UNIVERSIDAD DE LA REPÚBLICA URUGUAY

Servicio Central de Informática Universitaria · SeCIU

MANUAL DE USUARIO

Panel de Seguridad MFA

Cómo configurar y usar el segundo factor de autenticación en el inicio de sesión de la Udelar

Versión	Fecha	Cambios
1.0	09/11/2026	Traducción y adaptación del manual de CAFe/RNP
1.1	13/11/2026	Ajustes para la Udelar
1.2	13/11/2026	Revisión de redacción, terminología y formato; app MiUdelar como autenticador

Contenido

1. Objetivo....3
2. Panel de Seguridad MFA....3
2.1. Propósito del servicio....3
2.2. Público del servicio....3
3. Visión general....3
3.1. Conceptos importantes....3
3.2. Requisitos....3
4. Acceso al Panel de Seguridad MFA....4
4.1. Acceso desde la pantalla de inicio de sesión....4
5. Gestión de los factores y del acceso....5
5.1. Pantalla inicial....5
5.2. Menú lateral....5
6. Contraseña temporal (OTP)....6
6.1. Configurar el OTP....6
6.2. Generar un nuevo código QR....8
6.3. Definir el OTP como factor favorito....9
6.4. Eliminar el OTP....9
6.5. Iniciar sesión con OTP....9
7. Claves de acceso (passkeys)....10
7.1. Agregar una clave de acceso....10
7.2. Cambiar el nombre de una clave de acceso....12
7.3. Definir la clave de acceso como factor favorito....13
7.4. Eliminar una clave de acceso....13
7.5. Iniciar sesión con una clave de acceso....14
8. Códigos de emergencia....15
8.1. Códigos generados automáticamente....16
8.2. Generar nuevos códigos de emergencia....17
8.3. Iniciar sesión con un código de emergencia....17
9. Dispositivos confiables....18
9.1. Agregar un dispositivo confiable....18
9.2. Ver la lista de dispositivos confiables....19
9.3. Eliminar dispositivos confiables....20
10. Consideraciones finales....21

1. Objetivo

Este documento es el manual de usuario del Panel de Seguridad MFA (*Multi-Factor Authentication*, autenticación multifactor), versión 2.2.3, que incluye soporte para claves de acceso (*passkeys*) y mejoras de usabilidad.

2. Panel de Seguridad MFA

2.1. Propósito del servicio

El Panel de Seguridad MFA es el entorno donde usted puede configurar múltiples factores de autenticación y gestionar el nivel de seguridad de su cuenta Udelar, la misma que utiliza para iniciar sesión en los servicios de la Universidad.

El módulo fue desarrollado por CAFe (Comunidad Académica Federada) de la RNP (Red Nacional de Enseñanza e Investigación de Brasil) y adaptado por el SeCIU para la Udelar.

2.2. Público del servicio

Usuarios de la Udelar que inician sesión con su cuenta institucional a través del servicio de autenticación de la Universidad (login.udelar.edu.uy).

3. Visión general

3.1. Conceptos importantes

Factor de autenticación: método utilizado para verificar la identidad de una persona cuando accede a un sistema o servicio digital. Garantiza que solo las personas autorizadas puedan iniciar sesión y acceder a información protegida. Los factores se clasifican en tres categorías:

- **Algo que usted sabe:** por ejemplo, una contraseña o un PIN.
- **Algo que usted tiene:** por ejemplo, un teléfono con una aplicación autenticadora, una llave de seguridad física o un código enviado por SMS.
- **Algo que usted es:** datos biométricos, como la huella dactilar o el reconocimiento facial.

La **autenticación multifactor (MFA)** combina dos o más de estos factores para aumentar la seguridad: aunque alguien obtenga su contraseña, no podrá ingresar sin el segundo factor.

Proveedor de identidad (IdP, Identity Provider): servicio responsable de autenticar a los usuarios y gestionar sus credenciales de acceso a diferentes sistemas y aplicaciones. Actúa como intermediario entre el usuario y la aplicación a la que desea acceder, y garantiza que la identidad se valide de forma segura. En la Udelar es el servicio que muestra la pantalla de inicio de sesión institucional.

CAFe (Comunidad Académica Federada): infraestructura de identidad digital mantenida por la RNP de Brasil, que desarrolló el módulo MFA utilizado por la Udelar.

3.2. Requisitos

Para utilizar el Panel de Seguridad MFA necesita:

- **Una cuenta institucional de la Udelar activa**, con usuario y contraseña válidos.
- **Un dispositivo compatible:** un teléfono inteligente o una computadora con un sistema operativo y un navegador actualizados, compatibles con el método que quiera usar (aplicación autenticadora o claves de acceso).

4. Acceso al Panel de Seguridad MFA

4.1. Acceso desde la pantalla de inicio de sesión

1. Abra la pantalla de inicio de sesión de cualquier servicio que utilice el inicio de sesión de la Udelar.
2. Haga clic en el enlace «Panel de seguridad», debajo del botón «Ingresar» (figura 1). Se abrirá la pantalla de inicio de sesión del Panel.



Figura 1. *Enlace «Panel de seguridad» en la pantalla de inicio de sesión*

3. En la pantalla de inicio de sesión del Panel (figura 2), ingrese su documento y su contraseña y haga clic en «Ingresar».



Figura 2. *Pantalla de inicio de sesión del Panel de Seguridad MFA*

Advertencia: si el sistema le solicita un segundo factor de autenticación, pero ya no tiene acceso al factor que utilizaba y perdió sus códigos de emergencia, comuníquese con la mesa de ayuda del SeCIU para que desactiven el MFA de su cuenta.

5. Gestión de los factores y del acceso

5.1. Pantalla inicial

La pantalla inicial del Panel (figura 3) organiza las opciones en dos grupos. Cada una se detalla en los capítulos siguientes.

Factores de autenticación:

- **Claves de acceso:** registre claves de acceso (*passkeys*) para iniciar sesión de forma más segura.
- **Contraseña temporal (OTP):** configure una aplicación autenticadora que genere códigos temporales.
- **Códigos de emergencia:** obtenga códigos de respaldo para ingresar si pierde sus otros factores.

Facilidades de acceso:

- **Dispositivos confiables:** gestione los dispositivos en los que no se le pedirá el segundo factor durante un tiempo.

