



Aprende cómo detectar fraudes e información falsa en línea

MOVILIZATORIO

Conectando para el cambio

00 Meta

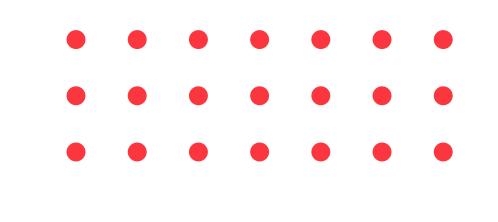
Soy 7% Digital



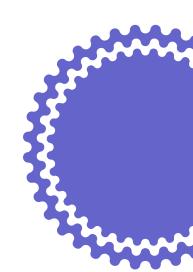
Indice

Pag
Cap. 1
¿La noticia que me mandaron por WhatsApp es verdad? ¿Cómo verificar información en internet y redes y por qué es importante?
Cap. 2
¿Cómo saber si tengo prejuicios al leer noticias? ¿Qué prejuicios tengo y cómo reconocerlos al revisar información en internet y redes?
Cap. 3
¿Cómo mejorar la seguridad de mis datos personales en internet? Anticípate a ataques de phishing, smishing, vishing y cómo actuar si recibes uno.
Cap. 4
¿Qué puede pasar con mi información personal en redes sociales? Mejores prácticas para tener el control de mi contenido en línea.





¿Qué vas a encontrar aquí y para qué te sirve?



¿Alguna vez has estado navegando por internet y te encuentras con una noticia que parece demasiado buena para ser verdad? Por ejemplo, imagina que estás en tu red social favorita y ves un titular que dice: "¡Descubre cómo volverte millonario en solo 3 pasos!" Todos sabemos que suena increíble, pero ¿es real?

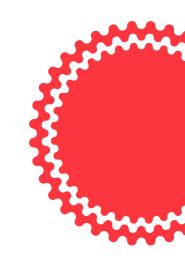
Esta guía te dará el conocimiento y las herramientas necesarias para responder esta y otras preguntas que te surjan al navegar por internet. En este mundo digital, la información es el recurso más valioso, por ello, es indispensable que conozcas las mejores estrategias para que tu experiencia en línea sea más segura.

El acceso masivo a información permite que estemos al tanto de eventos importantes alrededor del mundo, que conectemos con nuevas personas y negocios, que formemos un juicio más amplio. Sin embargo, este acceso también representa retos para discernir entre la información falsa y verdadera.

Esta guía te dará herramientas prácticas sobre cómo actuar en situaciones riesgosas en tu día a día.

¡Prepárate para aprender a detectar posibles fraudes de forma rápida y volverte un experto en seguridad digital! 🚀

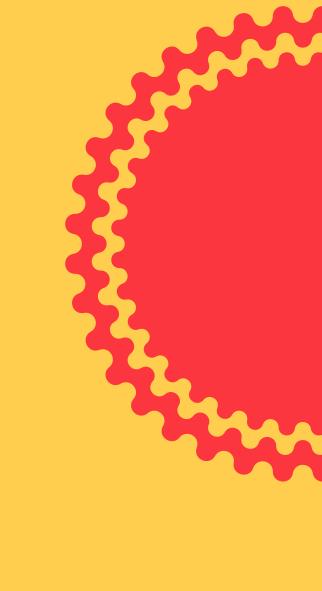
:VAMOS ALLÁ!







CAPÍTULO 17





¿La noticia que me mandaron por WhatsApp es verdad?

¿Cómo verificar información en internet y redes y por qué es importante?





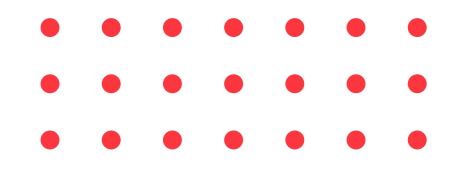
Dentro de tu recorrido por la red, te encontrarás con noticias parciales o falsas que tienen intereses específicos. Aprender a verificar información es clave para discernir entre el contenido verdadero y el falso, además de ayudarte a tomar decisiones más seguras.

Descubrir cómo hacerlo no solo te evitará malentendidos, sino que también te permitirá disfrutar de una experiencia en línea más positiva.

¡Exploremos juntos cómo navegar por este mundo digital de manera segura!







Inteligencia artificial y generación de contenido digital:

El desarrollo de nuevas tecnologías para crear y difundir información es una constante en la historia humana. Desde la invención de la escritura hasta las tecnologías de comunicación modernas, la humanidad ha ido refinando la forma en la conecta con otras personas.

Cada nueva tecnología representará nuevos desafíos. Por ejemplo, la inteligencia artificial, a pesar de que ya se ha venido utilizando desde hace años, hoy en día su acceso y uso se han democratizado lo que ha generado nuevos retos en el consumo y generación de contenido.

Ante ello, la organización Partnership on AI, ha venido trabajando de forma intersectorial para detectar y etiquetar contenido generado por IA, lo cual ayudará a reportar los contenidos que las personas generan a través de estas tecnologías.

