TRABAJO FIN DE GRADO

UCAM
UNIVERSIDAD CATÓLICA
DE MURCIA

ESCUELA POLITÉCNICA SUPERIOR

Grado en Ingeniería Informática

MANUAL DE ANÁLISIS DE AMENAZAS

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 ANÁLISIS DE AMENAZAS

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 ANÁLISIS DE AMENAZAS

Matriz STRIDE completa: treinta y dos amenazas con vectores, mitigaciones y riesgo residual

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 Análisis de Amenazas
Versión	1.0
Fecha	1 junio 2026
URL pública	https://tfg.marchernandez.es/manuales/Manual_Amenazas.pdf
TFG asociado	https://tfg.marchernandez.es

Este manual conserva la numeración interna original (sección G.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.

Documento complementario referenciado en el apartado 7.9 del TFG. Contiene la matriz STRIDE completa con las treinta y dos amenazas analizadas, sus vectores, mitigaciones técnicas implementadas y la justificación del riesgo residual asumido. La memoria del TFG conserva el resumen de la tabla 7.10 y la matriz global de la figura 7.9; este manual desarrolla el análisis detallado.

G.1 Metodología y alcance

G.1.1 Taxonomía STRIDE

El análisis se organiza siguiendo la taxonomía STRIDE propuesta por Howard y LeBlanc (2003) para Microsoft, que clasifica las amenazas en seis categorías ortogonales:

Sigla	Categoría	Propiedad de seguridad atacada
S	Spoofing (suplantación)	Autenticidad
T	Tampering (manipulación)	Integridad
R	Repudiation (repudio)	No repudio y trazabilidad
I	Information disclosure (fuga)	Confidencialidad
D	Denial of service (denegación)	Disponibilidad
E	Elevation of privilege (escalada)	Autorización

Cada amenaza se identifica con un código de dos letras (`SP-`, `TA-`, `RE-`, `ID-`, `DO-`, `EP-`) y un número secuencial dentro de su categoría.

G.1.2 Criterios de clasificación

Cada amenaza recibe tres etiquetas independientes:

1. **Activo afectado**: componente, dato o servicio del sistema cuya propiedad de seguridad se ve amenazada (BD SSO, BD PKI, clave privada de CA, sesión de usuario, *token* JWT, *responder* OCSP, etc.).
2. **Vector**: superficie y mecanismo por el que el ataque podría materializarse.
3. **Estado de mitigación** tras los controles del apartado 7.8 y de las capas de defensa de la tabla 7.9:
    - **Mitigada (M)**: existen al menos dos controles independientes que reducen el riesgo a un nivel aceptable.
    - **Parcial (P)**: el sistema mitiga el vector más probable pero queda una superficie residual documentada en el apartado 8.4 (limitaciones) o en el 9.4 (líneas futuras).
    - **Residual (R)**: el sistema no puede mitigarla por completo con controles propios; se documenta explícitamente como riesgo asumido.

G.1.3 Política de impacto y probabilidad

El impacto se valora cualitativamente en tres niveles (bajo, medio, alto) según la severidad del daño potencial sobre la organización; la probabilidad se estima sobre el riesgo residual (tras aplicar mitigaciones), no sobre el riesgo bruto. La matriz de la figura 7.9 del TFG posiciona las amenazas en un cuadrante impacto × probabilidad y se reproduce en G.9.

G.1.4 Alcance del análisis

El análisis cubre la superficie de ataque del sistema integrado PKI + SSO descrita en el cuerpo del TFG: portales SSO, CA y CRL; flujo OAuth 2.0 *Authorization Code* con PKCE; emisión, verificación, revocación y publicación de certificados X.509; auditoría centralizada; tareas automatizadas (`systemd` *timers*) y copias de seguridad. Quedan fuera del alcance las amenazas físicas al *hardware*, la cadena de suministro del sistema operativo y las amenazas a la persona del administrador (coacción, *insider threat* malicioso con acceso *root*), que se asumen como contexto operativo controlado.

G.2 Tabla agregada de cobertura

La tabla G.1 reproduce y amplía la tabla 7.10 del TFG, añadiendo la lista de códigos asignados a cada categoría.

Categoría STRIDE	Analizadas	Mitigadas	Parciales	Residuales	Códigos
Spoofing	6	3	2	1	SP-01 a SP-06
Tampering	6	5	1	0	TA-01 a TA-06
Repudiation	4	3	1	0	RE-01 a RE-04

Categoría STRIDE	Analizadas	Mitigadas	Parciales	Residuales	Códigos
Information disclosure	6	4	2	0	ID-01 a ID-06
Denial of service	5	3	1	1	DO-01 a DO-05
Elevation of privilege	5	5	0	0	EP-01 a EP-05
Total	**32**	**23**	**7**	**2**	-

Tabla G.1. Cobertura agregada por categoría STRIDE con el detalle de los códigos asignados.

