

GUÍA 2

¿CÓMO GUARDAR EVIDENCIA DIGITAL SIN PONERTE EN MÁS RIESGO?

Cuando vivimos violencia digital, es normal querer borrar mensajes, bloquear cuentas, cerrar perfiles o eliminar todo lo que nos recuerde lo que pasó. Esa reacción es comprensible. La violencia en línea puede generar miedo, enojo, vergüenza, ansiedad o cansancio.

Pero si es seguro hacerlo, guardar evidencia puede ayudarte a reportar en una plataforma, pedir apoyo, explicar lo ocurrido o presentar una denuncia ante autoridades.

UNICEF explica que el ciberacoso deja una “huella digital”; es decir, un registro que puede servir como prueba para ayudar a detener el abuso. Por eso, documentar lo ocurrido puede ser importante.

Sin embargo, guardar evidencia nunca debe ponerte en riesgo. La organización **Women’s Aid** advierte que, antes de recopilar evidencia, es importante pensar si hacerlo va a alertar a la persona agresora o aumentar el peligro. Tu seguridad siempre va primero.

Antes de empezar: pensá en tu seguridad

Antes de tomar capturas, descargar archivos o guardar conversaciones, pregúntate:

- ¿La persona agresora tiene acceso a mi teléfono, computadora o cuentas?
- ¿Revisa mis mensajes, fotos, galería, correo o nube?
- ¿Conoce mis contraseñas?
- ¿Puede ver mis notificaciones?
- ¿Tiene acceso físico a mis dispositivos?
- ¿Instaló alguna aplicación de monitoreo o rastreo?
- ¿Puede reaccionar con más violencia si nota que estoy guardando evidencia?

TechSafety Canada recomienda considerar siempre si capturar o conservar evidencia puede representar un riesgo para la seguridad de la persona afectada. Si hay riesgo, puede ser mejor pedir apoyo a alguien de confianza o a una organización especializada antes de actuar.

¿Qué formas pueden tomar las VGFT?

Las violencias digitales pueden manifestarse de muchas maneras. UNFPA, ONU Mujeres para América Latina y el Caribe y MESECVI/OEA han documentado distintas formas de violencia facilitada por tecnología, que pueden ir desde el acoso hasta la difusión no consentida de imágenes íntimas, la vigilancia, la suplantación de identidad, la explotación sexual, los ataques coordinados y otras formas de agresión digital.

Algunas de las más frecuentes pueden ser:

Acoso digital

Mensajes, comentarios, llamadas, etiquetas o interacciones insistentes, ofensivas, sexuales, intimidantes o humillantes. Puede ocurrir en público o en privado.

UNICEF describe el ciberacoso como un comportamiento que se repite y que busca atemorizar o humillar a otras personas mediante tecnologías digitales.

Amenazas

Mensajes o publicaciones que anuncian daño físico, sexual, emocional, económico o reputacional. También pueden incluir amenazas contra familiares, amistades, pareja, hijas, hijos o personas cercanas.

Difusión de imágenes íntimas sin consentimiento

Compartir, publicar, vender, enviar o amenazar con difundir fotos, videos, audios o capturas íntimas sin autorización de la persona que aparece en ellas.

UNFPA identifica la difusión no consentida de imágenes íntimas como una de las formas de violencia de género facilitada por tecnología porque puede utilizarse para controlar, humillar, extorsionar o castigar a una persona.

Sextorsión

Usar imágenes, conversaciones o información íntima para amenazar, manipular o exigir dinero, más imágenes, encuentros, silencio u otras acciones.

Suplantación de identidad

Crear cuentas falsas, usar fotos, nombre, datos personales o información de otra persona para hacerse pasar por ella, engañar a otras personas o dañar su reputación.

Doxing o exposición de datos personales

Publicar o compartir información privada, como dirección, teléfono, lugar de trabajo, ubicación, documentos, datos familiares o rutinas, con la intención de intimidar, exponer o poner en riesgo a alguien.

Vigilancia y control digital

Revisar teléfonos, exigir contraseñas, instalar aplicaciones de rastreo, monitorear ubicaciones, controlar redes sociales o leer conversaciones sin consentimiento.

UNFPA explica que la tecnología puede ser utilizada para perpetuar dinámicas de violencia tanto en relaciones de pareja como fuera de ellas. Esto incluye formas de control, monitoreo, vigilancia y abuso mediante herramientas digitales.

Acceso no autorizado a cuentas

Entrar a cuentas de correo, redes sociales, almacenamiento en la nube o mensajería sin permiso, cambiar contraseñas, borrar información o usar datos privados.

Qué guardar según el tipo de violencia

Si recibís amenazas, insultos o acoso por mensajes

Guardá:

- Capturas de la conversación completa.
- Nombre de usuario o número telefónico.
- Foto de perfil.
- Fecha y hora.
- Audios o notas de voz.
- Registro de llamadas, si hubo llamadas.
- Enlaces al perfil, si existen.

