

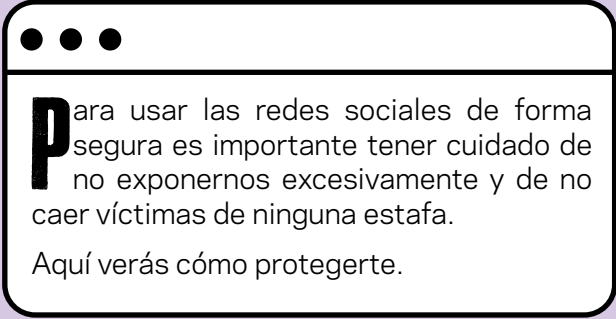
Redes sociales



Producción:

cert.br nic.br cgi.br

DISFRÚTALAS CON MODERACIÓN



Para usar las redes sociales de forma segura es importante tener cuidado de no exponernos excesivamente y de no caer víctimas de ninguna estafa.

Aquí verás cómo protegerte.

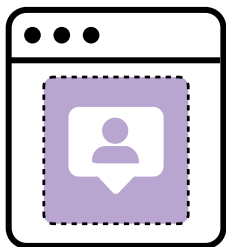
***CUIDADOS
BÁSICOS EN
LAS REDES
SOCIALES***



PIENSA BIEN ANTES DE PUBLICAR

En las redes sociales, la información se difunde rápidamente y, una vez que algo se publica, difícilmente se pueda borrar o controlar. Es posible que alguien ya lo haya copiado o compartido.

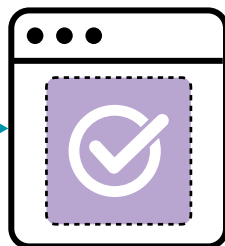
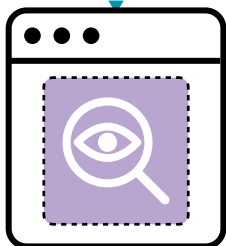
- » Recuerda: una vez publicado, queda publicado para siempre
- » Piensa que estás en un lugar público
 - cualquiera puede ver lo que publicas, tanto ahora como en el futuro



DEBES SER SELECTIVO AL ACEPTAR SEGUIDORES

Cuanto mayor sea tu red, mayor será la exposición de tus datos, publicaciones y listas de contactos. Esto aumenta el riesgo de que alguien abuse de esta información. Aceptar cualquier contacto les facilita el trabajo a las personas malintencionadas.

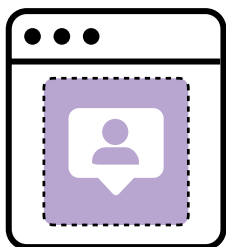
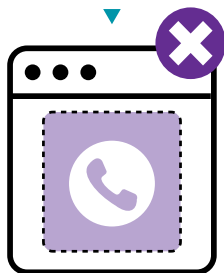
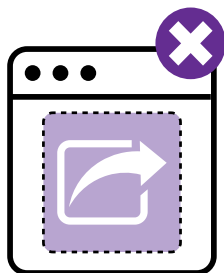
- » Siempre que sea posible, configura tu cuenta como privada
- » Verifica la identidad de la persona antes de aceptarla en tu red
 - bloquea las cuentas falsas

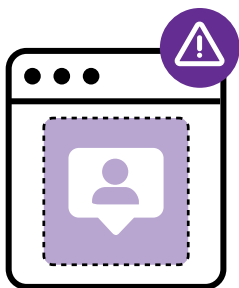


LIMITA LA INFORMACIÓN DE PERFIL QUE COMPARTES

Algunas redes sociales no permiten cuentas privadas y dan acceso público a tu información de perfil. Para controlar cómo se comparte esta información, puedes hacer algunos ajustes.

