TRABAJO FIN DE GRADO

ESCUELA POLITÉCNICA SUPERIOR

Grado en Ingeniería Informática

MANUAL DE USUARIO

Autor:

D. Marc Hernández Montesinos

Directora:

Dra. Dña. *Angélica Guzmán Ponce*

Murcia, Junio de 2026

TRABAJO FIN DE GRADO

UCAM
UNIVERSIDAD CATÓLICA
DE MURCIA

ESCUELA POLITÉCNICA SUPERIOR

Grado en Ingeniería Informática

MANUAL DE USUARIO

Autor:

D. Marc Hernández Montesinos

Directora:

Dra. Dña. *Angélica Guzmán Ponce*

Murcia, Junio de 2026

https://tfg.marchernandez.es/videos/video-demostrativo.mp4

ÍNDICE

MANUAL DE USUARIO

Registro, inicio de sesión, gestión del perfil y ciclo de certificados

Documento separado del Trabajo de Fin de Grado *"Diseño e implementación de un sistema integrado de PKI y SSO para organizaciones pequeñas"* de Marc Hernández Montesinos (UCAM, Grado en Ingeniería Informática).

Campo	Valor
Documento	Manual de Usuario
Versión	1.0
Fecha	1 junio 2026
URL pública	https://tfg.marchernandez.es/manuales/Manual_Usuario.pdf
TFG asociado	https://tfg.marchernandez.es

Este manual conserva la numeración interna original (sección H.x) por trazabilidad con las versiones previas del documento. Las referencias cruzadas que apuntan al cuerpo del TFG (capítulos 1-10, anexos A-D) se mantienen tal cual y son válidas frente al PDF principal del TFG.

Manual orientado al usuario final del sistema integrado PKI + SSO. Cubre el ciclo completo desde el primer acceso hasta la revocación de un certificado propio. Está pensado para que una persona sin experiencia previa pueda completar las tareas habituales en menos de treinta minutos. Las cuestiones técnicas de instalación, administración y operación interna se tratan en los manuales correspondientes (véase la tabla H.1 al final del manual).

H.1 Introducción y alcance

H.1.1 ¿Qué hace este sistema?

El sistema le permite, con una única cuenta, hacer dos cosas:

1. **Iniciar sesión** en cualquiera de las aplicaciones de la organización sin tener que volver a introducir su contraseña en cada una de ellas. A esto se le llama *Single Sign-On* (SSO).
2. **Solicitar y gestionar certificados digitales** propios para firmar documentos, autenticarse en servicios que lo requieran o cifrar correo, sin depender de autoridades externas.

Las dos funciones están integradas: la cuenta que utiliza para iniciar sesión es la misma con la que solicita y gestiona sus certificados.

H.1.2 Antes de empezar

Para usar el sistema necesita únicamente:

- Un navegador web actualizado (Chrome, Firefox, Edge o Safari de los últimos dos años).
- Una dirección de correo válida.
- Para las funciones de mayor confianza, opcionalmente un certificado FNMT o DNIe o un teléfono móvil con una aplicación de códigos TOTP (Google Authenticator, Authy, Microsoft Authenticator, FreeOTP).

No se requiere instalar ningún programa.

H.1.3 Idiomas

La interfaz está disponible en cuatro idiomas: español, inglés, francés y alemán. El idioma se selecciona desde el botón en la esquina superior derecha. La preferencia se conserva entre sesiones.

H.1.4 Convenciones de este manual

Convención	Significado
`texto en monoespaciado`	Nombre de un campo del formulario, identificador o ruta.

Convención	Significado
Negrita	Acción que debe ejecutar (por ejemplo, **pulse Aceptar**).
Cursiva	Concepto técnico introducido por primera vez.
Aviso	Información relevante para evitar problemas.

H.2 Registro y primer acceso

H.2.1 Crear una cuenta

1. Acceda a `https://sso.marchernandez.es/register.php`.
2. Rellene los cuatro campos del formulario:
    - **Nombre de usuario**: identificador único, sin espacios ni caracteres especiales (de 3 a 32 caracteres).
    - **Correo electrónico**: dirección válida; recibirá un mensaje de verificación.
    - **Contraseña**: mínimo doce caracteres con al menos una mayúscula, una minúscula y un dígito.
    - **Confirmación de la contraseña**.
3. **Pulse Crear cuenta**. Recibirá un correo con un enlace de confirmación.
4. **Abra el correo** y siga el enlace para activar la cuenta. El enlace caduca a las 24 horas; si caduca, puede solicitar uno nuevo desde la pantalla de inicio de sesión.