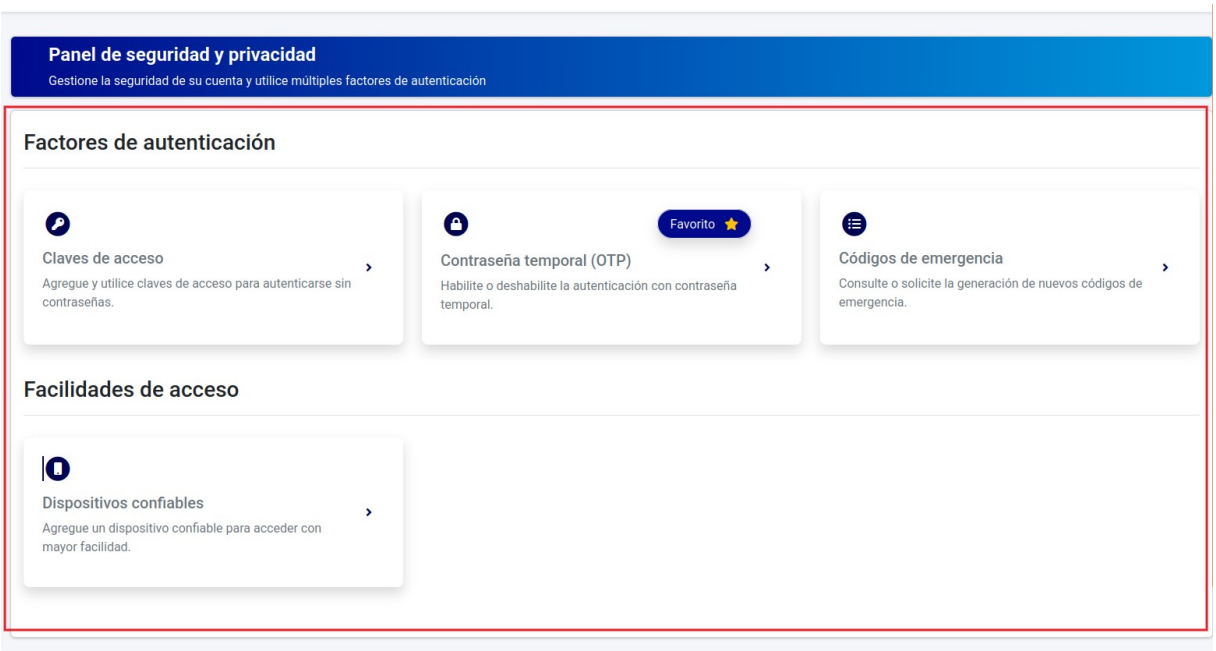


Figura 3. *Pantalla inicial del Panel de Seguridad MFA*

5.2. Menú lateral

En el menú lateral izquierdo (figura 4) encontrará las mismas opciones, junto con la opción para cerrar sesión. Para configurar cualquiera de ellas, haga clic en el elemento correspondiente y siga las instrucciones en pantalla.

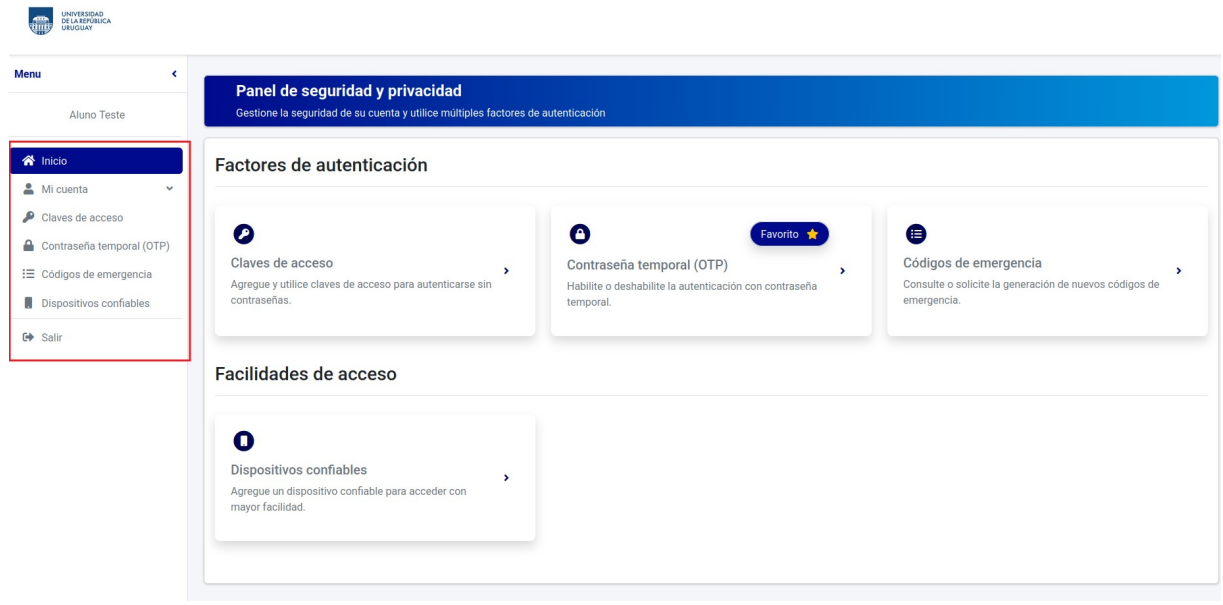


Figura 4. *Menú lateral del Panel*

6. Contraseña temporal (OTP)

La contraseña temporal (OTP, *One-Time Password*) es un código numérico de seis dígitos que genera una aplicación autenticadora instalada en su teléfono (por ejemplo, la app MiUdelar). Cada código es válido durante un período breve (normalmente 30 segundos) y se usa una sola vez, lo que impide su reutilización y reduce el riesgo de robo de credenciales.

6.1. Configurar el OTP

Necesitará una aplicación autenticadora en su teléfono. Recomendamos usar la **app MiUdelar**, que incluye un generador de contraseñas temporales, así no necesita instalar otra aplicación. También puede usar otra aplicación autenticadora de su preferencia (por ejemplo, Google Authenticator, Microsoft Authenticator o FreeOTP).

1. Acceda a «Contraseña temporal (OTP)» desde el menú lateral o desde la pantalla inicial del Panel.
2. Haga clic en «Configurar contraseña temporal (OTP)» (figura 5). Se abrirá la pantalla de activación.



Figura 5. *Botón «Configurar contraseña temporal (OTP)»*

En la pantalla de activación aparece un aviso (figura 6): debe completar todos los pasos de la página para que el OTP quede configurado.



Figura 6. *Aviso en la pantalla de activación del OTP*

Importante: si sale de la página antes de completar todos los pasos, el OTP no se activará y deberá reiniciar el proceso.

Siga los pasos indicados en la pantalla de activación, que se resumen a continuación:

1. Abra la app MiUdelar (o la aplicación autenticadora que utilice) en su teléfono. Si todavía no la tiene, instálela desde la tienda de aplicaciones.
2. En la aplicación, vaya a la opción para agregar una cuenta al autenticador (en muchas aplicaciones, el botón «+»).
3. Elija la opción de escanear un código QR y apunte la cámara al código que aparece en el paso 3 de la pantalla de activación (figura 7). Si está configurando desde el mismo teléfono y no puede escanear, haga clic en «Copiar», debajo del código QR, e ingrese ese código manualmente en la aplicación.



