Universidad Interamericana de Puerto Rico

Oficina Central del Sistema

Centro de Informática y Telecomunicaciones

Multi-Factor Authentication (MFA)

Guía de usuario final

Tabla de Contenido

Introducción

Recientemente empresas e individuos han experimentado un aumento sustancial en la cantidad de ataques cibernéticos, intentos de fraude y robo de identidad. Ante este escenario, los Centros de Informática y Telecomunicaciones (CIT) del Sistema Universitario se encuentran en un proceso de revisión de sus políticas de acceso a los sistemas más críticos. Como parte de nuestros esfuerzos por fortalecer la protección del acceso a los datos y aplicaciones, hemos implementado el Multi-Factor Authentication (MFA) para Banner Administrativo, Autoservicios (Inter Web) y Blackboard.

¿Qué es Multi-Factor Authentication?

Multi-Factor Authentication o MFA, por sus siglas en inglés, es una técnica de seguridad que requiere al usuario, al menos, dos métodos de autenticación para verificar su identidad al momento de iniciar sesión en un sistema o al realizar transacciones. Su objetivo es crear una defensa en capas que dificulta el acceso de personas no autorizadas a los sistemas. Bajo este tipo de seguridad, una vez comprometido uno de los métodos de autenticación, el atacante debe enfrentar al menos una barrera adicional antes de lograr acceso no autorizado a un sistema. Para lograrlo el MFA combina dos o más credenciales independientes donde la primera parte es la contraseña que actualmente utilizamos, y la segunda parte puede ser un token de seguridad que se envía a su teléfono, teléfono móvil o a un correo electrónico.

Para implementar este nivel de seguridad hemos contratado la plataforma Okta. Este documento le ofrece las instrucciones básicas que le guiarán en el proceso definición de los factores de autenticación, así como en la manera en que se autenticará con cada uno de ellos. Incluye, además, un enlace a la lista de contactos disponibles para ofrecerles apoyo técnico en cada una de las Unidades del Sistema Universitario.

Configuración inicial del Multi-Factor Authentication (MFA)

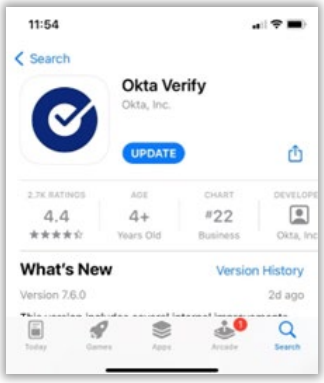
La plataforma Okta ofrece cinco alternativas de factores que pueden ser configurados y cuya descripción se muestra a continuación.

Okta Verify	Google Authenticator	Teléfono	Pregunta de Seguridad
• Aplicación que se descarga en el celular y que provee el código de validación requerido por Okta.	• Aplicación que se descarga en el celular y que provee el código de validación para ser utilizado en diversos sistemas de MFA.	• Envía un mensaje de texto que contiene el código de validación. • Realiza una llamada telefónica que dicta el código de validación.	• Puede seleccionar una de las preguntas definidas en Okta o definir una de su preferencia.

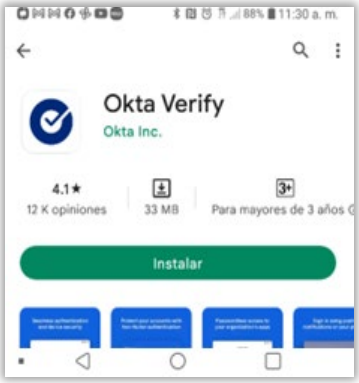
Cuando usted se autentica por primera vez, Okta le requerirá la activación de al menos uno de ellos. **Le recomendamos configure tantos factores como le sea posible, de acuerdo con los recursos tecnológicos que tenga disponible.** A continuación, se presenta cada uno de los factores disponibles.

Okta Verify

1. Utilizando un dispositivo móvil, descargue la aplicación Okta Verify desde Android Play Store o Apple App Store.



Apps Store

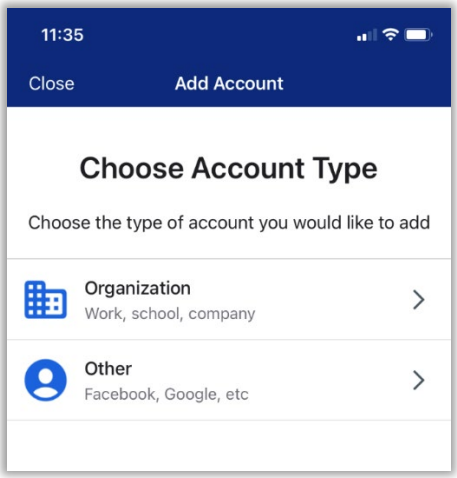


Play Store

2. Cuando utiliza Okta Verify por primera vez, se muestra una pantalla describiendo cómo funciona el Apps. Presione el botón titulado ***Next***.

