AUTENTICACIÓN MULTIFACTOR (MFA)

¡ USA EL MÚLTIPLE FACTOR DE AUTENTICACIÓN PARA PROTEGER TU IDENTIDAD Y LA SEGURIDAD DE TUS DATOS !

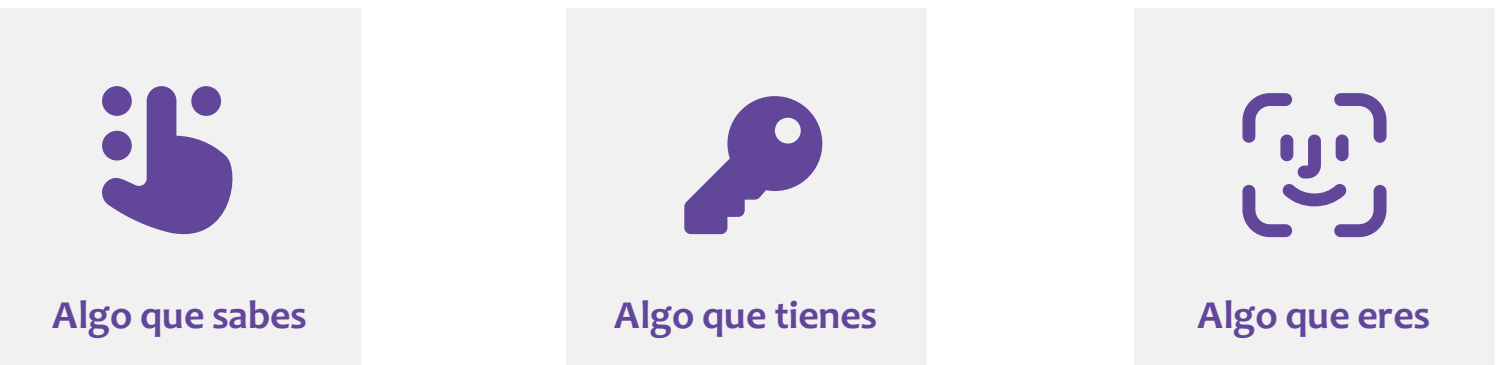
La **"Autenticación"** es el proceso de iniciar sesión en nuestras cuentas, esto se hace con un nombre de usuario y una contraseña. Desafortunadamente, ya no es una buena forma de hacerlo ya que suelen ser fáciles de descubrir.

Por esta razón, es posible que hayas escuchado lo que se denomina **"verificación en dos pasos"** o **"Autenticación Multifactor"**, una forma de acceso más seguro.

¿Qué es?

La autenticación multifactor (**MFA**) agrega una capa de protección al proceso de inicio de sesión. Cuando se accede a una cuenta o aplicación, los usuarios deben pasar por una verificación de identidad adicional.

Prácticamente consiste en solicitar dos o más de los métodos de autenticación. Los tres tipos más comunes de factores son los siguientes:



¿Cómo funciona?

Cuando inicias sesión en alguna de tus cuentas normalmente escribes tu nombre de usuario y contraseña, pero si tienes habilitada la Autenticación Multifactor; deberás ingresar tu nombre de usuario y contraseña como de costumbre y, después, te pedirá que escribas el segundo factor para comprobar tu identidad.

Por ejemplo: especificar un código que recibes en tu teléfono, correo electrónico o por un token.

Beneficios

Algunos de los beneficios de usar la autenticación multifactor son:

- Reduce la incidencia de robos de identidad y del acceso no autorizado a las cuentas personales.
- Mejora la respuesta de seguridad ante inconvenientes y ataques enviando un mensaje de alerta.
- Optimiza la protección de los datos durante las transacciones en línea.

PRÓXIMAMENTE

Los servicios asociados a tu cuenta Institucional contarán con esta característica.

¿Cómo debo prepararme?

Debes mantener estos datos actualizados: **Número de celular** y **correo electrónico alterno personal**.

Acércate al jefe de la Unidad de Informática de tu dependencia para realizar este proceso.