

Manual de registro

**Autenticación en
dos factores 2FA**

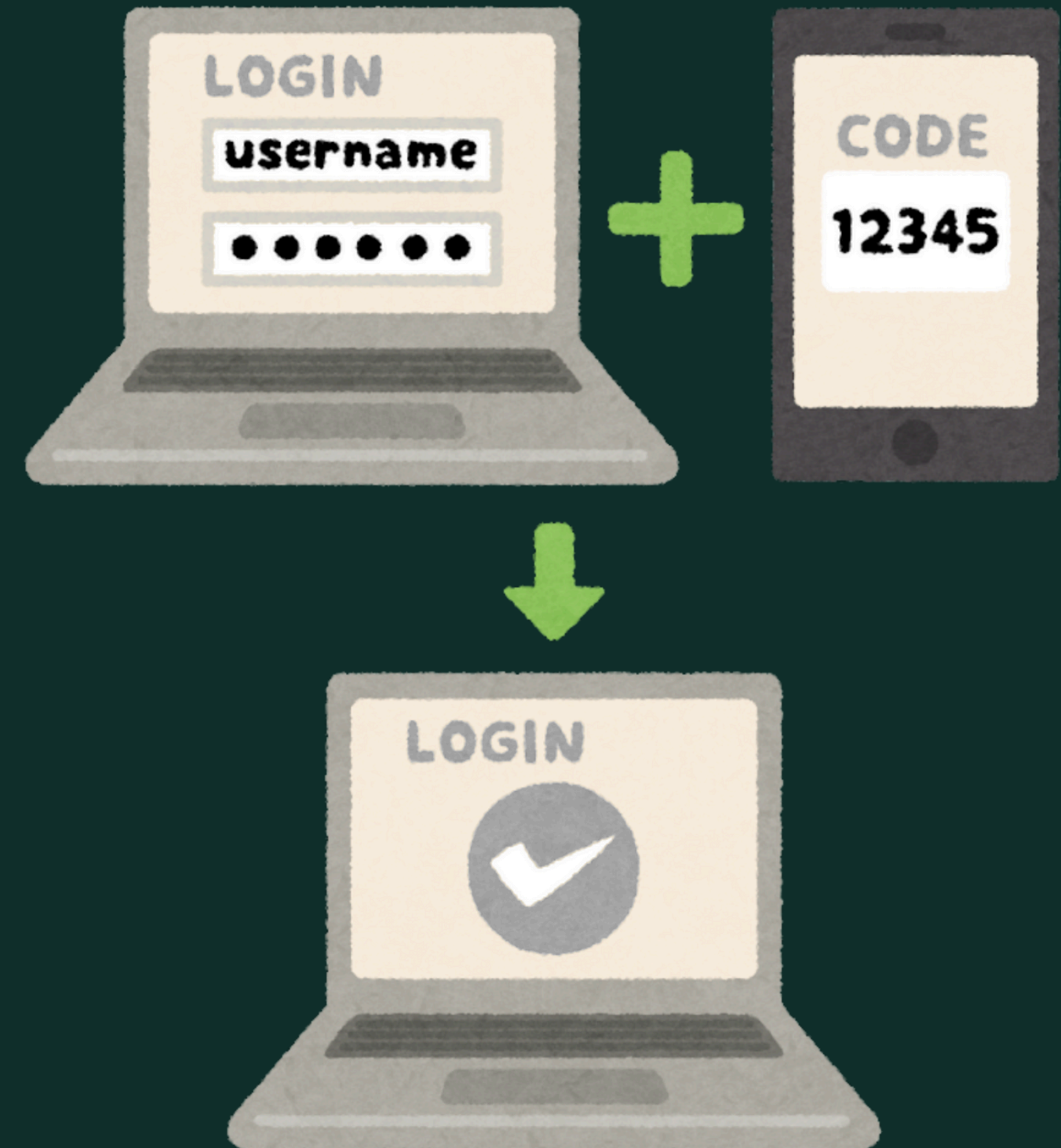
RECOMENDACIONES IMPORTANTES

- Contar con un dispositivo móvil.
- Contar con acceso a internet.
- Contar con usuario y contraseña a cualquiera de las siguientes plataformas: **Aula Virtual, Espacio Educativo, Escuela Pública de Código, Ciberseguridad.**
- Descargar previamente la aplicación de **Google Autentificador** en tu dispositivo móvil.
- ***Es importante no eliminar esta aplicación, ya que será utilizada para generar un código cada determinado tiempo.***



¿QUÉ ES LA AUTENTICACIÓN 2FA?

La Autenticación de Dos Factores (2FA) es un método de seguridad que exige dos formas de identificación diferentes (factores) para verificar tu identidad y darte acceso a una cuenta o sistema, añadiendo una capa extra de protección más allá de solo una contraseña.



