



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	1
¿Qué es Multi-Factor Authentication?	1
Activación de cuenta – usuarios nuevos.....	2
Activación de cuentas en Banner Administrativo y Autoservicios	2
Activación de cuentas desde Blackboard	5
Configuración inicial del Multi-Factor Authentication (MFA)	6
Okta Verify	6
Google Authenticator.....	9
Teléfono.....	11
Mensaje de texto	11
Llamada telefónica de confirmación	12
Pregunta de seguridad.....	13
Añadir y actualizar las opciones de MFA.....	14
Proceso de autenticación a Banner Administrativo	16
Okta Verify	17
Teléfono.....	17
Pregunta de seguridad.....	17
Solicitud de apoyo técnico	18

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.

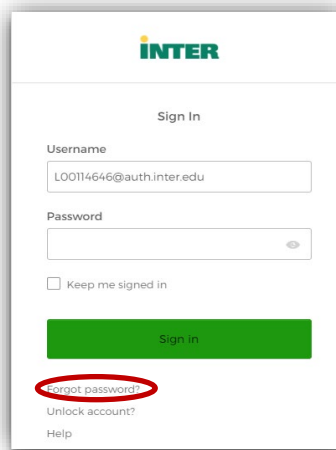
Para implementar este nivel de seguridad hemos contratado la plataforma Okta. Este documento le ofrece las instrucciones básicas que le guiarán en el proceso definición de los factores de autenticación, así como en la manera en que se autenticará con cada uno de ellos. Incluye, además, un enlace a la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

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 aplicaciones. A continuación, se enumeran los pasos que le guiarán en el proceso de definirla en Banner Administrativo o en Autoservicios de Banner.

Activación de cuentas en Banner Administrativo y Autoservicios

1. Acceda al enlace <https://uis.inter.edu/PROD> para activar su cuenta desde Banner Administrativo o al enlace <https://ssb.ec.inter.edu/ssomanager/c/SSB> para activarla desde Autoservicios de Banner.
2. Seleccione la opción **Forgot Password**.



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

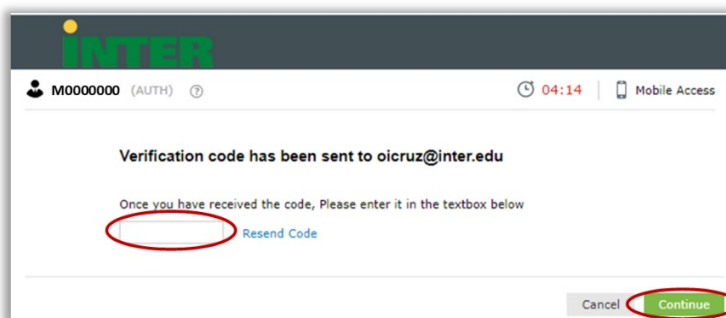


4. En la pantalla titulada ***Forgot your Password?***, debe ingresar su número de identificación, por ejemplo: M00000000. Luego, escriba los caracteres que se muestran en pantalla y presione el botón titulado ***Continue***.

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. Recibirá un correo electrónico de parte de adselfservice@auth.inter.edu que contiene el código, tal como se muestra en el siguiente ejemplo:

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



INTER

M00000000 (AUTH) 04:14 Mobile Access

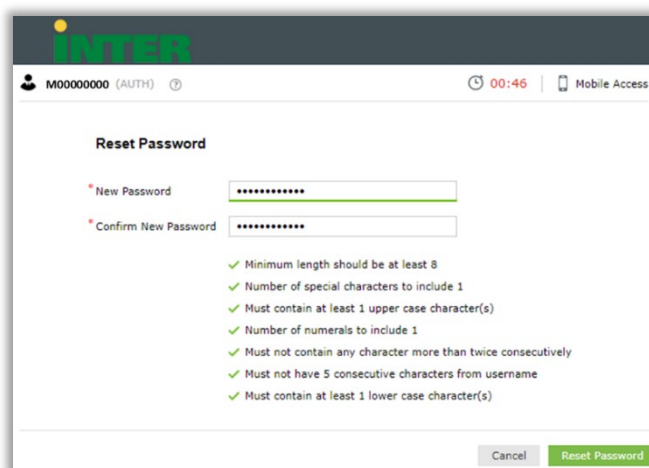
Verification code has been sent to oicruz@inter.edu

Once you have received the code, Please enter it in the textbox below

Resend Code

Cancel Continue

8. Escriba su nueva contraseña en ambos espacios. Esta 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**.



INTER

M00000000 (AUTH) 00:46 Mobile Access

Reset Password

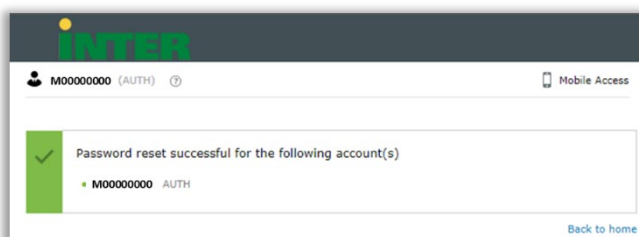
* New Password *****

* Confirm New Password *****

- ✓ Minimum length should be at least 8
- ✓ Number of special characters to include 1
- ✓ Must contain at least 1 upper case character(s)
- ✓ Number of numerals to include 1
- ✓ Must not contain any character more than twice consecutively
- ✓ Must not have 5 consecutive characters from username
- ✓ Must contain at least 1 lower case character(s)

