MFA

Nuevo proceso de acceso a GWC con Autenticación Multifactor

Netviax Glas

soporteglas@netviax.com

+598 2917 04 06

Sarandí 425 Of. 101
Montevideo, Uruguay

www.netviax.com

Guía para usuarios

Para seguir fortaleciendo la seguridad y proteger el acceso a tu cuenta, Netviax incorporará un nuevo proceso de autenticación al momento de ingresar a GWC (Netviax B2B). Este cambio implica una acción adicional al momento de ingresar a la herramienta, pero te brinda mayor protección frente a acceso no autorizados.

¿Qué es la Autenticación Multifactor (MFA)?

El MFA es un sistema que, además de tu usuario y contraseña, te solicita una segunda verificación para confirmar que realmente sos tu quien está accediendo.

¿Por qué se utiliza?

- Aumentar la seguridad de tu cuenta
- Evitar accesos indebidos incluso si alguien obtiene tu contraseña
- Es un estándar internacional de protección

¿Qué cambia en la página de acceso a GWC?

La pantalla de login se actualizará para incorporar este nuevo paso de verificación. Seguirás ingresando tu usuario y contraseña como siempre, pero luego se te solicitará la autenticación MFA.

¿Qué significa autenticarse?

Consiste en confirmar tu identidad a través de un método adicional. En esta primer versión lo podrás hacer de dos formas:

- Código enviado a tu cuenta de mail (la que usas como usuario de GWC)
- Aplicación Microsoft Authenticator

¿Cuándo se me pedirá MFA?

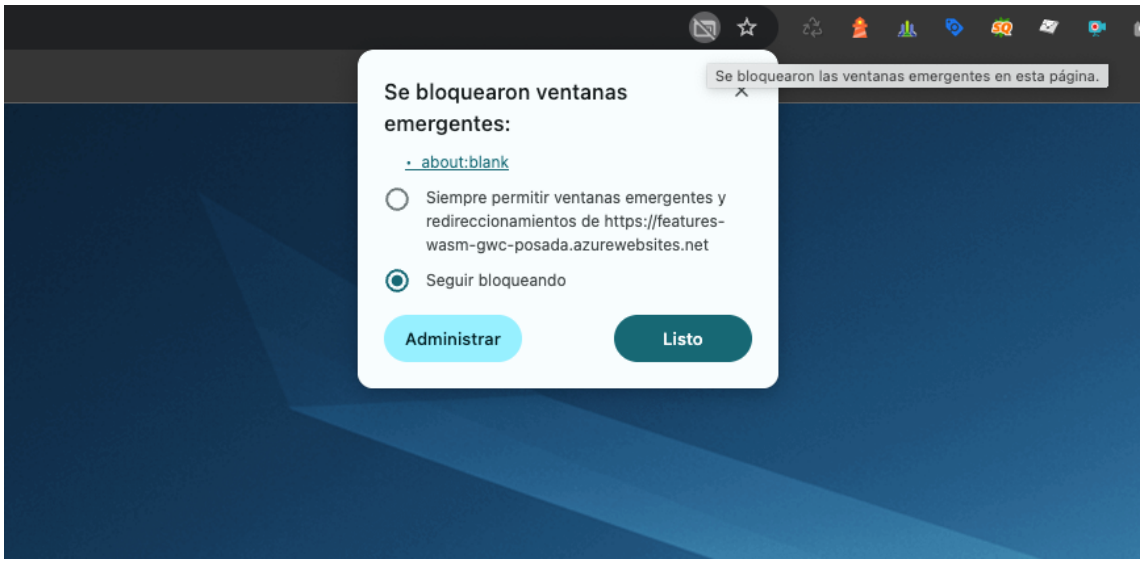
En esta primer etapa se solicitará:

- Al momento de ingresar a GWC por primera vez
- Si se detecta un intento de acceso desde otro dispositivo, aplicación o ubicación.

Bloqueo de ventanas emergentes (pop-ups)

La primera vez que ingreses a GWC utilizando el nuevo proceso de autenticación, es posible que tu navegador tenga bloqueadas las ventanas emergentes (pop-ups). Si esto ocurre, verás una pantalla similar a la siguiente:

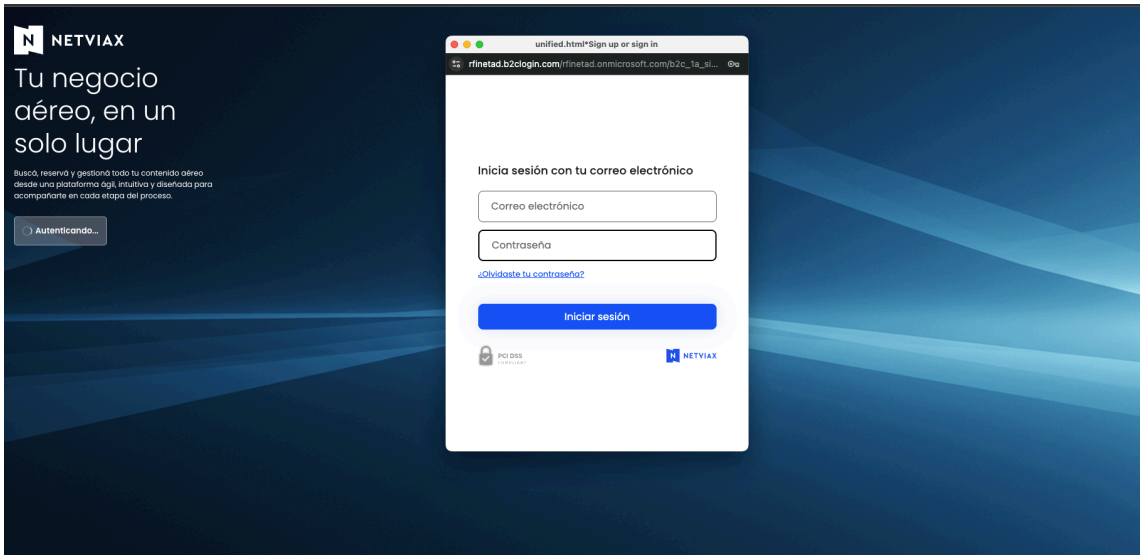
Para continuar, deberás habilitar las ventanas emergentes para el sitio de GWC. Una vez permitido el pop-up, el sistema te redirigirá automáticamente al proceso de autenticación y podrás ingresar sin inconvenientes.



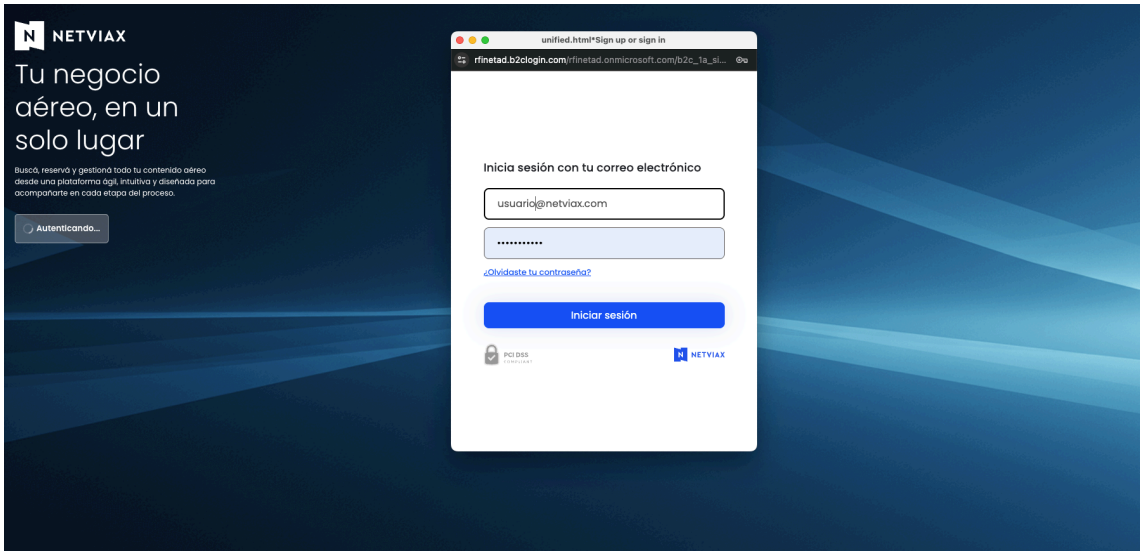
Inicio del proceso de acceso a GWC

Antes de seleccionar un método de autenticación, ya sea como parte del flujo login y autenticación o para el registro inicial, el usuario deberá iniciar sesión en GWC con sus credenciales habituales.

1. Ingresar a la url de acceso a GWC: https://gwc.glas.travel



2. Introducir usuario y contraseña



3. Clickear botón Iniciar Sesión.
4. Una vez validadas las credenciales, el sistema solicitará completar el segundo factor de autenticación.
   En la imagen se ve como sobre el lado izquierdo de la pantalla un indicador del

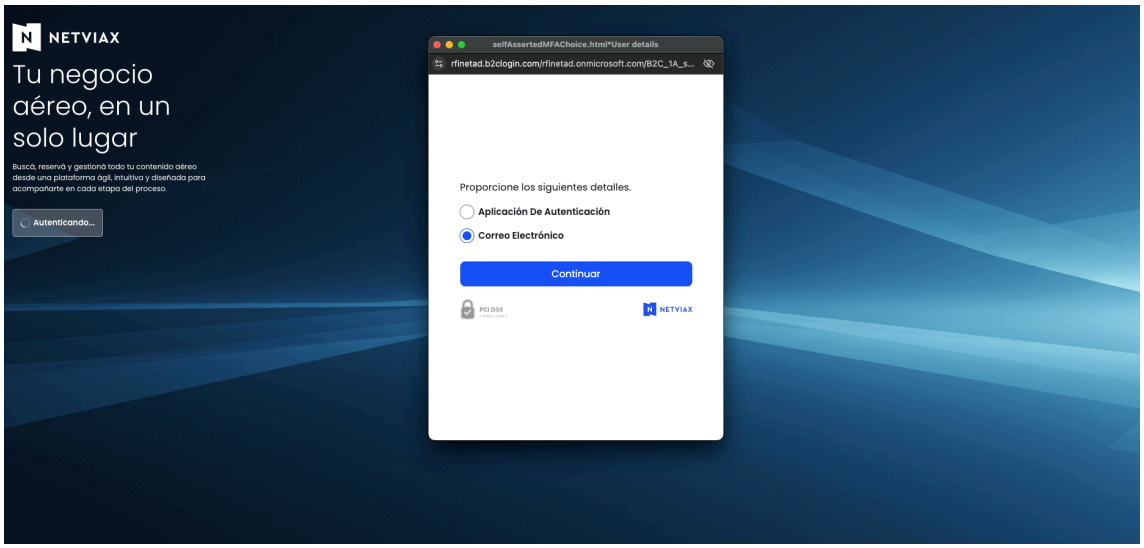
avance del proceso, donde se muestran los estados Autenticando u Obteniendo permisos y configuración.

