en una sociedad marcada por el uso intensivo de las nuevas tecnologías e Internet, un mundo en el que el entorno físico y el virtual se entremezclan en un continuo. La adopción de estas tecnologías por los menores cada vez se produce a edades más tempranas, ofreciéndoles grandes oportunidades para su desarrollo personal y profesional, pero también exponiéndoles a sus riesgos asociados cuando no se les brinda un acompañamiento adecuado.
La solución más propicia ante esta problemática es la llamada mediación parental.

¿Qué es la mediación parental y para qué sirve?

Es una forma responsable de realizar un acompañamiento y protección a las personas menores de edad cuando hacen uso de internet, redes sociales o plataformas digitales y consiste en un conjunto de estrategias psicosociales y tecnológicas que empleamos padres y madres, así como personas cuidadoras.

Nos sirve para:

- Prevenir riesgos mientras los menores hacen uso de internet.
- Detectar y afrontar problemáticas relacionadas con el uso de internet
- Acompañar y supervisar a los menores a que hagan un uso responsable de internet.

LA MEDIACIÓN PARENTAL SE DIVIDE EN DOS: LAS ESTRATEGIAS ACTIVAS Y LAS RESTRICTIVAS.

Las estrategias activas son aquellas en las cuales la persona adulta se encarga de dar una asesoría al menor. Una de las maneras más efectivas para mediar en el uso que hacen los menores en Internet, pasa por prestarle atención a lo que hace cuando está conectado. Los niños y niñas se comportan de manera diferente cuando sienten que alguien está prestando atención a lo que hacen. En este sentido, es recomendable que se les haga una supervisión amigable presencialmente, al menos en los comienzos, acompañándole en la exploración y en el aprendizaje. Las estrategias activas se dividen a su vez en tres acciones:

- **Supervisión:** Estar al tanto de su actividad en internet, por ejemplo: las aplicaciones, redes sociales, juegos en línea, entre otros que son de su preferencia o que más utiliza cuando navega en internet. También es importante que se tenga información sobre los contactos que frecuenta la persona menor de edad.
- **Acompañamiento:** Cuando las personas menores de edad están comenzando a utilizar internet, redes sociales y plataformas digitales, es importante que como familia también existan actividades que puedan realizar y compartir en línea, es decir, pasar tiempo dentro y fuera de internet de calidad.
- **Orientación.** Es importante fortalecer la relación de confianza con las personas menores de edad para que puedan acercarse a resolver dudas en caso de que existan, de igual manera con la orientación adecuada se busca potenciar sus habilidades sociales y su pensamiento crítico cuando hacen uso de internet

1. **Las estrategias restrictivas:** son aquellas que sirven para fomentar el orden y manejo adecuado del tiempo en el uso de internet, éstas a su vez se dividen en 3 acciones:

- **Normas y límites.** Las normas y los límites sirven para que existan acuerdos coherentes, consistentes y pactados con las personas menores de edad, en ellas se debe establecer cuanto tiempo, en qué lugares y

bajo que circunstancias se hará uso del internet y de los dispositivos, es de amplia recomendación anteponer las actividades escolares a las de ocio y entretenimiento en internet.

- **Controles parentales.**

Estas son herramientas son utilizadas como una especie de apoyos técnicos complementarios que limitan el contenido que pueden ver o no las personas menores de edad cuando hacen uso de internet, redes sociales o aplicaciones digitales, pudiendo restringir el contenido con base a las clasificaciones que se tiene de contenido apto o no para menores. De igual manera se puede hacer un seguimiento del tipo de uso que le dan los menores a ciertas aplicaciones.

- **Opciones de bienestar y seguridad.**

Algunas plataformas utilizan controles de bienestar con los cuales se puede configurar un horario para el uso de las pantallas en cuanto al tiempo de uso y posterior a este tiempo se emite una advertencia que invita a la persona menor de edad dejar de usar el dispositivo para que pueda descansar las horas adecuadas para su edad. Hay que tomar en cuenta que también existe la posibilidad de realizar las configuraciones adecuadas a las redes sociales para que únicamente las personas que seleccionemos tengan acceso a la información que publicamos.