Cancel Reset Password

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



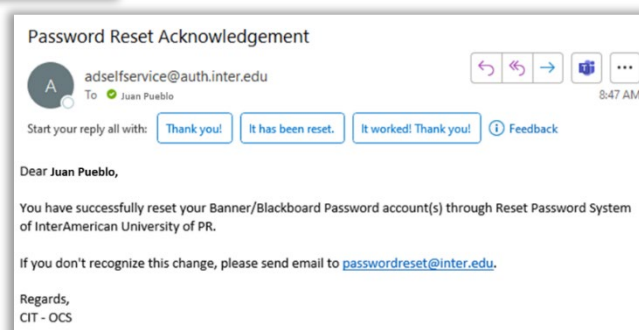
INTER

M00000000 (AUTH) Mobile Access

✓ Password reset successful for the following account(s)

- M00000000 AUTH

Back to home



Password Reset Acknowledgement

adselfservice@auth.inter.edu

To: Juan Pueblo 8:47 AM

Start your reply all with: Thank you! It has been reset. It worked! Thank you! Feedback

Dear Juan Pueblo,

You have successfully reset your Banner/Blackboard Password account(s) through Reset Password System of InterAmerican University of PR.

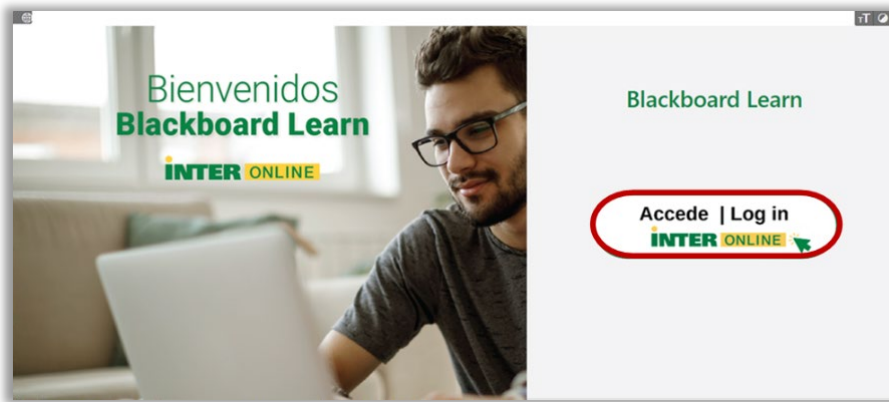
If you don't recognize this change, please send email to passwordreset@inter.edu.

Regards,
CIT - OCS

Activación de cuentas desde Blackboard

Para activar su cuenta desde la plataforma Blackboard debe acceder al siguiente enlace:
<https://pwdreset.inter.edu:9251/showLogin.cc>

1. Presione el botón titulado **Accede | Log in**.



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

3. A partir de este punto sigas los pasos 3 al 9 de la sección titulada **Activación de cuentas – usuarios nuevos**, localizada en la página número 2 de este documento.

Configuración inicial del Multi-Factor Authentication (MFA)

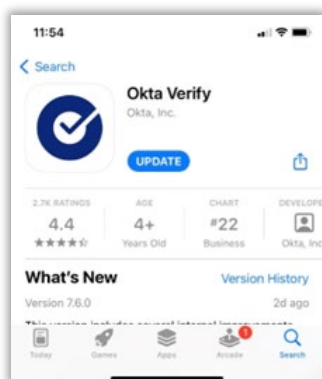
La plataforma Okta ofrece cinco alternativas de factores que pueden ser configurados y cuya descripción se muestra a continuación.

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.

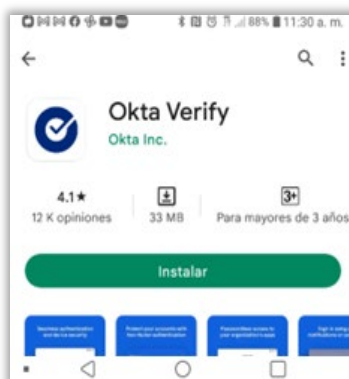
Cuando usted se autentica por primera vez, Okta le requerirá la activación de al menos uno de ellos. **Le recomendamos configure tantos factores como le sea posible, de acuerdo con los recursos tecnológicos que tenga disponible.** A continuación, se presenta cada uno de los factores disponibles.

