¿Por qué tengo que utilizar la Autentificación Multifactor (MFA)?

La Autenticación Multifactor es una medida de seguridad esencial que protege tu cuenta contra accesos no autorizados, añadiendo una capa adicional de verificación al iniciar sesión. Aunque utilices una contraseña robusta, esta puede verse comprometida mediante software maliciosos, filtraciones de datos en sitios web o técnicas de phishing.

Con MFA, incluso si alguien obtiene tu contraseña, no podrá acceder a tu cuenta sin el segundo factor de autentificación que solo tú posees.

En resumen, esta funcionalidad te brinda mayor seguridad y tranquilidad, ya que previene accesos no autorizados de tu cuenta. Es un proceso sencillo que toma solo unos minutos y refuerza significativamente la protección de tu información.

No tengo información confidencial en mi cuenta, ¿Por qué debería importarme la Autentificación Multifactor (MFA)?

Aunque creas que tu cuenta no contiene información sensible, los atacantes pueden utilizarla para enviar mensajes de phishing a otros usuarios (profesores, personal o estudiantes), comprometiendo sus dispositivos y accediendo a datos confidenciales.

¿Puedo optar por no participar en la Autentificación Multifactor (MFA)?

No. Todas las cuentas del ITESO deben tener al menos un segundo factor de autenticación activado.

¿Tengo que introducir el código de verificación cada vez que accedo a mi cuenta?

No necesariamente. La primera vez que ingresas a tu cuenta con MFA, te aparecerá la leyenda ***¿Quiere mantener la sesión iniciada?*** Puedes seleccionar la opción ***SI*** cuando accedas en un **dispositivo de confianza** para evitar ingresar el código en cada acceso.

Sin embargo, es posible que se te solicite con mayor frecuencia si utilizas una VPN, accedes desde varios dispositivos o borras con frecuencia la caché de tu navegador.

Recibí una Notificación de Microsoft Authenticator no solicitada, ¿Qué debo hacer?

Si no estás intentando iniciar sesión, selecciona **No, no soy yo** en la aplicación Microsoft Authenticator y cambia tu contraseña de inmediato en: https://password.iteso.mx

¿Necesito datos para usar el MFA?

Depende del método:

- Notificaciones de la app Microsoft Authenticator, si requieren conexión a internet.
- Códigos dinámicos generados por la app Microsoft Authenticator, no requieren conexión a internet.

No tengo teléfono, ¿qué puedo hacer?

La aplicación Microsoft Authenticator también puede instalarse en otros dispositivos móviles como iPads o tablets Android.

Puedo instalar Microsoft Authenticator en múltiples dispositivos

Sí, y es recomendable hacerlo para contar con una alternativa en caso de perder el acceso a tu dispositivo principal.

¿Qué debo de hacer si voy a cambiar de teléfono?

Deberás de seguir los siguientes pasos para registrar tu nuevo dispositivo y retirar al anterior.

1. Da de alta tu nuevo equipo en https://aka.ms/mfasetup (se te pedirá el código de tu aplicación Microsoft Authenticator de tu teléfono anterior).

2. Elimina tu dispositivo anterior en esa misma página.

3. Desinstala la aplicación Microsoft Authenticator de tu dispositivo viejo o reestablece el teléfono a valores de fábrica.

¿Qué debo de hacer si he extraviado o me han robado mi teléfono dónde tenía Microsoft Authenticator?

Debes reportarlo al equipo del ESI para que desactiven la aplicación en tu cuenta y para que te apoyen activando el MFA en otro dispositivo.

¿Qué datos recopila la aplicación Microsoft Authenticator?

Microsoft Authenticator recopila tres tipos de información:

1. Información de la cuenta que proporciona al momento de añadirla. Después de agregar la cuenta, según las características que habilite para la cuenta, es posible que los datos de la cuenta se sincronicen con la aplicación. Estos datos se almacenan en el dispositivo y se pueden remover quitando la cuenta.

2. Datos de uso no identificables personalmente, como detalles agregados sobre el éxito o el fracaso de operaciones importantes que se usan para detectar la disminución de la confiabilidad y los errores. Estos datos mínimos son necesarios para mantener la aplicación actualizada y segura. Debe aceptar el aviso de esta recopilación de datos cuando use la aplicación por primera vez.

También puede permitir el uso compartido de datos de uso no personales adicionales activando el botón de alternancia "Datos de uso" en la página Configuración de la aplicación o al usar la aplicación por primera vez. Estos datos permiten a nuestros ingenieros mejorar la aplicación de formas que son importantes para ti. Esta configuración se puede activar o desactivar en cualquier momento.

3. Datos de registro de diagnóstico que permanecen solo en la aplicación hasta que seleccionas Enviar comentarios en el menú superior de la aplicación para enviar registros a Microsoft. Estos registros pueden contener datos personales, como direcciones de correo electrónico, direcciones de servidor o direcciones IP. También pueden contener datos de dispositivo, como el nombre del dispositivo y la versión del sistema operativo. Los datos personales recopilados se limitan a la información necesaria para ayudar a solucionar problemas de las aplicaciones. Los ingenieros de Authenticator solo los usarán para solucionar problemas notificados por el cliente.