CONFIGURACIÓN
DOBLE FACTOR DE AUTENTICACIÓN
COMO RESPALDO
EN EL CORREO INSTITUCIONAL

Gerencia de Plataformas e Infraestructura Tecnológica - GPIT

Grupo Seguridad Informática - GSI

seguridad.informacion@unad.edu.co

Tel: 601-3443700 Ext 1687

Abril 17 de 2023

OBJETIVO

- **Mejorar la seguridad:** Al tener más de un método de autenticación, se reduce el riesgo de acceso no autorizado a la cuenta institucional. Esto ayuda a proteger la información confidencial y sensible.
- **Reducir la dependencia:** Al contar con varios métodos de autenticación, se evita depender de un solo método. En caso de que uno de los métodos falle o se bloquee, se puede acceder a la cuenta utilizando otro método.
- **Facilitar el acceso:** Dependiendo de la situación, algunos métodos de autenticación pueden ser más convenientes que otros. Al tener más de un método, se puede elegir el que mejor se adapte a las necesidades de cada momento.
- **Cumplir con regulaciones:** En algunos casos, regulaciones o políticas de la organización pueden exigir el uso de más de un método de autenticación para acceder a cuentas institucionales. Tener otro método de autenticación ayuda a cumplir con estas exigencias.

Google Authenticator como MFA de respaldo

- **Mayor seguridad:** Utiliza un código único generado por la aplicación en tu dispositivo móvil, lo que dificulta el acceso no autorizado a tu cuenta.

- **No requiere conexión a internet:** A diferencia de otros métodos de autenticación, como los mensajes de texto, Google Authenticator no requiere una conexión a internet para generar el código, lo que lo hace más confiable y seguro.

- **Fácil de usar:** La aplicación es fácil de descargar y utilizar en dispositivos móviles, lo que permite una autenticación rápida y segura.

- **Compatible con múltiples servicios:** Es compatible con muchos servicios en línea y aplicaciones, lo que te permite utilizarlo como método de autenticación para diferentes cuentas.

- **Gratuito:** No requiere ningún costo adicional para su uso.

En el celular vamos a descargar la siguiente aplicación, como lo muestra la Imagen No. 1:

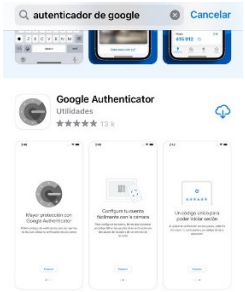

Imagen No. 1 Instalaremos en el dispositivo móvil la aplicación **Google Authenticator**

Ahora, procederemos a configurar otro método de autenticación como respaldo.

Navegador:

Una vez que ingresemos al correo institucional

1. Busca el logo de la UNAD en la parte superior derecha de la pantalla (A) y haz clic en él.
2. A continuación, haz clic en "**Gestionar tu Cuenta de Google**" (B), como se muestra en la imagen No. 2.

Imagen No. 2. **Consola de administración**

Navegador:

1. Una vez dentro de la gestión de la cuenta de Google, busca la opción "**Seguridad**" como se muestra en la Imagen No. 3.
2. Haz clic para ingresar a la configuración de seguridad de tu cuenta de Google.

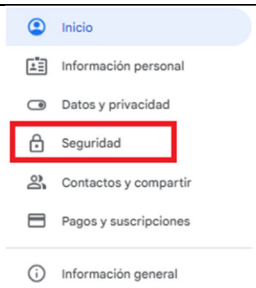

Imagen No. 3 Pantallazo de **Gestionar tu Cuenta de Google**

Navegador:

1. En la pantalla de seguridad, busca la sección de "**Verificación en dos pasos**".
2. Una vez que hayas encontrado esta sección, haz clic en la opción correspondiente, tal como se muestra en la Imagen No. 4.

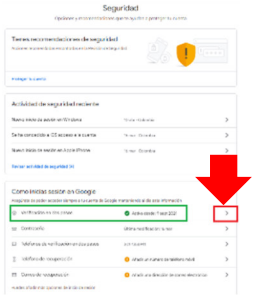

Imagen No. 4 pantallazo de **Seguridad**

Navegador:

1. En la sección de "Verificación en dos pasos", busca la opción "**Aplicación Authenticator**".
2. Haz clic en la opción correspondiente para acceder a la configuración de esta función de seguridad, tal como se muestra en la Imagen No. 5.

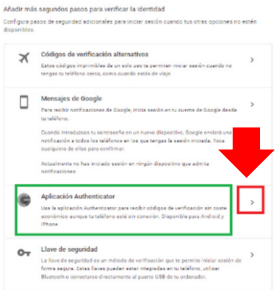

Imagen No. 5 Pantallazo de **Verificación en 2 pasos**

Navegador:

1. Haz clic en la opción correspondiente para acceder a la configuración, tal como se indica en la Imagen No. 6.

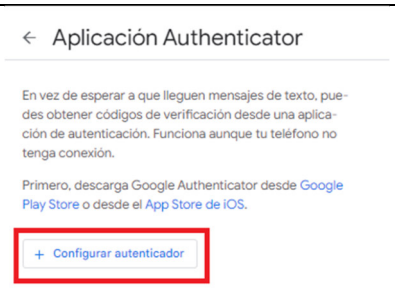

Imagen No. 6 Pantallazo de **Aplicación Authenticator**

Dispositivo Móvil:

1. Abre la aplicación "**Google Authenticator**" en tu dispositivo móvil
2. Una vez que tengas la aplicación abierta, busca la opción “empezar” como lo muestra la Imagen No. 7

Imagen No. 7 Aplicación del dispositivo móvil

Dispositivo Móvil:

1. Haz clic en la opción "**Escanear un código QR**" correspondiente para acceder a la función, tal como se muestra en la Imagen No. 8.

