Universidad Interamericana de Puerto Rico

Oficina Central del Sistema

Centro de Informática y Telecomunicaciones

Multi-Factor Authentication (MFA)
Guía de usuario final

Revisado: septiembre de 2024

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 constante 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 se compone de un token de seguridad que se envía a su correo electrónico institucional. Además, el usuario tiene la opción de añadir como métodos adicionales: Okta Verify, Google Authenticator o una pregunta de seguridad.

Para implementar este nivel de seguridad se contrató 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, la lista de contactos disponibles para ofrecerles apoyo técnico en cada una de las Unidades Académicas del Sistema Universitario.

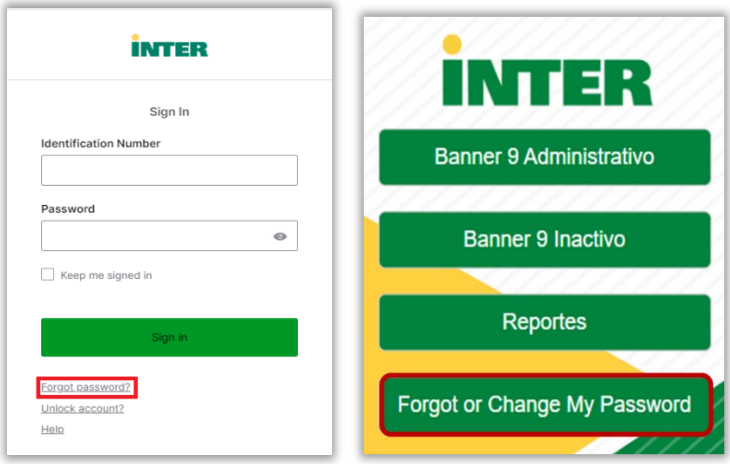
Activación de cuenta – usuarios nuevos

Todo usuario nuevo debe definir la contraseña con la cual accederá a los sistemas primarios, entiéndase, Banner Administrativo, Autoservicios de Banner (Inter Web) y Blackboard. El proceso de activación de la cuenta puede llevarse a cabo en cualquiera de las tres plataformas. A continuación, se enumeran los pasos que le guiarán en el proceso de definirla.

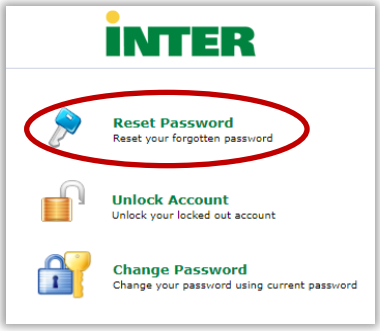
Activación de cuentas en Autoservicios de Banner y Banner Administrativo

1. Acceda a Autoservicios de Banner o a Banner Administrativo.

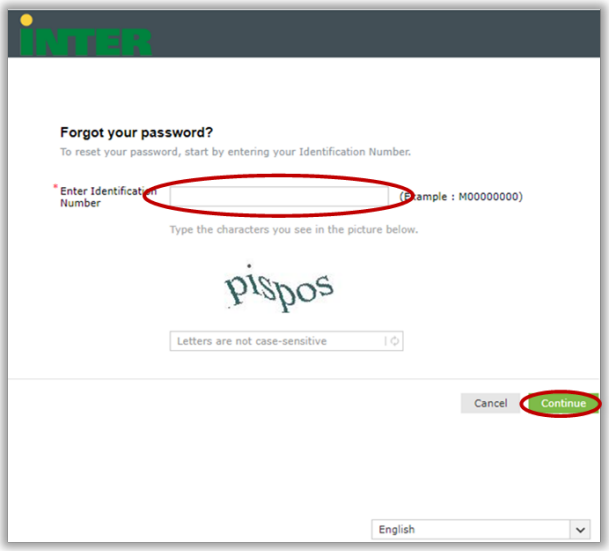
2. Seleccione la opción ***Forgot Password.***



3. Seleccione la opción ***Reset Password.***



4. En la pantalla titulada ***Forgot your Password?***, debe ingresar su número de identificación. Luego, escriba los caracteres que se muestran en pantalla y presione el botón titulado ***Continue***.