Okta Verify

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

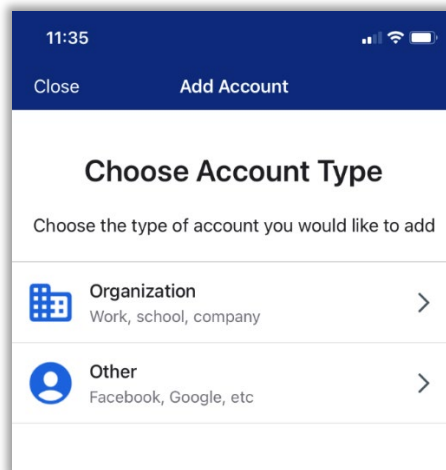


Apps Store

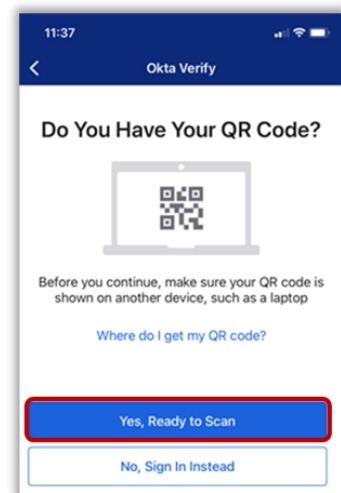


Play Store

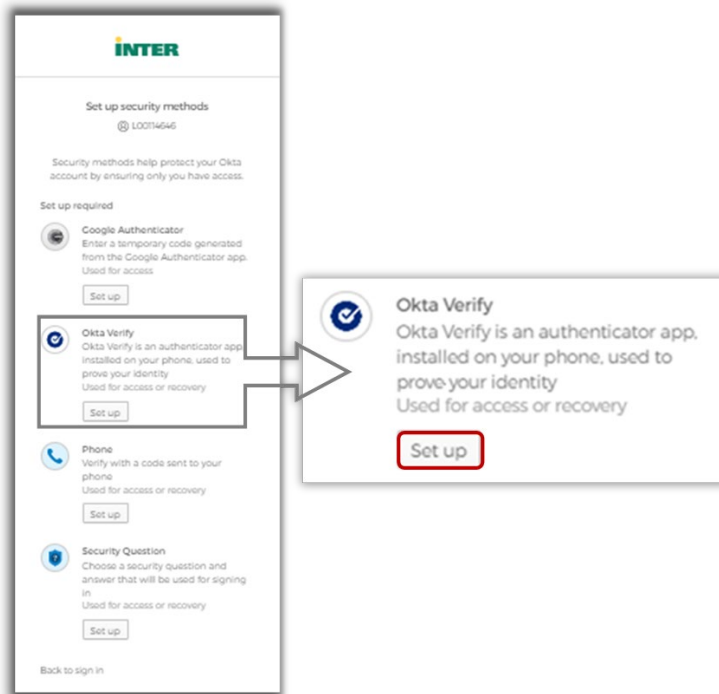
2. Cuando utiliza Okta Verify por primera vez, se muestra una pantalla describiendo cómo funciona el Apps. Presione el botón titulado **Next**.
3. En la pantalla principal de Okta Verify, debe seleccionar la opción agregar cuenta, la cual, puede estar representada por el signo de +.
4. Elija el tipo de cuenta que desea agregar a Okta Verify. Para efectos de la Universidad Interamericana de Puerto Rico, debe seleccionarse la opción **Organization**.



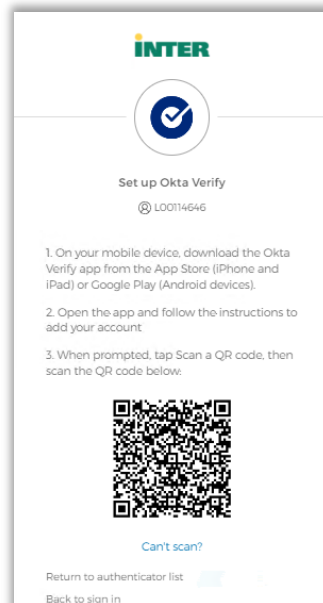
5. Okta Verify le requerirá leer el QR Code que Okta le presentará en la pantalla de la computadora.



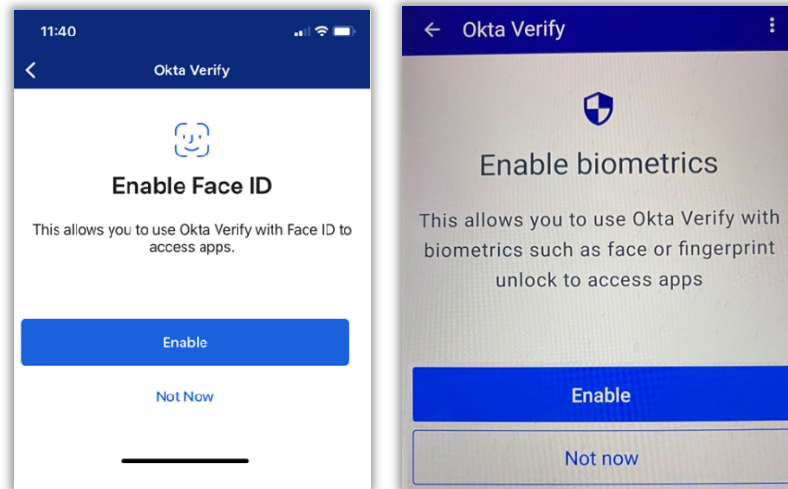
6. En el momento en que inicie sesión en la computadora, Okta le mostrará la lista de los factores de autenticación disponibles para ser activados. Presione el botón titulado **Set up** que aparece bajo la opción **Okta Verify**.



