Límites digitales

Las fronteras entre lo público, lo privado y lo íntimo.

Tres conceptos clave

En los entornos digitales, los límites entre lo público, lo privado y lo íntimo cambian según el contexto, el público, la configuración de la plataforma y las decisiones de otras personas. Por eso no alcanza con saber si un espacio pide usuario y contraseña: también hay que conocer cómo se recopila, se usa y se comparte la información.

Lo público	Contenidos o espacios accesibles para mucha gente. Que algo sea público no significa que se pueda reutilizar sin límites ni que deje de estar protegido por normas de datos personales, derechos de autor u otros derechos.
Lo privado	Información o intercambios a los que solo acceden ciertas personas. Un chat, una cuenta cerrada o un archivo en la nube pueden ser privados, pero igual pueden copiarse, reenviarse o quedar expuestos por errores de configuración o accesos no autorizados.
Lo íntimo	La información más reservada de la esfera personal. Protegerla exige consentimiento, cuidado y respeto. Difundirla sin consentimiento causa daños y, según el caso, puede tener consecuencias legales.

Huella y reputación digital

La **huella digital** es el conjunto de datos y registros que generamos al usar servicios, dispositivos y plataformas. Incluye lo que publicamos a conciencia y también los datos que se producen al navegar o usar aplicaciones.

- **Persistencia y circulación:** borrar una publicación no siempre elimina sus copias, capturas o reenvíos. Pero no todo queda público para siempre: según el caso, podés pedir que se corrija, actualice o elimine.
- **Impacto concreto:** lo que hacemos en línea puede afectar nuestra privacidad, nuestra seguridad y nuestra reputación personal o profesional.

Cuando los límites se desdibujan

- **Hostigamiento en línea:** un contenido publicado o reenviado puede usarse para acosar, intimidar o perjudicar a otras personas.
- **Exposición y pérdida de control:** una mala configuración, una captura o un reenvío pueden ampliar el público de un contenido. Eso reduce el control sobre su circulación, pero no elimina tus derechos sobre tus datos.

Buenas prácticas

1. Revisá quién lo ve	Antes de publicar, verificá quiénes van a poder ver el contenido. Una cuenta privada reduce la exposición, pero no impide capturas ni reenvíos.
2. Protegé tus cuentas	Usá contraseñas largas, únicas y difíciles de adivinar. Un gestor de contraseñas puede ayudarte.
3. Activá el MFA	Habilitá la autenticación multifactor, sobre todo en el correo, los servicios financieros y las redes sociales. Elegí el método más seguro disponible y no apruebes solicitudes inesperadas.
4. Hacé una pausa	Antes de compartir, reenviar o publicar, no difundas datos, conversaciones ni imágenes de otras personas sin su autorización.

Proteger la privacidad no depende solo de cada persona: también influyen las plataformas, las medidas de seguridad y quienes reciben o comparten la información. Antes de publicar o reenviar, hacé una pausa, revisá quién lo va a ver y respetá la privacidad de los demás. Recomendación de **BA-CSIRT**.