

PROCEDIMIENTO PARA GENERACIÓN DEL TOKEN PARA EL DOBLE FACTOR DE AUTENTICACIÓN EN SERVICIOS DEL CICESE



Departamento de Redes - Dirección de Telemática

INTRODUCCIÓN

Este documento ofrece una guía para realizar el registro y la configuración del segundo factor de autenticación (MFA) utilizando el portal institucional.

Requisito previo obligatorio:

Antes de comenzar, asegúrese de tener descargada y configurada en su dispositivo móvil una de las dos opciones de gestor de códigos MFA soportadas oficialmente por la Dirección de Telemática:

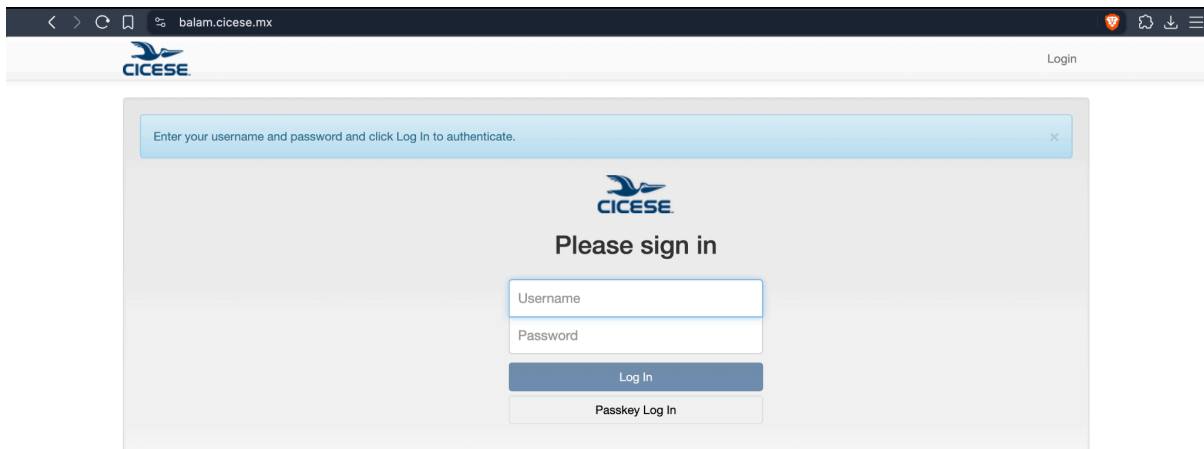
1. Google Authenticator
2. Proton Pass / Proton Authenticator

(Consulte los apartados o guías correspondientes para la descarga y preparación inicial de cualquiera de las dos aplicaciones en su dispositivo Android o iOS).

PROCEDIMIENTO

Para configurar y dar de alta su segundo factor de autenticación, siga los pasos detallados a continuación:

1. Abra su navegador web e ingrese a la siguiente dirección para acceder al portal de autenticación: <https://balam.cicese.mx/> e ingrese sus credenciales de acceso de la red CICESE.



The screenshot shows a web browser window with the address bar displaying 'balam.cicese.mx'. The page header features the CICESE logo on the left and a 'Login' link on the right. A blue notification bar at the top contains the text: 'Enter your username and password and click Log In to authenticate.' The main body of the page is titled 'Please sign in' and contains a login form with two input fields labeled 'Username' and 'Password', a blue 'Log In' button, and a grey 'Passkey Log In' button.

2. Una vez dentro del portal, localice y seleccione la opción correspondiente para iniciar el registro del token, haciendo clic en el botón de “Enroll Token” (ver figura).

The screenshot shows the 'Enroll a new token' page in the CICESE portal. The page has a header with the CICESE logo, a 'Tokens' tab, a 'Refresh' button, and a user profile 'jceja @todos (user)'. On the left, there is a sidebar with 'All Tokens' and 'Enroll Token' (selected). The main content area is titled 'Enroll a new token' and contains a dropdown menu set to 'TOTP: Time based One Time Passwords'. Below this, there is a paragraph explaining TOTP tokens. The 'Token data' section includes a checked checkbox for 'Generate OTP Key on the Server', a note about the server creating the OTP key and displaying a QR code, and three configuration fields: 'OTP length' (6), 'Timestep' (30 seconds), and 'Hash algorithm' (sha1). A blue 'Enroll Token' button is located at the bottom right of the form.

3. Al realizar el paso anterior, el sistema generará y mostrará en pantalla los datos del token (incluyendo el código QR). Haciendo uso de la aplicación de MFA de su preferencia de preferencia como Google Authenticator, proceda a escanear dicho código QR.

The screenshot shows the 'Enroll a new token' page after successful enrollment. The page header and sidebar are the same as in the previous screenshot. The main content area now displays a message: 'The token was successfully enrolled with serial number [redacted]'. Below this message is a large QR code. To the right of the QR code, there is a paragraph of text: 'Click [here](#) or scan the QR Code, if you want to add the Token to your smartphone authenticator app. The QR Code contains the secret key of your token. You need to protect it. If you are in doubt, that someone else saw it, please regenerate the QR Code, when no one else is watching.' Below this text is an orange 'Regenerate QR Code' button. At the bottom right of the main content area, there is a blue 'Enroll a new token' button.

4. Si la configuración se realiza correctamente, la aplicación de autenticación comenzará a generar códigos temporales de acceso que le permitirán validar sus próximas conexiones de forma segura.
5. Cuando ya haya finalizado el proceso de registro y verificación, cierre la ventana del navegador.