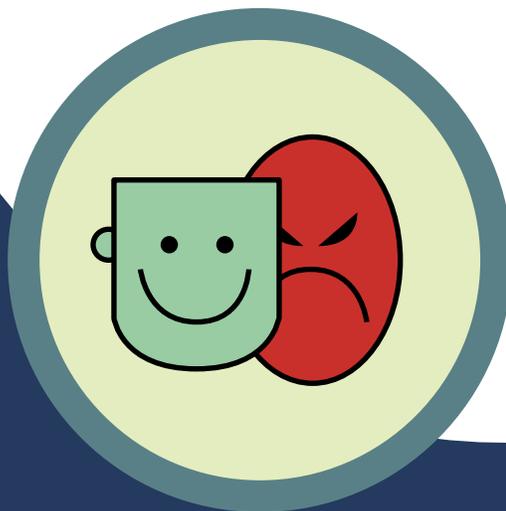


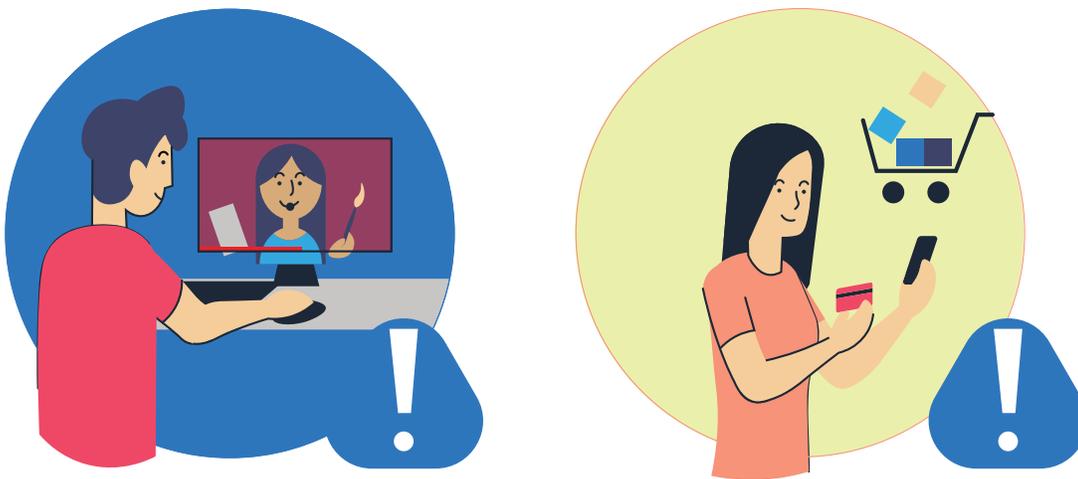
Esenciales de Seguridad Digital

¡Toma el control de tu vida en línea!



Contenido

¡Aprende a ser un buen ciudadano digital!.....	3
PROTEGE TU INFORMACIÓN	4
Quiz ¡Te queremos conocer!	5
¿Qué hace tu generación en internet?	6
¿Sabes identificar cuándo estás en una situación de riesgo? ¡Mantente alerta!.....	6
Quiz ¿Qué tipo de influencer eres?	7
¿Crees que tu contraseña es segura?.....	9
CONCIENTIZACIÓN: SEGURIDAD EN INTERNET	10
Toma el control de tu seguridad	11
Disfruta de las redes sociales sin exponer tu información	12
Tips básicos de seguridad	13
Que no te roben la identidad	15
BUENAS PRÁCTICAS EN INTERNET	17
Guía de empatía para principiantes ¡Piensa antes de enviar!	18
Quiz ¿Cuál es tu nivel de empatía?	20
¿Qué es la resiliencia?	21
Quiz ¿Sabes lo que puedes controlar?	22
¿Qué es el sexting y cuáles son sus riesgos?	23
Todo lo que tienes que saber del cyberbullying y online grooming ¡cuídate!	24
¿Qué son y cómo detecto las fake news (noticias falsas)?	26
Quiz ¿Puedes identificar noticias falsas?	27
Videojuegos, tips para tu seguridad	29
CIVILIDAD DIGITAL	31
Índice de Civildad Digital de Microsoft	32
Reto de Civildad Digital de Microsoft	33
¿NECESITAS AYUDA?	34
INFO PARA PADRES, TUTORES Y MAESTROS	37



Esenciales de Seguridad Digital

Creamos para ti este contenido con toda la información que necesitas para tomar el control de tu privacidad y seguridad en internet. ¡Aprende a ser un buen ciudadano digital!

¿Por dónde empezar?

Protege tus datos personales. Siempre pide ayuda a un adulto de confianza cuando un sitio web te solicite más información de la normal.

Usa contraseñas seguras. En tus contraseñas incluye letras, números y símbolos que sean fáciles de recordar, pero difíciles de adivinar para otros.

Piensa antes de dar clic. Antes de publicar una foto, comentario o ubicación, recuerda que cualquier persona podría verlos. No des clic en "Acepto", "OK" ni "Reclamar premio" en los anuncios emergentes de sitios web inseguros.

Sé parte de la solución, no del problema. Pon en práctica los principios del Reto de Civi- lidad Digital de Microsoft y haz del mundo digital un lugar más seguro y lleno de valores. Actúa con empatía, respeta las diferencias y a los demás.

Protege tus datos



Somos ciudadanos digitales. Aparte del lugar en que nacimos, vivimos en el infinito mundo del internet. Tenemos que aprender a respetar y a convivir con otros habitantes.

En este módulo:

- Aprenderás cuáles son los hábitos de uso del internet de acuerdo a tu país.
- Conocerás con quién compartes realmente tu vida en línea.
- Podrás determinar si eres adicto al internet y saber si podrías vivir sin él.

¿Cómo saber si somos buenos ciudadanos digitales?

- Respetamos las opiniones de los demás.
- Verificamos la información antes de compartirla.
- No descargamos contenido ilegal.
- No promovemos conductas ofensivas.
- Protegemos nuestra privacidad y la de otras personas.
- Denunciamos la violencia online.
- No respondemos de manera violenta.
- Cuidamos nuestra seguridad.

Quiz: ¡Te queremos conocer!



Este quiz te dirá cuál es tu personalidad digital. Elige las respuestas que te describan mejor, puedes seleccionar varias en cada pregunta. Cada una vale un punto, al terminar suma tus puntos y descubre qué tan importante es para ti el internet.

1. **¿Tienes perfil en alguna de estas redes sociales?**
 - a. Facebook (+1)
 - b. Instagram (+1)
 - c. TikTok o YouTube (+1)
 - d. Otra (+1)

2. **¿Para qué usas internet?**
 - a. Entretenimiento (+1)
 - b. Redes Sociales (+1)
 - c. Tareas (+1)
 - d. Videojuegos (+1)
 - e. Hablar con otras personas (+1)

3. **¿Qué tipo de contenido compartes en tus redes sociales?**
 - a. Fotos y videos de mi vida personal (+1)
 - b. Memes y noticias (+1)
 - c. Opiniones y reseñas (+1)
 - d. Contenido de otras cuentas (+1)
 - e. No comparto contenido (0)

4. **¿Cuánto tiempo al día usas tu celular? (selección única)**
 - a. 1 hora (+1)
 - b. De 2 a 3 horas (+1)
 - c. Más de 5 horas (+2)
 - d. No lo sé (0)
 - e. Duermo con él y es lo primero que reviso al despertar (+3)

Resultados

0 - 5 Puntos

¡El internet no es todo para ti!

Para ti conectarte a internet es una herramienta de apoyo. Sabes que existe vida más allá de las pantallas. Desconoces algunas plataformas o simplemente no te interesa formar parte de ellas. No importa si lo usas poco, es importante que conozcas cómo proteger tu seguridad y tomar el control de tus datos. Sigue leyendo para saber más.

6 - 11 Puntos

¡El perfecto equilibrio!

El internet es una gran herramienta de apoyo y entretenimiento para ti. Te gusta estar al pendiente, pero no es lo único que haces durante el día. ¿Sabes cómo proteger tus datos? Te invitamos a visitar nuestros módulos para informarte sobre cómo tomar el control de tu privacidad ;)

12 - 16 Puntos

¡Lo usas para todo!

¡Wow! Eres un especialista. No puedes vivir sin estar en conexión, seguramente conoces todas las plataformas a la perfección y no tienes ningún problema adaptándote a las nuevas tendencias. Pero, ¿conoces los riesgos a los que podrías estar expuesto? Por esto es muy importante que tengas en cuenta tu seguridad y privacidad. ¿Quieres saber más? ¡Sigue leyendo!

