



CÓMO USAR LA AUTENTICACIÓN DE DOBLE FACTOR

Guía para el proveedor

Contenido

Introducción	3
Pasos previos	3
Habilitar el doble factor de autenticación para un usuario	3
Utilización de la Autenticación de Doble Factor	6



Introducción

El doble factor de autenticación es una medida de seguridad adicional que sirve para verificar la identidad de la persona que quiere ingresar a una cuenta.

El doble factor de autenticación añade una segunda capa de protección, reforzando el nivel de seguridad de las cuentas de usuario. Esto lo logra **solicitando cada vez que se ingresa a su cuenta**, además de la contraseña, **un segundo código obtenido desde una aplicación en su teléfono celular**.

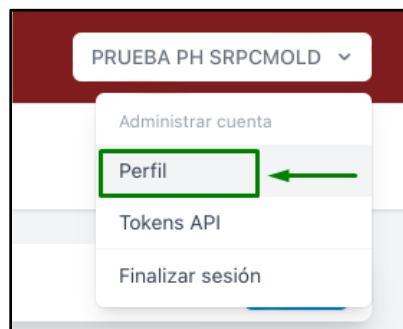
Importante: si habilita el doble factor de autenticación, se le solicitará el segundo código cada vez que intente iniciar sesión. En caso de no disponer de dicho código *no* se permitirá ingresar al sistema.

Pasos previos

Como primer paso, se debe haber instalado la aplicación “**Google Authenticator**” en el teléfono celular. De lo contrario, ingresar en *Google Play Store*, o en *Apple App Store* y buscar “Google Authenticator”. Desde ahí, instalar la aplicación en el dispositivo.

Habilitar el doble factor de autenticación para un usuario

A fin de habilitar el doble factor de autenticación, una vez que se haya ingresado a su cuenta en SRPCM, en la esquina superior derecha, desplegar el menú y hacer clic en “Perfil”, como se muestra a continuación:



Seguidamente, en la página donde se despliega el perfil, ir al apartado “Autenticación de dos factores” y hacer clic en el botón “Habilitar”:

Consejo de la Magistratura
Administración General

Listado Público Reemplazar AL Licitaciones Documentación Ayuda

PRUEBA PH SRPCMOLD

Perfil

Actualizar contraseña
Asegúrese que su cuenta esté usando una contraseña larga y aleatoria para mantenerse seguro.

Contraseña actual
Nueva Contraseña
Confirmar contraseña

GUARDAR

Autenticación de dos factores
Agregue seguridad adicional a su cuenta mediante la autenticación de dos factores.

Autenticación de dos factores: deshabilitada
Cuando la autenticación de dos factores esté habilitada, le pediremos un token aleatorio seguro durante la autenticación. Puede obtener este token desde la aplicación Google Authenticator de su teléfono.

IMPORTANTE: En caso de no disponer del código de autenticación en el momento del login **NO** podrá ingresar a su cuenta.

HABILITAR

Sesiones del navegador
Administre y cierre sus sesiones activas en otros navegadores y dispositivos.

Si es necesario, puede salir de todas las demás sesiones de otros navegadores en todos sus dispositivos. Algunas de sus sesiones recientes se enumeran a continuación; sin embargo, es posible que esta lista no sea exhaustiva. Si cree que su cuenta se ha visto comprometida, también debería actualizar su contraseña.

Luego, el sistema solicitará la contraseña del usuario logueado (administrador legitimado) y su confirmación:

Confirmar contraseña

Por su seguridad, confirme su contraseña para continuar.

Contraseña

CANCELAR CONFIRMAR

A continuación, deberá usar su teléfono celular para escanear el código QR desde la aplicación de Google Authenticator.

Luego de escanear el QR, se recibirá un código, el cual debe ser tipeado en el campo que se muestra en la imagen de abajo, y hacer clic en "Confirmar".



Autenticación de dos factores


Agregue seguridad adicional a su cuenta mediante la autenticación de dos factores.

Ha habilitado la autenticación de dos factores.

Cuando la autenticación de dos factores esté habilitada, le pediremos un token aleatorio seguro durante la autenticación. Puede obtener este token desde la aplicación Google Authenticator de su teléfono.

IMPORTANTE: En caso de no disponer del código de autenticación en el momento del login **NO podrá ingresar a su cuenta.**

Two factor authentication is now enabled. Scan the following QR code using your phone's authenticator application.