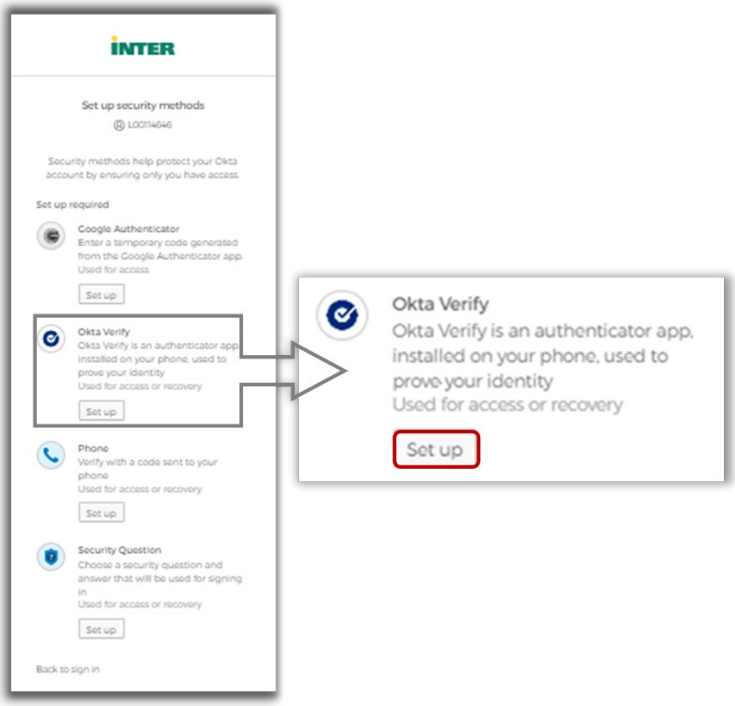
3. En la pantalla principal de Okta Verify, debe seleccionar la opción agregar cuenta, la cual, puede estar representada por el signo de **+**.

4. Elija el tipo de cuenta que desea agregar a Okta Verify. Para efectos de la Universidad Interamericana de Puerto Rico, debe seleccionarse la opción ***Organization***.



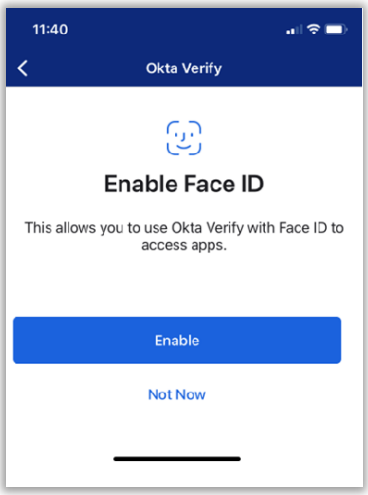
5. Okta Verify le requerirá leer el QR Code que Okta le presentará en la pantalla de la computadora.

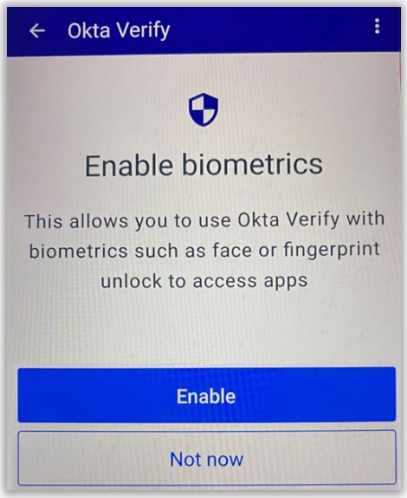
6. En el momento en que inicie sesión en la computadora, Okta le mostrará la lista de los factores de autenticación disponibles para ser activados. Presione el botón titulado ***Set up*** que aparece bajo la opción ***Okta Verify***.



7. Aparecerá en pantalla un QR Code que deberá leer con su dispositivo móvil utilizando la aplicación Okta Verify.
   a. En el dispositivo móvil vaya a Okta Verify y seleccione ***Yes, Ready to Scan*** y proceda a leer el código que tienen en la pantalla de la computadora. Es posible que previo a permitirle leer el código el dispositivo le requiera autorizar el uso de la cámara.

