Microsoft

Microsoft México
2022

¿Cómo proteger a tus niños y adolescentes de los riesgos en línea?

Guía de ciberseguridad para padres de familia

Capítulo I

Introducción

¿Permitirías que una niña o un niño que esté bajo tu cuidado salga a la calle sin compañía, que hable con las primeras personas desconocidas que se encuentre, que les diga su nombre, les proporcione datos de todos los miembros de la familia y les comparta detalles como el nombre de la escuela a la que asiste?

Pues esas son las actividades que muchas veces las niñas y los niños realizan cuando están en línea y en donde corren prácticamente los mismos riesgos que en el mundo real.

Conocer cuáles son los riesgos que enfrentan te permitirá cuidarles mejor. De hecho, el Índice de Civilidad Digital elaborado por Microsoft este año encontró que al menos 9 de cada 10 personas opinan que se necesita educar mejor a las personas sobre cómo hacer que el mundo digital sea más seguro.

Hacer que los dispositivos utilizados para acceder a contenidos en línea –como tabletas, computadoras portátiles o consolas de videojuegos– sean seguros es más sencillo de lo que parece, pero requiere que mamás, papás y adultos se involucren en el tema y conozcan cuáles son las herramientas, conductas y situaciones que se presentan en línea.

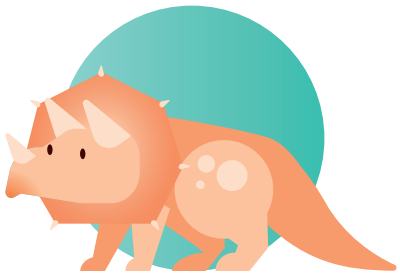
Por eso, aquí vamos a dar una rápida revisión a las actividades de los usuarios de internet, especialmente los menores cuando están en línea y desde dónde se conectan para después conocer algunos de los resultados del Índice de Civilidad Digital de Microsoft junto con consejos para empezar a tener prácticas más seguras.

También compartiremos consejos para acompañar a niñas y niños en sus primeros pasos en el mundo en línea y que sus madres, padres, cuidadores y cuidadoras puedan garantizar que usen el internet de forma segura y con la información que necesitan en cada periodo de su infancia.

Finalmente, daremos algunos consejos sobre la mejor manera de actuar cuando se es víctima de alguna situación de riesgo y cómo tener una reacción adecuada para que niñas y niños, así como sus familiares y amistades, no se expongan a riesgos adicionales.

Aprender a cuidarse es uno de los mejores regalos que se le puede dar a niñas y niños que hoy más que nunca se exponen al mundo en línea durante gran parte de sus actividades diarias, como estudiar y divertirse.

Vayamos juntos.



Capítulo II

Infancias, tecnología e internet

Casi 7 de cada 10 mexicanos y mexicanas de entre 6 y 12 años usan internet, mientras que prácticamente la mitad utiliza la telefonía celular.

En México, hay 84.1 millones de personas usuarias de internet, que representan 72% de la población de 6 años o más años del país, revela la **Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2020.**

Microsoft

Los tres principales medios por los que las personas se conectaron a internet en el país durante el último año son: **teléfonos inteligentes (Smartphone), con 96.0%; computadora portátil, con 33.7%, y TV inteligente, con 22.2%.**

Específicamente en el segmento entre 6 y 11 años, el 68% de las niñas y niños que habitan en México –alrededor de 9.1 millones– usan internet. De ese total, 4.8 millones manifiestan que usan computadora, y 4.5 millones respondieron que usan telefonía celular de manera constante.

De acuerdo con **datos de la Asociación de Internet MX,** la principal actividad de los menores mexicanos en la red es ver contenidos audiovisuales en plataformas gratuitas (84.1%), muy por encima de otras actividades, como enviar mensajes instantáneos (69.4%), utilzar redes sociales (69.3%) y jugar videojuegos en línea (46.5%).