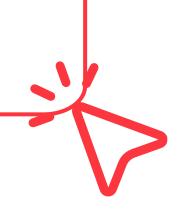
*Partnership on AI (PAI) es una asociación sin ánimo de lucro de organizaciones académicas, de la sociedad civil, de la industria y de los medios de comunicación que crea soluciones para que la IA avance hacia resultados positivos para las personas y la sociedad.

¿Qué debes hacer para comprobar si la información que te llega es verdadera?

Sigue los siguientes pasos:

NOTA

"La información falsa a menudo carece de detalles concretos o fuentes verificables."







Busca el origen de la noticia o información:

Para saber si una fuente de información es confiable, pregúntate: ¿La organización o la persona que publicó la información cuenta con credenciales académicas o profesionales que demuestren su experiencia en el tema?

Ten en cuenta que la forma en la que puede llegarte la información falsa puede variar. No siempre es por medio de un enlace a algún sitio, sino que también puede ser una imagen o un texto.

OJO: Si la información es sensacionalista o ataca a una persona en específico, ¡es probable que hayas recibido información falsa!

Revisa que haya un enlace a un sitio confiable, como el de un medio de comunicación reconocido, una organización gubernamental o instituciones educativas.

Analiza la evidencia:

Considera qué evidencia ofrece la noticia para probar lo que dice. Las fuentes primarias de información tienden a ser confiables ya que su contenido no ha sido tratado o analizado por otra persona, por ejemplo una entrevista a un testigo presencial de un acontecimiento.

Las fuentes secundarias recopilan o interpretan información de las fuentes primarias, por ejemplo, una noticia que se basó en esa entrevista. Las terciarias hacen referencia a información secundaria, como una enciclopedia cuya fuente es esa noticia. Tanto las secundarias como las terciarias pueden ser confiables pero están más alejadas de la información original.

Primaria	Secundaria	Terciaria
El video de una entrevista a una candidata presidencial	Una noticia sobre lo que dijo la candidata presidencial en la entrevista	Un artículo de enciclopedia sobre esa candidata, donde una de sus referencias sea la noticia de esa entrevista

Soy 7th Digital



Considera la fecha de publicación:

Revisa que la noticia sea reciente para que los datos presentados sean vigentes y relevantes, esto evitará que bases tus decisiones en información superada u obsoleta. Si es una imagen, busca al autor o el sitio en el que fue publicada.



Investiga si hay conflicto de intereses:

Identifica si la nota es tendenciosa y busca favorecer económica o políticamente a un individuo o grupo. Valora los artículos informativos que consideran a todas las y los actores involucrados y que exponen más de un solo ángulo de la historia.

Siempre verificar



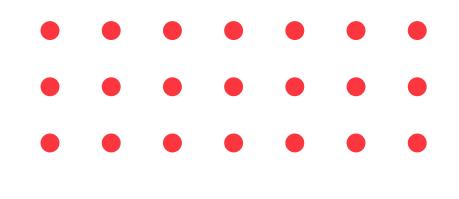
Revisa la fecha de la publicación

Contenido congruente y veraz

Busca y compara fuentes:

Aún si la información viene de una fuente en la que confías por su experiencia académica o profesional, es importante que compruebes siempre la información con fuentes secundarias. Busca contenidos a partir de una fuente primaria, por ejemplo, una noticia que hable sobre el testimonio del testigo presencial o bien una autoridad que en su discurso haga referencia al informe académico.





Diversas redes sociales y plataformas de mensajería cuentan con un sistema para verificar las cuentas oficiales de medios de comunicación y empresas. Procura buscar información de estas cuentas.

WhatsApp colabora con más de 50 verificadores de datos (Fact checkers) alrededor del mundo para garantizar que las personas tengan acceso a información precisa y puedan corroborar su veracidad. Si tienes duda si la noticia que te llegó es falsa da **CLICK AQUÍ** para encontrar al verificador de tu país y envíale la información para que la verifique.

Si aplicas estas recomendaciones podrás:

Tomar decisiones más informadas

Si verificas toda la información que te llega evitarás crear prejuicios, confusiones y pánico. La confianza de que cuentas con información verídica es fundamental para que tomes decisiones seguras.

Proteger a otras personas

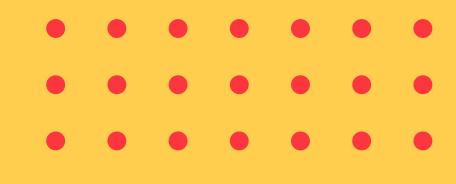
Recuerda que la desinformación comienza y termina al momento que decides no compartir una noticia cuya veracidad no has comprobado. Toma en cuenta que muchas personas no tienen acceso a las mismas herramientas educativas.

Mantener tu reputación y credibilidad

Al compartir solo información verificada, transmitirás confianza a tu comunidad.