¿DE QUÉ RIESGOS ESTAMOS PROTEGIENDO A LOS MENORES CON LA MEDIACIÓN PARENTAL?

Acerca de la hiperconectividad y el tiempo de uso.

Las redes sociales, plataformas digitales y en general en uso de internet tiene muchas ventajas y herramientas que pueden mantenernos conectados en una infinidad de tiempo y esta situación especialmente es atractiva para las personas menores de edad ya que justamente estas herramientas están diseñadas entre otras cosas para enganchar a sus usuarios con atractivas opciones para su uso.

Este “enganche” hace que las personas menores de edad puedan pasar la mayor parte de su día conectados a internet, lo peligroso no radica en que estén o no conectados, sino en el hecho de que por permanecer conectados o en actividad en línea pongan en riesgo otras actividades y relaciones interpersonales y esto disminuya su calidad de vida o pueda incluso poner en riesgo al menor de edad de padecer una ciberadicción.

Adicciones comportamentales relacionadas con las tic´s (ciberadicciones)

Debido justamente a los altos estímulos adictivos que conlleva el uso de las Tics, en las personas usuarias, muchas veces cuando se logra establecer un acompañamiento y mediación adecuada, las personas menores de edad pueden comenzar a depender cada día y en mayor medida de la tecnología, a continuación, conoce algunos indicadores que debes tomar en cuenta y observar en el comportamiento de tu hijo o hija para detectar a tiempo el inicio a una ciberadicción.

SINTOMAS:

1.Uso excesivo: Actividad predominante durante la mayor parte del día, todos los días.

2. Pérdida de control y del tiempo con necesidad de un uso cada vez mayor. Esto tiene que ver, por ejemplo, si en un inicio el menor dedicaba 2 horas al día a navegar en internet para entretenerse, ahora ya no le serán suficientes esas 2 horas, sino que buscará pasar más tiempo pudiendo incluso desvelarse con tal de permanecer en línea.

Es importante mencionar que el tiempo de uso en las actividades académicas no refiere como tal a un tiempo de uso inadecuado, sino más bien el tiempo destinado a navegar por ocio, para actualizar redes sociales, jugar en línea, entre otras acciones.

2. **Presentar reacciones de irritabilidad o nerviosismo ante la imposibilidad de realizar actividades online.**

Se observará un malestar psicológico evidente ante la falta de conexión a internet, o la imposibilidad de hacer uso de él. Dicho malestar puede observarse como falta de apetito, cambios en su estado de ánimo, dolores musculares, sensación de estar desesperado, entre otros.

3. **Afectaciones en cuanto a rendimiento académico.**

Este tipo de comportamiento es uno de los primeros que se observa en la persona menor de edad, sus calificaciones y rendimiento escolar se ve afectado notablemente y no existe otra razón aparente observable que un desajuste en el tiempo excesivo que pasa en línea.

4. **Anhedonia.**

Este término hace referencia a cuando la persona en cuestión pierde el interés en las actividades que antes le gustaba realizar o le generaban placer, por ejemplo, si a una persona antes le gustaba mucho sacar a pasear al perro, ahora eso lo verá como una actividad que no le genera placer ni interés por lo cual va a evitarla.

5. **Aislamiento o deterioro social, familiar.**

Se observa que la persona se aleja cada vez más de su círculo de amigos o familia, con tal de permanecer realizando actividades en línea.

7. Descuido en el arreglo personal.

La persona ya no toma en cuenta su apariencia o aspecto físico y descuida por completo su bienestar en general con tal de permanecer utilizando el internet o los dispositivos.

MATERIAL Y CONTENIDO QUE SE PUEDEN ENCONTRAR EN LÍNEA.

Material con violencia o contenido sexual no apto para las personas menores de edad:

Con frecuencia cuando navegan y no existen filtros o protecciones en cuanto al contenido se pueden topar como imágenes de personas en situación de desnudez o con contenido que haga apología a cualquier tipo de violencia, cuando los menores observan este tipo de información y no se les da una adecuada explicación de lo que están viendo les puede generar conflicto el percibir estas situaciones.

