| Procedimiento | |
|---|---|
| **Servicios Office 365** | **Versión** |
| **Enrolamiento Segundo Factor de Autenticación** | **1.7** |

## NOTA DE CONFIDENCIALIDAD

Queda prohibida cualquier apropiación, difusión, distribución o copia del presente procedimiento de seguridad de la información para ser utilizado fuera de la ACHS.

El incumplimiento de este procedimiento será considerado falta grave, pudiendo ser causal de sanciones disciplinarias según lo indicado en Reglamento Interno.

## DISTRIBUCIÓN Y ACCESO:

GERENCIA TRANSF. DIGITAL Y TECNOLOGÍA

## CONTROL DOCUMENTAL

| Versión | ELABORO | | REVISO | | APROBO | | MODIFICACIONES EN EL PROCESO |
|---|---|---|---|---|---|---|---|
| | Fecha | Nombre o Firma | Fecha | Nombre o Firma | Fecha | Nombre o Firma | |
| 1 | 05/2019 | Cristian Sáez | 09/2019 | Oscar Frías | 09/2019 | Oscar Frías | Creación del documento |
| 2 | 01/2020 | Cristian Sáez | 01/2020 | Oscar Frías | 01/2020 | Oscar Frías | Actualización de documento |
| 3 | 11/2020 | Néstor Díaz | 11/2020 | Rodrigo Soto | 11/2020 | Rodrigo Soto | Actualización de documento |
| 4 | 06/2021 | Rodrigo Lucero | 06/2021 | Rodrigo Soto | 06/2021 | Rodrigo Soto | Comprobación de seguridad adicional |
| 5 | 11/2022 | Cristian Sáez | 11/2022 | Néstor Díaz | 11/2022 | Rodrigo Soto | Actualización de información y procesos |
| 6 | 06/2023 | Cristian Sáez | 06/2023 | Néstor Díaz | 08/2023 | Christian Campodónico | Actualización para servicios Office 365 |
| 7 | 09/2023 | Cristian Sáez | 09/2023 | Christian Campodónico | 09/2023 | Christian Campodónico | Proceso de Office 365 |


Este documento es de propiedad exclusiva de ACHS y su uso debe estar ceñido a lo dispuesto en la clasificación de este, quedando prohibida la divulgación y/o reproducción total o parcial del contenido de éste sin la debida autorización por parte de la Jefatura TI. Su uso y distribución solo está autorizado al interior de ACHS y por parte del personal debidamente habilitado.

## Índice


**1. ¿Qué es un segundo factor de autenticación (2FA)?** ..... 3

**2. Método para verificar su identidad** ..... 4

**3. Habilitar segundo factor de autenticación (2FA)** ..... 4

3.1. Inicio de sesión ..... 4

3.2. Método para verificar su identidad ..... 5

3.3. Configuración en la aplicación móvil ..... 6

3.4. Configuración para comprobación de seguridad ..... 8

**4. Comprobar el funcionamiento de validación con 2FA** ..... 11

4.1. Ejemplo de conexión a Outlook 365 vía Web ..... 11





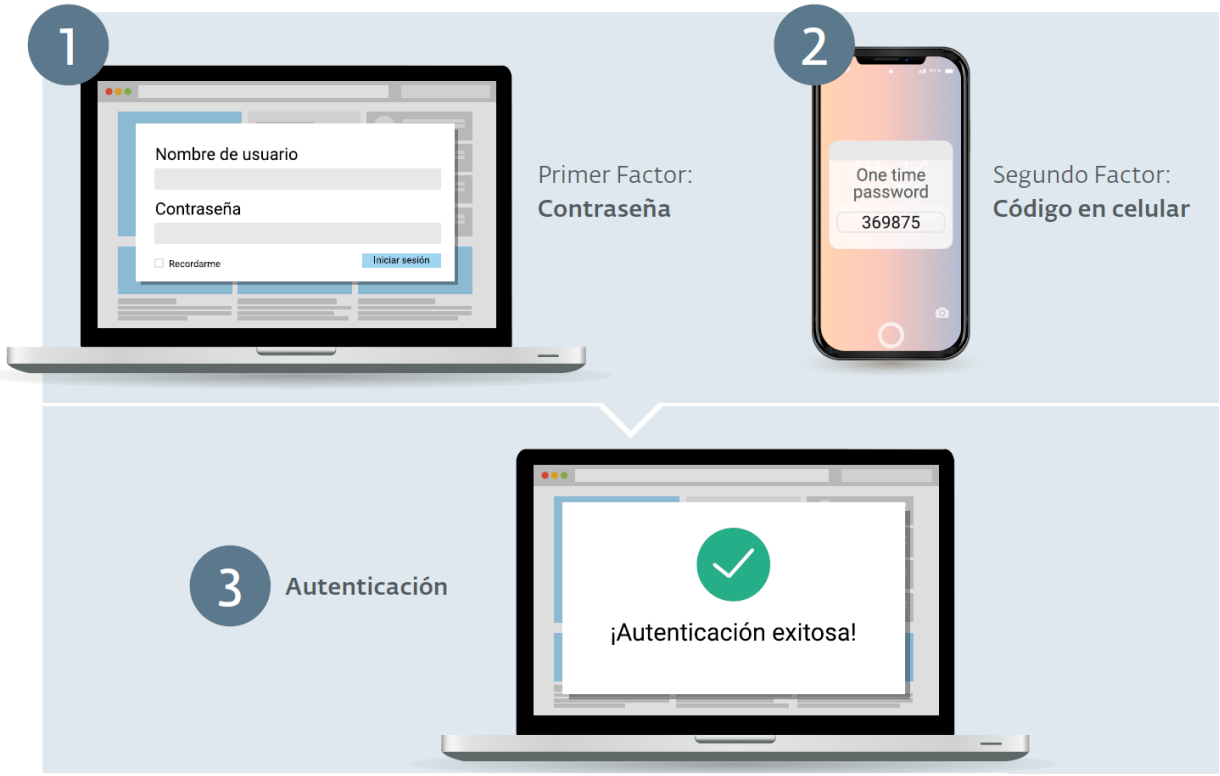



Este documento es de propiedad exclusiva de ACHS y su uso debe estar ceñido a lo dispuesto en la clasificación de este, quedando prohibida la divulgación y/o reproducción total o parcial del contenido de éste sin la debida autorización por parte de la Jefatura TI. Su uso y distribución solo está autorizado al interior de ACHS y por parte del personal debidamente habilitado.

## 1. ¿Qué es un segundo factor de autenticación (2FA)?

El segundo factor de autenticación es una capa adicional de seguridad, sumada a la contraseña, para verificar la identidad de un usuario. De este modo, en caso de que alguien robase sus credenciales para iniciar sesión, su cuenta no correría peligro.

La autenticación en dos pasos es una medida de seguridad muy efectiva para proteger nuestra cuenta de intento de accesos indebidos y garantizar que es ¡quien dice ser!.




Este esquema muestra el proceso de autenticación en una cuenta con la capa de seguridad adicional activada.

La solicitud del **segundo factor de autenticación (2FA)** solo será solicitada si la conexión es **fuera de la red corporativa** de la Asociación Chilena de Seguridad.


Este documento es de propiedad exclusiva de ACHS y su uso debe estar ceñido a lo dispuesto en la clasificación de este, quedando prohibida la divulgación y/o reproducción total o parcial del contenido de éste sin la debida autorización por parte de la Jefatura TI. Su uso y distribución solo está autorizado al interior de ACHS y por parte del personal debidamente habilitado.

## 2. Método para verificar su identidad

La opción más recomendable para validar la autenticación es utilizar notificaciones desde la aplicación móvil **Microsoft Autenticator**, disponible para dispositivos Android y iOS.

No obstante, es posible agregar otros métodos adicionales, como mensaje SMS o llamada telefónica. Puede seleccionar:

- Aplicación Microsoft Autenticator
- Número de teléfono (*procedimiento con nombre **PCDT - Habilitar 2FA Microsoft - Otros métodos***)
  - Recibir un mensaje de texto con un código
  - Responder a una llamada

Este procedimiento está orientado a utilizar la aplicación móvil **Microsoft Autenticator**

## 3. Habilitar segundo factor de autenticación (2FA)

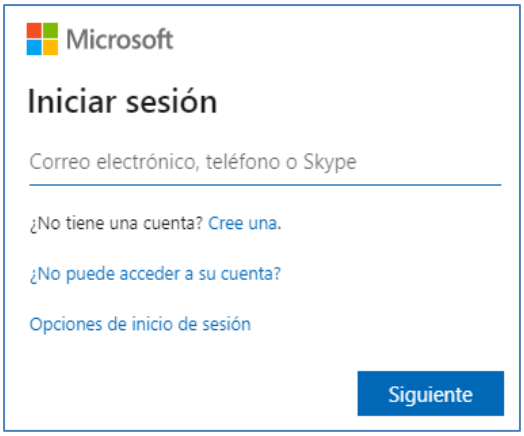
Para configurar el segundo factor de autenticación en su cuenta de usuario debe seguir los siguientes pasos.

- Ingresar a la url **https://aka.ms/mfasetup**

### 3.1. Inicio de sesión

Una vez haya ingresado a la url, solicitará iniciar sesión.

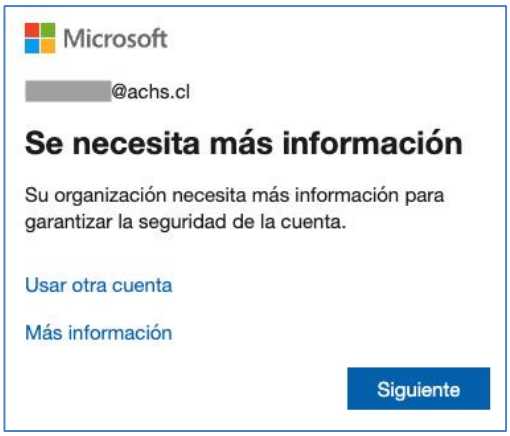
Debe ingresar su cuenta de usuario ACHS y posteriormente la contraseña.




Para las cuentas **@ext.achs.cl** debe ingresar con el dominio **@achs.cl**

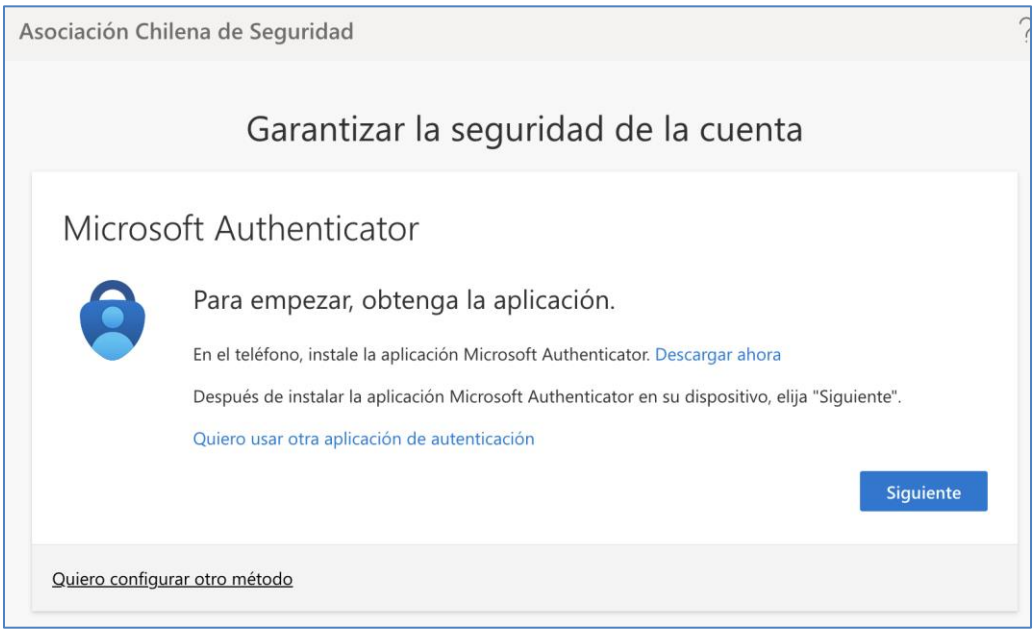

Este documento es de propiedad exclusiva de ACHS y su uso debe estar ceñido a lo dispuesto en la clasificación de este, quedando prohibida la divulgación y/o reproducción total o parcial del contenido de éste sin la debida autorización por parte de la Jefatura TI. Su uso y distribución solo está autorizado al interior de ACHS y por parte del personal debidamente habilitado.

Seguidamente solicitará ir al proceso de configuración, haga clic en **Siguiente**.




### 3.2. Método para verificar su identidad

En la siguiente página por defecto entrega la opción recomendada, de utilizar la aplicación móvil **Microsoft Authenticator**.

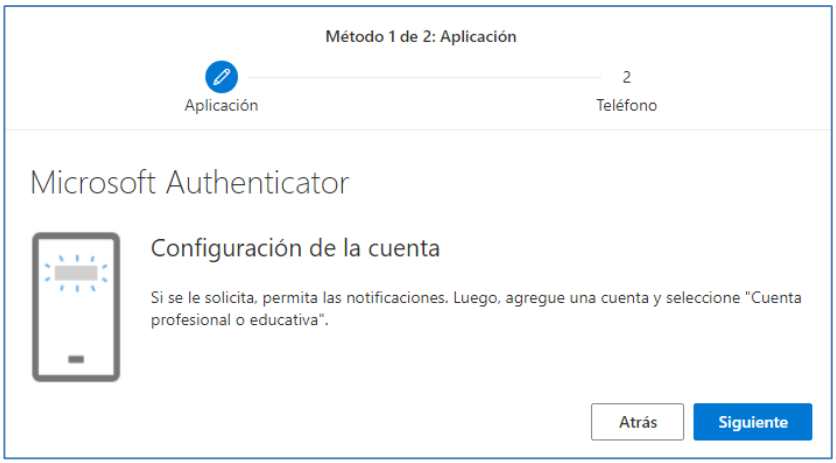



- En su teléfono, instale la aplicación **Microsoft Authenticator**.
- Después de instalar la aplicación en su dispositivo móvil, elija **Siguiente**.


Este documento es de propiedad exclusiva de ACHS y su uso debe estar ceñido a lo dispuesto en la clasificación de este, quedando prohibida la divulgación y/o reproducción total o parcial del contenido de éste sin la debida autorización por parte de la Jefatura TI. Su uso y distribución solo está autorizado al interior de ACHS y por parte del personal debidamente habilitado.

### 3.3. Configuración en la aplicación móvil

Una vez instalada la aplicación en el dispositivo móvil, el siguiente paso es configurar su cuenta usuario ACHS. A continuación, haga clic en **Siguiente**.

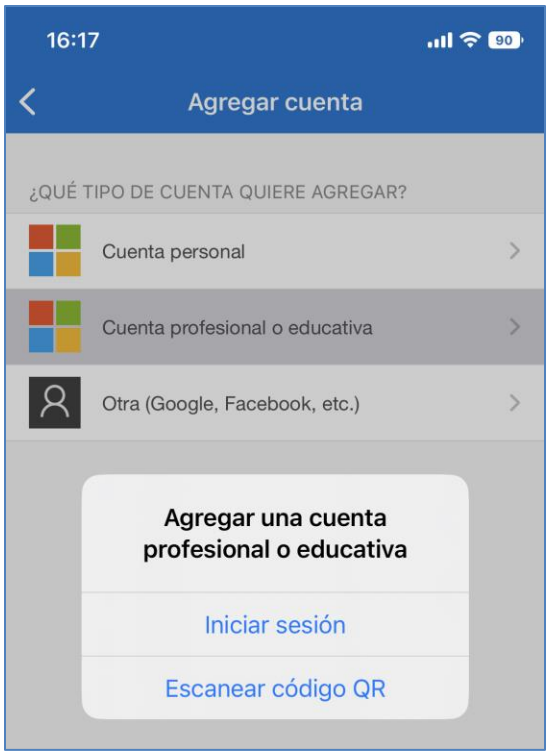



Seguidamente vaya a su teléfono móvil seleccione la aplicación **Microsoft Authenticator**.

Al acceder por primera vez a la aplicación, pulse el icono "**+**" y elegir la opción **cuenta profesional o educativa**.

La aplicación solicitará acceso a la cámara del dispositivo móvil para poder escanear el **código QR** que se muestra en la pantalla de su computador. Debe Permitir el acceso a la misma.

En este procedimiento se utilizará la opción "escanear código QR".





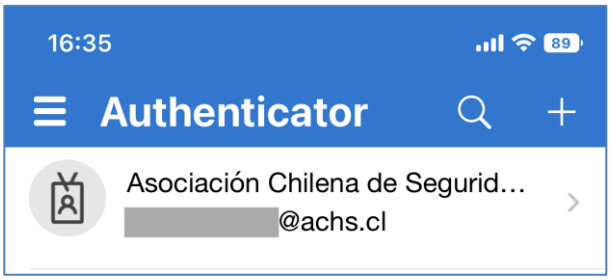
Este documento es de propiedad exclusiva de ACHS y su uso debe estar ceñido a lo dispuesto en la clasificación de este, quedando prohibida la divulgación y/o reproducción total o parcial del contenido de éste sin la debida autorización por parte de la Jefatura TI. Su uso y distribución solo está autorizado al interior de ACHS y por parte del personal debidamente habilitado.

En este procedimiento se utilizará la opción "**escanear código QR**".




Tras capturar el código y procesarlo correctamente, la aplicación solicitará permiso para enviar notificaciones. Pulse en **Permitir** para poder recibir los avisos de la misma.

Posteriormente de forma predeterminada quedará registrada en la aplicación móvil la cuenta de usuario de la empresa **Asociación Chilena de Seguridad**.

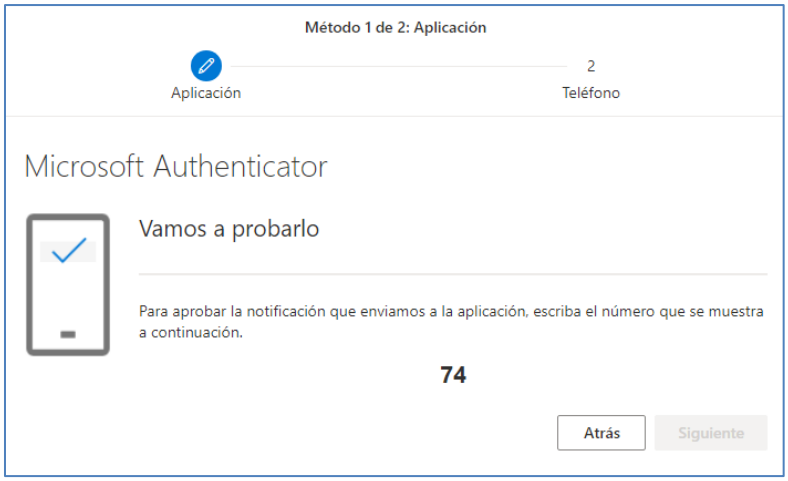



En el navegador aparecerá que se ha configurado la aplicación, seguidamente ir al icono **Siguiente**.


Este documento es de propiedad exclusiva de ACHS y su uso debe estar ceñido a lo dispuesto en la clasificación de este, quedando prohibida la divulgación y/o reproducción total o parcial del contenido de éste sin la debida autorización por parte de la Jefatura TI. Su uso y distribución solo está autorizado al interior de ACHS y por parte del personal debidamente habilitado.

### 3.4. Configuración para comprobación de seguridad

Luego está el proceso de comprobar la comunicación con la aplicación.




Para aprobar la autenticación, se enviará una notificación en el dispositivo móvil.

Escriba el **número** que se muestra en el paso anterior, para permitir la validación.

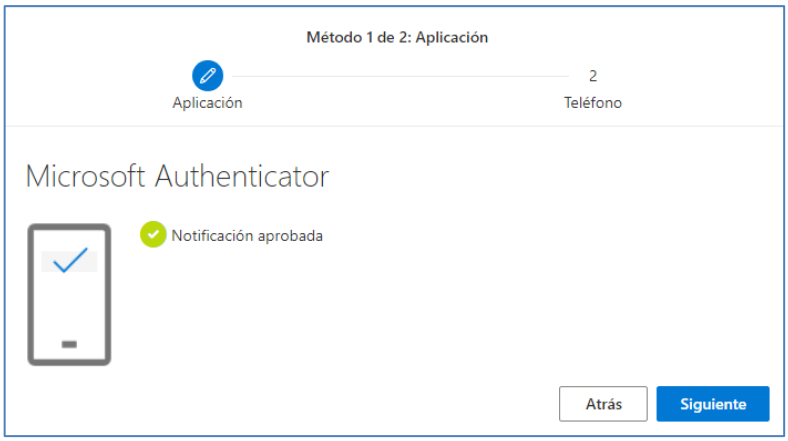
*En esta aplicación puede tener configuradas tantas cuentas como necesite, tanto a nivel personal como profesional.*




Este tipo de notificación aparecerá cada vez que se intente hacer un inicio de sesión con su cuenta. Ingrese el código sólo si se está seguro de que es Usted mismo el que está intentando iniciar sesión.


Este documento es de propiedad exclusiva de ACHS y su uso debe estar ceñido a lo dispuesto en la clasificación de este, quedando prohibida la divulgación y/o reproducción total o parcial del contenido de éste sin la debida autorización por parte de la Jefatura TI. Su uso y distribución solo está autorizado al interior de ACHS y por parte del personal debidamente habilitado.

En el navegador aparecerá que se ha configurado la aplicación, haga clic en el icono **Siguiente**.

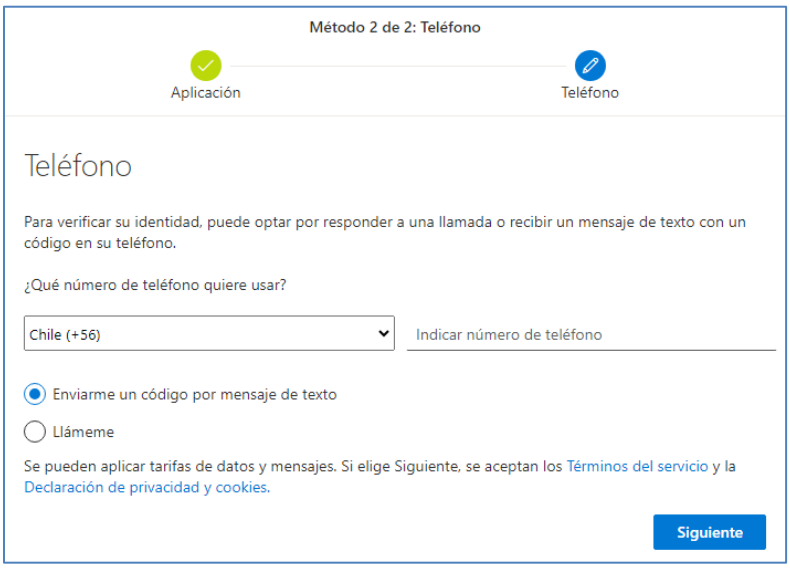



Como método de seguridad, debe ingresar el número de teléfono del dispositivo móvil donde añadió su cuenta. Para validar que Usted es quién está realizando la configuración.

Y seleccionar el tipo de notificación para responder.

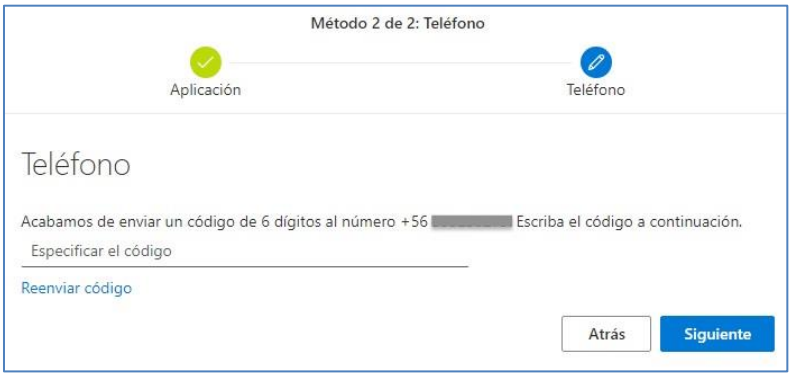
- Enviar mensaje de texto
- Llamada

Después, clic en **Siguiente**.




Luego debe ingresar el código que tuvo como notificación.

Para avanzar, haga clic en **Siguiente**.

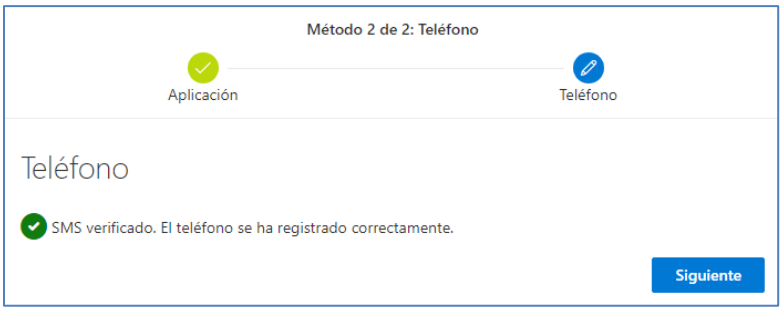




Este documento es de propiedad exclusiva de ACHS y su uso debe estar ceñido a lo dispuesto en la clasificación de este, quedando prohibida la divulgación y/o reproducción total o parcial del contenido de éste sin la debida autorización por parte de la Jefatura TI. Su uso y distribución solo está autorizado al interior de ACHS y por parte del personal debidamente habilitado.

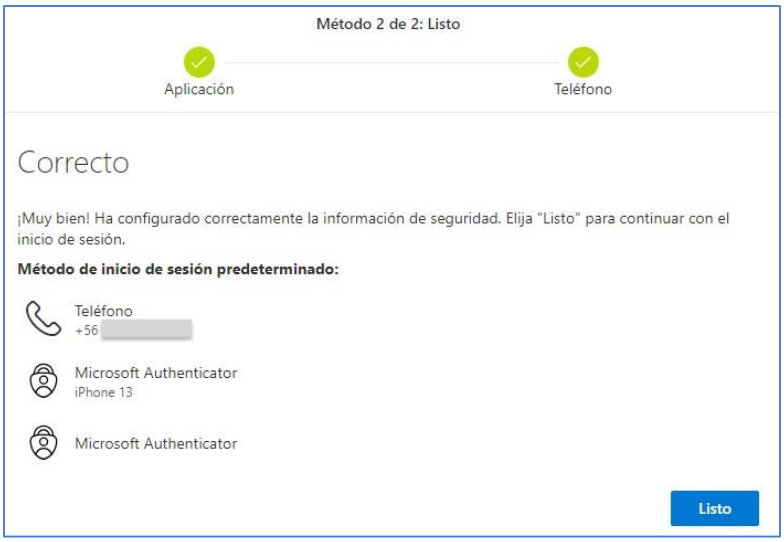
Si el código ingresado es el correcto, se indicará que se ha registrado de forma correcta el dispositivo móvil donde añadió su cuenta.

Después, clic en **Siguiente**.




Posteriormente, se mostrará que se ha configurado la aplicación y dispositivo móvil de forma correcta.

Para finalizar, haga clic en **Listo**.





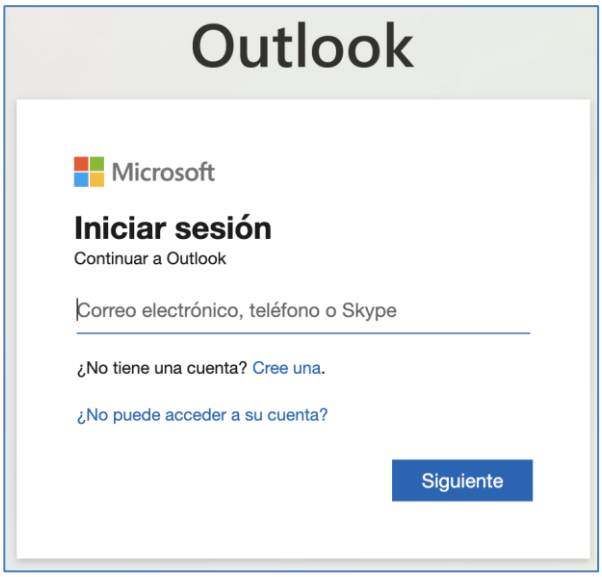
Este documento es de propiedad exclusiva de ACHS y su uso debe estar ceñido a lo dispuesto en la clasificación de este, quedando prohibida la divulgación y/o reproducción total o parcial del contenido de éste sin la debida autorización por parte de la Jefatura TI. Su uso y distribución solo está autorizado al interior de ACHS y por parte del personal debidamente habilitado.

## 4. Comprobar el funcionamiento de validación con 2FA

### 4.1. Ejemplo de conexión a Outlook 365 vía Web

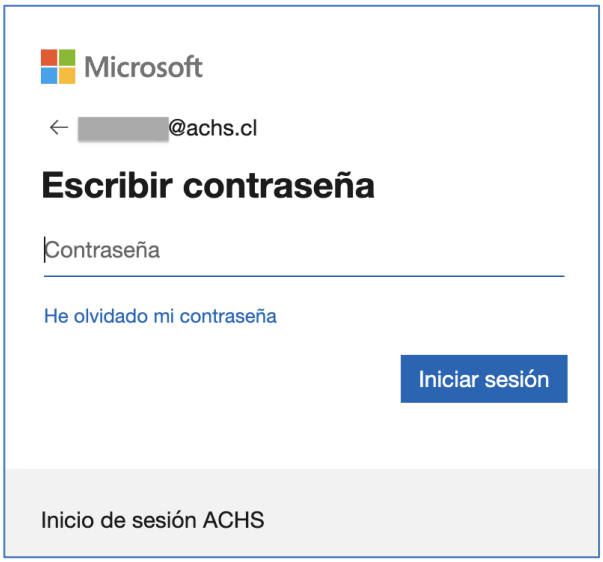
Para comprobar el correcto funcionamiento de la validación del segundo factor, acceda al **https://outlook.office.com/** en el computador entregado por la ACHS.

Después, clic en **Siguiente**.




Debe ingresar su cuenta de usuario ACHS y posteriormente la contraseña.

Después, clic en **Siguiente**.





Este documento es de propiedad exclusiva de ACHS y su uso debe estar ceñido a lo dispuesto en la clasificación de este, quedando prohibida la divulgación y/o reproducción total o parcial del contenido de éste sin la debida autorización por parte de la Jefatura TI. Su uso y distribución solo está autorizado al interior de ACHS y por parte del personal debidamente habilitado.

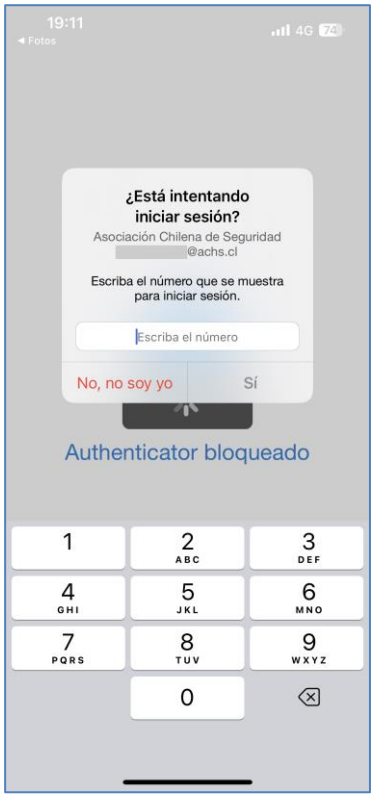
Luego de ingresar su usuario y contraseña, se mostrará la siguiente información a la espera de la **aprobación** desde el dispositivo móvil.