8. Okta Verify le dará opción de habilitar el Face ID en el caso de Apple o de habilitar la validación biométrica en el caso de Android.





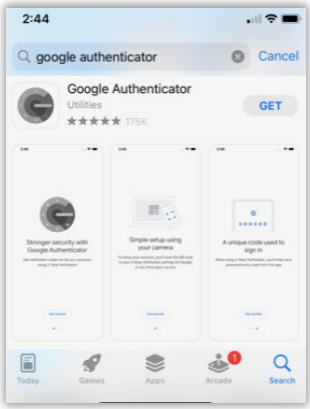
9. En el dispositivo aparecerá un mensaje confirmando la validación de la cuenta. Debe presionar el botón titulado ***Done***.

Notas:

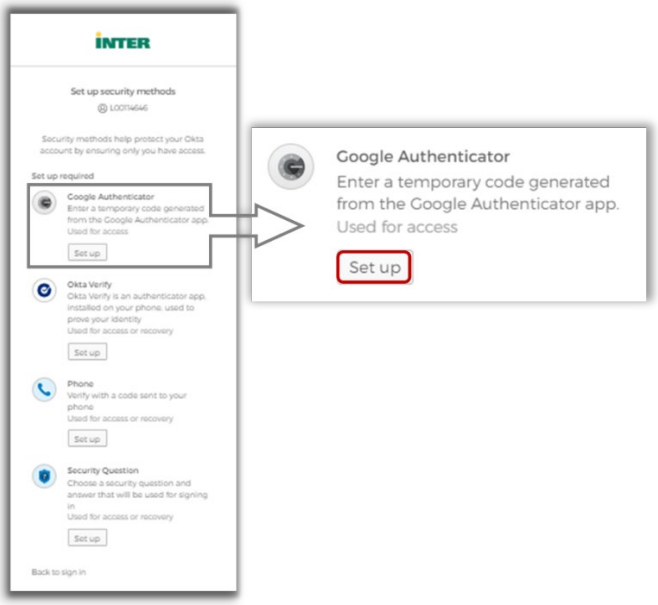
- Para información adicional sobre Okta Verify puede acceder al siguiente enlace: Okta Verify.
- Si un usuario obtiene un nuevo teléfono, debe configurar su cuenta Okta Verify nuevamente en el nuevo dispositivo.

Google Authenticator

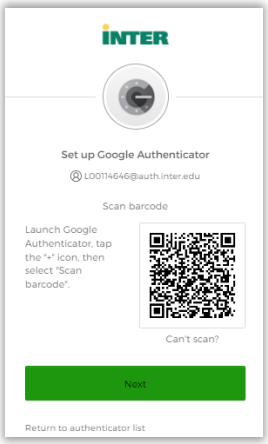
1. Utilizando un dispositivo móvil, descargue la aplicación Google Authenticator desde Android Play Store o Apple App Store.

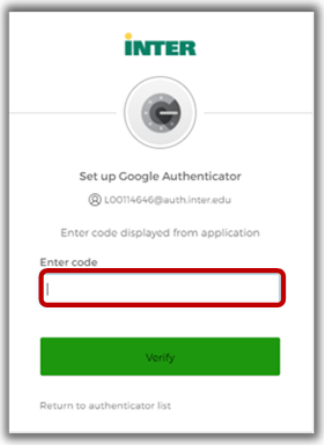


2. En la computadora presione el botón titulado ***Set up*** localizado bajo la opción ***Google Authenticator***.



3. Aparecerá en pantalla un QR Code que deberá leer con su dispositivo móvil utilizando la aplicación Google Authenticator.





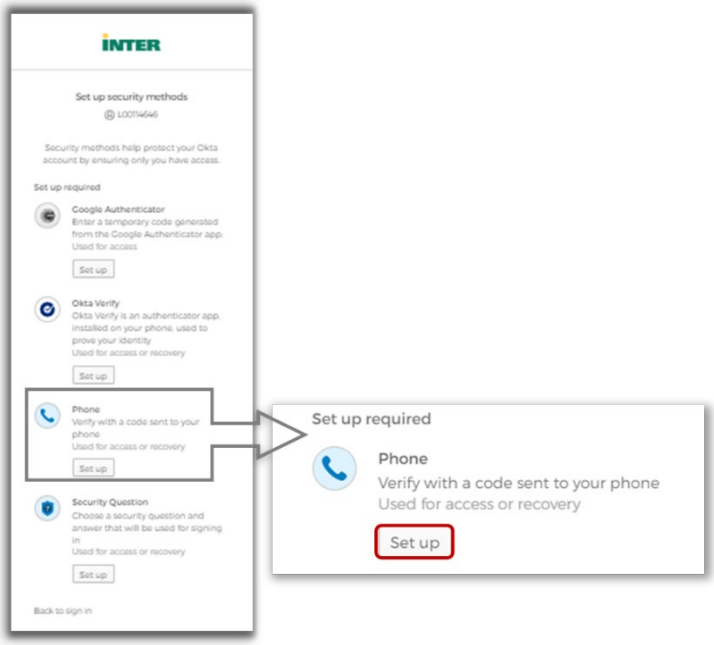
4. En la pantalla principal de Google Authenticator aparecerá un código que debe ingresar en el espacio provisto en la computadora.