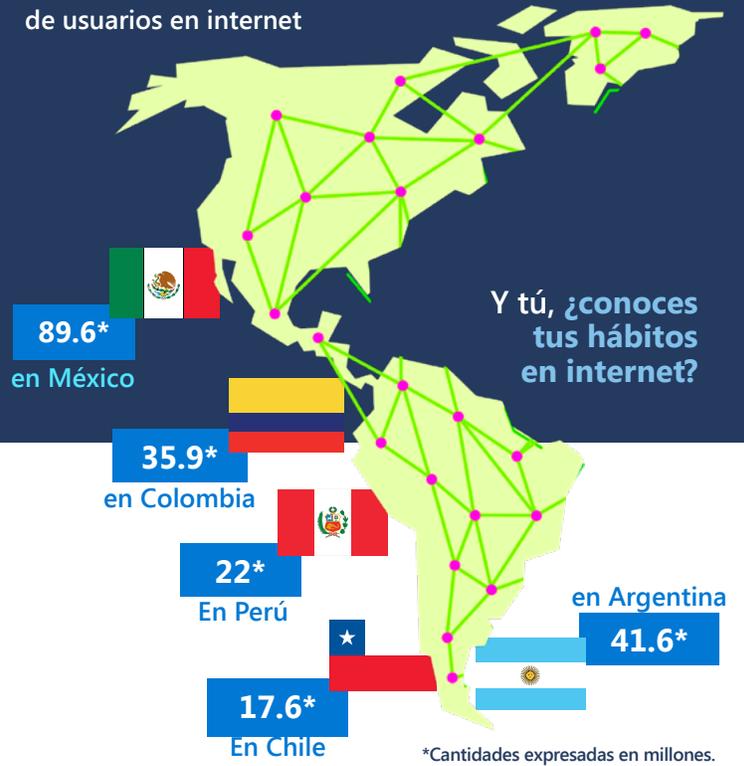
2020 ¿Qué hace tu generación en internet?

Todos los días usas internet para muchas cosas: hablar con tus amigos, ver películas y series o subir videos de tu vida diaria. Ahora ha llegado el momento de que sepas los números actuales detrás de uno de los mejores inventos de la humanidad.

FUENTE: <https://www.internetworldstats.com/>



En todo el mundo existen más de **4 mil 500 millones** de usuarios en internet



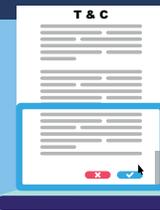
Y tú, ¿conoces tus hábitos en internet?

Protege tus datos No expongas tu privacidad y seguridad

Cosas que haces todo el tiempo que pueden ponerte en riesgo. Pueden robar tu información o entrar a tu computadora o celular.



No descargues apps de sitios desconocidos o con contenido ilegal.



No aceptes términos y condiciones sin leerlos antes.



No uses la misma contraseña en todas tus cuentas.



No publiques tu ubicación en todo momento.



Tu información es muy valiosa. Cuídala.
Así te proteges a ti y a los que te rodean.



No hables con personas desconocidas.



Estas situaciones **ponen en riesgo** tu privacidad y seguridad.

Quiz: ¿Qué tipo de influencer eres?

¡Todos mostramos nuestra identidad de manera diferente!

Descubre con este quiz qué tipo de influencer eres. Elige la respuesta que se adapte a tu personalidad. Tu tipo de perfil será revelado en función a la mayoría de respuestas que hayas seleccionado (a, b, c, d o e).

1. La verdad, ¿cuánto tiempo pasas en redes sociales?

- a. Me meto a revisarlas algunas veces al día
- b. Solo las uso para subir mi última selfie
- c. ¡Cuando tengo algo que decir!
- d. Nunca uso redes sociales, no me gustan
- e. A veces las reviso, una vez a la semana o menos

2. ¿Qué tipo de contenido compartes?

- a. Fotos con mis amigos o familia en alguna ubicación
- b. Peticiones e información sobre alguna causa
- c. Mi vida diaria, desde que despierto hasta que me duermo
- d. ¡Frasas positivas y de motivación!
- e. Algo chistoso que encontré en internet, por ejemplo ¡memes!
- f. No publico, solo navego por otras cuentas.

3. ¿Qué es lo primero que haces al llegar a otro lugar?

- a. Tomarte una selfie o pedir que te la tomen "¡Mira ese spot! ¿Me tomas una foto?"
- b. Quejarte sobre el servicio o la calidad de sus productos
- c. Hacer "check-in" y subir una historia o foto cada 5 minutos
- d. Buscar la página y darle like
- e. Ver el menú

4. ¿Te ha pasado alguna de las siguientes situaciones?

- a. Me reportaron como spam por subir muchas historias
- b. Pasar demasiado tiempo en línea, dar muchos "me gusta" y hacer más publicaciones de las habituales
- c. Enviarle una solicitud de amistad a alguien que acabo de conocer
- d. Usar hashtags de temas que no me interesan
- e. Envié una foto o captura de pantalla a la persona incorrecta
- f. Ninguna de las anteriores, ¡tengo mucho cuidado!

5. ¿Qué haces cuando te sientes triste?

- a. Comparto algo lindo en mis redes y me siento mejor
- b. Publico lo que estoy sintiendo y espero que me den consejos
- c. Me meto a ver memes y videos divertidos
- d. Platico con mis amigos
- e. Escucho música o leo un libro



6. Escoge entre estos hashtags lo que más te represente:

- a. #ganandocomosiempre
- b. #todoestabien #goodvibes
- c. #yabasta #eshoradeuncambio
- d. #perro #gato #foto #f4f #feliz #yo #todo
- e. #YOLO #TBT #GOALS
- f. No uso hashtags

7. Es más probable que comparta:

- a. Mi impresionante rutina de ejercicios
- b. Noticias escandalosas
- c. Mi ubicación
- d. Una solicitud de amistad con un conocido
- e. Mmm, no sé cómo compartir cosas en línea



Resultados

Más resultados a.

Ubicación, ubicación, ubicación,
eres un Influencer Traveler.

Me encanta compartir en donde estoy y dar reseñas o tips.

Recuerda: nunca compartas la ubicación de tus amigos sin su permiso. Espera a cambiar de lugar para compartir tu ubicación anterior. Tu ubicación en tiempo real te pone en riesgo y puede ser aprovechada por extraños.



Más resultados b.

¡Me tomo las mejores fotos y las edito increíble!
eres un Selfie Influencer.

Revisa que en tus fotos no salgan pistas de tu ubicación si es que no quieres compartirla. También pregúntate si realmente quieres que esa foto la pueda ver cualquier persona. Aunque tengas tu perfil privado, cualquiera puede descargarla y compartirla sin tu permiso.

Más resultados c.

#Trending #Viral #Reto
eres un Influencer viral.

Intenta usar no más de dos hashtags en una publicación. Usar muchos hashtags puede provocar que te reporten por spam. ¡Cúidate! Los hashtags pueden revelar tu ubicación y lo que estás haciendo en tiempo real.

Más resultados d.

Mis redes sociales me conocen más que mi familia.
Influencer 24/7.

Recuerda también ponerte en contacto con tus amigos y familiares, comparte tus gustos y pasatiempos con ellos. ¡No des información personal a personas extrañas!

Más resultados e.

No soy influencer.
Solo consumo contenido, no lo publico.

Aunque no compartas contenido, recuerda que tener una cuenta en cualquier red social y navegar por internet te hacen vulnerable a los riesgos de seguridad que existen. Verifica tu configuración de privacidad y actualiza el antivirus de tu compu ;)

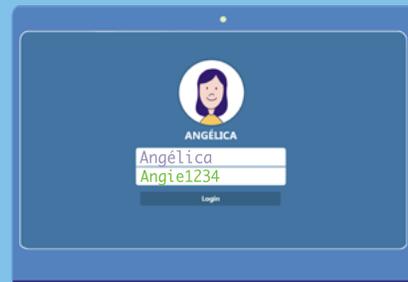
¿Crees que tus contraseñas son seguras? Conoce el caso de Angélica



Angélica usaba una contraseña para todas sus cuentas, era una contraseña sencilla **con su nombre y números consecutivos.**



Era muy fácil de adivinar, tan fácil **que un día alguien la consiguió.**



Con acceso a sus redes pronto comenzaron a hacerse pasar por ella.



Angélica no sabía qué estaba pasando. ¿Quién estaba usando sus cuentas? ¿Cómo podría detenerlo?

Angélica les contó a sus padres sobre su problema. Y la ayudaron a reportar la situación.

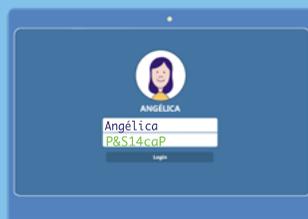


¡Recuerda que siempre puedes pedir ayuda!

Angélica aprendió la lección y ahora utiliza diferentes contraseñas para todas sus cuentas.



Combinando números, letras y caracteres especiales.



Para hacerlas más seguras y proteger sus datos y los de los que la rodean.

Si te hubiera pasado a ti, ¿cómo reaccionarías?

Concientización:

Seguridad en internet



El mal uso de la información que compartimos en internet es algo que pasa todos los días. Desde ataques cibernéticos como fraudes y estafas, hasta el robo de tu información y tus archivos, es importante que sepas cómo detectar las amenazas a tu privacidad.

En este módulo:

- Aprenderás a reconocer las amenazas digitales.
- Podrás cuidar la privacidad de tu hogar.
- Recibirás consejos para prevenir ataques online.
- Te protegerás del robo de identidad.

Toma el control de tu seguridad

Consejos para una mejor experiencia online



Pasamos muchas horas al día en internet, es el lugar donde expresamos nuestra identidad, por eso es **muy importante que tengas el control de tu privacidad.**

¿Cómo puedes protegerte?