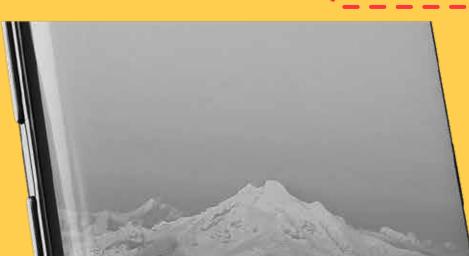


Pon a prueba tus conocimientos:

Recuerda que si no puedes confiar en la fuente que te suministra la noticia, lo mejor es hacer una búsqueda de noticias rápida y ver quién más la está difundiendo, además de apoyarte en fact checkers.

Busca la última noticia que te hayan compartido en alguna red social o plataforma de mensajería.





Con las herramientas que revisamos, analiza si hay alguna pista que te indique si es contenido original y si la fuente es confiable.

Busca al menos 3 fuentes de información adicionales que validen o contradigan la noticia que te llegó.



7/



Analiza la información que encontraste y reflexiona si cambió tu perspectiva de la noticia con base en la investigación que realizaste.

Si crees que la noticia es falsa verifícala enviándola a estos números por Whatsapp:





AFP Factual - México +52 (1) 55 2503 9334



Reuters Fact Check México +52 (1) 56 2001 8078

Recuerda que siempre es importante cuestionar a los medios y la procedencia de la información, así como corroborar su veracidad.

NOTA

"Las imágenes pueden ser sacadas de contexto para distorsionar la verdad."

Soy Tike Digital



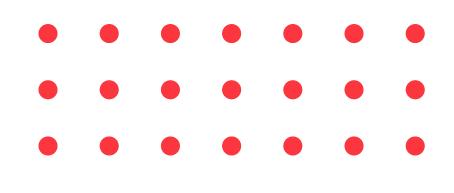
CAPÍTULO 2



¿Cómo saber si tengo prejuicios al leer noticias?

¿Qué prejuicios tengo y cómo reconocerlos al revisar información en internet y redes?





Un prejuicio es una predisposición irracional a adoptar comportamientos negativos hacia un grupo social y sus miembros, basados en una generalización errónea y rígida acerca de ellos.

La mayoría de las personas tenemos prejuicios conscientes o inconscientes. Es común que sin darnos cuenta repitamos las opiniones de personas cercanas sin reflexionar si en el fondo compartimos esa opinión.

Fuente: Consejo Nacional para Prevenir la Discriminación (CONAPRED)

¿Cómo darme cuenta de mis prejuicios y consolidar un punto de vista propio?

Sigue los siguientes pasos:

Reflexiona sobre tus creencias y experiencias:

Pregúntate cosas como: ¿Cómo surgió mi opinión ante este tema? ¿Dónde y de quién escuché una opinión similar? ¿Realmente pienso eso? ¿Qué otras perspectivas conozco del tema?

Busca diversidad de fuentes y compara opiniones:

Al cuestionar la información sobre algún tema, busca cuál es la fuente original.

Practica la objetividad y no sigas ciegamente la información que refuerce tus ideas. Busca alguna otra fuente de información que contradiga la postura que acabas de leer y compara sus argumentos. Esto te ayudará a crear una perspectiva más amplia y tener una visión equilibrada.

Desarrolla pensamiento crítico:

Investiga quién está detrás de la información que consumes y verifica posibles sesgos que tuviese el autor o autora. Examina los datos y hechos relacionados para generar tu propio criterio y sé consciente de los titulares exagerados o polarizados que reflejan prejuicios de algunos sectores de la población.



Practica la empatía:

Escucha y reflexiona ante diferentes puntos de vista. Siempre considera cómo las personas involucradas podrían verse afectadas por la noticia que compartes en redes sociales o servicios de mensajería.

Si aplicas estas recomendaciones, podrás:

Consolidar un punto de vista amplio y equilibrado



Te resultará mucho más fácil entender y convivir con personas de diferentes contextos y experiencias. Podrás aprender de ellas y fortalecer tus relaciones sociales.

✓ Fomentar una sociedad más diversa e inclusiva



Podrás enriquecer las perspectivas y experiencias de otras personas, fomentando un ambiente de respeto hacia las diferencias culturales, étnicas, de género y orientación sexual.

Impulsar la creatividad e innovación



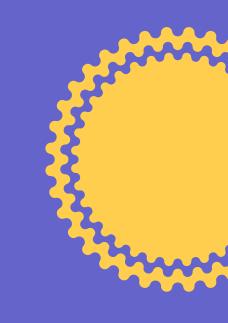
Todos tenemos algo que aportar, así que la apertura dará paso a generar soluciones más variadas y efectivas para tu desarrollo personal y profesional.