Figura 7. *Código QR para configurar la aplicación autenticadora*

4. La aplicación mostrará un código de seis dígitos. Ingréselo en los campos del paso 4 y haga clic en «Activar contraseña temporal (OTP)» (figura 8).



Figura 8. *Ingreso del código y activación del OTP*

Nota: los siguientes pasos solo aparecen si es el primer factor de autenticación que configura.

1. Aparecerá el mensaje «Factor de autenticación activado correctamente». Haga clic en «Continuar».
2. Aparecerá el mensaje «No tiene códigos de emergencia válidos. Se generarán nuevos códigos automáticamente». Haga clic en «Continuar» para ir a la pantalla de códigos de emergencia.

3. Guarde los códigos siguiendo las instrucciones: se muestran **una sola vez** y le permitirán ingresar si pierde el acceso a la aplicación autenticadora. Consulte el capítulo 8, «Códigos de emergencia».

Para comprobar la configuración, acceda a «Contraseña temporal (OTP)»: verá que el OTP está configurado y la fecha y hora en que se configuró (figura 9).



Figura 9. *OTP configurado*

6.2. Generar un nuevo código QR

Si necesita volver a configurar el OTP (por ejemplo, porque cambió de teléfono):

1. Acceda a «Contraseña temporal (OTP)» y haga clic en «Generar nuevo código QR» (figura 10).

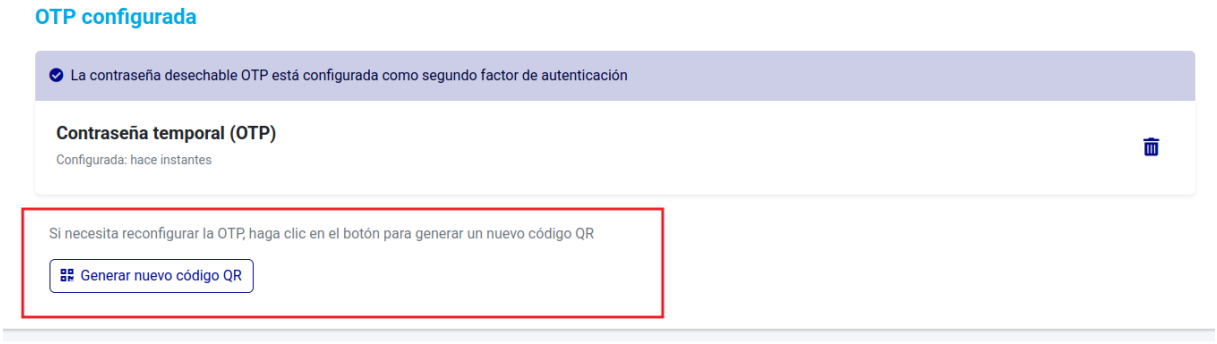


Figura 10. *Botón para generar un nuevo código QR*

2. Confirme con «Sí, generar nuevo código QR» (figura 11). Volverá a la pantalla de activación: repita los pasos de la sección 6.1.

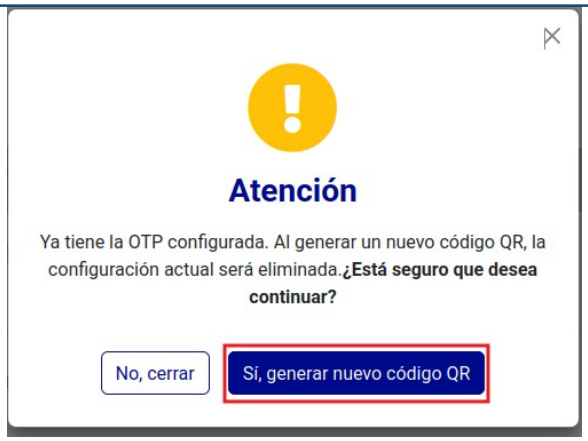


Figura 11. *Confirmación para generar un nuevo código QR*

> **Advertencia:** al generar un nuevo código QR, la configuración actual del OTP se invalida y se elimina del Panel. La cuenta guardada en su aplicación autenticadora **no** se elimina automáticamente: bórrela manualmente para evitar confusiones con códigos que ya no sirven.

6.3. Definir el OTP como factor favorito

Si tiene más de un factor configurado, puede elegir uno como favorito: será el que se le ofrezca primero al iniciar sesión.

1. Acceda a «Contraseña temporal (OTP)» y haga clic en el icono de estrella «Definir este factor como favorito», situado encima de la configuración del OTP.
2. Confirme con «Sí, continuar».

6.4. Eliminar el OTP

1. Acceda a «Contraseña temporal (OTP)» y haga clic en el icono de la papelera (figura 12).

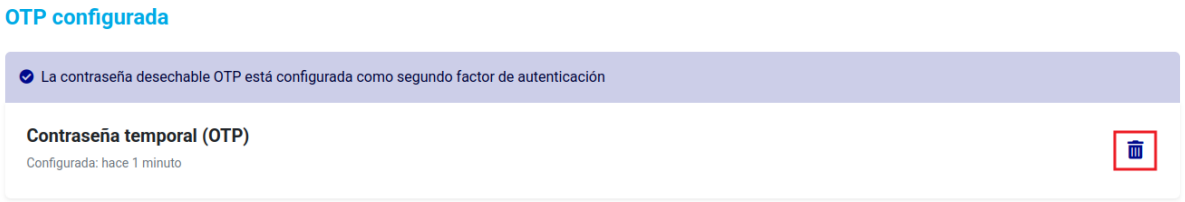


Figura 12. *Eliminar el OTP*

2. Aparecerá el mensaje «¿Está seguro de que desea eliminar este factor?». Haga clic en «Sí, eliminar».

> **Advertencia:** al eliminar el OTP, los códigos de su aplicación dejarán de funcionar. Si era su único factor configurado, su cuenta quedará sin segundo factor y, por lo tanto, más expuesta a accesos no autorizados.
>
> La cuenta guardada en la aplicación autenticadora no se elimina automáticamente: bórrela manualmente.

6.5. Iniciar sesión con OTP

Una vez configurado el OTP, después de ingresar su usuario y contraseña el sistema le pedirá el segundo factor. Pueden darse dos situaciones:

Escenario A: el OTP es su factor favorito (o el único)

1. Abra la aplicación autenticadora e ingrese el código de seis dígitos en los campos indicados.

2. Haga clic en «Ingresar» (figura 13).



Figura 13. *Inicio de sesión con contraseña temporal (OTP)*

Escenario B: tiene varios factores y el OTP no es el favorito

1. En la pantalla del factor favorito, haga clic en «Otras formas de autenticación», debajo del botón «Ingresar».
2. En la ventana «Elija el modo de acceso», seleccione «Contraseña temporal (OTP)». Las opciones que aparecen dependen de los factores que tenga configurados.
3. Continúe como en el escenario A.