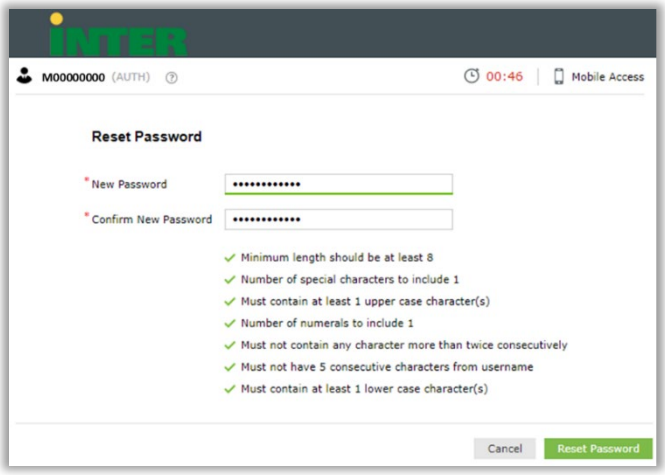


5. El sistema le presentará la dirección electrónica asignada por la Universidad, a la cual, será enviado un código de verificación. Presione el botón titulado ***Continue***.

6. En el espacio provisto, escriba el código recibido en su correo electrónico y presione el botón titulado ***Continue*****.**

    a. El código es enviado desde la dirección adselfservice@auth.inter.edu.

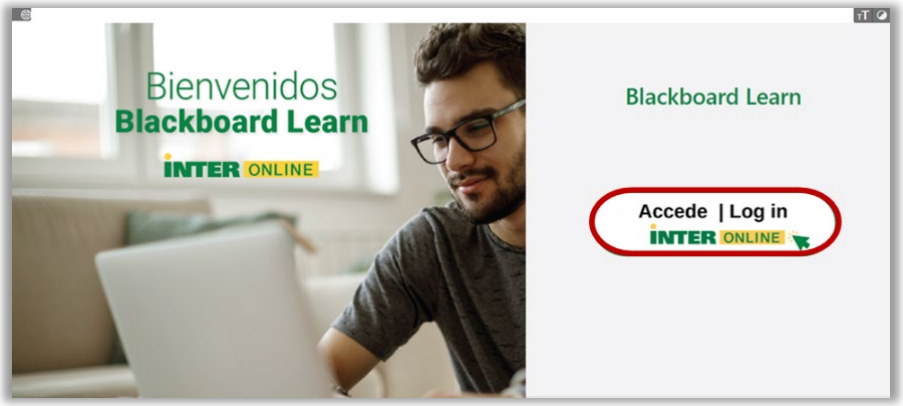
7. Escriba su nueva contraseña en ambos espacios. La contraseña debe cumplir con los requisitos que se muestran bajo los espacios provistos para escribir la contraseña. Mientras define la contraseña el sistema coloca una marca de cotejo al lado de cada requisito con el que ha cumplido. Al concluir debe presionar el botón titulado **Reset Password**.



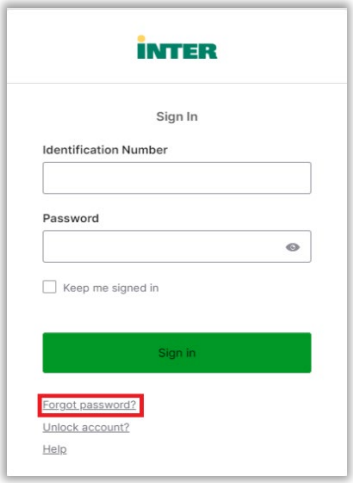
8. El sistema le confirmará que el proceso fue completado exitosamente, mostrando un mensaje en pantalla y enviando un mensaje de correo electrónico.

Activación de cuentas desde Blackboard

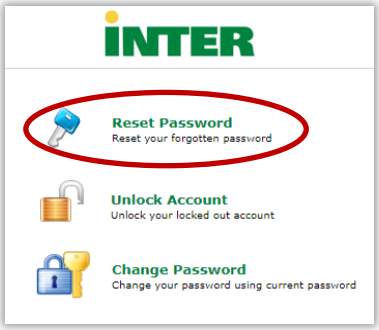
1. Acceda a la plataforma de Blackboard.



