

## Preguntas frecuentes

### General

**P: ¿Qué está cambiando?**

R: El proceso de inicio de sesión en las aplicaciones de AIG requerirá ahora autenticación multifactor (MFA). Esto significa que cuando inicia sesión con su nombre de usuario y contraseña, también se le pedirá que verifique el inicio de sesión a través de un medio secundario de verificación de su elección (aplicación móvil, SMS o llamada telefónica). Este cambio se implementará en las aplicaciones con un enfoque por fases, por lo que puede notar actualizaciones de la interfaz de inicio de sesión en ondas dependiendo del número de aplicaciones de AIG a las que acceda.

**P: ¿Por qué está cambiando la experiencia de inicio de sesión?**

R: AIG está integrando un sistema de autenticación actualizado en la experiencia de inicio de sesión para mejorar la seguridad de sus cuentas en línea.

**P: ¿Qué métodos de MFA tengo a mi disposición?**

R: Las opciones de MFA compatibles incluyen la aplicación de autenticación móvil (actualmente, Okta Verify y Google Authenticator), la autenticación SMS o la autenticación de llamada de voz.

**P: ¿Qué opción de MFA recomienda AIG?**

R: Las opciones de MFA que se admiten a través de la solución Okta CIAM utilizada por AIG incluyen la aplicación de autenticación móvil (actualmente, Okta Verify y Google Authenticator), autenticación por SMS o autenticación de llamada de voz. AIG no recomienda ningún método de autenticación y los usuarios pueden seleccionar cualquiera de los métodos admitidos que se ajusten a sus necesidades. Tenga en cuenta que la mejor práctica para una conexión segura es utilizar una aplicación de autenticación en lugar de SMS o Autenticación de llamadas de voz. Para obtener más información sobre las mejores prácticas de MFA, haga clic [aquí](#).

**P: ¿Puedo utilizar una aplicación diferente para MFA distinta de Okta Verify o Google Authenticator?**

R: En este momento, Okta Verify y Google Authenticator son las dos aplicaciones de autenticación compatibles. Opcionalmente, puede seleccionar verificar la autenticación mediante un mensaje SMS o una llamada de voz.

**P: ¿Dónde puedo descargar las aplicaciones de autenticación móvil (Okta Verify, Google Authenticator)?**

R: Puede descargar cualquiera de las aplicaciones de autenticación móvil desde App Store (Apple) o Google Play Store (Android). Si decide utilizar el autenticador móvil Okta, asegúrese de descargar Okta Verify (no Okta Mobile).

**P: ¿Qué pasa si no tengo un teléfono inteligente (p. ej., tengo un teléfono móvil plegable)?**

R: Hay otras opciones de MFA disponibles, incluida la autenticación por SMS o la autenticación de llamadas de voz, que se pueden utilizar sin un teléfono inteligente.

**P: ¿Necesito descargar e instalar una aplicación para MFA?**

R: Solo es necesaria una descarga de software adicional si elige verificar mediante OKTA Verify o Google Authenticator. También puede optar por verificar mediante autenticación por SMS o autenticación de llamada de voz, que no requieren la instalación de una aplicación.

**P: ¿Cómo iniciaré sesión si mi teléfono móvil no funciona o no está disponible?**

R: Tendrá que utilizar una MFA para verificar su inicio de sesión cada vez. Póngase en contacto con el Servicio de asistencia técnica adecuado para restablecer el método MFA.

**P: ¿Tendré que autenticarme más de una vez si utilizo varias aplicaciones de AIG?**

R: No es necesario volver a autenticar si accede a otras aplicaciones que utilizan el mismo método de MFA. Una vez que se haya autenticado, puede obtener acceso a todas las aplicaciones.

**P: ¿Cambiará el proceso de MFA cuando venza mi contraseña?**

R: No. El método MFA no cambiará si la contraseña vence o se restablece.

**P: ¿El proceso de tiempo de espera de la aplicación será diferente?**

R: El tiempo de espera de la aplicación seguirá siendo el mismo; sin embargo, tendrá que volver a autenticar el inicio de sesión con la MFA cuando vuelva a iniciar sesión.

### Información específica de la aplicación

**P: ¿Qué es Okta?**

R: **Okta CIAM** es una solución de terceros utilizada por AIG para la autenticación de usuarios para acceder a varios sistemas y aplicaciones de AIG.

**Okta Verify** es una aplicación MFA proporcionada por Okta para proporcionar un segundo factor para iniciar sesión y establecer una mayor garantía para la protección de su cuenta. Para obtener más información acerca de Okta Verify.

**P: ¿Qué información personal recopila Okta?**

R: Para autenticar la identidad de un usuario, AIG utiliza la solución Okta CIAM que recopila y almacena el nombre, la dirección de correo electrónico, el número de teléfono, los identificadores telefónicos únicos y las direcciones IP de los usuarios. Esta información se almacena en un entorno en la nube Okta CIAM siempre que un usuario necesite acceder a una aplicación y que deba autenticarse para el acceso. Esto permite a los usuarios que inician sesión en varias aplicaciones de AIG que solo necesitan autenticar su inicio de sesión una vez para todas las aplicaciones durante una sesión. Para obtener información sobre las prácticas de privacidad de AIG, visite <https://www.aig.com/privacy-policy>.

Okta Verify es una aplicación independiente administrada por Okta que proporciona códigos que se pueden utilizar como segundo factor de autenticación para iniciar sesión en otros servicios.

**P: ¿Qué información personal se necesita para Okta Verify?**

R: Okta Verify puede recopilar información personal como parte del proceso de verificación. AIG no tiene acceso a la información personal recopilada por Okta Verify. Para obtener más información sobre la Política de privacidad de Okta, consulte <https://www.okta.com/privacy-policy/>.

**P: ¿Qué es Google Authenticator?**

R: Google Authenticator es una aplicación administrada por Google que proporciona códigos que se pueden utilizar como segundo factor de autenticación para iniciar sesión en otros servicios. Si configura la verificación de 2 pasos, puede utilizar la aplicación Google Authenticator para recibir códigos. Puede recibir códigos sin conexión a Internet ni servicio móvil.

**P: ¿Qué información personal recopila Google Authenticator?**

R: Google Authenticator puede recopilar información personal como parte del proceso de verificación. AIG no tiene acceso a la información personal recopilada por Google Authenticator. Para obtener más información sobre la Política de privacidad de Google, consulte <https://policies.google.com/privacy>.

**P: ¿Puedo descargar y activar Okta Verify o Google Authenticator en más de un dispositivo?**

R: Por el momento, Okta Verify solo se puede activar en un dispositivo. Se puede utilizar Google Authenticator en varios dispositivos. La aplicación Google Authenticator debe descargarse en todos los dispositivos que desee utilizar.

**P: ¿Okta Verify o Google Authenticator utilizan datos móviles o requieren almacenamiento adicional?**

R: Okta Verify utiliza datos mínimos, solamente unos pocos bytes. No requiere almacenamiento adicional. Google Authenticator no requiere conexión a Internet ni móvil y no requiere almacenamiento adicional.

**P: ¿Qué información personal se recopila si utilizo SMS o autenticación de voz?**

R: Si decide utilizar la autenticación por SMS o por voz, una aplicación de autenticación no recopilará ninguna información personal, pero se recopilará información personal limitada a través de la solución Okta CIAM para autenticar su identidad, incluidos el nombre, la dirección de correo electrónico, el número de teléfono, los identificadores telefónicos únicos y la dirección IP.