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.



- 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.



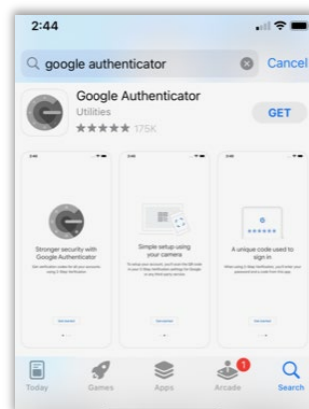
- En el dispositivo aparecerá un mensaje confirmando la validación de la cuenta. Debe presionar el botón titulado **Done**.

Notas:

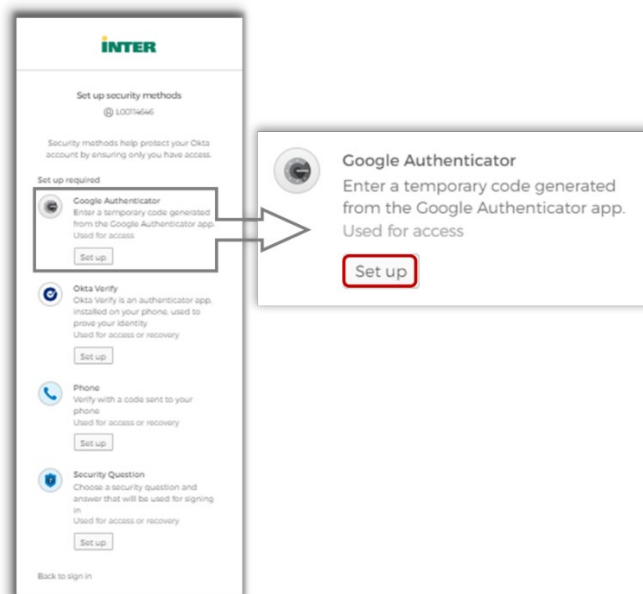
- Para información adicional sobre Okta Verify puede acceder al siguiente enlace: [Okta Verify](#).
- Si un usuario obtiene un nuevo teléfono, debe configurar su cuenta Okta Verify nuevamente en el nuevo dispositivo.

Google Authenticator

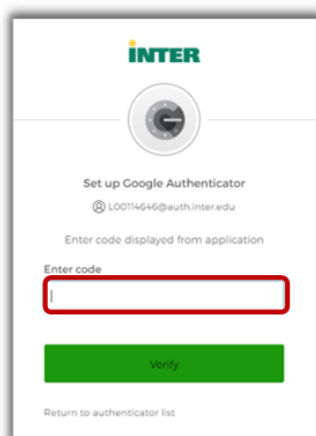
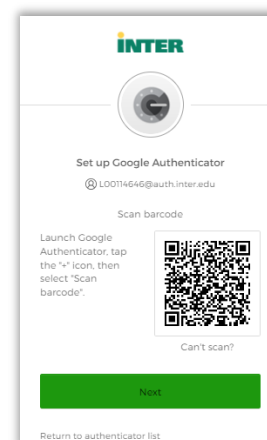
- Utilizando un dispositivo móvil, descargue la aplicación Google Authenticator desde Android Play Store o Apple App Store.



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.



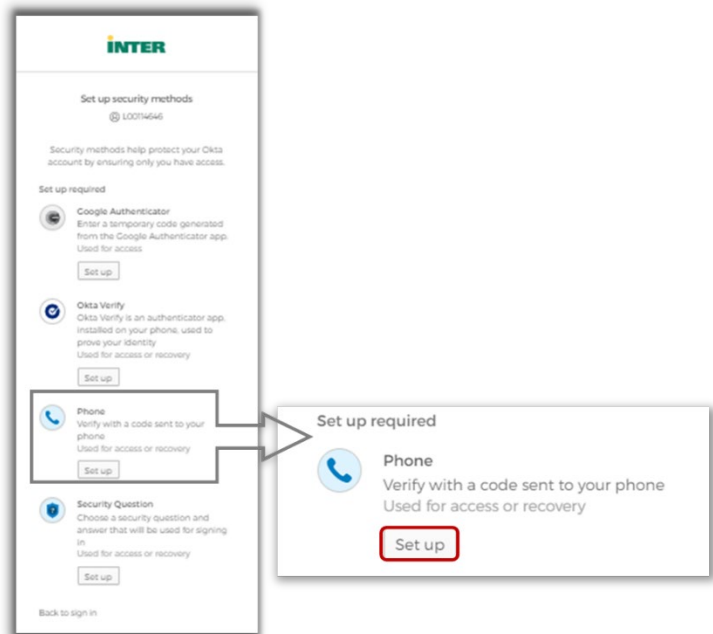
4. En la pantalla principal de Google Authenticator aparecerá un código que debe ingresar en el espacio provisto en la computadora.

