Servicio de Informática

Vicerrectorado de Universidad Digital

Acceso a los servicios TIC de la Universidad de Jaén (SIDUJA) con doble factor de autentificación

Guía de Usuario

Edición: 02
Última Actualización 04 de julio de 2023

Tabla de contenido

1.- Introducción

La adopción de esta medida de seguridad en la UJA da cumplimiento a lo establecido al respecto por el Esquema Nacional de Seguridad (ENS, RD 311/2022 de 3 de mayo), normativa de obligado cumplimiento en los organismos públicos. (https://www.boe.es/buscar/doc.php?id=BOE-A-2022-7191)

Si alguien te roba la contraseña, podría impedirte el acceso a tu cuenta y llevar a cabo acciones, en tu nombre, no deseadas.

El doble factor de autenticación, te ayudará a proteger tu cuenta y los servicios TIC de la Universidad de Jaén de personas malintencionadas, incluso en el caso de que conozcan tu contraseña. Proteges tu cuenta con un elemento que conoces (la contraseña) y un dato que obtienes (por ejemplo, un código de seguridad) mediante sms, app o aplicación móvil, correo electrónico, ….

Cuando actives la autenticación de doble factor, el acceso a tu cuenta funcionará de forma distinta:

- Cada vez que accedas a tu cuenta TIC, introducirás tu contraseña como de costumbre.
- A continuación, te enviaremos un código a alguno de los medios que tengamos registrados en tus datos personales (correo electrónico personal, teléfono móvil, …) o a una aplicación móvil que previamente hayas vinculado a tu cuenta TIC.

2.- Antes de activar el doble factor

Como se ha mencionado anteriormente, una vez activada la autenticación de doble factor, tras introducir usuario y contraseña, necesitará un código de seguridad (dato que obtienes), que se remitirá al método de contacto que selecciones o se generará en la aplicación para móvil (Google Authenticator, freeOTP Authenticator, Microsoft Authenticator, …).
Por lo que, antes de activar el doble factor de autenticación, comprueba que en Universidad Virtual has registrado al menos dos medios: un teléfono móvil, un correo electrónico, etc… En caso de pérdida del móvil, etc., esto garantiza que puedes recibir el código por otras vías. Para ello, sigue estos pasos:

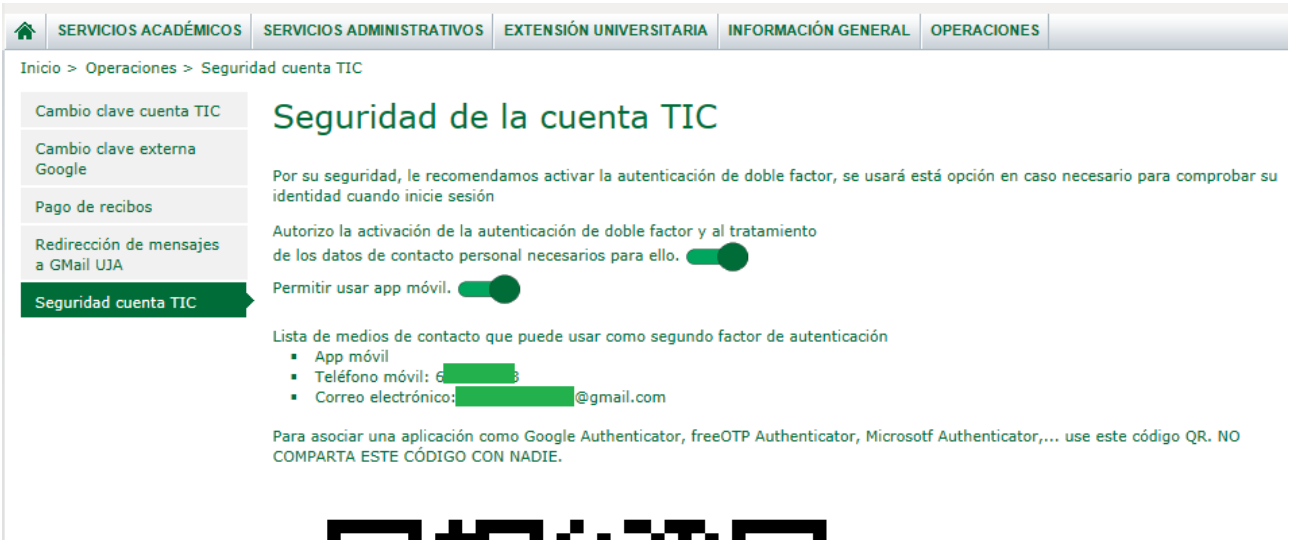
1. Entra en Universidad Virtual (https://uvirtual.ujaen.es)
2. Pulsa en:
   a. Empleado/a: Servicios Administrativos > Datos Personales

b. Estudiante: Servicios Académicos > Datos Personales

3. Escribe un teléfono móvil y un correo electrónico alternativo, si aún no están registrados

3.- Activación doble factor de autenticación

La activación del doble factor de autenticación se realiza en Universidad Virtual, opción Operaciones>Seguridad cuenta TIC, donde nos aparecerá una pantalla similar a la siguiente (tenga presente que en esta captura ya están activados el doble factor y la app móvil):



En esta pantalla, puede activar / desactivar (Activado: en verde o botón a la derecha; Desactivado: en gris o botón a la izquierda) la autenticación de doble factor, pulsando el botón tras el texto “Autorizo la activación de la autenticación …”.

