

Doble Factor de Autenticación Office 365

El habilitar el doble factor de autenticación se realizará para obtener una segunda capa de seguridad en la información que el usuario tiene en el servicio de Office 365, con esta va a minimizar el riesgo de que otra persona pueda obtener su información.

¿Qué es el doble factor de autenticación?

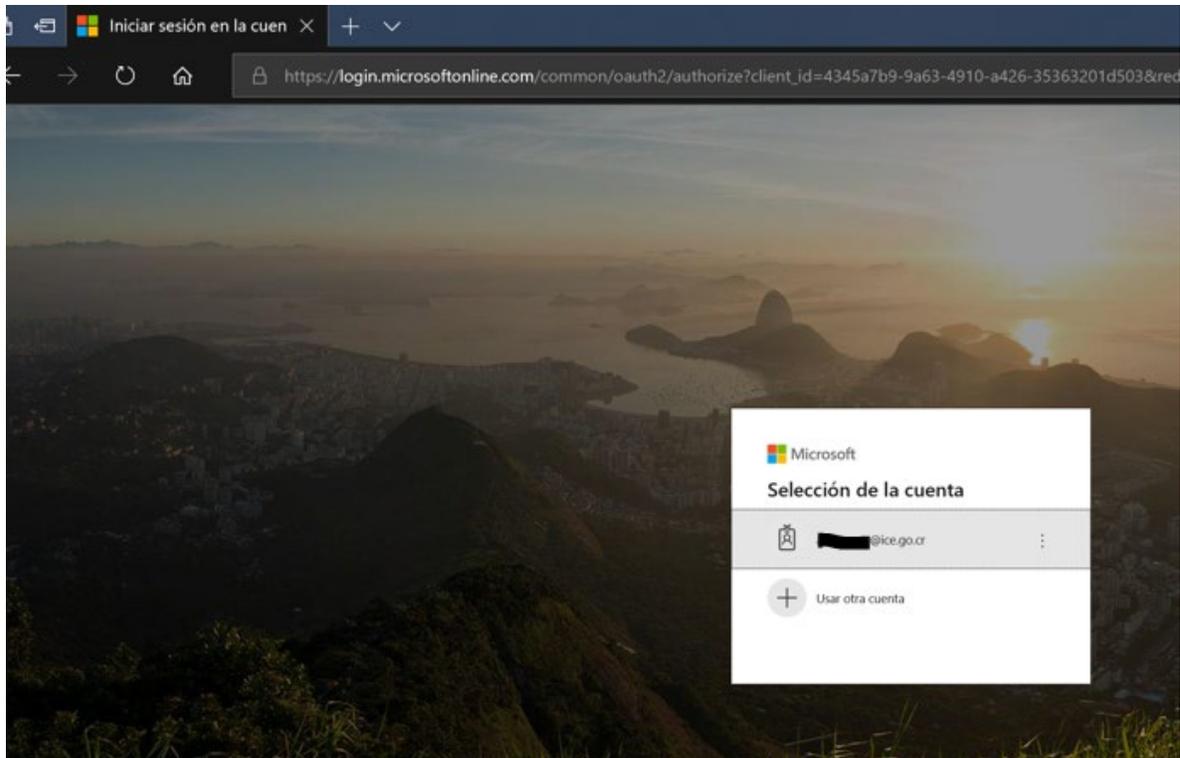
La autenticación por doble factor es un método de control de acceso informático en el que a un usuario se le concede el acceso solo después de que presente dos o más pruebas diferentes de autenticación verificando ser quien dice ser.

En el siguiente video podemos ver una descripción más clara del servicio.

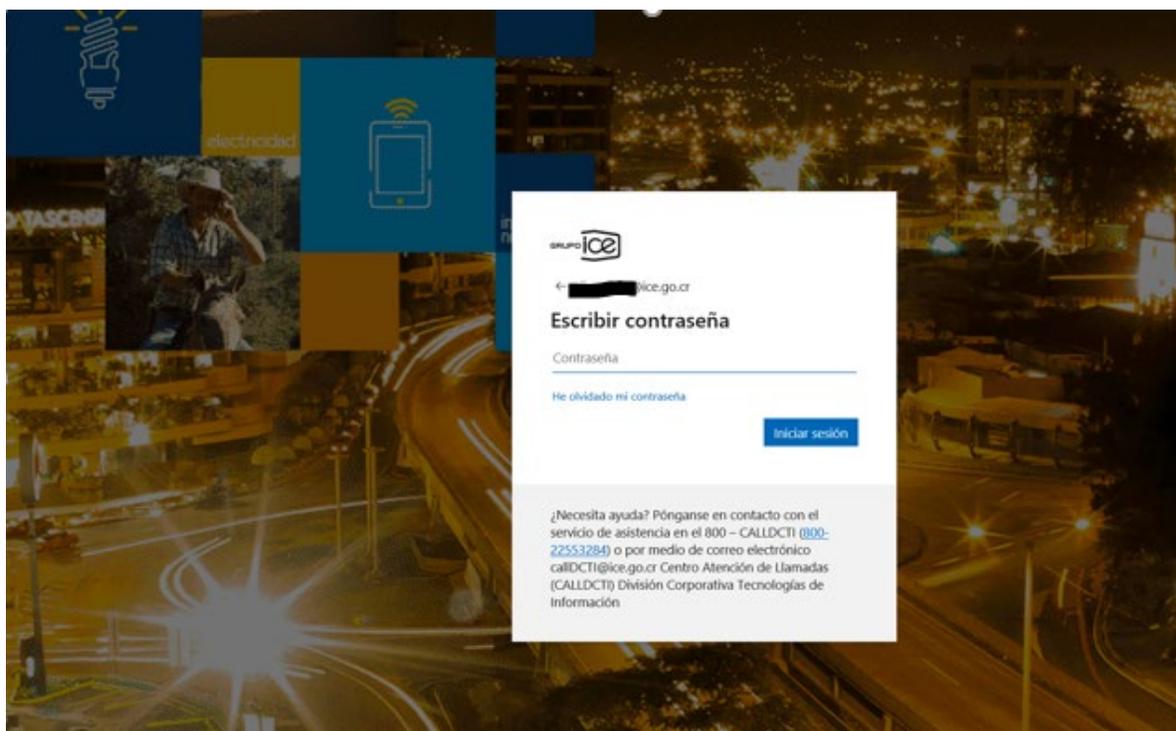
<https://www.youtube.com/watch?v=uWbkLu14g30>