Teléfono

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

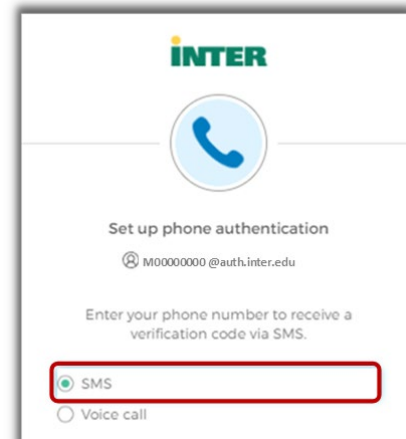
- recibir un mensaje de texto conteniendo el código
- una llamada telefónica en la cual le dictarán en dos ocasiones el código.

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.

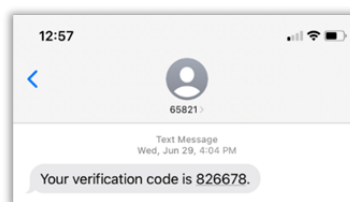


Mensaje de texto

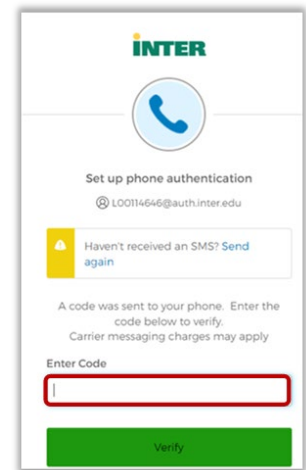
1. Seleccione el factor de autenticación **SMS**. Ingrese el número de teléfono en el espacio provisto, incluyendo código de área, y luego presione el botón titulado **Receive a code via SMS**.



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

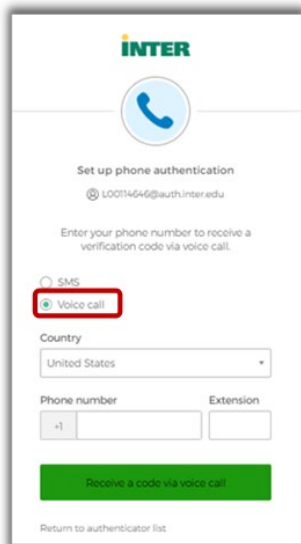


- Introduzca el código en el espacio provisto y presione el botón titulado **Verify**. Se desplegará en pantalla, por un corto periodo de tiempo, un mensaje que indica que el número de teléfono ha sido verificado correctamente.



The screenshot shows the 'Set up phone authentication' screen for the user 'LO0114646@auth.inter.edu'. It features a blue phone icon at the top. Below the header, there is a yellow alert box stating 'Haven't received an SMS? Send again'. The main instruction reads: 'A code was sent to your phone. Enter the code below to verify. Carrier messaging charges may apply.' There is a text input field labeled 'Enter Code' with a red border, and a green button labeled 'Verify' at the bottom.

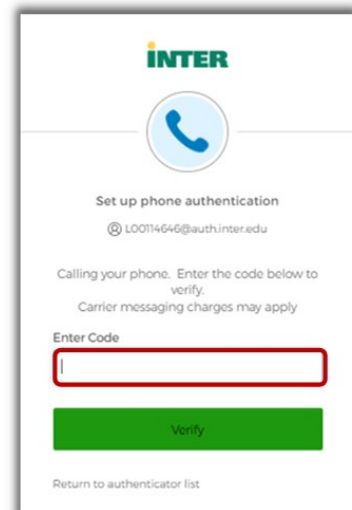
Llamada telefónica de confirmación



The screenshot shows the 'Set up phone authentication' screen. It has a blue phone icon and the user email 'LO0114646@auth.inter.edu'. The instruction says: 'Enter your phone number to receive a verification code via voice call.' There are two radio buttons: 'SMS' and 'Voice call', with 'Voice call' selected and highlighted by a red box. Below this is a 'Country' dropdown menu set to 'United States', and two input fields for 'Phone number' and 'Extension'. A green button labeled 'Receive a code via voice call' is at the bottom, along with a link 'Return to authenticator list'.

- 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.

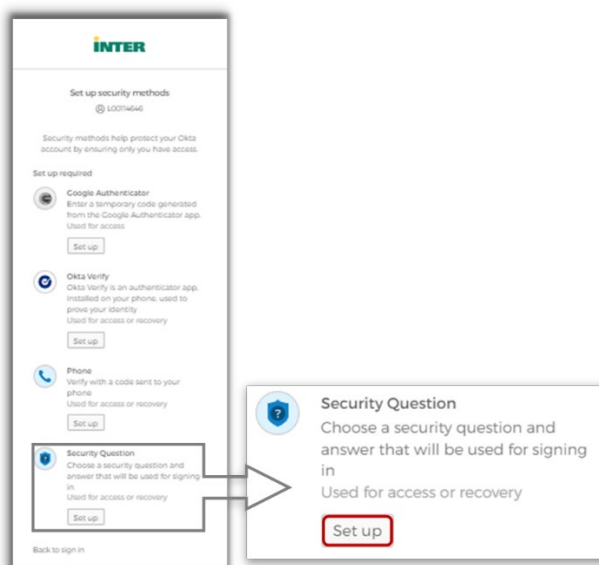
- Ingrese el código en el espacio provisto y presione el botón titulado **Verify**. Se desplegará en pantalla, por un corto periodo de tiempo, un mensaje que indica que el número de teléfono ha sido verificado correctamente.