Pon en práctica tus conocimientos:

Observa y analiza las siguientes noticias:



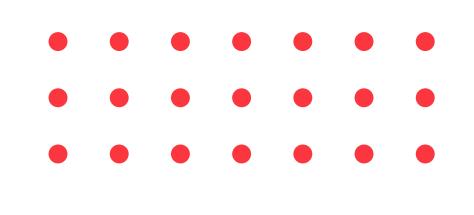




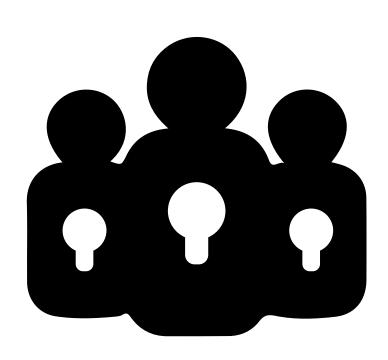


- Identifica cuáles podrían ser los prejuicios que contienen estas noticias.
- Propón un título diferente para cada imagen. El objetivo es que el titular y el contenido de la imagen sean lo más neutrales posibles sin caer en estereotipos y roles de género.









¿Cómo mejorar la seguridad de mis **datos personales** en internet?

Anticipate a ataques de **phishing, smishing** y cómo actuar si recibes uno





El phishing consiste en usurpar la identidad de una empresa u organización gubernamental para hacer llegar correos electrónicos con un enlace a una página aparentemente legal, que pide datos personales para después cometer algún tipo de fraude.

Dos variantes del phishing son el smishing y el vishing; en el primer caso se utilizan mensajes de texto SMS fraudulentos para obtener datos personales de la víctima y en el segundo, llamadas telefónicas o mensajes de voz.

Fuente: Consejo Nacional para Prevenir la Discriminación (CONAPRED)

Para evitar este tipo de abusos cibernéticos consulta más información para proteger tus cuentas de FACEBOOK, INSTAGRAM Y WHATSAPP.

¿Cómo darme cuenta que estoy frente a un ataque de phishing o smishing, y cómo hago para prevenir futuros robos de información?

Sigue los siguientes pasos:

Detente a analizar la situación antes de interactuar:

Busca comportamientos y/o indicios sospechosos antes de aceptar una solicitud de amistad o responder un mensaje. Si una persona afirma ser un amigo o un familiar en situación de emergencia, o te pide pagos adelantados para recibir préstamos, premios u otras ganancias, no interactúes con ella.

Reporta:

Si crees que encontraste una estafa es importante reportar en FACEBOOK, INSTAGRAM Y WHATSAPP.

Mantén tus dispositivos electrónicos actualizados:

Actualiza el sistema operativo de tus dispositivos y tus aplicaciones móviles de forma constante para que se instalen los parches de seguridad que las compañías crean para protegerte.





Siempre, es aconsejable que habilites las alertas sobre inicios de sesión no reconocidos para mejorar la seguridad de la cuenta, más información click aquí.



Evita descargar aplicaciones de sitios no oficiales o poco confiables:

Si vas a descargar alguna canción, video u archivo, usa tiendas de aplicaciones oficiales y evita hacer click sobre enlaces desconocidos.



Habilita la autenticación de dos pasos:

Agrega una capa extra de seguridad a las cuentas de las plataformas digitales que más utilizas. Con la verificación de dos pasos tu cuenta estará más protegida y será mucho más difícil que caiga en manos de malos actores. WhatsApp, por ejemplo, tiene diversos recursos que te pueden ser útiles. ¿Más información? DA CLICK AQUÍ.

Otras plataformas también cuentan con este tipo de verificación. Ruta para autentificar tu cuenta en dos pasos:







Protege tu conexión a internet en redes públicas y revisa correos detalladamente:

Utiliza una VPN* para cifrar tu conexión en redes Wi-Fi públicas y pon especial atención a los correos electrónicos y mensajes que parezcan sospechosos o soliciten información confidencial. Antes de compartir cualquier tipo de información personal verifica los remitentes y no hagas click en enlaces ni descargues archivos adjuntos de correos no solicitados o desconocidos.



Desconfía de los mensajes de personas desconocidas que te pidan dinero o te hagan ofertas poco comunes:

Algunas técnicas que usan las personas estafadoras son crear cuentas que se hacen pasar por personas que conoces y mandarte mensajes pidiéndote cosas inusuales, como pedirte dinero prestado, o bien, ofreciendo gangas y ofertas maravillosas que suenan poco creíbles. Antes de compartir más información verifica la identidad de esa persona, la existencia y fiabilidad del lugar desde donde te contactan.

Realiza estas acciones puntuales de prevención:



Cambia tus contraseñas:

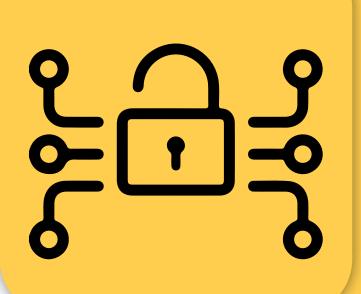
Cambia inmediatamente las contraseñas de cuentas comprometidas.

