

**Centro de Investigación Científica y de Educación Superior  
de Ensenada, Baja California**



## **DIRECCIÓN DE TELEMÁTICA**

Guía de configuración para habilitar doble  
factor de autenticación en el servicio de  
almacenamiento en la nube institucional

**Versión 1.0**

21 de agosto de 2026

## Guía de configuración para habilitar doble factor de autenticación en el servicio de almacenamiento en la nube institucional.

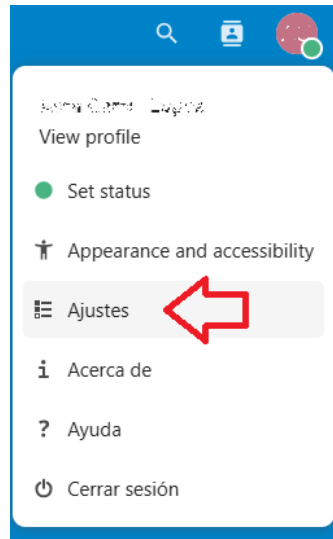
El doble factor de autenticación (2FA) es un método de seguridad que exige dos comprobaciones distintas para asegurar que quien intenta acceder a un sistema o servicio sea realmente quien dice ser.

En el presente documento se explicarán los pasos a seguir para habilitar el doble factor de autenticación en el servicio de almacenamiento en la nube institucional CIRRUS.

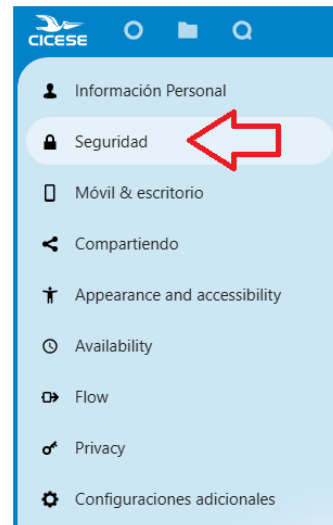
1.- Debe acceder al enlace del servicio de almacenamiento desde la interfaz web <https://cirrus.cicese.mx> con sus datos de acceso usuario y la contraseña correspondiente a su cuenta de la Red Cicese.



2. En la parte superior derecha debe hacer clic donde aparece un círculo con algunas de sus iniciales. Enseguida debe hacer clic en el botón “Ajustes”



3.- En el menú que se despliega en la parte izquierda dar clic en la opción “Seguridad”



4.- En la siguiente pantalla, ubique la sección “Two-Factor Authentication” (Autenticación de dos factores) y haga clic en el botón “Enable Two-Factor Authentication via Email”.



## Two-Factor Authentication ⓘ

Use a second factor besides your password to increase security for your account.

If you use third party applications to connect to Nextcloud, please make sure to create and configure an app password for each before enabling second factor authentication.

Email

Enable Two-Factor Authentication via Email



5.- Inmediatamente se indicará que un código fue enviado a su correo electrónico. En el buzón de correo debió llegar el código de 6 dígitos:



Your two-factor authentication code is: 123456

If you tried to login, please enter that code on CLOUD | CICESE. If you did not, somebody else did and knows your email address or username – and your password!

6. Para terminar la configuración, introduzca el código y de clic en el botón “Verify code”

## Two-Factor Authentication ⓘ

Use a second factor besides your password to increase security for your account.

If you use third party applications to connect to Nextcloud, please make sure to create and configure an app password for each before enabling second factor authentication.

Email

A code has been sent to [info@icecse.mx](mailto:info@icecse.mx)

123456

Verify code

Cancel activation

## 7.- Códigos de respaldo

Los códigos de respaldo sirven en caso de perder el segundo factor, siempre deberías generar códigos de respaldo para la autenticación de dos factores (2FA). Si no puedes tener acceso a tu correo electrónico para el segundo factor, podrás utilizar uno de estos códigos para desbloquear tu cuenta. En la práctica, funcionan como un segundo factor de respaldo. Para obtener los códigos de respaldo, da clic en Generar los códigos de respaldo.