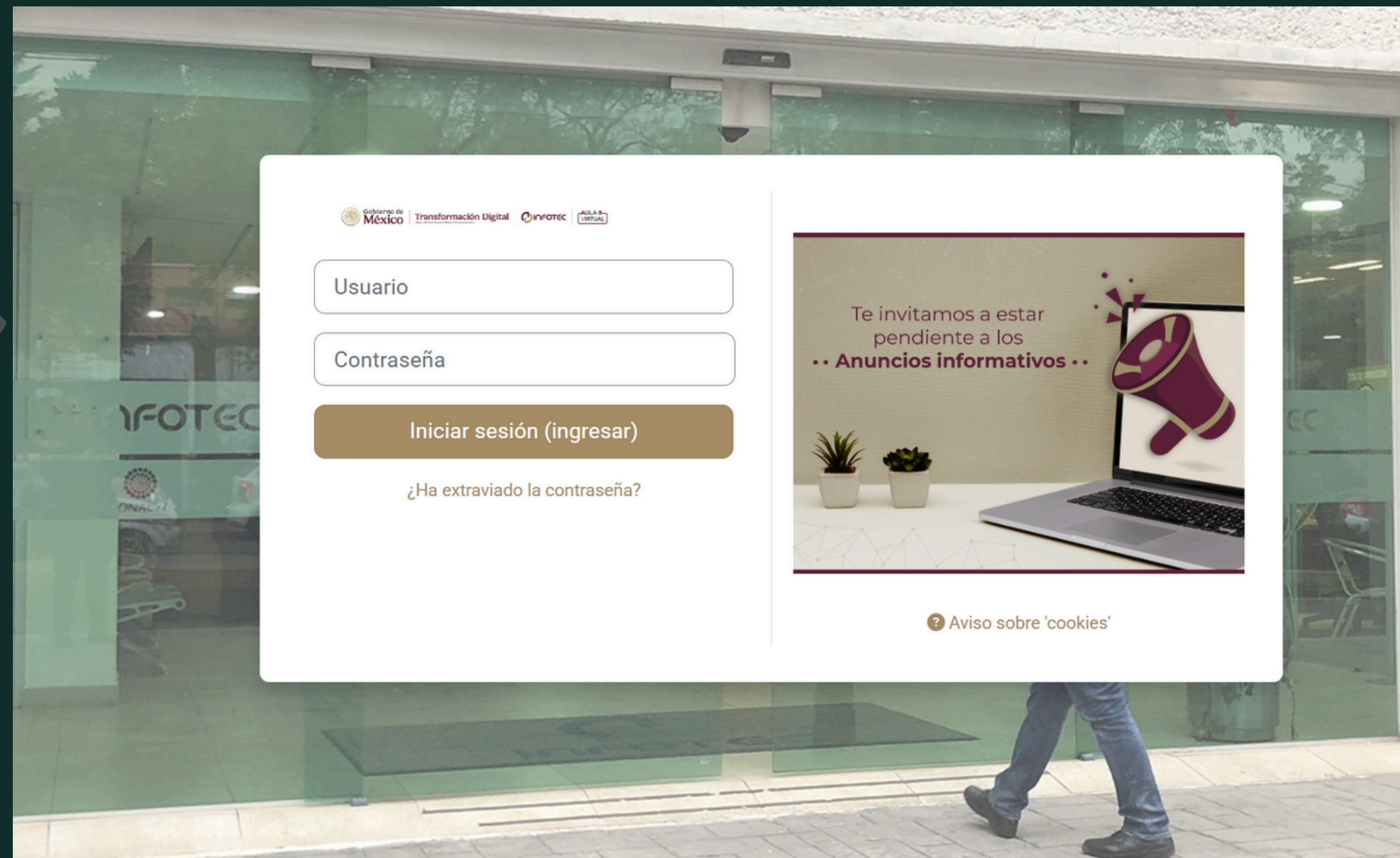
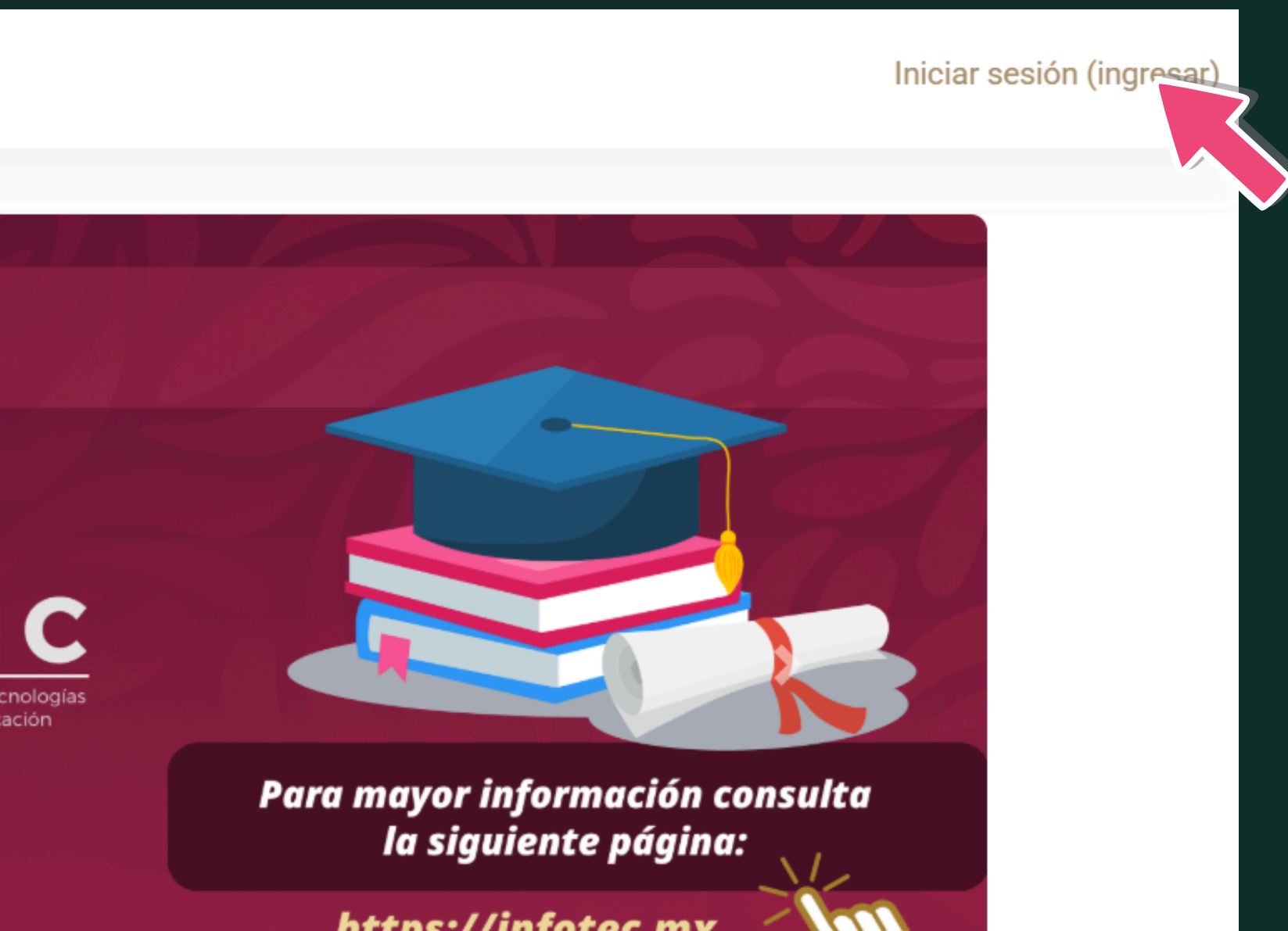
PASO 1: INGRESO A LA PLATAFORMA

Ingresa a la plataforma que sea de tu selección: Aula Virtual, Espacio Educativo, Escuela Pública de Código, Ciberseguridad.