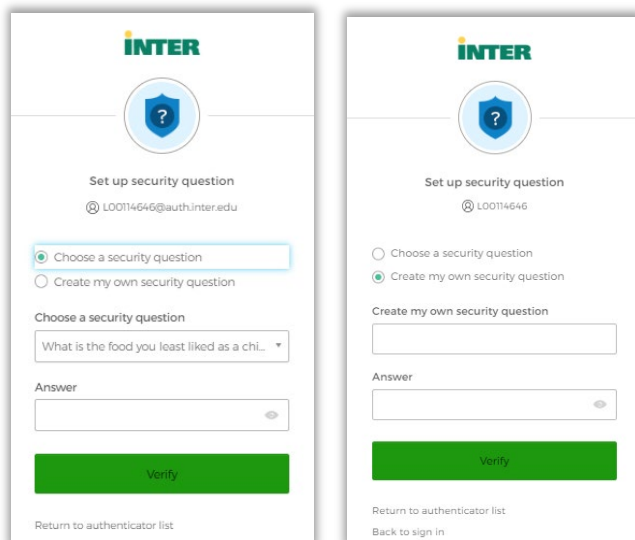
The screenshot shows the 'Set up phone authentication' screen for the user 'LO0114646@auth.inter.edu'. It features a blue phone icon. The main instruction reads: 'Calling your phone. Enter the code below to verify. Carrier messaging charges may apply.' There is a text input field labeled 'Enter Code' with a red border, and a green button labeled 'Verify' at the bottom. A link 'Return to authenticator list' is at the very bottom.

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

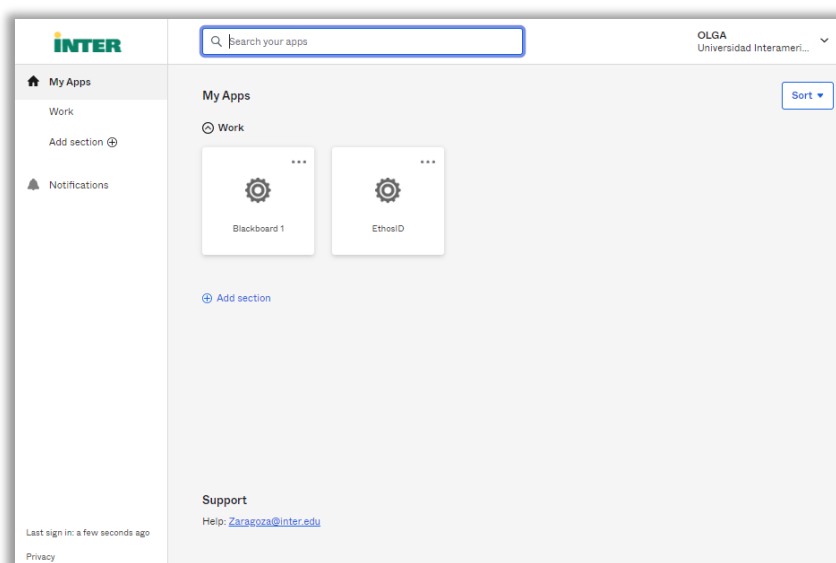
Luego de la configuración inicial de los factores de validación, es posible que necesite configurar factores adicionales o realizar cambios en alguno de los previamente definidos.

1. Inicie sesión en el portal <https://inter.okta.com>.
2. El sistema le requerirá validar con uno de los factores definidos previamente.

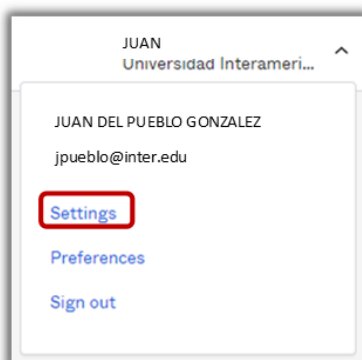
The first screenshot shows the 'Verify with your Security Question' screen. It features the INTER logo at the top, a shield icon with a question mark, and the text 'Verify with your Security Question'. Below this is a security ID 'L00T14646' and a text input field containing 'donde nacio papi'. A green 'Verify' button is at the bottom, along with a 'Back to sign in' link.

The second screenshot shows the 'Verify it's you with a security method' screen. It features the INTER logo at the top, the text 'Verify it's you with a security method', and a security ID 'L00T14646'. Below this is the text 'Select from the following options'. There are two options: 'Enter a code Okta Verify' and 'Get a push notification Okta Verify'. The 'Enter a code Okta Verify' option is selected, indicated by a checkmark icon. A 'Select' button is next to each option. At the bottom is a 'Back to sign in' link.

