

GESTIÓN DE CONTRASEÑAS SEGURAS

Las contraseñas son la primera línea de defensa contra el acceso no autorizado. ¡Aprende a protegerlas!

1

USA CONTRASEÑAS FUERTES Y ÚNICAS

- **Mínimo 12 caracteres**, combinando mayúsculas, minúsculas, números y símbolos.
- **Evita usar nombres**, fechas o palabras comunes.
- **Crea frases fáciles de recordar**, pero difíciles de adivinar (ej.: iniciales de una frase personal).
- **Utiliza una contraseña distinta** para cada cuenta.



2

NO LAS GUARDES EN LUGARES INSEGUROS

- **Evita anotarlas en papel**, notas del celular o capturas de pantalla.
- **No confíes en el almacenamiento automático** del navegador.
- **Utiliza un gestor de contraseñas** confiable para mantenerlas seguras.



3

NUNCA LAS COMPARTAS

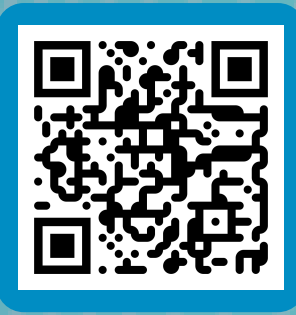
- **No proporciones tu contraseña por mensajes**, llamadas ni correos.
- **Los ciberdelincuentes** emplean técnicas de engaño (phishing).
- **Si alguna vez la compartiste**, cámbiala de inmediato.
- **Ni siquiera las personas de confianza** deben tener acceso a tus contraseñas.



4

REvisa SI HAN SIDO FILTRADAS

Ingresar a:



- **Verifica** si alguna de tus contraseñas ha sido comprometida.
- **Si lo ha sido**, cámbiala inmediatamente.



5

USA GESTORES DE CONTRASEÑAS

- **Almacena y genera contraseñas seguras** automáticamente.
- **Solo necesitas recordar una contraseña maestra.**
- **Activa el segundo factor** de autenticación en el gestor.
- **Algunas opciones recomendadas:** Bitwarden, 1Password, KeePass, LastPass.



6

PROMUEVE BUENAS PRÁCTICAS

- **Enseña a familiares, amigos y compañeros de trabajo.**
- **Revisen sus contraseñas juntos.**
- **Fomenta una cultura de seguridad digital** en tu entorno.



CONCLUSIÓN

"La seguridad comienza con una contraseña fuerte y única."