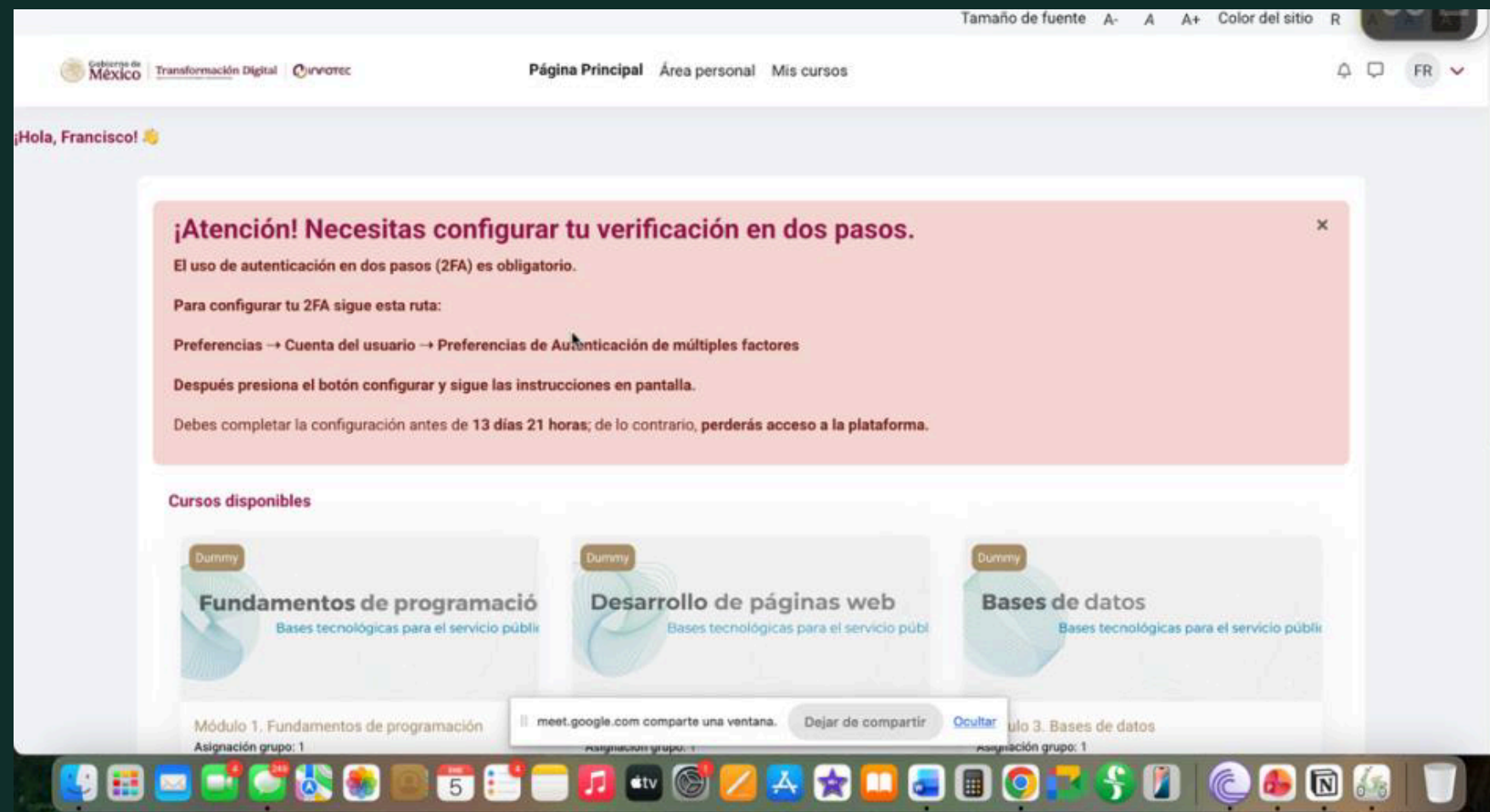
PASO 2: DA CLIC EN ACCEDER

Usa tu usuario y contraseña



PASO 3: MENSAJE DE CONFIGURACIÓN

El sistema nos enviará un mensaje de alerta donde nos indicará que es necesario configurar la verificación en dos pasos. Es importante leerlo cuidadosamente, ya que viene indicado el periodo de gracia restante, así como la ruta que se debe de seguir para realizar dicha configuración



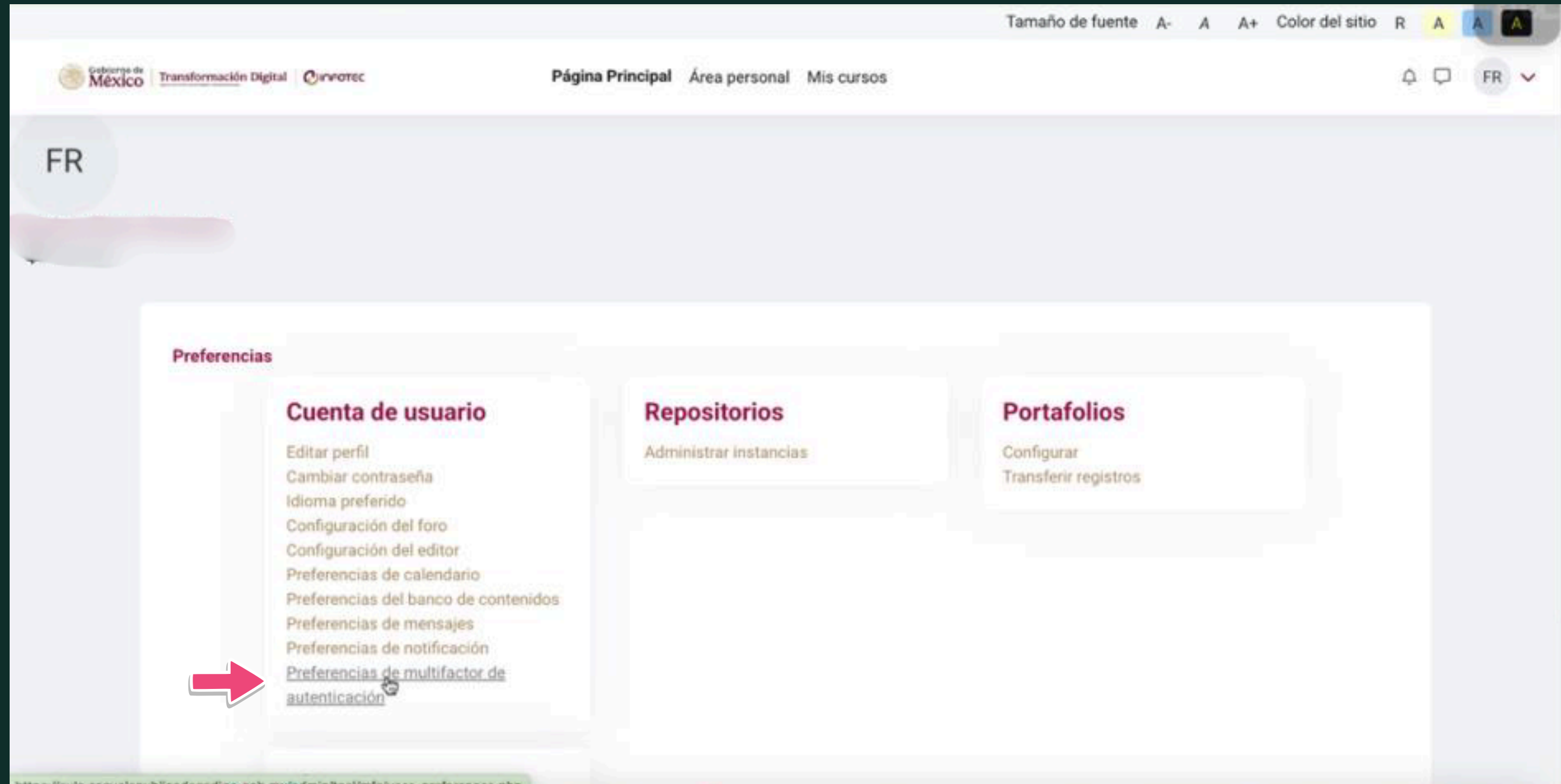
PASO 4: CONFIGURACIÓN DE LA AUTENTIFICACIÓN DE DOS FACTORES (2FA)

A continuación, seguiremos la ruta para la autenticación de nuestro usuario. Para ello damos clic en nuestro nombre de usuario, como se señala en la imagen, y seleccionaremos **Preferencias**