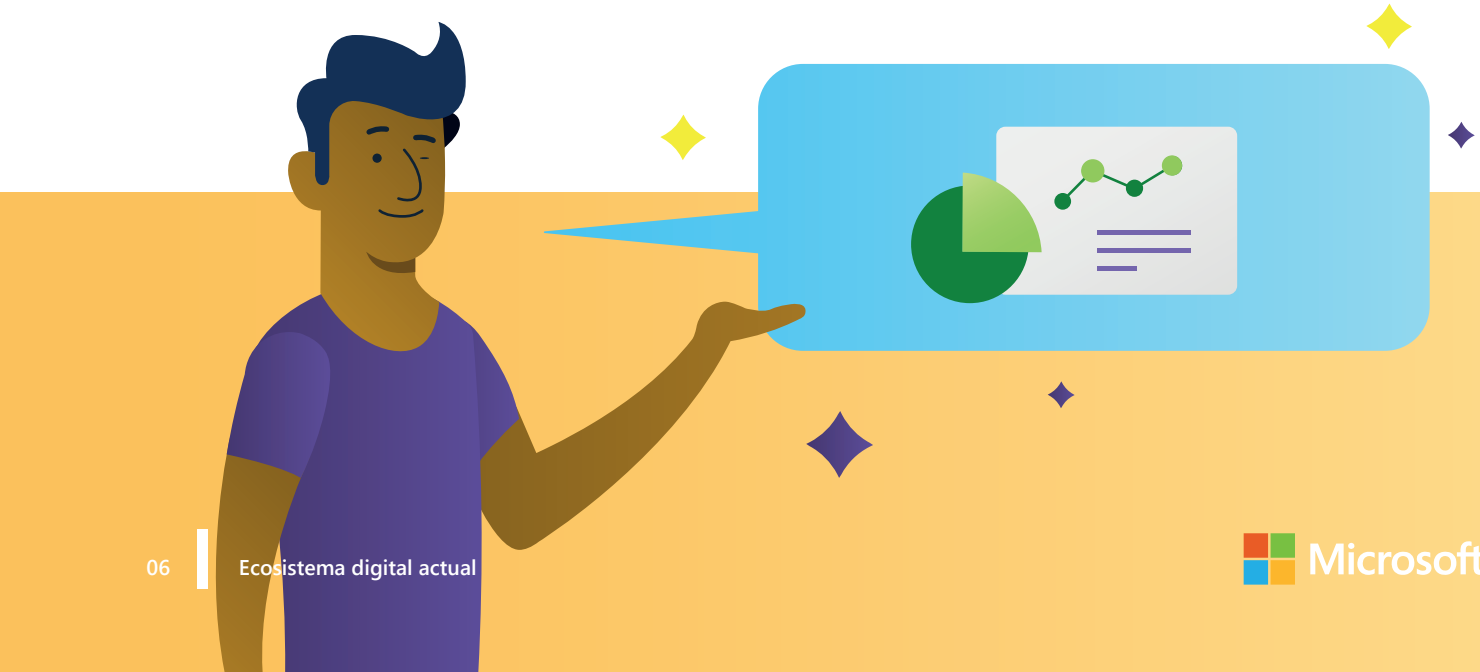
Las tecnologías son cada vez más accesibles en el país gracias a factores como la diversificación de precios en los dispositivos y a que hay cada vez más facilidades para usar internet, ya sea en sitios públicos, escuelas o a través de tarjetas de prepago para dispositivos móviles. Todo esto, a su vez, hace que también más niñas y niños puedan utilizar internet en su día a día.

Capítulo III

Ecosistema digital actual

A raíz de la pandemia se impulsó el uso de las tecnologías en niñas y niños de México, pero también aumentaron los riesgos a los que se exponen en el mundo digital.

De acuerdo con datos de la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) elaborada por el Instituto Nacional de Estadística y Geografía (INEGI), en 2018 había 7,494,996 mexicanas y mexicanos de 6 a 11 años que usaban internet, y para 2019 había 8,077,481 –un aumento de 582,485–. Pero para 2020 ya eran 9,128,507, lo que representó un crecimiento de 1,051,026 usuarios, **es decir, 13.01% en solamente un año.**



Microsoft

Algo similar pasó entre los usuarios de telefonía celular de este grupo de edad, ya que de 2018 a 2019, el número prácticamente no varió, pero de 2019 a 2020, se sumaron 828,689 niñas y niños.

En todo el país, más de 50% de las niñas, niños y adolescentes tiene un dispositivo electrónico propio, ya sea un teléfono inteligente o una tableta; y en más de 50% de los casos cuentan con más de 2 dispositivos, siendo la tableta (56%) y el smartphone (51%) los más comunes, revela el **Estudio Sobre Ciberseguridad en Empresas, Usuarios de Internet y Padres de Familia en México 2021 de la Asociación de Internet MX.**

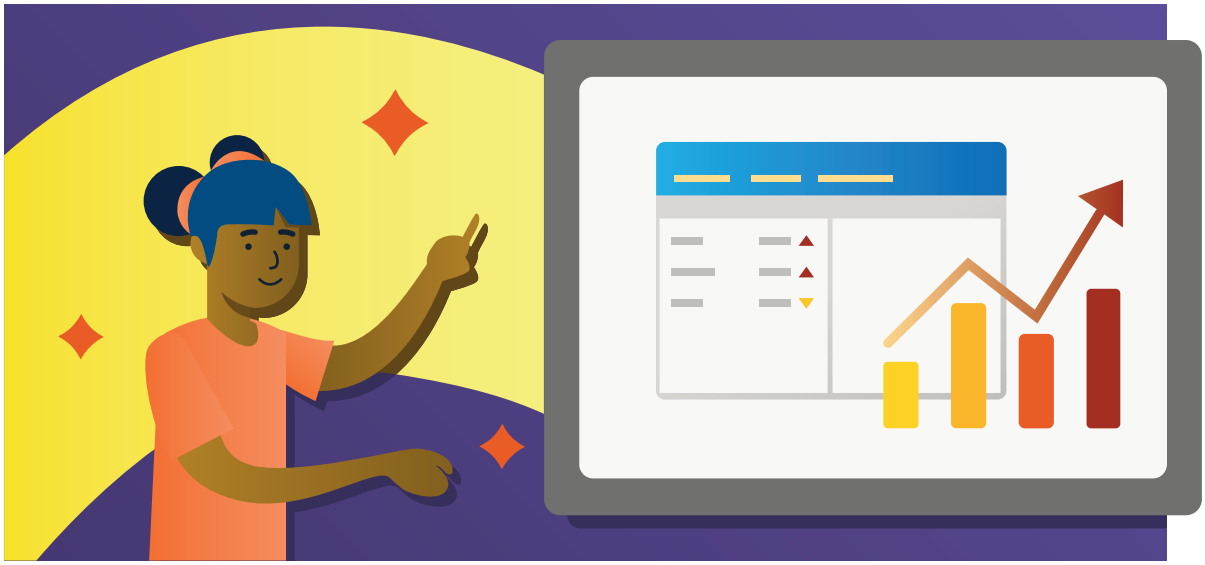
A su vez, todo este acceso acelarado a la tecnología también ha puesto en una situación de mayor riesgo a este sector de la población debido a que pasan más tiempo en plataformas virtuales, ya sea estudiando o divirtiéndose.