- » Evita compartir públicamente tu información personal
 - por ejemplo, tu número de teléfono
- » Configura el público objetivo de la información que compartes

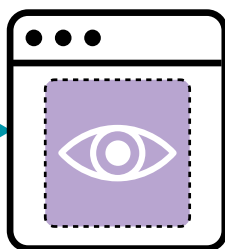
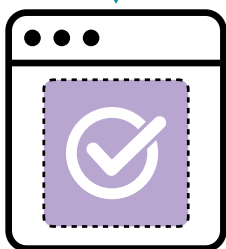
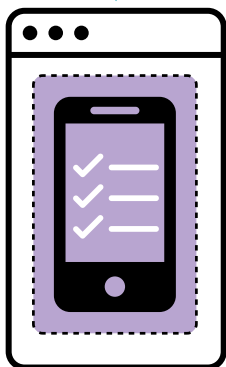




CONTROLA QUIÉN PUEDE VER TUS PUBLICACIONES

Tu red puede tener contactos de distintos tipos, algunos cercanos y otros no tanto. Puedes elegir compartir diferentes publicaciones con diferentes personas para así minimizar tu exposición.

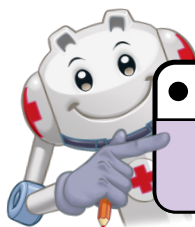
- » Selecciona el público objetivo de tus publicaciones
 - si la plataforma lo permite, crea listas personalizadas de contactos



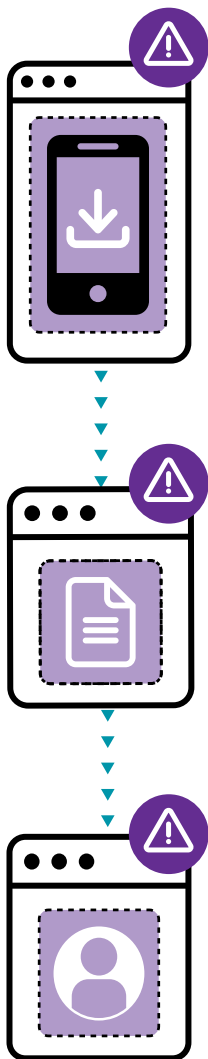
PROTEGE EL ACCESO A TUS CUENTAS

Las cuentas de las redes sociales son valiosas para los atacantes, que intentan invadirlas y usarlas para propagar *malware* y estafar a tu red de contactos. Se aprovechan de la confianza que existe entre los usuarios y de la velocidad con la que se propaga la información.

- » Crea contraseñas largas y activa la autenticación de dos pasos
- » Activa alertas y notificaciones en caso de cualquier intento de acceso a tus cuentas
 - presta especial atención a las cuentas que dan acceso a otras cuentas (las cuentas que usas como *login social*)
- » Si alguna de tus cuentas ha sido hackeada:
 - cambia la contraseña
 - de ser necesario, sigue los procedimientos para recuperar el acceso



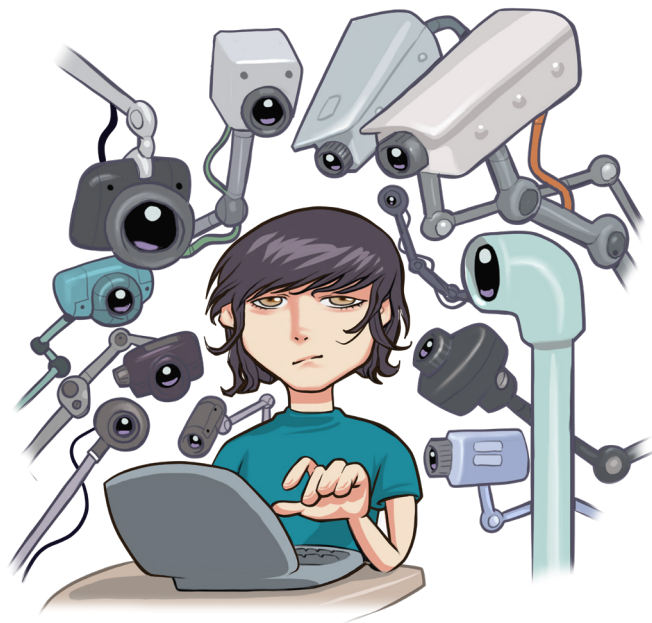
Puedes ver más consejos en el fascículo "Autenticación".