7. Claves de acceso (passkeys)

Las claves de acceso (*passkeys*) son una alternativa más segura y práctica que las contraseñas y los códigos temporales. En lugar de escribir un código, usted confirma su identidad con su dispositivo (huella, reconocimiento facial, PIN o bloqueo de pantalla), que guarda una clave criptográfica. La clave puede guardarse en el teléfono, en la computadora, en un gestor de contraseñas o en una llave de seguridad física.

Como segundo factor, la clave de acceso reduce los riesgos asociados a contraseñas débiles o reutilizadas y a códigos que pueden ser interceptados.

7.1. Agregar una clave de acceso

1. Acceda a «Claves de acceso» desde el menú lateral o desde la pantalla inicial del Panel.
2. Haga clic en «Agregar clave de acceso» (figura 14).

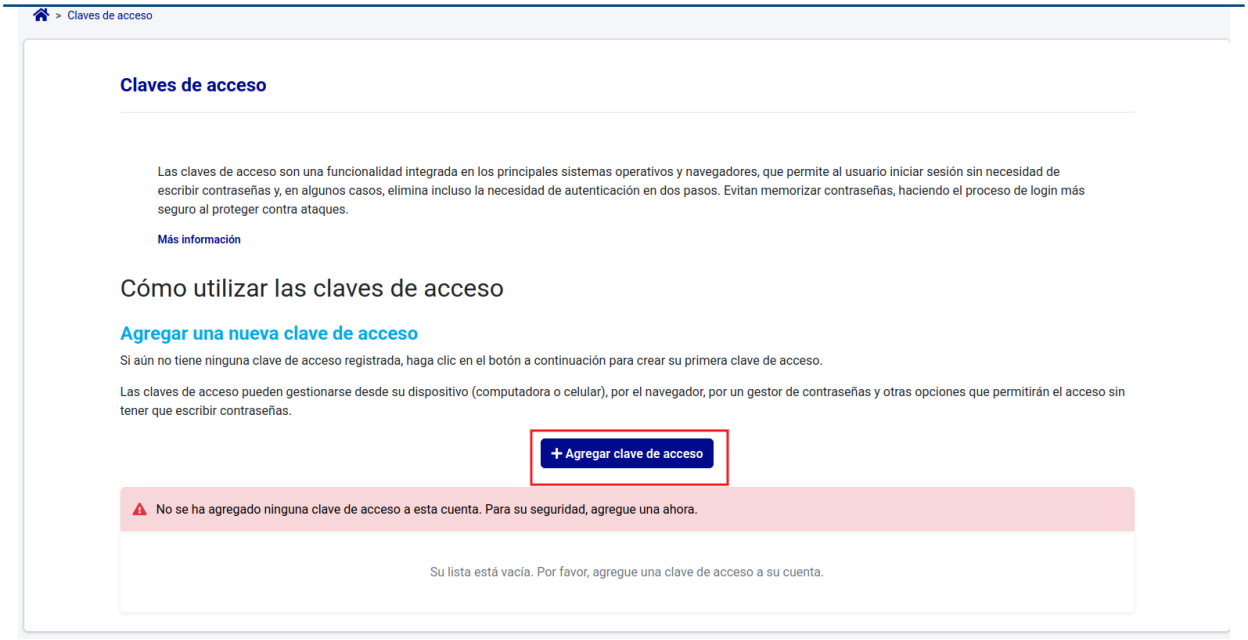


Figura 14. *Pantalla «Claves de acceso»*

3. Escriba un nombre que le permita identificar la clave, por ejemplo «Mi teléfono» o «Notebook trabajo», y haga clic en «Agregar» (figura 15).

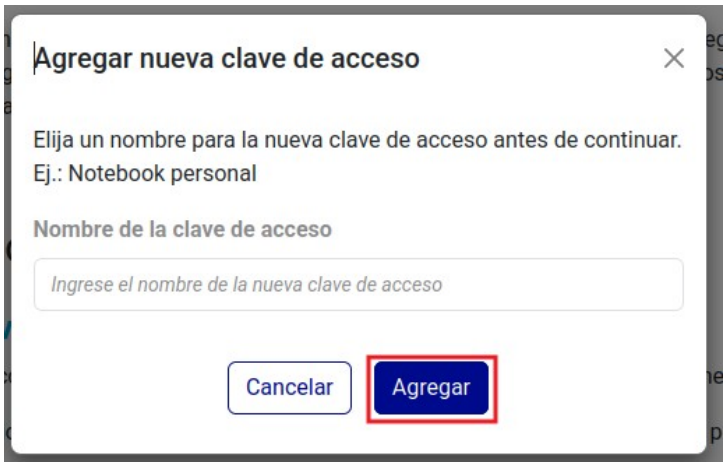


Figura 15. *Nombre de la nueva clave de acceso*

4. El navegador o el sistema operativo mostrará dónde guardar la clave. En el ejemplo (figura 16) se ofrece guardarla en el Administrador de contraseñas de Google; para elegir otro lugar, haga clic en «Usar una llave de acceso diferente».

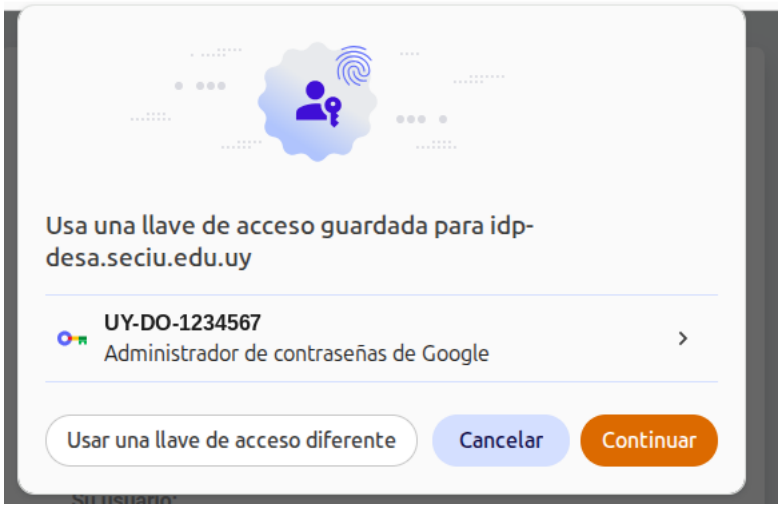


Figura 16. *Opciones del navegador para la clave de acceso (ejemplo en Chrome)*

Importante: las opciones dependen del sistema operativo, el navegador y el dispositivo que utilice. Algunos pueden no ser compatibles con las claves de acceso o serlo solo parcialmente.