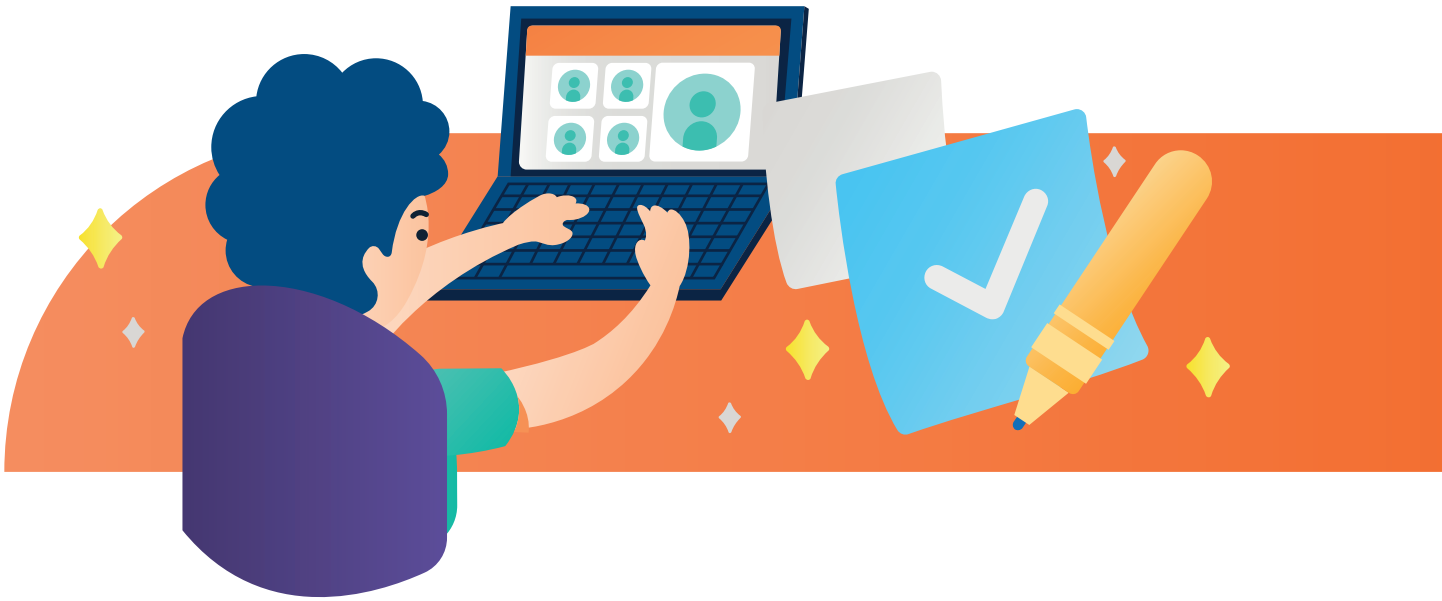
"Puede exponer en mayor medida a niñas y niños a la explotación sexual y el acoso en línea, ya que los depredadores buscan aprovecharse de la situación creada por la pandemia. La falta de contacto personal con sus amigos y parejas puede llevar a que asuman mayores riesgos, como el envío de imágenes sexualizadas, mientras que el tiempo sin estructurar que pasan en internet puede exponer a niñas y niños a contenidos potencialmente dañinos y violentos, así como a un mayor riesgo de sufrir ciberacoso".

Advirtió desde inicios de la pandemia, la **Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (Unesco).**

Y es que solo en 2020, los delitos cibernéticos cometidos contra menores de edad aumentaron 157%, mientras que el delito de pornografía infantil aumentó 73%, de acuerdo con un reporte de la Guardia Nacional recogido en el **Estudio Sobre Ciberseguridad en Empresas, Usuarios de Internet y Padres de Familia en México 2021,** elaborado por la **Asociación de Internet MX.**

Además, 33% de las niñas, niños y adolescentes no recibe orientación en la escuela sobre los peligros de internet, lo que puede exponerles todavía más debido a la falta de información para cuidarse y para actuar cuando se enfrenten a un caso de riesgo.