CUIDADO CON LAS APLICACIONES DE TERCEROS

Las aplicaciones de terceros — como los juegos, los tests de personalidad y los editores de imágenes— pueden capturar tu información personal, fotos, historial de navegación y lista de contactos para usos diversos y abusivos.

- » Piensa bien antes de permitir el acceso
 - lee los términos de uso y privacidad
- » Verifica periódicamente qué aplicaciones y sitios pueden acceder a tus cuentas
 - deshabilita los accesos que ya no utilices o que puedan ser maliciosos



AJUSTA LAS CONFIGURACIONES DE SEGURIDAD Y PRIVACIDAD

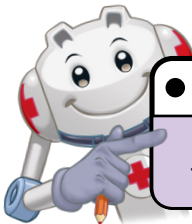
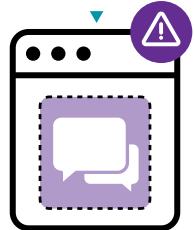
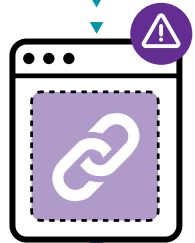
Las configuraciones de seguridad y privacidad de las plataformas ayudan a definir qué información personal se comparte y cómo se maneja esta información.

- » Configura tus redes sociales de forma que te sientas cómodo
 - intenta lograr un equilibrio entre la exposición, la seguridad y la privacidad

NO CREAS TODO LO QUE VES EN LA REDES SOCIALES

En las redes sociales circula información de todo tipo y origen, incluso información falsa y maliciosa. Creer ciegamente todo lo que recibes o cualquier información a la que accedes les facilita el trabajo a los atacantes.

- » Busca información en otras fuentes
- » Ten cuidado al hacer clic en los enlaces
 - incluso si vienen de gente que conoces
 - presta especial atención a los avisos patrocinados, ya que pueden ser maliciosos
- » Cuidado con los mensajes que recibes por chat



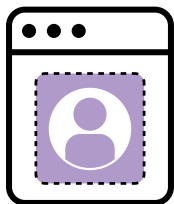
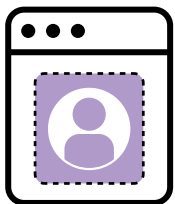
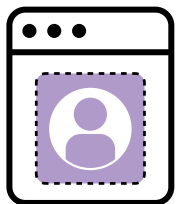
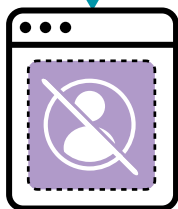
Puedes ver más consejos en el fascículo "Phishing y otras estafas".



DENUNCIA LOS CONTENIDOS MALICIOSOS Y LOS PERFILES FALSOS

Las denuncias permiten que las plataformas identifiquen cuentas falsas y contenidos inapropiados o maliciosos.

- » Usa las opciones para denunciar
- » Bloquea los contenidos o perfiles que te incomoden
- » Avisa a tus contactos si detectas cuentas falsas que se hacen pasar por ellos



