GUÍA COMPLETA DEL USO DEL SEGUNDO FACTOR DE AUTENTICACIÓN

EN TODAS TUS CUENTAS UCM

Cuenta Personal UCM

OBLIGATORIO A PARTIR DEL 15/04/2026

- Activación del Segundo Factor de Autenticación (2FA)
- Uso y Acceso a tu cuenta UCM
  - → Con el Segundo Factor de Autenticación
  - → Con Certificado Digital y Cl@ve
  - → Con DNI electrónico
- Recuperación del Segundo Factor de Autenticación (2FA)

Cuentas Institucionales o de Actividad UCM

- Activación del Segundo Factor de Autenticación (2FA)
- Cambio de titularidad de las cuentas institucionales o de actividad

Activación del Segundo Factor de Autenticación (2FA)

Protege tu cuenta de la Universidad Complutense de Madrid paso a paso.

CRÍTICO: Asegúrate de tener acceso a tu dispositivo móvil para completar la activación.

Una barrera infranqueable frente a los accesos no autorizados

El 2FA añade una verificación adicional. Aunque alguien robara tu contraseña, le resultaría imposible acceder a tu cuenta sin tu teléfono móvil.

Contraseña **Código Temporal** **Cuenta Segura**

Reglas de oro antes de empezar la instalación

MUY IMPORTANTE

Sincronización.
Comprueba que la fecha y la hora son exactamente iguales y correctas tanto en el ordenador como en tu teléfono móvil.

La Aplicación. Descarga la app Google Authenticator en tu teléfono móvil desde Google Play o AppStore.

Android
play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=es

iPhone
apps.apple.com/es/app/google-authenticator/id388497605

El paso previo fundamental: configura tu salvavidas digital

MUY IMPORTANTE
Antes de activar el 2FA, debes garantizas que podrás recuperar tu cuenta evitando desplazamientos en caso de olvido de clave, problemas con 2FA, pérdida o cambio de dispositivo.

1. Entra en tu ordenador a **www.ucm.es**, identifícate y accede a **Gestión de Identidad (IDM)** (idm.ucm.es).

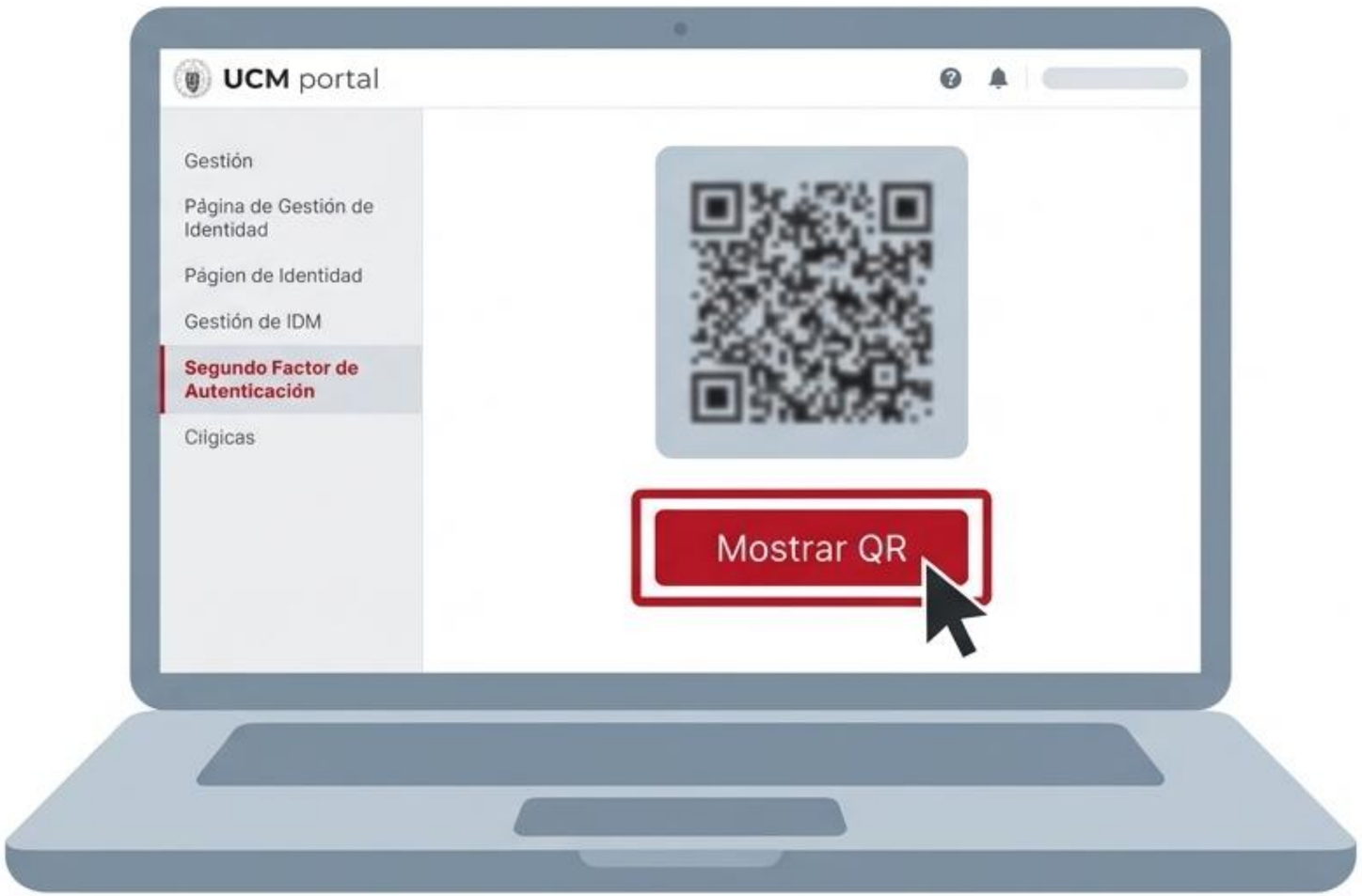
2. En la columna izquierda, ve a **Datos de Usuario**.