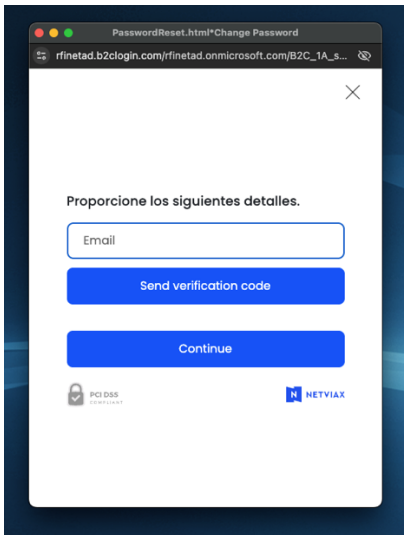
5. Finalizado el proceso inicial, el sistema solicitará completar la autenticación MFA, presentando al usuario las opciones disponibles para continuar:
    a. Autenticación por mail
    b. Autenticación mediante Microsoft Authenticator

    En este punto el usuario podrá seleccionar el método preferido.

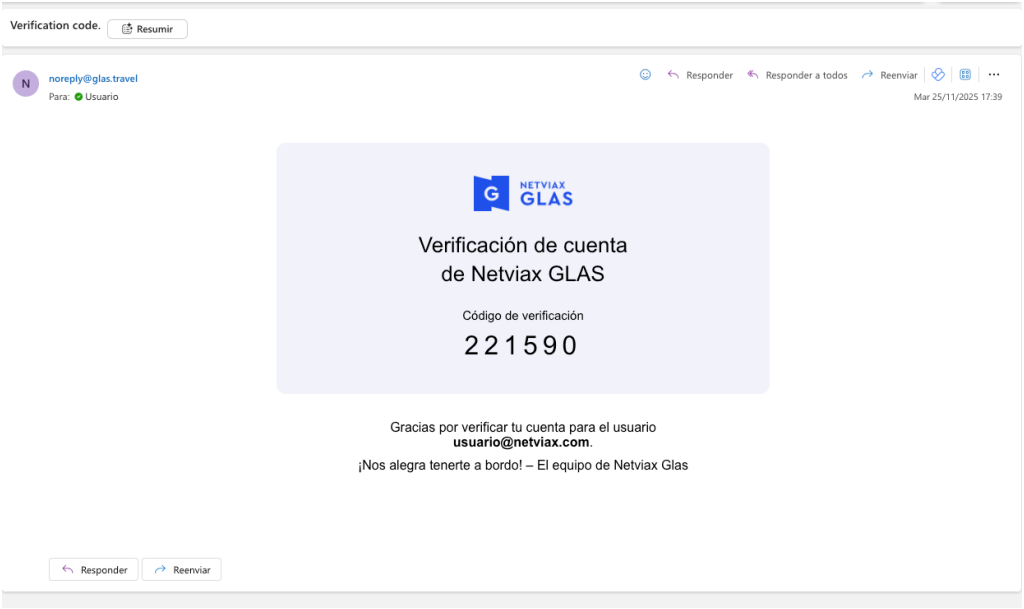
Método autenticación: código enviado al mail

