Guía para Activar el Doble Factor de Autenticación (2FA) en el Portal de Ofertantes GIPE UCM

Introducción

Para aumentar la seguridad de tu cuenta en el Portal de Ofertantes GIPE UCM, hemos implementado el Doble Factor de Autenticación (2FA). Esta medida de seguridad adicional requiere que, además de tu contraseña, introduzcas un código único generado por una aplicación en tu dispositivo.

A partir del 5 de mayo de 2025, el 2FA será obligatorio para acceder al portal.

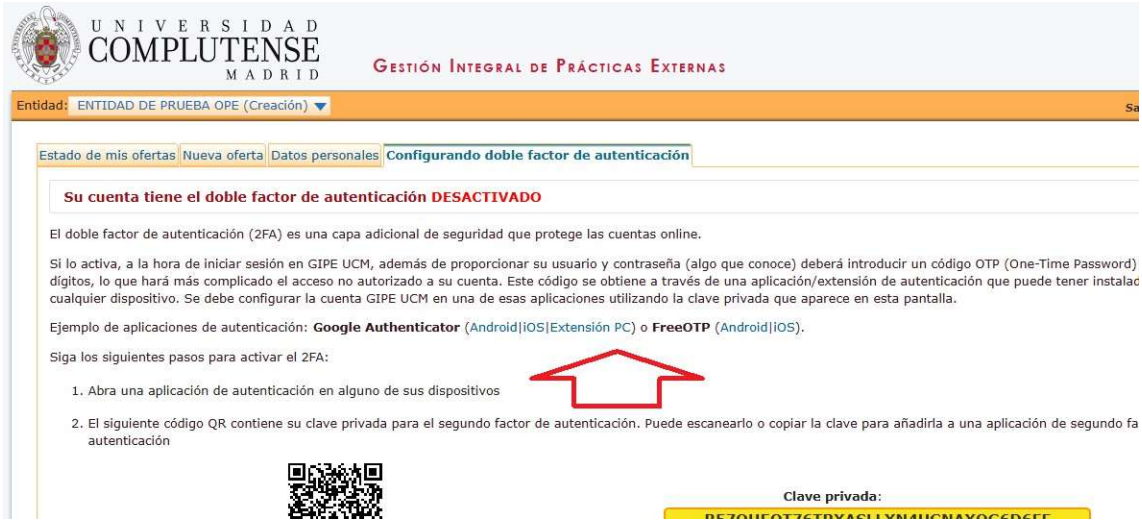
1. **Aviso de Activación Obligatoria:**
   - Al iniciar sesión, si esa cuenta no tiene activado el 2FA te llevará a la siguiente pantalla y la aplicación no permitirá realizar otra acción que no sea la activación del 2FA.

2. **Pantalla de Configuración del 2FA:**
   - Aparecerá una pantalla con un código QR y una clave alfanumérica (clave privada).
   - **Importante:** Esta clave es única para ti y cambia cada vez que accedes a esta pantalla hasta que actives el 2FA. Por lo tanto, debes configurarlo en ese momento. Además, es conveniente realizar una copia de seguridad de esta clave.

Pasos para Configurar el 2FA

1. **Instala una Aplicación de Autenticación:**
   - Necesitarás una aplicación de autenticación en tu teléfono móvil o como extensión en tu navegador. Algunas opciones populares son:
     - Google Authenticator (iOS y Android)
     - Microsoft Authenticator (iOS y Android)
     - Authenticator (Extensión de Chrome). Utilizaremos esta opción para mostrar el funcionamiento.
2. **Añade una Nueva Cuenta en la Aplicación:**
   - Abre la aplicación de autenticación y selecciona la opción para añadir una nueva cuenta.
   - La aplicación te dará dos opciones:

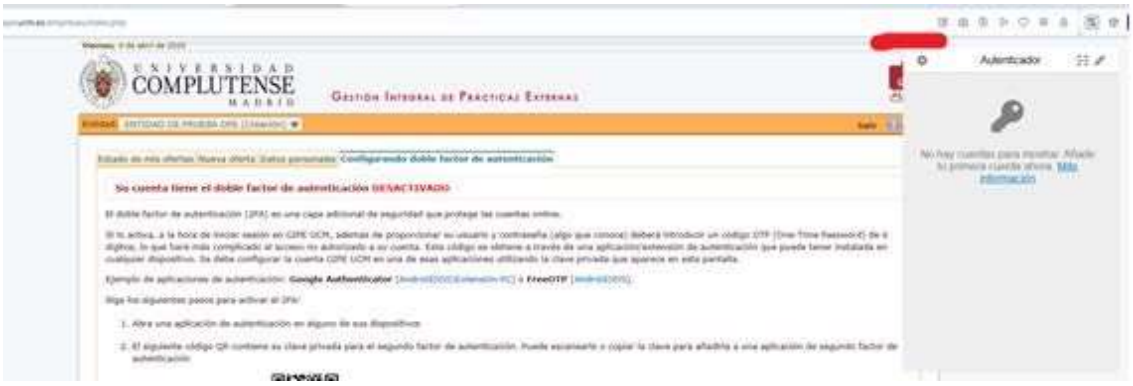
- Escanear el código QR que aparece en la pantalla de GIPE UCM.
- Introducir manualmente la clave alfanumérica. Te indicaré los pasos en este caso. Aparecerá una pantalla como la siguiente de la extensión de Google Autenticator (dependiendo de la aplicación que utilices puede variar)



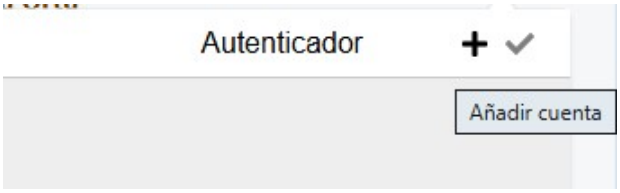
Pinchamos en Extensión PC. Ej Autenticador-Chrome

Seguimos las indicaciones para Añadir a Chrome y a la pregunta ¿Quieres instalar “Autenticador”? Añadir extensión

Una vez se ha añadido la extensión a la “barra menú” volvemos a la pestaña “GIPE EMPRESAS” y continuamos con la activación del 2FA,



Para activar el 2FA añadimos la cuenta bien marcando el icono de QR o el lápiz.



Si añadimos la cuenta manualmente se abre la siguiente ventana

En Emisor pondremos un nombre descriptivo que nos ayude a identificar para qué aplicación generará los códigos, por ejemplo, GIPE EMPRESAS. Y en Clave secreta, la clave privada que se muestra en GIPE al lado del código QR (en el recuadro amarillo). Acepto y aparecerá ya el primer OTP para esa cuenta:

3. **Introduce el Código OTP en GIPE UCM:**
    - La aplicación generará un código de 6 dígitos (OTP).

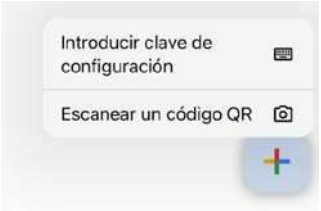
    - Introduce este código en el campo correspondiente en la pantalla de GIPE UCM.

Si hemos elegido “Escanear un código QR” directamente se nos habilita el primer Código OTP y seguimos los pasos anteriores para activar el 2FA.

4. **Activa el 2FA:**
    - Haz clic en el botón "Activar doble factor". Y con esto quedará activado.

Puedes descargar “Google Authenticator” en el móvil o PC. Para ello tienes que ir a Play Store /App Store y buscar por ejemplo Google Authenticator. En el PC lo encontrarás en el enlace del navegador.

Una vez descargado tienes que seleccionar una cuenta de correo y en la siguiente pantalla dar al +



La aplicación te dará dos opciones:

- Escanear el código QR que aparece en la pantalla de GIPE UCM.

- Introducir manualmente la clave alfanumérica.

Acepto y aparecerá el primer OTP para esa cuenta que introducimos en código generado.

Activamos el doble factor.

Inicio de Sesión con 2FA Activado

- A partir de ahora, cada vez que inicies sesión en GIPE UCM, además de tu usuario y contraseña, se te pedirá el código OTP generado por tu aplicación de autenticación.