Teléfono

Okta le ofrece dos factores de validación mediante el uso de un teléfono:

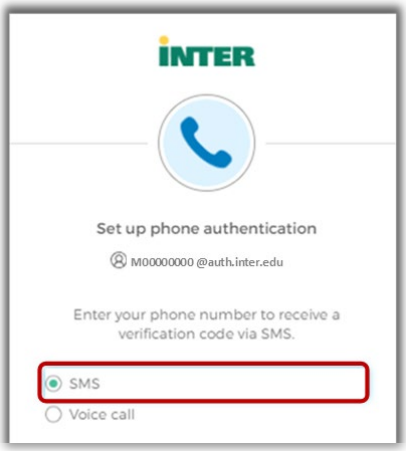
- recibir un mensaje de texto conteniendo el código
- una llamada telefónica en la cual le dictarán en dos ocasiones el código.

Para iniciar la configuración de estos factores de validación debe presionar el botón titulado ***Set Up*** localizado bajo la opción ***Phone***. En caso de que haya configurado otro factor previamente, el sistema solicitará se ingrese la contraseña y luego el código de validación que recibirá mediante ese factor.

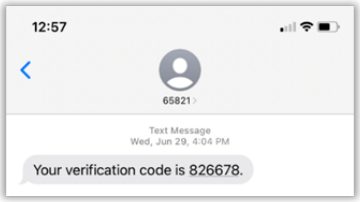


Mensaje de texto

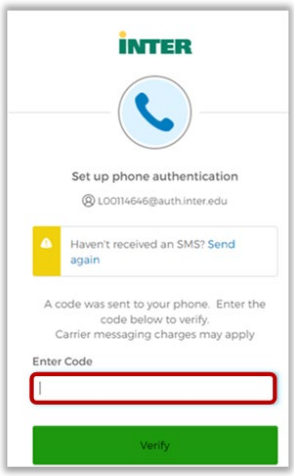
1. Seleccione el factor de autenticación ***SMS***. Ingrese el número de teléfono en el espacio provisto, incluyendo código de área, y luego presione el botón titulado ***Receive a code via SMS***.



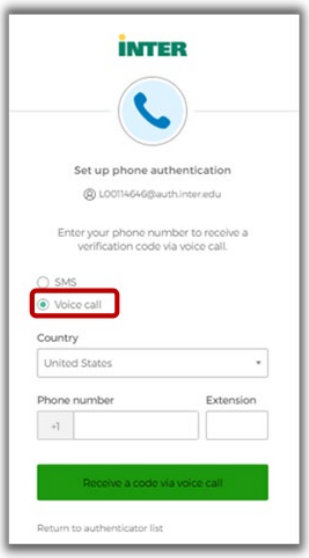
2. El dispositivo móvil recibirá un código de validación a través de un mensaje de texto SMS.



3. Introduzca el código en el espacio provisto y presione el botón titulado ***Verify***. Se desplegará en pantalla, por un corto periodo de tiempo, un mensaje que indica que el número de teléfono ha sido verificado correctamente.