TechSafety.org recomienda tomar capturas de mensajes de texto porque los mensajes almacenados solo en un teléfono pueden borrarse accidentalmente o perderse si el dispositivo se queda sin espacio.

Si alguien publica información privada sobre vos

Esto puede incluir dirección, teléfono, lugar de trabajo, ubicación, documentos personales, rutinas o datos de familiares. Guardá:

- Captura de la publicación completa.
- URL o enlace directo.
- Nombre de usuario o perfil que publicó.
- Fecha y hora.
- Plataforma donde apareció.
- Comentarios o interacciones que aumenten el riesgo.
- Cualquier mensaje previo donde te amenazaran con publicar esos datos.

La guía de eSafety Commissioner recomienda recopilar la evidencia pronto, porque si una cuenta es bloqueada o el contenido desaparece, puede ser más difícil demostrar dónde y cuándo fue publicado.

Si hay difusión de imágenes íntimas sin consentimiento

Si alguien compartió o amenaza con compartir fotos, videos, audios o capturas íntimas sin tu

consentimiento, intentá guardar evidencia sin redistribuir el contenido. Guardá:

- URL o enlace donde aparece el contenido.
- Captura del sitio, perfil o publicación.
- Nombre de usuario de quien publicó.
- Fecha y hora.
- Mensajes donde la persona amenaza con difundir el material.
- Conversaciones donde se demuestre que no diste consentimiento.
- Reportes enviados a la plataforma.

TechSafety Canada explica que la distribución no consentida de imágenes íntimas ocurre cuando se comparte una imagen íntima sin consentimiento de la persona, especialmente cuando existía una expectativa de privacidad. **Importante: no reenvíes imágenes íntimas para “probar” lo que pasó. Compartirlas puede aumentar el daño y la exposición. Si necesitás apoyo, buscá una persona u organización de confianza que pueda orientarte sin pedirte redistribuir el material.**

Si alguien crea una cuenta falsa con tu nombre o fotos

Guardá:

- Capturas del perfil falso.
- URL del perfil.
- Nombre de usuario.
- Foto de perfil y portada.
- Publicaciones realizadas desde esa cuenta.
- Mensajes enviados desde esa cuenta, si los tenés.
- Comparación con tu cuenta real, si es necesario.
- Fecha y hora en que encontraste el perfil.

Si hay acceso no autorizado a tus cuentas

Esto puede pasar si alguien entra a tu correo, redes sociales, nube, WhatsApp Web, Telegram, Instagram, Facebook u otra plataforma sin permiso. Guardá:

- Correos de alerta de inicio de sesión.
- Correos de cambio de contraseña.
- Notificaciones de acceso desde otro dispositivo.
- Capturas de sesiones abiertas.
- Ubicaciones o dispositivos desconocidos.
- Cambios en datos de recuperación.
- Mensajes enviados desde tu cuenta sin tu autorización.
- Fecha y hora en que notaste el acceso.

Después de guardar lo necesario, cambiá contraseñas desde un dispositivo seguro, activá verificación en dos pasos y cerrá sesiones abiertas que no reconozcás.

Si la violencia ocurre en grupos, canales o chats colectivos

Guardá:

- Nombre del grupo o canal.
- Enlace de invitación, si existe.
- Capturas de los mensajes.
- Fecha y hora.
- Nombre de usuario de quien publicó.
- Administradores visibles, si aparecen.
- Reacciones o respuestas que amplifiquen la violencia.
- Número de participantes, si es visible.

¿Cómo hacer capturas útiles?

Cuando tomés capturas de pantalla, intentá que se vea:

- El contenido violento o amenazante.
- El nombre de usuario o número.
- La fecha.
- La hora.
- La plataforma.
- El enlace o URL, si es una página web.
- La conversación completa o suficiente contexto.
- La foto de perfil, si ayuda a identificar la cuenta.

La guía de [Luke's Place](#) recomienda que las capturas incluyan fecha, hora, dirección del sitio web, logo de la página u otros elementos que ayuden a mostrar el lugar en línea donde ocurrió la agresión.

Si una captura no muestra todo, podés hacer varias capturas en orden. También podés hacer una grabación de pantalla, especialmente si el contenido desaparece rápido, como historias, estados o publicaciones temporales.

¿Cómo ordenar la evidencia?

Guardar evidencia sin orden puede hacer que luego sea difícil entender qué pasó. Podés crear una carpeta segura y organizar los archivos por fecha.

