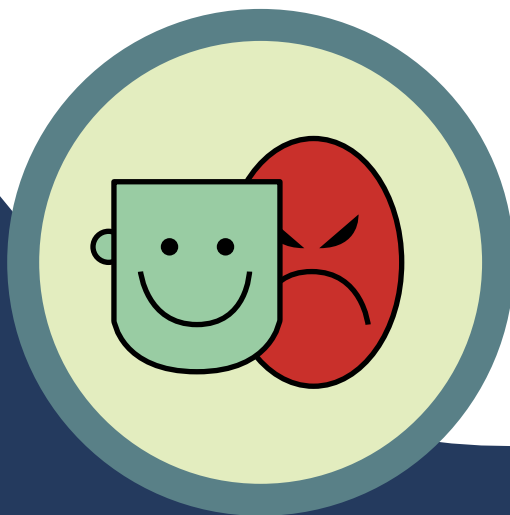


Esenciales de Seguridad Digital

¡Toma el control de tu vida en línea!





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 Ciudadanía 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.

2020

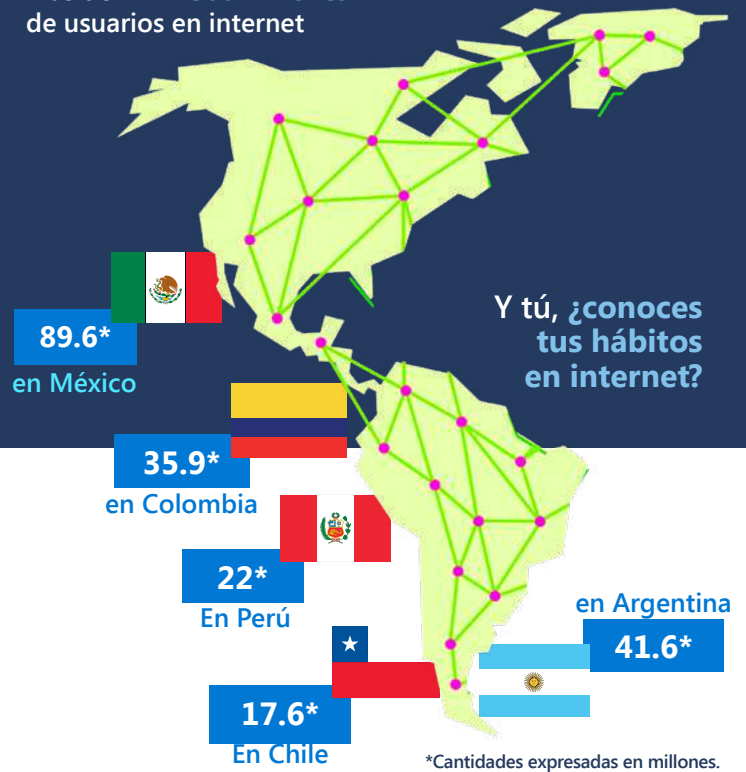
¿Qué hace tu generación en internet?

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?

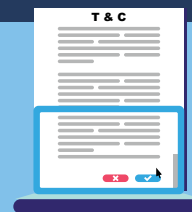
Protege tus datos

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.



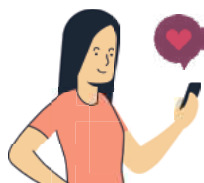
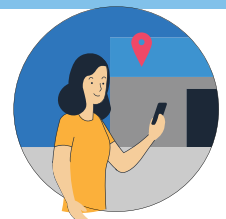
No aceptes términos y condiciones sin leerlos antes.



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.

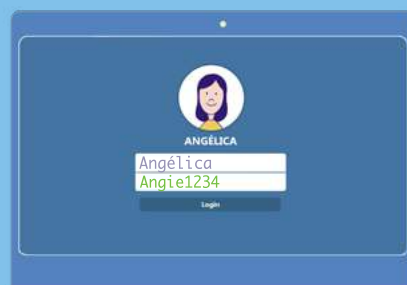
¿Crees que tus contraseñas son seguras? Conoce el caso de Angélica



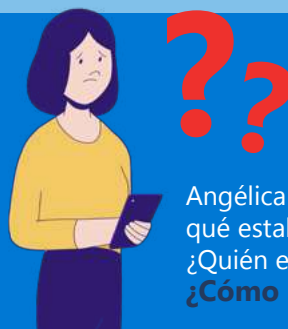
Angélica usaba una contraseña para todas sus cuentas, era una contraseña sencilla **con su nombre y números consecutivos**.



