# Recomendaciones para protección de contraseñas

**Si un usuario malicioso consigue apoderarse de la contraseña que da acceso a estos recursos, junto con violar nuestra privacidad, podría conocer y hacer uso indebido de valiosa información personal, como nuestros antecedentes financieros y datos sensibles, llegando incluso a suplantar nuestra identidad**.

**Cuanto más difícil y compleja sea la contraseña, menor será la probabilidad de que nuestra información personal sea objeto de una intrusión no deseada.**

A **continuación entregamos algunas recomendaciones básicas para proteger las contraseñas que utilizamos.**

## Recomendaciones para la protección de contraseñas:

- **No reveles ni compartas de ninguna forma tus contraseñas**. Son estrictamente personales e intransferibles. No las divulgues por teléfono, ni la anotes por correo electrónico, o a través de cualquier plataforma o red social, o de cualquier otra forma a nadie.

- **Presta atención cuando accedes a los servicios desde espacios públicos**. En este aspecto, existen programas que facilitan la interferencia de las plataformas y pueden almacenar las pulsaciones del teclado.

- **No utilices la opción de "guardar contraseña"** en el navegador, para no reintroducirla en cada conexión. Resulta fácil conseguir estas credenciales, ya que cualquier persona con acceso al ordenador podría consultar las contraseñas introducidas, en la configuración del navegador.

- **Mantén los sistemas operativos, softwares y aplicaciones actualizados,** para evitar la intromisión en los mismos, mediante ataques cibernéticos. Cada actualización incluye nuevas soluciones a las vulnerabilidades y no invertir el tiempo en instalarlas puede generar una puerta de entrada a diversos tipos de hackers.

- **Presta atención periódicamente a tus contraseñas,** esto es, cámbialas cada cierto tiempo. Esto cobra importancia en aquellos casos en que se intenta obtener tu contraseña bajo ataques de *"brute force"* (esto es, utilizando la técnica de ensayo y error, a través de un software que descifra claves empleando una sucesión de varias combinaciones de caracteres compuestos por dígitos, espacios y letras), ya que, al cambiarla, las combinaciones probadas por el ciberatacante quedan sin efecto.