Una forma sencilla puede ser nombrar los archivos así:

- 2026-05-28_Instagram_amenaza_usuario1
- 2026-05-28_WhatsApp_audio_numero
- 2026-05-29_TikTok_comentario_perfil
- 2026-05-30_Facebook_perfil-falso

[Women's Aid](#) recomienda que la evidencia se documente de forma sistemática, en orden y de manera segura. Esto puede ayudar a mostrar patrones de abuso a lo largo del tiempo.

¿Dónde guardar la evidencia?

La evidencia debe guardarse en un lugar seguro. No siempre el teléfono personal es el lugar más seguro, especialmente si la persona agresora tiene acceso físico o digital al dispositivo.

Podés considerar:

- Una carpeta protegida con contraseña.
- Una memoria USB guardada en un lugar seguro.
- Una cuenta de correo o nube a la que la persona agresora no tenga acceso.

- Enviar una copia a una persona de confianza.
- Guardar copias en más de un lugar seguro.
- Imprimir evidencia clave si es necesario y seguro.

No guardés evidencia en una cuenta compartida, en una nube familiar, en un dispositivo que la persona agresora revisa o en una galería donde pueda aparecer fácilmente.

¿Qué evitar?

Cuando estés guardando evidencia, evitá:

- Editar capturas.
- Recortar información importante.
- Borrar fechas, horas o usuarios.
- Reenviar imágenes íntimas.
- Responder impulsivamente si eso puede aumentar el riesgo.
- Guardar todo en un dispositivo que la persona agresora revisa.
- Publicar la evidencia en redes sociales si eso puede exponerte más.

- Confrontar a la persona agresora sin apoyo.
- Dependar únicamente de que la plataforma conserve el contenido.

Women's Aid advierte que la evidencia no debe ser editada o manipulada y que no se deben tomar pasos que puedan alertar a la persona agresora si eso aumenta el riesgo.

Antes de bloquear o reportar

Bloquear o reportar puede ser una medida necesaria para cortar el contacto o pedir que una plataforma revise el contenido. Pero antes de hacerlo, si es seguro, guardá evidencia.

Esto no significa que debás esperar si estás en peligro. Si necesitás bloquear para protegerte, hacelo. Tu seguridad es prioridad.

eSafety Commissioner advierte que, si bloqueás una cuenta o el contenido desaparece, puede perderse evidencia necesaria para mostrar dónde y cuándo ocurrió el abuso.

Si alguien más te ayuda a guardar evidencia

Podés pedir ayuda a una persona de confianza para que te acompañe, especialmente si revisar mensajes o imágenes te afecta emocionalmente.

Pero es importante que esa persona no comparta la evidencia, no la suba a redes y no la envíe a más personas. La evidencia debe manejarse con cuidado para evitar más exposición.

Esa persona puede ayudarte a:

- Tomar capturas.
- Ordenar archivos.
- Guardar enlaces.
- Hacer una línea de tiempo.
- Acompañarte a reportar.
- Acompañarte a denunciar.
- Recordarte que no es tu culpa.

Si sos periodista, activista o defensora

Si la violencia digital ocurre por tu trabajo público, activismo o participación política, también puede ser útil documentar si hay un patrón coordinado.

PENAmerica desarrolló un manual de campo sobre acoso en línea dirigido especialmente a personas que suelen estar desproporcionadamente expuestas a abuso digital, como escritoras, periodistas, artistas, activistas, mujeres, personas BIPOC y personas LGBTQIA+.

Guardá:

- Fechas en que empezaron los ataques.
- Publicaciones que detonaron la agresión.
- Cuentas que repiten los mismos mensajes.
- Hashtags usados para atacarte.
- Capturas de amenazas.
- Intentos de doxing.
- Reportes masivos contra tus cuentas.
- Mensajes que mencionen tu trabajo, identidad, género, orientación sexual o activismo.

En estos casos, puede ser útil que la documentación no sea solo individual, sino colectiva: una red, medio, colectiva u organización puede ayudar a registrar patrones, hacer reportes coordinados y activar protocolos de seguridad.



Nota de cuidado:

Esta guía ofrece información general y no sustituye asesoría legal, psicológica o acompañamiento especializado. Si estás en peligro inmediato, priorizá tu seguridad y buscá ayuda urgente.

Fuentes consultadas

- [UNICEF – Ciberacoso: qué es y cómo detenerlo](#)
- [eSafety Commissioner – How to collect evidence](#)
- [TechSafetyCanada – Preserving and Storing Evidence of TFGBV: Best Practices](#)
- [TechSafetyCanada – Image-Based Abuse and the Non-Consensual Distribution of Intimate Images](#)
- [TechSafety.org / NNEDV Safety Net – Documentation Tips for Survivors of Technology Abuse & Stalking](#)
- [Women's Aid – Cover your tracks online](#)
- [Luke's Place – 8 tips for tech abuse evidence for family court](#)
- [Access Now – Digital Security Helpline](#)
- [PEN America – Online Harassment Field Manual](#)