UNIVERSIDAD DE GRANADA

Centro de Servicios Informáticos y Redes de Comunicación

Doble Factor Autenticación para Servicios TIC UGR

El acceso a los servicios TIC de la Universidad de Granada desde Internet requiere de una autenticación que utiliza dos claves de usuario a los efectos de garantizar la máxima seguridad en las comunicaciones (Es lo que se le conoce como autenticación de doble factor de). El primer factor se corresponde con los datos de acceso de la cuenta personal de acceso a los servicios TIC UGR (Usuario del tipo xxx@ugr.es / xxx@correo.ugr.es y la correspondiente clave) y el segundo factor se corresponde con un código (clave) temporal asociado a dicha cuenta que se genera en el momento de realizar la conexión.

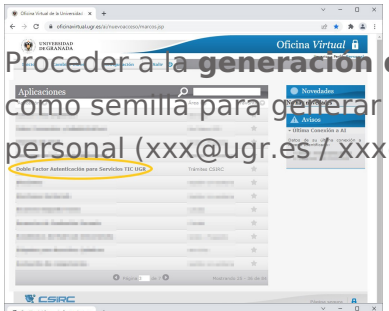
Configuración inicial del segundo factor de autenticación de usuario (2FA)

¡Importante!: Los siguientes tres pasos de configuración sólo se realizan una vez.

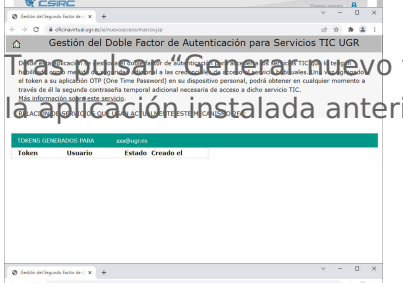
Para la generación de Códigos OTP o segunda contraseña necesitará instalar en su dispositivo móvil una aplicación como por ejemplo Google Authenticator. Si no se dispone de alguna aplicación para generar el Código OTP o segunda contraseña puede optar por una de estas:

- Google Authenticator (android, iOS)
- Microsoft Authenticator (android, iOS)
- FreeOTP Authenticator (android , iOS)
- Cualquier otra aplicación que permita obtener códigos TOTP (**T**ime-based **O**ne **T**ime **P**assword). Deberá localizar la que sea de su preferencia y configurarla adecuadamente.

Una vez tenga la aplicación instalada deberá introducir un token o semilla OTP mediante el escaneo un código QR. Para ello debe acceder mediante un navegador web a: https://oficinavirtual.ugr.es -> [**Doble Factor Autenticación para Servicios TIC UGR**]



Proceder a la **generación del token** (denominación que tiene el sistema que actúa como semilla para generar la clave temporal necesaria) asociado a la cuenta personal (xxx@ugr.es / xxx@correo.ugr.es). Es un dato personal e intrasferible.



Tras pulsar "Generar nuevo token" se genera un código (QR) que debe ser usado con la aplicación instalada anteriormente para ser añadido a la misma.

Seguidamente, para configurar el programa cliente que se va a utilizar en el dispositivo móvil que se desee, se muestra un ejemplo utilizando la app "Google Authenticator". Pulsar el botón de añadir (+).

Aparecerá la opción de escanear un código QR. Éste es el que se ha generado en la página de acceso identificado anterior.

Una vez añadido el token en la aplicación se genera una contraseña temporal (Código OTP ("One Time Password") que se usará más adelante en el servicio TIC UGR correspondiente. Los códigos OTP que se generan en el momento de conexión a los servicios TIC UGR son temporales y de duración limitada en el tiempo.