SITUACIONES DE ACOSO O ABUSO EN LÍNEA.

Ciberbullying.

Existen muchos casos en donde menores de edad se encuentran inmersos en una situación de acoso entre pares en los entornos digitales a esto le llamaremos “Ciberbullying”, esta situación puede generar mucho malestar en la víctima tanto, como si el acoso estuviera siendo de persona en persona.

Muchas de las veces pensamos que por tratarse de una situación de “bromas” en el entorno digital no es para tanto, sin embargo, esta problemática puede que trascienda desde “bromas hirientes” hasta una “ciberpersecusión” y “campañas de desprestigio en contra del menor de edad.

El ciberbullying es una situación de acoso, esta situación puede darse en forma de agresión o violencia verbal: insultos, descalificaciones, desprecios verbales amenazas verbales, intimidaciones, chantajes, exclusión social: rechazo manifiesto a la participación en actividades en grupo (tanto en el mundo físico como en la comunicación on line), difusión de rumores e informaciones dañinas.

Abuso sexual online. (Child-grooming)

Hablar de abuso sexual online toma en cuenta el hecho de que una persona se encuentre pendiente todo el tiempo de la actividad en línea de un menor de edad, esta persona puede ser igualmente un menor de edad o tratarse de una persona adulta y cuando la última situación está ocurriendo se trata de una forma de abuso sexual en los entornos digitales utilizando una técnica es llamada *Child-grooming* y consiste en que un adulto se hace pasar por otra persona utilizando una identidad digital falsa para que por medio de esta pueda contactar a un menor de edad y solicitarle material o contenido intimo o incluso un encuentro en persona, pueden contactar a menores de edad por medio de redes sociales, chats o grupos o por medio de video juegos en línea, dada la facilidad de acceso que tienen a los medios digitales.

Una de las consecuencias más graves que puede tener el Child-grooming es que el acosador por internet puede obtener información personal o imágenes intimas del menor de edad y chantajearlo para conseguir más contenido, o incluso convencer al menor de que se vean físicamente y entonces se realizan otro tipo de acciones en contra del menor pudiendo secuestrar y utilizar al menor en una de las formas de trata de personas.

Suplantación de identidad del menor en internet.

En muchas ocasiones las personas menores de edad se ven afectadas por esta problemática que consiste en que alguien toma información personal del menor de edad ya sea su foto, correo u otra información de relevancia y crea una cuenta con estos datos para perjudicar al menor.

Ciberacoso sexual.

Se refiere a la Conducta reiterativa y no solicitada que consiste en hostigar a una persona con la finalidad de obtener un beneficio de tipo sexual, se percibe por medio de mensajes de acoso, audios, llamadas, textos con insinuaciones o palabras que generan incomodidad en la víctima.

Trata de personas menores de edad en internet.

La captación de menores por internet para tema de trata de personas es una situación alarmante y que va en aumento, algunas veces los menores son las víctimas, pero no lo saben.

Los tratantes suelen esconderse en nombres falsos y, la mayoría de las veces, les ofrecen trabajos con pagos tan atractivos. A las adolescentes les dicen que las harán modelos cuando finalmente las convierten en “damas de compañía” y esta es una forma de explotación sexual comercial. En algunas ocasiones, hasta recurren a los chantajes y extorsiones con fotos íntimas para que las víctimas accedan. Los principales medios de captación son las redes sociales, los chats los foros, las aplicaciones digitales, los grupos de telegram o WhatsApp.

SITUACIONES QUE PUEDAN PONER EN RIESGO LA INTEGRIDAD DE MENORES EN INTERNET.

Reclutamiento de menores de edad por grupos delincuenciales.

El reclutamiento y la utilización de niñas, niños y adolescentes por grupos delictivos es un problema público que debe atenderse y visibilizarse de manera urgente en México ya que éste constituye una de las formas más graves de la violencia contra las niñas, niños y adolescentes en el país. Actualmente, los grupos de delincuencia organizados utilizan como medios de captación a menores las plataformas digitales, las redes sociales o los juegos en línea, debido justamente a la facilidad de acceso que tienen de estos medios.