***CUIDA TU
REPUTACIÓN
EN LÍNEA***



PROTEGE TU FUTURO PROFESIONAL

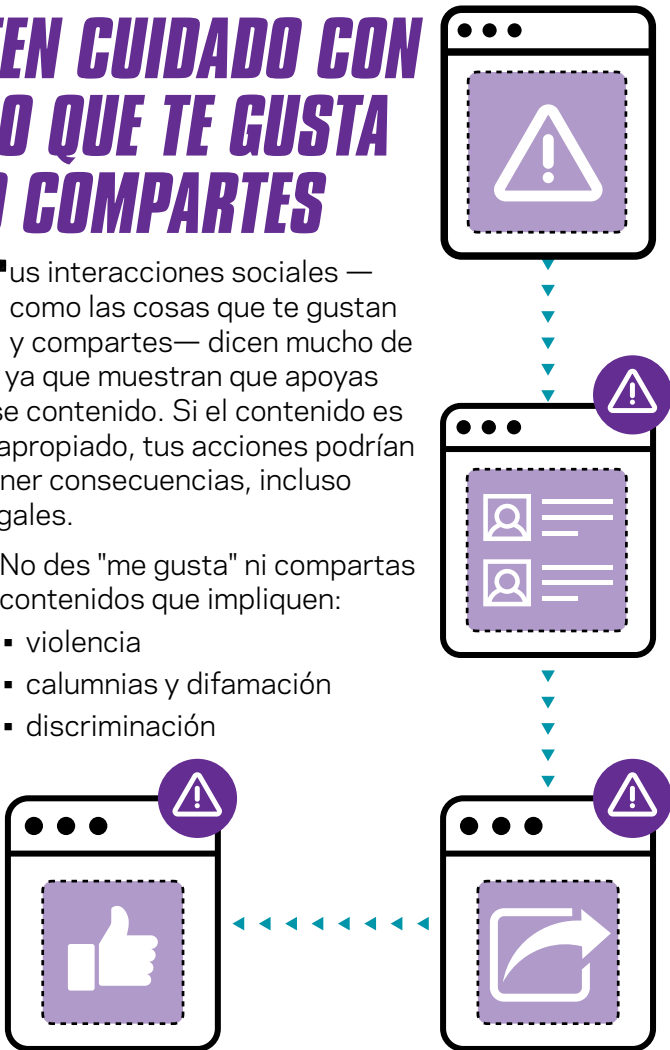
Las empresas y los reclutadores pueden usar la información publicada en las redes sociales para conocerte mejor.

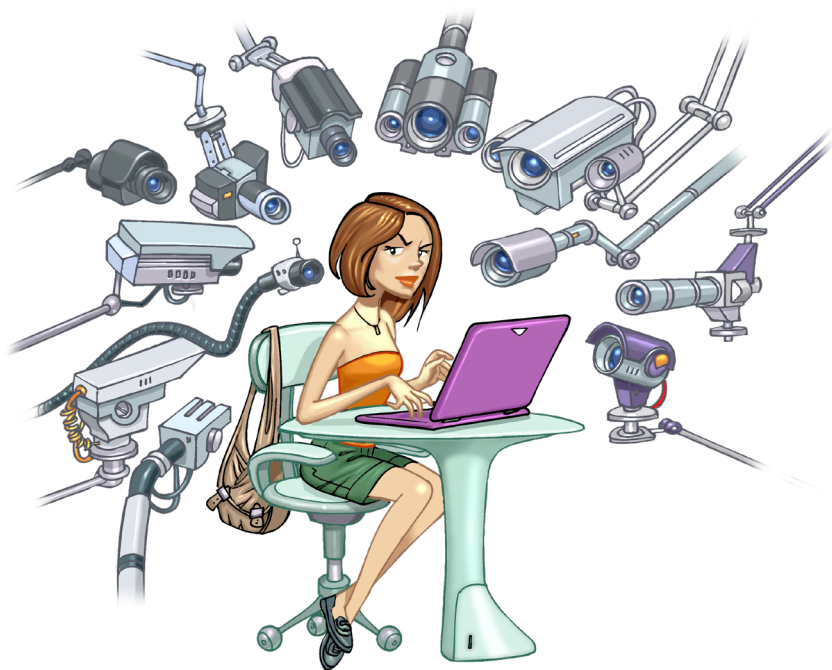
- » Evalúa si tus publicaciones pueden afectar tu imagen de forma negativa
- » Separa tus contactos en redes o listas específicas
 - publica contenido de acuerdo al público objetivo
- » Respeta la política de uso de redes sociales de tu empresa o de tu escuela

TEN CUIDADO CON LO QUE TE GUSTA O COMPARTES

Tus interacciones sociales — como las cosas que te gustan y compartes— dicen mucho de ti, ya que muestran que apoyas ese contenido. Si el contenido es inapropiado, tus acciones podrían tener consecuencias, incluso legales.