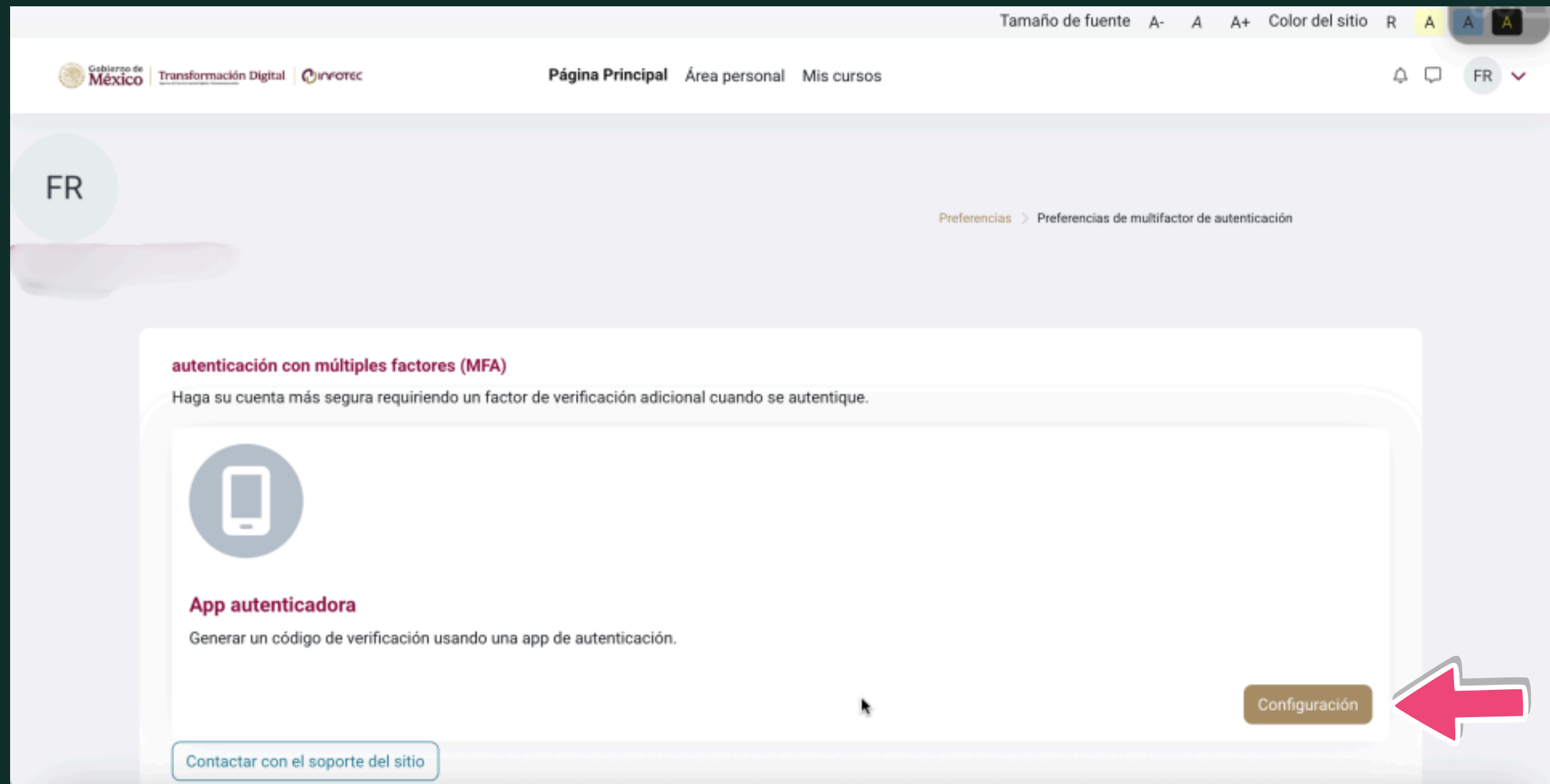
CONFIGURACIÓN DE LA AUTENTIFICACIÓN DE DOS FACTORES (2FA)

Seleccionaremos en **Cuenta de usuario** la opción de **Preferencias de multifactor de autenticación**.



CONFIGURACIÓN DE LA AUTENTIFICACIÓN DE DOS FACTORES (2FA)

El sistema nos enviará a la pantalla principal para empezar a configurar la autenticación con múltiples factores (MFA). Dar clic al botón de **Configuración**.



CONFIGURACIÓN DE LA AUTENTIFICACIÓN DE DOS FACTORES (2FA)

Para poder autenticar, es necesario tener instalada en tu dispositivo móvil la aplicación autenticadora. **Para lo cual te recomendamos utilizar Google Autenticador.**

Configuración de autenticador TOTP

Para configurar este método usted necesita tener un dispositivo con una app de autenticación. Si no tiene ninguna app, puede descargar una. Por ejemplo, 2FAS Auth, FreeOTP, Google Authenticator, Microsoft Authenticator o Twilio Authy.

1. Dé un nombre a su dispositivo.

Nombre del dispositivo

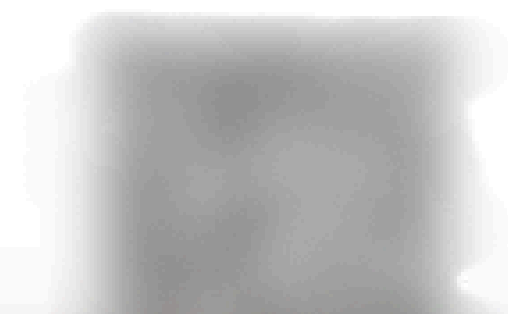


Por ejemplo, "Teléfono"



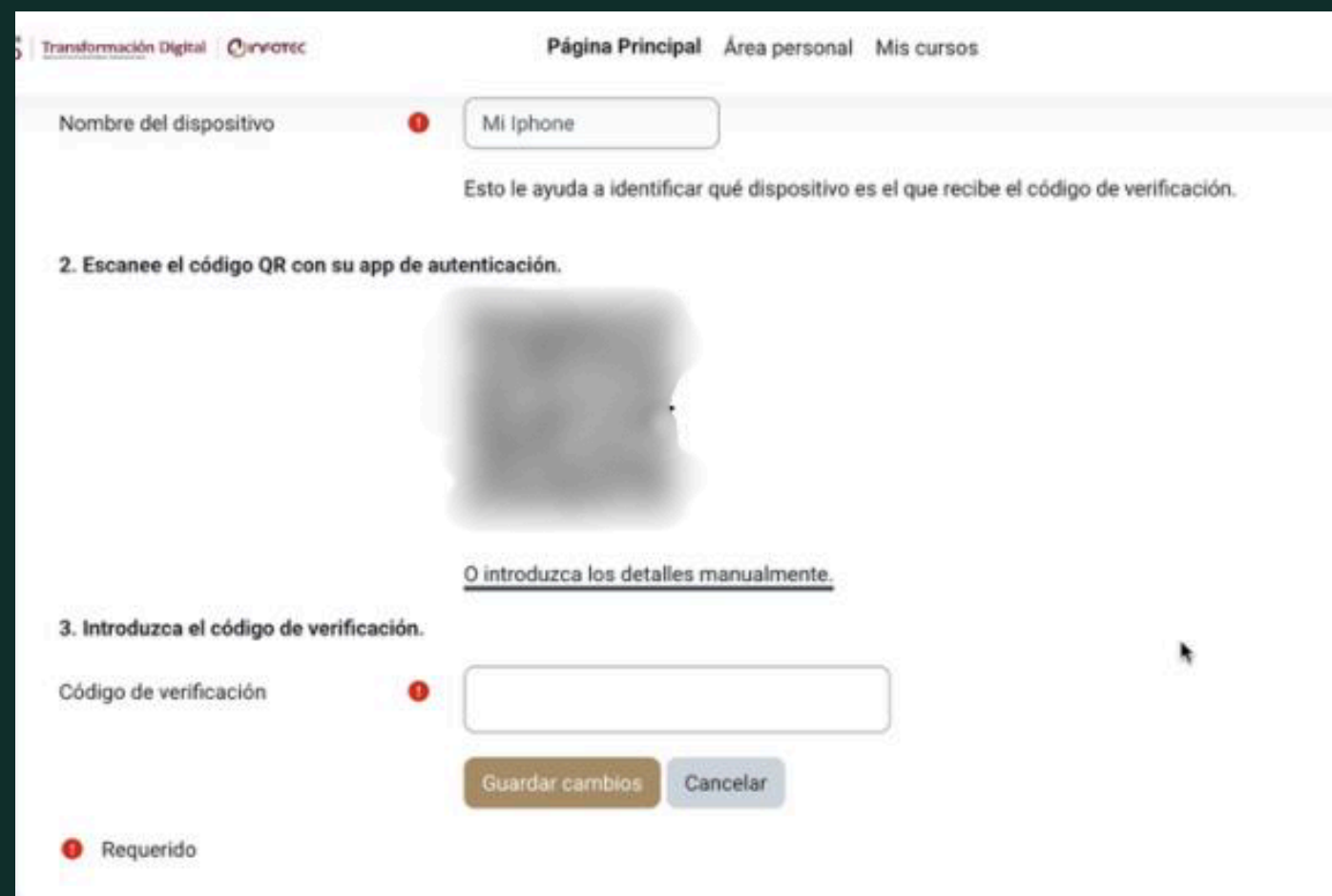
Esto le ayuda a identificar qué dispositivo es el que recibe el código de verificación.