Aviso. El sistema no permite recuperar la contraseña sin acceso al correo registrado. Asegúrese de utilizar una dirección estable.

H.2.2 Configurar el segundo factor (TOTP)

El sistema **requiere un segundo factor** para todas las cuentas. La forma más común es un código de seis dígitos generado por una aplicación móvil (TOTP, RFC 6238).

1. Tras activar la cuenta, el sistema le redirige a la pantalla **Configurar TOTP**.
2. Abra su aplicación de autenticación (Google Authenticator, Authy, Microsoft Authenticator o FreeOTP).
3. **Escanee el código QR** mostrado en pantalla, o introduzca manualmente la cadena alfanumérica que aparece debajo.
4. La aplicación móvil empezará a generar un código de seis dígitos que cambia cada treinta segundos.
5. **Introduzca el código actual** en el campo **Verificar código** y **pulse Confirmar**.
6. El sistema le mostrará **diez códigos de recuperación**. **Guárdelos en un lugar seguro** (gestor de contraseñas o impreso): le permitirán acceder si pierde el teléfono. Cada código sólo sirve una vez.

Aviso. Si pierde el teléfono y los códigos de recuperación, deberá contactar con un administrador para reiniciar el segundo factor; no existe vía automática de recuperación.

H.2.3 Vincular un certificado FNMT o DNIe (opcional)

Si dispone de un certificado de la FNMT o de DNIe y desea utilizarlo como método de autenticación principal, puede vincularlo a su cuenta:

1. Inicie sesión con contraseña + TOTP en `https://sso.marchernandez.es/`.
2. **Acceda a Mi perfil → Métodos de autenticación → Vincular certificado**.
3. **Pulse Iniciar vinculación**. El navegador le solicitará el certificado a presentar.

4. **Seleccione el certificado FNMT o DNIe** que quiera vincular y **pulse Aceptar**.

5. El sistema verifica el certificado contra los emisores reconocidos. Si es válido, queda vinculado a su cuenta y puede usarlo en lo sucesivo como método de inicio de sesión sin contraseña.

H.3 Inicio de sesión

El sistema admite cuatro métodos de inicio de sesión. Puede tener varios métodos vinculados a la misma cuenta y elegir cuál usar en cada acceso.

H.3.1 Contraseña + TOTP

Es el método por defecto y el único disponible inmediatamente tras el registro.

1. Acceda a `https://sso.marchernandez.es/login.php`.

2. **Introduzca su nombre de usuario y su contraseña** y **pulse Iniciar sesión**.

3. En la pantalla siguiente, **introduzca el código TOTP de seis dígitos** que muestre la aplicación móvil.

4. **Pulse Verificar**. Si el código es correcto, el sistema le redirige a la pantalla principal.

H.3.2 Certificado FNMT

1. Acceda a `https://sso.marchernandez.es/login.php`.

2. **Pulse Iniciar sesión con certificado**.

3. El navegador solicitará un certificado cliente. **Seleccione el certificado FNMT** vinculado previamente a su cuenta y **pulse Aceptar**.

4. Si el certificado es válido y está vinculado, el sistema inicia sesión sin pedir contraseña ni TOTP.

H.3.3 DNIe (DNI electrónico)

1. **Inserte el DNIe en el lector** y asegúrese de que el sistema operativo lo reconoce (en Windows, suele aparecer en el almacén de certificados; en macOS y Linux, requiere los módulos correspondientes).
2. Acceda a `https://sso.marchernandez.es/login.php`.
3. **Pulse Iniciar sesión con DNIe**.
4. **Introduzca el PIN del DNIe** cuando el sistema operativo lo solicite.
5. Si el certificado es válido, el sistema inicia sesión.

H.3.4 Certificado emitido por la propia organización

Si dispone de un certificado de cliente emitido por esta misma PKI (perfil `client-auth`), puede utilizarlo del mismo modo que un certificado FNMT (apartado H.3.2). El procedimiento es idéntico: seleccionar el certificado cuando el navegador lo solicite.

H.3.5 Cerrar sesión

Pulse el botón Cerrar sesión en la esquina superior derecha. Se cierran simultáneamente la sesión SSO y todas las sesiones abiertas en aplicaciones cliente vinculadas (cierre de sesión global, RFC 7009 *RP-Initiated Logout*).

H.4 Gestión del perfil

Acceda al panel **Mi perfil** desde el menú principal del SSO.

H.4.1 Cambiar la contraseña

1. **Mi perfil** → **Seguridad** → **Cambiar contraseña**.
2. **Introduzca la contraseña actual y la nueva** (con la nueva confirmada).
3. **Pulse Guardar**. El sistema cierra todas las sesiones activas excepto la actual y le pide reautenticarse en sus aplicaciones cliente abiertas.