3. Asegúrate de tener registrado un **email alternativo**. Si no lo tienes, inclúyelo y guarda los cambios. El email alternativo debe ser cuenta **NO UCM**

Vol ver al inicio

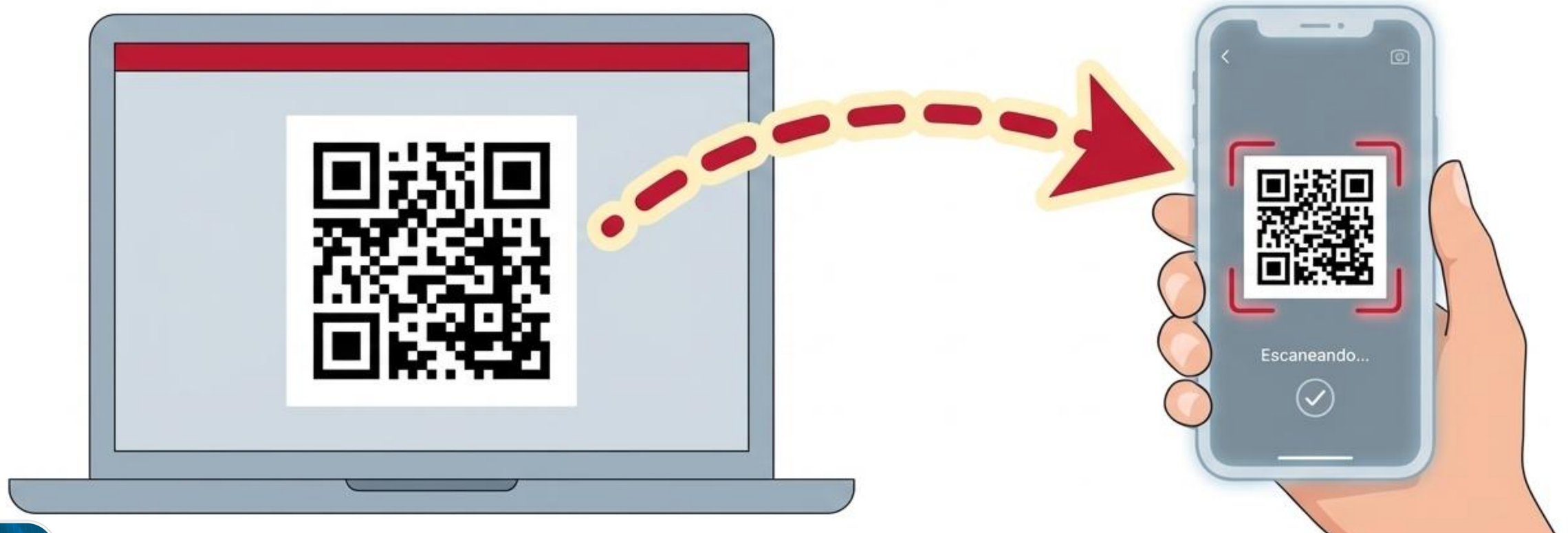
Paso 1: Genera el código QR desde tu ordenador

- Mantente en la página de Gestión de Identidad (IDM) en tu ordenador.
- Haz clic en **Segundo Factor de Autenticación** (columna de la izquierda).
- Pulsa en el botón **Mostrar QR**.



Paso 2: Vincula tu teléfono escaneando el código

Coge tu teléfono móvil y abre la aplicación Google Authenticator que descargaste previamente (puedes usarla con o sin cuenta UCM). Usa la cámara de la aplicación para escanear el código QR que aparece en la pantalla de tu ordenador.



Paso 3: Confirma la activación con tu primer código

Una vez escaneado el QR, la app en tu móvil generará automáticamente un número de 6 dígitos que cambia cada pocos segundos.

MUY IMPORTANTE: Introduce **inmediatamente** este código en la casilla correspondiente de la pantalla de tu ordenador para activar definitamente el 2FA.

Vol ver al inicio

Tu nuevo acceso diario en tres sencillos pasos

A partir de ahora, cada vez que accedas a los servicios de la UCM, el sistema requerirá tu identidad completa.

1. Usuario:
Tu correo electrónico **@ucm.es**

2. Contraseña:
La clave de tu cuenta UCM

3. Clave 2FA:
Abre Google Authenticator en el móvil e introduce el código aleatorio temporal (cambia cada 30 segundos).

Volver al inicio

La regla de los 14 días y los equipos compartidos

Durante el inicio de sesión, verás una casilla de Confiar en este equipo. Si la marcas, no se te pedirá el código 2FA durante 14 días en ese dispositivo.

☐ **CONFIAR EN ESTE EQUIPO**

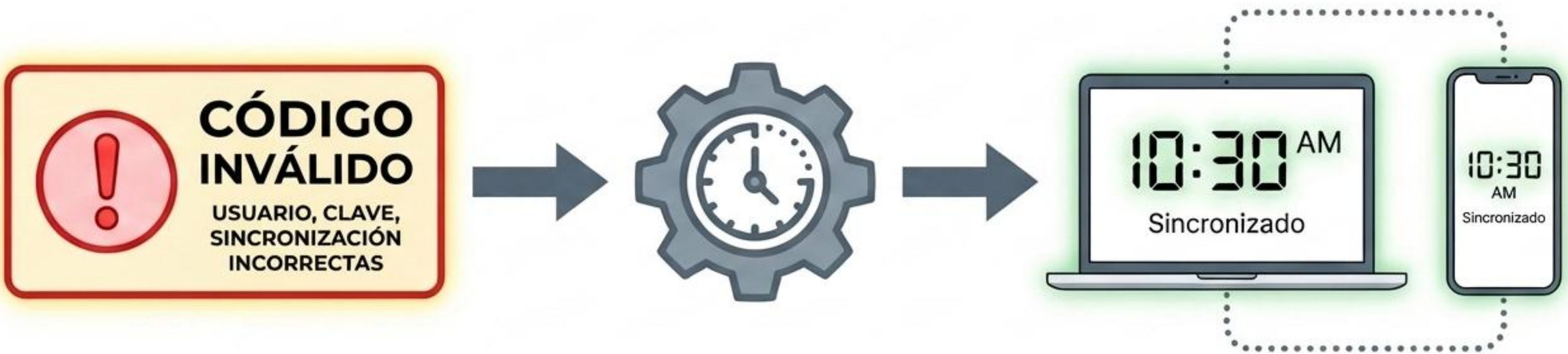
SÍ: En tu equipo personal y privado.

NUNCA pulses esta opción si estás accediendo desde un ordenador de uso ocasional, público o compartido (bibliotecas, laboratorios, cibercafés).

Volver al inicio

Solución rápida: ¿El código da error?

Si al introducir el código temporal el sistema te devuelve un error, el problema casi siempre es la desincronización de los relojes. Comprueba inmediatamente que la fecha y la hora son exactamente correctas, tanto en tu ordenador como en tu dispositivo móvil.



La sincronización corrige el error.

Cómo recuperar el acceso si cambias de teléfono móvil

Si tienes un dispositivo nuevo y necesitas reinstalar Authenticator, sigue estos pasos desde tu ordenador:

1. Ve a **www.ucm.es**, arriba a la derecha haz clic en **Navegar identificado**.
2. Pulsa en **Olvidó la contraseña**.
3. Marca la opción **Si no dispone de un código de Recuperación**.
4. Introduce tu tipo y número de documento de identidad.

El último paso para restaurar tu 2FA tras un cambio de equipo

Tras verificar tu identidad, el sistema utilizará **tu correo de respaldo**.

5. Se enviará un **Código de Reseteo** a tu dirección de correo electrónico **alternativa**.

6. Este correo incluirá un **enlace** para acceder de nuevo a **Gestión de Identidad**.

7. Una vez dentro, debes **desactivar el 2FA antiguo** y volver a activarlo siguiendo los pasos de esta guía.

Volver al inicio

Tu identidad digital en la UCM está protegida

Al completar este proceso, has asegurado tu cuenta contra accesos no autorizados. Tu entorno universitario es ahora mucho más seguro.

