



GUÍA DE CONFIGURACIÓN DEL DOBLE FACTOR DE AUTENTICACIÓN PARA EL ACCESO A LOS SISTEMAS DE INFORMACIÓN DE UNIVERSITAS XXI STU

1. INSTALACIÓN DE APLICACIÓN DE AUTENTICACIÓN

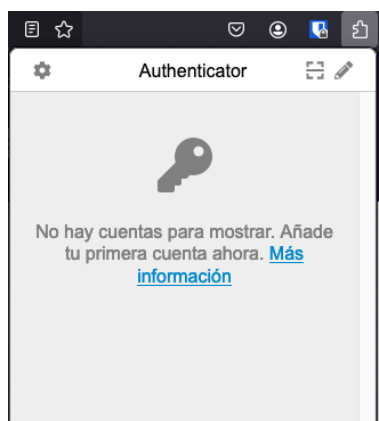
El primer paso que se debe realizar, si no se ha hecho previamente, es instalar la aplicación que permitirá el registro y generación del código de doble factor de autenticación. Desde UNIVERSITAS XXI STU, se recomienda la instalación de **Microsoft Authenticator** en un dispositivo móvil (aplicación gratuita disponible en las tiendas Google Play o App Store). Se puede obtener más información en la URL: <https://www.microsoft.com/es-es/security/mobile-authenticator-app>

Si la universidad ya está utilizando otra aplicación de autenticación de doble factor para el acceso a sus sistemas de información, es posible que no sea necesario realizar esta instalación porque sea compatible con las contraseñas de un solo uso (*OTP, One Time Password*) de Microsoft.

Si se opta por no instalar la aplicación en un dispositivo móvil, se puede realizar la instalación de una extensión en los navegadores compatibles: Microsoft Edge, Google Chrome, Mozilla Firefox o Safari. Se puede obtener más información sobre esta extensión en la URL: <https://github.com/Authenticator-Extension/Authenticator?tab=readme-ov-file>. Está disponible en las diferentes tiendas de extensiones de forma gratuita:

 Get it from Microsoft	https://microsoftedge.microsoft.com/addons/detail/ocglkepbibnabgmbachknglpdipecio
 Available in the Chrome Web Store	https://chrome.google.com/webstore/detail/authenticator/bhghoaamapcdpbohphigoooaddinpkbai
 Firefox Add-ons	https://addons.mozilla.org/en-US/firefox/addon/auth-helper
 Download on the App Store	https://apps.apple.com/us/app/authen/id1602945200

Una vez instalada la extensión en el navegador, aparecerá una nueva opción junto a la barra de dirección similar a la que se muestra en esta imagen:





2. REGISTRO DEL DOBLE FACTOR ASOCIADO A LA CUENTA DE ACCESO

En el primer acceso que se realice a los sistemas de información de UNIVERSITAS XXI STU, se solicitará la configuración de la contraseña de un solo uso que actuará como doble factor de autenticación. A continuación, se muestran los pasos a seguir para completar satisfactoriamente este proceso:

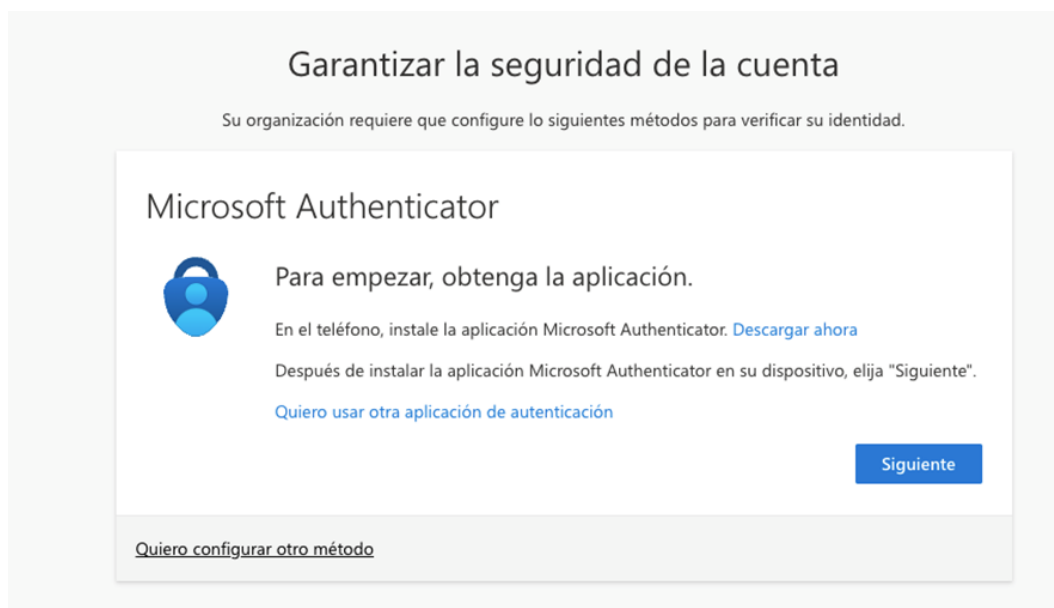
1. Abrir en el navegador web la URL de acceso a la aplicación. Por ejemplo: <https://qxxi.universitasxxi.com>. Se mostrará una ventana para introducir el nombre de usuario de la cuenta de acceso que utilices habitualmente, **seguido de una arroba (@) y el dominio ext.universitasxxi.com**, tal como se muestra en la imagen:

2. Tras pulsar en **Siguiente**, te solicitará tu contraseña habitual de acceso:

3. Una vez introducida una contraseña válida para el inicio de sesión, te indicará que se **necesita más información** para garantizar la seguridad de la cuenta y comenzará el proceso de registro:



4. A continuación, aparecerá la siguiente pantalla:



5. Si vas a utilizar la aplicación **Microsoft Authenticator**, puedes pulsar **Siguiente**. Si vas a utilizar otra aplicación de autenticación que ya vengas utilizando en tu universidad o vas a utilizar la extensión del navegador web, pulsa en **“Quiero usar otra aplicación de autenticación”** y ve al paso **13** de esta guía.
6. Cuando has pulsado **Siguiente**, te aparecerá una pantalla como esta. Selecciona en ella **“Aplicación móvil”** como método de contacto y **“Recibir notificaciones para verificación”** como uso de la aplicación móvil:



Comprobación de seguridad adicional

Proteja su cuenta agregando más comprobación de teléfono a su contraseña. Ver vídeo para saber cómo proteger su cuenta

Paso 1: ¿De qué manera deberíamos ponernos en contacto con usted?

Aplicación móvil

¿Cómo quiere usar la aplicación móvil?

☒ Recibir notificaciones para verificación

☐ Usar código de verificación

Para usar estos métodos de comprobación, debe configurar la aplicación Microsoft Authenticator.

Configurar

Configure la aplicación móvil.

Siguiente

- Una vez seleccionadas ambas opciones, pulsa sobre **Configurar**. Aparecerá una pantalla como la siguiente, con un código QR que tendrás que escanear desde la aplicación móvil de Microsoft Authenticator (los datos que mostramos aquí son de ejemplo, debes escanear el código que aparezca en tu pantalla):

Configurar aplicación móvil

Complete los pasos siguientes para configurar su aplicación móvil.

1. Instale la aplicación Microsoft Authenticator para Windows Phone, Android o iOS.
2. En la aplicación, agregue una cuenta y seleccione "Cuenta profesional o educativa".
3. Examine la imagen siguiente.



Si no puede examinar la imagen, especifique la información siguiente en la aplicación.