Capítulo IV

Civilidad digital

Civilidad, seguridad e interacción en línea: México 2021.

¿Qué es el “civismo digital”?

El civismo digital consiste en demostrar respeto por los demás, en comportarse con civismo y en proteger los derechos de todos (incluidos los del propio individuo). Se trata de aprender y aplicar las habilidades para comportarse de forma ética y ayudar a moldear las normas sociales en línea. Es lo que conocemos como convivencia.

El civismo digital, junto con la alfabetización digital, es uno de los dos elementos principales de la ciudadanía digital. Al convertirse en buenos ciudadanos digitales, las personas desarrollan un sentido de propiedad y responsabilidad personal que les ayudará a tomar decisiones éticas en el mundo online y, al hacerlo, a construir una Internet más segura y confiable. Es acudir y actuar con valores, como la honestidad, respeto y empatía.

En 2021, una investigación de Microsoft midió las experiencias de los adolescentes (de 13 a 17 años) y de los adultos con respecto a 21 riesgos diferentes en línea, en 22 países. Los resultados se utilizan para generar una puntuación del Índice de Civismo Digital (ICD) a nivel mundial y nacional.

¿Qué es el ICD?

El Índice de Civilidad Digital (ICD) mide la exposición de los consumidores a los riesgos en línea. Los riesgos en línea del estudio se dividen en cuatro grandes categorías:

- Riesgos de comportamiento (ser tratado de manera descortés o ser objeto de acoso en línea).
- Riesgos intrusivos (contactos no deseados o bromas, estafas y fraudes).
- Riesgos sexuales (como la recepción de mensajes sexuales no deseados o solicitudes sexuales).
- Riesgos para la reputación (como el doxing (***revelar información privada con el fin de intimidar, humillar o amenazar***) o el daño a la reputación personal).

Las puntuaciones **más bajas equivalen a una menor exposición a los riesgos en línea y a una mayor calificación de civismo digital.**

A continuación ofrecemos un resumen de los resultados de este año en México.

Molesta menos la incivilidad

Los efectos de COVID-19 continuaron impactando en México las percepciones de civilidad digital en Generación Z y los Millennials, ya que para estas generaciones la incivilidad se está convirtiendo en la "nueva normalidad".

"Hoy, me molesto menos que antes cuando encuentro a alguien en línea que es descortés conmigo".

50%

Las clases en línea ayudaron a mejorar la civilidad

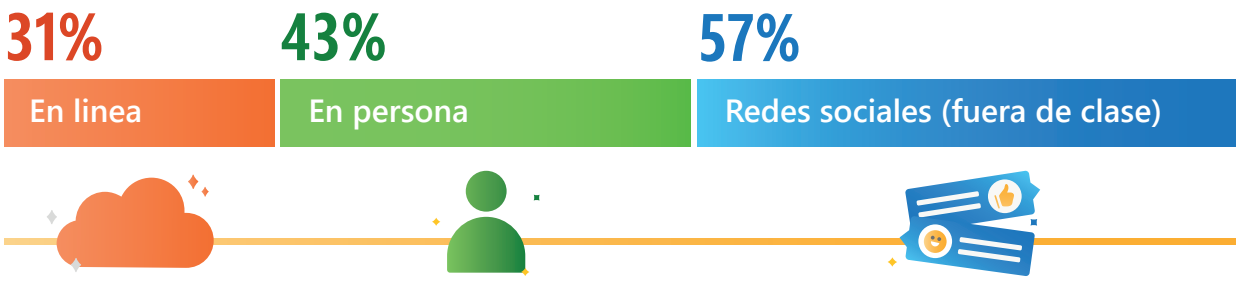
Las reuniones y clases en línea obligadas por el confinamiento también impulsaron el civismo en línea en México.

Dijo que las reuniones y clases en línea impulsaron una mejora en una mayor civilidad.

93%

Microsoft

La incivilidad es más común en redes sociales y en persona.
Frecuencia en la que se encontró incivilidad en las clases de la escuela.



En general, durante la pandemia los mexicanos modificaron sus percepciones sobre la civilidad en línea.

28%
Dijo que empeoró durante la pandemia.

21%
Dijo que el estado de la civilidad en línea era malo, 2 puntos menos que en 2020.

5%
Tuvo un mayor sentimiento de que estamos todos juntos en esto.

5%
Percibe menos ataques personales o comentarios negativos.

34%
Dijo que el estado de la civilidad en línea era bueno, 3 puntos más que en 2020.

14%
Vio a más gente ayudándose unos a otros.

5%
Considera que la gente se ha unido más para hacer frente a la crisis.

Sin embargo, también hubo señales que indican una mejora de la civilidad en línea.

16%
Menor difusión de información falsa o engañosa.

¡Habla de seguridad y civilidad digital en tu hogar!

En la encuesta, 93% de las personas participantes dijo que se necesita más educación sobre cómo hacer que el mundo digital sea más seguro, lo cual puede lograrse si se empieza desde casa.