1. Ingresa tu usuario y contraseña.
2. Selecciona la opción “email”.

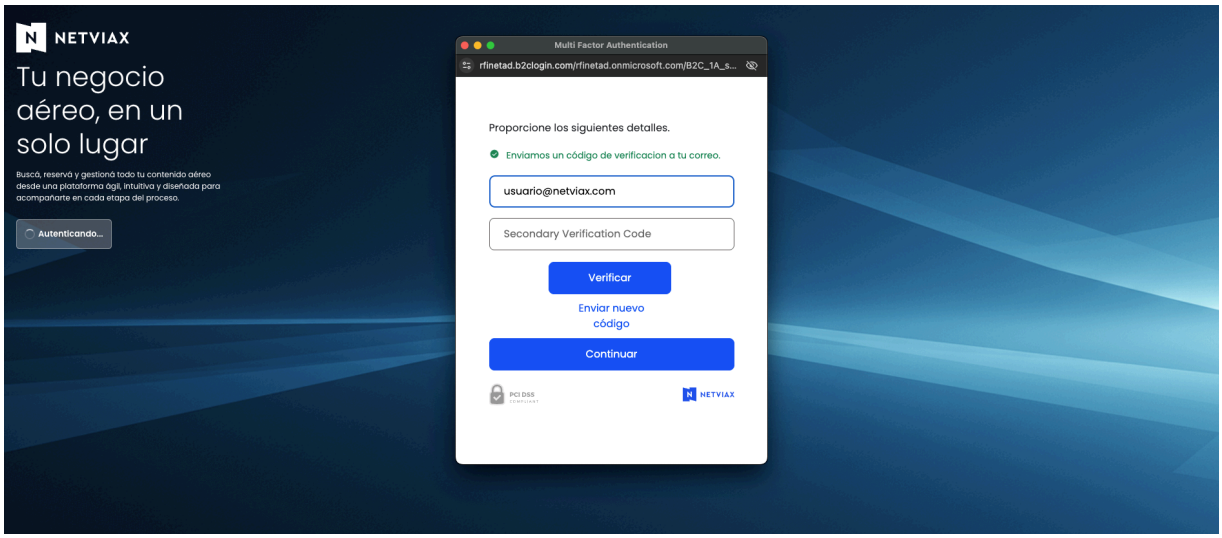




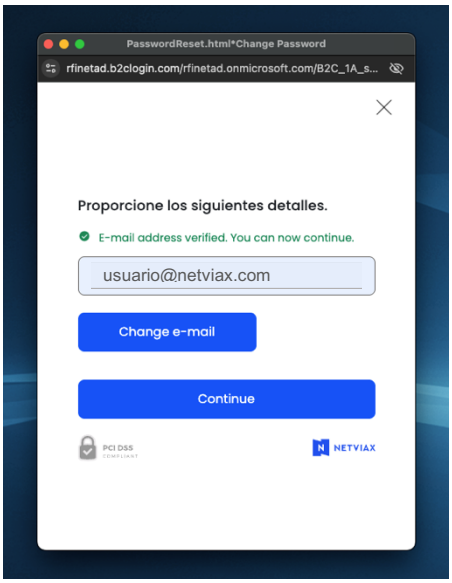
3. Revisa tu casilla de mail donde habrás recibido un mail con el código de verificación.



4. Ingresa el código recibido para completar el acceso y presiones Verificar.



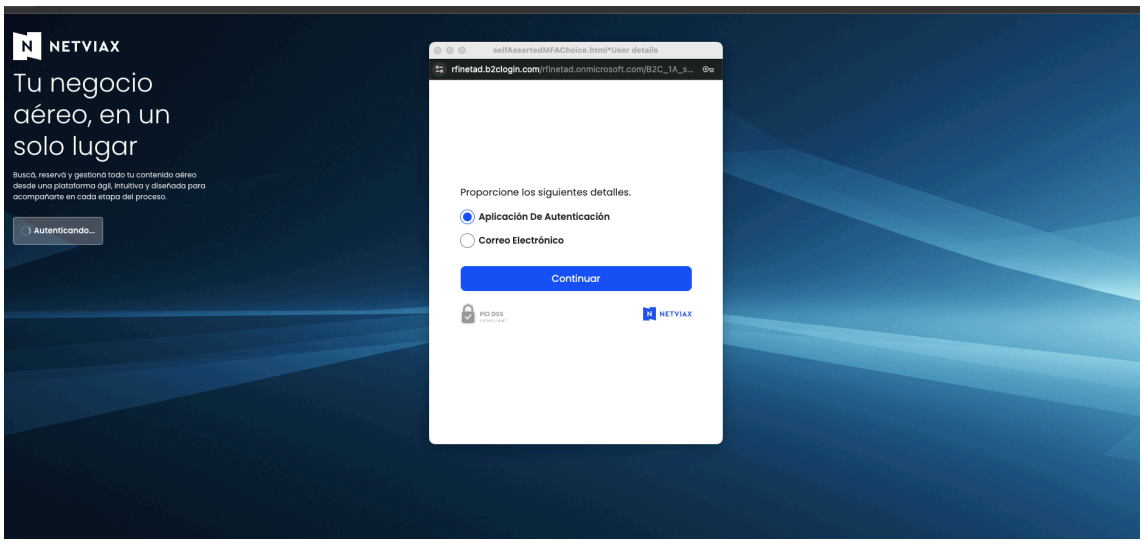
5. Una vez verificado, el sistema le indicará que el usuario fue verificado y que puede continuar. Hacer click en Continuar para completar el proceso de validación.