¿Necesitas Ayuda?

- Si tienes problemas para activar o utilizar el 2FA, contacta con nuestro equipo de soporte en soportegipe@ucm.es. Ellos pueden desactivar temporalmente el 2FA para que puedas intentarlo de nuevo.
- Consulta las FAQS al final del documento

Recomendaciones de Seguridad

- Mantén tu teléfono móvil seguro y protegido con un código de bloqueo.
- No compartas tu clave de 2FA con nadie.

FAQs

1. ¿Qué ocurre si pierdo mi dispositivo con la aplicación de autenticación?

Si pierdes el dispositivo donde tenía configurado la aplicación que te servía los códigos OTP, no podrá acceder a su cuenta.

Solución:

Puede descargarte el Google Authenticator en su PC o móvil y generar el 2FA. Necesitará que desde soporte gipe le desactivemos el doble factor y lo volvamos a activar para que pueda volver a configurarlo en sus dispositivos.

---

2. ¿Por qué el código es incorrecto?

Causas y soluciones:

Desincronización de la hora: Asegúrese de que la hora del dispositivo esté correctamente configurada o sincronícela desde Google Authenticator en "Corregir hora para códigos". El dispositivo con el que se accede a GIPE y el dispositivo que tenga la aplicación de autenticación debe tener configurada la misma zona horaria y la misma hora.

Código expirado: Los códigos cambian cada 30 segundos, intente ingresar uno nuevo.

Error en la configuración: Si el problema persiste, desactive y vuelva a configurar 2FA en la aplicación.

---

3. ¿Qué debo hacer si cambio de dispositivo?

Si cambia de teléfono sin transferir Google Authenticator/ la aplicación de autenticación, perderá los códigos.

Solución:

Si todavía tienes acceso al antiguo dispositivo, utilice la opción de exportar cuentas en Google Authenticator. Luego seleccionamos la cuenta que vamos a exportar y nos generará un QR que habrá que escanear en el otro dispositivo.

En el menú principal del nuevo dispositivo entramos en Transferir códigos y luego en Importar códigos. Escaneamos el QR y ya queda activado en el nuevo dispositivo.

---

4. ¿Qué hacer si desinstalo Google Authenticator por error?

Si elimina la aplicación sin haber guardado la clave secreta, perderá acceso a los códigos.

Solución:

Reinstale Google Authenticator y vuelva a configurar 2FA con su clave secreta o código QR.

---

5. ¿Puedo usar otro autenticador en lugar de Google Authenticator?

Solución:

Sí, siempre que el autenticador soporte el protocolo TOTP (Time-based One-Time Password).

Alternativas comunes: Microsoft Authenticator, FreeOTP, Authy, LastPass Authenticator.

---

6. ¿Se podría activar en dos equipos distintos una única cuenta de GIPE EMPRESAS?

Solución:

No. Las cuentas son personales y cada usuario debería tener su propia cuenta en GIPE asociado a sus datos personales.

---

7. ¿Puedo utilizar una aplicación de autenticación con dos cuentas diferentes (p.ej. una para identificarme en mi entidad y otra para GIPE)?

Solución:

Sí, puede utilizar esta aplicación para dos aplicaciones distintas. El procedimiento es el mismo que hemos descrito más arriba, la única diferencia es que tendrás que asignarle dos nombres distintos para identificar cada aplicación. Los códigos se generan de forma independiente para cada aplicación.

---

8. Que pasa si un gestor me deshabilita el doble factor de autenticación (DFA)

Solución:

Si un gestor te desactiva el DFA, el código que aparecía en tu aplicación de autenticación (Google Authenticator, etc..) asociado a GIPE Empresas ya no sirve. Por eso, lo primero que se debe hacer es dirigirte a tu aplicación de autenticación y eliminar la entrada que estabas utilizando hasta este momento (esos códigos ya no sirven). Cada aplicación de autenticación tiene su propia manera de eliminar estos códigos.

Una vez eliminada la cuenta, se debe proceder como si fuera a configurar por primera vez.