Si guarda la clave en otro dispositivo (por ejemplo, registra la clave desde la computadora pero la guarda en el teléfono), ambos dispositivos deben tener el **Bluetooth activado**.

5. Para guardarla en su teléfono, elija «Usa tu teléfono o tablet»: aparecerá un código QR (figura 17). Escanéelo con la cámara del teléfono y siga las instrucciones del dispositivo.



Figura 17. *Código QR para guardar la clave en un teléfono o tableta*

Si completa los pasos correctamente, la clave quedará agregada y podrá usarla como segundo factor en los próximos inicios de sesión.

Nota: si es el primer factor que configura, a continuación verá los mensajes «Factor de autenticación activado correctamente» y «No tiene códigos de emergencia válidos…». Haga clic en «Continuar» en ambos y guarde los códigos de emergencia, que se muestran **una sola vez** (ver capítulo 8).

7.2. Cambiar el nombre de una clave de acceso

1. Acceda a «Claves de acceso» y haga clic en el icono de edición de la columna «Acciones», junto a la clave que desea renombrar (figura 18).

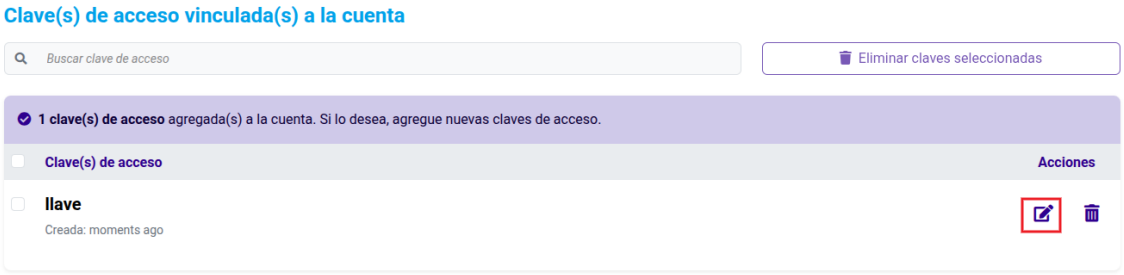


Figura 18. *Icono de edición de una clave de acceso*

2. Escriba el nuevo nombre y haga clic en «Guardar» (figura 19).

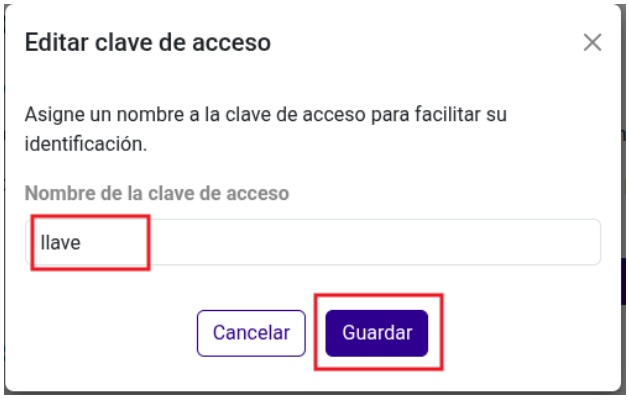


Figura 19. *Ventana «Editar clave de acceso»*

7.3. Definir la clave de acceso como factor favorito

Si tiene más de un factor configurado, puede elegir las claves de acceso como favorito para que se le ofrezcan primero al iniciar sesión.

1. Acceda a «Claves de acceso» y haga clic en el icono de estrella «Definir este factor como favorito», encima de la lista de claves (figura 20).

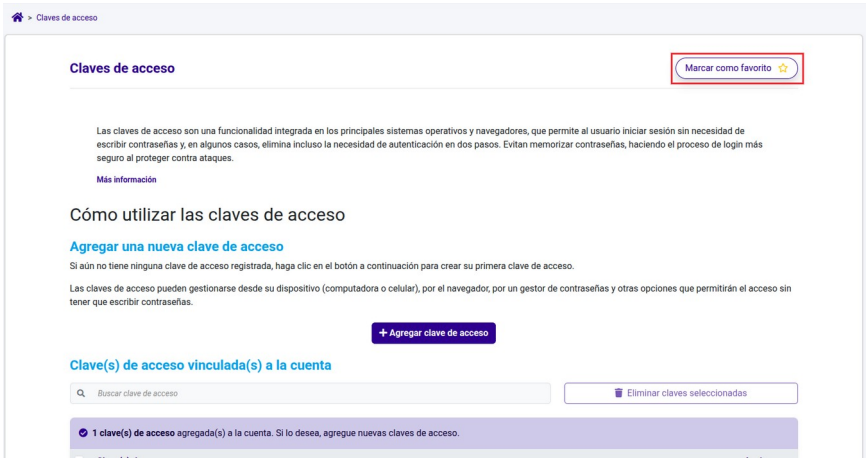


Figura 20. *Definir las claves de acceso como factor favorito*

2. Confirme con «Sí, continuar».

7.4. Eliminar una clave de acceso

1. Acceda a «Claves de acceso» y haga clic en el icono de la papelera de la columna «Acciones», junto a la clave que desea eliminar (figura 21).

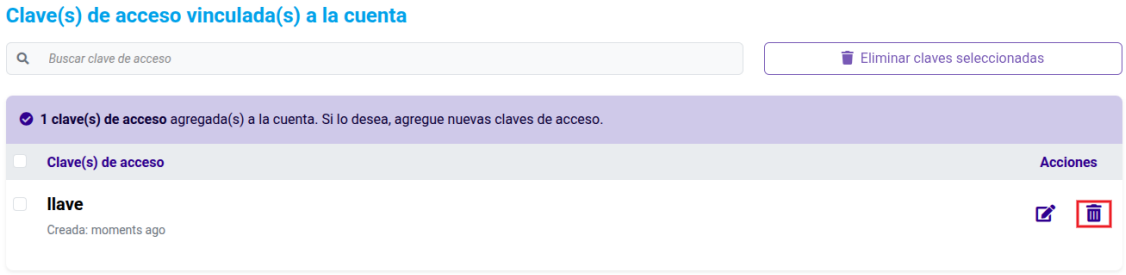


Figura 21. *Eliminar una clave de acceso*

2. Aparecerá el mensaje «¿Está seguro de que desea eliminar su clave de acceso?». Haga clic en «Sí, eliminar».

Advertencia: si era su única clave de acceso y no tiene otros factores configurados, su cuenta quedará sin segundo factor. Puede agregar una nueva clave en cualquier momento. Recuerde también borrar la clave guardada en su dispositivo o gestor de contraseñas.

