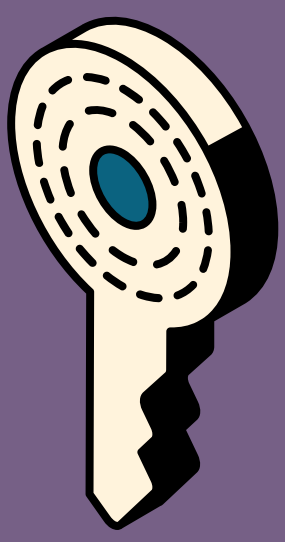
IEEG
INSTITUTO ELECTORAL
DEL ESTADO DE GUANAJUATO



MITOS Y REALIDADES
DE LA CIBERSEGURIDAD



01 "SOLO LAS GRANDES EMPRESAS SON ATACADAS"

- La realidad: Más del 40% de los ataques cibernéticos van dirigidos a pequeñas empresas, porque tienen defensas más débiles.
- Consejo práctico: Aplica medidas básicas de seguridad (antivirus, copias de seguridad, MFA), aunque tu organización sea pequeña.



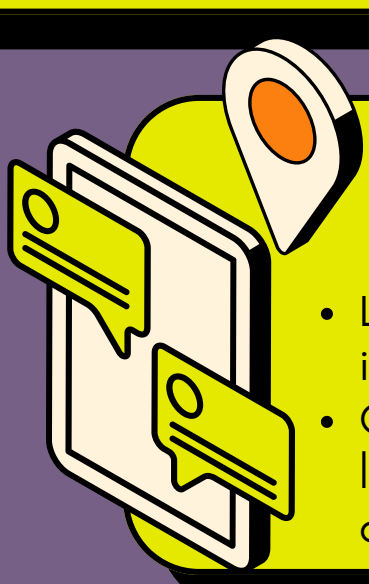
02 "UN ANTIVIRUS ES SUFICIENTE"

- La realidad: El antivirus solo cubre una parte; no previene phishing ni errores humanos.
- Consejo práctico: Mantente alerta con actualizaciones y señales de spam, no descargar archivos sospechosos, verificar remitentes y reportar correos extraños.

03 "LAS CONTRASEÑAS COMPLEJAS SON IMPOSIBLES DE HACKEAR"

- La realidad: Los hackers usan bases de datos filtradas y ataques de fuerza bruta. Si repites tu contraseña en varios sitios, estás en riesgo.
- Consejo práctico: Usa un gestor de contraseñas y activa autenticación multifactor (MFA).



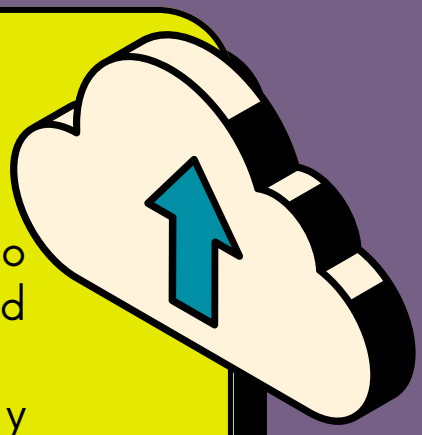


04 "SOLO LOS CRIMINALES O POLÍTICOS SON BLANCO DE HACKEOS"

- La realidad: Cualquiera puede ser víctima de robo de identidad, fraude bancario o ransomware.
- Consejo práctico: Desconfía de correos sospechosos, revisa la URL antes de hacer clic y protege tus cuentas con alertas de actividad.

05 "LA NUBE NO ES SEGURA"

- La realidad: Proveedores como Google, Microsoft o Amazon aplican cifrado y auditorías de seguridad constantes. El punto débil suele ser el usuario.
- Consejo práctico: Configura permisos correctamente y evita compartir enlaces sin control.



La verdadera fuerza de la ciberseguridad no está solo en la tecnología, sino en tus hábitos digitales. Tú eres la primera y más importante línea de defensa.