No aceptes llamadas ni mensajes de personas que no conoces.



Revisa que los sitios web que visitas sean seguros.



Usa la configuración de privacidad de tu compu, tablet o celular.

Ten cuidado donde descargas música, videos o juegos.



No des clic a links sospechosos ni a ofertas de sitios que no conoces.



Revisa que tu computadora tenga un antivirus actualizado.



Tu contraseña debe ser segura y difícil de adivinar.



Si vas a comprar online, hazlo desde tu celular o computadora personal.



Cubre tu webcam cuando no la estés usando.



Las redes públicas son inseguras, conéctate a WiFi solo si es necesario.



Tu información es muy valiosa. **Cuídala.**

¡Cuídate!

Disfruta las redes sociales sin exponer tu información

No hay nadie que sepa más de redes sociales que tú, ahí te expresas, te comunicas y pasas la mayor parte del tiempo.

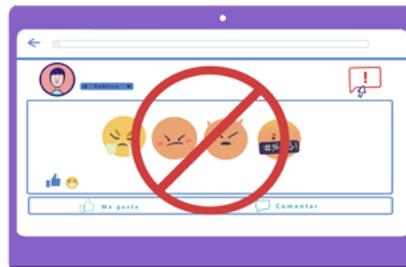
Por eso eres más vulnerable a fraudes y ciberacoso, ¿lo sabías?

¿Qué puedes hacer para proteger tu privacidad y seguridad?

Lo que publicas puede durar ¡para siempre!
Piensa antes de subir algo porque **DEJA DE SER TUYO.**



No publiques, des like ni compartas mensajes ofensivos.
¡Repórtalos!



Si alguno de tus amigos lo hace, recuérdale que **el ciberacoso causa mucho daño.**

- No compartas información personal tuya ni de tus amigos.
- No des muchas pistas acerca de tu ubicación exacta o los lugares que frecuentas.
- No publiques contenido que te exponga demasiado.

- Mantén tus cuentas personales privadas y solo acepta a las personas que conozcas.
- No des información personal a extraños o marcas con poca reputación.
- Revisa la configuración de privacidad de tus cuentas.



Tips básicos de seguridad

La mejor experiencia en internet, es la que tú controlas

Todos los días, muchas veces sin que nos demos cuenta, los sitios web que visitamos y las apps que descargamos recopilan datos acerca de nuestro historial de navegación. Estos datos, aunque son muy útiles para brindarte una mejor experiencia, suelen ser vulnerables a hackeos y fallos en la seguridad del sitio.

Aquí algunos tips de seguridad para que controles y protejas el uso de tus datos.

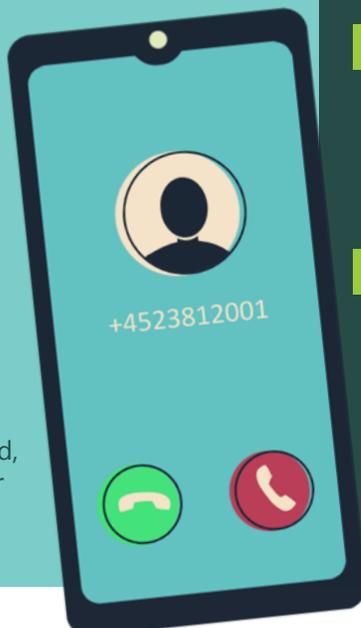


Establece un límite al uso del celular

Esto no es un castigo, poner un límite al tiempo en que usamos los dispositivos electrónicos nos hace menos vulnerables a estos ataques.

Reglas básicas:

Sólo responde llamadas de números de confianza. Pídeles consejos a tus padres o tutores acerca de tu seguridad, por ejemplo, a cómo configurar la privacidad de tu dispositivo.



Gánate la confianza

Para protegerte, es probable que tus padres o tutores establezcan ciertos límites. **Sigue estos tips para que confíen en que sabes lo que haces:**

- 1 Haz una lista de los sitios web que visitas.
- 2 Si usas una app, muéstrales para qué sirve y anímalos a descargarla.
- 3 Pasa tiempo con ellos. Encuentren actividades que no los obliguen a estar frente a una pantalla. 
- 4 Si necesitas cierta información para pagos online, indica para qué lo necesitas y deja que ellos ingresen los datos. 
- 5 Si conoces a alguien en línea, plátcales acerca de esa persona. Si tienes un mal presentimiento, acude a ellos. 

Datos que puedes compartir, sólo con familiares y amigos cercanos:

- Número telefónico
- Dirección
- Ubicación en tiempo real
- Fotografías de tu casa o colonia
- Tu actividad de compras en línea



¿Y las contraseñas?

Una contraseña segura hace toda la diferencia para todos los que están buscando cuentas vulnerables para atacar.

Tu contraseña es secreta. No la compartas. Si tienes que hacerlo, no lo hagas por mensaje o correo.



Utiliza al menos ocho caracteres, mezcla letras mayúsculas y minúsculas, números y símbolos, que sean fáciles de recordar para ti, pero difíciles de adivinar para los demás.



Usa diferentes contraseñas para todas tus cuentas. Crea tu propio código.

No repitas números (5555), no uses secuencias (1234), ni uses tu fecha de nacimiento.

1 2 3

No utilices como contraseña:

- Tu nombre
- Tu fecha de nacimiento
- Datos de tu familia o mascotas
- Nombres de celebridades



Cambia tu contraseña de manera periódica, de preferencia cada 3 meses por lo menos.

El internet es una herramienta casi infinita de información y entretenimiento. Por lo mismo, es vulnerable a fallos de seguridad que pueden perjudicarte a ti y a los que te rodean.

¡Toma el control de tus datos y ¡protege lo que más te importa!

Que no te roben la identidad

¿Por qué a mí?

Puede ser que no tengas una tarjeta de crédito o débito, sin embargo eres vulnerable a que algún cibercriminal haga mal uso de tus datos.



Tu identidad digital es muy valiosa porque:



No tienes historial de crédito

Es probable que no hayas pedido ningún préstamo, el perfecto escenario para un fraude.



Pasas mucho tiempo en internet

Probablemente tengas cuentas con datos personales en muchas plataformas. Ojo, ¡eso te hace más vulnerable!

Los crímenes a adolescentes son más difíciles de detectar
Puedes darte cuenta muchos años después.



Los datos personales que compartes

Nombres, correos, números telefónicos tuyos o de tus familiares son datos que se venden en todo el mundo. ¡Ten cuidado!

¿Qué pueden hacer

con estos datos?



Hacer compras online sin tu autorización.



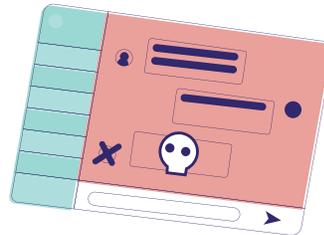
Acceder a tus dispositivos y ver tus fotos, apps y mensajes.



¿Qué pueden hacer con estos datos?



Realizar actividades ilegales como fraudes a tu nombre.



Enviar mensajes a tus amigos con un link peligroso, como un virus.

¿Cómo puedes protegerte?

1 ¡Cierra tu sesión! Si estás usando un dispositivo ajeno, siempre borra el historial y sal de tus cuentas.



No descargues contenido de sitios sospechosos.

2 No compartas datos personales. Si tienes que hacerlo, que no sea por mensaje o correo electrónico.



4 Usa contraseñas muy seguras en tus cuentas y dispositivos.

5 No des clic a links que no conozcas, incluso si ofrecen premios, o sitios que no indiquen de manera clara lo que contienen.