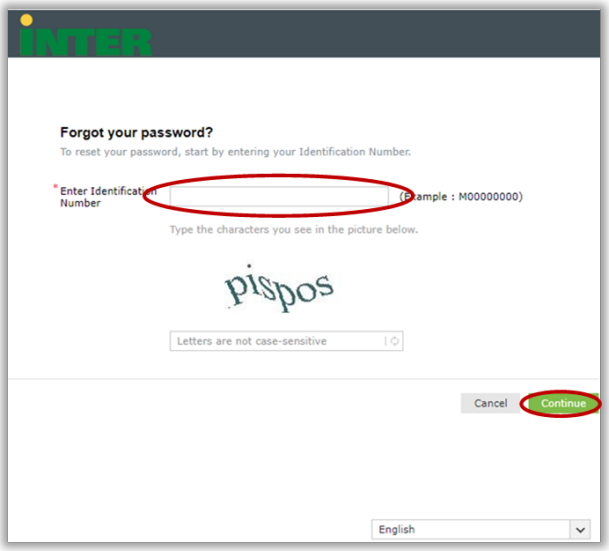
2. Seleccione la opción ***Forgot Password*** localizada bajo el botón titulado ***Sign in.***



3. Seleccione la opción ***Reset Password.***



4. En la pantalla titulada ***Forgot your Password?***, debe ingresar su número de identificación. Luego, escriba los caracteres que se muestran en pantalla y presione el botón titulado ***Continue***.

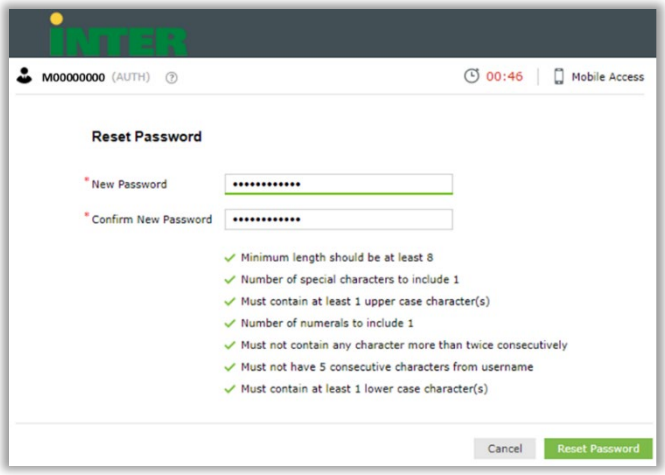


5. El sistema le presentará la dirección electrónica asignada por la Universidad, a la cual, será enviado un código de verificación. Presione el botón titulado ***Continue***.

6. En el espacio provisto, escriba el código recibido en su correo electrónico y presione el botón titulado ***Continue*.**

    a. El código es enviado desde la dirección adselfservice@auth.inter.edu.

7. Escriba su nueva contraseña en ambos espacios. La contraseña debe cumplir con los requisitos que se muestran bajo los espacios provistos para escribir la contraseña. Mientras define la contraseña el sistema coloca una marca de cotejo al lado de cada requisito con el que ha cumplido. Al concluir debe presionar el botón titulado **Reset Password**.



8. El sistema le confirmará que el proceso fue completado exitosamente, mostrando un mensaje en pantalla y enviando un mensaje de correo electrónico.

Añadir opciones de Multi-Factor Authentication (MFA) adicionales

Una vez usted se autentique por primera vez en alguno de los servicios, Okta activará como factores de autenticación la contraseña definida por usted y el correo electrónico institucional. Además, usted puede activar alguno de los siguientes métodos opcionales:

1. Okta Verify - es una aplicación que se descarga en el celular y que provee el código de validación requerido por Okta. Puede descargarla en el Apple Apps Store o en el Android Play Store.

2. Google Authenticator - es una aplicación que se descarga en el celular y que provee el código de validación para ser utilizado en diversos sistemas que requieren múltiples factores de autenticación. Puede descargarla en el Apple Apps Store o en el Android Play Store.

3. Pregunta de Seguridad - es una opción que le permite seleccionar una de las preguntas definidas en Okta o definir una de su preferencia.