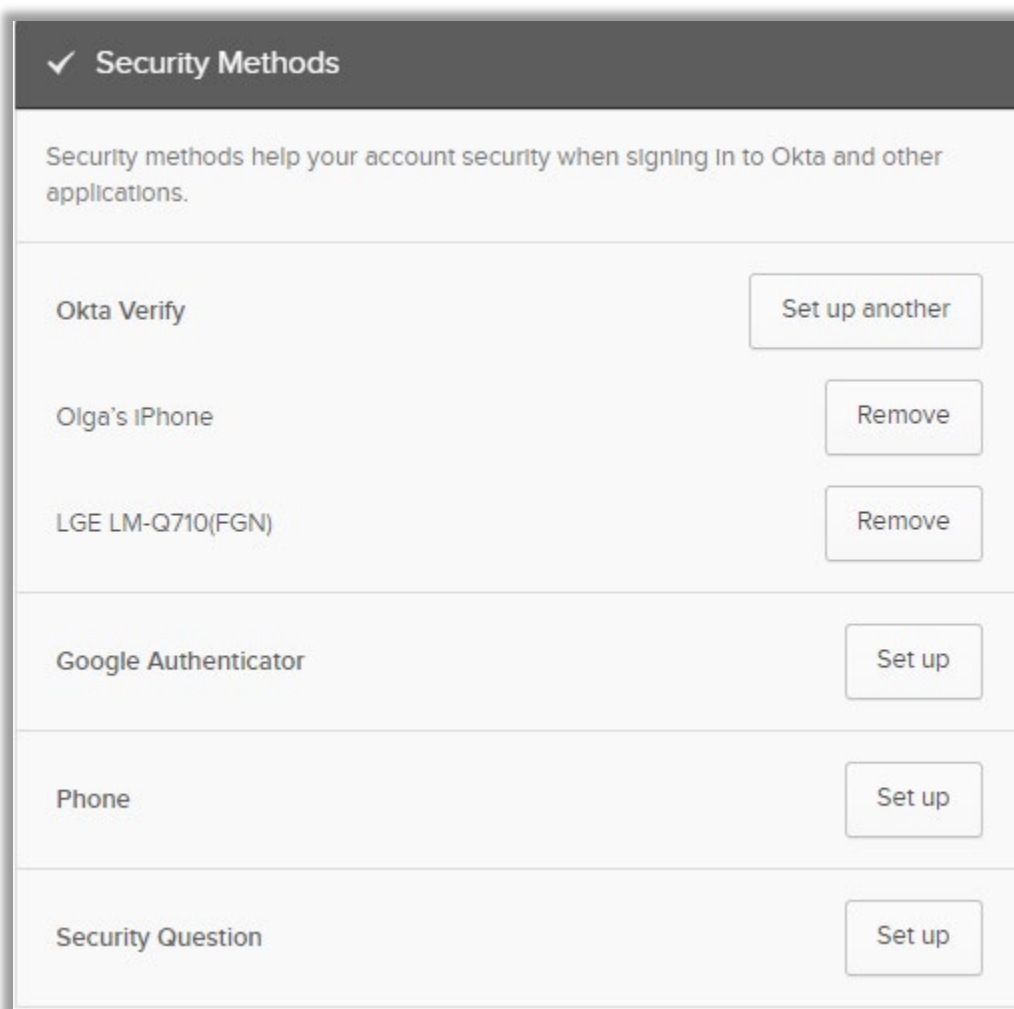
3. Una vez validado con éxito, tendrá acceso a la página de inicio de autenticación en Okta para la Universidad Interamericana de Puerto Rico.



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

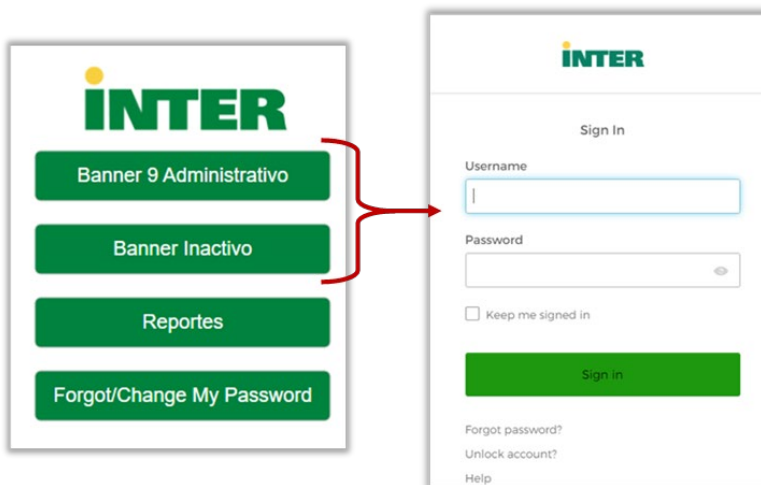


5. Diríjase a la sección titulada **Security Methods**. En esta sección podrá:
- a. Configurar (set up) factores adicionales.
 - b. Eliminar (remove) factores que necesita actualizar o que no desee seguir utilizando.

