Activación y uso de Google Authenticator

Autenticación en dos factores 2FA

Sistema de Gestión de Pago
Departamento de Salud Municipal de Curicó

Mayo 2026

Índice

1. Objetivo del manual

El presente manual tiene por finalidad orientar a los usuarios del sistema en el proceso de activación y uso de la autenticación en dos factores, también conocida como **2FA**, mediante la aplicación **Google Authenticator**.

Esta funcionalidad permite reforzar la seguridad de la cuenta del usuario, agregando una capa adicional de protección al momento de ingresar al sistema o validar acciones sensibles.

Con esta medida, además de ingresar usuario y contraseña, el sistema podrá solicitar un código temporal de seis dígitos generado desde el teléfono móvil del usuario.

2. ¿Qué es la autenticación en dos factores?

La autenticación en dos factores, o 2FA, es un mecanismo de seguridad que permite confirmar la identidad del usuario mediante dos elementos:

1. **Algo que el usuario sabe:** su contraseña.
2. **Algo que el usuario posee:** su teléfono móvil con Google Authenticator configurado.

De esta forma, aunque una contraseña fuera conocida por un tercero, no sería suficiente para acceder o validar acciones protegidas dentro del sistema, ya que también se requerirá el código temporal generado en el dispositivo del usuario.

3. Aplicación requerida

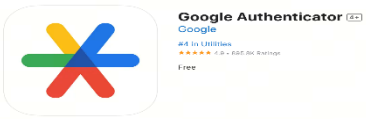
Para utilizar esta funcionalidad, el usuario debe contar con la aplicación **Google Authenticator** instalada en su teléfono móvil.

La aplicación está disponible para dispositivos:

- Android.
- iPhone.

El usuario debe instalarla desde la tienda oficial correspondiente a su dispositivo:

- Google Play Store.
- App Store.



3.1. Descarga de la aplicación Google Authenticator

Para utilizar la autenticación en dos factores, el usuario debe instalar la aplicación **Google Authenticator** en su teléfono móvil. Esta aplicación es gratuita y se encuentra disponible en las tiendas oficiales de aplicaciones para dispositivos Android y iPhone.

La aplicación permite generar códigos temporales de verificación, incluso sin conexión a internet o red móvil, lo que facilita su uso en distintos escenarios de acceso al sistema.

Dónde descargar

Para teléfonos Android:
Descargar desde **Google Play Store**, buscando:

- ✓ `Google Authenticator`

El usuario debe verificar que el desarrollador sea **Google LLC**.

Para teléfonos iPhone:
Descargar desde , buscando:

- ✓ `Google Authenticator`

El usuario debe verificar que la aplicación corresponda a la oficial de Google.

Costo de la aplicación

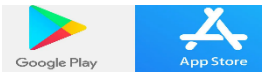
Google Authenticator **no tiene costo para el usuario**. No se debe pagar por instalarla, configurarla ni utilizar los códigos generados para ingresar al sistema.

El sistema tampoco cobra por la cantidad de códigos generados o validaciones realizadas, ya que el código se genera localmente desde la aplicación y se valida directamente contra la configuración segura del sistema.

Recomendación de seguridad

Se recomienda descargar la aplicación únicamente desde las tiendas oficia les:

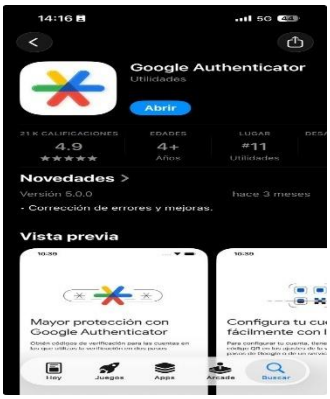
1. `Google Play Store`
2. `App Store`



“No se recomienda instalar aplicaciones desde enlaces desconocidos”, archivos APK descargados desde internet o sitios no oficiales, ya que podrían representar un riesgo para la seguridad de la cuenta.

Importante:

Google Authenticator es una aplicación gratuita. Descárguela únicamente desde Google Play Store o App Store y verifique que corresponda a la aplicación oficial de Google.