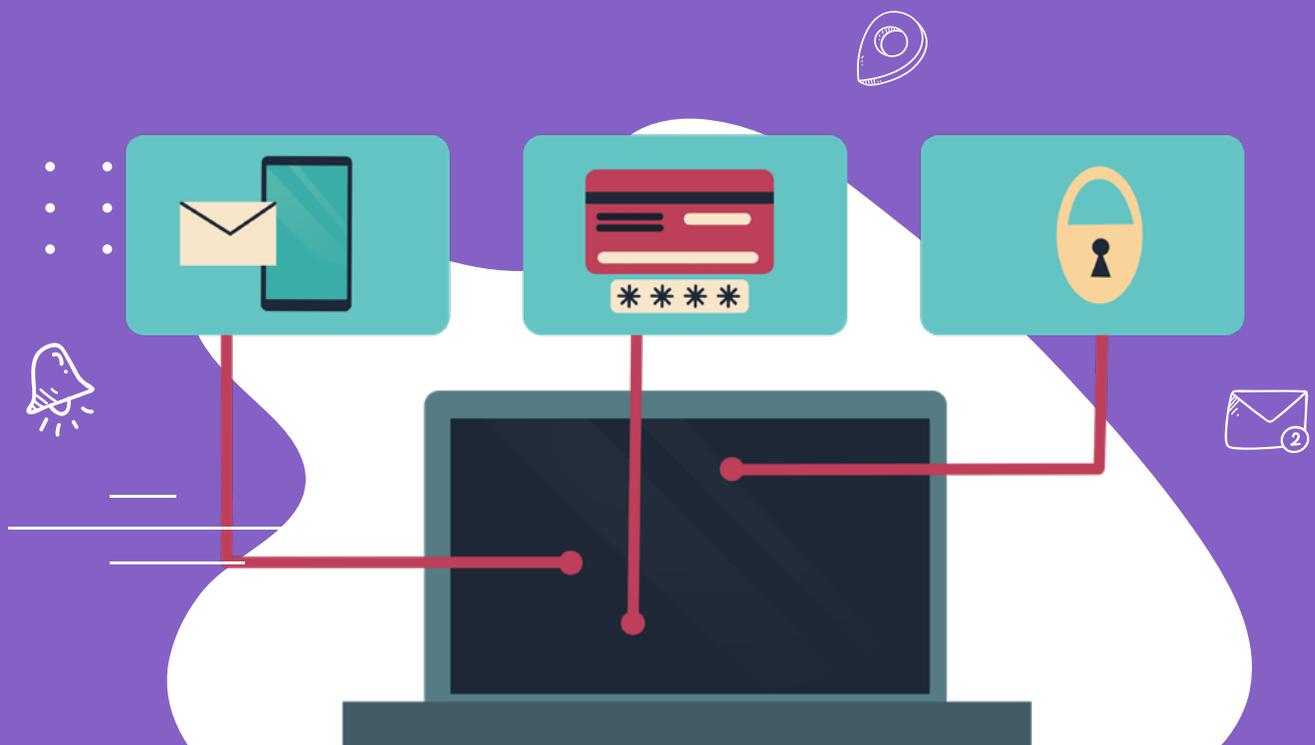


6 Cuando hagas compras online, acompáñate de un adulto de confianza.



Recuerda que tu seguridad está en tus manos. Si sospechas que te han robado la identidad o los datos, ¡repórtalo y plátalo con alguien de confianza!

Buenas prácticas en internet



Aparte de los fraudes y el mal uso de datos, los riesgos de las actividades online también nos afectan emocional y mentalmente. El ciberbullying es una práctica muy común que afecta a millones de adolescentes en todo el mundo, ¡es momento de que ayudes a detenerlo!

En este módulo:

- Aprenderás qué es la empatía y por qué hay que pensar antes de dar clic en enviar.
- Te protegerás del robo de identidad y el grooming.
- Conocerás la resiliencia, tu mejor arma contra el ciberbullying.
- Identificarás noticias falsas para así combatir la desinformación.
- Podrás identificar los riesgos del sexting, una práctica cada vez más popular.

¡Piensa antes de enviar!

Guía de Empatía para Principiantes

Más veces de las que quisiéramos, nos encontramos con publicaciones en internet que logran enojarnos o entristecernos mucho. Nos provoca tanto, que a veces solo queremos responder lo primero que nos pasa por la cabeza.

Te invitamos a detenerte y pensar lo siguiente:

¿Por qué lo publicó?

- Ponte en el lugar de la otra persona. Piensa cómo se sintió cuando escribió la publicación o mensaje.
- Entiende su enojo, aunque no lo compartas.
- Reconoce su experiencia, puedes contar la tuya.
- Si quieres, ofrece apoyo.
- No contestes con enojo. Respira profundo. Una vez que te sientas mejor para responder, no ataques a la persona. Por ejemplo:

"No estoy de acuerdo con tu opinión, porque...",
en lugar de: *"Estás equivocado porque..."*

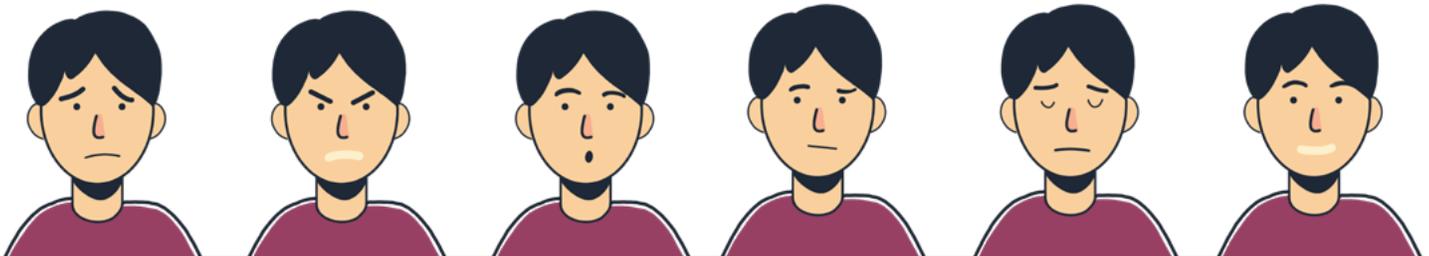


Haz preguntas

Si no logras entender el porqué de su comentario, haz preguntas para conocer los motivos.

- No supongas ni ofendas.
- Pregunta cómo obtuvieron esa información o cómo llegaron a esa opinión.

"Gracias por compartir. Estoy interesado en conocer más sobre este tema, ¿puedes compartirme más información?"



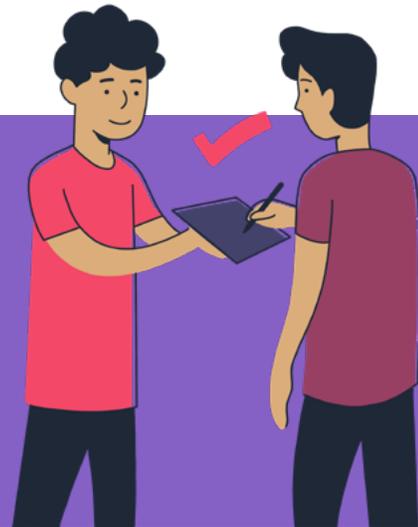
Responde a la idea, no a la persona

1

Encuentra cosas en común

¿Estás de acuerdo con alguna parte de la publicación? Puedes utilizar esto como punto de arranque. Por ejemplo:

“Me interesa o me gusta... pero no estoy de acuerdo con... porque...”



2



Defiende tu opinión con respeto

¡No te lo hagas más difícil! Cuida las palabras que usas. Respeto la opinión de los demás y acepta los diferentes puntos de vista. Por ejemplo:

“Hay muchas opiniones diferentes sobre esto. Mi opinión es ...”, o “Fue interesante escuchar tu perspectiva. Mi perspectiva es”

3

Piensa antes de enviar

Tú eres responsable de lo que publicas. Lee tu respuesta. Si todavía dudas de estar ofendiendo o respondiendo con mucho enojo, pídele a un amigo que lo lea.



Recuerda:

A veces no responder puede ser la mejor respuesta

Cuando alguien te responde con empatía, te das cuenta. No te hace sentir mal, aunque no compartan las mismas opiniones. Si te cuesta trabajo saber qué hacer, empieza por la regla de oro: No hagas algo que no te gustaría que te hicieran a ti.

Quiz: ¿Sabes ponerte en el lugar de otras personas?

Conoce tu nivel de empatía a través de este quiz. Imagina que te encuentras en alguna de las siguientes situaciones, elige la respuesta que describa mejor cómo reaccionarías.

Cada respuesta equivale a un punto, al terminar suma todos tus puntos.

Finalizando descubrirás si eres capaz de ponerte en el lugar de otras personas.

1. Lees una publicación de una persona que conoces: "Amigos, necesito ayuda. Mi familia está pasando por un momento muy difícil. Necesitamos su apoyo para poder seguir adelante"
¿Cómo reaccionas?

 - a. Me cuesta trabajo conectar con lo que le está pasando. No veo por qué ayudaría a alguien que apenas conozco. (0)
 - b. Creo que imagino cómo se siente. Es probable que lo platique con mis padres para ver si podemos apoyarlo de alguna manera. (+1)
 - c. Quiero apoyarle. Le escribo para ver qué necesita y si puedo, le ayudo en cualquier cosa que necesite. (+3)
2. Una de tus mejores amigas subió una foto con su cantante favorita. Está siendo ciberbulleada por varias personas que se burlan de sus gustos musicales.

 - a. Respondo a los comentarios pidiendo que respeten los gustos de mi amiga. (+3)
 - b. Le recomiendo a mi amiga que borre la publicación y me burlo de ella en broma. (+1)
 - c. No hago nada. No es mi problema. (0)
3. Alguien que quieres sube una historia donde está llorando. Explica que se siente muy mal por haber terminado una relación amorosa. ¿Qué le dirías?

 - a. Le preguntaría si quiere platicar del tema y cómo puedo ayudarle. (+3)
 - b. Reaccionaría con una carita triste. (+1)
 - c. Ignoro la historia. Qué pena que suba esas cosas. (0)
4. Recibes un mensaje de un amigo: "Necesito hablar". Inmediatamente te entra la llamada de esa persona.

 - a. ¿Llamada? ¡No le contesto! No me gusta hablar por teléfono. (0)
 - b. Si no puedo contestar, le mando un mensaje preguntando si todo está bien. (+1)
 - c. Contesto y lo escucho. Si me lo pide, le doy un consejo. (+3)
5. Alguien en tu círculo de amigos acaba de ganar un premio muy importante. Está muy feliz y no deja de presumirlo en todas sus redes sociales.