G.3 Spoofing: suplantación de identidad

Total: **6 amenazas** (3 mitigadas, 2 parcialmente mitigadas, 1 residual). Ataca la propiedad de autenticidad: la capacidad del sistema de asegurar que un actor es quien dice ser.

SP-01. Suplantación por contraseña débil o fugada

Campo	Valor
Activo afectado	Cuenta de usuario en `sso_users`
Vector	Diccionario, *credential stuffing* desde fugas externas, reutilización de contraseñas
Impacto / Probabilidad	Medio / Media

Campo	Valor
Mitigaciones	(a) Argon2id para *hashing* (capa 4 de la tabla 7.9); (b) política mínima de complejidad y validación con `InputValidator`; (c) segundo factor TOTP obligatorio en perfiles administrativos; (d) `RateLimiter` por IP + cuenta (capa 7); (e) auditoría de intentos fallidos en `sso_audit_log` (capa 9)
Estado	**Mitigada**
Justificación	El TOTP RFC 6238 anula la utilidad de la contraseña fugada para autenticación interactiva; el *rate limiting* impide ataques por fuerza bruta automatizada en línea.

SP-02. Phishing de credenciales SSO con TOTP

Campo	Valor
Activo afectado	Sesión SSO de un usuario legítimo
Vector	Sitio fraudulento que reproduce la pantalla de *login*, *proxy* en tiempo real (AiTM, *adversary-in-the-middle*) capaz de reenviar contraseña + TOTP al portal real antes de que expire la ventana de 30 s
Impacto / Probabilidad	Alto / Media
Mitigaciones	(a) HSTS y CSP estrictas en cabeceras (capa 8); (b) cookie de

Campo	Valor
	sesión `SameSite=Lax` y `Secure`; (c) educación del usuario y aviso visible en la pantalla de *login*; (d) método alternativo`CertificateAuth` (FNMT/DNIe) que no es phishable porque la clave privada nunca abandona la *smart card*
Estado	**Residual**
Justificación	Ningún control puramente técnico sobre TOTP RFC 6238 ofrece protección absoluta frente a un *proxy* AiTM: el atacante puede reenviar contraseña + código en tiempo real. El sistema documenta explícitamente esta limitación y ofrece `CertificateAuth` como vía preferente para operaciones críticas. Reclasificada como vía futura (WebAuthn / FIDO2) en el apartado 9.4 del TFG.

SP-03. Robo o clonación de certificado cliente

Campo	Valor
Activo afectado	Certificado X.509 cliente almacenado en perfil personal o *smart card*
Vector	Exportación del certificado con su clave privada desde un equipo sin protección, malware con acceso al

Campo	Valor
	almacén de certificados del sistema operativo
Impacto / Probabilidad	Medio / Baja
Mitigaciones	(a) Recomendación documentada de usar *smart card* con clave no exportable; (b) validación contra CRL en cada *handshake* TLS (apartado 7.7); (c) política de revocación expedita ante notificación del titular; (d) auditoría de uso del certificado en `audit_log` (capa 9)
Estado	**Parcialmente mitigada**
Justificación	Si el usuario opta por almacenamiento *software* exportable, el sistema no puede impedir la copia del fichero `.p12`. La detección a posteriori es posible vía revisión de patrones anómalos de uso en `audit_log`, pero la prevención completa requiere *smart card* o módulo TPM, que excede la decisión del propio sistema.

SP-04. Suplantación del servidor SSO (TLS strip / MITM)

Campo	Valor
Activo afectado	Confianza del cliente en el dominio del portal SSO

Campo	Valor
Vector	Punto de acceso Wi-Fi hostil, DNS *spoofing*, certificado fraudulento aceptado por el navegador
Impacto / Probabilidad	Alto / Baja
Mitigaciones	(a) Certificado TLS válido emitido por Let's Encrypt con renovación automática (capa 1); (b) HSTS con `preload` y `max-age` de un año (capa 1, capa 8); (c) CSP `upgrade-insecure-requests`; (d) ausencia total de redirección HTTP→HTTPS asumida tras la primera visita
Estado	**Mitigada**
Justificación	HSTS *preloaded* impide al navegador aceptar conexiones HTTP al dominio incluso ante DNS *spoofing*; el certificado fraudulento sería rechazado salvo compromiso de una CA del *trust store* del navegador, escenario fuera del alcance del sistema.