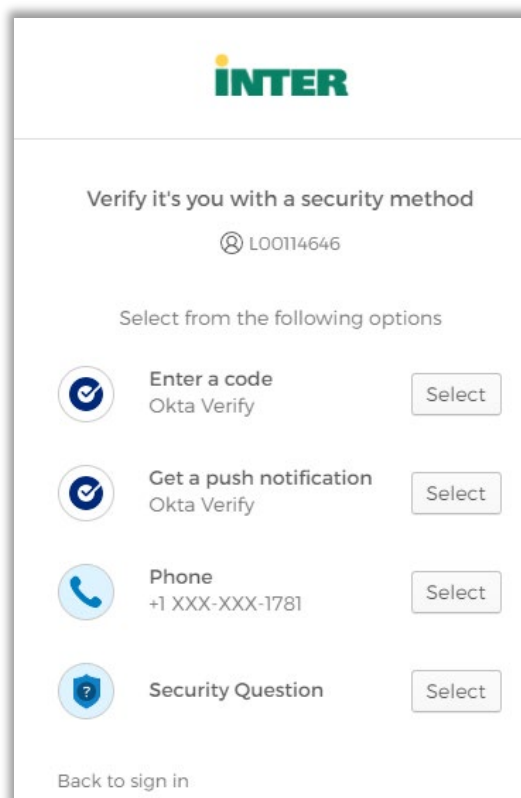


Proceso de autenticación a Banner Administrativo

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.

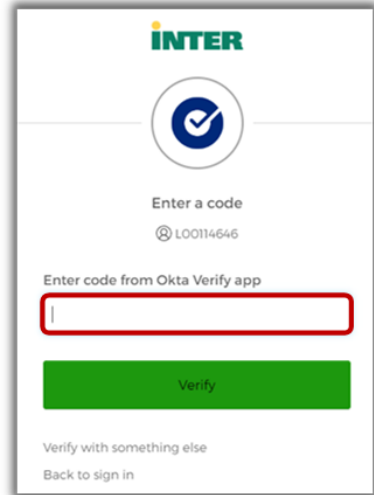


Al presionar el botón titulado Sign in, su solicitud de acceso será redirigida a la plataforma Okta, quien maneja los factores de autenticación que usted configuró previamente. Okta presentará la lista de los factores configurados para que usted se autentique utilizando el de su preferencia.



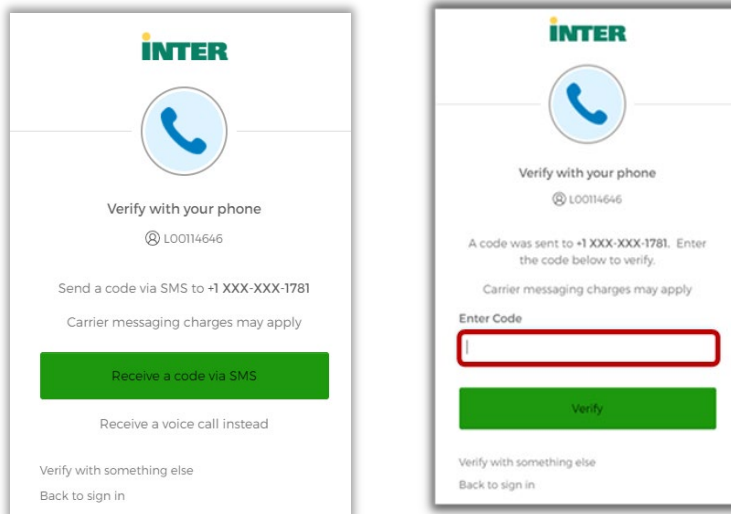
Okta Verify

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.

The image shows the Okta Verify app interface. At the top is the 'INTER' logo. Below it is a circular icon with a checkmark. The text 'Enter a code' is displayed, followed by a small icon and the text 'L00114646'. Below this is a text input field with the placeholder 'Enter code from Okta Verify app'. A red rectangular box highlights this input field. Below the input field is a green button labeled 'Verify'. At the bottom, there are two links: 'Verify with something else' and 'Back to sign in'.

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.

The image shows two screens of the phone verification process. The left screen has the 'INTER' logo and a phone icon. It says 'Verify with your phone' and 'L00114646'. Below that, it says 'Send a code via SMS to +1 XXX-XXX-1781' and 'Carrier messaging charges may apply'. There is a green button labeled 'Receive a code via SMS'. Below that, it says 'Receive a voice call instead'. At the bottom, there are two links: 'Verify with something else' and 'Back to sign in'. The right screen also has the 'INTER' logo and a phone icon. It says 'Verify with your phone' and 'L00114646'. Below that, it says 'A code was sent to +1 XXX-XXX-1781. Enter the code below to verify.' and 'Carrier messaging charges may apply'. There is a text input field with the placeholder 'Enter Code'. A red rectangular box highlights this input field. Below the input field is a green button labeled 'Verify'. At the bottom, there are two links: 'Verify with something else' and 'Back to sign in'.

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.