Consejos para crear contraseñas seguras: CLICK AQUÍ



Monitorea tus cuentas:

Mantente alerta de actividades inusuales y reporta cualquier cosa sospechosa.



Herramientas de seguridad:

Infórmate sobre las herramientas de seguridad y privacidad de las plataformas WhatsApp, Instagram, Facebook.

*Una red privada virtual o VPN es una conexión cifrada a internet desde un dispositivo a una red. La conexión cifrada ayuda a garantizar la transmisión segura de datos confidenciales. Evita que las personas no autorizadas espíen el tráfico y permite que el usuario trabaje de manera remota.

Fuente: CISCO Systems



Si aplicas estas recomendaciones, podrás:

Mantener tu información personal privada



Tu información sensible estará segura y será compartida sólo con personas de confianza.

Evitar ponerte en situaciones de riesgo



Podrás prevenir situaciones de vulnerabilidad, manteniendo el control de tu información en todo momento.

Procurar un entorno digital más seguro



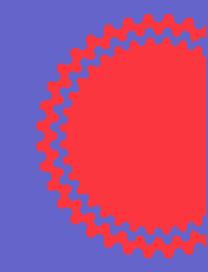
Podrás navegar con confianza y seguridad y sacar el máximo provecho de tus redes sociales favoritas.

NOTA

"¡Ojo a los mensajes de números que parecen sospechosos! Si tienes dudas, no los abras."



Es hora de actuar:

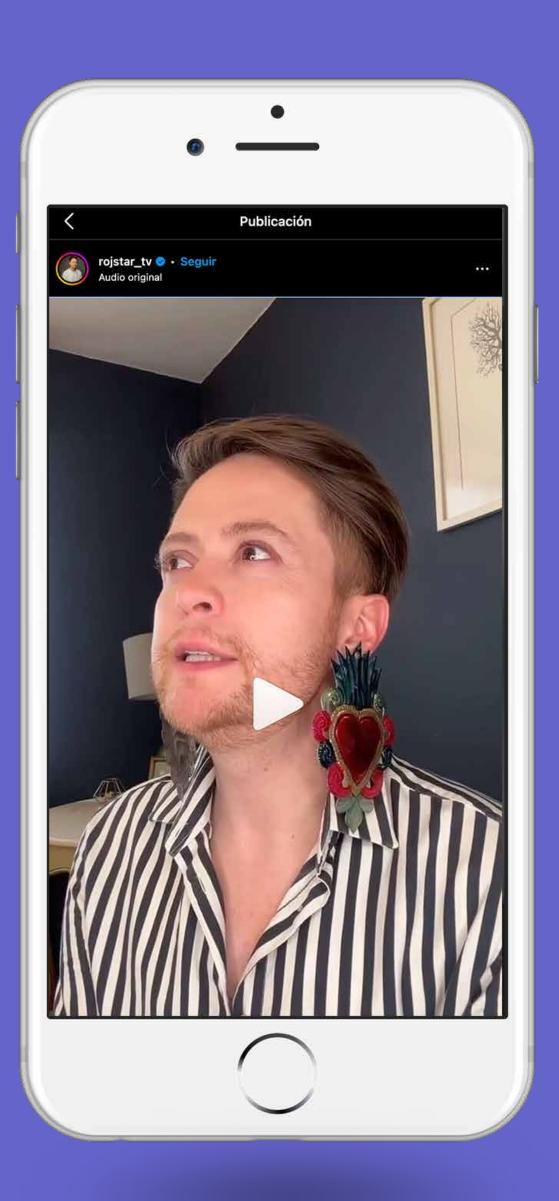


Te invitamos a realizar la revisión de seguridad en FACEBOOK, INSTAGRAM Y WHATSAPP.

Revisa los siguientes videos:

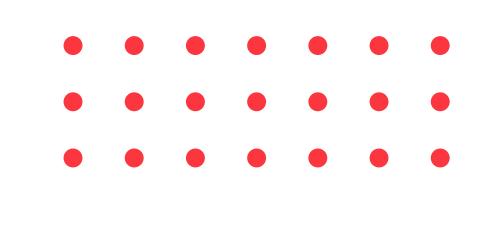


DA CLICK en la imagen para ver videos.