SP-05. Reutilización o robo de JWT firmado

Campo	Valor
Activo afectado	*Token* JWT emitido tras autorización OAuth 2.0
Vector	Captura del *bearer token* en logs, cabeceras `Referer`, *cross-site*

Campo	Valor
	scripting, almacenamiento inseguro en el cliente
Impacto / Probabilidad	Medio / Media
Mitigaciones	(a) Firma RS256 con clave privada de 4096 bits exclusiva del SSO; (b) `exp` corto (10 min para *access tokens*) y *refresh tokens* rotativos con detección de reutilización; (c) `aud` validada en cada *relying party*; (d) revocación inmediata vía `sso_tokens` con borrado en `logout` global; (e) cabeceras `Cache-Control: no-store` en las respuestas que portan *tokens*
Estado	**Parcialmente mitigada**
Justificación	La firma asimétrica impide la falsificación, pero un *token* válido capturado puede usarse hasta su expiración o revocación explícita. La rotación de *refresh tokens* con detección de reutilización limita el daño a una sola sesión activa. La adopción de DPoP (RFC 9449) para vincular el *token* al dispositivo se documenta como vía futura en el apartado 9.4 del TFG.

SP-06. Suplantación de relying party en flujo OAuth 2.0

Campo	Valor
Activo afectado	Código de autorización OAuth 2.0
Vector	Aplicación fraudulenta que se registra con un `redirect_uri` similar al de una aplicación legítima e intercepta el código tras la autorización del usuario
Impacto / Probabilidad	Medio / Baja
Mitigaciones	(a) PKCE obligatorio (RFC 7636) con `code_challenge_method=S256` para todas las *relying parties*; (b) registro centralizado en `sso_applications` con `redirect_uri` validado por coincidencia exacta, sin *wildcards*; (c) `state` obligatorio para defensa CSRF en el flujo; (d) auditoría del par `client_id` ↔ `redirect_uri` en `sso_audit_log`
Estado	**Mitigada**
Justificación	PKCE vincula criptográficamente la solicitud de autorización con el intercambio del código, anulando la utilidad de un código interceptado por un atacante sin el `code_verifier`. La validación exacta del `redirect_uri` impide la suplantación por dominios similares.

G.4 Tampering: manipulación de datos

Total: **6 amenazas** (5 mitigadas, 1 parcialmente mitigada, 0 residuales). Ataca la propiedad de integridad: la garantía de que los datos no se han modificado sin autorización.

TA-01. Manipulación de parámetros HTTP

Campo	Valor
Activo afectado	Entrada de cualquier endpoint REST o formulario
Vector	Modificación del cuerpo de la *request*, cabeceras o *query string* para forzar comportamientos no previstos
Impacto / Probabilidad	Medio / Media
Mitigaciones	(a) `InputValidator` con *whitelist* por endpoint (capa 5); (b) validación de tipo, longitud, formato y rango antes de cualquier operación; (c) rechazo explícito de campos no esperados; (d) registro del payload anómalo en `sso_audit_log`
Estado	**Mitigada**
Justificación	La validación estricta por *whitelist* en lugar de *blacklist* impide la inyección de parámetros no previstos; el rechazo de campos desconocidos elimina la superficie de mass assignment.

TA-02. Inyección SQL

Campo	Valor
Activo afectado	Bases de datos SSO y PKI
Vector	Construcción de consultas SQL por concatenación de cadenas, *blind SQL injection*, *time-based injection*
Impacto / Probabilidad	Alto / Baja
Mitigaciones	(a) PDO con *prepared statements* en todas las consultas sin excepción (capa 5); (b) `InputValidator` previo a la consulta; (c) usuario MariaDB con permisos mínimos por aplicación; (d) ModSecurity con reglas OWASP CRS en Apache (capa 1)
Estado	**Mitigada**
Justificación	El uso uniforme de *prepared statements* elimina la clase completa de vulnerabilidades por concatenación; el principio de menor privilegio en MariaDB limita el daño en caso de fallo en una capa superior.

TA-03. Cross-site scripting (XSS)

Campo	Valor
Activo afectado	Cualquier vista que renderice contenido proveniente de la BD o del usuario

Campo	Valor
Vector	Inyección de `<script>` o atributos `on*` en campos de entrada que luego se renderizan en HTML
Impacto / Probabilidad	Medio / Baja
Mitigaciones	(a) `htmlspecialchars()` con `ENT_QUOTES | ENT_HTML5` por defecto en toda salida; (b) CSP estricta con `script-src 'self'` y `nonce` por respuesta (capa 8); (c) `X-Content-Type-Options: nosniff`; (d) sanitización adicional para campos que admiten HTML (descripción de aplicaciones) con *whitelist* de etiquetas
Estado	**Mitigada**
Justificación	La combinación de escapado en plantilla y CSP por *nonce* anula tanto XSS reflejado como almacenado; el bloqueo de scripts *inline* sin `nonce` neutraliza la mayor parte de los vectores comunes.