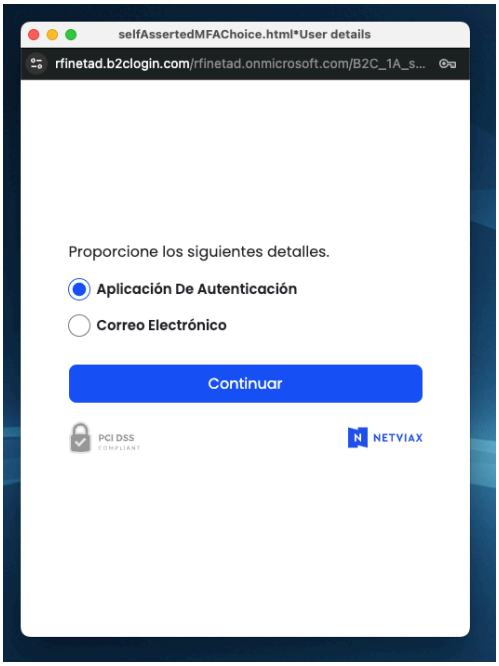


Una vez confirmado el código, el sistema permitirá el acceso al usuario y la sesión quedará autenticada correctamente.

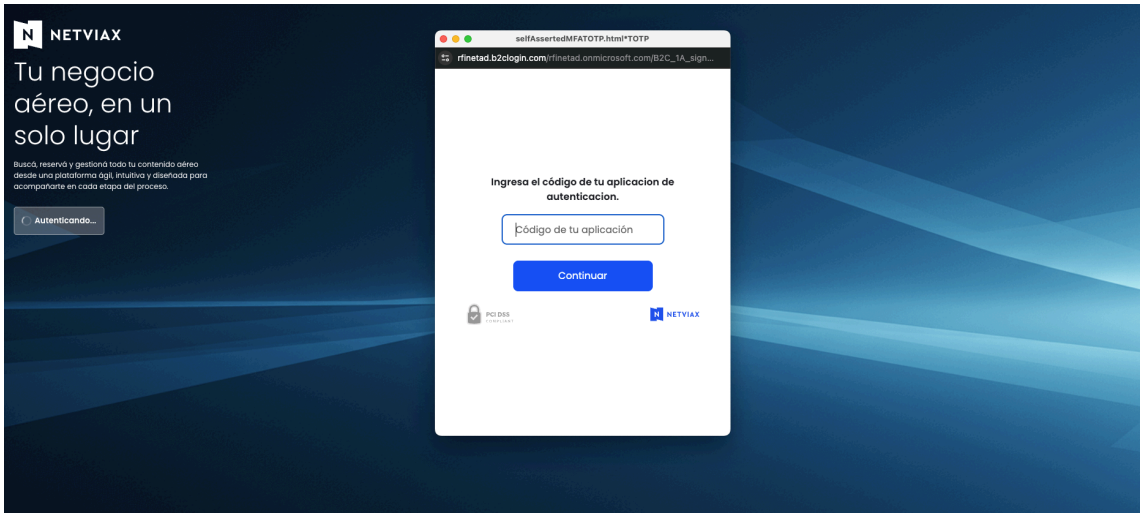
Método autenticación: Microsoft Authenticator

1. Ingresa tu usuario y contraseña.
2. Selecciona la opción Aplicación de autenticación.





3. Abrir la aplicación Microsoft Authenticator en su celular.
4. Dentro de la aplicación, localizar la cuenta asociada a GWC identificada como Glas Auth, la cual mostrará el correo del usuario que está iniciando sesión.
5. Verificar el código temporal generado por la app (código dinámico).
6. Ingresar este código en el campo Código de tu aplicación que aparece en la pantalla de autenticación.

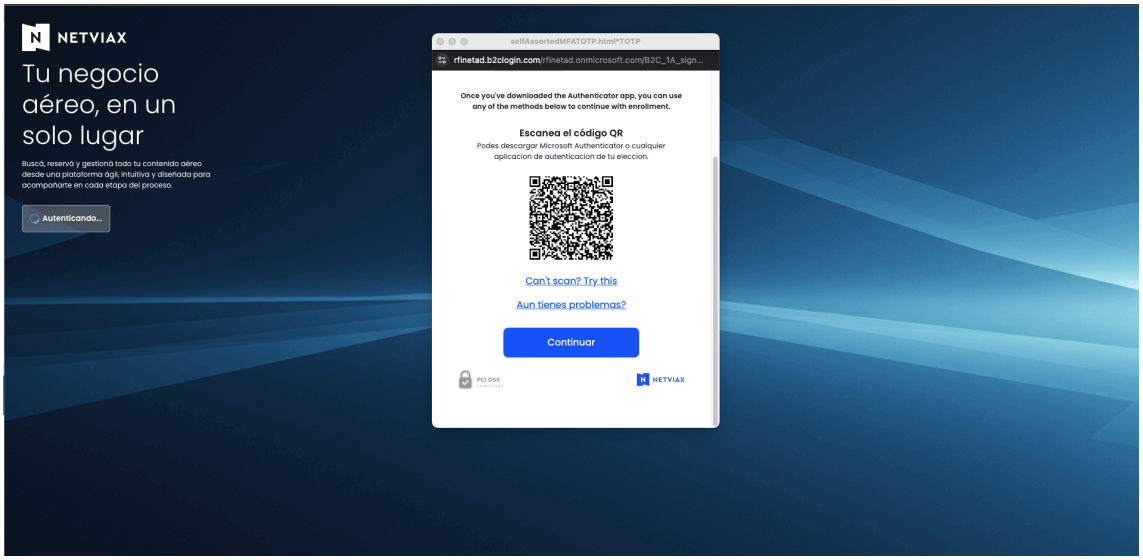


7. Clickear Continuar para completar el proceso de validación.

Una vez confirmado el código, el sistema permitirá el acceso al usuario y la sesión quedará autenticada correctamente.

