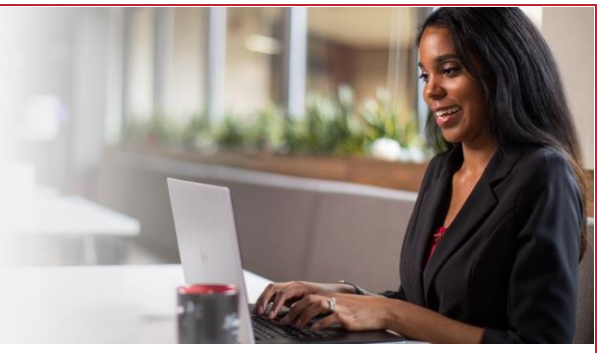
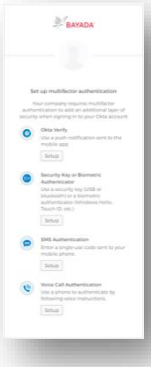


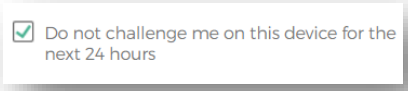
Configuración de autenticación multifactor (MFA) de Okta



Elementos requeridos

- Dispositivo con conexión a Internet (computadora o smartpad)
  Teléfono celular inteligente (smartphone)

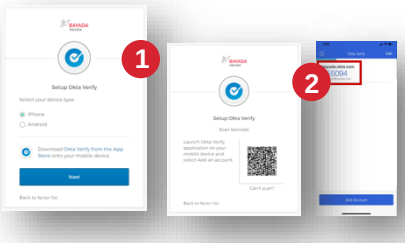
Una vez que se le haya habilitado la autenticación multifactor (Multifactor Authentication), se le pedirá que configure sus factores. Se le pedirá que complete el desafío de autenticación una vez al día y cuando acceda a las aplicaciones seguras. Asegúrese de marcar esta casilla para que no le aparezca el desafío cada vez que inicie sesión.



Recomendamos configurar la MFA por anticipado; para esto, ingrese en **Settings** (configuración) > **Extra Verification** (verificación extra), elija una o más opciones de la lista a continuación y siga las instrucciones paso a paso.

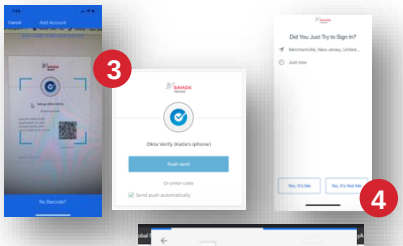
Acerca de Okta Verify

Nota: Recomendamos encarecidamente descargar Okta Verify en su dispositivo inteligente e inscribirse tanto para Okta Verify como para SMS.



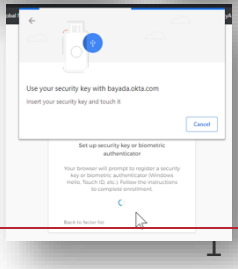
Pasos:

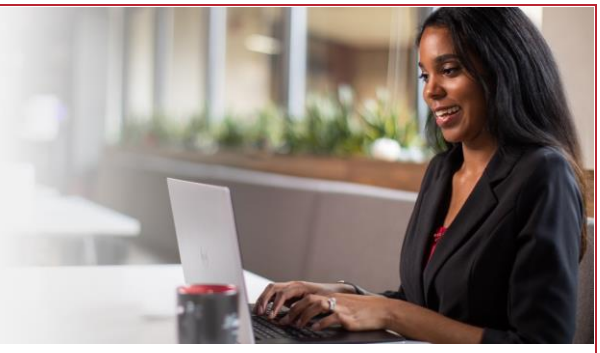
1. Seleccione el tipo de su dispositivo y descargue Okta Verify si no lo hizo todavía.
2. Inicie la aplicación Okta Verify y seleccione *Add Account* (agregar una cuenta).
3. Escanee el código de barras con su dispositivo inteligente o seleccione *Can't Scan?*(¿no puede escanear?) para ingresar un código.
4. Ahora su cuenta está configurada con MFA. A partir de ahora, se le presentarán dos opciones para verificar su identidad:
   - Se enviará una notificación push a su dispositivo, a la que puede responder haciendo clic en *Yes, It's Me* (Sí, soy yo).
   - Seleccione *Or enter code* (o ingresar código) e ingrese el código que reciba por mensaje de texto (SMS) de parte de Okta.
   -



Acerca de la clave de seguridad o la autenticación biométrica

Esta opción usa una parte de su cuerpo (huella digital, reconocimiento facial, escaneo de iris) o una clave física (pequeño dispositivo USB que puede llevar con usted) para verificar su identidad (p. ej., Touch ID, Windows Hello o YubiKey).



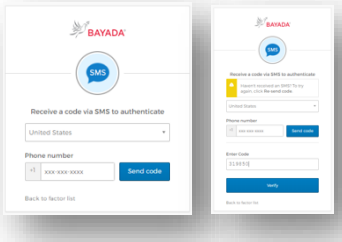


Hoy en día, los usuarios con dispositivos que cuentan con TouchID pueden aprovechar esta función. Planeamos habilitar más dispositivos en un futuro cercano.

Siga las instrucciones de la pantalla.

Acerca de la autenticación por mensaje de texto SMS

SMS es la sigla de servicio de mensajes breves (short message service). Quizá conozca el término por los textos en su teléfono celular. **Recomendamos encarecidamente que se inscriba para autenticación por SMS.**

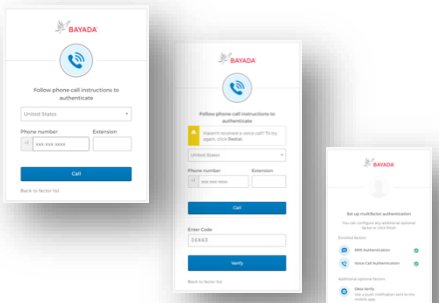


Pasos:

1. Ingrese los 10 dígitos de su número de teléfono celular.
2. Haga clic en *Send Code* (enviar código).
3. Ingrese el código de verificación de seis dígitos que se le envío por texto a su teléfono celular.
4. Haga clic en *Verify* (verificar).

Acerca de la autenticación por llamada de voz

La autenticación por llamada de voz funciona de manera similar a la autenticación por SMS, pero en lugar de recibir un mensaje de texto, recibe una llamada de voz con un código de seguridad.



Pasos:

1. Ingrese los 10 dígitos de su número de teléfono.
2. Ingrese el código de verificación de cinco dígitos que recibirá en la llamada telefónica.
3. Haga clic en *Verify* (verificar).

Nota: Cuantas más opciones de MFA elija configurar, más segura será su cuenta.

Una vez que haya verificado con éxito su identidad, se le dirigirá a la página de inicio de Okta. Elija *MyApps* para acceder a sus aplicaciones de BAYADA.