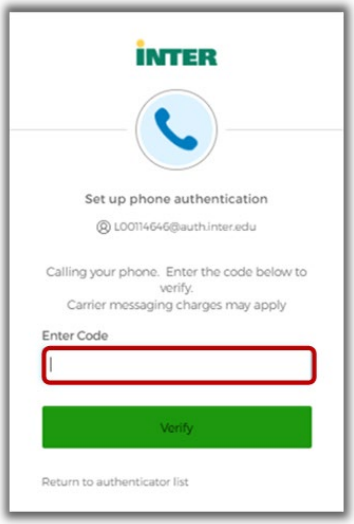


Llamada telefónica de confirmación



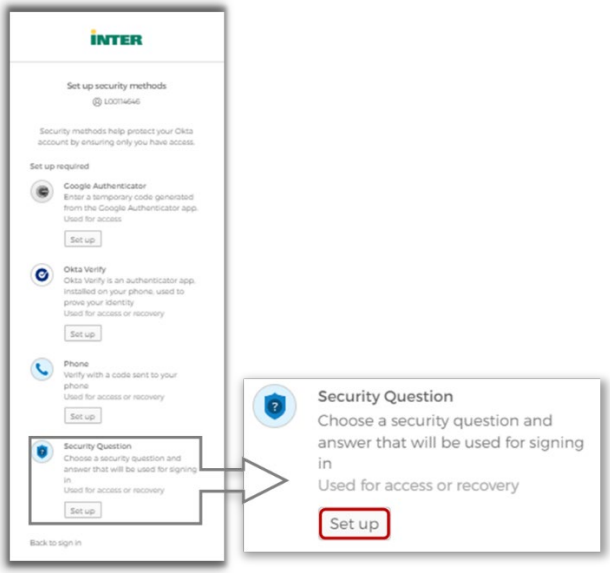
1. Seleccione el factor de autenticación ***Voice call*** e introduzca el número de teléfono en el espacio provisto. Se provee un espacio para agregar un número de extensión, pero es opcional. Presione el botón titulado ***Receive a code via voice call***. Recibirá una llamada telefónica que anunciará el código de verificación y lo repetirá por segunda ocasión.

2. Ingrese el código en el espacio provisto y presione el botón titulado ***Verify***. Se desplegará en pantalla, por un corto periodo de tiempo, un mensaje que indica que el número de teléfono ha sido verificado correctamente.



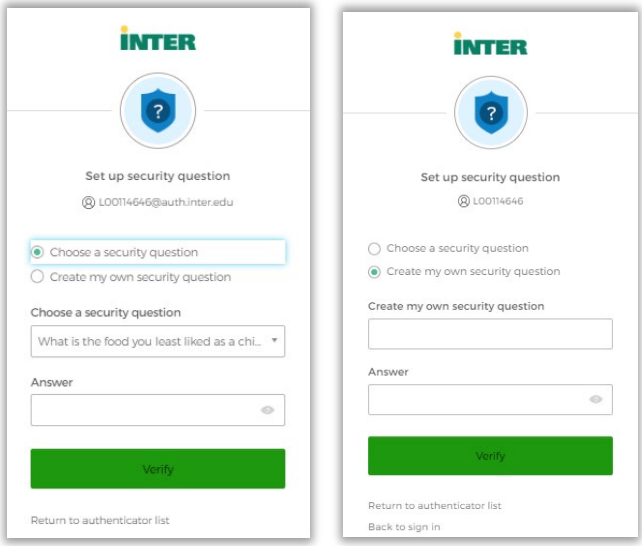
Pregunta de seguridad

1. Después de iniciar sesión, presione el botón titulado ***Set up*** localizado bajo de la opción ***Security Question***.



2. Determine si desea seleccionar una de las preguntas definidas o si establecerá una pregunta propia.
    a. En caso de determinar utilizar una de las preguntas previamente definidas, solamente debe seleccionarla y escribir la respuesta en el espacio provisto. Presione el botón titulado ***Verify***.

    b. En caso de determinar definir una pregunta propia, escriba la pregunta y la respuesta en los espacios provistos. Presione el botón titulado ***Verify***.



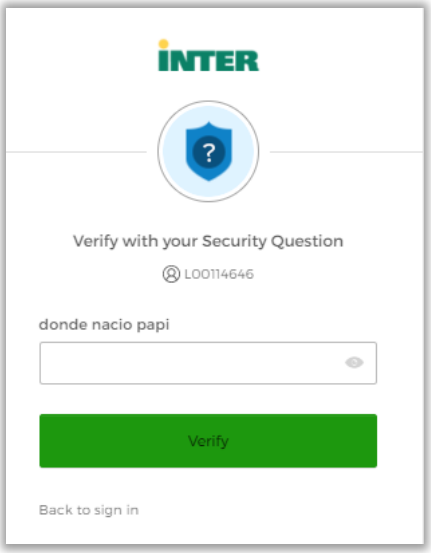
3. Se desplegará en pantalla, por un corto periodo de tiempo, un mensaje que indica que la pregunta de seguridad fue registrada correctamente.