Llegado este momento, saltará una notificación en el dispositivo móvil que asoció a la cuenta, a la espera de ingresar el número que se muestra para iniciar sesión.

Proceder a ingresar el **número** y pulsar en la opción **Sí**.



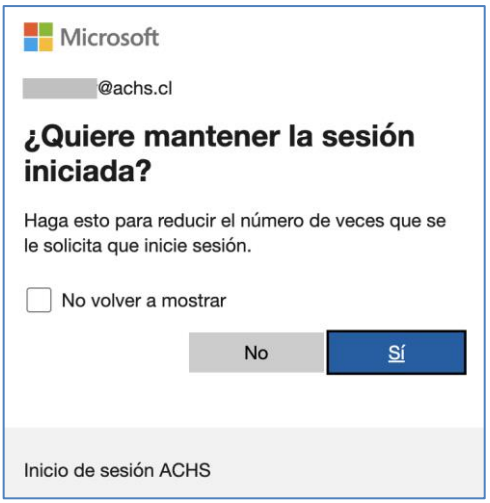





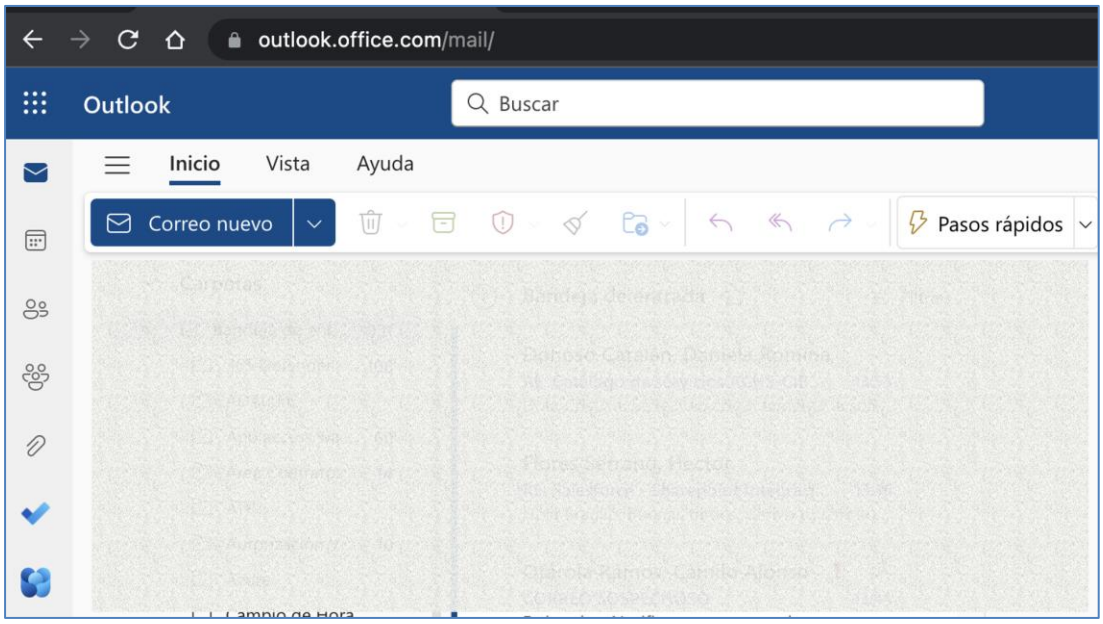
Este documento es de propiedad exclusiva de ACHS y su uso debe estar ceñido a lo dispuesto en la clasificación de este, quedando prohibida la divulgación y/o reproducción total o parcial del contenido de éste sin la debida autorización por parte de la Jefatura TI. Su uso y distribución solo está autorizado al interior de ACHS y por parte del personal debidamente habilitado.

Una vez ingresado el número en el dispositivo móvil, será aprobada la sesión.

En el navegador aparecerá el siguiente mensaje, pulse en **Sí** para concluir con el inicio de sesión.




Posteriormente se debe generar acceso Outlook 365 y visualizar los correos.





Este documento es de propiedad exclusiva de ACHS y su uso debe estar ceñido a lo dispuesto en la clasificación de este, quedando prohibida la divulgación y/o reproducción total o parcial del contenido de éste sin la debida autorización por parte de la Jefatura TI. Su uso y distribución solo está autorizado al interior de ACHS y por parte del personal debidamente habilitado.