H.4.2 Restablecer el segundo factor

Si su teléfono cambia y aún tiene acceso a la cuenta:

1. **Mi perfil → Seguridad → Restablecer TOTP**.
2. **Introduzca la contraseña actual** y **un código de recuperación** o el código TOTP del dispositivo anterior.
3. El sistema mostrará un nuevo código QR para configurar la nueva aplicación móvil.

H.4.3 Sesiones activas

Mi perfil → Sesiones activas muestra todas las sesiones abiertas en su cuenta con su origen (IP), navegador y fecha de inicio.

- **Pulse Cerrar** sobre cualquier sesión sospechosa para terminarla inmediatamente.
- Si ve sesiones que no reconoce, cambie la contraseña a continuación.

H.4.4 Datos personales

Mi perfil → Datos personales permite actualizar:

- Correo electrónico (requiere reverificación).
- Idioma preferido.
- Preferencias de notificación.

Aviso. No es posible cambiar el nombre de usuario una vez creada la cuenta. Si necesita un nombre diferente, contacte con un administrador.

H.5 Solicitar un certificado

El portal PKI le permite solicitar certificados digitales emitidos por la organización para uso personal o profesional. La solicitud sigue cuatro fases: **solicitud → aprobación → emisión → descarga**.

H.5.1 Acceder al portal PKI

1. Inicie sesión en el SSO (apartado H.3).
2. Acceda a `https://pki.marchernandez.es/`.

3. El portal le reconoce automáticamente por la sesión SSO. La primera vez le pedirá completar su perfil PKI (nombre completo y unidad organizativa).

H.5.2 Elegir el perfil de certificado

El sistema ofrece seis perfiles de certificado según el uso al que vaya destinado:

Perfil	Para qué sirve	Validez
Autenticación de servidor (TLS)	Sitios web HTTPS	398 días
Autenticación de cliente (mTLS)	Iniciar sesión en aplicaciones, VPN	825 días
Firma de código	Firmar instaladores, *scripts*	3 años
Firma de documentos	Firmar PDF, contratos	2 años
S/MIME (correo)	Cifrar y firmar correo	825 días
VPN	Conexiones VPN cliente	825 días

Tabla H.1. Perfiles de certificado disponibles.

H.5.3 Crear la solicitud

1. **Acceda al portal PKI → Mis certificados → Solicitar nuevo**.
2. **Seleccione el perfil** apropiado de la lista (apartado H.5.2).
3. **Rellene los campos del formulario**:
    - **Nombre común** (`CN`): por defecto su nombre completo; puede personalizarlo si la solicitud lo requiere.
    - **Correo** (cuando aplique al perfil): por defecto el de su perfil.
    - **DNS o IPs alternativos** (`SAN`, sólo perfiles de servidor): uno por línea.
4. **Pulse Generar y descargar clave privada**. El sistema:

- Genera una **clave RSA-2048** en su navegador.
- Crea una **solicitud (CSR)** firmada con esa clave.
- **Le ofrece descargar la clave privada inmediatamente** en formato `.key`.
- **Envía la CSR al servidor** sin guardar la clave privada en ningún momento.

Aviso. La clave privada sólo se le ofrece una vez. Si no la descarga ahora, no podrá recuperarla más tarde y deberá iniciar una nueva solicitud. Guárdela en un lugar seguro (preferiblemente cifrada con contraseña).

H.5.4 Esperar la aprobación

La solicitud queda en estado pendiente hasta que un administrador la apruebe. Recibirá un correo cuando se aprueba o se rechaza.

- Tiempo habitual: Por lo general, menos de un día hábil.
- Si transcurren más de cuarenta y ocho horas sin respuesta, contacte con un administrador.

H.5.5 Descargar el certificado emitido

Cuando el administrador aprueba la solicitud, el sistema firma el certificado y se lo notifica:

1. **Acceda al portal PKI → Mis certificados**.
2. La solicitud aparece como **emitida**.
3. **Pulse Descargar certificado**. Puede descargarlo en tres formatos:
   - `.crt` (PEM): el certificado público en texto legible.
   - `.pfx` (PKCS#12): el certificado y la clave privada juntos en un fichero protegido por contraseña, listo para importar en Windows o macOS. Pedirá una contraseña al exportar.

- `.p7b`: el certificado con la cadena completa (raíz + intermedia), útil para servidores web.