Muchas veces las personas menores de edad acceden a realizar actividades ilícitas o delictivas debido a que en la mayoría de las ocasiones los delincuentes les ofrecen atractivas sumas de dinero o artículos lujosos con tal de convencer a los menores y tener sus servicios en los grupos delictivos.

Ciberdelincuencia juvenil.

“Es importante hablar con menores de edad y adolescentes sobre las conductas ilícitas que se llevan a cabo en los entornos digitales”.

El "modelo de negocio" de la ciberdelincuencia se basa en la creación de una cadena de valor que ofrece nuevos métodos, por ejemplo, la ciberdelincuencia como servicio, es decir, la práctica de facilitar las actividades ilegales a través de los servicios. En otras palabras, cualquiera podría adquirir todo lo que necesita para organizar fraudes o ciberataques, independientemente de sus habilidades o conocimientos técnicos, recientemente ha aumentado la actividad de jóvenes que se ven relacionados en este tipo de situaciones. Sabemos que los ciberdelincuentes casi siempre buscan ganancias financieras, pero parece que esto no suele ser lo que los jóvenes ciberdelincuentes tienen en mente cuando dan sus primeros pasos hacia el "lado oscuro". Muchos de los jóvenes que realizan estas acciones no están necesariamente motivados por la recompensa financiera. De hecho, el reconocimiento de sus compañeros, la popularidad en los foros a los que pertenecen y una sensación de éxito son factores de influencia más grandes. "La sensación de logro al completar un desafío y probarse a sí mismo ante sus compañeros son las principales motivaciones para aquellos involucrados en la cibercriminalidad”. Hay otro factor importante que tienta a muchos jóvenes a involucrarse en el mundo de la ciberdelincuencia: la sensación de que no es un delito en el "sentido tradicional", y que no serán arrestados por llevar a cabo un ciberataque. Otro factor que tomar en cuenta es que a los jóvenes les atrae es la facilidad con la que pueden comenzar a lanzar ataques o actividades maliciosas. Hay todo tipo de herramientas disponibles en línea que no son ni caras ni difíciles de usar.

Medidas para la prevención de riesgos en línea.

MEDIDAS PARA LA PREVENCIÓN DE RIESGOS.

ESTRATEGIAS AFECTIVAS:

Lo más importante para tener un acercamiento adecuado con los menores es establecer una comunicación abierta y sencilla acerca de las situaciones que pueden pasar en línea, considerando aquellas en las que se pueden poner en riesgo, así como las áreas de oportunidad y de crecimiento en temas de seguridad en internet. Una comunicación abierta y neutral sobre los usos adecuados e inadecuados de internet, redes sociales, plataformas y herramientas digitales. La confianza adecuada ayudará a los menores a decir sus inquietudes o situaciones de incomodidad con el uso de internet.

ESTRATEGIAS TÉCNICAS:

Herramientas de control parental.

Las herramientas de control parental son utilizadas como una herramienta en el aprendizaje y vida digital de los menores, ayuda para limitar las funciones, lo que pueden observar o no, así como el alcance que tienen sus dispositivos cuando se conectan a internet.

Filtrado de contenidos: mediante diferentes sistemas, bloquea el acceso del menor a ciertos contenidos inapropiados (habitualmente de connotación sexual o violenta).

Control de tiempo: emite alertas o interrumpe la navegación al alcanzar determinada hora o límite de tiempo.

Supervisión de actividad: genera informes con el historial de navegación, búsquedas o reproducción multimedia.

Geolocalización: sigue la posición actual y el recorrido anterior del dispositivo.

Protección de la configuración: evita modificaciones no deseadas de los ajustes de control parental.

Xbox, Netflix, Amazon, Disney, YouTube, aplicaciones para control parental

SOBRE LAS CONTRASEÑAS SEGURAS.

Es cierto que establecer contraseñas ayuda en la privacidad y el la protección de dispositivos, por ello es importante establecer una contraseña adecuada para la protección de estos.

¿Cómo establecer una contraseña adecuada?