Volver al inicio

Acceso Seguro UCM

Guía rápida para la Autenticación de Doble Factor (2FA) en la Universidad Complutense.

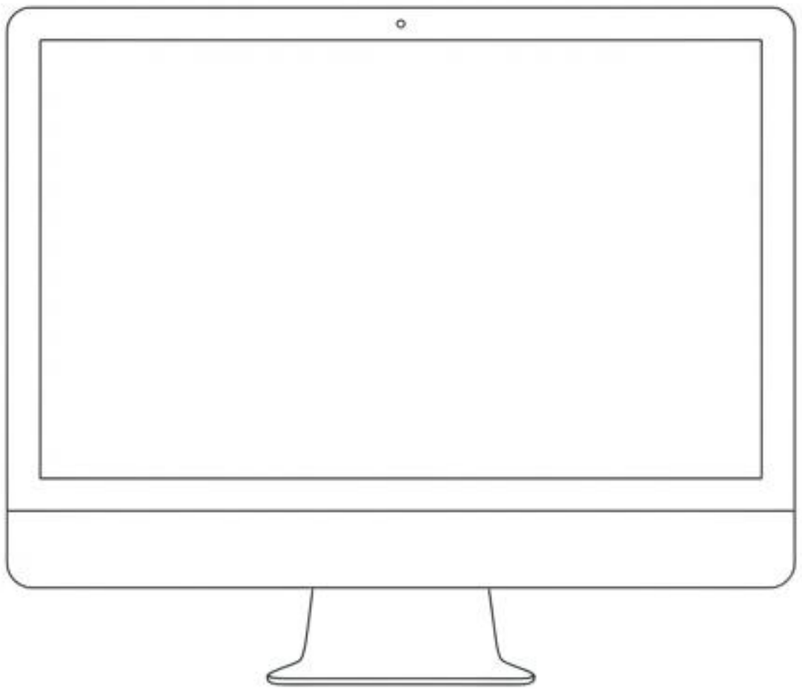
5 pasos sencillos para validar su identidad y acceder al portal SSO.

Servicios Informáticos - Área de Gobierno TI y Asistencia Técnica al Usuario

Volver al inicio

UNIVERSIDAD COMPLUTENSE MADRID

Dos dispositivos, una sola llave de acceso.



1. Su Equipo

Portal SSO UCM (Email + Contraseña)

2. Su Móvil

App Authenticator (Llave temporal)

El flujo de autenticación paso a paso.

1

Ingrese su cuenta email y contraseña en la web de SSO de la UCM.

2

Abra la app Authenticator en su móvil para generar su código.

3

Introduzca el número en el campo CLAVE SEGUNDO FACTOR DE AUTENTICACIÓN.

4

Pulse el botón INICIAR SESIÓN.

La ventana de seguridad de 30 segundos.

El código en su app Authenticator es dinámico. Cambia automáticamente cada 30 segundos para garantizar la máxima seguridad frente a interceptaciones.

Si el tiempo se agota antes de pulsar Iniciar Sesión, simplemente introduzca el nuevo número que aparezca en pantalla.

Cuándo utilizar la opción Confiar en este equipo.

Dispositivo Personal y Privado

SÍ. Marque la casilla.

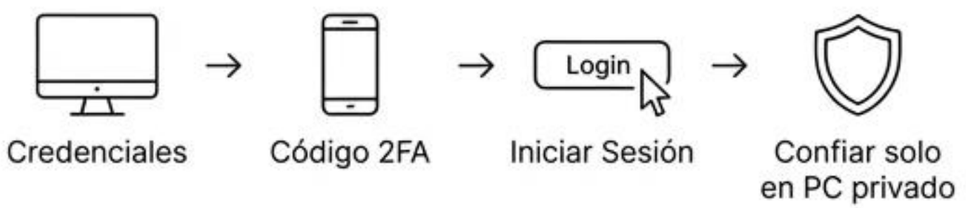
Durante 14 días NO se le pedirá el 2FA en ese **equipo y navegador específico**. (**Nota:** Transcurrido el tiempo, o si cambia de navegador/perfil, el sistema volverá a solicitarlo).

Equipo de Uso Común o Compartido

NUNCA. Deje la casilla en blanco.

No **confíe la sesión en aulas, bibliotecas o cibercafés** para evitar comprometer sus datos.

Resumen de acceso.



Sesión iniciada con éxito en la red de la Universidad Complutense de Madrid.

Servicios Informáticos - Área de Gobierno TI y Asistencia Técnica al Usuario

Volver al inicio

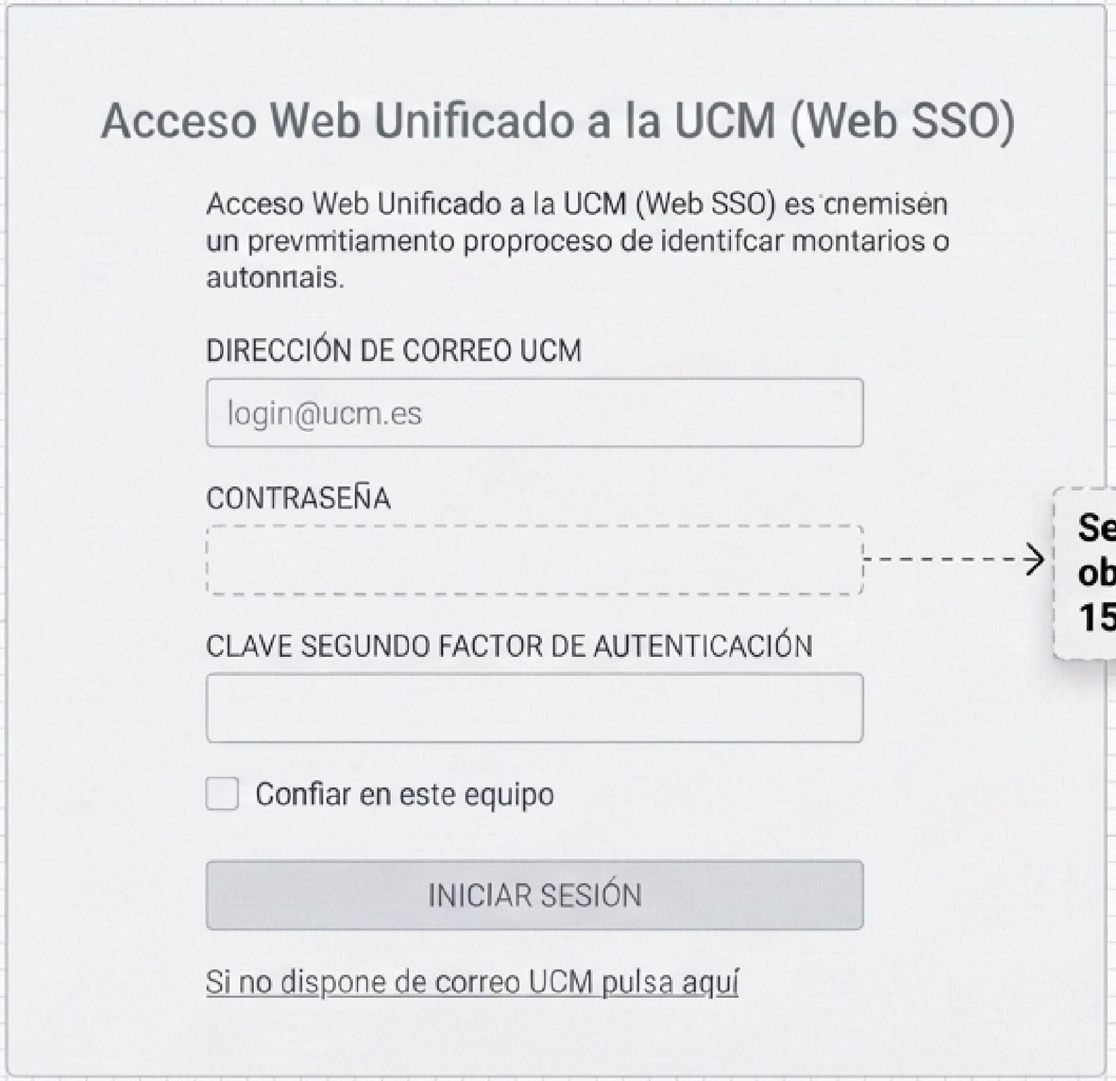
Acceso UCM: Guía Visual de Otros Medios de Autenticación Segura