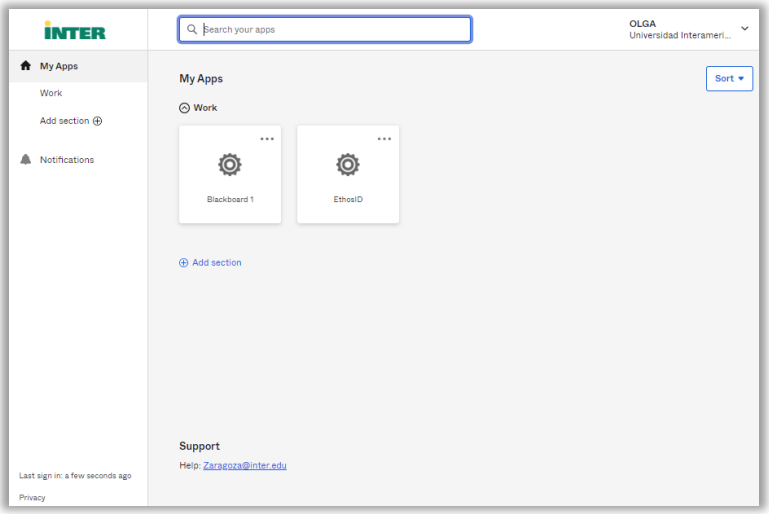
Le recomendamos configure tantos factores como le sea posible, de acuerdo con los recursos tecnológicos que tenga disponible.

Para añadir factores de autenticación adicionales o realizar cambios en algún factor opcional previamente definido:

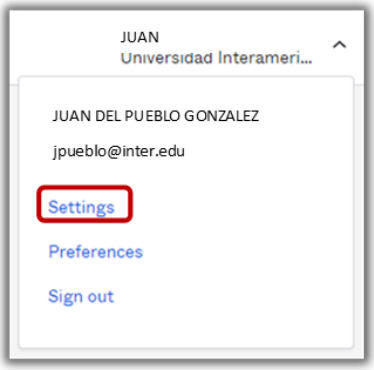
1. Inicie sesión en el portal Inter Okta.

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

3. Una vez validado con éxito, tendrá acceso a la página de 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 factores adicionales presionando el botón titulado **Set up** localizado al lado derecho de cada método no configurado.

   b. Eliminar factores que necesita actualizar o que no desee seguir utilizando, presionando el botón titulado **Remove** localizado en el lado derecho de cada método previamente configurado.

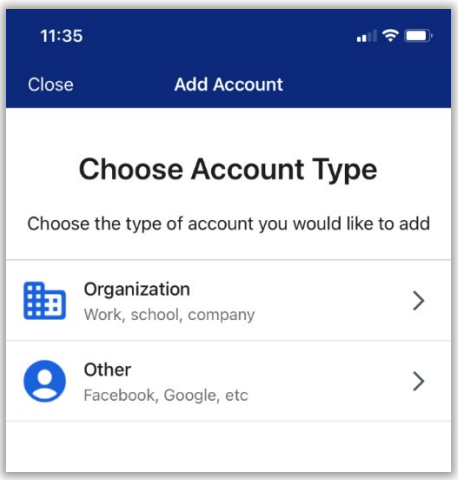
Cómo configurar Okta Verify

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

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

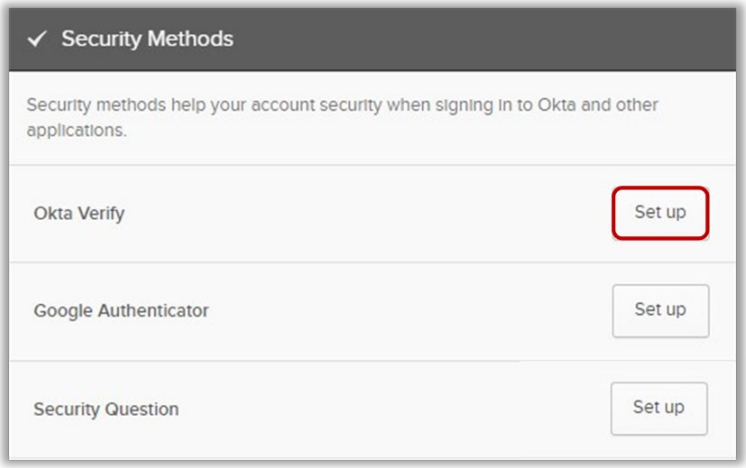
3. En la pantalla principal de Okta Verify, debe seleccionar la opción agregar cuenta, la cual, puede estar representada por el signo de **+**.