1. Evitar poner datos personales que puedan identificarse fácilmente, por ejemplo: minombre123
2. Es recomendable utilizar signos mayúsculas y números en ella, por ejemplo:

Contraseña no recomendada:	**Contraseña recomendada:**
Hola123comoestas	**H0l@123#C0mo3st4s#**

Métodos de doble factor de autenticación.

Si bien es cierto que las contraseñas protegen, no debemos de confiar al 100% de su capacidad por ello es recomendable establecer métodos de doble autenticación para iniciar sesiones en dispositivos etc.

La verificación en dos pasos, también conocido como doble factor de autenticación (2FA). Se trata de una metodología de autenticación que, además de requerir un nombre de usuario y contraseña, solicita el ingreso de un segundo factor, el cual podría ser un código de seguridad o un dato biométrico para que la autenticación sea exitosa.

Dicho en otras palabras, un sistema de doble autenticación es aquel sistema que utiliza 2 de los 3 factores de comprobación para una validación segura de un usuario.

Estos Factores de autenticación son los siguientes.
FACTOR 1: Algo que sabes (CONOCE): contraseña
FACTOR 2: Algo que tienes (POSEE): teléfono recibir código (OTP) o SMS.
FACTOR 3: Algo que eres (CARACTERÍSTICA ÚNICA) como huella dactilar o iris (este es uno de los niveles más altos de seguridad.

¿Dónde implementar estrategias técnicas de control parental?

Juegos de video.
PlayStation.

Opciones de control parental en los modelos de PlayStation PS5, PS4, PS3, PS Vita y PSP.
Filtrado de contenidos: permite establecer una restricción de edad para los juegos y otros contenidos audiovisuales según el código PEGI. Al conectarse a Internet en PlayStation Network, es posible impedir la comunicación con otros usuarios de PlayStation y el acceso a contenidos creados por otros jugadores.
Control de tiempo: puedes establecer un horario semanal de tiempo de juego, una duración para cada sesión de juego y/o una hora de finalización.
Bloqueo de aplicaciones: permite restringir las compras en la tiendas virtual de PlayStation creando un límite de gasto mensual.

XBOX.

Ajustes de control parental en la consola Xbox One.
Filtrado de contenidos: creando un grupo de cuentas familiar administrado por un adulto, permite limitar los juegos a los que puede acceder el menor, las búsquedas web y páginas concretas. También es posible restringir el acceso a aplicaciones y juegos determinados por el administrador familiar, así como limitar las compras en la tienda virtual.
Control de tiempo: permite configurar un recordatorio diario de tiempo, que avisará al menor cuando haya superado el tiempo establecido.
Supervisión: puedes recibir un informe semanal por correo electrónico con un resumen de las sesiones de juego, la duración de estas, los juegos y contenidos a los que ha accedido y durante cuánto tiempo.
Notificaciones: te llegará un aviso para que aceptes o deniegues la solicitud de tu hijo/a cuando quiera acceder a un contenido concreto o realizar una compra.
Control multidispositivo: puedes modificar la configuración a través de la página web de Xbox o desde la propia consola, controlando varias cuentas simultáneamente.

Plataformas digitales.

Opciones de control parental disponibles en el servicio de YouTube Kids.

Aplicación limitada con ajustes personalizables por edad y preferencias.

Filtrado de contenidos: permite adecuar los vídeos que se muestran a la madurez del menor: preescolares (menores de 5 años), niños pequeños (entre 5 y 7 años) y niños mayores (entre 8 y 12 años).

Control de tiempo: puedes establecer un tiempo de visualización, y una vez terminado, la aplicación se bloquea automáticamente.

Protección de la configuración: permite establecer un código PIN o verificar los ajustes resolviendo una operación matemática sencilla.

Bloqueo de canales: puedes bloquear canales y vídeos que consideres adecuados.

Desactivación de la función 'búsqueda': restringe los canales a los que se puede tener acceso, limitándolo a aquellos verificados por YouTube Kids como adecuados para los menores.

Opciones de control parental disponibles en el servicio de Netflix.