Desmitificando el acceso seguro mediante Certificado Digital y Cl@ve

Volver al inicio

Servicios Informáticos - Gobierno TI y Asistencia Técnica al Usuario

UNIVERSIDAD COMPLUTENSE MADRID



El acceso tradicional (izquierda) requiere de verificación en dos pasos.

Segundo factor obligatorio desde el 15 de abril de 2026

OTROS MEDIOS DE AUTENTICACIÓN

- Certificado Digital
- Cl@ve

Alternativa de autenticación (derecha).

Elija el método de autenticación UCM alternativo

	Certificado Digital	Cl@ve
Naturaleza	Archivo local o hardware (DNIe)	Ecosistema en la nube y App móvil
Requisitos Previos	Instalación de AutoFirma y certificado en el navegador	Registro previo y App Cl@ve Móvil instalada
Ideal para...	Equipos propios de oficina o uso intensivo	Cualquier dispositivo, movilidad y fricción cero en equipos compartidos

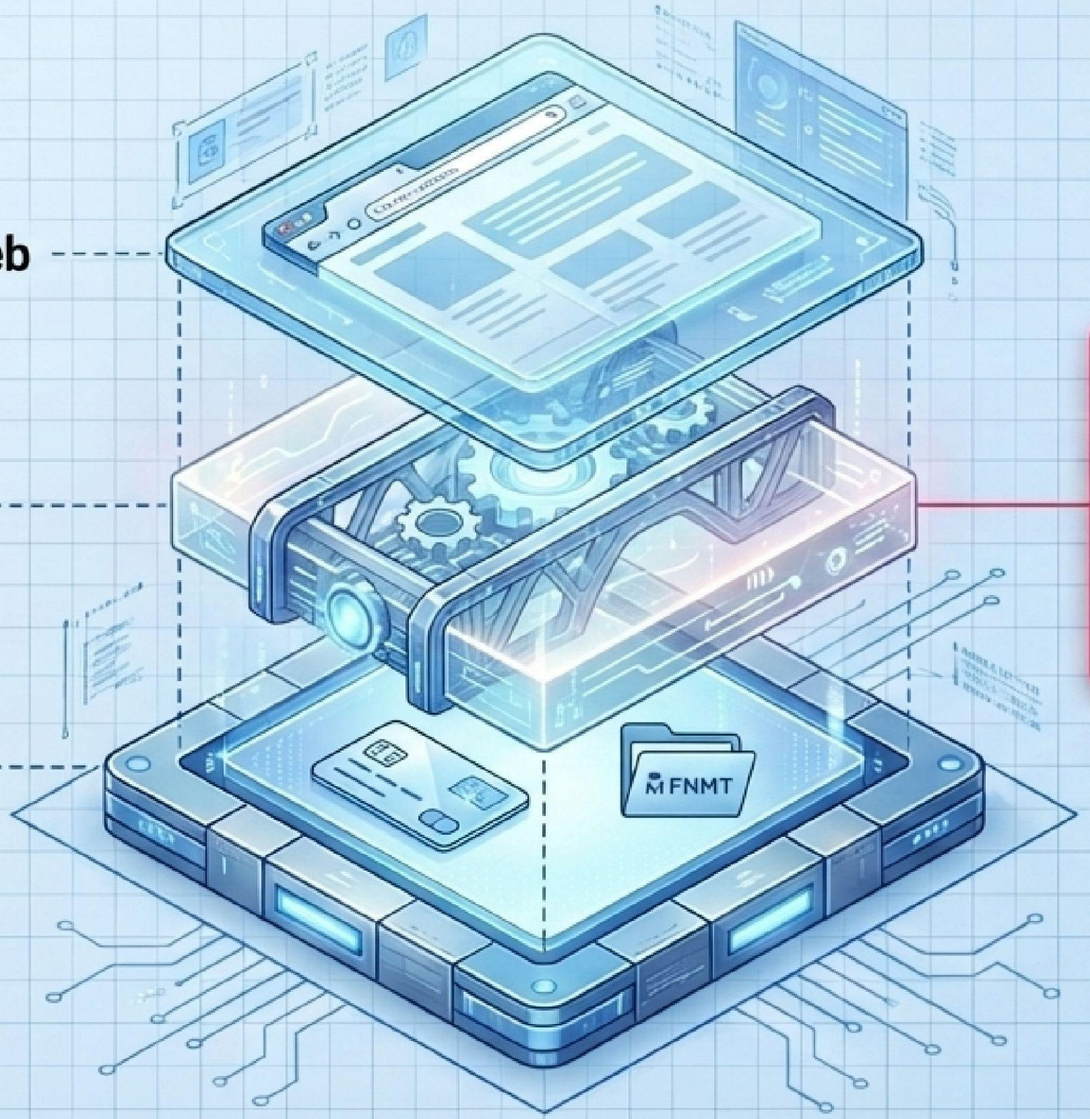
Autenticación con Certificado Digital

El acceso con Certificado Digital requiere configuración de su dispositivo

Interfaz: El Navegador Web

Puente: AutoFirma

Base: El Certificado
(Archivo FNMT o tarjeta DNIe insertada)



Nota

AutoFirma es indispensable. Es el motor que permite al navegador acceder de forma segura al almacén de certificados (KeyStore) de su sistema operativo sin exponer sus claves privadas.

