

# PROTEGE TUS CONTRASEÑAS

## FORTALEZCAMOS NUESTRA SEGURIDAD INFORMÁTICA

En el marco del fortalecimiento del Buen Gobierno Corporativo y alineados a nuestro valor de la excelencia en el servicio, el equipo de Gestión Integral de Riesgos nos invita a proteger nuestras contraseñas para evitar acciones fraudulentas.



Los ciberdelincuentes emplean, principalmente cuatro tipos de ataques.



### Ataque heylogger

La víctima instala el malware (software malicioso) en su equipo al hacer clic en un enlace o al descargar un archivo en internet. Una vez instalado el malware, el keylogger captura todas las publicaciones del teclado, incluyendo las contraseñas y se las envía a los ciberdelincuentes.



### Fuerza Bruta

Consiste en adivinar la contraseña a base de ensayo error. Los ciberdelincuentes prueban distintas combinaciones al azar, conjugando nombres, letras y números, hasta que dan con el patrón correcto.



### Ataques de diccionario

Un software se encarga, de manera automática, de intentar obtener la contraseña. Empiezan con letras simples, como "a", "AA" y de forma progresiva va probando con palabras más complejas.



### Phishing

Es la técnica más utilizada por los cibercriminales para robar contraseñas y nombres de usuario. Se engaña a la víctima para que complete un formulario fraudulento que suplanta a un servicio con sus credenciales de inicio de sesión.

## ¿CÓMO PROTEGER NUESTRAS CONTRASEÑAS?



**Emplea contraseñas complejas.** Utiliza más de ocho caracteres incluyendo mayúsculas, minúsculas, números y caracteres especiales.



**Utiliza contraseñas diferentes,** no uses la misma para todas tus cuentas.



**Cambia tus contraseñas con regularidad.**