- » No des "me gusta" ni compartas contenidos que impliquen:
 - violencia
 - calumnias y difamación
 - discriminación





MANTENTE AL TANTO DE LO QUE PUBLICAN SOBRE TI

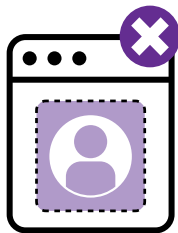
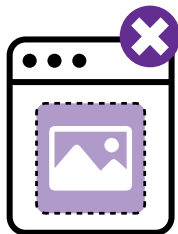
Otros usuarios te pueden etiquetar o mencionar en sus publicaciones y exponer tu privacidad. Si bien es imposible evitarlo, puedes optar por no incluir esas publicaciones en tu perfil.

- » Configura tus redes para que puedas revisar las publicaciones en las que estás etiquetado
 - si no te sientes cómodo, pídele a la persona que elimine la etiqueta o la publicación

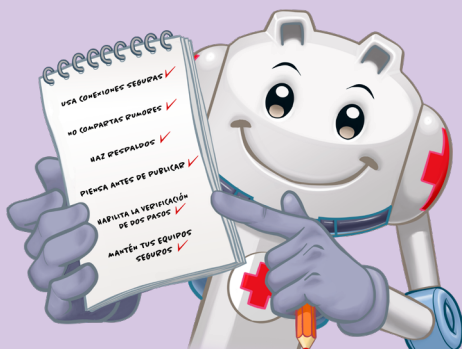
RESPETA LA PRIVACIDAD AJENA

A algunas personas no les gusta exponer su privacidad en las redes sociales. Piensa cómo te sentirías si te hicieran lo mismo.

- » Evita hablar de las acciones, los hábitos y las rutinas de otras personas
 - piensa cómo se sentirían si se hiciera público
- » Pide autorización antes de:
 - publicar imágenes en las que aparezcan otras personas
 - compartir publicaciones de otras personas



Si tienes hijos, encontrarás más consejos en la guía "Internet segura para tus hijos".



MÁS INFORMACIÓN

» Para obtener más información sobre este y otros asuntos relacionados con los cuidados que debes tener en Internet, consulta los demás Fascículos de la Cartilla de Seguridad para Internet, disponibles en:

<https://cartilla.cert.br/>

cert.br

CERT.br (<https://cert.br/>) es un Grupo de Respuesta a Incidentes de Seguridad (CSIRT) con jurisdicción nacional y de último recurso, mantenido por NIC.br. Además de la gestión de incidentes, también trabaja en la sensibilización en temas de seguridad, conciencia situacional y transferencia de conocimiento, siempre respaldado por una fuerte integración con las comunidades de los CSIRT nacionales e internacionales.

nic.br

El Núcleo de Información y Coordinación del Punto BR - NIC.br (<https://nic.br/>) es una entidad civil de derecho privado y sin fines de lucro, encargada de la operación del dominio .br, así como de la asignación de números IP y del registro de Sistemas Autónomos en Brasil. Lleva adelante acciones y proyectos que benefician la infraestructura de Internet en Brasil.

cgi.br

El Comité Gestor de Internet en Brasil (<https://cgi.br/>) es responsable por el establecimiento de directrices estratégicas relacionadas con el uso y el desarrollo de Internet en Brasil. Coordina e integra todas las iniciativas de servicios de Internet en Brasil, promoviendo la calidad técnica, la innovación y la difusión de los servicios ofrecidos.