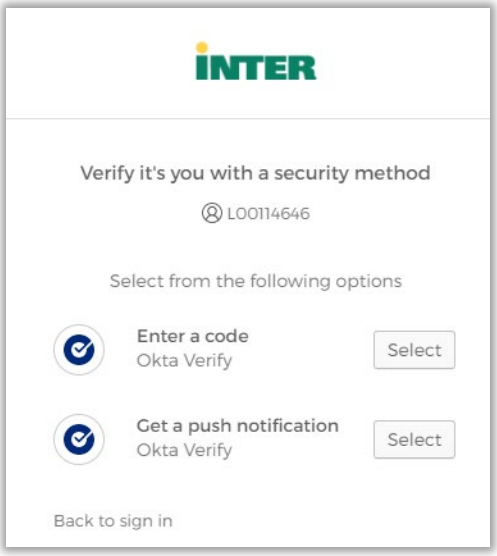
Añadir y actualizar las opciones de MFA

Luego de la configuración inicial de los factores de validación, es posible que necesite configurar factores adicionales o realizar cambios en alguno de los previamente definidos.

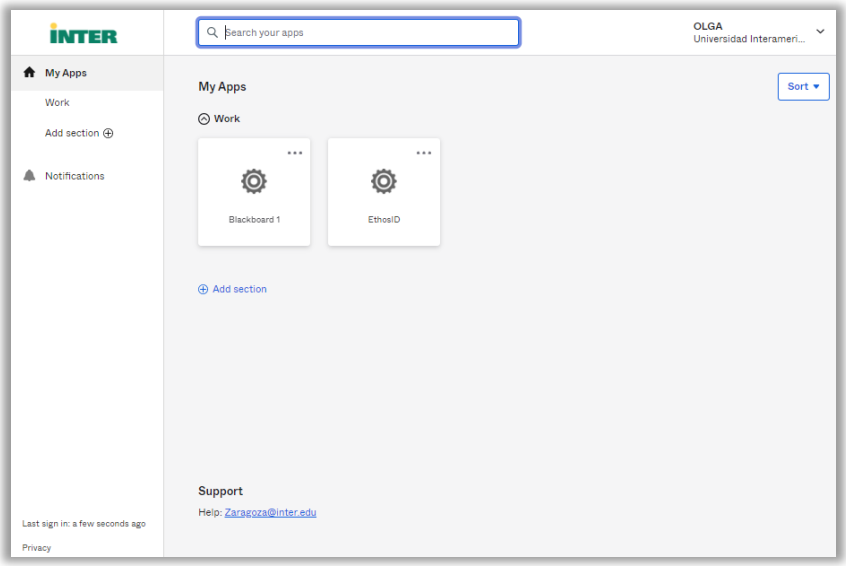
1. Inicie sesión en el portal https://inter.okta.com.