 - a. ¡Qué bien! Le felicito y quizá comparto su logro en mi perfil. (+3)
 - b. Siento que presumir está de más. Ojalá no lo hiciera. (0)
 - c. Le doy like a su publicación. (+1)

Resultados



De 10 a 15 puntos

¡Felicidades!
La empatía se te da muy natural.

Sabes ponerte en el lugar de otras personas y ofreces lo que está en tus posibilidades para ayudar. ¡No toleres el ciberacoso!

De 6 a 10 puntos

Te gusta estar ahí para tus amigos.

Hay veces que prefieres ignorar los problemas de los demás pero si alguien te necesita no dudarás en darle una mano.

De 0 a 5 puntos

La empatía no es tu punto fuerte.

Trata de pensar cómo te sentirías si estuvieras en el lugar de otra persona cuando tienen un problema. ¡Inténtalo!



¿Qué es la resiliencia?

Cuando tenemos un problema, la resiliencia es la capacidad de resistir y recuperarse. **Recuperas el control y transformas las situaciones difíciles en oportunidades.**

¡La resiliencia te hace más fuerte!

En internet, la resiliencia te sirve para enfrentar el ciberacoso y otras situaciones complicadas.

Ya sabes, los haters.

El ciberacoso puede provocar que sientas alguna de estas emociones:

- Enojo
- Tristeza
- Ansiedad
- Soledad



¡Lo bueno es que la resiliencia puede aprenderse! ¿Qué puedes hacer?:



1 Reconoce el problema.
Identifica las emociones que te hace sentir y acéptalas.



2 Abre la conversación
Un ¿podemos hablar? puede cambiar las cosas. Haz preguntas, escucha y habla de manera clara sobre tus emociones y opiniones.

4 Da un paso atrás
Aléjate un poco de la situación. Verás las cosas más claras. No te exijas mucho, tus sentimientos son válidos y es muy probable que después las cosas se sientan mejor.

3 Pide apoyo
Si se están complicando las cosas, habla con un adulto de confianza. Sabrá qué hacer y te ayudará con la carga del problema.



Desconéctate
Pasar tiempo a solas o con tus amigos y familia, sin estar frente a una pantalla, te ayudará a poner las cosas en perspectiva.



Es muy válido sentir enojo o tristeza cuando nos enfrentamos a un problema. Lo que nos enseña la resiliencia es que un mal momento no tiene que significar un mal día o semana.

¡Podemos salir adelante! ¿Qué estrategias utilizas tú para sentirte mejor?

Quiz: ¿Sabes lo que puedes controlar?

En esta actividad te invitamos a tener más resiliencia, identificando las cosas sobre las que tienes control. ¡Llena tu mochila! El peso de la mochila es mayor si incluimos aquello sobre lo que no tenemos influencia. ¡Esto no nos permite avanzar!

Instrucciones: De la siguiente lista de frases, selecciona las cosas que sí puedes controlar. Al terminar **revisa tu puntaje aquí**

Tengo el control de

- Lo que yo opino sobre mí
- Quiénes son mis amigos
- Las noticias de mi país
- El lugar donde nació
- La opinión que las otras personas tienen sobre mí
- Lo que publico en redes sociales
- El futuro
- Mi salud
- Mi opinión
- Los comentarios que otras personas hacen en las redes
- Lo que otras personas sienten
- Los videojuegos que elijo jugar
- Mis acciones
- La manera en que otras personas me tratan
- La opinión de otras personas
- Mis gustos
- Mi edad
- Quiénes son mis papás
- Mi talento
- Mi privacidad en internet
- Mi seguridad al jugar videojuegos
- Lo que otras personas dicen
- Lo que otras personas hacen
- La familia en la que nació
- Mi color de piel
- Los desastres naturales
- Lo que hago con mi tiempo
- El pasado
- El clima
- La felicidad de otras personas
- Mi actitud



Resultados

9 - 13 puntos

¡Felicidades! Puedes cargar la mochila sin problemas.

Recuerda que dejando ir las cosas sobre las que no tenemos control nos ayuda a vivir con más tranquilidad y a salir adelante más fácilmente.

5 - 9 puntos

¡Todavía hay cosas que puedes dejar ir!

Recuerda que mientras más claras tengamos las cosas sobre las que podemos influir, más fácil va a ser salir adelante y enfrentar los problemas.

0 - 4 puntos

¡La mochila todavía está muy pesada!

Dejar ir las cosas sobre las que no tenemos control nos permite vivir una vida más tranquila. ¡Vuelve a intentarlo!

La resiliencia es nuestra capacidad de afrontar los problemas y salir adelante.

Para esto es necesario que sepas las cosas que sí puedes cambiar. Todo lo demás es inevitable, así que puedes relajarte un poco :). Lo que sientes es válido. Si crees que te está costando mucho trabajo afrontar tus problemas o a esa persona que te hace sentir mal, te recomendamos que lo platiques con tus papás, tutores o maestros. Ellos podrán ayudarte y enseñarte un poco más acerca de la resiliencia para hacer tu vida más fácil.

¿Qué es el sexting y cuáles son sus riesgos?

La palabra sexting viene de las palabras en inglés 'sex' (sexo) y 'texting' (mensajear) y consiste en enviar mensajes, fotos o videos sexualmente explícitos o sugestivos utilizando medios electrónicos, puede ser voluntario o forzado, en este último caso es una forma de violencia y acoso sexual y representa un riesgo grave para los adolescentes.

Recuerda el sexting debe ser una decisión personal y puede tener muchos riesgos y consecuencias.



¡Ten cuidado! el sexting si es forzado es violencia sexual y es un delito en varios países, recuerda que todo lo que compartes es público.



Aunque cualquier persona que tiene al alcance un medio electrónico puede recibir o mandar este tipo de mensajes, **los adolescentes son quienes lo hacen con más frecuencia.**

En los últimos años ha aumentado el envío de material sexual, se calcula que **1 de cada 4 jóvenes han recibido fotos o videos de este tipo.**



Riesgos

El mayor riesgo del sexting es perder el control de tus fotos o videos íntimos y que sean utilizados para perjudicarte. Tal vez porque la persona a quien lo enviaste le da un uso indebido o porque no fue una práctica segura. Ten cuidado: **El 90% de este tipo de contenido termina siendo accesible para cualquier persona en internet.**



Si tienes algún problema relacionado con tu contenido íntimo no dudes en hablar con un adulto de confianza. **Que no te dé pena, es muy importante cuidarte.**



Ciberacoso

Divulgación

Que tus fotos o videos terminen en sitios públicos o redes sociales.

Extorsión

Que algún agresor te amenace o chantajee.



Si ves que alguien está haciendo uso indebido de las fotos o videos íntimos de otra persona en un chat o en cualquier otra plataforma, ¡detente! **¡No compartas este tipo de contenido, no seas parte del problema!**

**¡Evita ponerte en riesgo!
Cuida lo que compartes.**

¡Cuídate!

Lo que tienes que saber del cyberbullying y el online grooming

La violencia que se ejerce contra niños, niñas y adolescentes en el mundo físico, también se presenta en internet. Así como existen el acoso (bullying) y el abuso o acoso sexual infantil, también existen el cyberbullying y el acoso sexual infantil conocido como online grooming.

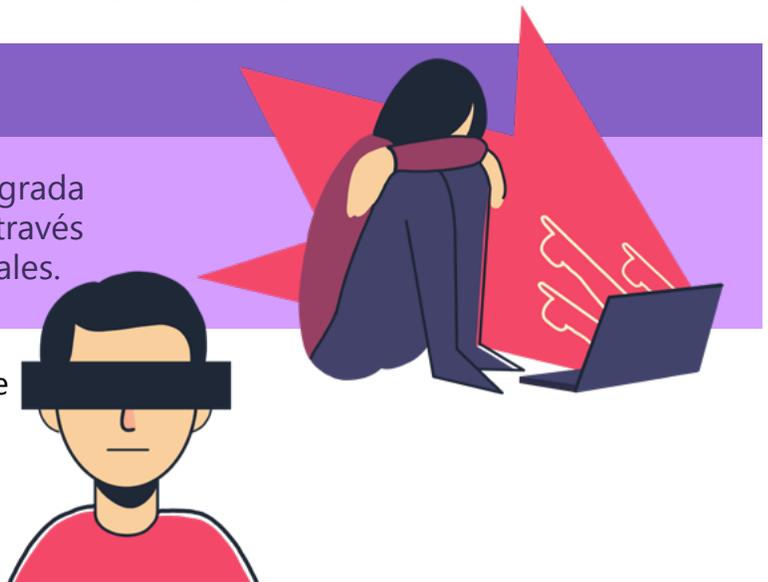
Es muy importante que los identifiques para poder detenerlos.

¿Qué es el cyberbullying?

El cyberbullying es cuando se provoca, degrada o acosa a alguien de manera constante a través de mensajes de texto, juegos o redes sociales.

Lo más peligroso del cyberbullying es que puede seguir una vez que sales de la escuela, ya que tenemos acceso a las redes todo el tiempo.

Si el agresor es anónimo puede ser más violento porque se siente protegido.



¿Por qué sucede?

Los agresores tienen muchas razones para hacerlo, algunas son:

- También fueron agredidos
- Piensan que es divertido
- Para obtener aprobación



Muchas veces no se dan cuenta de lo graves que pueden ser sus acciones ni del dolor que están causando.