 Código de respaldo

Generar los códigos de respaldo



A continuación, se le mostrará una lista de códigos de respaldo de un solo uso:

 Código de respaldo

Estos son tus códigos de respaldo. Por favor resguárdalos y/o imprímelos ya que no podrás leerlos otra vez después.

eTHyS48iciS9eEyD  
Y8Tkc3nYYQpABY9j  
2sWYwAYNsTJdP9Xr  
rCZb47QYZqNXBYX5  
TkdK2c66sF3A9E9o  
fxLH9ERb7oZmwKSi  
XpAkiXscLLAdaf23  
Ys9PfMCDnLWoizfH  
3SL7eEp87psFmCo4  
8s9jayMqqiwMsgzL

Guardar códigos de respaldo

Imprimir códigos de respaldo

Regenerar códigos de respaldo

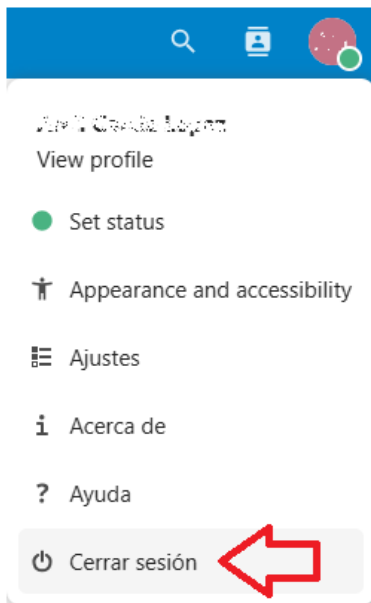
Si regeneras los códigos de respaldo, automáticamente invalidarás los anteriores.

Puedes:

- **Guardar códigos de respaldo:** genera un archivo de texto con los códigos.
- **Imprimir códigos de respaldo:** envía a impresión.
- **Regenerar códigos de respaldo:** genera nuevos códigos de respaldo invalidando los anteriores.

**Es MUY IMPORTANTE guardar estos códigos en un lugar seguro.**

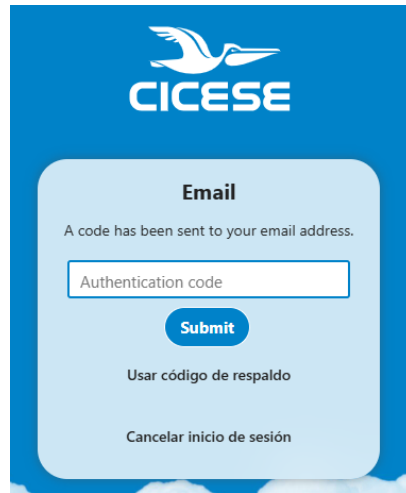
8.- Cerrar la sesión, en la parte superior derecha debe hacer clic donde aparece un círculo con algunas de sus iniciales. Enseguida debe hacer clic en el botón “Cerrar sesión”



9.- Volver a la página de inicio, proporcionar usuario y la contraseña correspondiente a su cuenta de la Red Cicese:

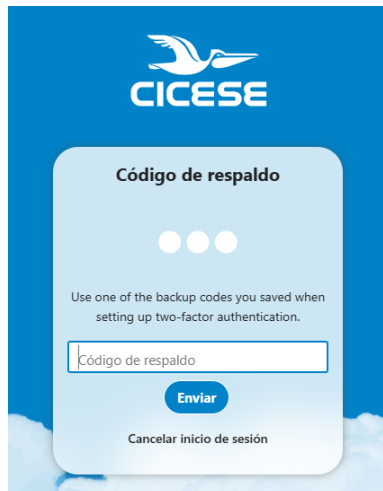


10. Aparecerá una segunda pantalla, donde se debe proporcionar el nuevo código enviado a su correo electrónico y dar clic en “Submit”



The image shows a blue-themed mobile application interface for CICESE. At the top is the CICESE logo. Below it, the screen is titled "Email". A message states: "A code has been sent to your email address." There is a text input field labeled "Authentication code". Below the field is a blue "Submit" button. At the bottom, there are two links: "Usar código de respaldo" and "Cancelar inicio de sesión".

11. En caso de requerir utilizar un código de respaldo, elegir la opción Usar código de respaldo:



The image shows a blue-themed mobile application interface for CICESE. At the top is the CICESE logo. Below it, the screen is titled "Código de respaldo". There are three white dots indicating a sequence. A message states: "Use one of the backup codes you saved when setting up two-factor authentication." There is a text input field labeled "Código de respaldo". Below the field is a blue "Enviar" button. At the bottom, there is a link: "Cancelar inicio de sesión".

12. Introducir uno de los códigos de un solo uso generados en el paso número 7 de esta guía y dar clic en "Enviar".