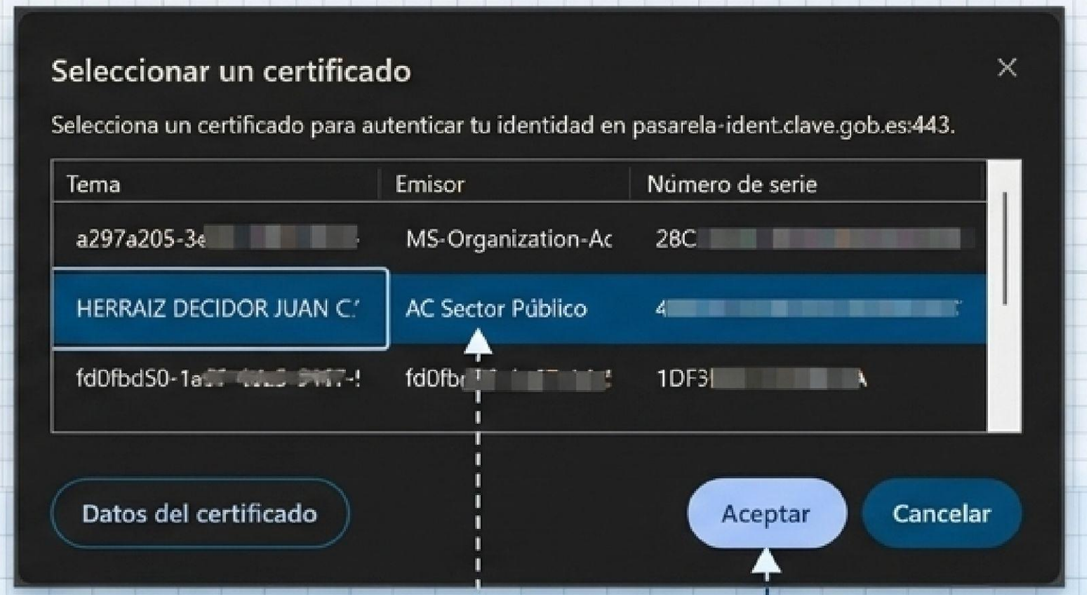
Volver al inicio

Vía 1: Certificado Digital - El Flujo de Acceso

1

Certificado Digital

2



Emisor
Verifique que corresponde a una entidad de confianza (ej. AC Sector Público).

Acción Única
Solo requiere seleccionar su identidad y hacer clic en Aceptar. Acceso instantáneo completado.

Volver al inicio

UNIVERSIDAD COMPLUTENSE MADRID

Autenticación con Clave

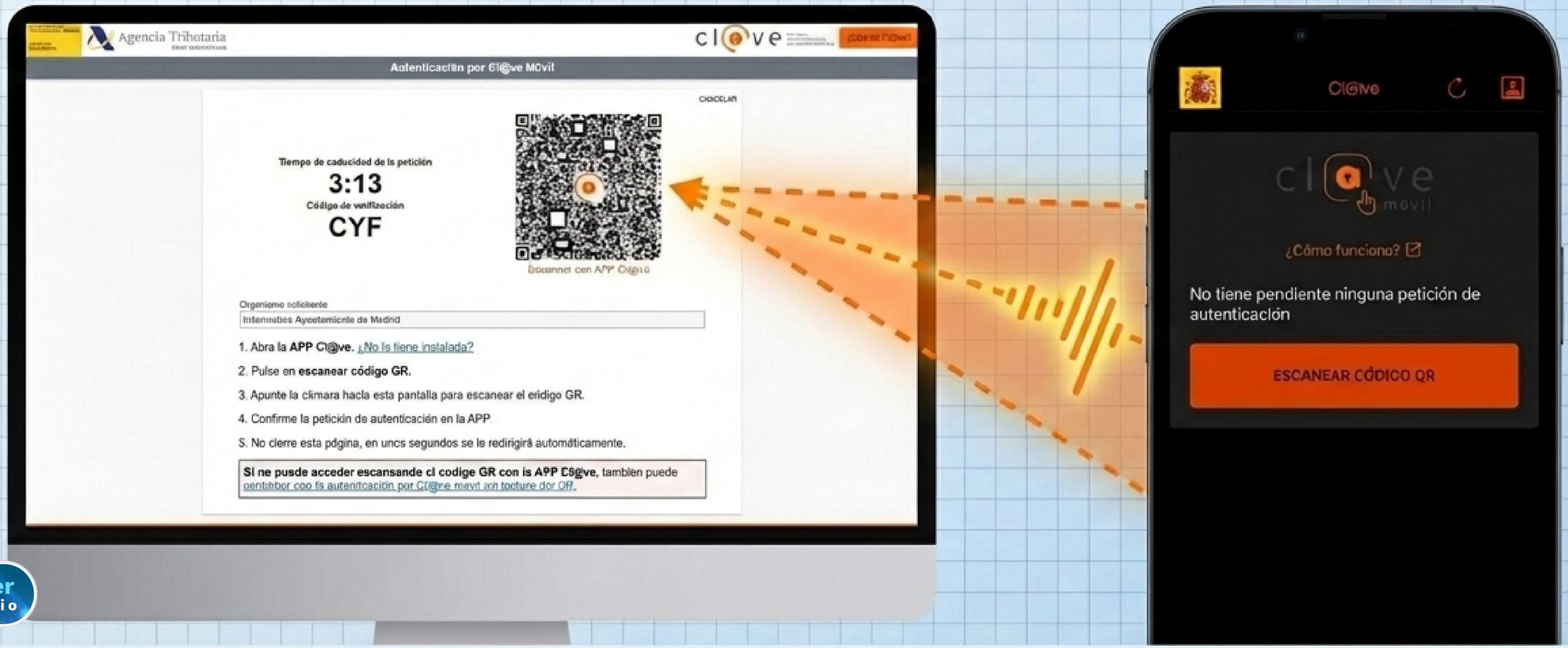
La pasarela del Gobierno ofrece múltiples vías.

La Vía Recomendada: Cl@ve Móvil

Sustituye los antiguos sistemas de PIN y contraseñas permanentes por una validación biométrica directa desde su smartphone, **sin requerir certificados locales en el PC.**

Vía 2: Cl@ve Móvil - El Puente Pantalla-Móvil

El navegador de escritorio solicita el acceso; su dispositivo móvil personal confirma su identidad mediante un escaneo seguro.



Volver al inicio

Verificación y Confirmación

Compruebe siempre que el organismo solicitante es legítimo antes de pulsar **Confirmar**.
El acceso en su ordenador se habilitará de forma automática en segundos.

Compruebe que la página web de su navegador comienza por **https://www2.agenciatributaria.gob.es/**

Volver al inicio

Resumen de uso de métodos alternativos de Autenticación

Vía Certificado

- Certificado en vigor instalado en el sistema.
- Aplicación AutoFirma instalada y actualizada.

Vía Cl@ve

- Registro en el sistema estatal Cl@ve completado.
- App Cl@ve Móvil activa en su smartphone con notificaciones permitidas.

Tu Identidad Digital, Sin Frustraciones

La guía definitiva paso a paso para configurar tu DNI electrónico (DNIe) al primer intento.