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.

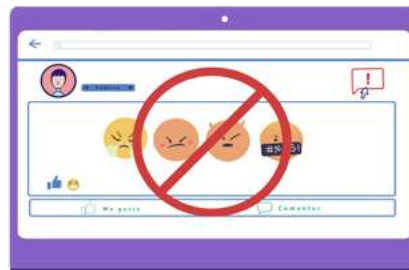
Por eso eres más vulnerable a fraudes y ciberacoso, ¿lo sabías?

¿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.

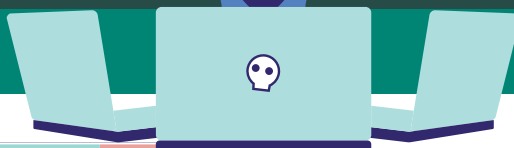


Los datos personales que compartes

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

¿Qué pueden hacer

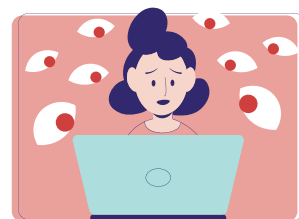
con estos datos?



Hacer compras online sin tu autorización.



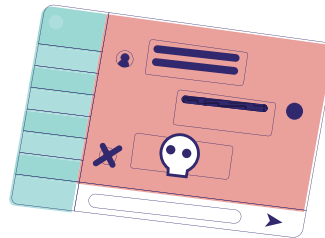
Acceder a tus dispositivos y ver tus fotos, apps y mensajes.



¿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.



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.



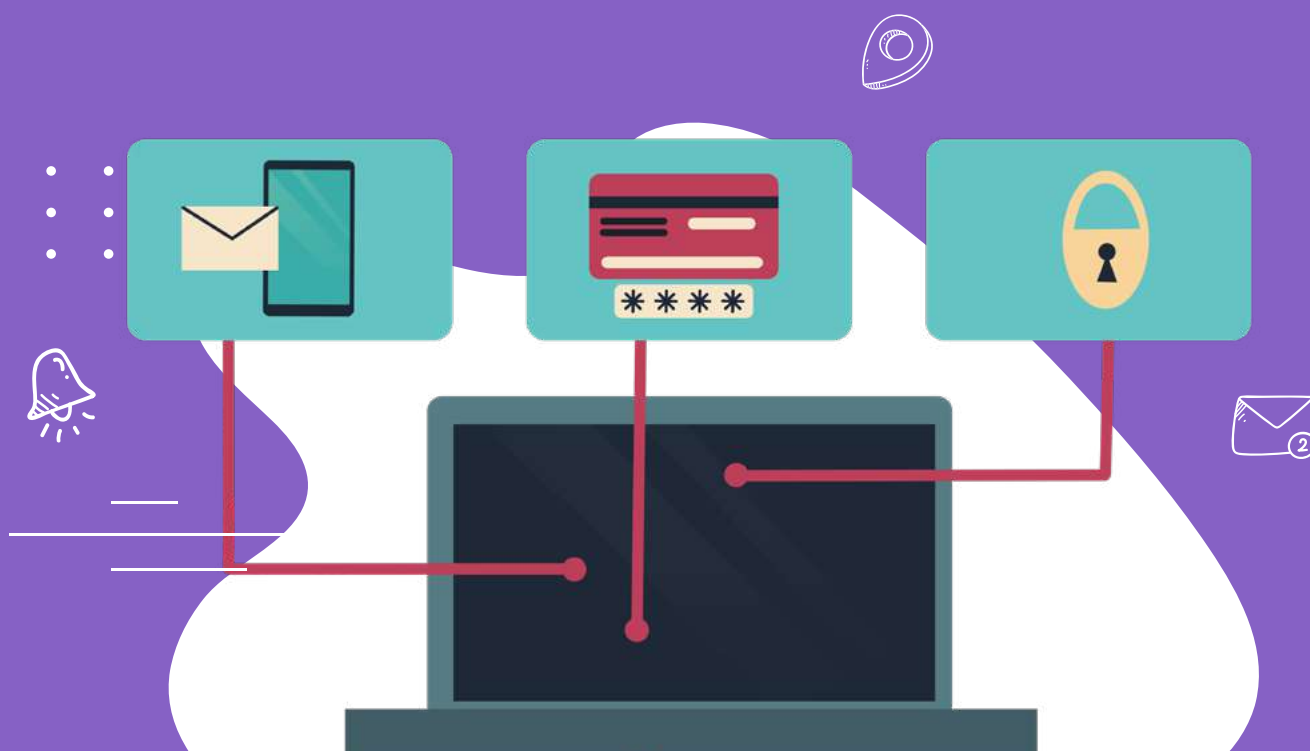
- 6 Cuando hagas **compras online,** acompáñate de un adulto de confianza.