¿Cómo combatirlo?

Sé parte de la solución, no caigas en el cyberbullying:

- Si no se lo puedes decir de frente, no se lo digas en redes sociales.
- No participes en conversaciones que acosan a otra persona. ¿Te gustaría que dijeran esas cosas sobre ti?
- Si ves que están agrediendo a alguien, reporta y ayuda a detener estos abusos.
- Borra el contenido de los mensajes de bullying.
- **¡No lo sigas compartiendo!** Piensa en cómo te sentirías.



¿Qué es 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.



Los groomers están por todos lados, incluido el internet. **¿Cómo identificar a un groomer?:**

- Se pone en contacto a través de redes sociales, videojuegos o foros digitales.
- Puede ofrecerte regalos o prometer cosas.
- Una vez que se gana tu confianza, puede empezar a sextear contigo o abusar sexualmente de ti.
- Si no quieres hacer lo que esta persona te dice, te amenazará con hacer daño a familiares o amigos, o hacer pública alguna foto comprometedor.

¡Es muy importante detectarlo y detenerlo!

¿Cómo puedo protegerme del grooming?

No hables con extraños. Recuerda que no sabes quiénes son realmente y podrían tener una identidad falsa. No lo mantengas en secreto Si alguien te amenaza o te presiona para hacer cualquier cosa que no quieras, cuéntale a un adulto de confianza.



Su mayor miedo es que sean descubiertos. ¡El poder está en ti! Reporta a esta persona o acude con un adulto de confianza para que te apoye.

Reporta

Cuando reportas a un posible groomer, estás ayudando a que otros menores de edad no se expongan a este tipo de abusos.

No te intimides con las amenazas del groomer. Generalmente usan información que tú ya tienes en tus redes sociales.



¡Dile NO a la violencia online!
Confía en tus instintos. Detecta y denuncia el ciberbullying y el grooming.



¿Qué son y cómo detecto las fake news (noticias falsas)?

Las fake news son noticias que se difunden a través de distintos medios y llegan a ser virales. El problema es que son falsas.

¿Quieres saber cómo detectarlas? Sigue leyendo.



Seguro has leído alguna noticia que te parece difícil de creer, pero que se vuelve viral muy rápido. Esto te hace dudar si es cierta o no. Por ejemplo:

- El cambio de equipo de un deportista
- La muerte de una celebridad
- Imágenes filtradas de versiones nuevas de videojuegos de Xbox

Difundir noticias falsas puede tener consecuencias muy graves, algunas son:

- Destruir la reputación de una persona
- Cambiar la opinión de mucha gente sobre un tema
- Alarmar o incitar discursos de odio
- Hacerte entrar a sitios no seguros donde pueden hacer mal uso de tu información

Lo bueno es que combatir las fake news es muy sencillo: sólo hay que confiar en nuestro instinto para detectarlas y así no compartirlas

Algunos tips para reconocer las fake news:

1 Fíjate en qué fecha se publicó, a veces es información muy vieja.



2 Comprueba si hay faltas de ortografía o errores en el texto, un portal de noticias serio no las tendría.



3 Revisa si las imágenes tienen muy baja resolución o parecen retocadas, algo anda mal en esa foto...



4 Confirma de qué fuente viene, sólo confía en medios autorizados.



5 Compara, si te parece que la noticia es un poco extraña, revisa si ese tema se está hablando en otro medio.

6 Ahora ya sabes cómo detectarlas así que, antes de compartir cualquier noticia, asegúrate de que la información sea verdadera y reflexiona sobre las consecuencias que podría tener compartir fake news.

Acabar con las fake news está en ti.
Di NO a la desinformación.

Quiz: ¡No caigas en Fake News!

¿Sabes diferenciar las noticias falsas de las verdaderas?
¡Descúbrelo con este quiz!

Instrucciones:

A continuación te mostramos 5 noticias. ¿Son verdaderas o falsas?

¡Pon a prueba tus habilidades de detective! Al terminar [revisa tu puntaje aquí](#)

1

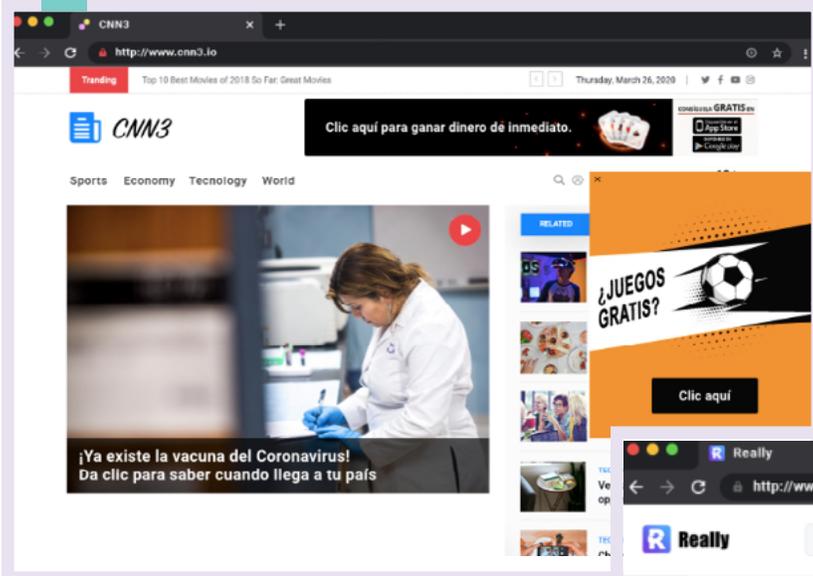
2

3

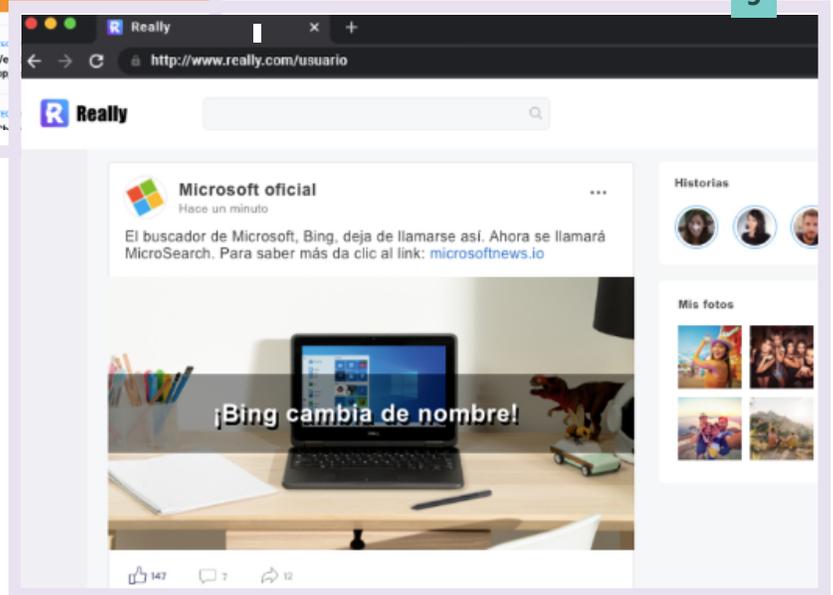
The image displays three screenshots of fake news content. The first screenshot shows a website titled 'NOTINUEVAS' with a headline '¡Se cancela el lanzamiento del Xbox Series X!' and a video player showing a man speaking. The second screenshot shows a YouTube channel '2.YOUTUB' with a video titled '¡CANCELA SUS REDES SOCIALES!!'. The third screenshot shows a social media post from 'Microsoft' on 'Really' with a video of a person working on a laptop.

Quiz: ¡No caigas en Fake News!

4



5



Resultados



5 correctos

¡Eres un gran detective!

No hay quien pueda engañarte, sabes detectar muy bien las noticias falsas. Cada que veas que alguien comparta una, recuerda hacerle saber la importancia de revisar y verificar que la información no sea engañosa. ¡Felicidades!

3-4 correctos

¡Muy bien! Eres un detective en entrenamiento.

Descubrir noticias falsas no es fácil. Recuerda revisar cada uno de los elementos que le dan veracidad a una noticia. ¡Vas en buen camino!

1-2 correctos

¡Pon más atención!

Las noticias falsas están por todo el internet. Además de desinformar, los sitios que las comparten suelen ser inseguros y pueden hacer mal uso de tus datos. ¡Vuelve a intentarlo!

Videojuegos

Tips para tu seguridad

Los videojuegos son súper divertidos. Hay una cantidad infinita de opciones para todos los gustos. Jugarlos en línea incrementa las posibilidades de conocer gente nueva, pero también aumenta el peligro para tu seguridad.

Estos son algunos tips para que tengas la mejor experiencia.



Revisa la edad para la que está hecho el videojuego que quieres jugar. Si está hecho específicamente para ti, ¡te divertirás mucho más!



Si te informas, podrás aprovechar mejor todo lo que el juego te ofrece. Investiga con ayuda de un adulto de confianza el tipo de contenido y las reseñas.

Desarrolla la confianza con tus papás o tutores.