Guía Cívica Moderna

Servicios Informáticos - Gobierno TI y Asistencia Técnica al Usuario

Volver al inicio

El Mapa de Ruta

Mundo Físico
Hardware y Comisaría

El Puente
Instalación de Drivers

El Navegador
Configuración Web

La Victoria
Verificación y Trámites

Un proceso lógico, dividido en cuatro hitos predecibles. Empezemos por la base física.

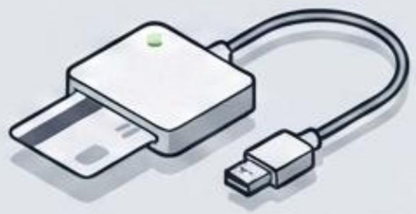
Volver al inicio

El Peaje Físico: Lo que necesitas en tu mesa

El Ordenador

PC Compatible (Intel Pentium III o superior).

Sistemas soportados:
Windows (XP, 7, 8, 10, 11)
Linux, Unix o Mac



El Lector

- Estándar ISO-7816 (1, 2 y 3)
- Tarjetas asíncronas (T=0 y T=1)
- Velocidad mínima de 9.600 bps
- Soporte API PC/SC o CSP / PKCS#11

El Único Paso Fuera de Casa: Activación Presencial

1

La Máquina Oficial

Acude a una comisaría de expedición de la Policía Nacional. Busca las máquinas de activación específicas. No se puede hacer desde casa.

2

Biometría

Introduce tu DNIe en la ranura y coloca tu dedo en el lector de huella dactilar para verificar tu identidad.

3

El Código Maestro

Establece un PIN de seguridad en la pantalla táctil.

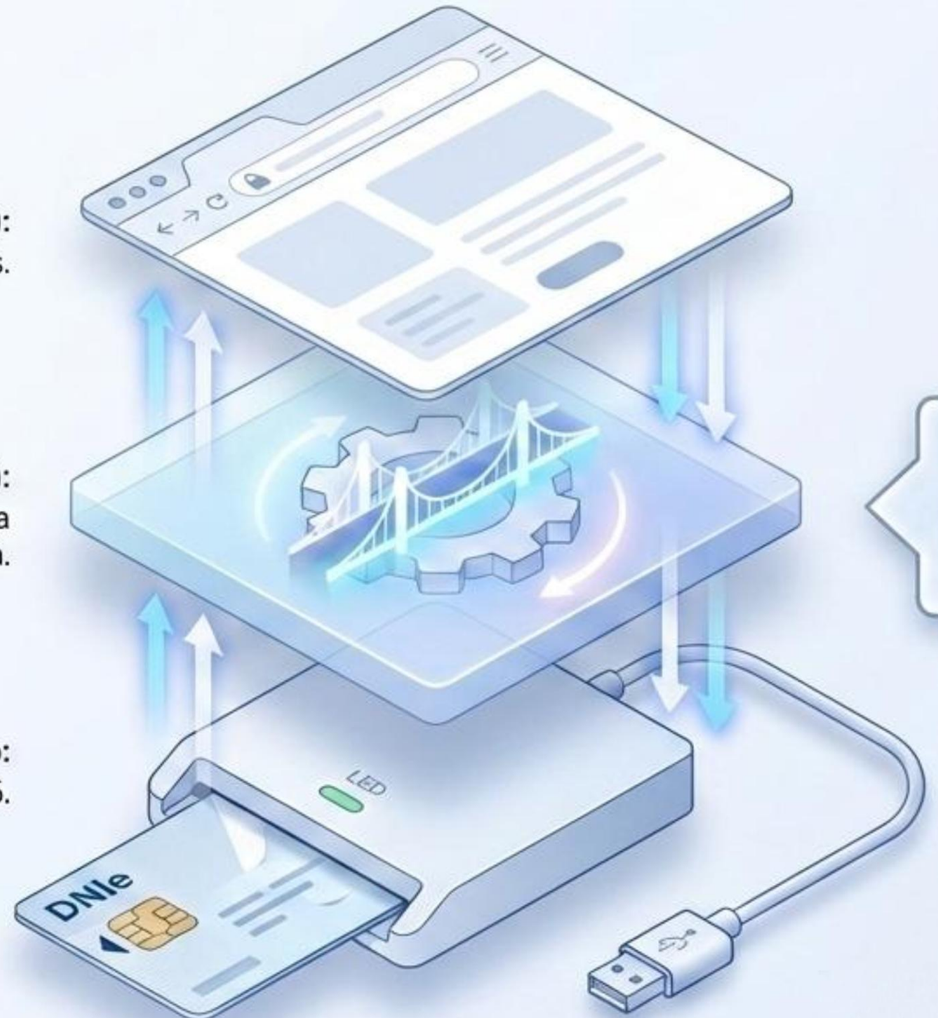
¡Regla de Oro! El PIN debe ser alfanumérico e incluir un símbolo especial. Guárdalo como si fuera la llave de tu casa. Sin él, el resto del proceso es inútil.

Anatomía de una Conexión Segura

La Ventana al Mundo (Navegador Web):
Chrome, Edge o Firefox gestionando tus trámites.

El Traductor (Drivers / Módulo Criptográfico):
El software base que permite al sistema operativo entender el chip de tu tarjeta.

Hardware Físico:
Tarjeta insertada en el Lector ISO-7816.



Nuestro próximo paso es construir la Capa 2: El Traductor.

Volver al inicio

El Origen de la Confianza: Descarga Oficial

1. Accede a **dnielectronico.es**

2. Navega al "Área de Descargas"

3. Elige tu Sistema Operativo. En Windows modernos, casi siempre será 64 bits.

4. Descarga el instalador del módulo criptográfico

Acceso Directo Oficial

Instalación y la Regla del Reinicio

Ejecutar

Abre el archivo descargado (Ej: DNIe_v11...exe).

Instalar

Sigue el asistente para instalar el Módulo Criptográfico (CSP para Windows).

NO Conectar Aún

Mantén el lector **desconectado** durante la instalación.

¡ALTO! REINICIO OBLIGATORIO.

Para que tu ordenador registre los certificados raíz y detecte el lector correctamente, es **absolutamente obligatorio reiniciar el equipo** ahora mismo.
Si saltas este paso, **nada funcionará.**

La Encrucijada del Navegador: Elige tu Ruta

A
La Vía Integrada
Google Chrome & Microsoft Edge

Tecnología: Smart Card Minidriver (Plug & Play)

Comportamiento: Automático. Windows detecta la tarjeta y configura todo.

Nivel de Esfuerzo: Bajo. Listo en minutos.

B
La Vía Independiente
Mozilla Firefox

Tecnología: Arquitectura PKCS#11

Comportamiento: Manual. Requiere cargar el módulo criptográfico (.dll) en los ajustes del navegador.

Nivel de Esfuerzo: Medio. Requiere configuración paso a paso.

Ruta A: Configuración en Chrome o Edge

Paso 1: Inserción

Conecta el lector e **introduce el DNIe**. El sistema instalará el driver automáticamente de forma silenciosa.

Paso 2: Menús

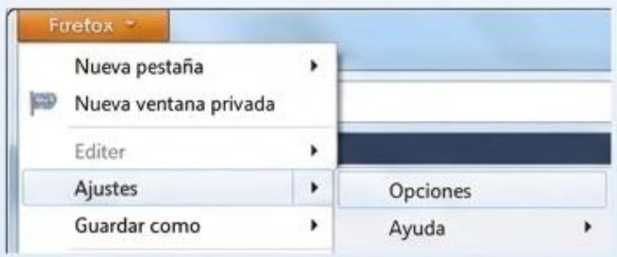
Navega a Herramientas → Opciones de Internet → Contenido → Certificados.

Paso 3: Verificación Rápida

Al abrir la ventana, deberías ver tus certificados listados listos para usarse.

Ruta B: El Módulo Manual en Firefox

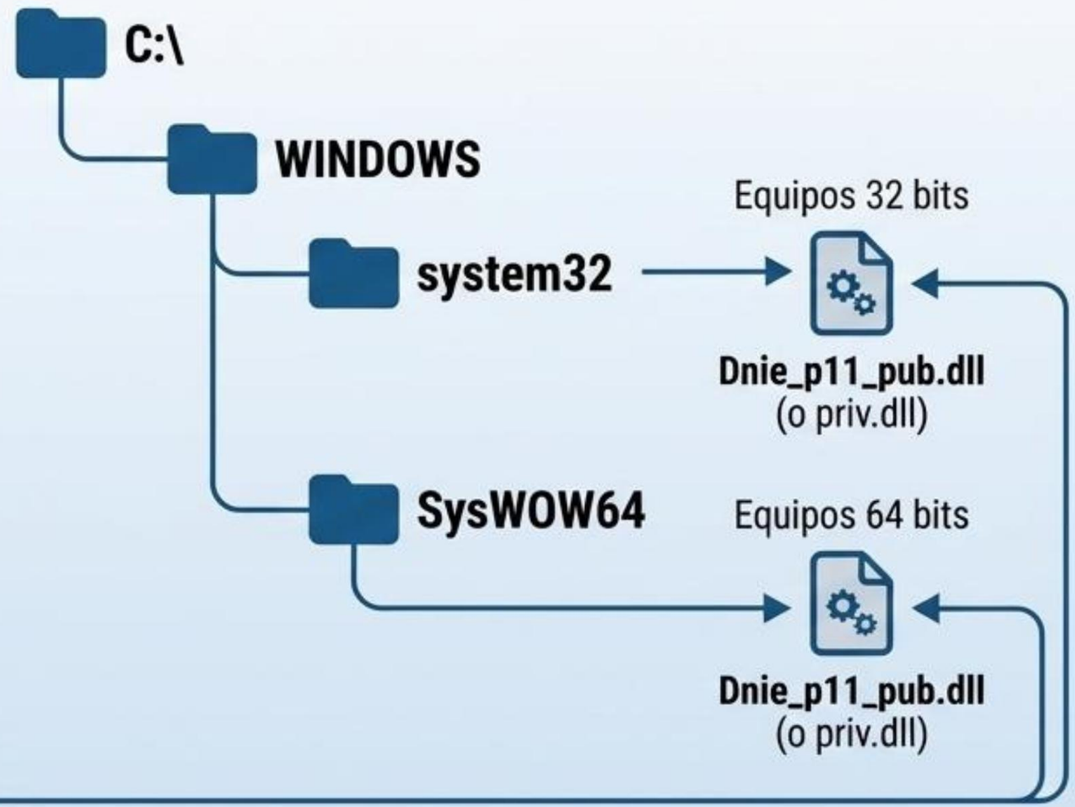
1. 1. Abre Firefox. Ve a **Ajustes → Privacidad & Seguridad → Seguridad → Certificados.**



2. 2. Haz clic en el botón **Dispositivos de Seguridad**.

3. 3. Haz clic en **Cargar** para añadir un **nuevo módulo PKCS#11**.

4. 4. Busca y seleccione el archivo **DLL correspondiente a tu sistema**:



Estado: Los certificados aparecerán en la pestaña 'Sus certificados'.

Volver al inicio

La Prueba de Fuego

La Acción

1. Introduce el DNIe en el lector.
2. Entra en un entorno de prueba oficial: www.usatudnie.es
3. Selecciona un servicio para identificarte.

El Resultado Esperado

Aparecerá un aviso de seguridad de Windows pidiendo tu PIN. Introduce el PIN que creaste en la comisaría.

Al acceder, verás dos certificados activos: **(AUTENTICACIÓN)** y **(FIRMA)**.

Recuperación del Segundo Factor de Autenticación

Guía visual para volver a escanear tu código QR

Vol ver al inicio

UNIVERSIDAD COMPLUTENSE MADRID

El proceso de recuperación en 3 fases

Fase 1: Petición

Solicita un código de rescate automático a tu correo electrónico alternativo.

Fase 2: Validación

Demuestra tu identidad utilizando el código recibido.

Fase 3: Configuración

Accede al portal y vuelve a escanear tu nuevo QR.

Fase 1: Solicitar el Código de Recuperación

A: En la página de validación SSO de la UCM, pulsa

Olvidó la Contraseña

B. Marca la casilla

SI NO dispone de un Código de Recuperación

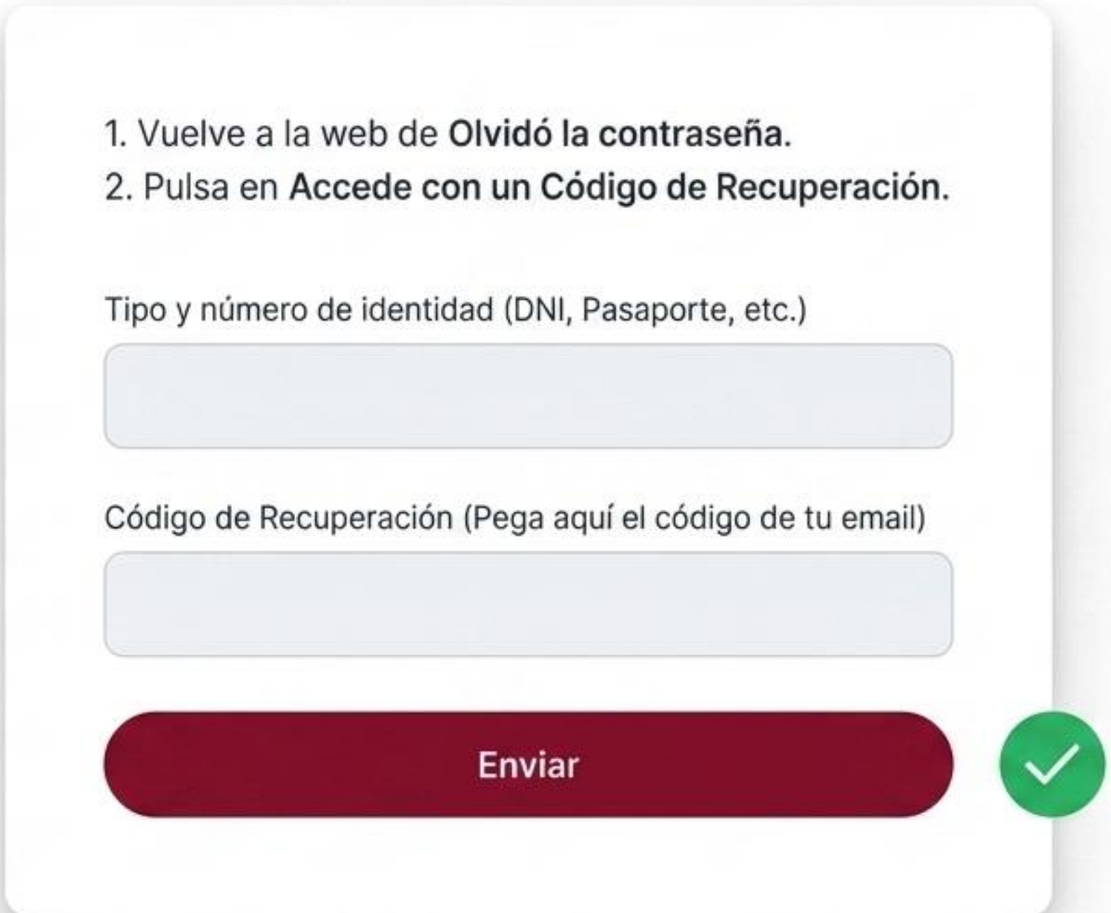
C. Rellena tu identificador, verifica que tu dirección alternativa esté marcada y pulsa