Pregúntate
¿Qué dispositivos, aplicaciones y plataformas usa tu familia?

Asegúrate de que tu familia conozca los fundamentos de la seguridad digital y usa las herramientas de seguridad disponibles en dispositivos y software.

Tú conoces mejor a tu familia: Establece pautas basadas en los niveles de madurez y los valores de cada miembro de tu familia.

Mantén la conversación abierta: Enseña a niñas y niños a confiar en sus instintos y hazles saber que pueden acudir a ti en cualquier momento.

¡Acepta el Desafío de Civilidad Digital!

Abraza la civilidad digital en familia siguiendo estos sencillos pasos.

1. **Vive la regla de oro**
   Actuaré con empatía, compasión y amabilidad en cada interacción y trataré a todas las personas con las que me conecte en línea con dignidad y respeto.

2. **Respeta las diferencias**
   Apreciaré las diferencias culturales y honraré las diversas perspectivas. Cuando no esté de acuerdo, lo haré con consideración y evitaré los insultos y los ataques personales.

3. **Pausa antes de responder**
   Haré una pausa y pensaré antes de responder a las cosas con las que no estoy de acuerdo. No publicaré ni enviaré nada que pueda lastimar a otra persona o amenazar mi seguridad o la seguridad de los demás.

4. **Defenderme a mí y a los demás**
   Le diré a alguien si siento inseguridad, ofreceré apoyo a quienes son víctima de abuso o crueldad en línea e informaré actividades que amenacen la seguridad de cualquier persona.

5. **Daré lo mejor de mí mismo cuando participe en línea**
   - ¿Siento molestia o enojo? Tomaré un momento y respiraré.
   - Responderé a una idea, no a la persona.
   - Haré preguntas y buscaré puntos en común.
   - Me pondré en el lugar de la otra persona:
     ¿Qué podría haber estado pensando o sintiendo?
   - Me defenderé a mí y a mis amigos, pero lo haré con respeto.

6. **No dejaré que el drama me deprima**
   - Reconocer cómo me hace sentir una situación.
   - Confiar en mis instintos y buscar apoyo si lo necesito.

7. **¿Te preocupa una publicación? Repórtala a la plataforma en la que se publicó**
   - Da un paso atrás y trata de poner las cosas en perspectiva.
   - Deja tu dispositivo y desconéctate.

Capítulo V

Acompaña a niñas y niños en sus primeros pasos en internet

El aumento de dispositivos móviles hace que cada vez sea más complicado dar seguimiento a lo que niñas y niños hacen en la red, por eso hay que asegurarse de que no corran riesgos manteniendo comunicación constante y estableciendo acuerdos en familia.

¿Qué debo decirles?

Esta es la información básica que deben saber las niñas y niños antes de empezar a usar un dispositivo conectado a internet:

No compartas información personal (que incluye, entre otros datos: nombre, domicilio, números de teléfono, fotografías, números de tarjetas bancarias o de documentos de identificación) tuya ni de la familia ni de tus amigos.

Microsoft

No des información personal a extraños, ya sean personas o marcas.

No informes nunca tu ubicación exacta o los lugares que frecuentas, como la escuela o el parque al que sueles ir a jugar.

Siempre pregunta a un adulto si tienes una duda.

No des clic a enlaces (links) que no conozcas, incluso si ofrecen premios.

Si estás usando un dispositivo ajeno, como los de la escuela, siempre cierre la sesión de tus cuentas y borra tu historial de navegación.

No compartas contraseñas con otras personas y no las envíes por mensajes o correos electrónicos.

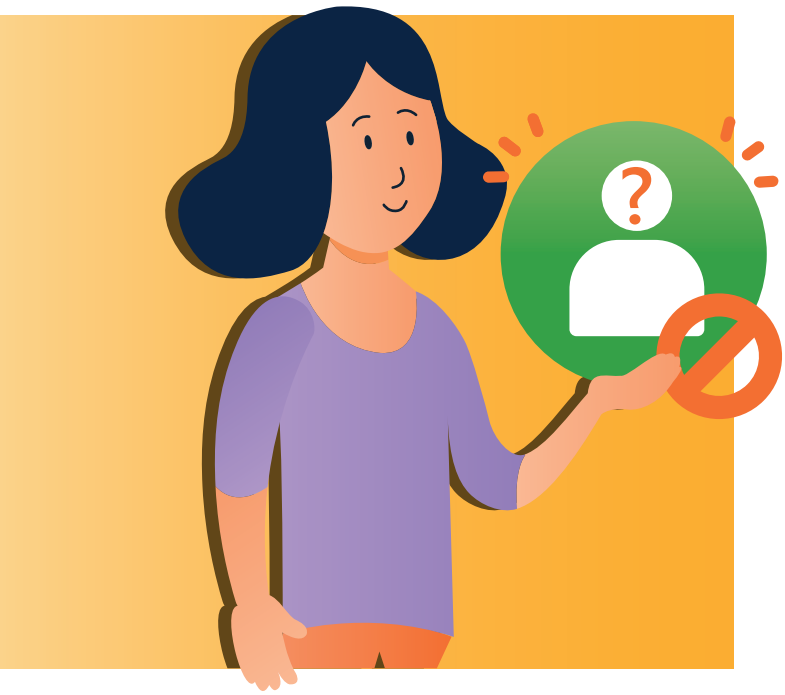
Cuando uses Outlook, marca como "Correo No Deseado" todas las direcciones que te resulten sospechosas y no respondas ningún mensaje.