7.5. Iniciar sesión con una clave de acceso

Después de ingresar su usuario y contraseña, el sistema le pedirá el segundo factor. Pueden darse dos situaciones:

Escenario A: la clave de acceso es su factor favorito (o el único)

1. Haga clic en «Ingresar» para iniciar la autenticación con la clave (figura 22).



Figura 22. *Inicio de sesión con clave de acceso*

2. El navegador o el sistema operativo mostrará las opciones disponibles (como en la figura 16). Si la clave está en ese dispositivo o en su gestor de contraseñas, haga clic en «Continuar» y confirme con su huella, PIN o bloqueo de pantalla.
3. Si la clave está en su teléfono, elija «Usar una llave de acceso diferente» y luego «Usa tu teléfono o tablet». Escanee el código QR con el teléfono y siga sus instrucciones (recuerde tener el Bluetooth activado).

Si completa los pasos correctamente, se iniciará la sesión.

Escenario B: tiene varios factores y la clave de acceso no es el favorito

1. En la pantalla del factor favorito, haga clic en «Otras formas de autenticación», debajo del botón «Ingresar» (figura 23).



Figura 23. *Enlace «Otras formas de autenticación»*

2. Seleccione «Clave de acceso» (figura 24).

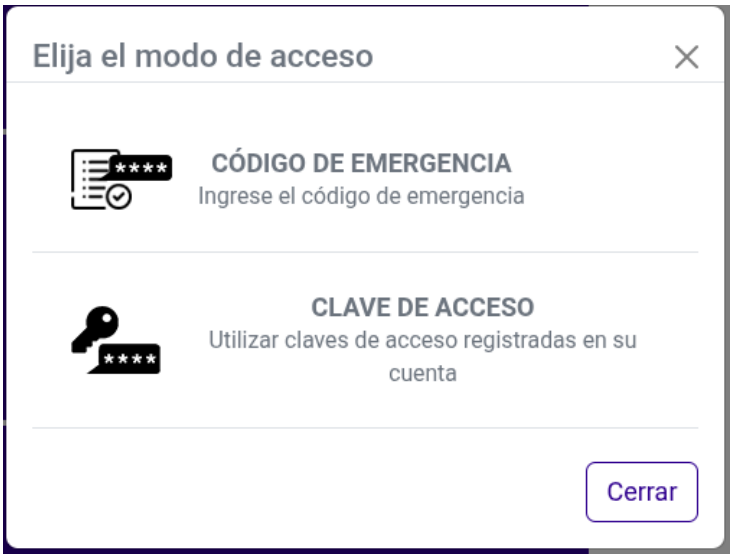


Figura 24. *Elegir «Clave de acceso»*

3. Continúe como en el escenario A.

8. Códigos de emergencia

Los códigos de emergencia (también llamados códigos de respaldo o *backup codes*) le permiten ingresar cuando no puede usar sus factores habituales, por ejemplo si perdió el teléfono. Cada código sirve **una sola vez**.

8.1. Códigos generados automáticamente

Los códigos se generan automáticamente al activar su primer factor de autenticación (OTP o clave de acceso) (figura 25).



Figura 25. *Códigos de emergencia generados*

Elija cómo guardarlos (figura 26):

- **Imprimir los códigos:** para conservar una copia en papel en un lugar seguro.
- **Guardar en PDF:** crea un archivo con los códigos; guárdelo en un dispositivo protegido.
- **Copiar al portapapeles:** para pegarlos, por ejemplo, en un gestor de contraseñas.

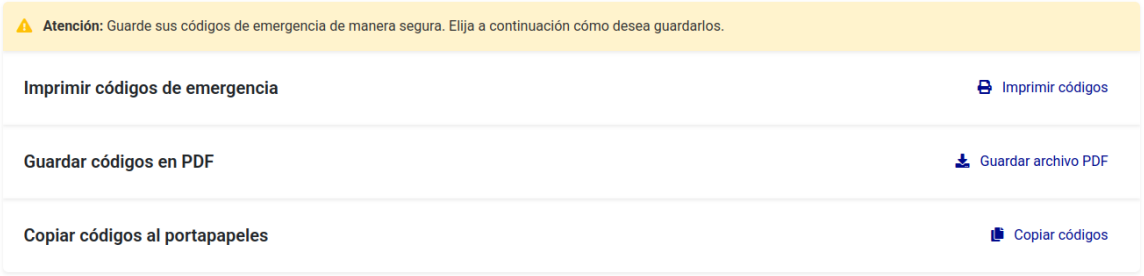


Figura 26. *Opciones para guardar los códigos de emergencia*

Importante: no comparta estos códigos con nadie. Cada código puede usarse una sola vez. Cada vez que se generan códigos nuevos, los anteriores quedan invalidados.

Los códigos no se pueden volver a ver una vez que sale de esta pantalla. Por eso, para continuar debe marcar «Ya guardé mis códigos de emergencia» y hacer clic en «He guardado los códigos y deseo continuar» (figura 27).



Figura 27. *Confirmación de que guardó los códigos*

8.2. Generar nuevos códigos de emergencia

Acceda a «Códigos de emergencia» desde el menú lateral o la pantalla inicial. Verá la fecha y hora de la última generación, cuántos códigos siguen siendo válidos y el botón para generar nuevos (figura 28).

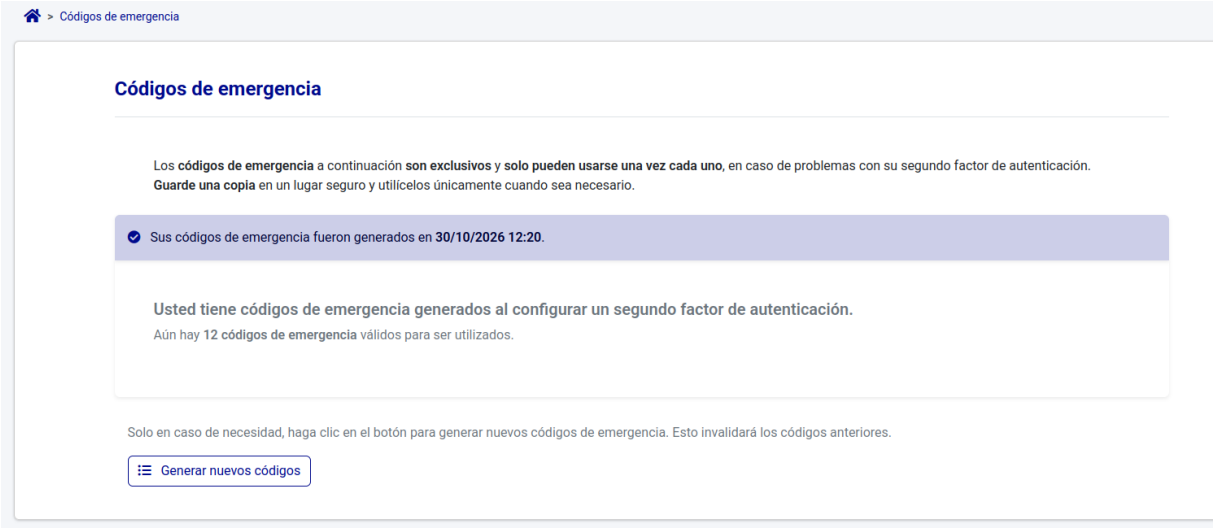


Figura 28. *Pantalla «Códigos de emergencia»*

Si todavía tiene códigos válidos y acceso a ellos, no es necesario generar otros. Para generar nuevos:

1. Haga clic en «Generar nuevos códigos».
2. Confirme con «Sí, generar nuevos códigos de emergencia» (figura 29). Los códigos anteriores quedarán invalidados inmediatamente.

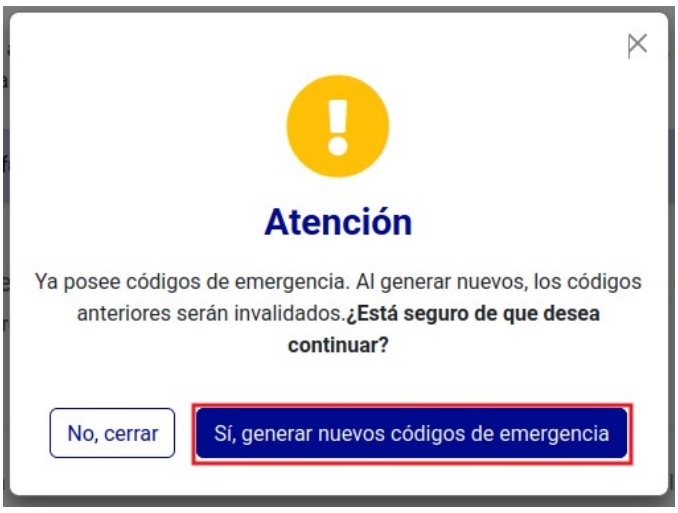


Figura 29. *Confirmación para generar nuevos códigos*

8.3. Iniciar sesión con un código de emergencia

Si tiene factores configurados (OTP o clave de acceso) pero no puede usar ninguno, puede ingresar con un código de emergencia. Es la forma recomendada de recuperar el acceso al propio Panel para reconfigurar sus factores.

1. Después de ingresar usuario y contraseña, en la pantalla del segundo factor haga clic en «Otras formas de autenticación», debajo del botón «Ingresar» (como en la figura 23).
2. Seleccione «Código de emergencia» (figura 30).



Figura 30. *Elegir «Código de emergencia»*

3. Ingrese uno de sus códigos válidos y haga clic en «Ingresar» (figura 31).



Figura 31. *Inicio de sesión con código de emergencia*

> **Nota:** una vez dentro del Panel, configure nuevamente su factor (por ejemplo, genere un nuevo código QR para el OTP) y, si le quedan pocos códigos, genere códigos nuevos.

9. Dispositivos confiables

Un dispositivo confiable es un navegador en un equipo (por ejemplo, «Ubuntu - Firefox») en el que no se le pedirá el segundo factor durante un tiempo. Agiliza el inicio de sesión, pero use esta opción solo en dispositivos propios, seguros y de uso exclusivo suyo.

9.1. Agregar un dispositivo confiable

1. Desde el dispositivo que desea marcar, acceda a «Dispositivos confiables» y haga clic en «Sí, agregar dispositivo» (figura 32).

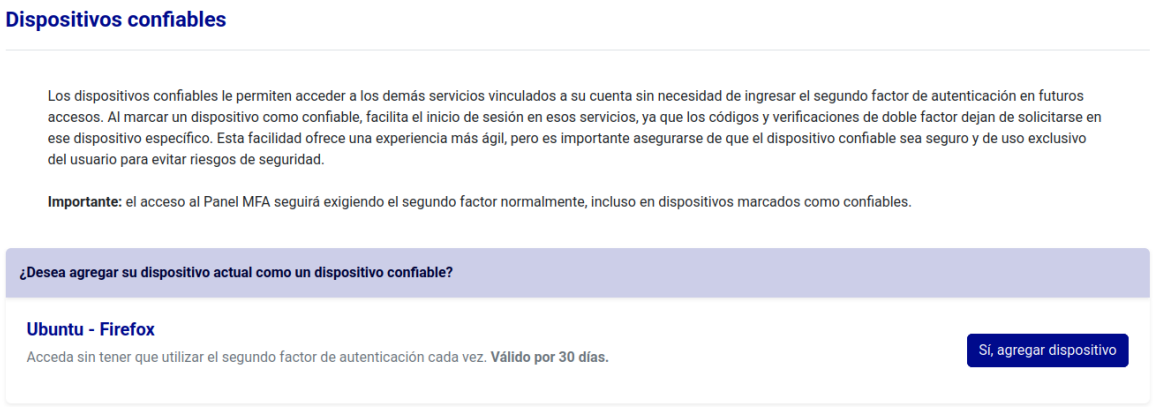


Figura 32. *Agregar el dispositivo actual como confiable*

2. Si lo desea, cambie el nombre del dispositivo y haga clic en «Guardar» (figura 33).



Figura 33. *Nombre del dispositivo confiable*

Tenga en cuenta:

- El dispositivo queda como confiable durante el período indicado en pantalla (actualmente 30 días). Puede renovarlo en cualquier momento; al vencer, se le volverá a pedir el segundo factor.
- Cada navegador de cada equipo se registra una sola vez. Mientras esté activo, no se puede volver a agregar; si lo elimina o vence, volverá a aparecer el botón «Sí, agregar dispositivo».
- **El acceso al Panel de Seguridad MFA siempre exige el segundo factor**, aunque el dispositivo sea confiable.
- No funciona en ventanas de navegación privada o incógnito: al cerrarlas se borran las cookies y se pierde la configuración.

9.2. Ver la lista de dispositivos confiables

En «Dispositivos confiables» verá, para cada dispositivo registrado (figura 34):

- **Dispositivo:** nombre del dispositivo, por ejemplo «Windows - Chrome».
- **Información:** navegador y sistema operativo.
- **Fecha de configuración:** cuándo se registró como confiable.
- **Validez:** fecha de vencimiento; se muestra en rojo cuando está próxima.
- **Indicador de dispositivo actual:** destaca el dispositivo que está usando en este momento.