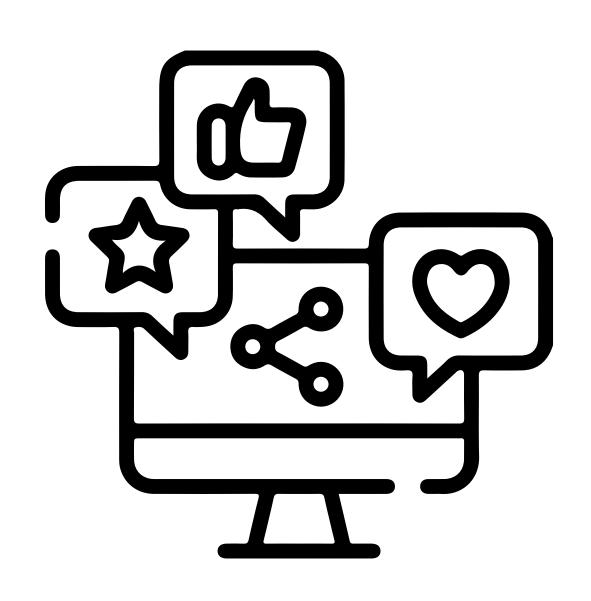


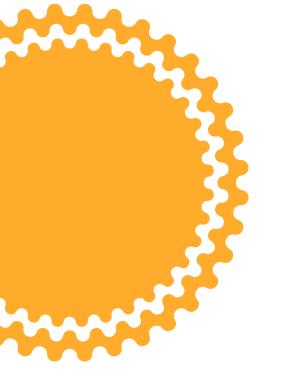
DA CLICK en la imagen para ver videos.







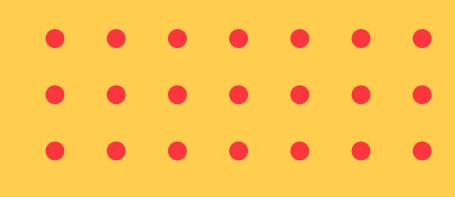




¿Qué puede pasar con mi información personal en redes sociales?

Mejores prácticas para tener el control de mi contenido en línea





Tus redes sociales te permiten conectarte con tus seres cercanos e interactuar con diferentes personas en todo el mundo; no obstante, te recomendamos que antes de compartir imágenes e información personal con otras personas, reflexiones sobre el tipo de uso que podrían darle a esa información.

SABÍAS QUE

¿Sabías que en los últimos años se ha incrementado el número de reportes de violencia digital en México?



Fuente: Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios. (INFOEM)

Existen diversos tipos de violencia digital, en México uno de los más comunes es la sextorsión.

La sexortisón es el uso de imágenes íntimas no consensuadas, es decir, el acto de compartir imágenes o videos íntimos de una persona, ya sea en línea o fuera de línea, sin su consentimiento.

Fuente: StopNCII.org, 2023

SABÍAS QUE

La violencia digital causa daños a la dignidad, la integridad y/o la seguridad de las víctimas?





Alejandra, una estudiante universitaria apasionada por la tecnología, entabló una amistad virtual que tomó un giro inesperado.

Después de 2 meses de conversar con su amigo virtual, ella le compartió un par de fotos personales íntimas. Sin preverlo, este individuo, comenzó a extorsionar a Alejandra, exigiendo dinero a cambio de no hacer públicas las imágenes.

Aunque inicialmente estaba abrumada por la situación, Alejandra decidió buscar ayuda. Reportó en redes sociales y se comunicó con las autoridades pertinentes. Con el apoyo adecuado, lograron capturar al responsable y poner fin a la extorsión.

Alejandra logró recuperar el control de su vida y se convirtió en una defensora de la conciencia digital, compartiendo su experiencia para educar a otras personas sobre los riesgos en el mundo digital.





¿Qué hago ante un caso de violencia digital hacia mi persona o hacia alguna persona cercana?

Sigue estos pasos:

Manten la calma:

No realices acciones impulsivas, pensar los siguientes pasos con sinceridad te ayudará a tomar mejores decisiones.

Repórtalo:

La mayoría de las plataformas tienen métodos para denunciar el acoso y la violencia digital. Denunciar contenidos es muy importante para que las plataformas puedan detectar estos comportamientos y eliminarlos. Como parte de las políticas de Meta puedes denunciar infracciones en cualquier momento.

O bien consulta cómo puedes denunciar aquí:



Instagram



Messenger



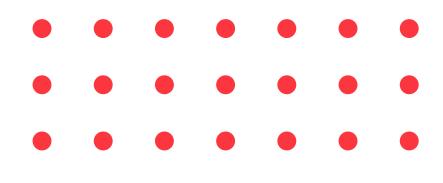
Facebook

Si alguien te amenaza con difundir imágenes o vídeos íntimos tienes herramientas para evitarlo. CLICK AQUÍ.

Pide ayuda, no estás sola(o):

Si estás siendo víctima de algún tipo de violencia digital busca ayuda de alguna persona cercana; puede ser un familiar, una persona con la que trabajes o estudies o a quien más confianza le tengas.





También existen plataformas que se dedican a acompañar a personas víctimas de sextorsión como Stop NCII.org (un proyecto que busca prevenir la difusión de imágenes y videos íntimos sin consentimiento) Si quieres más información CLICK AQUÍ.

A la par, Instagram y Facebook son miembros fundadores de Take It Down, una nueva plataforma del NCMEC para ayudar a evitar que las imágenes íntimas de los jóvenes se publiquen en línea en el futuro. Puedes ir a TakeItDown.NCMEC.org/es y seguir las instrucciones para presentar tu caso.

Conoce la guía de Cultivando Género A.C. sobre Resistencia digital entre amigas "En la red no navegas sola".