No descargues archivos adjuntos que te envíen desde un correo que no conoces.

No hables con personas desconocidas cuando juegues en línea.

Microsoft

Dale información que pueda comprender



A medida que crecen, las niñas y niños usan la tecnología de manera diferente, por lo que debes usar las formas más apropiadas de abordar los temas de seguridad en línea.

Para detectar cuánto saben y cuánto apoyo necesitan de tu parte, haz preguntas abiertas para que ellos y ellas puedan dirigir las conversaciones hacia los temas que les preocupan e interesan.

Establece acuerdos

Como sucede en la vida cotidiana, las actividades que realizas deben tener un horario y límites establecidos, lo mismo aplica para las que son en línea. Hablen en familia y establezcan primero para qué quieren usar internet; con base en eso, pueden establecer, por ejemplo, cuánto tiempo pueden pasar en línea o con quién sí pueden tener comunicación:

- **¿Qué nos gusta hacer en línea?**
- **¿Qué dispositivos, tecnología, juguetes o juegos tenemos con acceso a internet?**
- **¿Cuánto tiempo pasamos en nuestros dispositivos?**
- **¿Qué se siente cuando usamos la tecnología durante demasiado tiempo?**
- **¿Cuándo está bien descargar archivos, juegos o aplicaciones, o hacer clic en un enlace?**

¿Qué sitios web podemos usar?

¿Con quién podemos hablar/chatear/jugar en línea? ¿Solo los conocemos en línea o también fuera de línea?

¿Qué debemos hacer si alguien que solo conocemos en línea nos pide fotos, para quedar o para compartir información personal?

¿Qué pasará si uno de nosotros rompe el acuerdo familiar?

¿Cuándo debemos revisar nuestro acuerdo familiar?

Así, todos sabrán cómo y por qué llegaron a los acuerdos que establecen límites en casa para que todos puedan estar seguros en internet. No se trata de prohibir, se trata de acompañar a los menores en el descubrimiento de nuevas modalidades de relacionamiento. Realizar las preguntas correctas cuando se tiene acceso a tanta información, es la forma en que los menores sean autocríticos frente a el "qué" y el "para qué" publican o comparten información en el mundo digital.

Si quieres una guía para elaborar y dejar por escrito esos acuerdos, aquí hay un formato que puede ayudarte a ti y a tu familia (en inglés): **childnet.com/resources/parent-and-carer-toolkit.**

Capítulo VI

Cuida que usen internet de forma segura

La mejor forma de cuidar a niñas y niños es asegurándose de que las herramientas que usen estén correctamente configuradas para realizar tareas y mostrar contenidos que sean apropiados para su edad.

Configurar dispositivos

Ayuda siempre a los menores a crear sus cuentas usando, por ejemplo, un correo electrónico familiar y mantente pendiente, a través de las opciones de los dispositivos, de su actividad. Prácticamente todos los dispositivos que pueden usar tienen opciones de configuración para que naveguen de manera segura.

Recuerda que las niñas y niños no deben ser los responsables de las compras que se hagan en línea y que estas siempre deben hacerse con tu autorización y supervisión.

Xbox

En Xbox, estos son los pasos para limitar el contenido para menores:

- Inicia sesión con tu cuenta en la consola.
- Pide al menor que inicie sesión en su cuenta.
- Busca el contenido al que quieres que tenga acceso.
- En la pantalla elegir quién dará permiso, selecciona tu cuenta.
- Escribe la dirección de correo y la contraseña de tu cuenta o la clave de paso de la consola.
- Selecciona Siempre o Solo por esta vez (o únicamente Solo esta vez si tu cuenta no está en la consola).
- Luego de conceder permiso al menor para usar este contenido, puede abrirlo inmediatamente.

Más información:
support.xbox.com/es-MX/help/family-online-safety/online-safety/manage-online-safety-and-privacy-settings-xbox-one

Microsoft Family Safety

Esta aplicación gratuita para dispositivos móviles iOS y Android te permite desarrollar hábitos saludables en el uso de la tecnología.
Con ella, por ejemplo, puedes establecer límites de tiempo de pantalla que se apliquen a dispositivos, aplicaciones y juegos. Asimismo, puedes bloquear aplicaciones y juegos poco apropiados y limitar la navegación a sitios aptos para niños con Microsoft Edge en Xbox, Windows y Android.

Más información: microsoft.com/es-mx/microsoft-365/family-safety

Modo infantil de Edge

El navegador Edge tiene esta opción que permite entregar una experiencia web más enriquecida y segura para niñas y niños.

- Busca el Modo Infantil en las opciones de cuenta
- Establece la edad apropiada: de 5 a 8 y de 9 a 12 años.