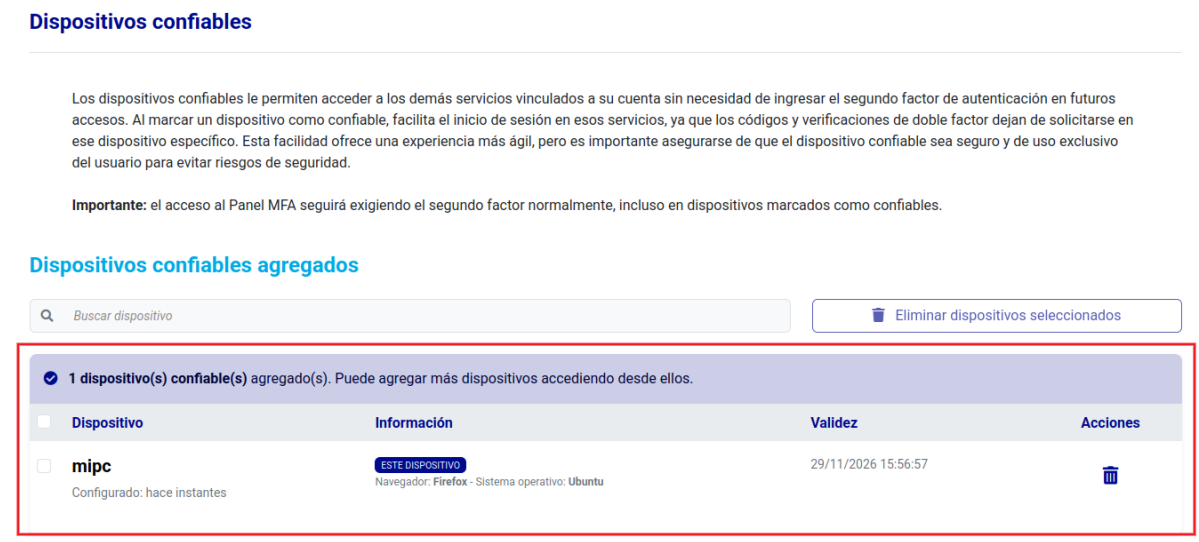


Figura 34. *Lista de dispositivos confiables*

9.3. Eliminar dispositivos confiables

Para eliminar un dispositivo:

1. Haga clic en el icono de la papelera de la columna «Acciones», junto al dispositivo (figura 35).

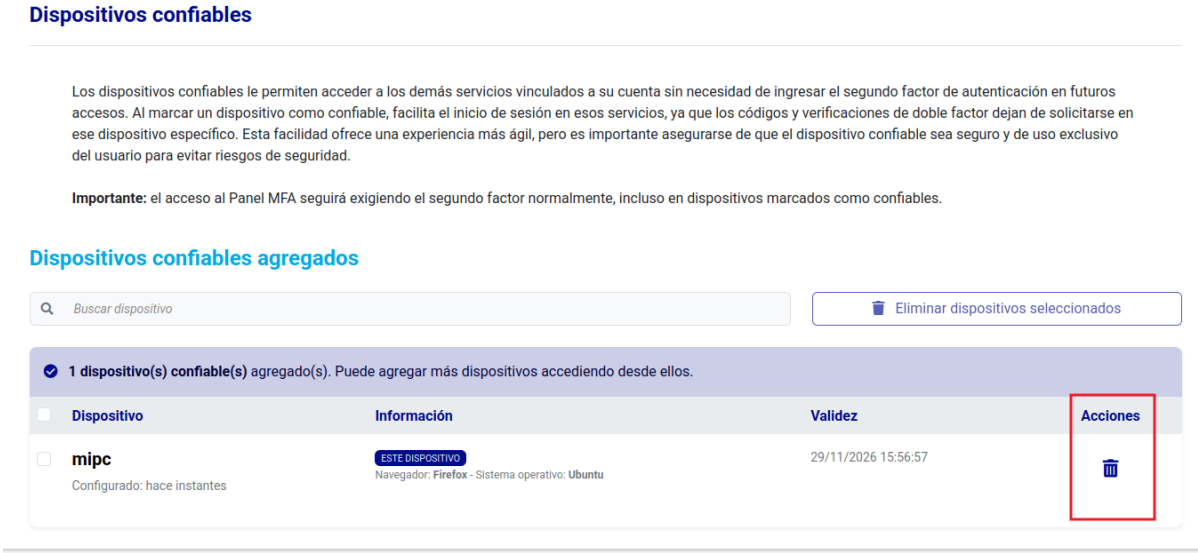


Figura 35. *Eliminar un dispositivo confiable*

2. Confirme con «Sí, eliminar» (figura 36).

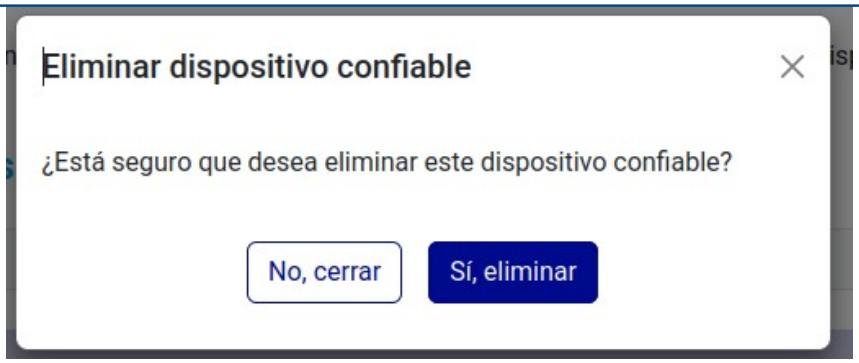


Figura 36. *Confirmación de eliminación*

Para eliminar todos los dispositivos a la vez (opción disponible solo si tiene más de uno):

1. Haga clic en «Eliminar todos los dispositivos».
2. Confirme con «Sí, eliminar todos».

> **Importante:** si pierde un dispositivo marcado como confiable o se lo roban, elimínelo de la lista lo antes posible y cambie su contraseña.

10. Consideraciones finales

La autenticación multifactor protege su cuenta incluso si alguien obtiene su contraseña. En resumen:

- **Contraseña temporal (OTP):** códigos que genera una aplicación en su teléfono y que caducan en segundos.
- **Claves de acceso:** la opción más práctica y segura; su dispositivo confirma su identidad sin escribir códigos.
- **Códigos de emergencia:** su respaldo si pierde los otros factores. Guárdelos en un lugar seguro.
- **Dispositivos confiables:** evitan pedir el segundo factor en sus equipos personales durante un tiempo. Úselos solo en dispositivos seguros y de uso exclusivo.

Recomendación: configure al menos dos factores (por ejemplo, OTP y una clave de acceso) y mantenga sus códigos de emergencia a mano. Así nunca quedará sin forma de ingresar.