Filtrado de contenidos: limita las series, películas o programas calificados para edades superiores a la establecida en cada perfil, y permite bloquear manualmente aquellos contenidos que consideras inadecuados.

Protección de la configuración: permite establecer un código PIN para proteger el acceso a los ajustes de la aplicación frente a modificaciones no deseadas.

Perfiles de usuario: puedes establecer diferentes perfiles adaptados a su edad y madurez, donde se almacenarán las preferencias según contenidos que visualicen.

Opciones de control parental disponibles en el servicio de Facebook

Control de tiempo: puedes configurar un recordatorio diario de tiempo, que avisará al menor cuando haya superado el tiempo establecido.

Supervisión: la aplicación crea un informe diario indicando el tiempo empleado en la red social.

Filtrado de contenidos: es posible configurar que la cuenta sea privada, restringir los comentarios de personas desconocidas (fuera de su lista de contactos) o bloquear comentarios.

Opciones de privacidad: permite revisar el listado de amistades o configurar las notificaciones que recibirá el menor desde la aplicación.

Aplicaciones para control parental:

Herramienta de Google para dispositivos móviles con sistema Android.

Filtrado de contenidos: permite restringir las aplicaciones aprobando o bloqueando las que quiera descargar de Google Play Store.

Control de tiempo: puedes establecer límites de tiempo diarios y configurar una hora de dormir en el dispositivo.

Supervisión: permite consultar cuánto tiempo usa cada aplicación mediante informes de actividad semanales o mensuales.

Geolocalización: permite ver la ubicación del dispositivo móvil de tu hijo/a.

Protección de configuración: permite restringir la modificación de los ajustes de control parental en el sistema Android.

Herramientas de control parental para dispositivos móviles con sistema Android, iOS y Kindle.

Family time.

Filtrado de contenidos: permite restringir las aplicaciones inadecuadas para el menor.
Control de tiempo: puedes establecer un tiempo máximo para cada aplicación o juego.
Supervisión: recopila información sobre las aplicaciones instaladas, contactos, mensajes y navegación. También rastrea los mensajes y llamadas.
Geolocalización: ofrece información sobre la ubicación del dispositivo.
Notificaciones: alertas automáticas de situaciones peligrosas.

ESET parental control.

Herramienta de control parental para dispositivos móviles Android.
Filtrado de contenidos: permite filtrar páginas web por categorías, restringiendo determinados tipos de sitios web, recibiendo alertas cuando el menor quiera acceder a una web tipificada como inapropiada. También puedes bloquear el acceso a aplicaciones.
Control de tiempo: permite el uso de aquellas aplicaciones calificadas como juego y diversión durante el número de horas/días especificado.
Supervisión: realiza informes de control web y de uso de aplicaciones.
Geolocalización: opción de seguimiento de localización del dispositivo.
Notificaciones: es posible configurar alertas personalizadas.
Control remoto del dispositivo: opción de seguimiento de la localización del dispositivo.

“Recuerda que la mejor manera de acercarte a los mejores de edad es estableciendo un diálogo sincero e interesarse por sus intereses en línea”.

RECOMENDACIONES DE MEDIACIÓN PARENTAL POR GRUPOS DE EDAD.

Prepara un entorno TIC ajustado a la madurez del menor.
Es recomendable que acorde a la edad en la que los menores comienzan a hacer un uso de la tecnología pueda haber ciertas adecuaciones al espacio de manera que les sean sencillos de utilizar y resulten seguros, eliminando la posibilidad de exponerle a riesgos innecesarios (ej. contenidos inapropiados) o comprometer la seguridad del dispositivo.

Prepara el sistema y dispositivos contra los virus

- Instala un antivirus y mantenlo actualizado para analizar todo lo que se descarga.
- Mantén el sistema operativo (SO), el navegador y todas las aplicaciones actualizadas.
- Asegúrate de que está protegido a la última activando las actualizaciones automáticas.
- Utiliza una cuenta de usuario con permisos limitados para navegar.
- Utiliza controles parentales en los dispositivos a los que dan uso.

Sobre la protección de sus datos personales y sensibles:

¿Qué son los datos personales?

