4.

## CUIDA TUS OBJETOS DIGITALES DE VALOR

**Al igual que cuidas de los objetos valiosos en tu casa, recomendamos que hagas lo mismo con la información que guardas en internet** — ya sean tus papeles del banco, una copia de tu pasaporte o hasta tu dirección o número de teléfono, vale la pena pensar dónde almacenas tus datos personales más preciados y cómo los vas a resguardar.

Una **limpieza por encima** viene super bien para hacer algunas mejoras 'exprés'. Busca este tipo de información en tu buzón de correo o en tus cuentas y elimínala: copias de DNI, detalles bancarios, seguros de salud y cosas por el estilo. Si después te va a hacer falta, puedes descargarlo y hacer un respaldo digital o imprimirlo en físico antes de eliminarlo.

Una **limpieza más a fondo** es más exhaustiva y te recomendamos hacerla cada año. Respalda todo lo que quieres guardar de tus cuentas de correo y plataformas de redes sociales y bórralo de internet. **¡Un nuevo comienzo!**

**Consejo:** No solo elimines —¡vacía tu papelera y archivos temporales!

Es tu decisión si quieres respaldar tus archivos en "la nube" o guardarlos offline en un disco duro o USB. Independientemente de cómo hagas tu respaldo, asegúrate de no perderlo y utilizar una contraseña segura que recuerdes después.

5.

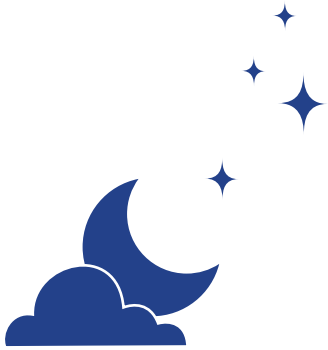
## PASA LA VOZ

Aunque puede ser fácil de olvidar, la red se llama "red" por algo. **Las personas estamos todas conectadas** a través de diferentes redes, no sólo como "amistades" en plataformas de redes sociales, sino a través de contactos de correo y las fotos que compartimos en internet.

Cuando aseguras tus cuentas, cuando usas contraseñas más fuertes y limpias tus datos, el beneficio no es solo para ti sino— **todas las personas con las que te conectas gracias a tu esfuerzo.**

Cuando estás haciendo limpieza en tus cuentas de correo y redes sociales, evalúa qué más puedes descargar y eliminar para **ayudar a cuidar la seguridad y privacidad de tus amistades y las personas con quienes trabajas**: los datos bancarios de tu hermana, el código clave para entrar en el edificio de tu oficina, la copia de pasaporte de tu hijo... son ejemplos de registros que pueden darte un dolor de cabeza si acaban en las manos equivocadas.

**¡Pasa la voz!** Mejorar tu seguridad digital puede ser tan sencillo como seguir unos cuantos pasos básicos. Comparte este Data Detox con tu gente y ayúdala a cambiar sus hábitos de la manera que tenga más sentido.



DATA DETOX KIT

## CAMBIA TU CONFIGURACIÓN

para asegurar tus datos

Si internet fuera un lugar donde solo compartes imágenes de perros disfrazados de dinosaurios, no serviría de mucho tener contraseñas. Sin embargo, en internet pagamos nuestros recibos, pedimos citas médicas y nos registramos para votar. Cuando te pones a pensar en todos tus "objetos digitales de valor" que se comparten por internet –y se almacenan en tu dispositivo–¿qué razón tendrías para no mantenerlos a salvo como si fueran tu monedero o llaves?

Hay una manera muy sencilla de ponérselo difícil a alguien que quiera acceder a tus objetos digitales de valor: no uses contraseñas fáciles de adivinar. La mayoría de las personas no necesitan habilidades técnicas especializadas para entrar en tus cuentas –pueden simplemente adivinar tus contraseñas o usar un programa automatizado.

Y una vez que entran en una de tus cuentas, pueden usar esa misma contraseña en tus otras cuentas y tomar control sobre ellas para obtener información sobre ti y tu estilo de vida, y hasta suplantar tu identidad en línea(hacerse pasar por ti).