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 al lado de la opción ***Okta Verify***.



7. Aparecerá en pantalla de la computadora 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.

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:

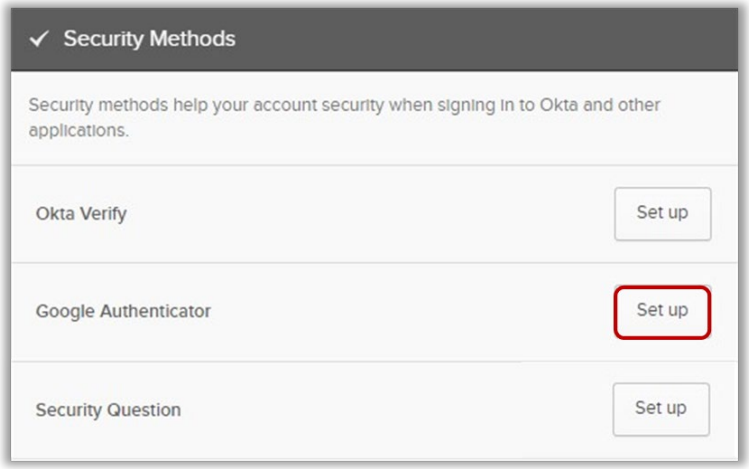
- Para información adicional sobre Okta Verify puede acceder al siguiente enlace: Okta Verify.

- Si un usuario obtiene un nuevo teléfono, debe configurar su cuenta Okta Verify nuevamente en el nuevo dispositivo.

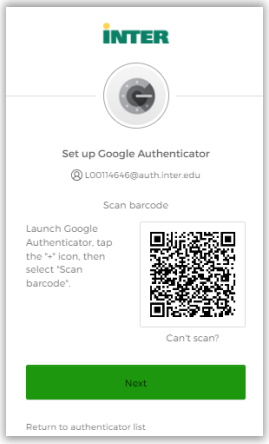
Cómo configurar Google Authenticator

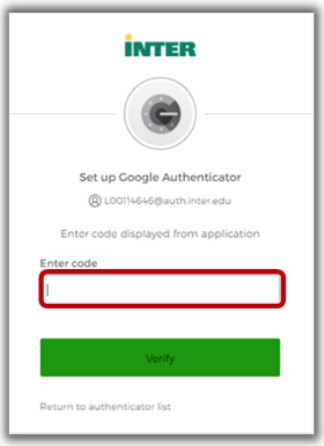
1. Utilizando un dispositivo móvil, descargue la aplicación Google Authenticator desde Android Play Store o Apple App Store.

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



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

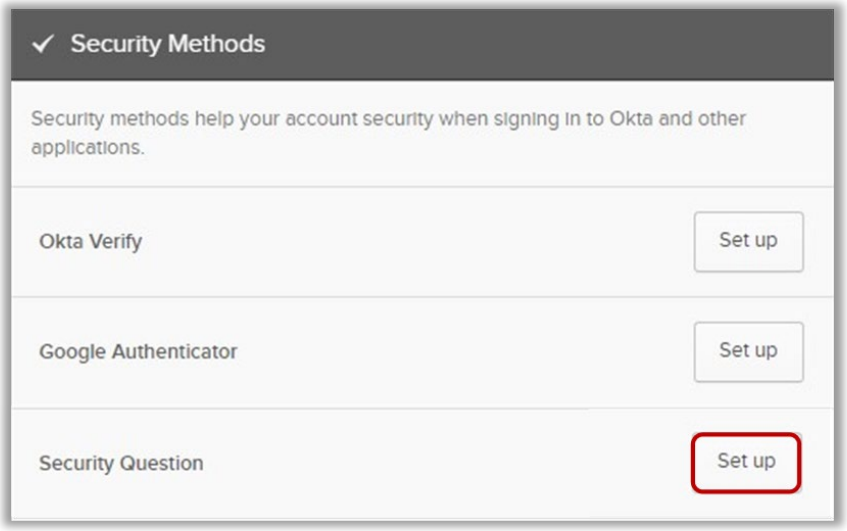




4. En la pantalla principal de Google Authenticator aparecerá un código que debe ingresar en el espacio provisto en la computadora.