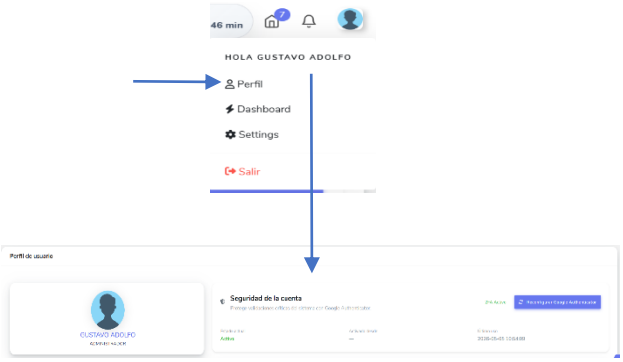
4. Acceso a la configuración de seguridad

Para activar Google Authenticator, el usuario debe ingresar al sistema con sus credenciales habituales.

Una vez dentro, debe dirigirse al menú superior derecho, donde aparece el ícono o imagen de perfil del usuario.

Al desplegar el menú, se visualizarán opciones como:

1. Perfil
2. Dashboard
3. Settings
4. Salir



El usuario debe seleccionar la opción:

- Perfil

5. Sección “Seguridad de la cuenta”

Dentro del perfil del usuario se encontrará el bloque denominado:

Seguridad de la cuenta

Esta sección permite administrar la autenticación en dos factores mediante Google Authenticator.

El sistema mostrará información relevante, como:

- Estado actual
- Activado desde
- Último uso

Cuando la autenticación se encuentra correctamente configurada, el sistema mostrará el estado:

✓ 2FA Activo ó Activo

Esto indica que la cuenta ya cuenta con protección adicional mediante Google Authenticator.

6. Activación de Google Authenticator

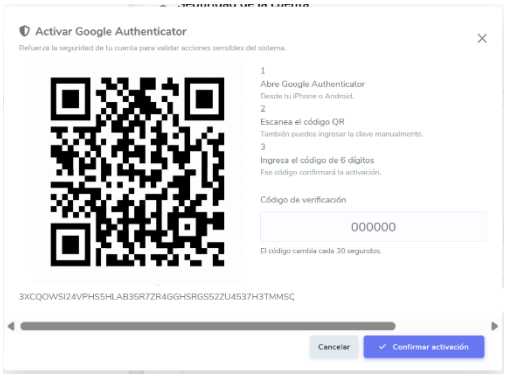
Para activar la autenticación en dos factores, el usuario debe presionar el botón correspondiente a la configuración o reconfiguración de Google Authenticator.

Dependiendo del estado de la cuenta, el botón puede aparecer como:

Activar Google Authenticator ó Reconfigurar Google Authenticator

Al presionar el botón, el sistema abrirá una ventana emergente con el título:

✓ Activar Google Authenticator



En dicha ventana se mostrará un código QR y una clave de respaldo o configuración manual.

7. Escaneo del código QR

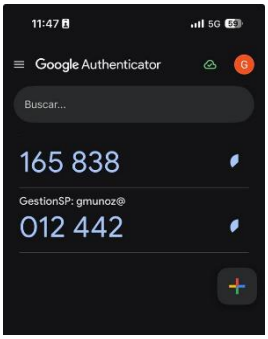
El sistema mostrará un código QR que debe ser escaneado desde la aplicación Google Authenticator.

Para realizar este proceso, el usuario debe seguir los siguientes pasos:

1. Abrir la aplicación Google Authenticator en su teléfono móvil.
2. Presionar la opción para agregar una nueva cuenta.

3. Seleccionar la opción para escanear código QR.
4. Apuntar la cámara del teléfono al código QR mostrado por el sistema.
5. Verificar que se agregue una nueva cuenta asociada al sistema.

Una vez escaneado correctamente, Google Authenticator comenzará a generar códigos temporales de seis dígitos.



8. Ingreso manual de la clave

En caso de que el usuario no pueda escanear el código QR, el sistema también mostrará una clave de configuración manual.

Esta clave puede ser ingresada directamente en Google Authenticator utilizando la opción de configuración manual.

El usuario debe tener especial cuidado de no compartir esta clave, ya que permite vincular la cuenta con una aplicación autenticadora.

9. Código de verificación

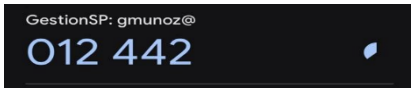
Después de escanear el código QR o ingresar la clave manualmente, Google Authenticator mostrará un código numérico de seis dígitos.

El usuario debe ingresar este código en el campo:

- ✓ `Código de verificación`

El código debe ser ingresado exactamente como aparece en la aplicación.

Ejemplo: 123456



El código cambia aproximadamente **cada 30 segundos**, por lo que se recomienda ingresar uno vigente y presionar rápidamente el botón de confirmación.