Así, tendrán acceso a contenidos previamente seleccionados y una configuración adecuada para cada grupo de edad.

Más información: microsoft.com/es-es/edge/kids-mode

Ayúdalos a crear contraseñas seguras

El acompañamiento de los adultos debe ir más allá de la supervisión, orientando a niños y niñas frente a los contenidos que consumen y las páginas a las que acceden. Un primer paso fundamental es guiarlos en la creación de perfiles en línea, de modo que eviten compartir información personal, sus cuentas estén configuradas con permisos adecuados a sus edades y puedan acceder de manera segura.

Desde la generación de su correo electrónico hasta el ingreso a redes sociales, un aprendizaje clave es la generación de contraseñas, el primer escudo de la seguridad digital. Para hacerlo, es recomendable tomar las siguientes medidas:

1. No incluir datos sensibles como nombres o fechas significativas, sean personales o de familiares cercanos.

2. Optar por utilizar frases en lugar de palabras aisladas, así como emplear signos y números, a mayor número de caracteres es más complejo de descifrar.

3. - Incluir doble factor de autenticación, es decir, más de un paso para autorizar el acceso. En seguridad lo recomendable es usar tres parámetros, los cuales pueden remitir al dispositivo o verificación de un adulto para autorizar el acceso:
   - Algo que sé (contraseña)
   - Algo que tengo (token)
   - Algo que soy (biométricos)

4. Evitar repetir contraseñas, ya que si uno se ve comprometido puede dar acceso a más cuentas que utilicen la misma contraseña.

5. Pueden usar un gestor de contraseñas, una aplicación con certificados de seguridad capaz de generar contraseñas que cumplan con los parámetros de seguridad y que, además las almacena con relación al sitio o plataforma en que se registraron, para autocompletar el formulario cuando quieran volver a entrar, evitando el problema de los olvidos.

6. Establece periodos de actualización para tus contraseñas, cambiarlas cada cierto número de meses fortalece la protección de sus accesos.

7. Verifica constantemente que tus datos de recuperación estén vigentes, para que, si necesitas restablecer la contraseña en algún punto, puedas hacer el proceso fácilmente.

Enséñales a actuar

Es importante que las niñas y niños sepan qué hacer cuando enfrentan un problema en internet que les represente un riesgo. Por eso, siempre debes darles estos mensajes:

- "Siempre puedes venir a mí si necesitas ayuda". Deben sentir confianza para hablar contigo cuando necesitan apoyo.
- "¿Qué harías si esto sucede?". Dales estrategias para lidiar con las malas experiencias en línea.
- "Recuerda que no todo el mundo es quien dice ser en línea". Recuérdeles que siempre le diga a un adulto cuando alguien que solo conocen en línea los hace sentir incómodos o les pide reunirse o compartir información personal o imágenes.
- "Mantén tu información personal segura, y la de otras personas también". Esto incluye nombres completos, contacto, detalles y ubicaciones en tiempo real.
- "Respeta a los demás en línea". Enséñales que deben tratar a los demás como ellas y ellos quieren ser tratados.
- "Piensa antes de publicar". Ayúdalos a ser conscientes de que sus acciones en línea pueden tener consecuencias.

Cuando en un ambiente como Xbox alguien empieza a incomodar, **lo mejor es eliminar a esa persona de los contactos a la primera actitud inadecuada.** Recuerda que mientras más pronto se solucione un problema, menos efectos tendrá. Si las niñas y niños aprenden a resolver problemas desde un inicio, seguramente no se volverán graves.

47%

De padres, madres y cuidadores no usa o no sabe qué es un sistema de control parental.
*Estudio sobre ciberseguridad en México 2021, Asociación de Internet MX.

Microsoft

Capítulo VII

¿Cómo actuar tras ser víctima de algún tipo de riesgo?

Mantener comunicación constante con las niñas y niños es importante para saber cómo se conducen en las actividades que realizan en internet. Así, en caso de surgir algún problema, será más sencillo y efectivo darles consejos y sugerirles soluciones.

Para comenzar, es importante que antes de darle un dispositivo a una niña o un niño, realices las configuraciones necesarias para que puedan navegar de manera segura.

Comunícate

Mantenerte en comunicación con niñas y niños es esencial. Garantízales que siempre pueden acudir a ti si algo les molesta o les preocupa mientras están en línea.

Siempre que haya algún problema, guarden la evidencia que sea posible, como capturas de pantalla, correos electrónicos, mensajes de texto o conversaciones en línea, todo esto puede servirte para hacer la denuncia correspondiente en la plataforma en la que se registró el problema.

Cómo actuar ante el ciberbullying

El ciberbullying es el uso de la tecnología para demostrar comportamientos — a menudo repetidos — de burla, degrado y/o acoso a alguien menos poderoso.

A menudo hay señales para identificar este tipo de agresión, como ansiedad constante, dificultad para dormir o concentrarse e, inclusive, no asistir a clases. En caso de confirmar que tu hija o hijo es víctima de ciberbullying, hay que mostrarles apoyo incondicional y escucharles para entender cómo se originó.