2. El sistema le requerirá validar con uno de los factores definidos previamente.

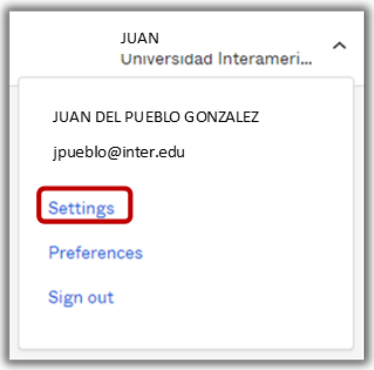




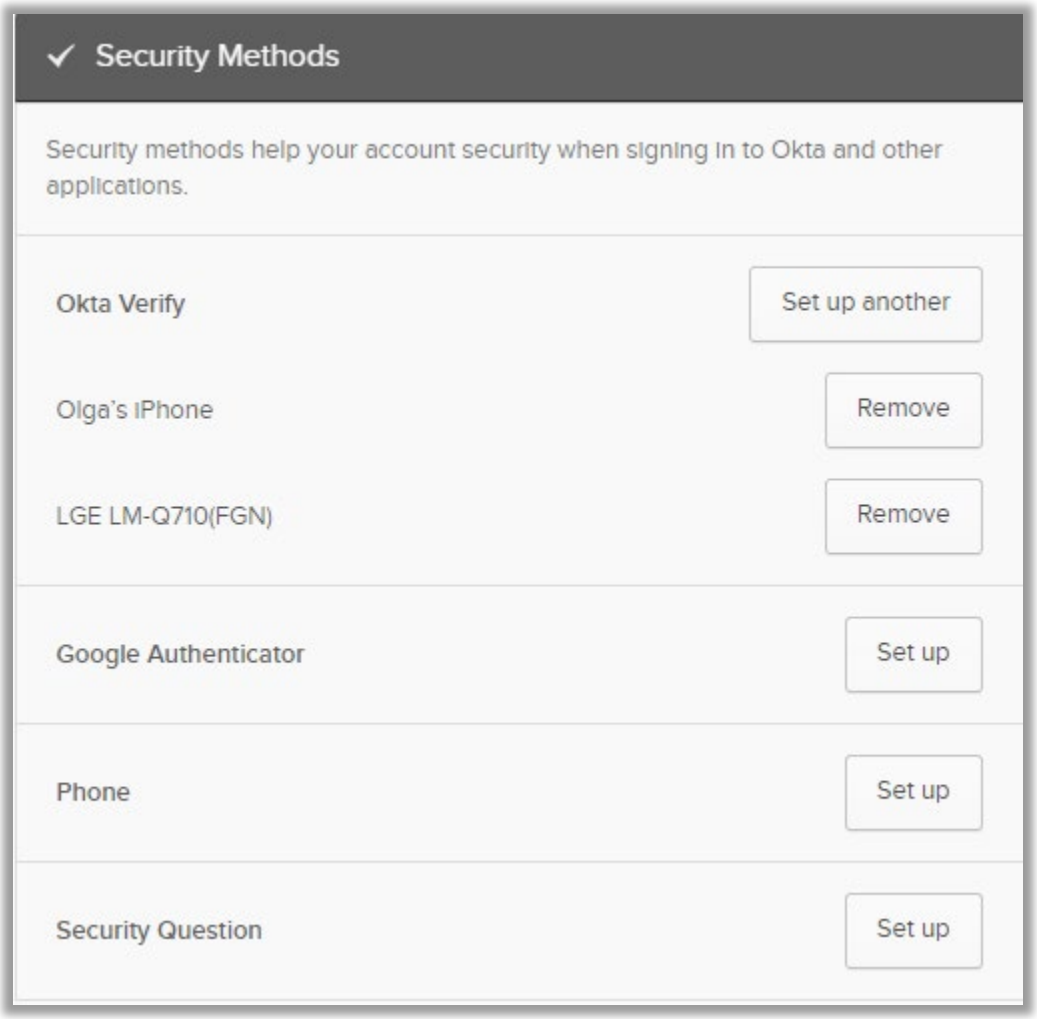
3. Una vez validado con éxito, tendrá acceso a la página de inicio de autenticación en Okta para la Universidad Interamericana de Puerto Rico.



4. Haga clic sobre el nombre de usuario localizado en la esquina superior derecha de la pantalla y seleccione la opción ***Settings***.

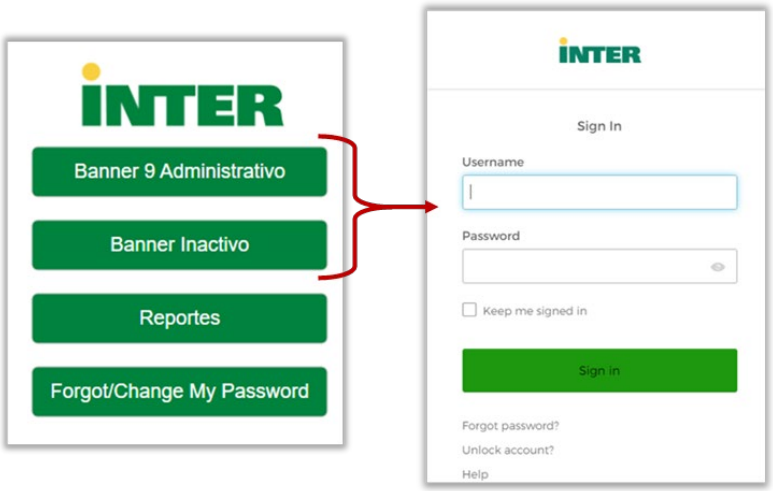


5. Diríjase a la sección titulada ***Security Methods.*** En esta sección podrá:
    a. Configurar (set up) factores adicionales.
    b. Eliminar (remove) factores que necesita actualizar o que no desee seguir utilizando.