10. Confirmación de activación

Una vez ingresado el código de seis dígitos, el usuario debe presionar el botón:

- ✓ `Confirmar activación`

Si el código es correcto, el sistema confirmará la activación de Google Authenticator y la cuenta quedará protegida con **2FA**.

Desde ese momento, el sistema podrá solicitar este código en el inicio de sesión o en acciones sensibles que requieran una validación adicional.

11. Estado de activación

Cuando la configuración se completa correctamente, en la sección de seguridad se mostrará el estado:

- ✓ `2FA Activo`

Además, el sistema puede mostrar información como la fecha de último uso del código 2FA.

Ejemplo:

```
Último uso: 2026-05-05 10:54:09
```

Esto permite dejar trazabilidad del uso de la autenticación en dos factores.

12. Uso de 2FA al iniciar sesión

Cuando el usuario tiene Google Authenticator activado, el inicio de sesión se realizará en dos etapas.

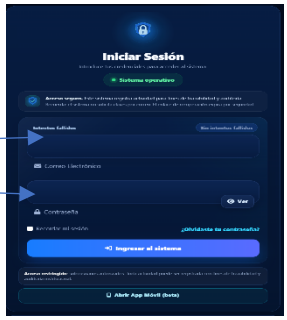
Diferencia entre contraseña y código 2FA:

La contraseña corresponde a la clave habitual de ingreso al sistema.

El código 2FA corresponde a un número temporal de seis dígitos generado por Google Authenticator. Este código cambia periódicamente y no reemplaza la contraseña, sino que actúa como una segunda validación de seguridad.

Primero, el usuario debe ingresar:

1. Correo electrónico
2. Contraseña



Si las credenciales son correctas, el sistema solicitará el código de autenticación 2FA.

El usuario debe abrir Google Authenticator, copiar el código vigente de seis dígitos e ingresarlo en la ventana de validación.

Solo **si el código es correcto**, el sistema **permitirá el acceso**.

13. Intentos incorrectos

Por seguridad, el sistema controla los intentos fallidos de validación 2FA.

Si el usuario ingresa un código incorrecto, el sistema informará que el código no es válido e indicará los intentos restantes.

Ejemplo:

```
Código 2FA incorrecto. Intento 1 de 5. Intentos restantes: 4.
```

El usuario dispone de un máximo de cinco intentos para ingresar correctamente el código.

14. Bloqueo por intentos fallidos

Si el usuario supera el máximo de intentos permitidos, el sistema bloqueará temporalmente la validación 2FA.

En ese caso, se mostrará un mensaje indicando que se superaron los intentos permitidos y que el usuario deberá iniciar sesión nuevamente.

Además, el sistema enviará un correo informativo de seguridad, dejando trazabilidad del evento.

Este correo puede incluir información como:

1. Usuario
2. Fecha y hora
3. Dirección IP
4. Navegador o dispositivo utilizado
5. Cantidad de intentos fallidos
6. Módulo afectado

Esta medida permite reforzar la seguridad y detectar posibles intentos de acceso no autorizados.

15. Reconfiguración de Google Authenticator

Si el usuario cambia de teléfono, pierde el dispositivo o necesita volver a vincular la cuenta, podrá utilizar la opción:

- ✓ Reconfigurar Google Authenticator

Al realizar este proceso, el sistema generará un nuevo código QR y una nueva clave de configuración.

El usuario deberá repetir el proceso de escaneo y confirmación del código de seis dígitos.

Es importante considerar que, al reconfigurar Google Authenticator, la configuración anterior puede dejar de ser válida.

16. Recomendaciones de seguridad

Para un uso seguro de Google Authenticator, se recomienda:

1. No compartir el código de seis dígitos con otras personas.
2. No compartir la clave manual de configuración.
3. Mantener el teléfono móvil protegido con clave, huella o reconocimiento facial.
4. No instalar aplicaciones desde fuentes desconocidas.

5. Mantener la hora automática activada en el teléfono.
6. Cerrar sesión al utilizar equipos compartidos.
7. Informar a soporte si se pierde el dispositivo móvil.

17. Problemas frecuentes

El código aparece como inválido

Esto puede ocurrir cuando:

1. El código ya expiró.
2. La hora del teléfono no está sincronizada.
3. Se ingresó un código de otra cuenta.
4. El usuario tardó demasiado en confirmar.

Se recomienda esperar a que Google Authenticator genere un nuevo código e intentarlo nuevamente.