Los datos personales se refieren a la información que identifica a una persona y que tiene relación con su vida familiar, su patrimonio, sus opiniones políticas, sus creencias religiosas, sus preferencias sexuales, entre otras (INAI)

Es importante que, desde sus primeros pasos en el uso de internet, redes sociales, juegos de video etc. Sepan cuales son sus datos personales que los hacen únicos e identificables, como por ejemplo su nombre completo, su edad, el sexo con el que nacieron etc. De igual manera debes enseñar que en ninguna circunstancia deben revelar o dar información a personas que conocen en internet o que no están seguros de su identidad en la vida real, ya que esto puede ponerlos en riesgo.

"Enséñales que nadie debe pedirles información personal, como su nombre, donde viven, dónde estudian, dónde trabajan sus padres etc."

GRUPOS DE EDAD.

Menores de 0 a 2 años.

De acuerdo con la asociación Americana de Pediatría, los menores en este rango de edad no deben estar expuestos a las pantallas debido a que la luz de las pantallas afecta en el desarrollo y calidad de su visión.

Menores de (3 a 5 años)

Sus primeros contactos con las tecnologías. En esta etapa inicial se recomienda una supervisión total, de su actividad para asegurar que se desarrolla de manera segura, a la vez que se les inicia en las pautas básicas de uso:

Elige contenidos infantiles. Selecciona previamente los contenidos a los que tendrán acceso. Al comenzar a utilizarlos acompáñalos para asegurarte de que se sienten cómodos y sobre todo de que el material al cual estén teniendo acceso sea el adecuado para su edad y su desarrollo cognitivo, puedes configurar con controles parentales.

Supervisa su actividad. Mantén los dispositivos en un lugar central de la casa para supervisar su uso por el menor. Presta atención a sus reacciones, pregúntales por lo que han visto y escúchalos con atención. Es el momento de empezar a fomentar el diálogo familiar.

Menores De (6 a 9 años) "Sus primeros pasos en Internet".
En esta etapa de desarrollo, los niños disfrutan de actividades divertidas y buscan más independencia. Piensan aquí y ahora y pueden seguir reglas simples impuestas por adultos
Prepara entornos TIC controlados con conexión a Internet.
Es importante comenzar a adecuar los entornos haciendo uso de los controles parentales disponibles en los dispositivos que vaya a utilizar el menor, (teléfonos, tabletas, ordenadores, consolas, Smart TV).

Facilítale contenidos de calidad.
sugiérele contenidos de calidad para su edad que le ayuden a desarrollar sus habilidades, a ser más creativo y participativo.
Amplía las buenas prácticas de uso. Ahora que tiene acceso a Internet, además de seguir insistiendo sobre la privacidad y la importancia de no compartir información personal o sensible, puedes empezar a trasladarle pautas para una navegación segura.
En la medida de lo posible sigue manteniendo los dispositivos en un lugar central de la casa para supervisar su uso.
Fomenta pláticas con respecto a las actividades que realiza en línea y si se encuentra con algún contenido que lo hace sentir incómodo para que tenga la confianza de decírtelo.

De 10 a 13 años.
Comienza a adecuar entornos digitales más flexibles.
Continua con entornos controlados que minimicen los riesgos, prestando especial atención a los controles parentales de teléfonos móviles inteligentes y consolas.
Cabe señalar que por la naturaleza de su nivel cognitivo probablemente comiencen a sentir que estas restricciones están invadiendo su espacio personal para lo cual es recomendable establecer diálogos abiertos y sin prejuicios para no perder la confianza del menor.

Fomenta el respeto a los demás. Los adolescentes no siempre son conscientes del daño que pueden ocasionar a un amigo o compañero con una 'simple broma'. El supuesto anonimato de la red y la dificultad para percibir el daño causado desde la distancia física que interpone Internet, por tal razón en muchas ocasiones se les hace fácil poder decir comentarios que muchas veces pueden dañar a alguien más, es válido recalcar el respeto dentro y fuera de la red.

Insiste sobre las buenas prácticas de uso. En esta franja de edad ya deben tener una idea clara de las pautas necesarias para una navegación segura

Menores de 14 y más años.