Conforme vas siguiendo este Data Detox, aprenderás a tomar pasos prácticos para mejorar tu seguridad en línea.

¡Empezamos!

Un proyecto de TACTICAL TECH

Con el apoyo de Firefox

**datadetoxkit.org**
**#datadetox**

1.

## CIERRA TU PUERTA DIGITAL

Bloqueo de pantalla: la contraseña, el patrón, la huella o el identificador facial que utilizas para acceder a tu dispositivo es **tu mejor defensa** contra alguien que quiere meter sus narices en tu dispositivo. Pero hay muchas formas de acceso y te puede resultar difícil saber cuál te conviene más.

Tener cualquier tipo de **bloqueo** en tu móvil, tablet u ordenador te da mucha más protección que no tener nada. Y, al igual que todos los diferentes tipos de cerrojos que pueden tener tus puertas, **algunos bloqueos de pantalla son más robustos que otros.**

De todos los bloqueos, las contraseñas largas, nuevas y únicas (es decir, que sólo utilizas para una cosa) son las más seguras y fuertes. Esto implica que la contraseña incluya letras, números y caracteres especiales.

Digamos que hasta ahora, para desbloquear tu móvil solo pasas tu dedo (haces 'swipe'). Puedes mejorar tu seguridad poco a poco poniéndole una contraseña larga a tu móvil. O, si utilizas un patrón de bloqueo. ¿Por qué no lo haces más largo y complejo? ¿Tu PIN es 1234? ¿Por qué no usas un dado y lo tiras 7 veces para escoger un patrón aleatoriamente y te lo aprendes de memoria? **Un cambio pequeño puede ayudarte mucho a tener control sobre tu dispositivo.**

2.

## TÚ DECIDES QUIÉN ENTRA

Crear contraseñas de alto nivel es fácil. Solo tienes que seguir algunos principios básicos. Tus contraseñas deberían ser:

Largas: **un mínimo de 8 caracteres, mejor aún entre 16 y 20 caracteres.**

Únicas: **una contraseña diferente para cada página y cuenta.**

Aleatoria: **que no siga un patrón lógico o fácil de adivinar. Los gestores de contraseñas pueden ser útiles.**

Las contraseñas más robustas y seguras utilizan una combinación de letras, números y caracteres especiales. Este consejo valioso te ayuda a crear una contraseña más difícil de averiguar. A veces, la página o la herramienta no te deja usar caracteres especiales (como @#$%-=+). En estos casos, una combinación suficientemente larga de letras y números es, por lo menos, más segura que una contraseña corta.

Idealmente, te recomendamos usar tu propio **gestor de contraseñas** para generar y almacenar tus contraseñas. Un gestor de contraseñas es, básicamente, un programa cuyo propósito es proteger tus credenciales de acceso y otros datos sensibles. En el ámbito de la seguridad digital, se suelen recomendar opciones como 1Password y KeePassXC.

3.

## PON UNA SEGUNDA LLAVE

Configurar la autenticación de dos factores (2FA) o autenticación de múltiples factores (MFA) implica que si alguien encuentra tu contraseña, **seguramente no tenga los demás factores necesarios para acceder.**

Echa un vistazo a la configuración de seguridad de las páginas y apps que más utilizas para ver si aparece esta opción. Empieza con las más importantes y relevantes —apps de tu banco o tu correo con el que sueles recuperar acceso a tus otras cuentas.

Google:
**Inicia sesión en myaccount.google.com → Seguridad → Verificación en dos pasos → Comenzar**

Facebook:
**Menú → Configuración → Seguridad e inició de sesión → Usar autenticación en dos pasos**

**Consejo:** a la hora de escoger una capa adicional de verificación, necesitarás seleccionar una segunda vía para confirmar tu identidad. Evita usar mensajes de texto SMS porque puedes llegar a perder tu móvil. El correo electrónico suele ser una opción más fiable.