2. Escanee el código QR con su app de autenticación.



PASO 5:

El primer paso es ingresar un nombre corto de tu dispositivo móvil. Por ejemplo “**móvil 1**”.

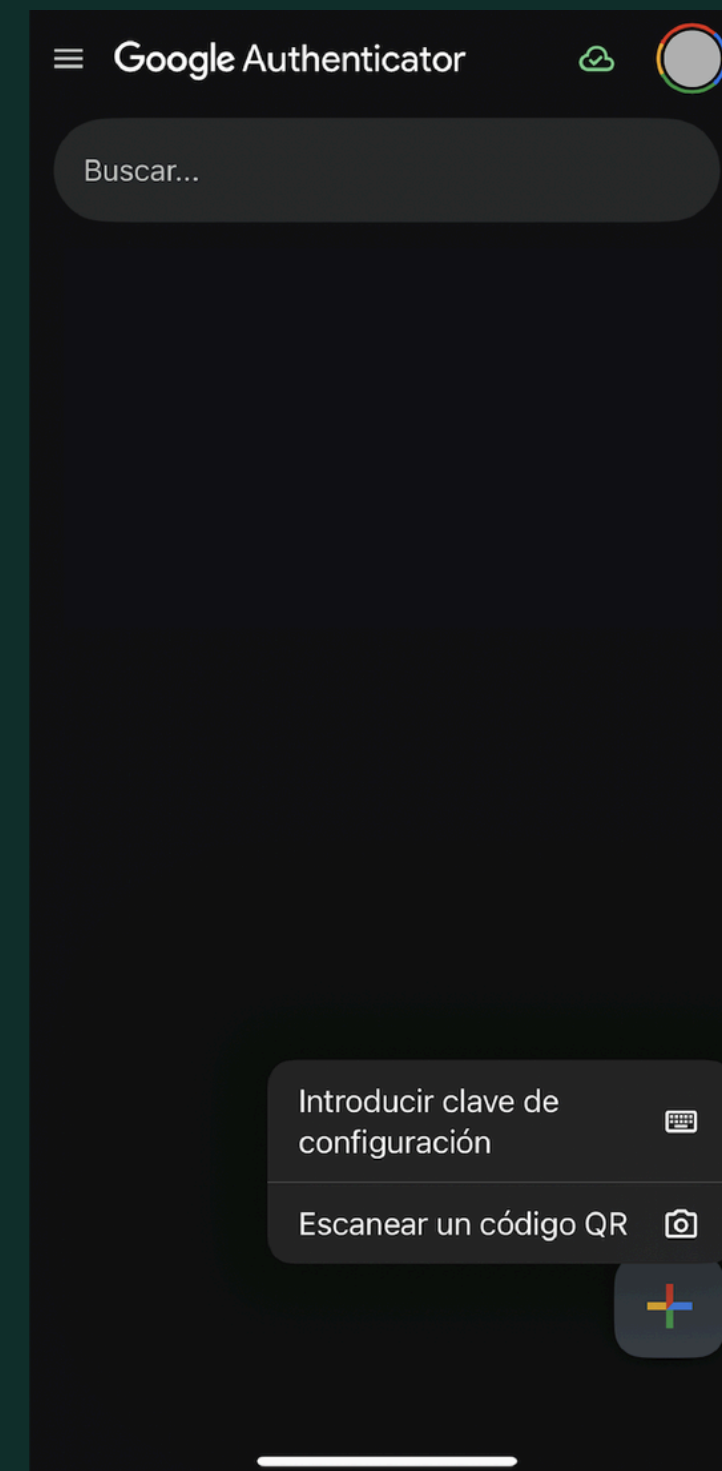


The screenshot shows a web interface for setting up Google Authenticator. At the top, there are tabs for 'Página Principal', 'Área personal', and 'Mis cursos'. Below the tabs, there is a section for 'Nombre del dispositivo' with a text input field containing 'Mi Iphone'. A red information icon is next to the field. Below this, there is a step indicator '2. Escanee el código QR con su app de autenticación.' followed by a QR code. Below the QR code, there is a link 'O introduzca los detalles manualmente.' and a step indicator '3. Introduzca el código de verificación.' followed by a text input field for the verification code. At the bottom, there are two buttons: 'Guardar cambios' and 'Cancelar'. A red required icon is next to the verification code field.

PASO 6:

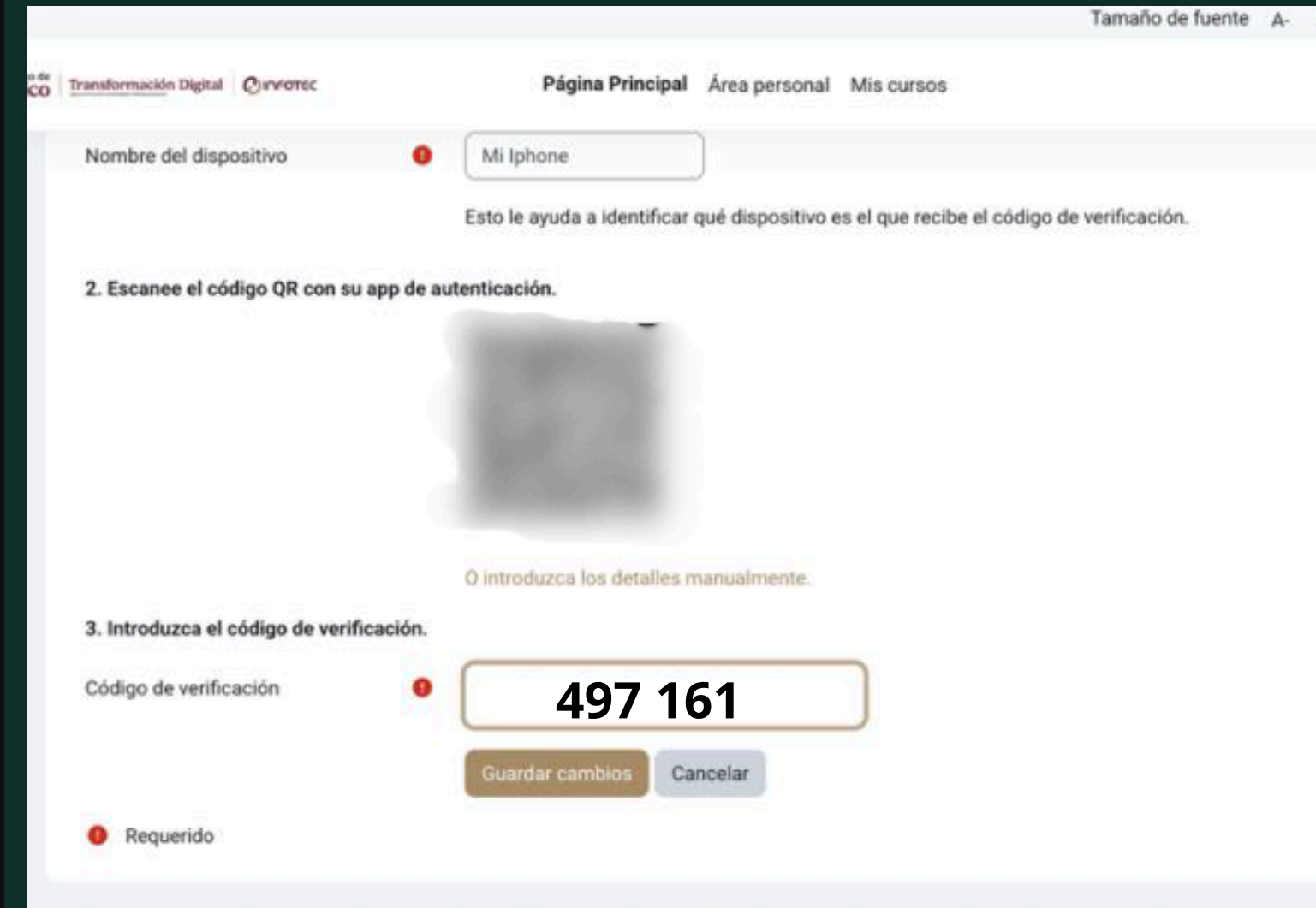
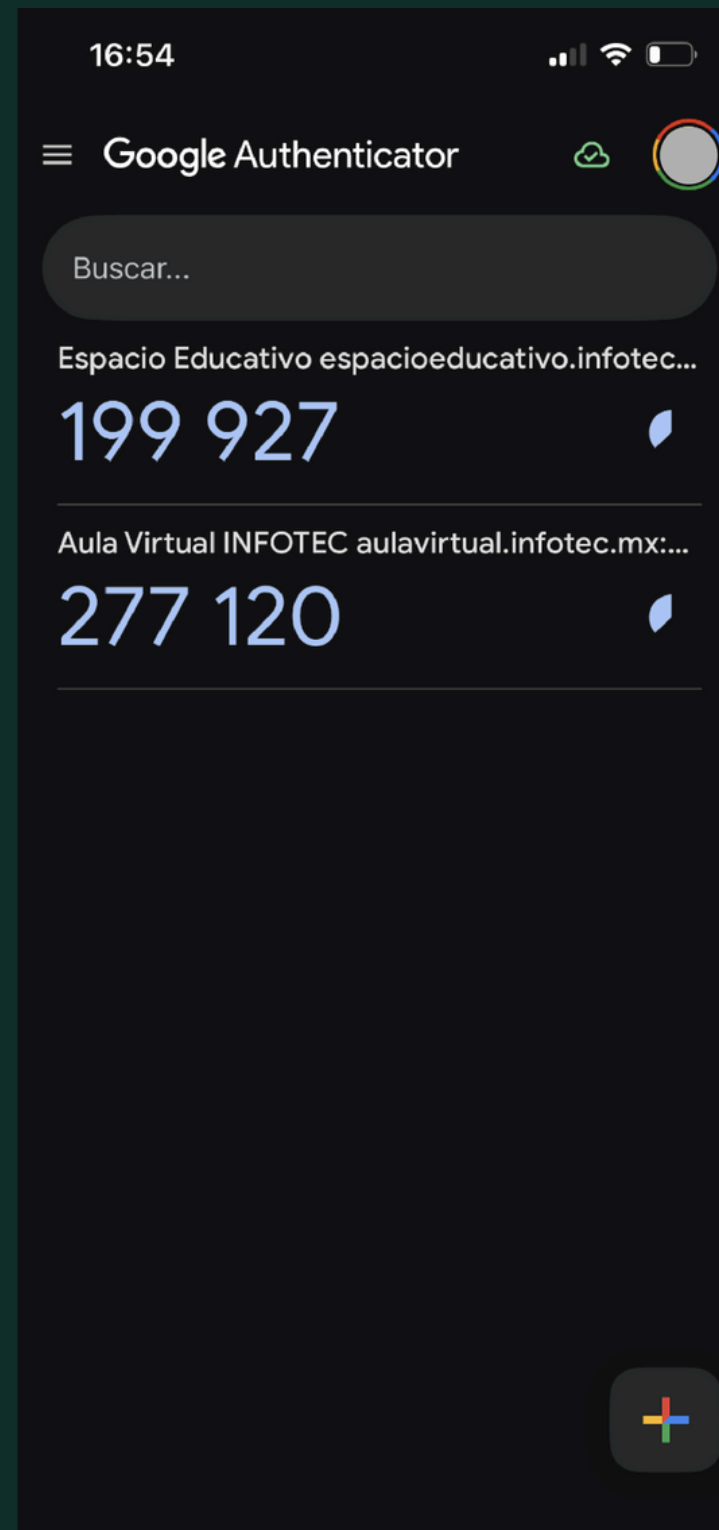
Abrir la aplicación de **Google Authenticator**.

- Selecciona el ícono de más y escanea el código QR de la plataforma.



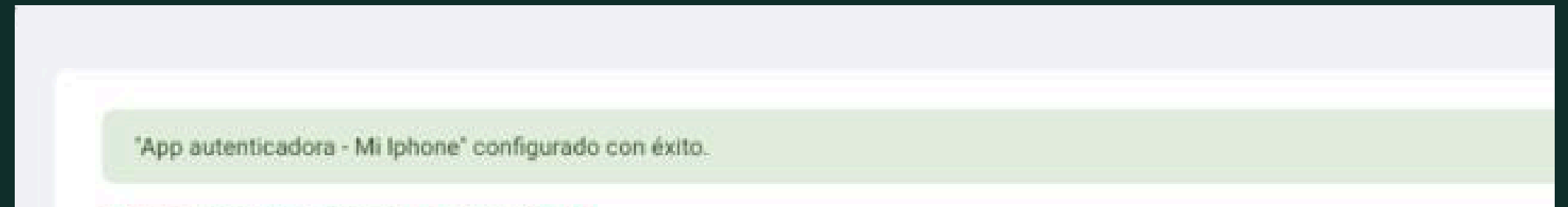
PASO 7:

La aplicación nos mostrará el código de verificación, el cual, ingresaremos en la sección de “**Código de verificación**” en tu plataforma. Dar clic en **Guardar cambios**.