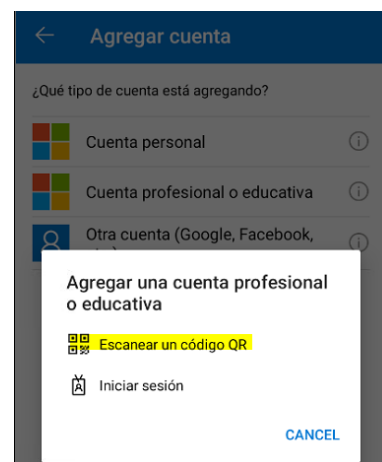
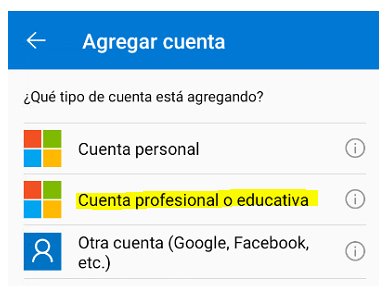
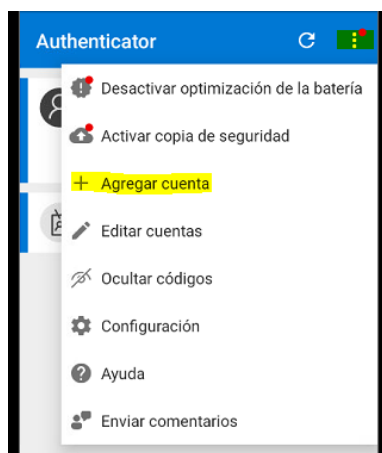
Código: 439 783 404

Dirección URL: <https://mobileappcommunicator.auth.microsoft.com/mac/MobileAppCommunicator.svc/965418155>

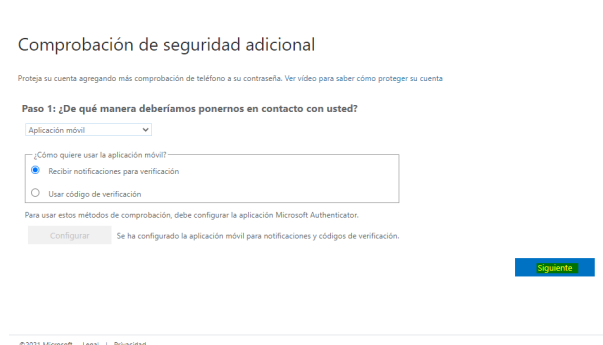
Si la aplicación muestra un código de seis dígitos, elija "Siguiente".

Siguiente cancelar

- Para escanear el código QR, abre Microsoft Authenticator en tu dispositivo móvil, selecciona **" + Agregar cuenta "** desde el menú de opciones, elige **"Cuenta profesional o educativa"** y, a continuación, **"Escanear un código QR"** (si el dispositivo móvil te solicita permisos en la aplicación para acceder a la cámara, concédeselos):



9. Cuando el dispositivo móvil nos indique que ha añadido la cuenta correctamente, ya se puede pulsar en el botón **Siguiente** en las pantallas anteriores:



10. Antes de finalizar la configuración, el proceso comprueba que el registro ha sido correcto enviando una notificación al dispositivo móvil. Puede ser una simple notificación de aprobación o que solicite la introducción de un número que aparece en pantalla. Aprueba la solicitud de acceso y la aplicación de autenticación habrá quedado correctamente registrada:



Comprobación de seguridad adicional

Proteja su cuenta agregando más comprobación de teléfono a su contraseña. [Ver vídeo para saber cómo proteger su cuenta](#)

Paso 2: asegurarse de que podemos comunicarnos con usted a través del dispositivo con aplicaciones móviles



Responda a la notificación en su dispositivo.

Siguiente

11. Como método alternativo y para poder iniciar sesión en caso de que se haya perdido el acceso a la aplicación de autenticación (se haya desinstalado por error, por ejemplo), se solicita la aportación de un número de teléfono. UNIVERSITAS XXI STU **nunca utilizará este número de teléfono** para ponerse en contacto contigo (salvo autorización expresa), ni enviarte ningún tipo de información, **sólo se utilizará** cuando necesites recibir un SMS para poder conectarte a nuestros sistemas de información:

Comprobación de seguridad adicional

Proteja su cuenta agregando más comprobación de teléfono a su contraseña. [Ver vídeo para saber cómo proteger su cuenta](#)

Paso 3: En el caso de que haya perdido el acceso a la aplicación móvil

España (+34)

Siguiente

Sus números de teléfono sólo se usarán para proteger su cuenta. Se aplicará la tarifa estándar de teléfono y SMS.