Bloquea a las personas que inciten a la violencia:

Reporta y bloquea a personas que insistan en usar contenido violento o compartan contenido ofensivo. Por ejemplo, en WhatsApp, se puede bloquear y reportar un contacto pulsando sobre su nombre y seleccionando la opción de bloquear contacto. Al bloquear a alguien, esa persona no podrá ver tu información ni tu perfil.

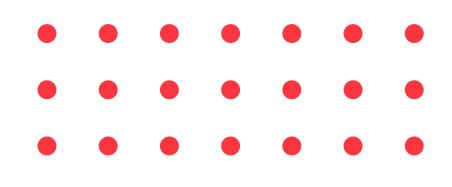
En Facebook también puedes limitar el acceso y búsqueda de tu perfil a través de la opción bloquear a un usuario y en Instagram existe la opción de filtrar los mensajes directos que puedan ser ofensivos. ¿Quieres saber más herramientas de seguridad? DA CLICK AQUÍ.

Puedes denunciar ante las autoridades:

Denunciar es una decisión personal. Pide ayuda a expertas(os) del Consejo Ciudadano quienes pueden brindarte atención jurídica y psicológica sin costo, 24/7 y la organización Sin Fronteras, recibe ayuda AQUÍ.

Si tienes más dudas o quieres hacer una denuncia, DA CLICK AQUÍ.

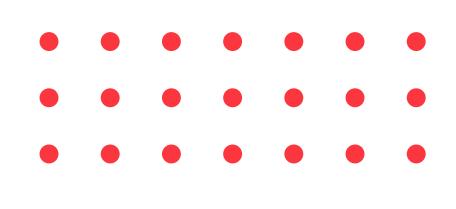




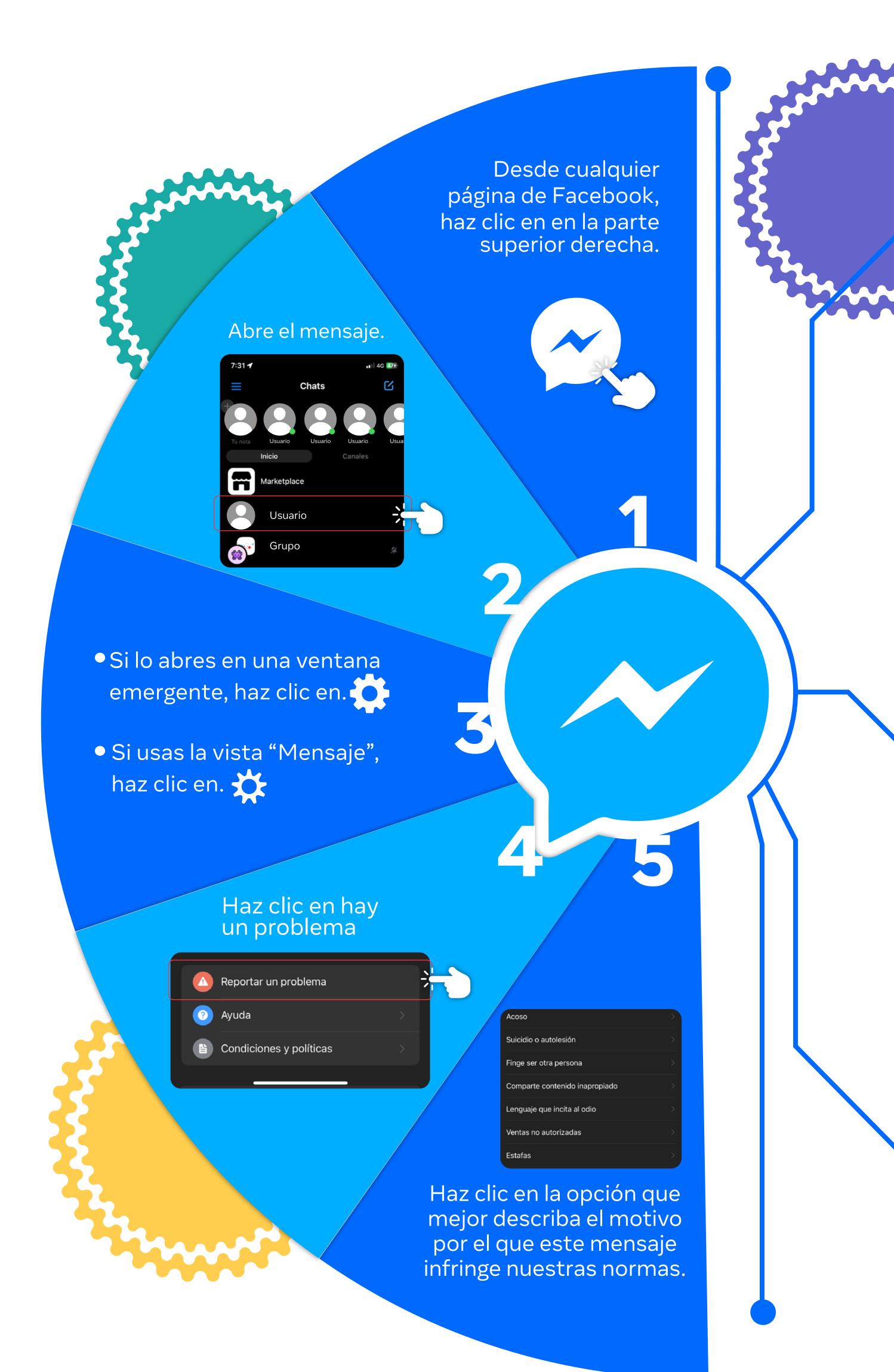
Reportar a un contacto en WhatsApp:



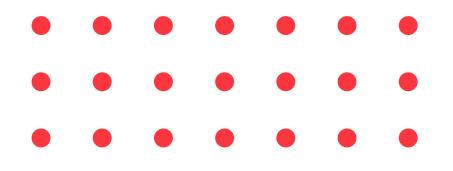




Reportar mensajes que infrinjan las Normas comunitarias en Messenger:



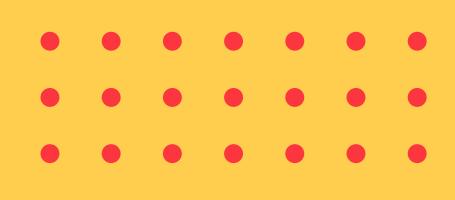




¿Cómo reporto un mensaje que recibí o cómo impido que alguien me envíe mensajes en Instagram?







Si aplicas estas recomendaciones, podrás:

Proteger tu información personal

Mantener el control de tu información personal e imágenes. Sabrás que hacer para mantener tu privacidad y seguridad en tus redes sociales favoritas, así como los pasos a seguir si eres víctima de sextorsión.

Saber cómo proceder ante abusos

Cuando alguien haga mal uso de tu información sabrás cómo actuar ante ello y podrás apoyarte de las plataformas y organizaciones que te acompañarán en tu proceso de reporte y denuncia.

Pon en práctica tus conocimientos.

Tu mejor amigo te envía una imagen de una compañera de trabajo que ambos conocen. En la imagen se puede ver que ella está cambiándose el uniforme en el baño de mujeres de tu oficina, se ve semidesnuda.

Con base en lo anterior contesta las siguientes preguntas:

¿Cuál sería la acción que seguirías una vez que te comparten la imagen a tu WhatsApp?

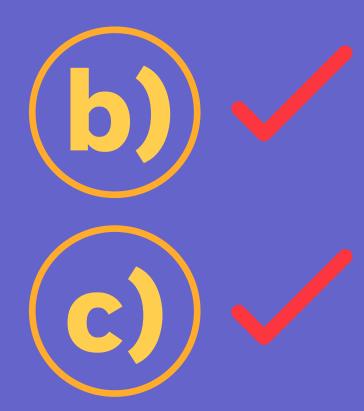
- a) La enviaría a un grupo que tengo con amigos donde compartimos fotos de nuestras ex parejas y amigas.
- b) Hablaría con mi amigo sobre cómo está dañando la integridad de la compañera al difundir ese contenido, además le mencionaría que está cometiendo un delito.
- c) Me reiría y le diría que me envíe más de esas fotografías.



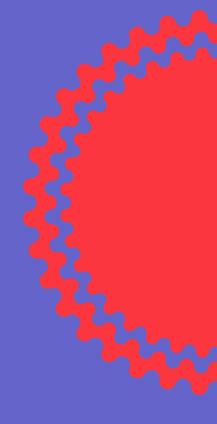


- ¿Cuáles podrían ser las consecuencias por compartir imágenes de tu compañera de trabajo sin su consentimiento?
 - a) Ninguna, ella no se va a enterar porque es algo que sólo se comparte entre hombres.
 - b)Pocas, ya que no la estamos usando para chantajear o extorsionar, sólo lo hacemos para divertirnos.
 - c) Muchas, ya que podría enojarse mucho y levantar cargos legales contra mi y mi amigo ya que en México existe una ley llamada Olimpia que castiga con penas de seis meses a tres años a quien difunda imágenes o audiovisuales íntimos de personas sin su consentimiento.

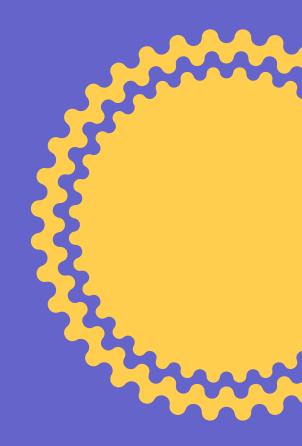
Opciones legales y éticamente correctas:



Las demás opciones son ilegales e incorrectas.







Navega con seguridad



Aprende cómo detectar fraudes e información falsa en línea