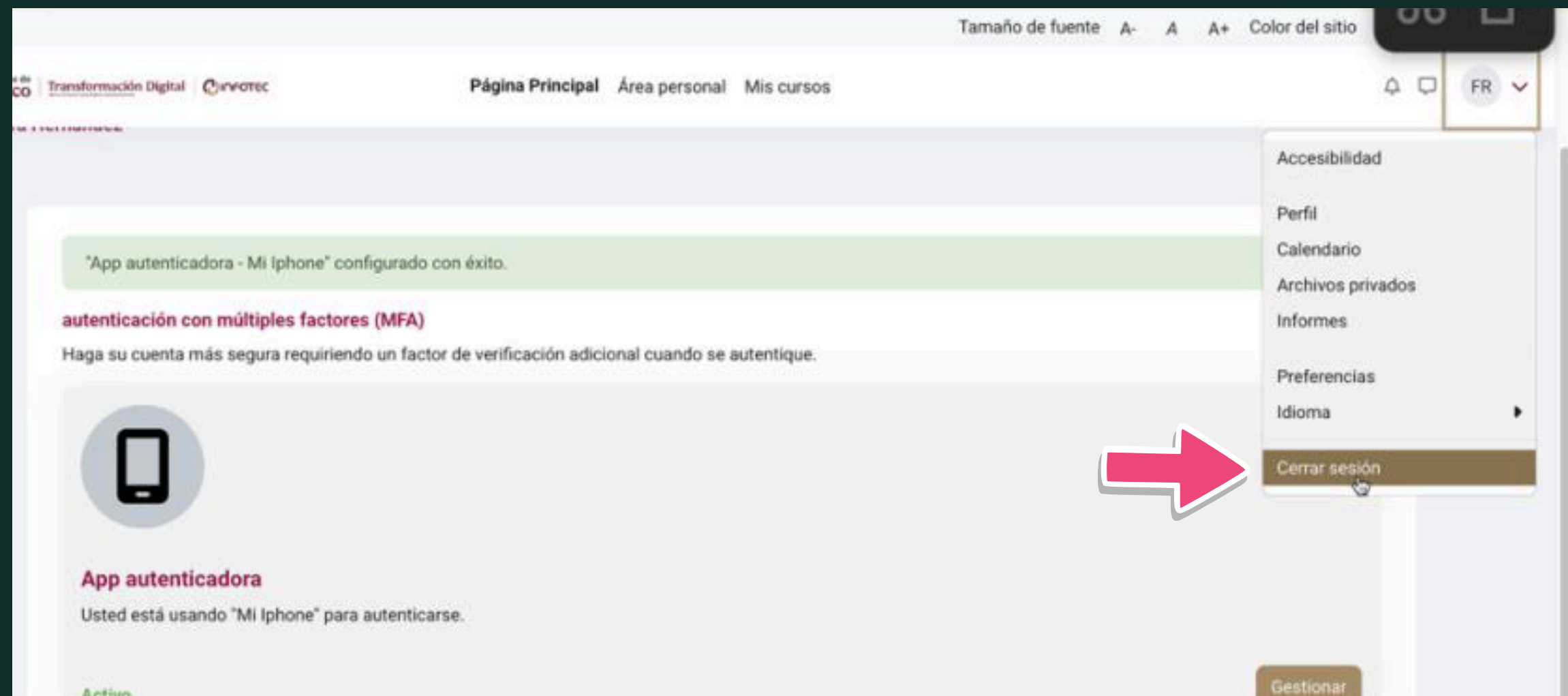
PASO 8:

Enseguida el sistema nos enviará un mensaje de que el dispositivo se ha configurado con éxito



PASO 9:

Para validar que la autenticación en dos pasos funciona de manera correcta cerraremos sesión y volveremos a entrar



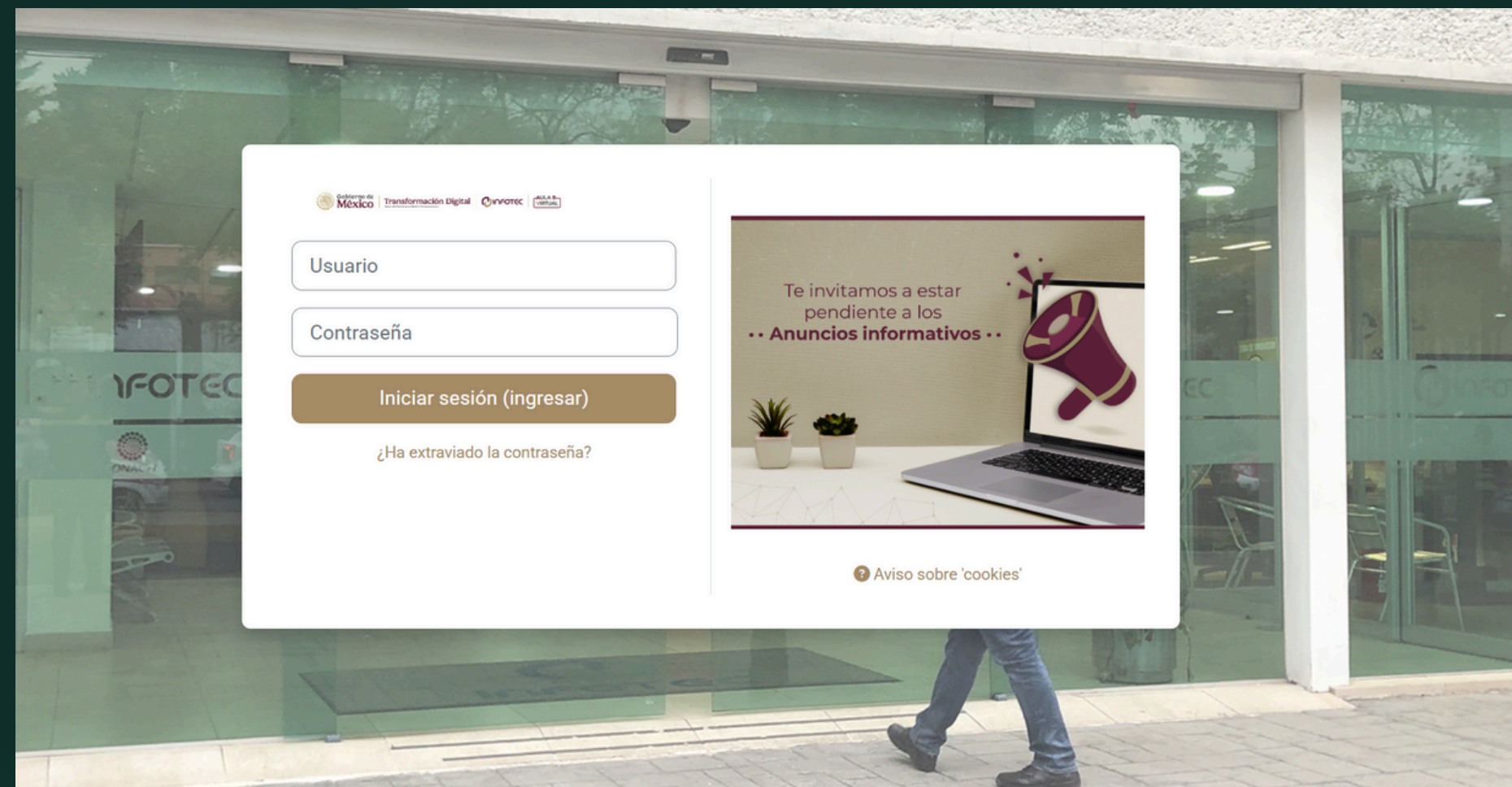
PASO 10:

Volvemos a ingresar a la URL de la plataforma seleccionada.