12. Después del último paso, ya no tendrás que hacer nada más. Sólo pulsar en **Listo** y el proceso de registro habrá finalizado:



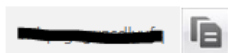
Comprobación de seguridad adicional

Proteja su cuenta agregando más comprobación de teléfono a su contraseña. [Ver vídeo para saber cómo proteger su cuenta](#)

Paso 4: Siga usando las aplicaciones existentes

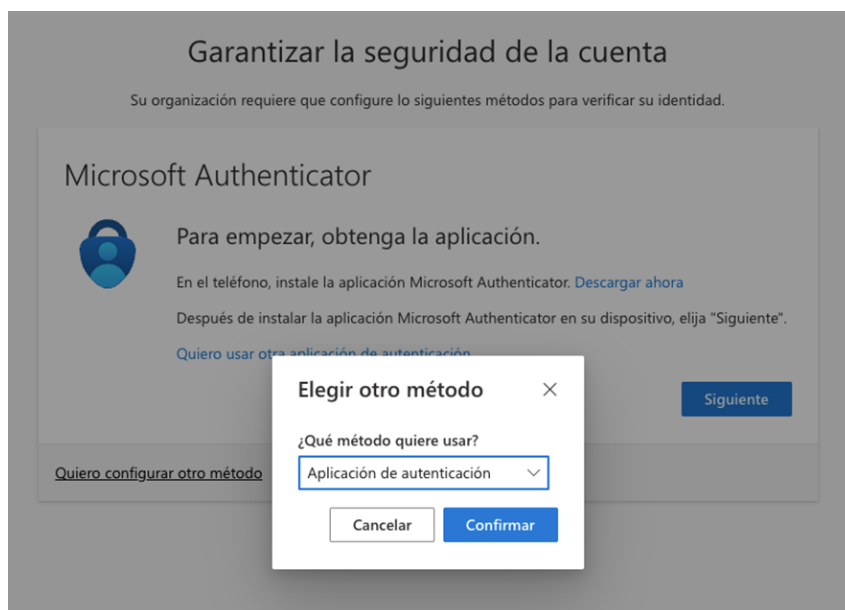
En algunas aplicaciones, como Outlook, Apple Mail y Microsoft Office, no puede usar un teléfono para proteger su cuenta. Para usar estas aplicaciones, tendrá que crear una nueva "contraseña de aplicación" para usarla en lugar de la contraseña de su cuenta profesional o educativa. [Más información](#)

Empiece con esta contraseña de la aplicación:



Listo

13. Si habías elegido la configuración de Microsoft Authenticator, ya has terminado la guía de configuración. A partir de este punto, se indican las instrucciones para configurar la extensión del navegador. Cuando se ha seleccionado **"Quiero usar otra aplicación de autenticación"**, aparecerá una pantalla como la siguiente. Elige como método **Aplicación de autenticación**:



14. Después de pulsar en **Continuar**, comenzará el proceso de registro de la otra aplicación de autenticación. El proceso es similar al de Microsoft Authenticator. Lo primero que solicitará es que se cree una nueva cuenta en la aplicación de autenticación y después se pulse en **Siguiente**. En el caso de la extensión del navegador, **no hay que crear** la cuenta primero, sólo pulsar en **Siguiente**:



Garantizar la seguridad de la cuenta

Su organización requiere que configure lo siguientes métodos para verificar su identidad.

Aplicación de autenticación



Configuración de la cuenta

En la aplicación, agregue una cuenta nueva.