Procedimiento para configurar el servicio de doble factor de autenticación.

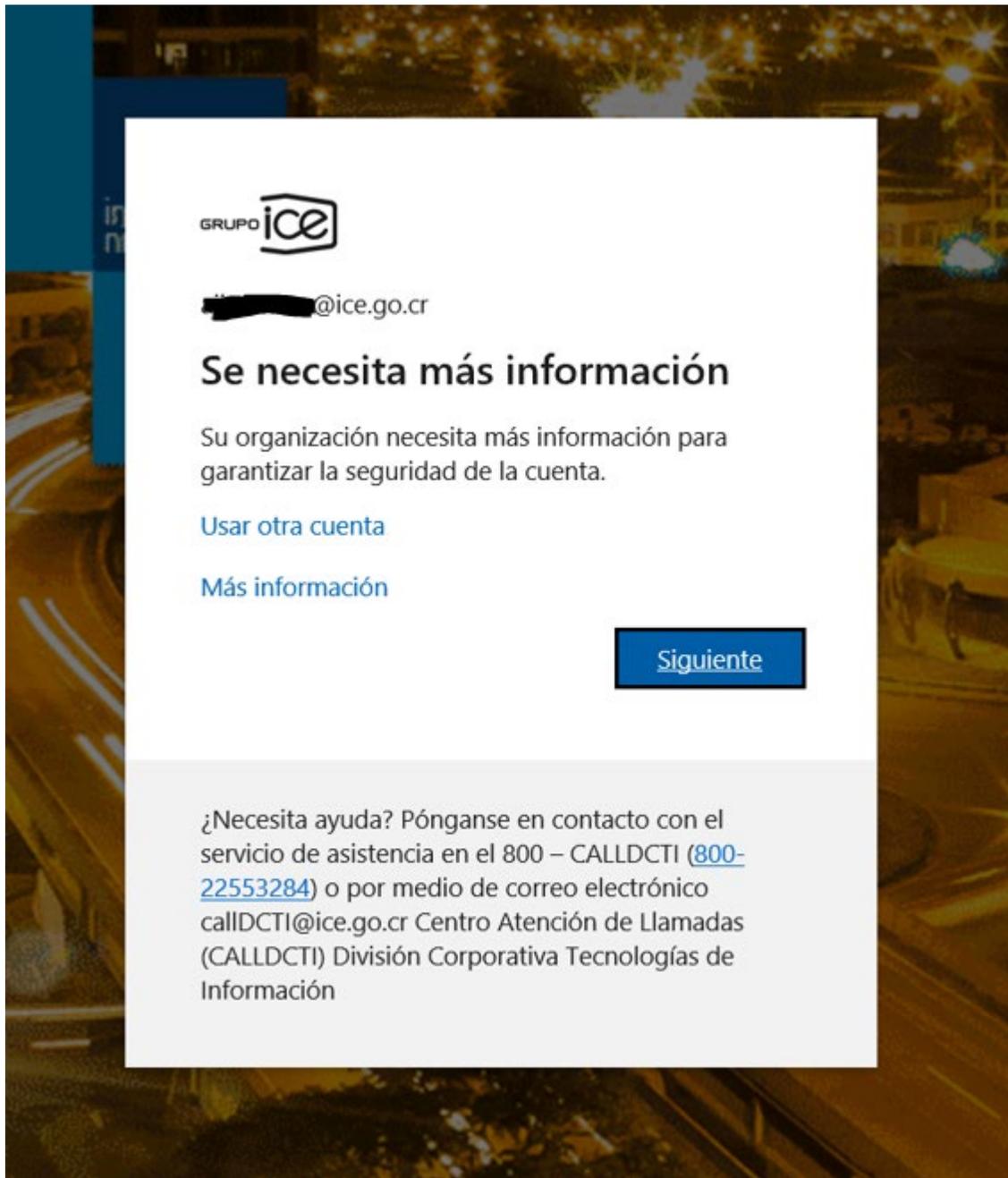
- Primeramente, se debe validar que el usuario cuente con una licencia de Office 365 activa, el equipo que utiliza tenga la última versión de Sistema Operativo y Office (en el caso que tenga instalada las aplicaciones), también que este al día con las actualizaciones de seguridad.
- Después de que se le informe que el servicio fue habilitado, debe cerrar correo (Outlook) o si está en el portal de Office 365 cerrarlo también.
- Ingresar al portal <https://portal.office365.com/> en el momento de ingresar le solicita autenticarse si nunca lo ha realizado, de lo contrario le va mostrar su dirección de correo para ingresar.



- Al seleccionar la dirección de correo le va solicitar que ingrese su contraseña de dominio, en este punto validar que sea su dirección de correo electrónico. Después de ingresar la contraseña le debe dar iniciar sesión.



Seguidamente le va mostrar una pantalla donde le indica "Su organización necesita más información para garantizar la seguridad de la cuenta", debe dar siguiente.

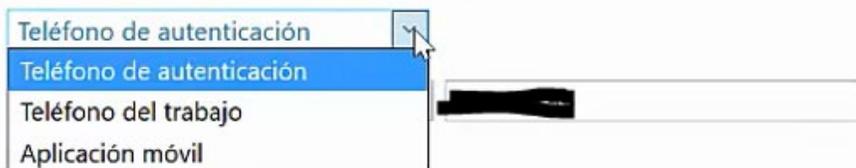


- En el siguiente paso es donde se va realizar el registro del segundo método de autenticación que queremos elegir. Aparecen tres opciones a elegir (Teléfono de autenticación, Teléfono del trabajo y Aplicación móvil)
 - Teléfono de autenticación: normalmente un teléfono celular, al cual se le enviar un mensaje de texto (SMS) cada vez que trate de iniciar sesión en cualquiera de las aplicaciones de Office 365 (dependiendo del plan que se tenga o el operador, esto puede generar un costo)
 - Teléfono del trabajo: normalmente un teléfono fijo al cual le realizaran una llamada con los pasos a seguir.
 - Aplicación móvil: se debe descargar la aplicación Microsoft Authenticator por la cual se va autorizar ingreso a las aplicaciones de Office 365, esta conlleva un proceso adicional en la cual debe enlazar la aplicación instalada en el teléfono móvil a su cuenta de Office 365. Puede descargar la aplicación para versiones de sistema operativo Android ([Google Play](#)) o sistemas operativos IOS ([App Store](#)). Esta es la opción que recomendamos seleccionar.

Comprobación de seguridad adicional

Proteja su cuenta agregando más comprobación de teléfono a su contraseña. [Ver vídeo](#)

Paso 1: ¿De qué manera deberíamos ponernos en contacto con usted?



Teléfono de autenticación
Teléfono de autenticación
Teléfono del trabajo
Aplicación móvil

Aplicación móvil:

Si decide optar por la opción de Aplicación móvil, que es la opción que recomendamos utilizar, se debe configurar de la siguiente manera:

Selecciona la opción de Aplicación móvil y seleccionar como quieres realizar el proceso si por medio de un código de verificación o recibir una notificación para aprobar el ingreso, luego de seleccionar el método deseado presiona el botón Configurar.

Recibir notificación para verificación: Debes ingresar a la app Authenticator donde te mostrara un mensaje para aprobar o denegar.

Usar código de verificación: Debes ingresar a la app Authenticator para ver el código que te genera.

Comprobación de seguridad adicional

Proteja su cuenta agregando más comprobación de teléfono a su contraseña. [Ver vídeo para saber cómo proteger su cuenta](#)

Paso 1: ¿De qué manera deberíamos ponernos en contacto con usted?

Aplicación móvil

¿Cómo quiere usar la aplicación móvil?

- Recibir notificaciones para verificación
- Usar código de verificación

Para usar estos métodos de comprobación, debe configurar la aplicación Microsoft Authenticator.

Configurar

La aplicación móvil se configuró.

Siguiente

Pero para configurar primero se tiene que tener descargado la app "Authenticator" en el dispositivo móvil y configurado.

Pasos para configurar primero la app Aplicación móvil en el dispositivo:

Cuando se ingresa a la app Microsoft Authenticator por primera vez muestra una serie de pasos que se debe omitir.

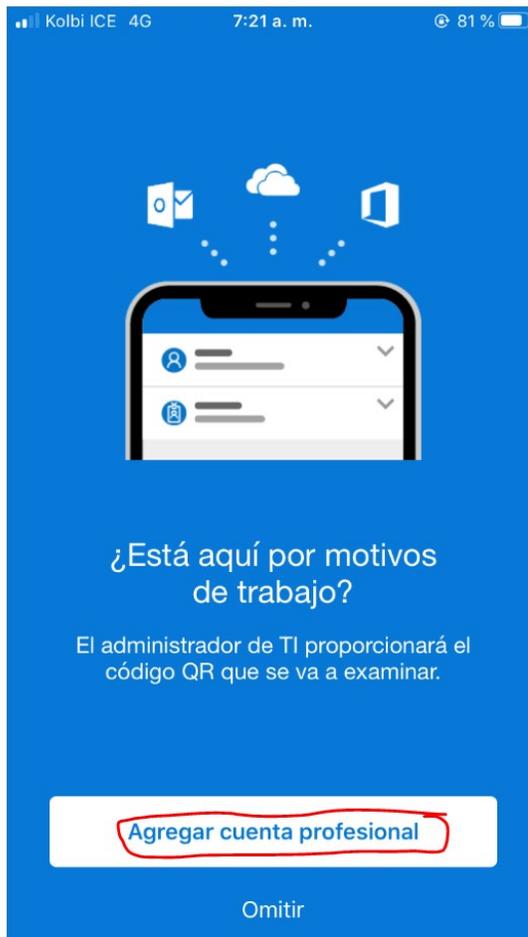
Seleccionar **“Omitir”** en esta primera.



Le vuelve a mostrar otra pantalla similar volver a seleccionar **“Omitir”**.



En la tercera opción seleccionar **“Agregar cuenta profesional”** en esta opción debes incluir su dirección de correo institucional.



Teniendo la app instalado en el dispositivo móvil volvemos a los pasos de configuración. Damos clic en el botón **“Configurar”**

Comprobación de seguridad adicional

Proteja su cuenta agregando más comprobación de teléfono a su contraseña. Ver video para saber cómo proteger su cuenta

Paso 1: ¿De qué manera deberíamos ponernos en contacto con usted?

Aplicación móvil

¿Cómo quiere usar la aplicación móvil?

- Recibir notificaciones para verificación
- Usar código de verificación

Para usar estos métodos de comprobación, debe configurar la aplicación Microsoft Authenticator.

Configurar

La aplicación móvil se configuró.

Siguiente

En ese momento nos va mostrar un código QR, con la app “Microsoft Authenticator” ya configurado en el dispositivo móvil lo vamos a escanear y una vez que muestra el mensaje de sincronizado damos siguiente.

The screenshot shows a web interface for configuring a mobile app. The main heading is "Comprobación de seguridad adicional" (Additional security check). Below it, there's a sub-heading "Paso 1: ¿De qué manera deberíamos ponernos en contacto con usted?" (Step 1: How should we contact you?). There are two radio button options: "Recibir notificaciones para verificación" (Receive verification notifications) and "Usar código de verificación" (Use verification code). The "Usar código de verificación" option is selected. A "Configurar" button is visible. A modal window titled "Configurar aplicación móvil" (Configure mobile app) is open, displaying a QR code. Below the QR code, there's a link "Configurar la aplicación sin notificaciones" (Configure app without notifications). At the bottom of the modal, there are instructions: "Si no puede examinar la imagen, especifique la información siguiente en la aplicación." (If you can't view the image, specify the following information in the app.) followed by "Código: 338 183 590" (Code: 338 183 590) and "Dirección URL: https://bn1napad01.na.phonefactor.net/pad/211215996" (URL: https://bn1napad01.na.phonefactor.net/pad/211215996). At the very bottom of the modal, it says "Si la aplicación muestra un código de seis dígitos, elija 'Siguiente'." (If the app shows a six-digit code, choose 'Next'). There are "Siguiente" and "cancelar" buttons at the bottom right of the modal.

Comprobación de seguridad adicional

Proteja su cuenta agregando más comprobación de teléfono a su contraseña. Ver video para saber cómo proteger su cuenta

Paso 1: ¿De qué manera deberíamos ponernos en contacto con usted?

¿Cómo quiere usar la aplicación móvil?

Recibir notificaciones para verificación

Usar código de verificación

Para usar estos métodos

Configurar

Configurar aplicación móvil

Complete los pasos siguientes para configurar su aplicación móvil.

1. Instale la aplicación Microsoft Authenticator para Windows Phone, Android o iOS.
2. En la aplicación, agregue una cuenta y seleccione "Cuenta profesional o educativa".
3. Examine la imagen siguiente.



[Configurar la aplicación sin notificaciones](#)

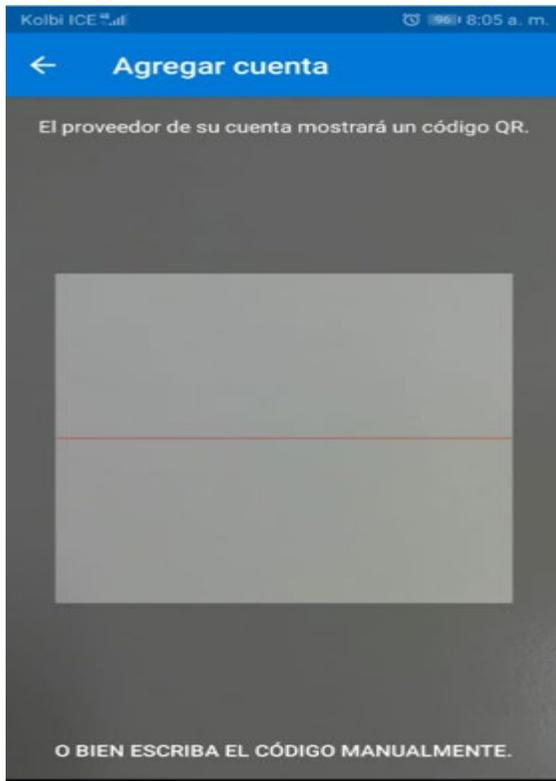
Si no puede examinar la imagen, especifique la información siguiente en la aplicación.

Código: [338 183 590](#)

Dirección URL: <https://bn1napad01.na.phonefactor.net/pad/211215996>

Si la aplicación muestra un código de seis dígitos, elija "Siguiente".

Siguiente cancelar



Seguidamente mostrara una pantalla de comprobación de seguridad adicional. Este punto es muy importante. Obtendrá una contraseña de aplicación que puede usar con Outlook, Apple Mail, Skype, etc. Elija el icono Copiar para copiar la contraseña y almacené esta clave, porque hay aplicaciones que no aceptan el doble factor de autenticación y va requerir esta clave para ingresar.



Comprobación de seguridad adicional

Proteja su cuenta agregando más comprobación de teléfono a su contraseña. [Ver video para saber cómo proteger su cuenta](#)

Paso 4: Siga usando las aplicaciones existentes

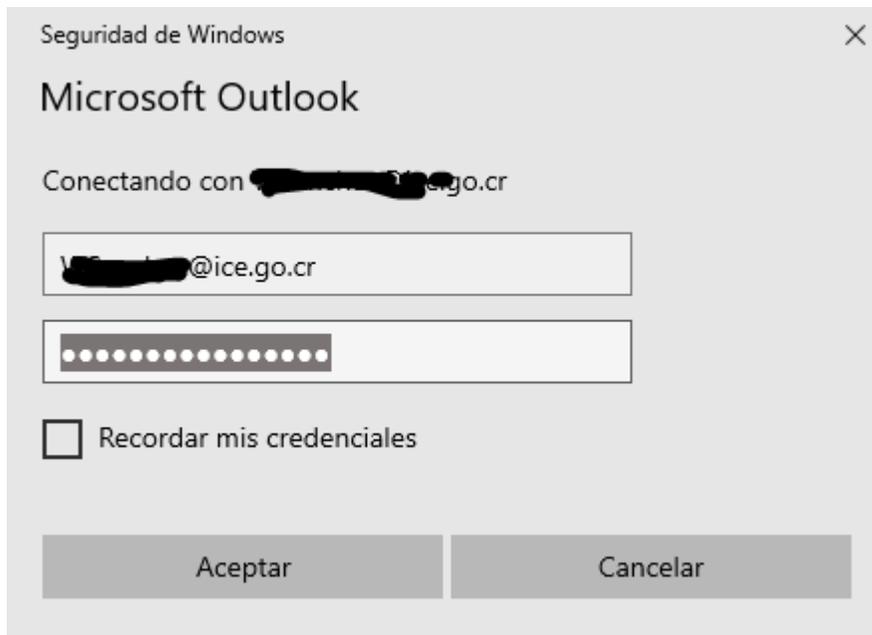
En algunas aplicaciones, como Outlook, Apple Mail y Microsoft Office, no puede usar un teléfono para proteger su cuenta. Para usar estas aplicaciones, tendrá que crear una nueva "contraseña de aplicación" para usarla en lugar de la contraseña de su cuenta profesional o educativa. [Más información](#)

Empiece con esta contraseña de la aplicación:



[Listo](#)

Si tienes configurado el Outlook que te pida contraseña al ingresar le muestra la ventana donde se ingresaba la contraseña de dominio, ahora debe ingresar contraseña que guardo en el paso anterior para poder ingresar al Outlook.



Seguridad de Windows

Microsoft Outlook

Conectando con [redacted]@ice.go.cr

[redacted]@ice.go.cr

[Redacted password field]

Recordar mis credenciales

Aceptar Cancelar

Recibir notificación para verificación: Debes ingresar a la app Authenticator donde te mostrara un mensaje para aprobar o rechazar.



GRUPO **ice**

[redacted]@ice.go.cr

Aprobar la solicitud de inicio de sesión

Hemos enviado una notificación a su dispositivo móvil. Abra la aplicación Microsoft Authenticator para responder.

¿Tiene problemas? [Inicie sesión de otra forma.](#)

[Más información](#)

¿Necesita ayuda? Pónganse en contacto con el servicio de asistencia en el 800 – CALLDCTI (800-22553284) o por medio de correo electrónico callDCTI@ice.go.cr Centro Atención de Llamadas (CALLDCTI) División Corporativa Tecnologías de Información



Cuentas



Instituto Costarricense de Elec...

██████████@ice.go.cr



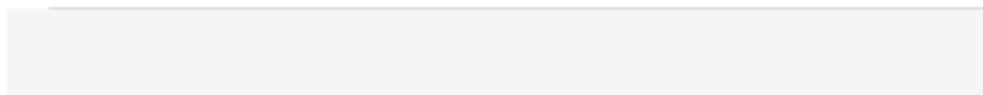
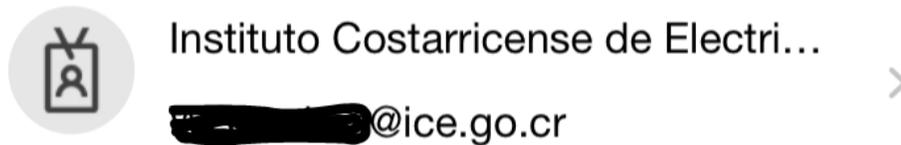
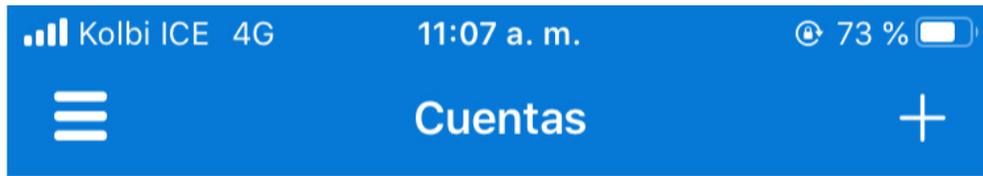
¿Quiere aprobar el inicio de sesión?

Instituto Costarricense de Electricidad
ajimenez@ice.go.cr

Denegar

Aprobar

Usar código de verificación: Debes ingresar a la app Authenticator para ver el código que te genera, ingresar a tu cuenta.



 **Notificaciones habilitadas**
Puede usar este dispositivo para aprobar notificaciones para verificar sus inicios de sesión.

 **Código de contraseña de un solo uso**
462 383

 **Habilitar inicio de sesión en el teléfono** >

 **Quitar cuenta**

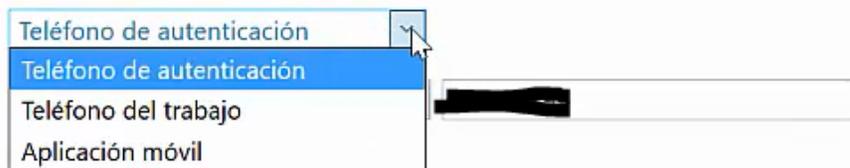
Teléfono de autenticación

La opción de “Teléfono de autenticación”, es similar a la anterior se utiliza el dispositivo móvil y cuando usted acceda a su cuenta de Office 365 le va solicitar el segundo factor de autenticación. Después de seleccionar la opción de “Teléfono de autenticación” tiene dos opciones para que lo contacten (Enviarme un código mediante mensaje de texto o Llamarme) la opción queda a su decisión.

Comprobación de seguridad adicional

Proteja su cuenta agregando más comprobación de teléfono a su contraseña. [Ver vídeo](#)

Paso 1: ¿De qué manera deberíamos ponernos en contacto con usted?

A screenshot of a web interface showing a dropdown menu. The menu is open, displaying four options: 'Teléfono de autenticación' (highlighted in blue), 'Teléfono de autenticación', 'Teléfono del trabajo', and 'Aplicación móvil'. A mouse cursor is pointing at the top right corner of the dropdown. To the right of the dropdown is a text input field containing a redacted phone number.

- Enviarme un código mediante mensaje de texto
- Llamarme

Al realizar el registro validar que sea Costa Rica (+506) y tener cuidado de digitar el número bien, el número que registra sea un número al cual se tiene acceso en todo momento porque a ese número que se registra es al que se le va contactar para validar el segundo factor de autenticación. Después de ingresar el número y seleccionar el método por el cual quiere que se le notifique, dar clic en siguiente.

Comprobación de seguridad adicional

Proteja su cuenta agregando más comprobación de teléfono a su contraseña. [Ver video para saber cómo proteger su cuenta](#)

Paso 1: ¿De qué manera deberíamos ponernos en contacto con usted?

Teléfono de autenticación

Costa Rica (+506)

Método

Enviarme un código mediante mensaje de texto

Llámame

Siguiente

Sus números de teléfono sólo se usarán para proteger su cuenta. Se aplicará la tarifa estándar de teléfono y SMS.

©2020 Microsoft Legal | Privacidad

Inmediatamente después se le estará notificando para validar el número que registro, debe ingresar el código de verificación y dar clic en comprobar.

GRUPO 

Comprobación de seguridad adicional

Proteja su cuenta agregando más comprobación de teléfono a su contraseña. [Ver video para saber cómo proteger su cuenta](#)

Paso 2: Hemos enviado un mensaje de texto a su teléfono +506 83 [redacted]

Escriba aquí el código de verificación cuando lo reciba

Cancelar Comprobar

©2020 Microsoft Legal | Privacidad

Seguidamente mostrara una pantalla de comprobación de seguridad adicional. Este punto es muy importante. Obtendrá una contraseña de aplicación que puede usar con Outlook, Apple Mail, Skype, etc. Elija el icono Copiar para copiar la contraseña y almacené esta clave, porque hay aplicaciones que no aceptan el doble factor de autenticación y va requerir esta clave para ingresar.



Comprobación de seguridad adicional

Proteja su cuenta agregando más comprobación de teléfono a su contraseña. [Ver video para saber cómo proteger su cuenta](#)

Paso 3: Siga usando sus aplicaciones existentes

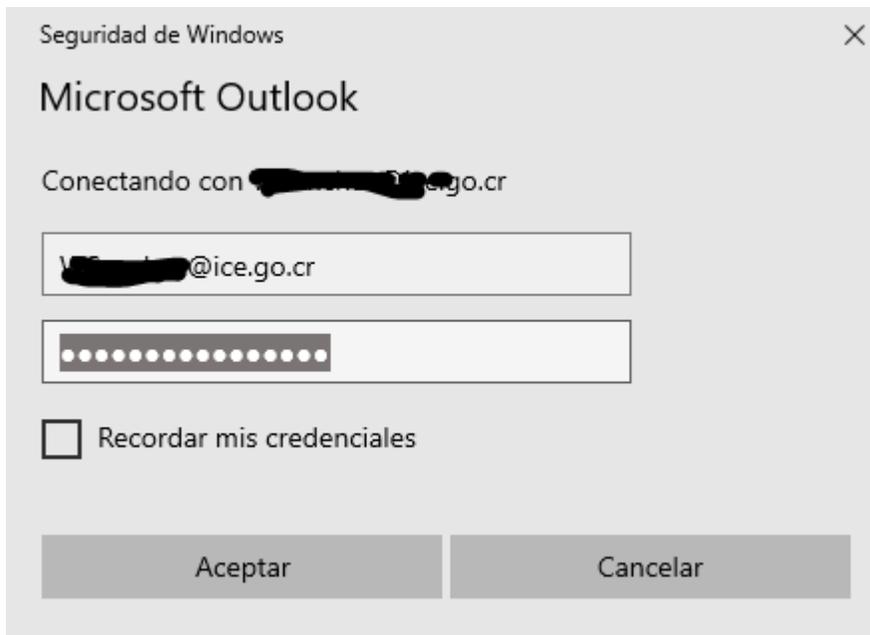
En algunas aplicaciones, como Outlook, Apple Mail y Microsoft Office, no puede usar un teléfono para proteger su cuenta. Para usar estas aplicaciones, tendrá que crear una nueva "contraseña de aplicación" para usarla en lugar de la contraseña de su cuenta profesional o educativa. [Más información](#)

Empiece con esta contraseña de la aplicación:

ctqvqgzrwsxwrxdp 

Listo

Si tienes configurado el Outlook que te pida contraseña al ingresar le muestra la ventana donde se ingresaba la contraseña de dominio, ahora debe ingresar contraseña que guardo en el paso anterior para poder ingresar al Outlook.



Una vez que seleccionaste el método que deseaste y terminaste con el proceso de registro quedó habilitado el doble factor de autenticación. La próxima vez que inicies sesión en Office 365, se te pedirá que introduzcas el código si seleccionaste un código ó aprobar si lo que hiciste es seleccionar la opción de “recibir notificaciones para verificación”.



← [redacted]@ice.go.cr

Escribir contraseña

●●●●●●●●

[He olvidado mi contraseña](#)

Iniciar sesión



[redacted]@ice.go.cr

Especificar el código

Le hemos enviado un mensaje de texto al teléfono +XXX XXXXXX65. Escriba el código para iniciar sesión.

Código

[¿Tiene problemas? Inicie sesión de otra forma.](#)

[Más información](#)

Comprobar

¿Necesita ayuda? Pónganse en contacto con el servicio de asistencia en el 800 – CALLDCTI ([800-22553284](tel:800-22553284)) o por medio de correo electrónico callDCTI@ice.go.cr Centro Atención de Llamadas (CALLDCTI) División Corporativa Tecnologías de Información

¿Necesita ayuda? Pónganse en contacto con el servicio de asistencia en el 800 – CALLDCTI ([800-22553284](tel:800-22553284)) o por medio de correo electrónico callDCTI@ice.go.cr Centro Atención de Llamadas (CALLDCTI) División Corporativa Tecnologías de Información



[redacted]@ice.go.cr

Aprobar la solicitud de inicio de sesión

Hemos enviado una notificación a su dispositivo móvil. Abra la aplicación Microsoft Authenticator para responder.

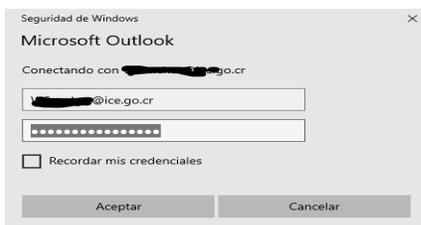
[¿Tiene problemas? Inicie sesión de otra forma.](#)

[Más información](#)

¿Necesita ayuda? Pónganse en contacto con el servicio de asistencia en el 800 – CALLDCTI ([800-22553284](tel:800-22553284)) o por medio de correo electrónico callDCTI@ice.go.cr Centro Atención de Llamadas (CALLDCTI) División Corporativa Tecnologías de Información



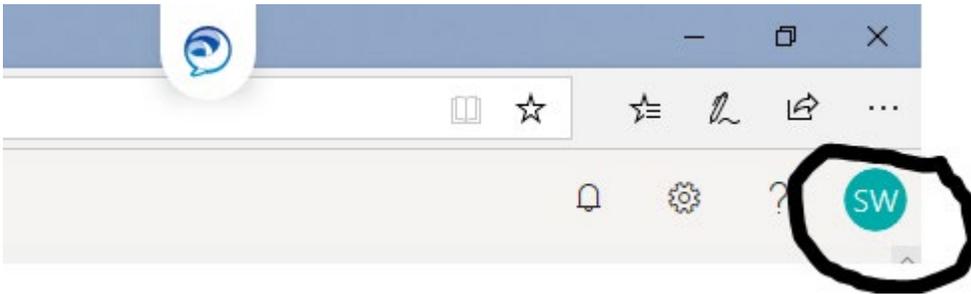
Como nota muy importante en cualquiera de los métodos que seleccione en el último paso “Comprobación de seguridad adicional” este código debe guardarlo bien y tener acceso porque si en el cliente de Outlook lo tienes configurado que te pida contraseña cuando ingresar, en lugar de digitar su contraseña de dominio debes ingresar este código.



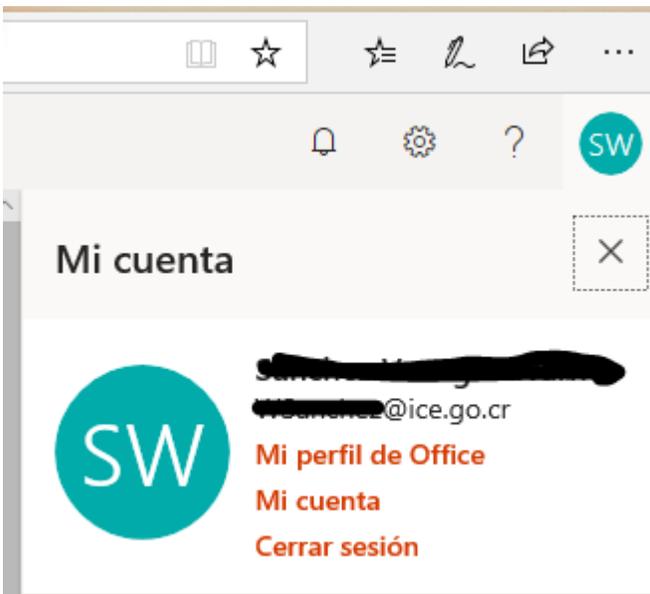
Información extra:

Si días después que se habilito el servicio se olvida la contraseña de “Comprobación de Seguridad adicional” o volver a “Configurar aplicación autenticadora”, los pasos para volver a realizarlo.

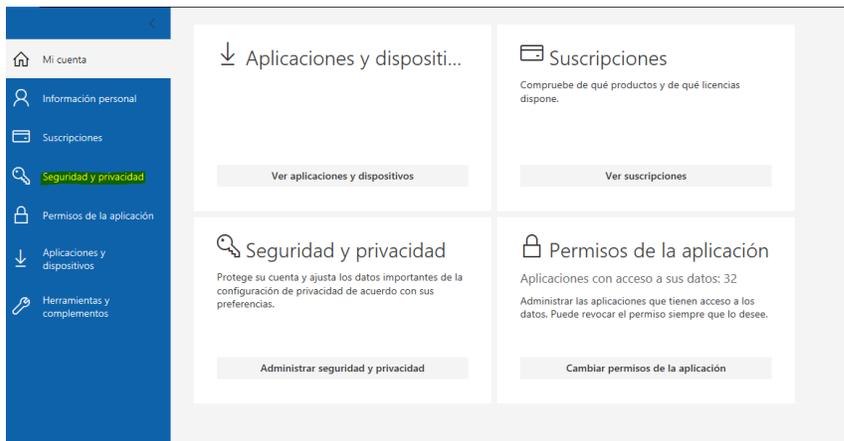
Se debe ingresar en <https://portal.office365.com/> vamos en la pantalla en la parte superior derecha donde las iniciales.



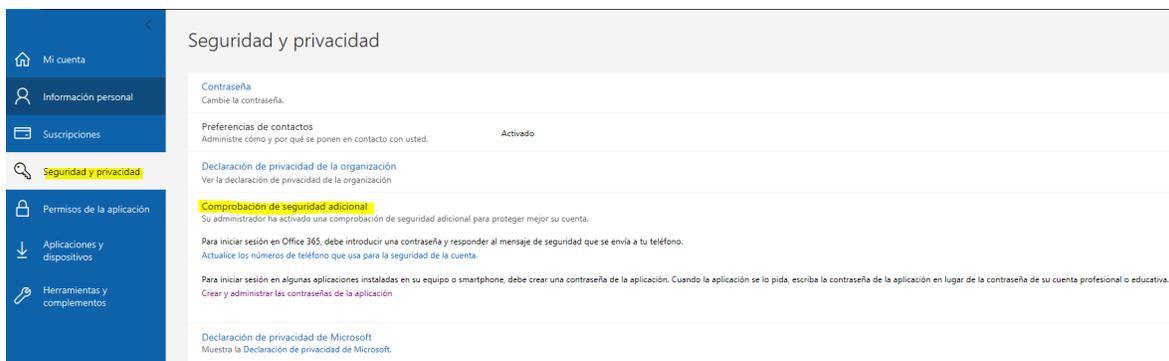
Damos clic sobre ellas y vamos a la opción a dar clic sobre “Mi cuenta”



Nos muestra la siguiente ventana y damos clic sobre “Seguridad y privacidad”



Al ingresar en seguridad damos clic sobre “Comprobación de seguridad adicional” ahí se va desplegar y nos va aparecer las dos opciones “Crear y administrar las contraseñas de la aplicación” y “Actualice los números de teléfono que usa para la seguridad de la cuenta”



Si damos clic sobre “Crear y administrar las contraseñas de la aplicación” nos va mostrar la que habíamos creado, se puede eliminar y crear una nueva.

comprobación de seguridad adicional contraseñas de aplicación

Para iniciar sesión en Outlook, Lync u otras aplicaciones instaladas en el equipo o en el smartphone, necesitará crear una contraseña de aplicación. Cuando lo solicite la aplicación, escriba la contraseña de aplicación, en lugar de la contraseña de su cuenta profesional o educativa.

Puede usar la misma contraseña de aplicación en varias aplicaciones o crear una contraseña de aplicación nueva para cada aplicación. [¿Cómo consigo que mis aplicaciones funcionen con contraseñas de aplicación?](#)

Nota: si es el administrador de un servicio de Microsoft, le recomendamos no utilizar contraseñas de aplicación.

Marcar esta página

crear

NOMBRE	FECHA DE CREACIÓN	
Contraseña de aplicación inicial20200312124525	12/03/2020	Eliminar

Si damos clic para “Actualice los números de teléfono que usa para la seguridad de la cuenta” para volver a configurar aplicación autenticadora, vamos a dar clic en el botón “Configurar aplicación autenticadora” y volvemos a realizar el proceso de configuración.

Comprobación de seguridad adicional Contraseñas de aplicación

Al iniciar sesión con su contraseña, ahora también deberá responder desde un dispositivo registrado. De este modo, los hackers tendrán más dificultades para iniciar sesión solo con una contraseña robada. [Ver vídeo para saber cómo proteger su cuenta](#)

¿cuál es su opción preferida?

Se usará esta opción de configuración de forma predeterminada.

Use el código de verificación de s

¿cómo desea responder?

Seleccione y configure una o más de estas opciones. [Más información](#)

<input checked="" type="checkbox"/> Teléfono de autenticación	<input type="text" value="██████████"/>	<input type="text" value="██████████"/>
<input type="checkbox"/> Teléfono del trabajo	Seleccione su país o región	2000-8678
		Extensión
<input type="checkbox"/> Teléfono de autenticación alternativo	Seleccione su país o región	<input type="text"/>

Aplicación autenticadora o token **Configurar aplicación autenticadora**

Aplicación de autenticación - iPhoneWaSaVe **Eliminar**

Guardar cancelar

Sus números de teléfono sólo se usarán para proteger su cuenta. Se aplicará la tarifa estándar de teléfono y SMS.