Cómo configurar una pregunta de seguridad

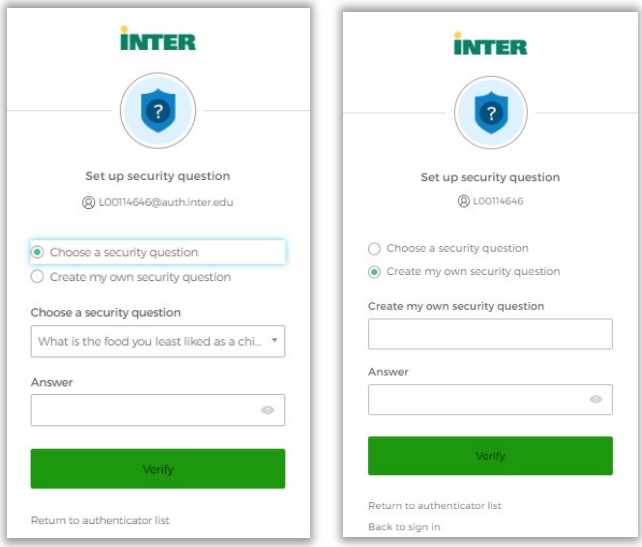
1. Después de iniciar sesión en el portal Inter Okta, presione el botón titulado ***Set up*** localizado al lado de la opción ***Security Question***.



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.

Proceso de autenticación a Banner Administrativo

1. Acceda a Banner Administrativo.
2. Seleccione la instancia que necesita acceder: PROD o INAC.
3. El sistema le presentará la pantalla de autenticación en la que deberá escribir su número de identificación y su contraseña.
4. 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.
    a. Okta Verify - se le requerirá que escriba un código de validación que podrá obtener de la aplicación instalada en su teléfono y presionar el botón titulado Verify.
    b. Google Authenticator – se le requerirá que escriba un código de validación que podrá obtener de la aplicación instalada en su teléfono y presionar el botón titulado Verify.

c. Pregunta de Seguridad - 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 puede comunicarse con el Centro de Informática y Telecomunicaciones de su Unidad Académica.

Recinto de Aguadilla

- Correo electrónico: apoyo_cit@aguadilla.inter.edu
- Teléfono: 787-891-0925 extensiones #2517, #2406

Recinto de Arecibo

- Correo electrónico: serviciostecnicos@arecibo.inter.edu
- Teléfono: 787-878-5475 extensiones 3403, 3404, 3405

Recinto de Barranquitas

- Correo electrónico: apoyo@br.inter.edu
- Teléfono: 787-857-3600 extensiones #2013, #2063, #2075, #2022, #2076, #2064, #2024, #2080, #2237

Recinto de Bayamon

- Correo electrónico: cit@bayamon.inter.edu
- Teléfono: 787-279-1912 extensiones 2095, 2097, 2047, 2044

Escuela de Optometría

- Correo electrónico: cit@opto.inter.edu
- Teléfono: 787-765-1915 extensiones #1115, #1024

Facultad de Derecho

- Correo electrónico: itservicedesk@juris.inter.edu
- Teléfono: 787-751-1912 extensiones #2519, #2045, #2511 #3021, #2066

Recinto de Fajardo

- Correo electrónico: apoyotecnico@fajardo.inter.edu
- Teléfono: 787-863-2390 extensiones #2197, #2230, #2193, #2235, #2198

Recinto de Guayama

- Correo electrónico: apoyo.tecnico@guayama.inter.edu
- Teléfono: 787-864-2222 extensiones #2392, #2394, #2208

Recinto Metropolitano

- Correo electrónico: cit2@metro.inter.edu
- Teléfono: 787-250-1912 extensiones 2519, 2273

Recinto de Ponce

- Correo electrónico: citayuda@ponce.inter.edu
- Teléfono: 787-284-1912 extensiones #2067, #2066

Recinto de San Germán

- Correo electrónico: tecnicos@intersg.edu
- Teléfono: 787-264-1912 extensiones #7674, #7675, #7103