Una vez activada, puede a su vez, seleccionar como medio de generación del código correspondiente al segundo factor una aplicación móvil (botón: Permitir usar app móvil).

Y tras estos botones, se muestra la lista de medios de contacto que figuran registrados entre sus datos personales, para poder enviar información y completar el proceso de verificación. Se recomiendan al menos dos métodos.

Además, si deseas realizar la verificación a través de una app en el móvil, pulsando en el botón “Permitir usar app móvil” te aparecerá un código QR que te permitirá vincular esta app a tu cuenta TIC y poder recibir los códigos en dicha APP (más adelante se detalla el proceso).

4.- Factores de autentificación

Recomendamos definir y configurar cuantos más medios mejor y usar en primer lugar la app para móvil, el email y, por último, la opción de sms.

Medio	
APP en móvil (Google Authenticator, freeOTP Authenticator, Microsoft Authenticator, …)	Rapidez y comodidad El código se genera de forma instantánea No requiere conexión activa de datos o wifi en el móvil No se usa su número de teléfono de ese móvil
Email	Acceso a dicho email tanto con un móvil como con un ordenador Requiere de una conexión de datos o wifi Es posible que se tarde en recibir el código
Teléfono móvil	Se recibe un SMS Requiere cobertura Es posible que se tarde en recibir el código

Vinculación App móvil Google Authenticator (opción recomendada)

Dispones de varias apps para doble factor, como Google Authenticator (desarrollador Google LLC), freeOTP Authenticator (desarrollador Red Hat) o Microsoft Authenticator (desarrollador Microsoft Corporation).

A continuación, se describe cómo vincular la app Google Authenticator.

Para generar los códigos de doble factor a través Google Authenticator:

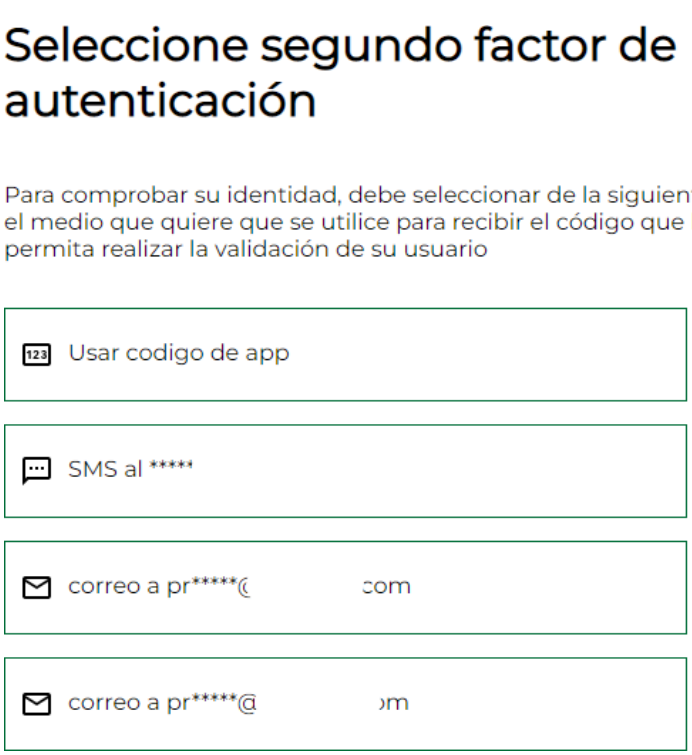
- Descarga Google Authenticator, según el sistema operativo
  - Android: Google Authenticator - Aplicaciones en Google Play
  - iOS: Google Authenticator en App Store (apple.com)
- En Universidad Virtual
  - Asegúrate que está activa la opción “Autorizo la activación de la autenticación …”.
  - Activa la opción Permitir usar app móvil. Tras ello, se mostrará un código QR de vinculación (personal e intransferible). NO COMPARTA ESTE CÓDIGO CON NADIE.
- Abre Google Authenticator, pulsa el botón “+” y luego “Escanear código QR” para vincular la app.

5.- Acceso a los servicios TIC de la Universidad de Jaén con doble factor de autentificación activado

Accede los servicios TIC de la UJA como lo realizabas habitualmente (Universidad Virtual, correo electrónico, Platea, VPNSSL, etc..). Después de activar el doble factor de autenticación en Universidad Virtual, el Servicio de Identidad de la UJA (SIDUJA) incorporará la nueva protección de seguridad. Te pedirá el usuario/contraseña y a continuación el código de 6 dígitos.

Una vez accedamos a SIDUJA y se introduzcan los datos de nuestra cuenta TIC (usuario y contraseña), pulsamos en INICIAR SESION

Una vez validada la contraseña, se mostrarán aquellas opciones que tenemos disponibles para obtener el código de verificación como segundo factor de autenticación.



Recibirás un código de 6 dígitos en el medio que hayas seleccionado.

Finalmente, introduce el código de 6 dígitos "segundo factor de autenticación" en el recuadro correspondiente, para finalizar el proceso de autenticación y acceder al servicio TIC.

Si se marca la casilla de recordar este dispositivo, a partir de ese momento, cuando accedas desde ese dispositivo, solo tendrás que ingresar la contraseña de la cuenta TIC y no se solicitará la doble autentificación durante un periodo de tiempo. Esta opción sólo está aconsejada para equipos privados, a los que no tengan acceso varias personas.

Tu cuenta seguirá protegida, ya que cuando tú o cualquier otro usuario intenten acceder a ella en otro dispositivo, tendrán que completar la verificación en dos pasos.