Deja que revisen el juego antes de comprarlo o descargarlo. Muéstrales que no hay peligro. Tendrás menos problemas con ellos ;)



No compartas información personal con extraños

NUNCA compartas tu nombre real, correo electrónico, dirección de casa, escuela o edad.



Usa contraseñas seguras

Ya que en tu perfil de jugador compartes datos personales, protege tu cuenta con una contraseña difícil de adivinar.

No toleres ni practiques el ciberacoso



Si te topas con algún hater o troll, avísale a tus padres para que puedan reportarlo. Ignora y bloquea a este tipo de jugadores.

Tu nombre de usuario es una oportunidad perfecta para mostrar tu creatividad.

Por tu seguridad no incluyas tu nombre real, edad ni país.



Tu seguridad es muy importante. Cuidate para que jugar videojuegos no deje de ser divertido ;)

Hoja de respuestas

Resiliencia

TENGO EL CONTROL DE:

Va en la mochila +1

No va en la mochila 0

- Lo que yo opino sobre mí
- Quiénes son mis amigos
- Las noticias de mi país
- El lugar donde nací

- La opinión que las otras personas tienen sobre mí
- Lo que publico en redes sociales
- El futuro
- Mi salud

- Mi opinión
- Los comentarios que otras personas hacen en las redes sociales
- Lo que otras personas sienten
- Los videojuegos que elijo jugar

- Mis acciones
- La manera en que otras personas me tratan
- La opinión de otras personas
- Mis gustos

- Mi edad
- Quiénes son mis papás
- Mi talento
- Mi privacidad en internet

- Mi seguridad al jugar videojuegos
- Lo que otras personas dicen
- Lo que otras personas hacen
- La familia en la que nací

- Mi color de piel
- Los desastres naturales
- Lo que hago con mi tiempo

- El pasado
- El clima
- La felicidad de otras personas
- Mi actitud

Fake news

Noticia 1.

VERDADERA: Recuerda revisar bien el URL de la página y detalles en las fotografías que te revelen si la noticia es falsa. (0)
FALSA: ¡Muy bien! Los sitios web de noticias falsas normalmente usan imágenes alteradas y las URL que las contienen no son seguras. Fíjate que la URL sea segura. (+1)

Noticia 2.

VERDADERA: ¡Respuesta incorrecta! Recuerda revisar bien el URL al que vas a dar clic y la fuente que está compartiendo la información. (0)
FALSA: ¡Muy bien! Para compartir fake news muchas veces se crean perfiles falsos, además, dar clic en URLs sospechosos puede ser peligroso para la seguridad de tu computadora. (+1)

Noticia 3.

VERDADERA: ¡Excelente, la noticia es verdadera! La cuenta desde la que se publicó el video está verificada y el título no parece ser clickbait. (+1)
FALSA: Recuerda que si la fuente que comparte el video está verificada, es casi seguro que sea información en la que puedes confiar. (0)

Noticia 4.

VERDADERA: Recuerda revisar el URL. Existen muchos sitios web falsos que ganan dinero por los clics a los anuncios que muestran. (0)
FALSA: La noticia es falsa.
 ¡Tienes un excelente ojo para esto! (+1)

Noticia 5.

VERDADERA: Recuerda revisar bien el URL al que vas a dar clic y la fuente que está compartiendo la información, ¿está verificada? (0)
FALSA: ¡Excelente! No hay que olvidar revisar cada detalle de las publicaciones para no caer en fraudes ni sitios con malware. (+1)

Civilidad Digital



Además del mundo en el que vivimos, habitamos otro digital e infinito: el internet. Nos encontramos con personas de todo el mundo que varían en edad, ocupación y gustos. ¿Cómo tratas a otras personas online?

En este módulo:

- Aprenderás qué es el Índice de Civilidad Digital y por qué es importante conocer la conducta en línea.
- Podrás participar en nuestro reto, #DigitalSafetyChallenge, donde te invitamos a convertirte en líder de la civilidad en internet.
- Identificarás noticias falsas para así combatir la desinformación.
- Podrás identificar los riesgos del sexting, una práctica cada vez más popular.

Índice de Civildad Digital

Con el objetivo de hacer del internet un lugar más seguro para ti, cada año Microsoft realiza una encuesta en distintos países para estudiar las conductas en internet. La idea es que con estos resultados se puedan prevenir riesgos de seguridad y mejorar la experiencia en línea.

Estos son algunos datos del Índice de Civildad Digital 2020*:



2019

La civildad digital mundial alcanza su nivel más bajo en 4 años

La conducta en las interacciones se vuelve negativa debido a:

- Apariencia física
- Tendencia política
- Orientación sexual

La falta de civildad digital genera interacciones negativas en línea que traen consecuencias emocionales.

Lugar por país en Civildad Digital:

(de 25 países encuestados)



Argentina:

19



Colombia:

23



México: 17



Perú:

24



Chile: 18



Dos tercios de los encuestados declararon que **son las redes sociales** el lugar más frecuente para la falta de civildad

75%

de los usuarios de internet han sido incivilizados con otras personas

Se detectaron 21 riesgos en línea que entran dentro de estas categorías



Los 5 riesgos principales:

En los adolescentes los riesgos más comunes fueron contacto no deseado por gente extraña, sexting no deseado y ciberacoso. La civildad digital nos permite tener una mejor experiencia navegando por internet.

1. Contacto no deseado
2. Engaños / Fraudes / Estafas
3. Sexting no deseado
4. Maltrato
5. Trolling

¿Tú ya aceptaste nuestro #DigitalSafetyChallenge?

Sigue los 4 acuerdos y sé parte de la solución, no del problema ;)

*Digital Civility Index 2020

Reto de Civildad Digital

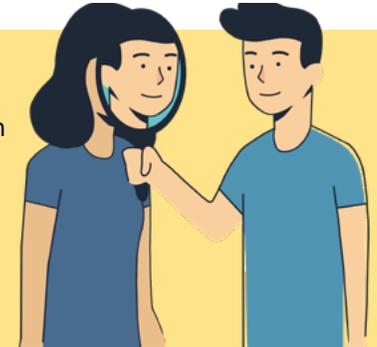
#DigitalSafetyChallenge

En Microsoft hemos puesto manos a la obra y creamos el Reto de Civildad Digital. ¿Quieres saber de qué se trata? **El reto consiste en seguir estos 4 acuerdos para la mejor y más segura experiencia en internet:**

1 Vive la regla dorada. Palabra Clave: **Empatía**

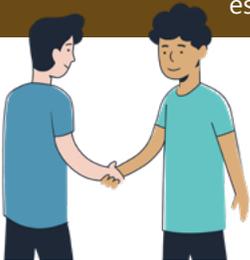
Trata a los demás como quieres que te traten a ti. Actúa con empatía, compasión y amabilidad y trata a todos con dignidad y respeto. Esto es muy fácil, antes de publicar o responder, pregúntate:

- ¿Me gustaría que me dijeran esto a mí?
- ¿A quién puedo afectar con esta publicación?
- ¿Estoy dando mi opinión con respeto a los demás?



Recuerda que actuar con respeto y empatía es un tema muy importante, si todos siguiéramos esta regla, los problemas por ciberbullying desaparecerían.

2



Respetar las diferencias. Palabra Clave: **Respeto**

Aprecia las diferencias culturales y honra las perspectivas e ideas diferentes a las tuyas, cuando estás en desacuerdo cuestiona y pláticalo evitando insultos y ataques personales.

3 Piensa antes de hablar y dar una respuesta. Palabra Clave: **Resiliencia**

Si no estás de acuerdo con algo y te causa mucho enojo y tristeza, antes de responder haz una pausa y reconoce tus emociones. Al responder:

- No dañes la reputación de otras personas
- No amenaces a nadie
- No pongas en riesgo tu seguridad ni la de los demás



¡Practica tus habilidades de resiliencia!

En el módulo de Buenas Prácticas podrás encontrar más información al respecto.

4



Defiéndete a ti mismo y a los demás. Palabra Clave: **Valentía**

¿Eres testigo o víctima de ciberbullying o te has sentido inseguro en línea?

¡Que no sea un secreto!

- Pide ayuda
- Ofrece apoyo si notas una situación de ciberbullying
- Reporta publicaciones y perfiles que amenacen la seguridad de cualquier persona
- ¡Guarda la evidencia con capturas de pantalla!

Comparte en redes sociales tus acciones para hacer del Internet un lugar mejor.
 ¡Utiliza los hashtags #DigitalSafetyChallenge, #challenge4civility y #Im4DigitalCivility e invita a tus amigos a unirse! Publicaremos tus experiencias en nuestras redes :)

¿Necesitas ayuda?



La seguridad en internet es un tema que nos afecta a todos. Recuerda que si tienes algún problema en el que te sientas incapaz de resolver, siempre puedes acercarte con un adulto de confianza o reportarlo en las redes sociales o con el proveedor del servicio, en la sección destinada para ello.

Preguntas frecuentes

¿Qué hago si una persona que no conozco me pide datos personales como nombre completo, dirección o nombre de mis familiares?

Si una persona extraña te solicita tus datos NO se los des. Los cibercriminales tienen una gran variedad de técnicas para obtener datos de manera ilegal. Te recomendamos no compartir estos datos personales de manera digital, incluso si conoces a la persona. Si es necesario que lo hagas y no puedes hacerlo en persona, lo mejor es que sea a través de métodos un poco más seguros como una llamada o un mensaje de texto cifrado.