Configuración inicial de Microsoft Authenticator

Para poder utilizar Microsoft Authenticator como segundo factor de autenticación (MFA) en GWC, es necesario contar con la aplicación instalada y asociada previamente al usuario.
La primera vez que el usuario selecciona este método de autenticación GWC mostrará una pantalla con las instrucciones para descargar la aplicación, en caso de no tenerla instalada aún.



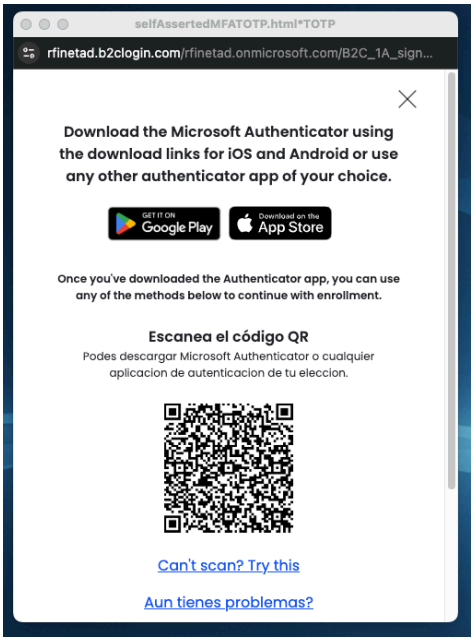
Este método brinda mayor seguridad y rapidez al autenticarse. Es una aplicación gratuita disponible en Google Play y App Store.

Descargar la aplicación

- Google Play (Android): buscar Microsoft Authenticator
- App Store (iPhone): buscar Microsoft Authenticator

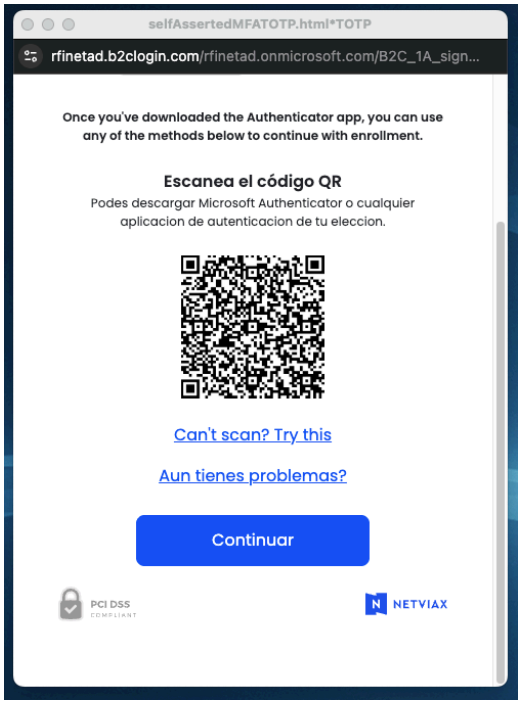
Abrir la aplicación en el celular y agregar la cuenta

1. Al ingresar seleccionar el ícono con el QR, esto permitirá que captures el código QR
2. Cuando estes configurando el ingreso en GWC, se mostrará un código QR que capturarás con la aplicación como indica el punto anterior.

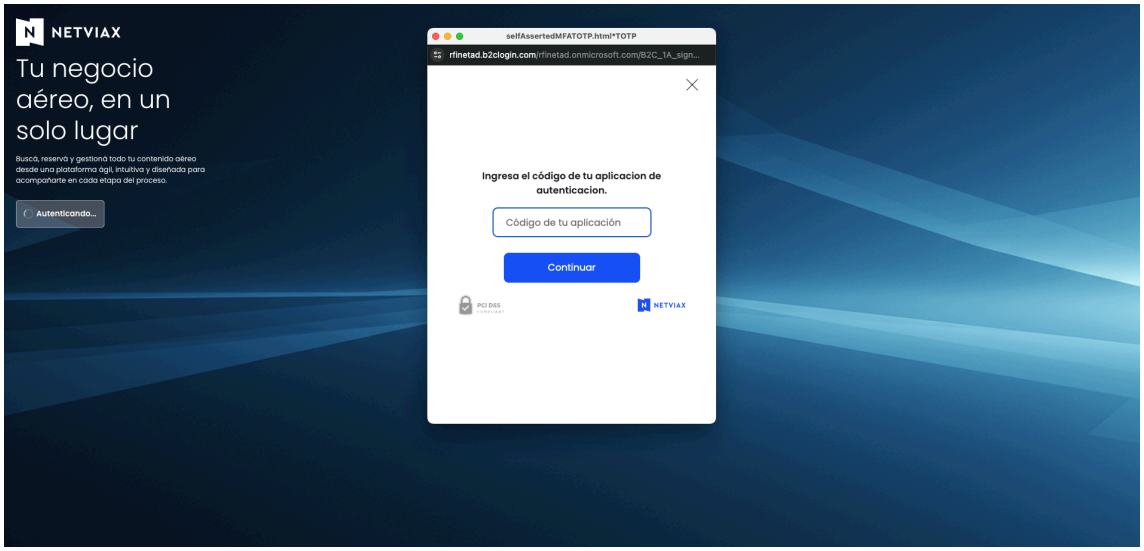


Este procesos solo debe realizarse una vez. Luego de configurado, el usuario solo deberá utilizar los códigos generados por la app para validar su acceso.
Al finalizar, aparecerá en la app la entrada identificada como Glas Auth, junto al correo asociado al acceso.