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..."**

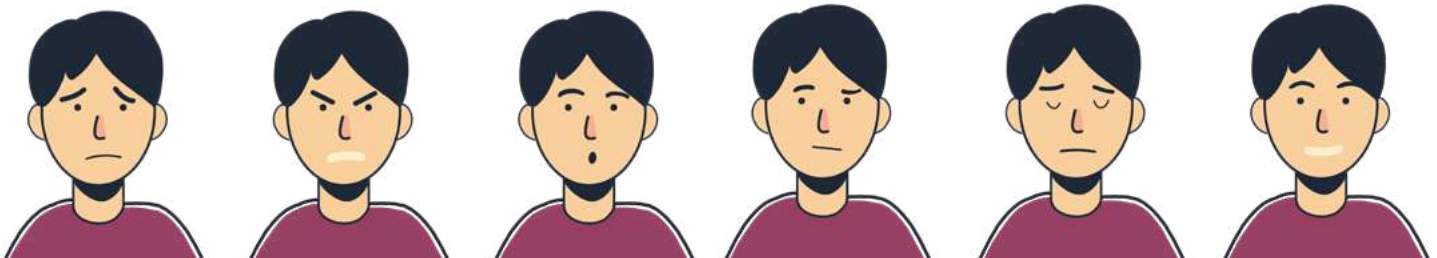


Haz preguntas

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?"



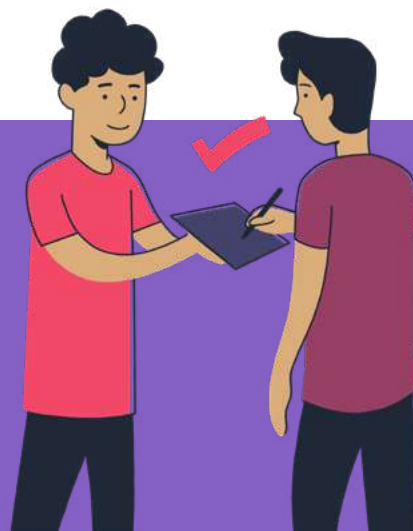
Responde a la idea, no a la persona

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. Respeta 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.

¿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](#)

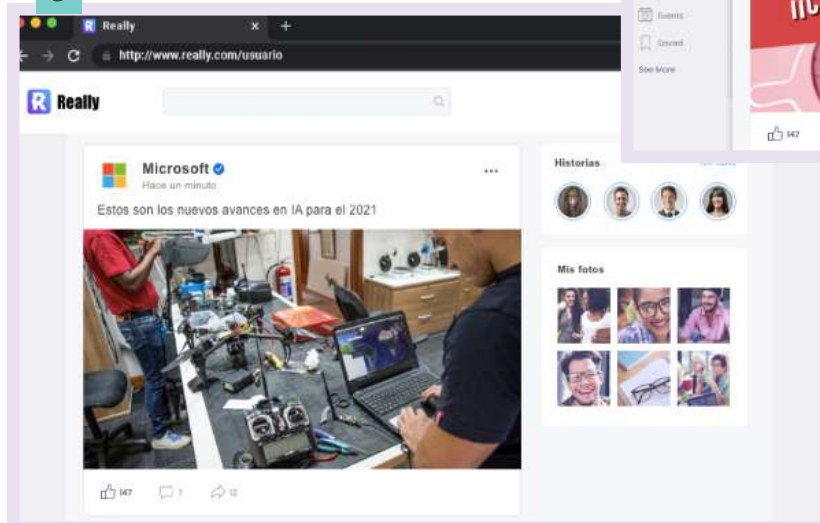
1



2



3





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.