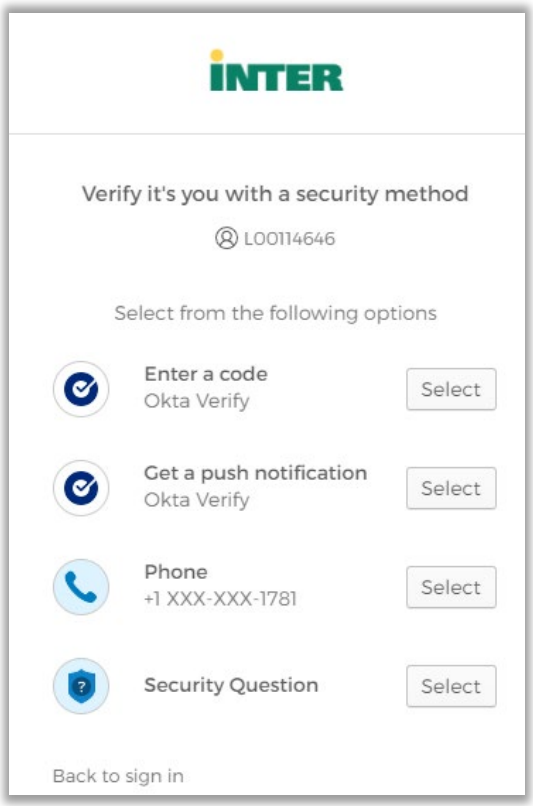


Proceso de autenticación a Banner Administrativo

El proceso de autenticación inicia accediendo al enlace https://uis.inter.edu/prod y seleccionando la instancia que necesita acceder: PROD o INAC. Luego, se presentará la pantalla de autenticación en la que deberá escribir su nombre de usuario (número de identificación) y su contraseña.

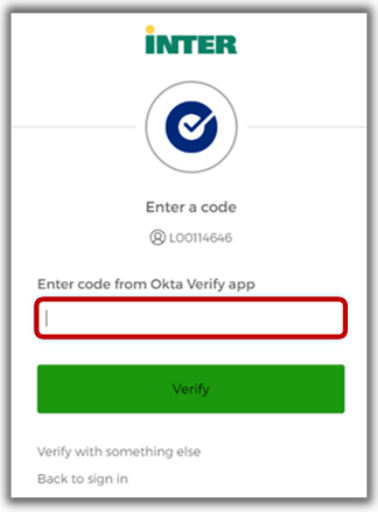


Al presionar el botón titulado Sign in, su solicitud de acceso será redirigida a la plataforma Okta, quien maneja los factores de autenticación que usted configuró previamente. Okta presentará la lista de los factores configurados para que usted se autentique utilizando el de su preferencia.



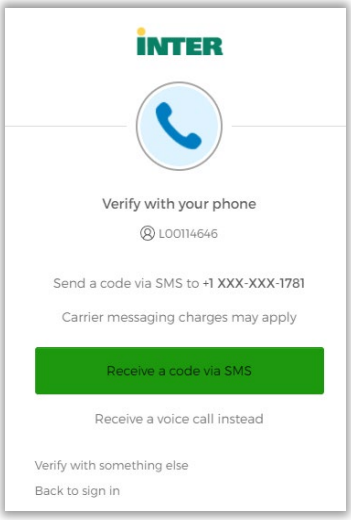
Okta Verify

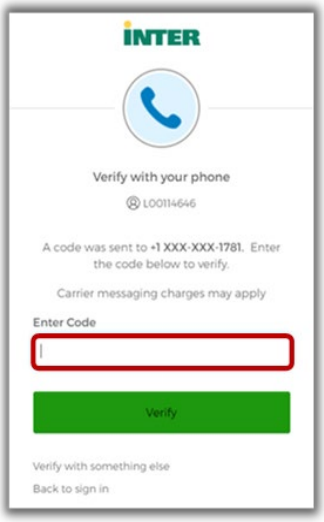
Al seleccionar el método MFA utilizando Okta Verify se le requerirá que escriba un código de validación que podrá obtener de la aplicación instalada en su teléfono. Debe ingresarlo en el espacio provisto y presionar el botón titulado Verify.



Teléfono

El factor de autenticación vía telefónica le permite recibir un código de validación mediante un mensaje de texto o el recibo de una llamada. Seleccione una de las opciones y una vez reciba el código debe ingresarlo en el espacio provisto y presionar el botón titulado Verify.





Pregunta de seguridad

El método de validación mediante pregunta de seguridad solamente le requiere ingresar la respuesta a la pregunta que fue definida. Una vez ingrese la respuesta correcta, debe presionar el botón titulado ***Verify***.

Solicitud de apoyo técnico

De necesitar apoyo o confrontar alguna situación, comunicarse con el Centro de informática de su Unidad. El siguiente enlace le ofrece una lista con la información de contacto por Unidad: https://www.inter.edu/Apoyo_Tecnico.