H.5.6 Importar el certificado en su sistema

Windows

1. **Doble clic** sobre el fichero `.pfx`.
2. Seleccione **Almacén personal del usuario actual**.
3. **Introduzca la contraseña** que asignó al exportar.
4. El certificado queda disponible en el almacén de Windows; cualquier aplicación (Outlook, navegador, VPN) podrá utilizarlo.

macOS

1. **Doble clic** sobre el fichero `.pfx`.
2. **Llavero** se abre y le pide la contraseña del fichero.
3. **Confirme la importación al llavero** `inicio de sesión`.

Firefox

1. **Configuración → Privacidad y seguridad → Certificados → Ver certificados → Sus certificados → Importar**.
2. Seleccione el fichero `.pfx` e introduzca la contraseña.

H.6 Revocar un certificado propio

Un certificado emitido se puede **revocar** en cualquier momento si:

- La clave privada se ha perdido, ha sido robada o se sospecha que ha sido comprometida.
- El motivo del certificado ha desaparecido (cambio de puesto, cierre del servicio).
- El certificado contiene información incorrecta.

Importante. La revocación es irreversible. Una vez revocado, el certificado no puede reactivarse: si lo necesita de nuevo, deberá solicitar uno nuevo.

H.6.1 Procedimiento

1. **Acceda al portal PKI → Mis certificados**.
2. **Localice el certificado** que desea revocar.
3. **Pulse Revocar**.
4. **Seleccione el motivo de revocación** de la lista:
    - **Compromiso de clave**: si sospecha que la clave privada está en manos de un tercero. Selecciónelo siempre que tenga la mínima duda.
    - **Cambio de afiliación**: si el certificado se asocia a un puesto que ya no ocupa.
    - **Sustituido**: si ha solicitado uno nuevo que reemplaza a este.
    - **Cese de operación**: si el servicio asociado ya no existe.
    - **Sin especificar**: sólo si ninguno de los anteriores aplica.
5. **Pulse Confirmar revocación**.
6. El sistema:
    - Marca el certificado como revocado en la base de datos.
    - Regenera la **lista de revocación (CRL)** y la publica en `http://crl.marchernandez.es/`.
    - Actualiza la respuesta del **OCSP** (`http://ocsp.marchernandez.es/`).
7. La propagación es **inmediata**: cualquier verificador recibirá la respuesta de revocación al instante.

H.6.2 Verificar que la revocación se ha publicado

Si necesita confirmar que el certificado revocado figura ya en la CRL:

1. Acceda a `http://crl.marchernandez.es/`.
2. Seleccione la CA que emitió el certificado.

3. **Descargue la última CRL**.
4. Inspecciónela con `openssl crl -in nombre.crl -text -noout` y busque el número de serie de su certificado.

H.7 Preguntas frecuentes

H.7.1 Sobre la cuenta y el inicio de sesión

P. He olvidado la contraseña. ¿Cómo la recupero? R. Desde la pantalla de inicio de sesión, **pulse "He olvidado mi contraseña"**. Recibirá un enlace de restablecimiento en el correo registrado. El enlace caduca a las dos horas. Necesitará confirmarlo con un código TOTP o de recuperación.

P. He cambiado de teléfono y no puedo generar el código TOTP. ¿Qué hago? R. Si guardó los códigos de recuperación, utilice uno de ellos como segundo factor durante el inicio de sesión y, una vez dentro, restablezca el TOTP (apartado H.4.2). Si no guardó los códigos, contacte con un administrador.

P. ¿Puedo usar la misma cuenta desde varios dispositivos? R. Sí. Cada dispositivo abrirá su propia sesión, visible y revocable desde **Mi perfil → Sesiones activas**.

P. Cuando inicio sesión con FNMT o DNIe, ¿también necesito código TOTP? R. No. La presentación del certificado equivale al segundo factor (algo que tiene), por lo que el sistema no exige TOTP en esos métodos.

H.7.2 Sobre los certificados

P. ¿Por qué no puedo descargar la clave privada después de la primera vez? R. Por seguridad: el sistema **nunca almacena la clave privada**. Se genera en su navegador y sólo se le ofrece en la pantalla de creación de la solicitud. Esto garantiza que ni el administrador ni un atacante con acceso al servidor pueden recuperarla.

P. ¿Cuánto tarda la aprobación? R. En horario laboral, habitualmente menos de un día hábil. Las solicitudes urgentes deben coordinarse con un administrador.

P. ¿Puedo solicitar un certificado para un dominio que no es mío? R. El administrador rechazará cualquier solicitud cuyo dominio no le sea asignable. Si el dominio pertenece a la organización, pero a un proyecto distinto del suyo, deberá indicar al administrador la justificación.