Una vez que la cuenta haya sido agregada exitosamente el usuario deberá seleccionar el botón Continuar (ubicado debajo del código QR de la pantalla GWC como se muestra en la siguiente imagen).



A continuación el sistema solicitará ingresar el código dinámico generado por la aplicación Microsoft Authenticator.



Una vez ingresado el código correctamente, la cuenta quedará configurada y Microsoft Authenticator estará habilitado para generar los códigos que se utilizarán en los próximos accesos.

Cada vez que GWC te pida la autenticación MFA:

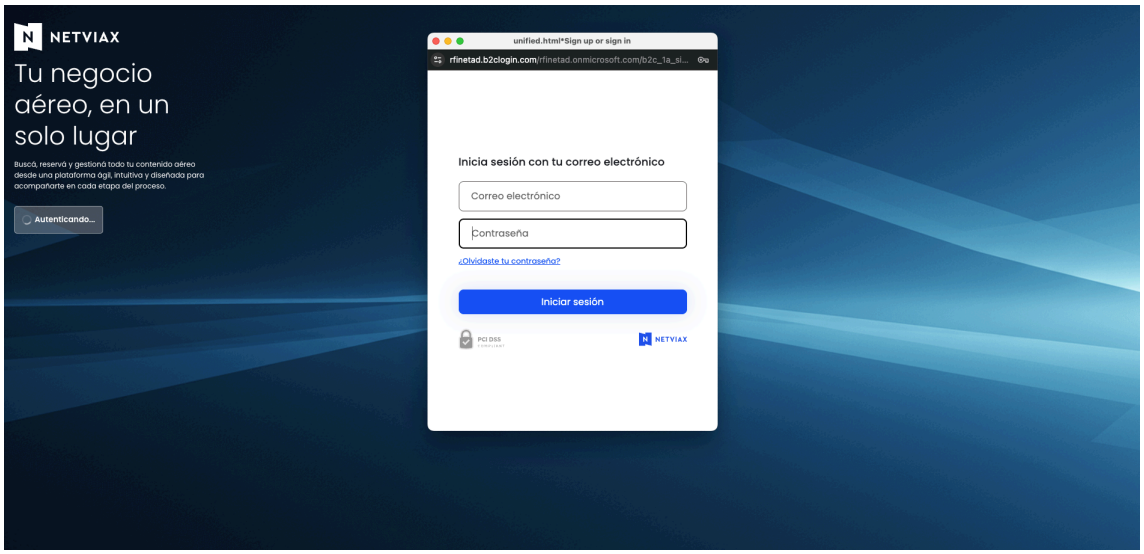
1. Abrir Microsoft Authenticator
2. Revisar el código que se genera
3. Ingresar el código en GWC (el código cambia cada 10 segundos por seguridad)

Nota importante:
Para completar correctamente la configuración del Microsoft Autenticator, el usuario deberá utilizar únicamente el código QR que se muestre en la pantalla de GWC durante el proceso de vinculación. El código QR incluido en esta guía es solo ilustrativo y no debe ser escaneado, ya que no permitirá asociar la cuenta real del usuario ni completar el registro.
Escanear el QR equivocado impedirá la vinculación correcta del autenticador y bloqueará la finalización del proceso.

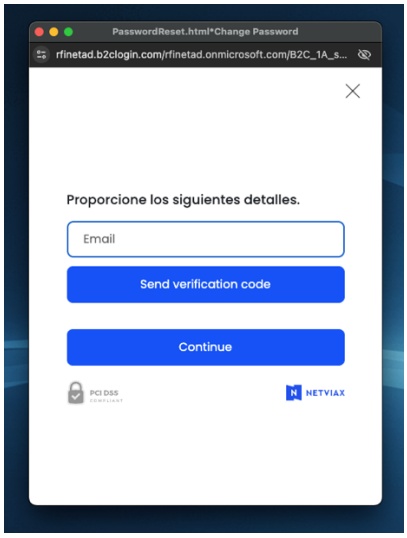
Olvidaste tu contraseña

Si el usuario no recuerda su contraseña, podrá reestablecerla fácilmente siguiendo estos pasos:

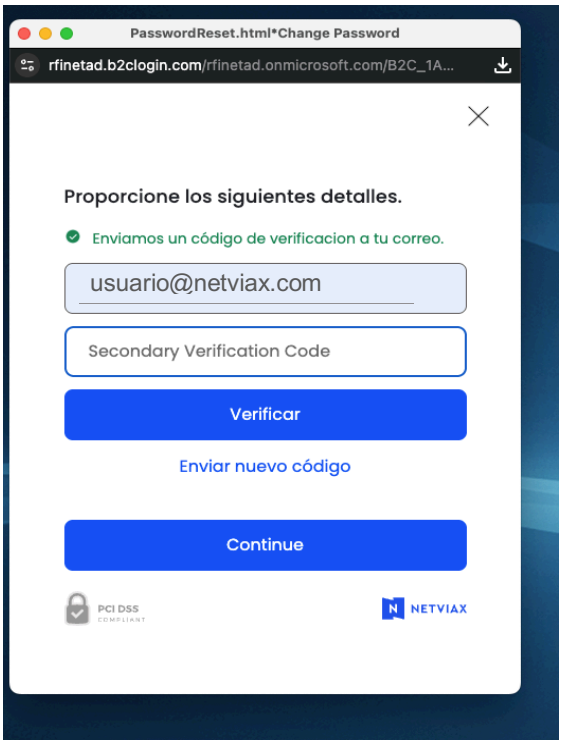
1. Acceder a la pantalla de inicio de la sesión de GWC.
   Allí deberá seleccionar la opción “¿Olvidaste tu contraseña?”



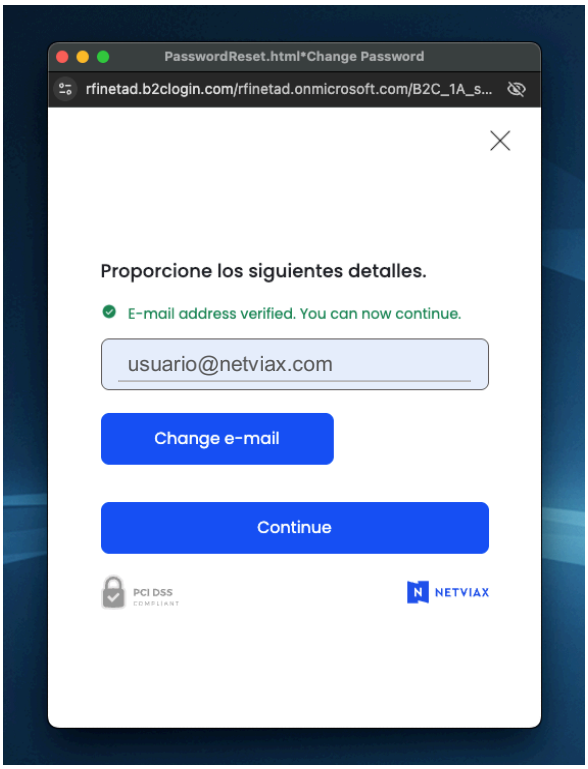
2. Ingresar la dirección de correo electrónico registrada.
   El sistema solicitará el correo asociado a la cuenta de GWC para validar la identidad del usuario. Una vez ingresado el mail deberá presionar el botón “Send Verification Code”.



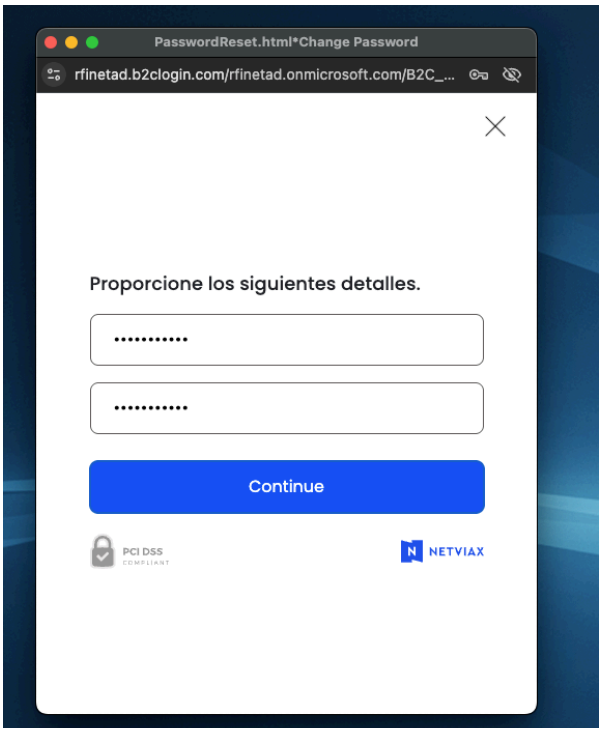
3. Revisar casilla de correo.
   GWC enviará un mail a la cuenta indicada con un código de verificación que deberás ingresar en el cuadro “Verification Code” y seleccionar Verificar.



4. Avanzar luego de la verificación
   Una vez verificado el sistema informará que la verificación fue realizada y que puedes continuar, para esto deberás seleccionar el botón “Continuar”.



5. Crear una nueva contraseña
   La nueva contraseña debe cumplir con la política de seguridad vigente, una vez confirmada el sistema guardará los cambios. La contraseña debe contener al menos:
   - 12 caracteres
   - 1 mayúscula
   - 1 número
   - 1 carácter especial



6. Iniciar sesión nuevamente
   Tras actualizar la contraseña, el usuario podrá ingresar a GWC normalmente utilizando su nueva contraseña.