TA-04. Cross-site request forgery (CSRF)

Campo	Valor
Activo afectado	Endpoints de mutación de estado (cambio de contraseña, emisión de certificado, revocación)
Vector	Sitio externo que provoca al navegador la ejecución de una

Campo	Valor
	petición autenticada por la cookie de sesión
Impacto / Probabilidad	Medio / Baja
Mitigaciones	(a) Token CSRF por sesión inyectado en todos los formularios y verificado en el servidor (capa 6); (b) cookie de sesión `SameSite=Lax` y `Secure`; (c) verificación de la cabecera `Origin` / `Referer` en endpoints sensibles; (d) política CSP con `frame-ancestors 'none'` para impedir *clickjacking* asociado
Estado	**Mitigada**
Justificación	El *double-submit* implícito del *token* CSRF combinado con `SameSite=Lax` impide el envío de credenciales de sesión desde orígenes terceros en operaciones de mutación.

TA-05. Manipulación de la tabla de auditoría

Campo	Valor
Activo afectado	`sso_audit_log` y `audit_log` (PKI)
Vector	Acceso *root* a MariaDB y ejecución de `UPDATE` o `DELETE` sobre las tablas de auditoría para borrar evidencias de un incidente
Impacto / Probabilidad	Medio / Baja

Campo	Valor
Mitigaciones	(a) Usuario de aplicación con permisos `INSERT` y `SELECT` sobre las tablas de auditoría, pero **sin `UPDATE` ni `DELETE`** (capa 3); (b) copia diaria cifrada GPG en servidor *off-site* (capa 9); (c) registro de comandos `mysql` con privilegios elevados en `journalctl`
Estado	**Parcialmente mitigada**
Justificación	El sistema impide la manipulación desde la aplicación, pero un atacante con privilegios `root` sobre el servidor podría operar directamente sobre MariaDB. La copia *off-site* permite la detección y reconstrucción posterior, pero no la prevención en tiempo real. La adopción de un *append-only log* con firma encadenada (estilo *transparency log*) se documenta como vía futura en el apartado 9.4.

TA-06. Manipulación de cookies de sesión

Campo	Valor
Activo afectado	Cookie de sesión PHP del portal SSO
Vector	Modificación del valor de la cookie por el cliente, *session fixation*
Impacto / Probabilidad	Medio / Baja
Mitigaciones	(a) Identificador de sesión de 256 bits generado por `random_bytes()`; (b)

Campo	Valor
	atributos `HttpOnly`, `Secure`, `SameSite=Lax`; (c) regeneración del ID de sesión en *login* exitoso y al cambiar de privilegio; (d) expiración por inactividad y absoluta; (e) almacenamiento server-side en `sso_sessions`
Estado	**Mitigada**
Justificación	El espacio de identificadores (2^256) impide adivinación; `HttpOnly` impide el robo por XSS; la regeneración en *login* anula `session fixation`; el almacenamiento *server-side* permite revocación inmediata por logout global.

G.5 Repudiation: repudio de acciones

Total: **4 amenazas** (3 mitigadas, 1 parcialmente mitigada, 0 residuales). Ataca la propiedad de no repudio: la imposibilidad de que un actor niegue haber realizado una acción.

RE-01. Repudio de emisión de certificado

Campo	Valor
Activo afectado	Certificados X.509 emitidos por las CAs
Vector	Usuario que niega haber solicitado un certificado posteriormente cuestionado
Impacto / Probabilidad	Alto / Baja

Campo	Valor
Mitigaciones	(a) Registro en `audit_log` del PKI con: identidad autenticada del solicitante, *hash* SHA-256 de la CSR, perfil aplicado, *timestamp*, IP de origen; (b) almacenamiento de la CSR original en BD; (c) firma del registro de emisión por la CA con marca temporal; (d) trazabilidad del operador que aprueba la emisión cuando aplica
Estado	**Mitigada**
Justificación	La cadena identidad SSO → registro de CSR → certificado firmado → marca temporal constituye evidencia técnica suficiente para imputar la solicitud al usuario autenticado.