¿Cómo detengo una situación de ciberbullying si estoy bajo amenaza?

Bloquea o elimina a la persona y haz el reporte en la sección destinada para ello. Si la amenaza persiste, acércate con un adulto de confianza para que te apoye. Al final de esta sección de preguntas encontrarás links que te serán de utilidad para reportar ataques de odio y abusos.

¿Cómo protejo mi reputación online?

Recuerda ¡Siempre piensa antes de dar clic en publicar o enviar! Aunque las cuentas que tienes en redes sociales sean privadas, cualquiera puede tomar capturas de pantalla o compartir tus publicaciones sin tu consentimiento. Si no has tomado medidas de seguridad y privacidad, te expones también a ataques cibernéticos y hackeos. También recuerda publicar y responder siguiendo la regla de oro: No hagas lo que no quieres que te hagan.

¿Cómo sé si tengo una adicción al celular o a las redes sociales?

La adicción a las redes sociales puede empezar a notarse cuando te alejas de la vida real por estar en línea. Además, la sensación de ansiedad aumenta y tu autoestima se ve afectada. El uso no consciente de tus dispositivos puede provocar situaciones negativas a tu persona. Si crees que necesitas ayuda, pídelas.

¿Cómo sé que un videojuego es seguro?

Lo primero que tienes que hacer es fijarte en la edad para la que está hecha. Las características y tipo de juego estarán diseñados específicamente para ti, lo que hará que no te encuentres con sorpresas poco favorecedoras que te pueden poner en riesgo si juegas en línea. También, revisa con tus padres o con un adulto de confianza las reseñas del juego, por lo general habrá algún tipo de advertencia si representa un riesgo para los usuarios.

¿Qué necesito instalar para proteger mi computadora?

Lo esencial es instalar una aplicación antimalware y un firewall. En [este link](#) podrás encontrar los pasos que puedes seguir para asegurar que tu computadora esté protegida contra todo tipo de ataques.

¿Qué hago si recibo un mensaje inapropiado (sexting) sin autorización?

Si recibiste el mensaje en una red social, bloquea y reporta esa cuenta. Si conoces a la persona, puedes hablar y pedir que no vuelva a suceder. Si la conducta se repite o te enteras que lo está haciendo con más personas repórtalo. Recuerda que siempre puedes pedir ayuda a tus padres o con un adulto de confianza.

¿Cómo hablo con mis padres o tutores para que me tengan más confianza?

La mejor manera de generar confianza con tus padres o tutores, es explicándoles y mostrándoles para qué usas el internet. Les dará más confianza saber con quién hablas, sin necesidad de decirles específicamente de qué, pero dales también la confianza de que estén al pendiente para que puedan hacer acuerdos de tiempo y uso.

¿Es seguro confiar en alguien que conocí en internet?

Conocer a personas en línea es algo muy común, por lo que hay que tomar en cuenta algo muy importante: el lenguaje no verbal. Cuando una relación es cara a cara, podemos ver la realidad de la otra persona. Una relación cibernética da mucho más lugar a la imaginación: podemos idealizar a alguien y posteriormente, decepcionarnos. Debes tener mucho cuidado, puedes pedir que hablen por videollamada y seguirlos en sus redes sociales para saber que esta persona existe y hay otras personas a su alrededor que si le conocen.

¿Cómo sé que un sitio web es seguro?

Los sitios seguros por lo general comienzan con "https://" y tienen un candado a un lado. Tu navegador también tiene herramientas para identificarlos, por lo general te dará una advertencia si estás entrando a un sitio web inseguro. Si sigues las recomendaciones, evitarás situaciones de riesgo.

¿Por qué mi información es atractiva para los cibercriminales?

Los datos que compartimos en internet son muy valiosos. Las marcas, por ejemplo, los utilizan para mostrarte anuncios que están específicamente diseñados para ti. Pero los cibercriminales se dedican a buscar fallos de seguridad en todos los usuarios de internet, con el fin de realizar fraudes de dinero, robo de identidad y robo de datos personales. ¡Ten cuidado!

Recomendaciones

- [Denuncia o reporta un incidente al Centro Nacional para Niños Desaparecidos y Explotados \(NCMEC\)](#)
- [Formulario para reportar la distribución no consensuada de imágenes íntimas](#)
- [Formulario para reportar lenguaje de odio](#)
- [Reportar abusos en OneDrive](#)
- [Reportar un problema en Bing](#)
- [Formulario para reportar contenido terrorista](#)

Conoce sobre el gaming



La configuración familiar de Xbox ya está disponible y ofrece un gaming divertido y positivo, así como nuevas herramientas para juegos interplataforma, [¡Leer más!](#)



Nuevos límites en juegos y aplicaciones se integran a las opciones de configuración familiar [¡Leer más!](#)



Sigue estos 5 tips de los Xbox Ambassadors para un juego en línea seguro [¡Leer más!](#)



Xbox anuncia la aplicación Configuración familiar de Xbox (Preview) para ayudarte a administrar el juego de tus hijos [¡Leer más!](#)

Padres, tutores y maestros



Como adultos, debemos estar preparados para ayudar a los adolescentes a resolver los problemas, situaciones o preguntas que pudieran tener relacionadas con sus interacciones en línea. Es importante conocer cómo se comportan e interactúan, qué contenido buscan, las principales actividades que realizan y las tendencias actuales del mundo digital; entre más información y conocimiento tengamos a nuestro alcance, podremos reaccionar mejor y proporcionar consejos y/o soluciones.

Estos módulos también son para ti, te ayudarán a actualizarte sobre estas situaciones y a identificar posibles riesgos. Aprender y conectarse a través de la tecnología es vital, lo que significa que ser un buen ciudadano digital adquiere cada vez mayor importancia. Es por esto que debemos seguir aprendiendo sobre los beneficios y riesgos del mundo en línea, así como desarrollar los hábitos que puedan ayudarnos a estar más seguros y proteger lo que más nos importa.

Preguntas frecuentes

La seguridad digital es un tema que nos afecta a todos. Este material está enfocado en compartir información importante sobre la seguridad en internet, específicamente la de los adolescentes. Estas son algunas de las preguntas más frecuentes que hacen los padres de familia o tutores al respecto:

¿Cuáles son las señales del ciberbullying?

A menudo no las hay, pero hay que poner atención si el adolescente presenta dificultad para dormir, revisa sus redes sociales constantemente y con ansiedad, no quieren asistir a clases o notas su autoestima baja.

¿Qué hago si hay una situación de ciberbullying?

Mostrar su apoyo incondicional. No llamar la atención por haberse metido en ese problema, sino escuchar y tratar de entender el porqué. Lo mejor que pueden hacer es bloquear y reportar a la persona, y en caso de ser de la misma escuela, hablarlo con las autoridades escolares. Es importante hacerle sentir al adolescente que pueden tomar el control de la situación por sí mismos.

¿Qué hago si un adolescente ciberacosa a otras personas?

No hay que reaccionar de manera agresiva. Probablemente el problema sea interno, por lo que lo mejor es escuchar, apoyar y buscar soluciones juntos; además de poner ciertas restricciones al uso de dispositivos para conectarse.

¿Qué pasos puedo seguir para mantener segura a mi familia?

Todos los dispositivos de casa deben estar protegidos y los sistemas operativos actualizados. No permitas que se instalen aplicaciones desconocidas y enseñe con el ejemplo a regular y medir sus tiempos de uso.

¿Por qué es importante identificar el discurso de odio?

Los comentarios negativos y con mala intención, traen consecuencias negativas mentales y emocionales. A veces hasta pueden llegar a la violencia física. El ciberbullying puede convertirse en discurso de odio cuando degrada a una persona o grupo de personas con base en su identidad de género, orientación sexual, religión, discapacidades o imagen corporal. Fomenten la empatía y la resiliencia en casa, además de brindar la información necesaria para evitar prejuicios.

¿Qué es el sexting y cómo prevenirlo?

Es una forma de coqueteo o una demostración de afecto, en forma de imágenes o videos íntimos. El problema es que puede ser un comportamiento impulsivo o generado por la presión social. Es importante hablar con honestidad y sin tabúes acerca del tema ya que muchos pueden no tener las precauciones necesarias al hacerlo.

La confianza entre ustedes siempre será la mejor herramienta de seguridad, les invitamos a visitar [nuestros módulos](#) para aprender más acerca de estos temas.



Microsoft



“Esenciales de Seguridad Digital”
es un proyecto creado para preadolescentes y adolescentes. Está enfocado
a temas de seguridad y civildad digital para que navegues seguro en Internet
y puedas ser un mejor ciudadano digital.

2020 Microsoft Corporation. Todos los derechos reservados.

Este documento se proporciona “tal cual.” La información y las opiniones expresadas en este documento, incluidas las URL
y otras referencias a sitios web de Internet, pueden cambiar sin previo aviso. Usted asume el riesgo de usarlo.

Este documento no le proporciona ningún derecho legal sobre ninguna propiedad intelectual en ningún producto de
Microsoft. Puede copiar y utilizar este documento para sus propósitos internos de referencia.