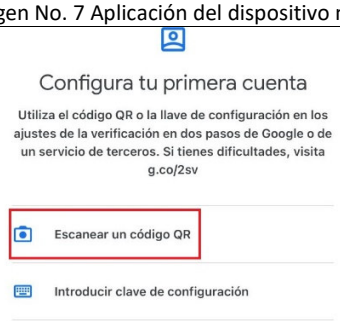

Imagen No. 8 Seleccionar la opción en el dispositivo móvil

Dispositivo Móvil:

1. Si se te solicita permiso para acceder a la cámara de tu dispositivo móvil, asegúrate de otorgar el permiso correspondiente para poder escanear el código QR. como lo muestra la Imagen No. 9

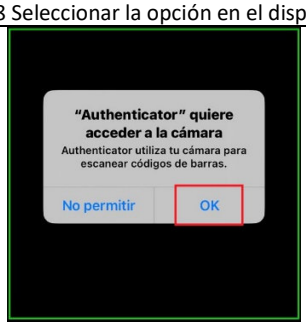

Imagen No. 9 permiso para acceder a la cámara del dispositivo móvil

Navegador:

1. Se te mostrará un código QR en la pantalla, como se muestra en la Imagen No. 10. Este código QR lo utilizarás para configurar la aplicación Google Authenticator en tu dispositivo móvil.
2. Escanea el código QR que aparece en la pantalla de configuración de "Autenticador"
3. Una vez que hayas escaneado el código QR, la aplicación "Google Authenticator" generará un código de verificación de 6 dígitos que deberás ingresar, una vez de clic en "**siguiente**"

Imagen No. 10 Código QR,

Navegador:

1. Este código se actualiza constantemente
2. Ingresa el código de 6 dígitos que se muestra en la aplicación Google Authenticator en el campo correspondiente
3. Una vez que hayas ingresado el código de verificación, haz clic en el botón "**Verificar**" para completar la configuración como lo muestra la Imagen No. 11

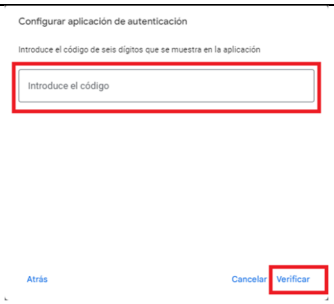

Imagen No. 11 Ingresar código suministrado por el dispositivo móvil de la aplicación Google Authenticator

Navegador:

1. Después de ingresar el código de verificación, se mostrará una confirmación de que la configuración se ha completado con éxito.
2. Una vez que se haya confirmado, haz clic en la flecha
3. Esto se puede visualizar en el siguiente pantallazo, como se muestra en la Imagen No. 12.

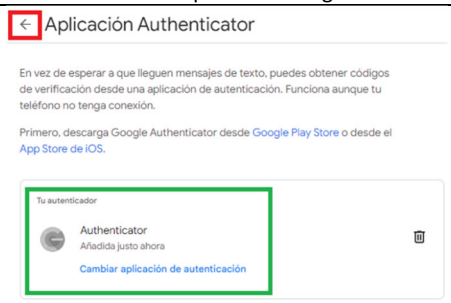

Imagen No. 12 Activador Google Authenticator

Navegador:

1. Es importante verificar que los dos métodos de autenticación estén activados. Para hacerlo, debes volver a la sección de "**Verificación en 2 pasos**" y comprobar que se han agregado los dos métodos: Mensaje de voz o de texto y la aplicación Google Authenticator.
2. Puedes verificarlo en la Imagen No. 13 que muestra los dos métodos activados.
3. Fin del proceso de la configuración

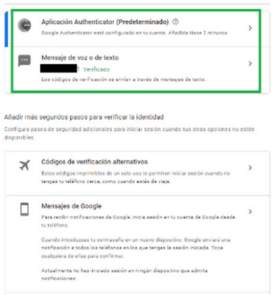
Imagen No. 13 Verificación de dos métodos de autenticación

Navegador:

1. Si en algún momento necesitas autenticarte para acceder al correo institucional y no puedes utilizar el método de autenticación que has configurado, puedes seleccionar la opción "**Probar otra manera**", como se muestra en la Imagen No. 14.

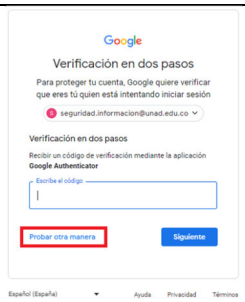

Imagen No. 14 Probar otro método de autenticación

Navegador:

1. Al seleccionar esta opción, se te proporcionarán otras alternativas para completar el proceso de autenticación, como puede ser:
   a. Recibir un código de verificación a través de un mensaje de texto o una llamada en tu teléfono móvil.
   b. Abrir la aplicación YouTube
   c. Abrir la aplicación Google Authenticator.

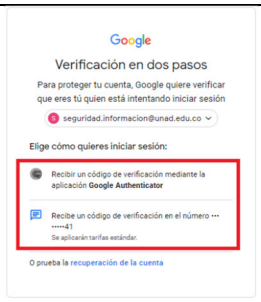

Imagen No. 15 Seleccionamos el método de autenticación deseado

Elaborado por LMM