RE-02. Repudio de acción administrativa

Campo	Valor
Activo afectado	Cualquier operación de administrador: alta de aplicación, cambio de `access_mode`, revocación, asignación de rol
Vector	Administrador que niega haber realizado una operación crítica
Impacto / Probabilidad	Medio / Baja
Mitigaciones	(a) Registro nominal en `sso_audit_log` con `user_id`, acción, recurso, *timestamp*, IP, *user agent*; (b)

Campo	Valor
	trazabilidad del cambio de estado en la entidad afectada (campos `created_by`, `updated_by`, `revoked_by`); (c) política de cuentas administrativas individuales (sin cuentas compartidas); (d) alerta Telegram en acciones críticas
Estado	**Mitigada**
Justificación	La política de cuentas individuales combinada con el registro nominal impide el repudio salvo en el escenario de credenciales robadas, ya cubierto por SP-01 y SP-02.

RE-03. Borrado o manipulación de logs

Campo	Valor
Activo afectado	`sso_audit_log`, `audit_log`, `journalctl`
Vector	Atacante con privilegios suficientes que borra registros de su actividad
Impacto / Probabilidad	Medio / Baja
Mitigaciones	(a) Cuenta de aplicación sin permisos `DELETE`/`UPDATE` sobre las tablas de auditoría (capa 3); (b) copia diaria cifrada GPG *off-site* (capa 9); (c) `journalctl` con rotación firmada por systemd; (d) alerta Telegram ante operaciones de borrado masivo

Campo	Valor
Estado	**Parcialmente mitigada**
Justificación	Igual que TA-05, el sistema impide el borrado desde la aplicación, pero no desde acceso *root* directo. La detección a posteriori por comparación con la copia *off-site* es posible, pero la prevención completa requiere un *append-only log* externo (vía futura, apartado 9.4 del TFG).

RE-04. Repudio de inicio de sesión

Campo	Valor
Activo afectado	Sesión SSO de un usuario
Vector	Usuario que niega haber iniciado sesión desde un dispositivo concreto
Impacto / Probabilidad	Bajo / Baja
Mitigaciones	(a) Registro de cada inicio de sesión exitoso en `sso_audit_log` con `user_id`, método de autenticación (`password`+`totp` o `certificate`), IP, *user agent*, *timestamp*; (b) panel de "sesiones activas" visible al usuario; (c) notificación opcional por correo en accesos desde IPs no vistas previamente
Estado	**Mitigada**
Justificación	La constancia de los metadatos del *login* en combinación con el método

Campo	Valor
	de autenticación empleado (especialmente certificado cliente) constituye evidencia técnica suficiente.

G.6 Information disclosure: fuga de información

Total: **6 amenazas** (4 mitigadas, 2 parcialmente mitigadas, 0 residuales). Ataca la propiedad de confidencialidad: la garantía de que la información solo es accesible para actores autorizados.

ID-01. Fuga de contraseñas en BD

Campo	Valor
Activo afectado	Hashes de contraseñas en `sso_users.password_hash`
Vector	*Dump* de BD por inyección SQL, copia de seguridad mal protegida, compromiso del servidor
Impacto / Probabilidad	Alto / Baja
Mitigaciones	(a) Argon2id con `memory_cost=65536`, `time_cost=4`, `parallelism=2` y `salt` aleatorio de 16 bytes por contraseña (capa 4); (b) copias de seguridad cifradas con GPG (clave del administrador); (c) ausencia total de almacenamiento en claro o reversible; (d) parámetros revisables anualmente para acompañar la mejora del *hardware* atacante
Estado	**Mitigada**

Campo	Valor
Justificación	Argon2id es el algoritmo recomendado por OWASP para *password hashing*: la combinación de coste en memoria y CPU hace inviable el *cracking* masivo incluso con GPU/ASIC en el horizonte temporal del sistema.

ID-02. Exposición de claves privadas de CA

Campo	Valor
Activo afectado	Ficheros `ca-key.pem` de las CAs Root e Intermedias
Vector	Acceso al sistema de ficheros del servidor, *backup* mal protegido, robo de la *passphrase* maestra
Impacto / Probabilidad	Alto / Baja
Mitigaciones	(a) Cifrado jerárquico de *passphrases* con AES-256-CBC: una *passphrase* aleatoria por CA, cifrada con la *passphrase* maestra del `.env` (capa 4, apartado 7.4.4); (b) ficheros de clave con permisos `0600` y propiedad del usuario PHP-FPM; (c) la *passphrase* maestra no se almacena en BD, solo en `.env` con permisos `0600`; (d) copia de seguridad en GPG con clave externa al servidor; (e) auditoría de acceso a `pki/ca/` en `journalctl`

Campo	Valor
Estado	**Parcialmente mitigada**
Justificación	El sistema implementa cifrado en reposo robusto, pero un compromiso simultáneo del servidor que dé acceso al `.env` y a los ficheros cifrados anula la barrera criptográfica. La adopción de un HSM (Hardware Security Module) o TPM que custodie la clave maestra fuera del sistema de ficheros se documenta como vía futura prioritaria en el apartado 9.4 del TFG.