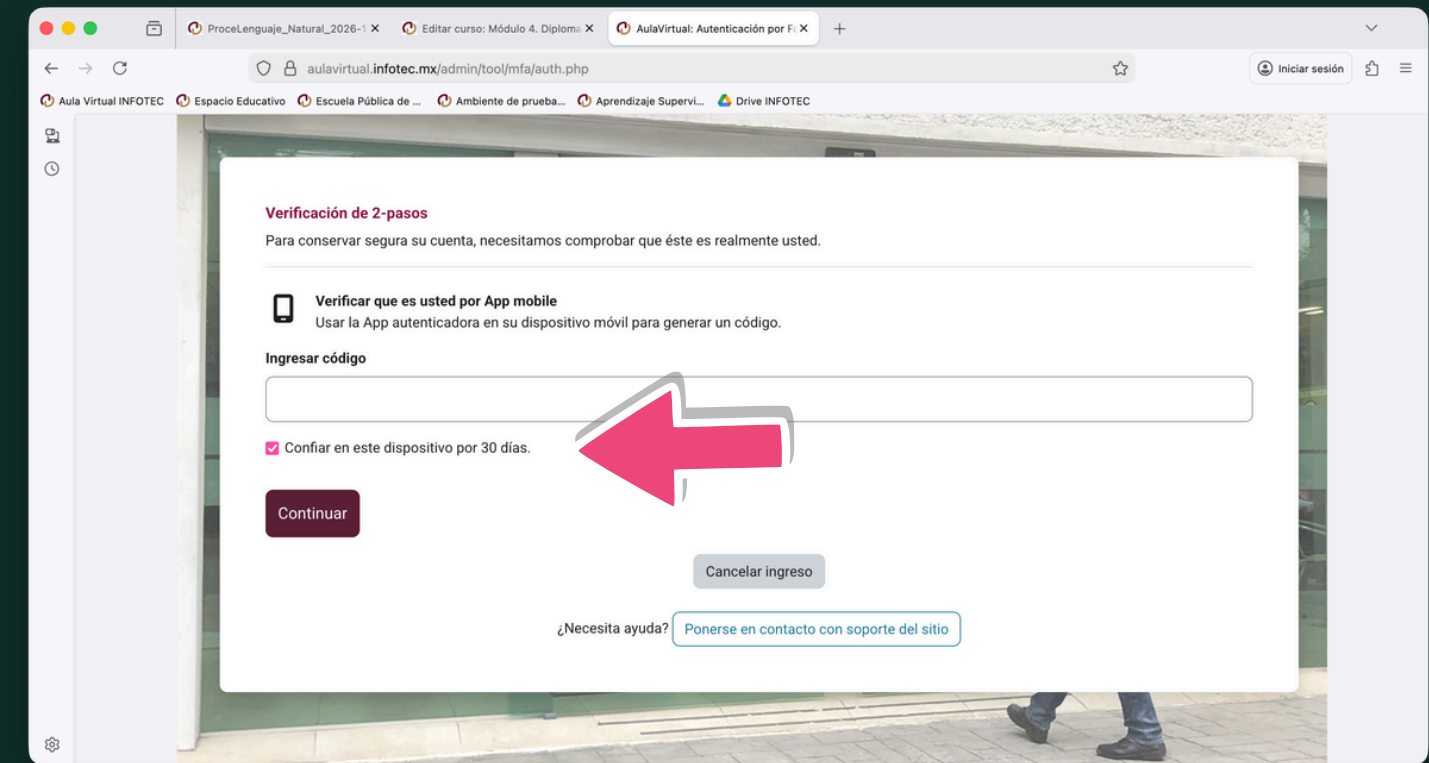
PASO 11:

Accedemos con nuestras credenciales



PASO 12:

El sistema nos pedirá el código de la autenticación en dos pasos. Es importante marcar la casilla de **Confiar en este dispositivo por 30 días**.



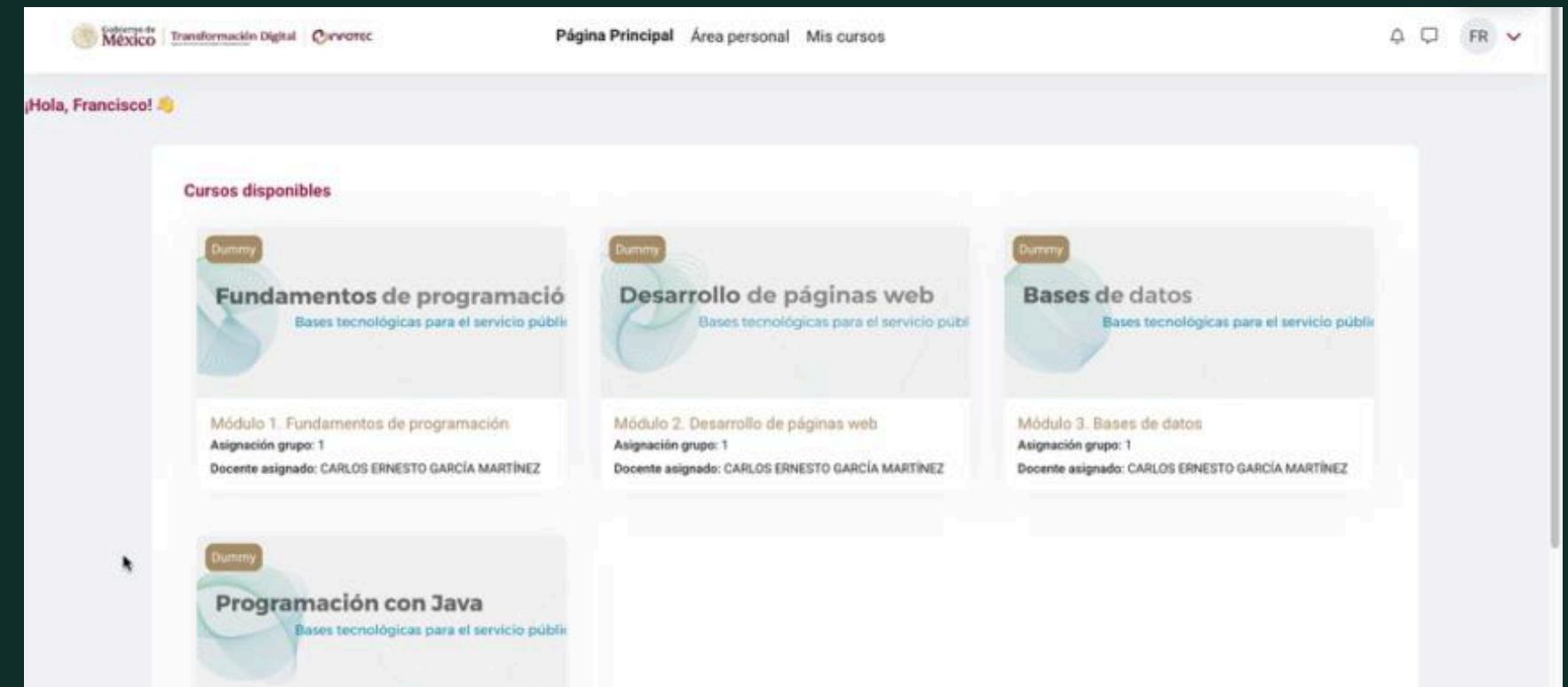
PASO 13:

Abrimos nuestra aplicación de **Google Autenticador** en nuestro móvil para generar un nuevo código el cual debemos colocar en el espacio de **Introducir código**.

Nota: es importante considerar que el código es visible durante 30 segundos” y pasado este tiempo nos generara uno nuevo*

PASO 14:

Una vez autenticados el sistema nos permitirá el ingreso de manera correcta



PASO 15: CONSIDERACIONES IMPORTANTES

- El sistema tiene un contador de intentos fallidos, si se ingresa varias veces con un código erróneo se bloqueará tu cuenta.
- Tendrás 30 días para poder utilizar un dispositivo de confianza, después de ese periodo de tiempo tendrás que volver a ingresar un nuevo código de verificación.

El sistema también tiene un contador de intentos fallidos



Verificación en 2 pasos
Para mantener segura su cuenta, necesitamos confirmar que realmente es usted.

 **Verificar que es usted mediante app móvil**
Use la app de autenticación de su dispositivo móvil para generar un código.

Introducir código

Código de verificación incorrecto Le quedan aún 9 intentos.

[Continuar](#)

[Cancelar autenticación](#)

[¿Necesita ayuda?](#) [Contactar con el soporte del sitio](#)