P. ¿Cómo verifica un tercero que mi certificado es válido? R. Mediante uno de los dos canales que el sistema publica: - **CRL**: descargando la lista de revocación desde `http://crl.marchernandez.es/`. - **OCSP**: enviando una petición a `http://ocsp.marchernandez.es/`. Casi todos los clientes y servidores lo hacen automáticamente al validar el certificado.

P. He revocado un certificado por error. ¿Puedo deshacerlo? R. No. La revocación es irreversible. Solicite un nuevo certificado.

H.7.3 Sobre la privacidad

P. ¿Qué datos personales almacena el sistema? R. Únicamente los necesarios para el funcionamiento: nombre de usuario, correo electrónico, contraseña *hasheada* (Argon2id, no recuperable) y, opcionalmente, los certificados que vincule. La política completa figura en `https://sso.marchernandez.es/privacy.php`.

P. ¿Puedo borrar mi cuenta? R. Sí. **Mi perfil → Datos personales → Solicitar baja**. La cuenta queda inactiva y se anonimiza tras un periodo de retención de noventa días para registros de auditoría requeridos por normativa.

H.8 Glosario rápido

Término	Definición breve
CA (autoridad certificadora)	Entidad que firma los certificados y avala su autenticidad.
Certificado	Documento digital que vincula una identidad a una clave pública.
Clave privada	Pareja secreta de un certificado; nunca debe compartirse.

Término	Definición breve
CRL (lista de revocación)	Listado firmado de certificados revocados.
CSR (solicitud de certificado)	Petición firmada que se envía a la CA para emitir un certificado.
DNIe	Documento Nacional de Identidad electrónico (España).
FNMT	Fábrica Nacional de Moneda y Timbre, autoridad pública española.
OCSP	Protocolo en línea para verificar el estado de un certificado.
PKI	Infraestructura de clave pública: el conjunto de CAs, certificados y procesos.
PKCS#12 / `.pfx`	Formato que empaqueta certificado y clave privada con contraseña.
SSO	*Single Sign-On*: una sola credencial sirve para varias aplicaciones.
TOTP	Código de un solo uso basado en el reloj (RFC 6238).

H.9 Soporte y problemas habituales

H.9.1 Soporte

Canal	Para qué
Correo `ayuda@apps.marchernandez.es`	Consultas funcionales, dudas de uso.

Canal	Para qué
Formulario `https://sso.marchernandez.es/support.php`	Incidencias con la cuenta.
Administrador (vía organización)	Reinicio de TOTP, recuperación sin código.

H.9.2 Problemas habituales y soluciones

El correo de activación no llega. - Compruebe la carpeta de correo no deseado. - Verifique que la dirección introducida es correcta. - Si tras 30 minutos no llega, solicite un nuevo correo desde la pantalla de inicio de sesión.

El navegador no me ofrece elegir el certificado. - Asegúrese de que el certificado está importado en el almacén del sistema operativo o en el navegador (apartado H.5.6). - Cierre el navegador y ábralo de nuevo. - En Firefox, compruebe que tiene activada la opción **Configuración → Privacidad y seguridad → Certificados → Preguntarle siempre**.

El TOTP no es aceptado, aunque la aplicación móvil lo muestre. - Compruebe que el reloj del teléfono y del ordenador están sincronizados (zona horaria correcta y minuto exacto). El TOTP tolera un desfase de ±30 segundos; más allá, falla. - Si el problema persiste, utilice un código de recuperación.

Tras revocar un certificado, una aplicación todavía lo acepta. - La mayoría de aplicaciones cachean la respuesta OCSP durante minutos u horas. La revocación es efectiva en el sistema de inmediato; el cliente puede tardar en reflejarla. Reinicie el cliente o limpie la caché de validación si es urgente.

Cuando solicito un certificado, el navegador descarga un fichero, pero no la clave privada. - Algunos navegadores con bloqueadores de descargas múltiples bloquean la segunda descarga. Compruebe la barra de descargas y permita la descarga del fichero `.key`. Si falla repetidamente, anule la solicitud actual e inicie una nueva con el bloqueador desactivado.

H.10 Para más información

Tema	Documento
Instalación del sistema (administradores)	Manual de Instalación
Operación interna y mantenimiento	Manual del Administrador
Detalles de la API REST (desarrolladores)	Manual de la API REST
Política de privacidad y términos	Portal SSO, sección legal

Tabla H.2. Documentos relacionados.

El presente manual cubre exclusivamente la interacción del usuario final con el sistema. Las cuestiones técnicas, operativas o de desarrollo se tratan en los manuales correspondientes referenciados en el TFG asociado.