ID-03. Fuga de información por mensajes de error

Campo	Valor
Activo afectado	Cualquier endpoint REST o vista que muestre errores
Vector	Mensaje detallado de excepción mostrado al cliente, *stack trace* en producción, *banner* del *backend*
Impacto / Probabilidad	Bajo / Media
Mitigaciones	(a) `display_errors=Off` en `php.ini` de producción; (b) capa de manejo de errores que devuelve mensajes genéricos al cliente y vuelca el detalle a `php-fpm error_log`; (c) cabecera `Server` minimizada en Apache; (d) eliminación de cabeceras `X-Powered-By`

Campo	Valor
Estado	**Mitigada**
Justificación	La política de mensajes genéricos al cliente elimina la fuga de información de la pila tecnológica y de la estructura interna.

ID-04. Token JWT o refresh expuesto

Campo	Valor
Activo afectado	*Access tokens* y *refresh tokens* en tránsito o almacenamiento
Vector	Captura en `Referer`, registro accidental en logs, almacenamiento en `localStorage` accesible por XSS, transmisión sobre HTTP
Impacto / Probabilidad	Medio / Media
Mitigaciones	(a) Transmisión exclusiva sobre TLS 1.3 (capa 1); (b) cabeceras `Cache-Control: no-store` en respuestas que portan *tokens*; (c) política recomendada de almacenamiento en cookie `HttpOnly` `Secure` `SameSite=Strict` para *refresh tokens*; (d) ausencia de *tokens* en `query string` (`Authorization: Bearer` en cabecera); (e) filtro de *logs* para que el `Authorization` no quede registrado
Estado	**Parcialmente mitigada**

Campo	Valor
Justificación	El sistema impide la fuga por canales que controla (transporte, logs, *query string*), pero la decisión final sobre dónde almacena el cliente el *token* queda fuera del control del servidor. La transición a DPoP (RFC 9449) o a *tokens* vinculados al dispositivo se documenta como vía futura en el apartado 9.4 del TFG.

ID-05. Lectura no autorizada de directorios sensibles

Campo	Valor
Activo afectado	`pki/ca/`, `vendor/`, `.env`, ficheros de configuración
Vector	*Path traversal*, configuración incorrecta de Apache que expone directorios bajo `DocumentRoot`, `Indexes` activo
Impacto / Probabilidad	Alto / Baja
Mitigaciones	(a) Estructura de directorios con `pki/`, `vendor/` y `.env` fuera de `DocumentRoot`; (b) `Options -Indexes` global en Apache; (c) reglas `<DirectoryMatch>` que bloquean acceso a `.env`, `.git`, `*.log`; (d) `InputValidator` con rechazo de `..` y secuencias de codificación URL en parámetros de ruta; (e) ModSecurity con reglas OWASP CRS contra *path traversal* (capa 1)

Campo	Valor
Estado	**Mitigada**
Justificación	La estructura física del despliegue impide el acceso por URL a los directorios sensibles incluso ante un fallo en una capa superior; las reglas de Apache añaden defensa redundante.

ID-06. Inferencia por enumeración

Campo	Valor
Activo afectado	Existencia de cuentas de usuario, certificados, aplicaciones registradas
Vector	Mensajes diferentes según el usuario exista o no, tiempos de respuesta distintos, presencia o ausencia de recursos por ID secuencial
Impacto / Probabilidad	Bajo / Media
Mitigaciones	(a) Mensajes de error uniformes en login (`Credenciales inválidas`, sin distinguir usuario inexistente de contraseña errónea); (b) *timing* uniforme: se ejecuta el hashing Argon2id incluso si el usuario no existe; (c) identificadores de aplicación y certificado **no** secuenciales (UUID v4); (d) `RateLimiter` que limita peticiones por IP y endpoint

Campo	Valor
Estado	**Mitigada**
Justificación	La uniformidad de mensaje y de *timing* elimina los canales laterales habituales de enumeración; los UUIDs impiden la inferencia por contadores.

G.7 Denial of service: denegación de servicio

Total: **5 amenazas** (3 mitigadas, 1 parcialmente mitigada, 1 residual). Ataca la propiedad de disponibilidad: la capacidad del sistema de responder a peticiones legítimas dentro del SLA acordado.