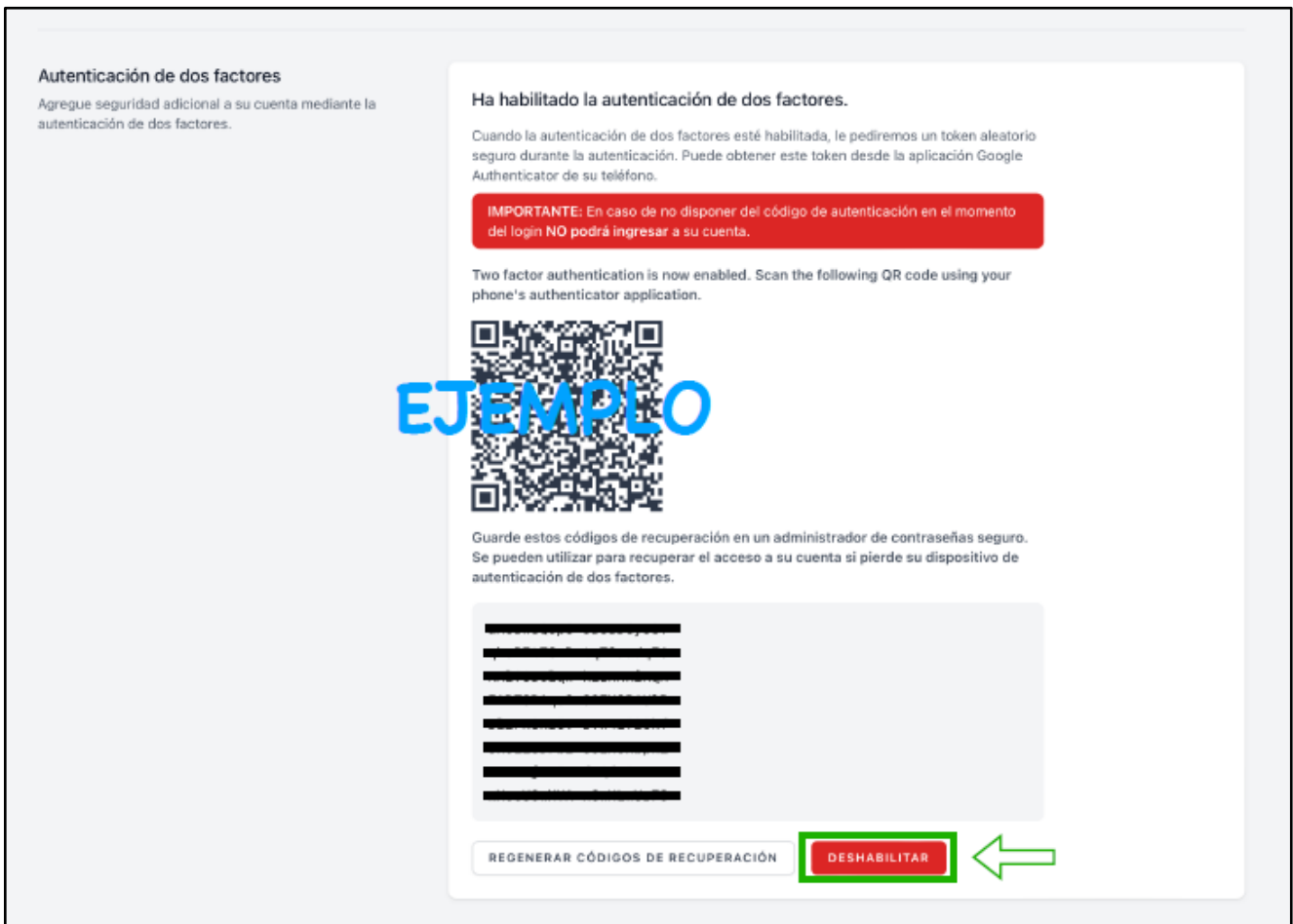
EJEMPLO

Setup Key: ██████████

Code

CONFIRM **CANCEL**

Luego de habilitar la Autenticación de Doble Factor, la aplicación presentará diferentes códigos de recuperación. **Estos códigos deben ser guardados de forma segura para poder utilizarlos en un futuro, cuando se necesiten:**



NOTA: En caso de que desee dejar sin efecto la utilización del doble factor de autenticación, deberá presionar “DESHABILITAR”.

Se recuerda que cada vez que ingrese a su cuenta se le pedirá el código del doble factor de autenticación. En caso de no disponer de dicho código el sistema *no* permitirá iniciar sesión.