[Quiero configurar otro método](#)

[Atrás](#) [Siguiente](#)

15. A continuación, se presentará un código QR que es el que tienes que registrar con la extensión del navegador. El que se muestra a continuación es de ejemplo, el que sirve es el que te aparezca en tu pantalla:

Garantizar la seguridad de la cuenta

Su organización requiere que configure lo siguientes métodos para verificar su identidad.

Aplicación de autenticación

Digitalización del código QR

Use la aplicación de autenticación para escanear el código QR. Así, la aplicación de autenticación y la cuenta quedarán emparejadas.

Después de escanear el código QR, elija "Siguiente".

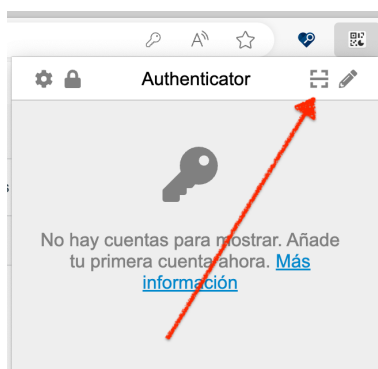


[¿No puede escanear la imagen?](#)

[Atrás](#) [Siguiente](#)

[Quiero configurar otro método](#)

16. La extensión del navegador permite la captura del código QR mediante la selección de este en la pantalla. Para ello, pulsa en el icono de la extensión del navegador y pulsa en el icono de escanear QR. La pantalla se oscurecerá un poco y tendrás que seleccionar un cuadrado que abarque el código QR mostrado en la pantalla. Automáticamente, se añadirá la cuenta en la extensión del navegador:



17. Si, por cualquier motivo, la captura del código QR no funcionase, se puede añadir la cuenta de forma manual, pulsando en “**¿No puede escanear la imagen?**” en la página donde aparece el QR. La información contenida en el código QR se mostrará entonces en pantalla (recuerda, lo que se muestra en esta imagen son datos de ejemplo, los que son válidos son los que se muestren en tu pantalla):

Aplicación de autenticación ×

Digitalización del código QR

Use la aplicación de autenticación para escanear el código QR. Así, la aplicación de autenticación y la cuenta quedarán emparejadas.

Después de escanear el código QR, elija "Siguiente".



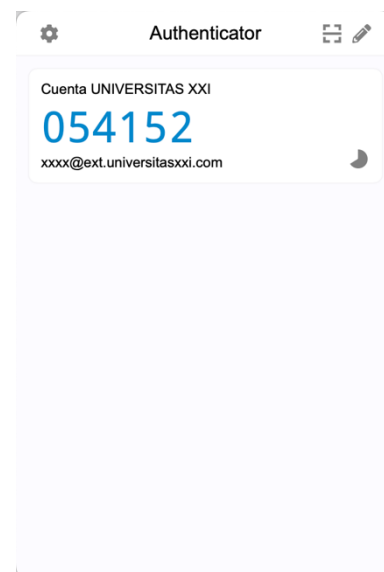
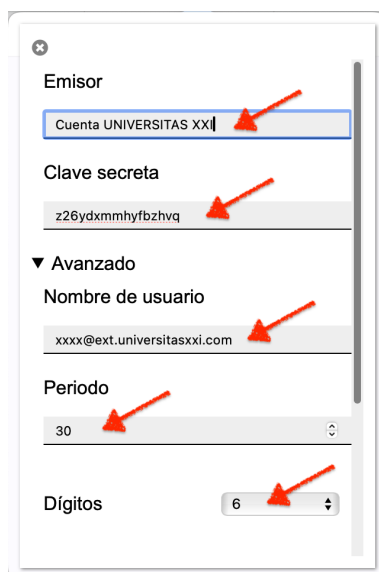
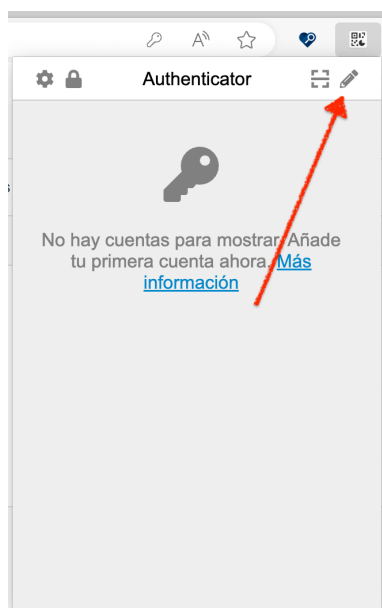
Indique la siguiente información en la aplicación:

Nombre de cuenta: UNIVERSITAS XXI Soluciones y Tecnología para la Universidad,

S.A. @universitasxxi.com

Clave secreta: z26ydxmmhyfbzhvq

18. Abriendo la extensión del navegador y pulsando sobre el icono de añadir cuenta de forma manual, se solicitará la información sobre el **Emisor**, el **Nombre del usuario** y la **Clave secreta** (entre otros). Como nombre de emisor se puede poner cualquier nombre significativo e identificativo para la cuenta; por ejemplo, **Cuenta UNIVERSITAS XXI**. El nombre de usuario es tu cuenta **seguida de arroba (@) y ext.universitasxxi.com**. Y la clave secreta es la que aparece en la pantalla. Introduce también un periodo de rotación de **30 segundos** y una longitud de **6 dígitos**. Una vez introducidos todos los datos, puedes pulsar en **Aceptar** y verás que la extensión del navegador comienza a generar números de 6 dígitos cada 30 segundos:



19. Por último, una vez se estén generando los códigos, se puede pulsar en **Siguiente** en la pantalla del código QR y se solicitará confirmación para dar el proceso por finalizado:

Aplicación de autenticación



Especificar el código

Escriba el código de 6 dígitos que se muestra en la aplicación Authenticator.

Especificar el código

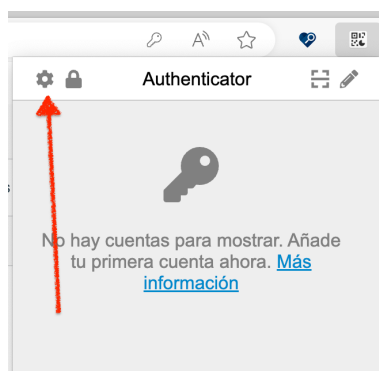
Atrás

Siguiente

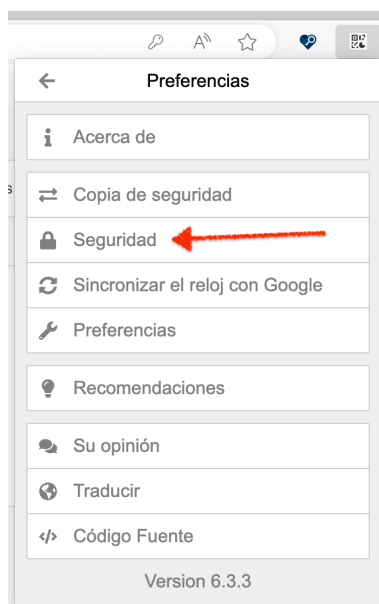
20. Introduce el código generado por la extensión del navegador y, si todo es correcto, el proceso de registro habrá finalizado.

3. RECOMENDACIONES DE SEGURIDAD EN EL USO DE LA EXTENSIÓN DEL NAVEGADOR

Al igual que cuando se utiliza un dispositivo móvil, éste tiene una protección de acceso mediante un código PIN, una contraseña o una verificación biométrica, es conveniente y recomendable que se proteja el acceso a los códigos que genera la extensión del navegador web. Para hacer esto, simplemente tienes que ir a las opciones de configuración de la extensión, pulsando en el icono de la rueda dentada:



Seleccionar las opciones de **Seguridad**:



Y establecer una contraseña o código PIN. Este código te lo solicitará cuando vayas a acceder a los códigos generados en una ventana nueva del navegador web o cuando haya pasado mucho tiempo de inactividad:

