

BOLETÍN DIGITAL
N°026AGETIC
CONECTA

Una contraseña débil, compartida o filtrada puede abrir la puerta a fraudes, robo de información o suplantación de identidad. Desde AGETIC te compartimos recomendaciones clave para que gestiones tus contraseñas de forma segura y mantengas tu información protegida.

🌐 CONECTA CON NOSOTROS

📌 Más sobre este convenio y próximos proyectos:

🔗 www.agetic.gob.bo

📱 Síguenos:

📷 Instagram: @agetic_bolivia

🐦 Twitter: @agetic_bolivia

📘 Facebook: AGETIC Bolivia

**CIBERCONSEJOS: GESTIÓN
DE CONTRASEÑAS SEGURAS**

**Tus contraseñas son la
primera línea de defensa
para proteger tu identidad
digital.**

PRINCIPALES RIESGOS:

- Contraseñas débiles o repetidas pueden ser adivinadas en segundos.
- Guardar contraseñas en notas, navegadores o capturas facilita que sean robadas.
- Compartirlas expone tu información a usos no autorizados.
- Millones de contraseñas filtradas circulan en internet sin que sus dueños lo sepan.

TUS PRIMEROS PASOS HOY:

- Cambia tu contraseña más débil por una robusta (mínimo 12 caracteres, combinando letras, números y símbolos).

- Revisa si tus contraseñas han sido filtradas en plataformas como Have I Been Pwned.
- Instala y configura un gestor de contraseñas confiable.
- Activa la verificación en dos pasos (2FA) en todas tus cuentas.

CONSEJOS CLAVE

- Usa una contraseña diferente para cada cuenta.
- Nunca las compartas, ni siquiera con personas de confianza.
- No las guardes en notas, capturas o navegadores.
- Protege tus credenciales con gestores como Bitwarden, 1Password o KeePass.
- Promueve estos hábitos en tu familia, amigos y compañeros.



Seguridad comienza con una contraseña... pero no termina ahí. Mantén tus cuentas protegidas y fomenta una cultura de seguridad digital en tu entorno.