Utilización de la Autenticación de Doble Factor

Como fuera explicado previamente, cada vez que inicie sesión deberá ingresar la contraseña y luego el código del doble factor de autenticación. A continuación, se explica el paso a paso:

Para iniciar sesión en SRPCM, primero el sistema solicitará el correo electrónico y la contraseña del usuario:

Sistema de Registro de Proveedores

Correo electrónico
usuario@ejemplo.com

Contraseña
[Oculto]

Mantener sesión activa

[¿Olvidó su contraseña?](#) INICIAR SESIÓN

A continuación, el sistema solicitará el código del segundo factor de autenticación:



Sistema de Registro de Proveedores

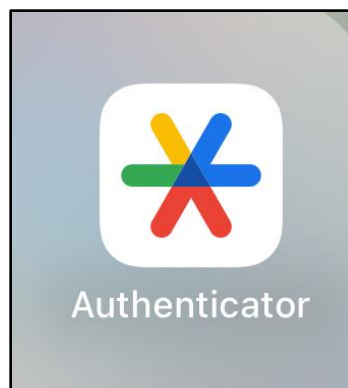
Por favor confirme el acceso a su cuenta digitando el código de autenticación provisto por su aplicación autenticadora.

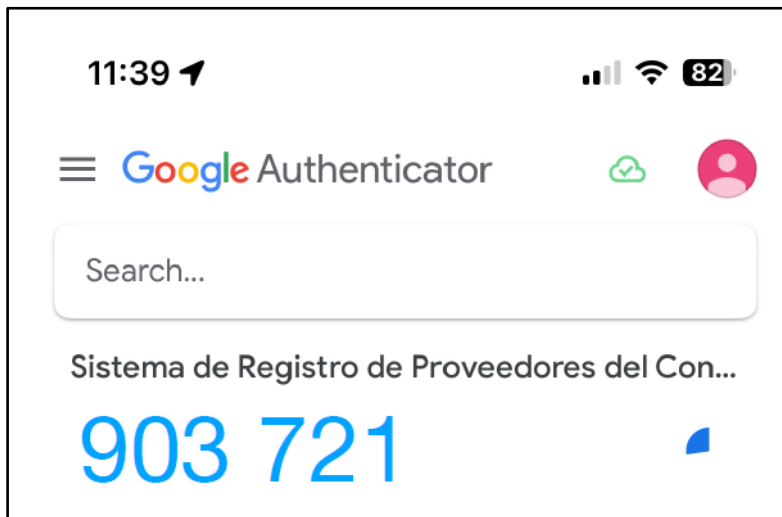
Código

[Use un código de recuperación](#) **INICIAR SESIÓN**

Se debe leer el código actual desde la aplicación “Google Authenticator” en el teléfono celular e ingresar dicho código:

Recordar que, previamente, se debe abrir la aplicación “Google Authenticator”.





El código que se muestra en la aplicación Google Authenticator del celular se deberá ingresar en el sistema SRPCM, tal como se expone a continuación.

Si el código es correcto, el usuario iniciará sesión y será redirigido a la pantalla principal (escritorio) de la aplicación, como se muestra a continuación:



Consejo de la Magistratura
Administración General

Listado Público Reemplazar AL Licitaciones Documentación Ayuda

PRUEBA PH SRPCMOLD

Escritorio

PRUEBA 'SRPCM' Actualización en curso [Editar](#)

Licitaciones Vigentes Disponibles 2

Mis Órdenes de Compra 0

Estado Última Solicitud de Verificación

Buscar 10

TÍTULO	MENSAJE	TIPO	FECHA
Cambios requeridos	ok	Recibida	7 de ago. de 2023 8:37
Solicitud de verificación		Enviada	7 de ago. de 2023 8:03
Cambios requeridos	Cambiamelo!	Recibida	4 de ago. de 2023 12:10
Solicitud de verificación		Enviada	4 de ago. de 2023 12:08
Cambios requeridos	-	Recibida	14 de feb. de 2023 13:07
Solicitud de verificación		Enviada	14 de feb. de 2023 13:06
Cambios requeridos	-	Recibida	14 de feb. de 2023 13:06
Solicitud de verificación		Enviada	14 de feb. de 2023 13:02
Cambios requeridos	Probando el cambio de estado al enviar a verificar. Queda en require cambios para no ponerlo ni rechazado ni inscripto.	Recibida	7 de dic. de 2022 8:45
Solicitud de verificación		Enviada	7 de dic. de 2022 8:43

Mostrando 10 resultados

¡Eso es todo! A través de los pasos descritos, se ha iniciado sesión exitosamente en la aplicación de Proveedores del Consejo de la Magistratura, utilizando "Google Authenticator".