No puedo escanear el código QR

En este caso, el usuario puede utilizar la clave manual que aparece debajo del código QR.

Debe ingresar esa clave en Google Authenticator usando la opción de configuración manual.

Cambié de teléfono

Si el usuario cambió de dispositivo, debe solicitar o realizar la reconfiguración de Google Authenticator desde su perfil, siempre que tenga acceso al sistema.

Si no puede ingresar, debe contactar a soporte.

Superé los intentos permitidos

Si se superan los intentos permitidos, la validación quedará bloqueada temporalmente.

El usuario deberá esperar el tiempo indicado o contactar a soporte si el problema persiste.

18. Importancia institucional

La implementación de autenticación en dos factores permite fortalecer la seguridad del sistema y proteger información sensible asociada a procesos administrativos, financieros y operativos.

Esta medida contribuye a:

1. Reducir riesgos de acceso no autorizado.

2. Aumentar la trazabilidad de acciones críticas.
3. Proteger cuentas de usuarios.
4. Fortalecer controles internos.
5. Mejorar la gobernanza tecnológica del sistema.

19. Buenas prácticas para usuarios

Cada usuario es responsable del correcto uso de su cuenta institucional.

Por ello, se recomienda:

1. Mantener actualizada su contraseña.
2. No compartir credenciales.
3. Activar Google Authenticator dentro del plazo definido por la administración.
4. Revisar periódicamente la seguridad de su cuenta.
5. Informar cualquier actividad sospechosa.

20. Mensaje final para el usuario

La autenticación en dos factores es una herramienta simple, gratuita y efectiva para proteger el acceso al sistema.

Una vez activada, el usuario solo deberá ingresar el código temporal de Google Authenticator cuando el sistema lo solicite.

Este proceso mejora la seguridad de la cuenta y permite validar de forma confiable la identidad del usuario antes de acceder o ejecutar acciones sensibles.

21. Glosario breve.

2FA:
Autenticación en dos factores. Mecanismo que agrega una segunda validación de identidad.

Código temporal:
Número de seis dígitos generado por Google Authenticator.

Código QR:
Imagen que permite vincular la cuenta del sistema con la aplicación autenticadora.

Clave manual:
Código alternativo para configurar Google Authenticator cuando no es posible escanear el QR.

Bloqueo temporal:
Medida de seguridad aplicada cuando se superan los intentos permitidos.

Anexo: Resumen rápido del proceso

1. Ingresar al Sistema de Gestión de Pago con sus credenciales habituales.
2. Abrir el menú de usuario ubicado en la parte superior derecha.
3. Seleccionar la opción Perfil.
4. Dirigirse a la sección Seguridad de la cuenta.
5. Presionar Activar Google Authenticator o Reconfigurar Google Authenticator, según corresponda.
6. Abrir la aplicación Google Authenticator en el teléfono móvil.
7. Escanear el código QR mostrado por el sistema.
8. Ingresar en el sistema el código temporal de seis dígitos generado por la aplicación.
9. Presionar Confirmar activación.
10. Verificar que el estado de seguridad quede como 2FA Activo.

Resultado esperado:

Al finalizar correctamente el proceso, la cuenta del usuario quedará protegida mediante autenticación en dos factores. El sistema deberá mostrar el estado 2FA Activo en la sección Seguridad de la cuenta, confirmando que Google Authenticator quedó correctamente vinculado a la cuenta del usuario.

Conclusión

La implementación de **Google Authenticator** como mecanismo de **autenticación en dos factores (2FA)** constituye una medida concreta y efectiva para fortalecer la seguridad de acceso al **Sistema de Gestión de Pago**. Su uso permite proteger las cuentas de usuario frente a accesos no autorizados, reforzar la validación de identidad y mejorar la trazabilidad de acciones críticas dentro de la plataforma.

A través de este manual se ha descrito el proceso de activación, configuración, validación y uso de esta funcionalidad, junto con las principales recomendaciones de seguridad y consideraciones operativas para su correcta utilización. La incorporación de este mecanismo no solo representa una mejora técnica, sino también un avance en materias de **control interno, resguardo de la información y buenas prácticas institucionales**.

Se recomienda a todos los usuarios realizar la activación de esta herramienta dentro de los plazos establecidos y mantener un uso responsable de sus credenciales y dispositivos asociados. La seguridad del sistema es una tarea compartida, y la correcta utilización de la autenticación en dos factores contribuye de manera directa a la protección de los procesos, datos y operaciones institucionales.