DO-01. Brute force de credenciales

Campo	Valor
Activo afectado	Portales SSO de *login* y endpoints `/api/auth/*`
Vector	Peticiones masivas de *login* contra una cuenta para adivinar la contraseña o agotar la cuenta de TOTP
Impacto / Probabilidad	Medio / Media
Mitigaciones	(a) `RateLimiter` con ventanas progresivas por IP + cuenta (capa 7); (b) bloqueo temporal de la cuenta tras N fallos consecutivos; (c) `fail2ban` con reglas sobre `sso_audit_log` y `apache access_log` (capa 1); (d) CAPTCHA opcional tras umbral; (e) alerta Telegram sobre ráfagas anómalas

Campo	Valor
Estado	**Mitigada**
Justificación	La combinación de *rate limiting* en aplicación, bloqueo temporal de cuenta y `fail2ban` a nivel de red eleva el coste del ataque a niveles inviables sin botnet, escenario cubierto por DO-05.

DO-02. Inundación de consultas OCSP

Campo	Valor
Activo afectado	*Responder* OCSP del PKI
Vector	Cliente o botnet que solicita validación de un mismo certificado o de cientos miles aleatorios para agotar el *responder*
Impacto / Probabilidad	Medio / Media
Mitigaciones	(a) `RateLimiter` específico para el endpoint OCSP; (b) caché de respuestas pre-firmadas por número de serie con expiración configurable; (c) registro selectivo en `ocsp_queries` (solo consultas distintas) para evitar inflar la BD; (d) métricas en `ocsp_queries` para detección reactiva
Estado	**Parcialmente mitigada**
Justificación	La caché pre-firmada limita el coste por consulta, pero un volumen suficiente sigue pudiendo saturar el

Campo	Valor
	responder. La mitigación completa requiere CDN o *anycast*, lo que excede la arquitectura de un único VPS. Documentada como vía futura en el apartado 9.4 del TFG.

DO-03. Agotamiento de conexiones a BD

Campo	Valor
Activo afectado	MariaDB (servicio compartido por SSO y PKI)
Vector	Apertura masiva de sesiones sin cerrar, consultas largas que monopolizan el *pool* de conexiones
Impacto / Probabilidad	Medio / Baja
Mitigaciones	(a) Pool de conexiones con límite configurado en `php-fpm` (`pm.max_children`); (b) `max_connections` configurado en MariaDB con margen sobre la carga máxima esperada; (c) `wait_timeout` corto para sesiones inactivas; (d) cierre explícito de PDO al final de la petición; (e) MariaDB sobre Unix socket local que reduce *overhead* y aísla del tráfico de red (capa 1)
Estado	**Mitigada**
Justificación	Los límites configurados aíslan el impacto: en el peor caso, una ráfaga

Campo	Valor
	agota el *pool* de PHP-FPM sin afectar a MariaDB, y los procesos se reciclan.

DO-04. Subida masiva de CSRs

Campo	Valor
Activo afectado	Endpoint de emisión de certificados, espacio en disco, CPU
Vector	Generación automatizada de CSRs por un usuario autenticado para saturar el sistema o llenar el disco
Impacto / Probabilidad	Bajo / Baja
Mitigaciones	(a) `RateLimiter` específico por usuario para emisión (e.g. máximo N por hora); (b) cuota de certificados activos por usuario y por perfil; (c) auditoría detallada en `audit_log`; (d) alerta Telegram ante ráfagas; (e) cuotas de disco a nivel de sistema operativo sobre el directorio de operación
Estado	**Mitigada**
Justificación	La cuota por usuario y el *rate limiting* hacen económicamente inviable el ataque desde cuentas legítimas; cualquier ráfaga deja huella en `audit_log` y dispara la alerta.

DO-05. DoS volumétrico de red

Campo	Valor
Activo afectado	Conectividad del VPS hacia Internet
Vector	Botnet que satura el ancho de banda del proveedor IaaS con tráfico legítimo o reflejo de protocolos (DNS, NTP, SSDP)
Impacto / Probabilidad	Alto / Baja
Mitigaciones	(a) Mitigación contractual con el proveedor IaaS (filtro *upstream* básico contra tráfico claramente anómalo); (b) `fail2ban` para IPs con patrones agresivos (capa 1); (c) plan de comunicación con el proveedor ante incidente
Estado	**Residual**
Justificación	Ningún control del propio sistema puede mitigar un DoS volumétrico que supere el ancho de banda contratado. La mitigación completa requiere protección *upstream* del proveedor o un servicio especializado (CDN con *anycast*, *scrubbing center*), cuya adopción se documenta en el apartado 9.4 del TFG como mejora futura dependiente de la criticidad alcanzada por el sistema.