Supervisa su actividad respetando su privacidad y refuerza el diálogo.
A esta edad generalmente las y las adolescentes ya buscan tener más independencia y autonomía en sus dispositivos y toma de decisiones, por lo cual el utilizar herramientas de control parental puede que se torne un poco complicado, por ello se debe de tener un dialogo de confianza con los menores acerca de su actividad en línea sin que se torne en una situación de incomodidad para ellas y ellos, puedes comenzar con charlas de tipo "que stikers o meme está en tendencia" y hablar sobre sus intereses en línea.

Sensibilízale sobre los contenidos inadecuados. Respecto al tema del acceso a páginas con contenido inapropiado (violencia, pornografía, modas absurdas y peligrosas) y comunidades peligrosas (discursos de odio, autolesiones, retos peligrosos etc.), esta edad es la más crítica. Ellos quieren conocer, explorar, experimentar, además de tener cierta tendencia al riesgo y es necesario que aprendan a discernir, pero es importante que lo hagan desde una visión crítica.

Fomenta el uso responsable de las redes sociales.
Es la franja de edad en la que legalmente pueden empezar a utilizar servicios de la Red como las redes sociales o los servicios de mensajería instantánea.

Adapta las normas de forma consensuada.
Para que las normas sean respetadas es conveniente que no se impongan, sino que sean de mutuo acuerdo en dialogo con los menores.

"Fomenta en ellas y ellos la autoestima adecuada para que puedan gestionar sus emociones y tomar decisiones adecuadas cuando están en línea".

Empezar a gestionar su digitalización emocional.
Debe empezar a saber cómo desenvolverse de forma autónoma en algunas de las situaciones (ej. Gestionar un enfado en el grupo de WhatsApp de amigos, saber trasladar su rechazo o malestar de forma asertiva ante un comentario malintencionado) de igual forma fomenta el dialogo persona a persona cuando exista la oportunidad, esto con la finalidad de reforzar sus habilidades sociales también fuera de línea.

Promueve actividades en familia y espacios de desconexión.
Es bien sabido que las redes sociales y los dispositivos inteligentes funcionan de forma en la que se puede tornar adictivo para las personas usuarias su uso y aún más cuando se trata de menores de edad, por ellos se deben promover ambientes "libres de tecnología" que inciten al dialogo en familia como por ejemplo en la hora de la comida, antes de dormir etc.

Aconséjale mantener la información sensible en privado. Hazle saber que cuanta más información sensible difunda -especialmente las imágenes donde comparte su actividad- más vulnerable será en internet. Asegúrate de que sepa que la información que publica en internet, difícilmente se controla fuera de línea.

Y la más importante de todas, SÉ EL EJEMPLO, si pones una regla en cuanto al lugar y tiempo de uso de los dispositivos, naturalmente tienes que seguirla, no olvides que el dialogo abierto siempre es importante.

Referencias bibliográficas:

1.- Guía de seguridad en redes sociales para familia, INCIBE, sitios web. http://www.incibe.es y http://menores.osi.es.

2.- Enrique Echeburúa Odriozola y Ana Requesens Moll, 2012, Adicción a las redes sociales y a las nuevas tecnologías en niños y adolescentes, guía para educadores, ediciones pirámide.

3.- Robb, M. B., Bay, W. y Vennegaard, T. (2019). *The new normal: Parents, teens, and mobile devices in Mexico* (La nueva realidad: Padres, adolescentes y dispositivos móviles en México). San Francisco, CA: Common Sense.

4.- CIBERPSICOLOGÍA, COMPORTAMIENTO Y REDES SOCIALES Volumen 17, Número 6, 2014 ª Mary Ann Liebert, Inc.

5.- WHO guideline: recommendations on digital interventions for health system strengthening. Geneva: World Health Organization; 2019. Licence: CC BY-NC-SA 3.0 IGO.

6.- Rivas, Vocar, Cantergiani, *Use of mobile technological devices by children: Between consumption and family care, Universidad Católica de Temuco, Chile*

7.- INEGI; Instituto Federal de Telecomunicaciones de México. Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH).