



Secretaría de Informática | Mayo de 2026

Manual de Uso



Microsoft Authenticator CCH-UNAM



Índice

Manual de uso – Microsoft Authenticator	3
Introducción.	3
Objetivo.....	3
Beneficios utilizar Microsoft Authenticator.....	3
Requisitos previos.	4
Procedimiento para la configuración	4
1. Desde la computadora, acceda al portal del correo institucional.....	4
2. Configurar la seguridad de la cuenta	5
3. Desde el celular, descargar Microsoft Authenticator	5
4. Configurar la privacidad de la aplicación	6
5. Agregar cuenta profesional o educativa.....	6
6. Escanear el código QR.....	7
7. Confirmar el número de verificación	8
8. Autenticarse en el celular.....	8
9. Finalizar configuración	9
10. Regresar al correo institucional.....	9
Uso cotidiano después de la configuración	10
Recomendaciones de seguridad	10
Problemas frecuentes y solución sugerida.....	11
Cambio o pérdida de celular	11
Soporte institucional	11
Control de versiones	12

Manual de uso – Microsoft Authenticator



Microsoft Authenticator CCH-UNAM

Sitio web: <https://www.microsoft.com/es-es/security/mobile-authenticator-app>

Introducción.

El correo institucional es una herramienta de comunicación académica y administrativa. Por ello, debe protegerse contra accesos no autorizados, robo de contraseñas, suplantación de identidad y correos fraudulentos.

Microsoft Authenticator es una aplicación móvil que ayuda a proteger el acceso al correo institucional; permite agregar una segunda verificación al inicio de sesión. Además de escribir la contraseña, la persona usuaria confirma desde su celular que realmente está intentando ingresar a su cuenta; evitando que alguien pueda entrar a la cuenta únicamente con la contraseña. Esta medida ayuda a proteger la información personal, académica y laboral asociada al correo institucional.

Objetivo.

Orientar a las personas usuarias del correo institucional del CCH en la configuración y uso de **Microsoft Authenticator** como **método de autenticación de doble factor** para acceder de forma segura al correo institucional vinculado con Microsoft 365.

Beneficios utilizar Microsoft Authenticator.

- ✓ Reduce el riesgo de acceso no autorizado aunque una contraseña haya sido comprometida.
- ✓ Permite confirmar el inicio de sesión desde el celular de la persona titular de la cuenta.
- ✓ Ayuda a proteger información personal, académica y profesional asociada al correo institucional.
- ✓ Facilita el acceso seguro a servicios vinculados con Microsoft 365, como Outlook, OneDrive y Teams, cuando estén habilitados para la cuenta.

Requisitos previos.

Requisito	Descripción	Observación
Cuenta institucional	Correo y contraseña vigentes.	Debe ser una cuenta @cch.unam.mx o @alumno.cch.unam.mx.
Celular	Dispositivo Android o iPhone.	Debe tener bloqueo de pantalla activo.
Aplicación	Microsoft Authenticator instalada.	Descargar desde Google Play o App Store.
Internet	Conexión en computadora y celular.	Evitar redes públicas si se maneja información sensible.
Navegador	Microsoft Edge, Chrome o Firefox actualizado.	Se recomienda no usar equipos compartidos para la configuración inicial.

Advertencia

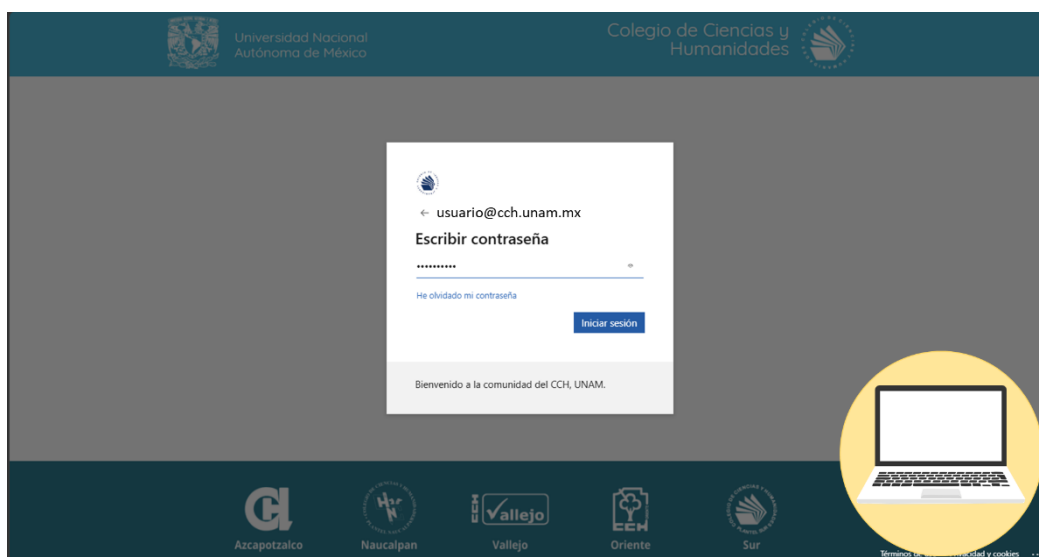
No se debe instalar una aplicación con nombre parecido. La aplicación correcta debe identificarse como **Microsoft Authenticator** y estar publicada por **Microsoft Corporation**.

Procedimiento para la configuración

Realice la configuración con la computadora y el celular al mismo tiempo. La computadora mostrará las pantallas del **correo institucional** y el celular servirá para instalar y activar **Microsoft Authenticator**.

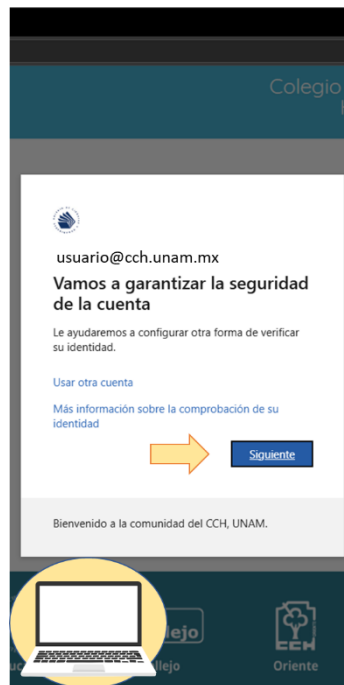
1. Desde la computadora, acceda al portal del correo institucional

- Abra el navegador e ingrese al portal del correo institucional.
<https://m365.cloud.microsoft/>
- Escriba la cuenta institucional completa y la contraseña vigente. Después, seleccione Iniciar sesión.



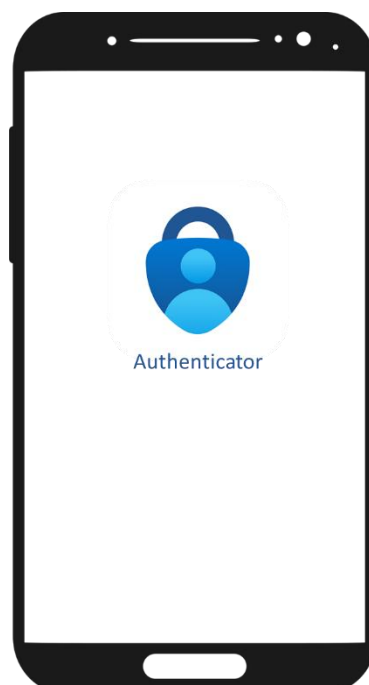
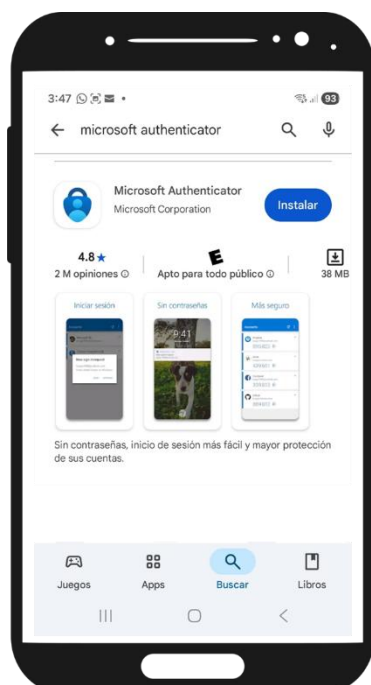
2. Configurar la seguridad de la cuenta

- Si aparece el mensaje para garantizar o actualizar la seguridad de la cuenta, seleccione **Siguiente**. El sistema abrirá el asistente de configuración de **Microsoft Authenticator**.



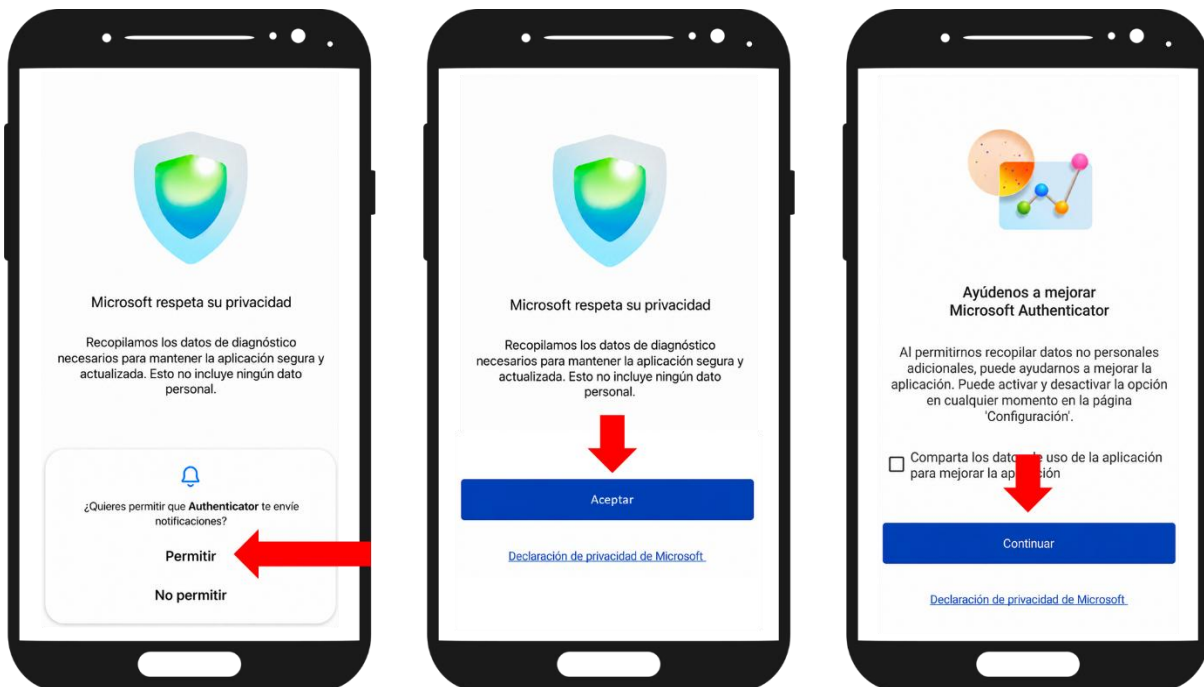
3. Desde el celular, descargar Microsoft Authenticator

- Abra **App Store** o **Google Play**, busque **Microsoft Authenticator** e instale la aplicación oficial. La aplicación quedará instalada en el celular y lista para agregar la cuenta institucional.



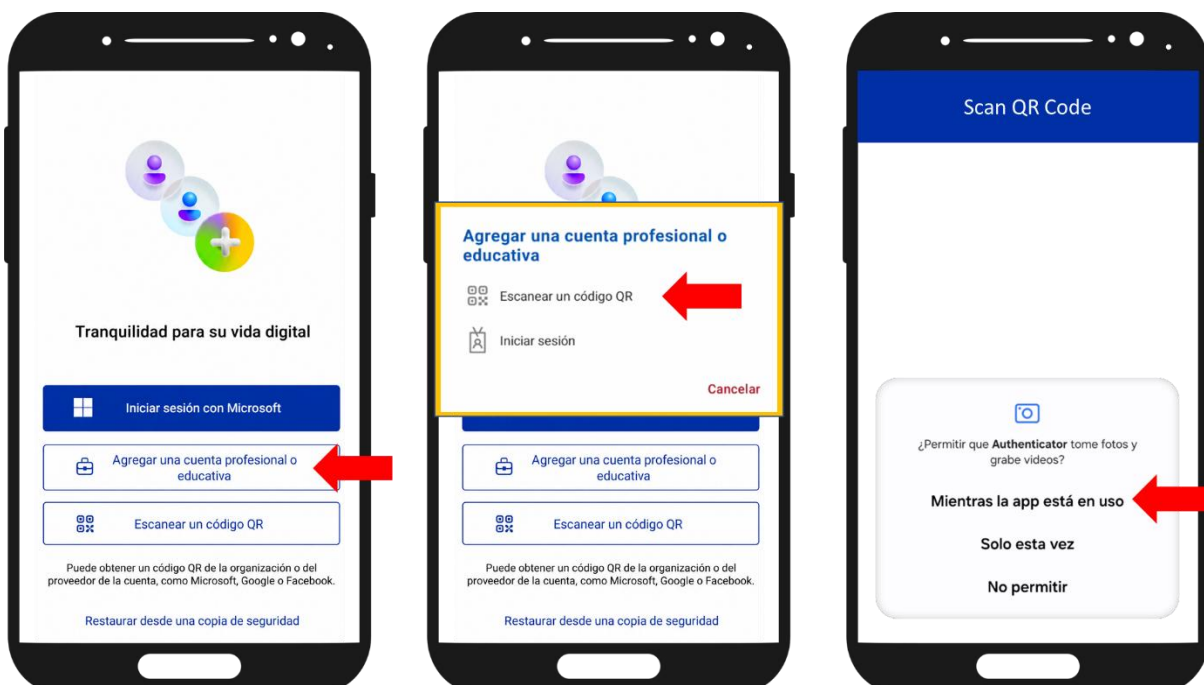
4. Configurar la privacidad de la aplicación

- Abra **Microsoft Authenticator** y permita las notificaciones. Acepte las condiciones de privacidad y haga clic en **continuar**.



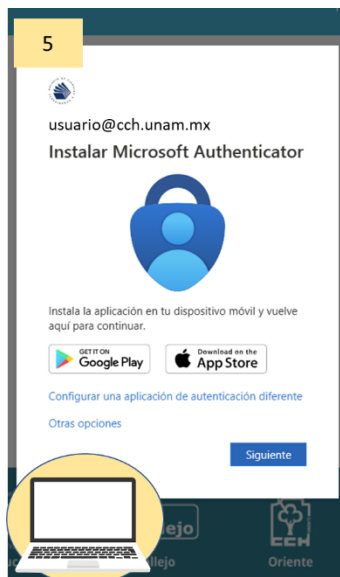
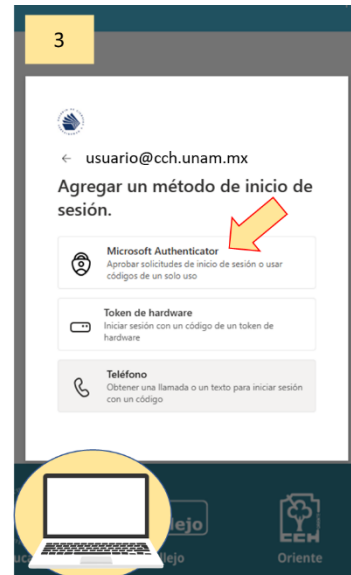
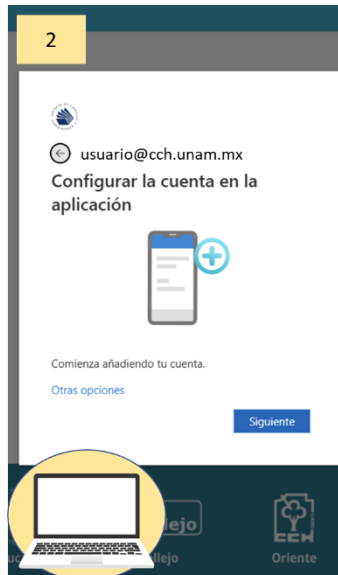
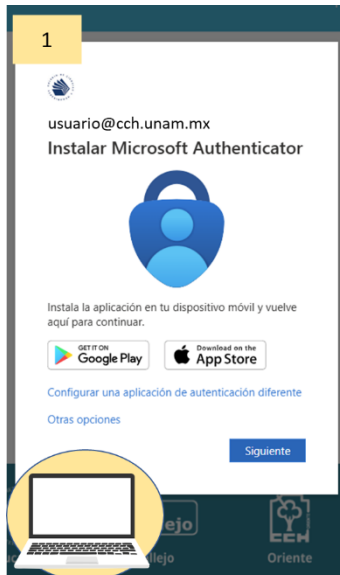
5. Agregar cuenta profesional o educativa

- Seleccione la opción «Agregar cuenta profesional o educativa».
- Elija la opción para «Escanear código QR».
- Permita que Authenticator tome fotos y grabe videos mientras la app está en uso



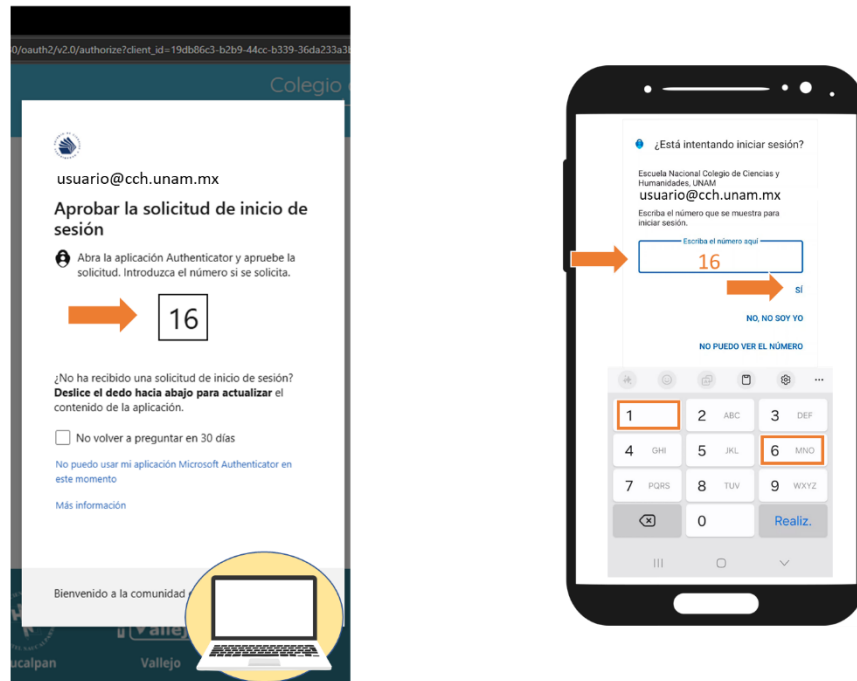
6. Escanear el código QR

- Regrese a la **computadora** y seleccione **Siguiente** hasta que se muestre el **código QR**.
- **Escanee** el código con la cámara de su teléfono celular desde **Microsoft Authenticator**.
- La cuenta institucional se agregará a la aplicación.



7. Confirmar el número de verificación

- Cuando aparezca un número en la **computadora**, escríbalo en **Microsoft Authenticator** y apruebe la solicitud.
- El sistema comprobará que el celular pertenece a la persona que está configurando la cuenta.



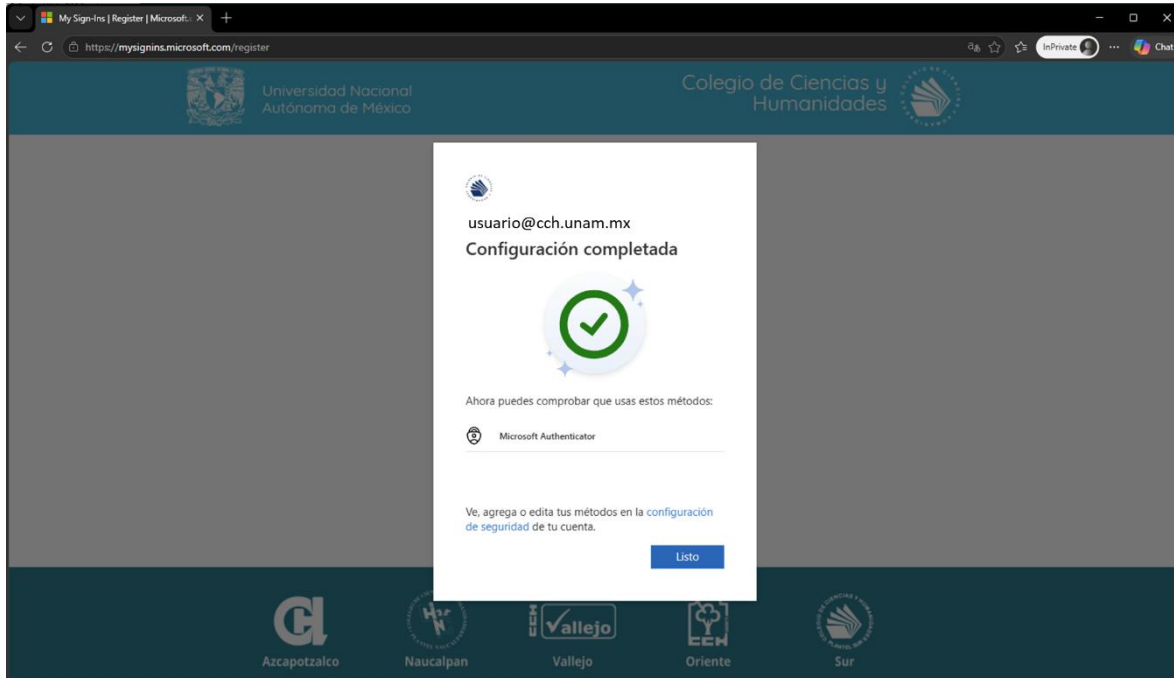
8. Autenticarse en el celular

- Confirme la identidad con el método de bloqueo del teléfono: PIN, contraseña, huella digital o reconocimiento facial.
- La aplicación completará la aprobación de la solicitud.



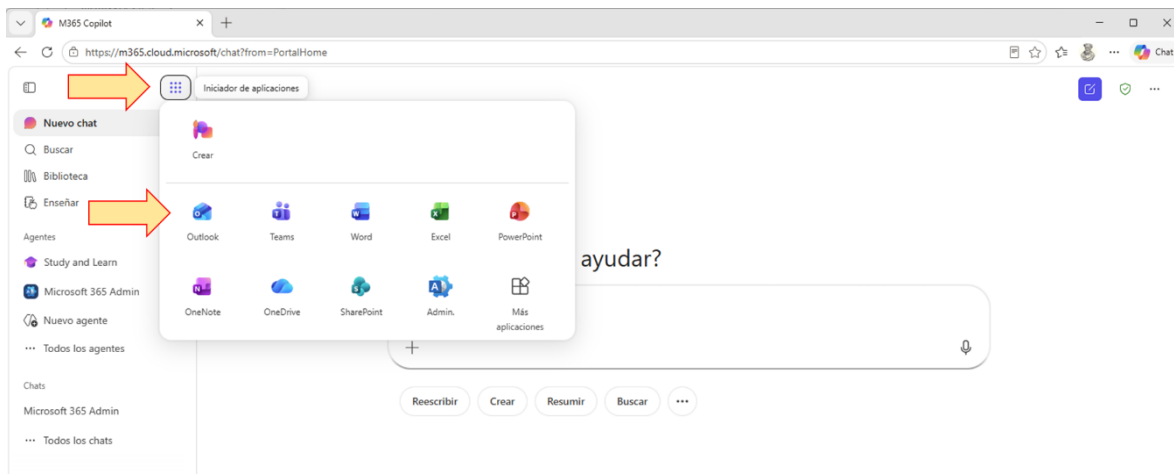
9. Finalizar configuración

- Cuando el navegador confirme que el emparejamiento fue exitoso, seleccione **Siguiente** y después **Listo**.
- **Microsoft Authenticator** quedará registrado como método de validación.



10. Regresar al correo institucional

- Vuelva al portal del correo institucional e inicie sesión nuevamente si el sistema lo solicita. Después abra **Outlook**. La cuenta quedará lista para utilizar el correo institucional de manera segura.



Uso cotidiano después de la configuración

Después de configurar **Microsoft Authenticator**, el inicio de sesión puede solicitar una confirmación adicional. El flujo normal será el siguiente:

- Entrar al correo institucional desde el portal correspondiente.
- Escribir correo y contraseña.
- Revisar el número que aparece en la pantalla de la computadora.
- Abrir **Microsoft Authenticator** en el celular.
- Escribir o confirmar el número mostrado.
- Aprobar el inicio de sesión únicamente si la solicitud fue iniciada por la propia persona usuaria.

Importante

Si llega una solicitud de **Microsoft Authenticator** sin que la persona usuaria esté intentando entrar a su correo, debe rechazarse. Después se recomienda cambiar la contraseña y reportar el incidente al área de soporte institucional.

Recomendaciones de seguridad

- No compartir la contraseña institucional con ninguna persona.
- No aprobar solicitudes de **Microsoft Authenticator** que no hayan sido iniciadas por la persona usuaria.
- Mantener el celular protegido con PIN, contraseña, huella digital o reconocimiento facial.
- Evitar configurar la cuenta institucional en celulares prestados o compartidos.
- No marcar la opción Mantener sesión iniciada en equipos públicos o compartidos.
- Actualizar el sistema operativo del celular y la aplicación **Microsoft Authenticator**.
- Reportar de inmediato cualquier intento de acceso sospechoso o correo fraudulento.
- Antes de cambiar de celular, conservar el dispositivo anterior hasta confirmar que el nuevo ya permite iniciar sesión.

Problemas frecuentes y solución sugerida

Situación	Acción sugerida
No llega la notificación al celular.	Revise la conexión a internet, permisos de notificación y que la aplicación esté actualizada. Abra manualmente Microsoft Authenticator y vuelva a intentar.
No puedo escanear el código QR.	Limpie la cámara, aumente el brillo de la pantalla o use la opción para escribir el código manualmente, si aparece disponible.
Cambié de celular y ya no puedo entrar.	Contacte al soporte institucional para restablecer el método de autenticación.
Me aparece un número, pero no sé dónde escribirlo.	Abra Microsoft Authenticator en el celular y escriba el número en la solicitud de aprobación activa.
Recibo solicitudes que no inicié.	Rechace la solicitud, cambie la contraseña y reporte el incidente.
La app muestra varias cuentas.	Verifique que está seleccionando la cuenta institucional correcta antes de aprobar el acceso.
No me pide Authenticator en cada inicio.	Puede depender de políticas de sesión o del estado del navegador. No necesariamente indica una falla.

Cambio o pérdida de celular

Si la persona usuaria cambia de celular, debe conservar el teléfono anterior hasta terminar la configuración en el nuevo dispositivo. No se recomienda borrar **Microsoft Authenticator** del dispositivo anterior antes de confirmar que el nuevo ya permite acceder al correo institucional.

En caso de robo, extravío o daño del celular, será necesario contactar al área de soporte institucional para que se restablezca el método de autenticación de la cuenta. Por seguridad, el restablecimiento debe realizarse mediante los canales institucionales definidos.

Soporte institucional

Para problemas de acceso a cuentas @cch.unam.mx o @alumno.cch.unam.mx, comuníquese a:

Atención a Usuarios	Secretaría de Informática
Correo	informatica@cch.unam.mx
Teléfono	55 5622 0021
Mesa de ayuda	Disponible en https://www.cch.unam.mx/aulas-virtuales

Control de versiones

Versión	Fecha	Área responsable	Descripción
1.0	27 de mayo de 2026	Secretaría de Informática	Primera versión del manual de uso de Microsoft Authenticator .



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Dr. Leonardo Lomelí Vanegas
Dra. Patricia Dolores Dávila Aranda
Mtro. Hugo Alejandro Concha Cantú
Mtro. Tomás Humberto Rubio Pérez
Dra. Diana Tamara Martínez Ruiz
Mtro. Fernando Macedo Chagolla
Dr. Manuel Palma Rangel
Lic. Mauricio López Velázquez

Rector
Secretaría General
Abogado General
Secretaría Administrativa
Secretaría de Desarrollo Institucional
Secretaría de Servicio y Atención a la Comunidad Universitaria
Secretaría de Prevención y Apoyo a la Movilidad y Seguridad Universitaria
Director General de Comunicación Social

ESCUELA NACIONAL COLEGIO DE CIENCIAS Y HUMANIDADES

Mtra. María Patricia García Pavón
Mtro. Keshava Rolando Quintanar Cano
Lic. Rocío Carrillo Camargo
Lic. María Elena Juárez Sánchez
QBP. Taurino Marroquín Cristóbal
Mtra. Dulce María Santillán Reyes
Mtro. José Alfredo Núñez Toledo
Mtra. Araceli Mejía Olguín
Mtro. Héctor Baca Espinoza
Ing. Armando Rodríguez Arguijo