Enviar

Ve a tu email alternativo.
Habrás recibido un correo automático.
Copia el Código de Recuperación.

Vol ver al inicio

Fase 2: Validación de Identidad



Fase 3: Acceso a IDM y Re-escaneo

idm.ucm.es

¡Validación exitosa! Eres redirigido a este panel.

Opción A: Realizar un cambio de contraseña.

Opción B: Volver a escanear el Segundo Factor de Autenticación (2FA) para tu uso habitual.

Matriz de Métodos de Acceso a Servicios UCM

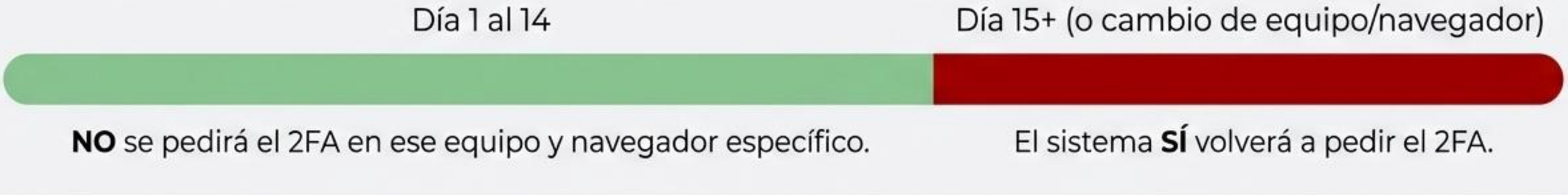
⚠ Recordatorio: Una vez activado, es IMPRESCINDIBLE introducir el 2FA para acceder a los servicios UCM.

Método de Acceso	¿Requiere Contraseña?	¿Requiere 2FA?
Estándar (Email Institucional)	✓ Sí	✓ Sí (App/Dispositivo)
Alternativa 1 (Certificado Digital)	✗ No	✗ No (Acceso directo)
Alternativa 2 (Sistema Cl@ve)	✗ No	✗ No (Acceso directo)

Volver al inicio

Gestión de Equipos: La regla de los 14 días

Si marcas la casilla Confiar en este equipo...



Recomendación de uso

No marques esta casilla al comienzo de usar el 2FA. Si confías el equipo el primer día, al llegar el día 15 habrás olvidado cómo funcionaba el proceso. Es mejor practicar durante las primeras semanas para asimilar el hábito.

Resumen de Seguridad UCM

Mantén siempre actualizada tu dirección de correo electrónico alternativo; es tu única vía de rescate.

Si fallas al entrar, busca siempre la ruta "Olvidó la Contraseña" para reiniciar el proceso.

Practica el uso del 2FA antes de usar la función "Confiar en este equipo" para no olvidar el procedimiento.

Vol ver al inicio

Activación del Segundo Factor de Autenticación (2FA) en Cuentas Institucionales

Procesos, plazos y gestión de titularidad en la UCM.

Clarificación de Plazos: Qué vence y cuándo

Cuentas Personales

Fecha límite estricta: 15/04/2026.

La obligatoriedad de esta fecha aplica exclusivamente a su cuenta personal de la Universidad.

Cuentas Institucionales

Obligatorio en breve, pero NO inmediato.

Existe un margen de tiempo para ayudarles con la activación y aclarar dudas. No requiere acción urgente hoy.

Volver al inicio

La Regla de Oro de la Titularidad

La activación del 2FA en una cuenta institucional SÓLO la puede realizar el Titular de esa cuenta.

⚠ Arquitectura de Acceso No intente iniciar sesión con el correo institucional. Debe navegar identificado dentro de la UCM con sus datos personales.

Vol ver
al inicio

Paso 1: Acceso al Gestor de Identidad

1. Inicie sesión en **idm.ucm.es** con su usuario personal.
2. Navegue al menú lateral izquierdo.
3. Seleccione **Buzones vinculados**.

Nota: Esta opción sólo le aparecerá si dispone de alguna cuenta institucional en la que es titular.

Paso 2: El Panel de Control Institucional

A la izquierda aparecerán las cuentas institucionales a su nombre. Al seleccionar una, tendrá 3 opciones de gestión:

Cambiar la contraseña.

Activar el 2FA.

Pulse sobre este icono para iniciar el proceso.

Transferir la titularidad a otra cuenta personal UCM.

Paso 3: Generación y Escaneo del Código

Al pulsar el icono QR, se abrirá una nueva ventana con su código único.

Escanee el código con su app Authenticator.
(La aplicación permite añadir tantos códigos de cuentas distintas como desee).

Introduzca el código numérico generado de 6 dígitos en el campo inferior y pulse **Activar**.

El Protocolo de Acceso Compartido

¿Qué ocurre con el resto del equipo?

El código QR es el secreto compartido del equipo.

- El titular debe coordinarse con todas las personas que usen la cuenta institucional.
- Regla vital: Todos los usuarios deben configurar el 2FA en sus respectivos dispositivos escaneando ese mismo código QR original.

> Si no es el titular de la cuenta, póngase en contacto con él para que le facilite el acceso a este código.

Volver al inicio

Síntesis de Activación: Sus 4 Claves

Tranquilidad

Dispone de margen de tiempo. La urgencia del 15/04/26 es solo para cuentas personales.

Identidad

Opere siempre desde idm.ucm.es validado como el Titular con sus credenciales personales.

Ejecución

Localice Buzones vinculados, genere el código QR y actívelo con su app Authenticator.

Equipo

Sincronice a sus colaboradores asegurándose de que todos escaneen el mismo código QR original.