Lo mejor es bloquear a la persona y seguir los pasos que marque, por ejemplo, Xbox, para **reportar al usuario.** En caso de ser alguien de la escuela, hay que hacer el reporte correspondiente ante las autoridades escolares.

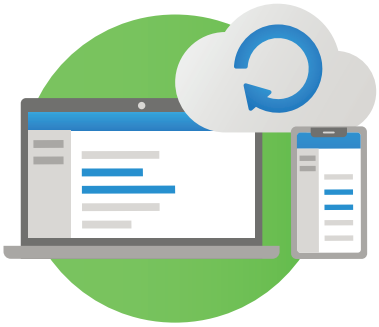
El ciberbullying podría llegar a evitarse casi en su totalidad, si los menores toman medidas sencillas como bloquear al acosador (bully), no compartir o reenviar el contenido y reportar en las diferentes plataformas esta conducta.

También puede darse el caso de que tu hijo o hija sea quien acosa. De ser así, escucha, apoya y busquen soluciones juntos. Es buen momento para poner ciertas restricciones al uso de dispositivos para conectarse usando herramientas como **Microsoft Family Safety.**

Cómo saber si un videojuego es seguro

Fíjate en **la edad recomendada del título, las características y el tipo de juego**. Revisa también las reseñas del juego y define si es apropiado para la niña o el niño. Configura tu consola para **recibir un resumen de la actividad en la cuenta Microsoft de la niña o niño.**

Mantén actualizado tu software



Cuida que los sistemas operativos de tus dispositivos estén siempre actualizados, no lo dejes para después, ya que esas actualizaciones suelen tener correcciones a riesgos de seguridad que se han detectado a través del tiempo.

En ningún caso instales en tus dispositivos apps desconocidas o software pirata o de dudosa procedencia.

Ten cuidado con el grooming

Es cuando un adulto se pone en contacto con un menor de edad con el fin de ganarse su confianza para luego hacerlo participar en alguna actividad sexual online o en persona.

Este tipo de ciberdelincuentes están presentes en lugares de intercambios de mensajes y tienen diversas técnicas, como ofrecer regalos. Y una vez que logra su objetivo, suele amenazar a las víctimas con hacer daño a sus familiares o amigos o publicar imágenes o informaciones comprometedoras.

Es muy importante detectar y detener a tiempo este tipo de ataques, empezando por bloquear y reportar al usuario que está atacando a los menores. Si se llega a presentar algún delito, denúncialo.

Sexting

Hablamos de sexting cuando nos referimos al intercambio de mensajes, fotos y videos de carácter sexual explícito. Esta práctica se ha extendido en los últimos años, como parte del acceso masivo a la tecnología; de acuerdo con cifras del INAI, México es uno de los países latinoamericanos en los que más se ejercen estas actividades donde 36% de los jóvenes entre los 12 y 16 años conocen a una persona que ha enviado contenido sexual, y más de 10% aceptó haber participado en el sexting.

Microsoft

Ante este panorama, pueden tomarse medidas para prevenir filtraciones de este tipo de contenido:

- Hay que tomar en cuenta que todo contenido en línea puede ser accesible por diferentes vías, por lo que un archivo que se compartió entre dos personas en una red poco segura puede filtrarse. El 90% de las imágenes de este tipo terminan siendo disponibles al público en general.

- Del mismo modo, siempre hay que tratar de corroborar que la persona a la que se le envían este tipo de archivos los reciba de manera consensuada y bajo el entendido de que no debe difundirlo con terceros.

- Además del riesgo reputacional, en ocasiones se presentan extorsiones, donde se amenaza al usuario con publicar los videos.

De presentarse un caso de extorsión o filtración de estos archivos, se aconseja actuar de la siguiente manera:

- Reportar la publicación dentro de la plataforma en que se encuentre.

De presentarse un caso de acoso dirigido o persistente, modificar la configuración de la cuenta para bloquear contactos y/o desactivar comentarios, de ser necesario. Si crees que la filtración puede ser resultado de una vulneración a tu cuenta:

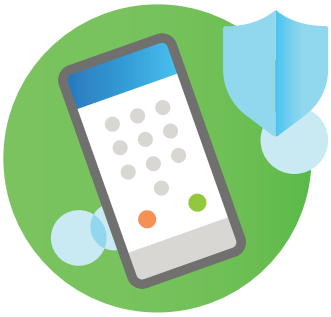
- Cambia las contraseñas de tus redes sociales, haz autenticación de dos pasos y revisa la privacidad de tus publicaciones.

- Elimina contactos que no conozcas de tus redes sociales.

- Intenta no intimidarte con las amenazas del agresor.

- Si el incidente escala, pueden tomarse medidas legales relacionadas con la violencia sexual, puedes denunciar frente al Ministerio Público o la Policía Cibernética.

Guardia Nacional



En caso de que consideres que se cometió un delito acude a Centro de Respuesta a Incidentes Cibernéticos de la **Dirección General Científica de la Guardia Nacional:**

- Al teléfono 088 (desde cualquier lugar del país)
- Al correo electrónico cert-mx@sspc.gob.mx
- A la cuenta de Twitter @CNAC_GN