Directora General
Secretaría General
Secretaría Administrativa
Secretaría Académica
Secretaría de Servicios de Apoyo al Aprendizaje
Secretaría de Planeación
Secretaría Estudiantil
Secretaría de Programas Institucionales
Secretaría de Comunicación Institucional
Secretaría de Informática

Mtra. Martha Patricia López Abundio
Lic. Antonio Nájera Flores
Mtro. Arturo Palacios Mejía
Lic. Óscar Iván Méndez Dávalos
Lic. Noemí Jiménez Martínez
Mtro. Raúl Espinosa Rojas
Lic. José Roberto Salinas Sánchez
Lic. Adriana Astrid Getsemaní Castillo Juárez
Mtra. Verónica Coria Olvera
Lic. Verónica Andrade Villa

Mtra. Verónica Berenice Ruiz Melgarejo
Ing. Damián Alberto Feltrín Rodríguez
Mtra. Teresa de Jesús Sánchez Serrano
Mtro. Jesús Medina Cabrera
Lic. Rogelio Aurelio Rojas Reyes
Ing. Blanca Elizabeth Cruz Estrada
Lic. Ana Laura Yáñez Piñón
Mtra. Ana Rocío Alvarado Torres
Mtro. Miguel Ángel Zamora Calderilla
LDG. Cristo Rey Policarpo Martínez

Lic. Maricela González Delgado
Mtro. Manuel Odilón Gómez Castillo
Lic. Diana Reyna Alatorre Hernández
Mtra. María Xóchitl Megchún Trejo
Lic. María del Rocío Sánchez Sánchez
Lic. Armando Segura Morales
Lic. Carlos Ortega Ambríz
IQ. Georgina Guadalupe Góngora Cruz

Q.F.B. Reyes Flores Hernández
Mtra. Belem Torres Romero
Mtra. Alejandra Barrios Rivera
Mtra. Laura Tayde Mejía Ramírez
Lic. Oscar López García
Dra. Elsa Rodríguez Saldaña
Mtra. Claudia Verónica Morales Montaño
Ing. Angélica Nohelia Guillén Méndez

Lic. Noé Israel Reyna Méndez
Mtro. Javier Millán Martínez
Lic. Emmanuel Roberto Orozco García
Mtra. Rosa Angélica Gómez Armas
Mtro. Armando Moncada Sánchez
Mtro. Aldo Estrada Quiroz
Mtro. Reynaldo Cruz Contreras
Mtra. Nohemí Claudia Saavedra Rojas
Mtra. Clara León Ríos

AZCAPOTZALCO

Directora
Secretario General
Secretaría Administrativa
Secretaría Académica
Secretaría Docente
Secretaría de Asuntos Estudiantiles
Secretaría de Servicios de Apoyo al Aprendizaje
Jefa de la Unidad de Planeación
Secretaría Técnica del SILADIN
Secretaría Particular y Coordinación de Gestión

NAUCALPAN

Directora
Secretario General
Secretaría Administrativa
Secretaría Académica
Secretaría Docente
Secretaría de Servicios Estudiantiles
Secretaría de Apoyo al Aprendizaje y Cómputo
Secretaría de Administración Escolar
Secretario Técnico del SILADIN
Coordinador de Gestión y Planeación

VALLEJO

Directora
Secretario General
Secretaría Administrativa
Secretaría Académica
Secretaría Docente
Secretaría de Asuntos Estudiantiles
Secretaría de Servicios de Apoyo al Aprendizaje
Secretaría Técnica del SILADIN

ORIENTE

Director
Secretario General
Secretaría Administrativa
Secretaría Académica
Secretaría Docente
Secretaría de Asuntos Estudiantiles
Secretaría de Administración Escolar
Secretaría Técnica Del SILADIN

SUR

Directora
Secretario General
Secretaría Administrativa
Secretaría Académica
Secretaría Docente
Secretaría de Asuntos Estudiantiles
Secretaría de Servicios de Apoyo al Aprendizaje
Secretaría Técnica del SILADIN
Jefa de la Unidad de Planeación



DIRECTORIO

Revisión

Ing. Armando Rodríguez Arguijo
Edición, redacción y diseño
M. en I. Víctor Hugo Leyva García

SECRETARÍA DE INFORMÁTICA