G.8 Elevation of privilege: escalada de privilegios

Total: **5 amenazas** (5 mitigadas, 0 parciales, 0 residuales). Ataca la propiedad de autorización: la garantía de que un actor solo puede realizar acciones acordes a su rol.

EP-01. Escalada por manipulación de `role` en BD

Campo	Valor
Activo afectado	Campo `role` en `sso_users`
Vector	Inyección SQL o acceso directo a la BD para promover una cuenta a `admin`
Impacto / Probabilidad	Alto / Baja
Mitigaciones	(a) PDO *prepared statements* (mitiga inyección SQL, ver TA-02); (b) usuario MariaDB de la aplicación sin permisos sobre la columna `role` (solo el script de administración con cuenta separada puede modificarla); (c) auditoría de cambios de rol con `sso_audit_log` y alerta Telegram; (d) verificación del rol en cada petición sobre el lado del servidor, sin confiar en la sesión del cliente
Estado	**Mitigada**
Justificación	La política de permisos en MariaDB impide la promoción salvo desde la cuenta administrativa; los cambios quedan registrados y notifican al administrador en tiempo real.

EP-02. Bypass de chequeo RBAC en endpoint

Campo	Valor
Activo afectado	Cualquier endpoint que dependa del rol del actor
Vector	Programador que olvida la verificación de rol en un endpoint nuevo, *insecure direct object reference* (IDOR) sobre identificadores predecibles
Impacto / Probabilidad	Medio / Baja
Mitigaciones	(a) Patrón de capa de autorización centralizada (un *middleware* obligatorio antes del despacho a la lógica de negocio); (b) tests de integración por endpoint en el plan de pruebas (apartado 8.3 del TFG) que ejecutan cada acción con un actor sin rol y verifican que se rechaza; (c) revisión por pares en *commits* que añaden endpoints; (d) auditoría de accesos denegados
Estado	**Mitigada**
Justificación	El *middleware* centralizado convierte la omisión en error de configuración inmediato; los tests de integración detectan regresiones antes del despliegue.

EP-03. Cambio no autorizado de `access_mode` de aplicación

Campo	Valor
Activo afectado	`sso_applications.access_mode` (controla qué usuarios pueden acceder a una RP)
Vector	Administrador o usuario con rol intermedio que cambia el modo de acceso a `public` para una aplicación restringida
Impacto / Probabilidad	Medio / Baja
Mitigaciones	(a) Permiso de modificación de `access_mode` restringido a `admin` global, no a propietarios de aplicación; (b) auditoría detallada de cada cambio con valor anterior y nuevo en `sso_audit_log`; (c) alerta Telegram ante transición `restricted → public`; (d) revisión periódica del catálogo de aplicaciones
Estado	**Mitigada**
Justificación	La separación entre rol de propietario de aplicación y rol de administrador global impide el cambio unilateral; la alerta automática asegura visibilidad inmediata.

EP-04. Reutilización de sesión administrativa

Campo	Valor
Activo afectado	Sesión activa de un administrador

Campo	Valor
Vector	Sesión administrativa olvidada sin cerrar en un equipo compartido o tomado por un atacante
Impacto / Probabilidad	Medio / Baja
Mitigaciones	(a) Expiración corta por inactividad para sesiones de administrador (frente a sesiones de usuario regular); (b) re-autenticación con TOTP requerida para acciones críticas (revocación de CAs, cambio de permisos); (c) panel de "sesiones activas" con capacidad de cierre remoto; (d) cierre global de todas las sesiones del usuario en `logout`
Estado	**Mitigada**
Justificación	La política de re-autenticación para acciones críticas anula la utilidad de una sesión administrativa olvidada para el peor caso (escalada destructiva); la expiración por inactividad cierra la ventana de oportunidad.

EP-05. Carga arbitraria de configuración OpenSSL

Campo	Valor
Activo afectado	Proceso de emisión de certificados
Vector	Usuario que controla parámetros de la CSR o del perfil para forzar la

Campo	Valor
	inclusión de extensiones no autorizadas (`basicConstraints CA:TRUE`, EKU privilegiada)
Impacto / Probabilidad	Alto / Baja
Mitigaciones	(a) Plantillas OpenSSL estáticas por perfil, no editables por usuario (anexo F del TFG); (b) extensiones X.509 v3 fijadas en la plantilla, no derivadas de la CSR; (c) validación del perfil contra `sso_application_profile_bindings` antes de la firma (apartado 7.4.6); (d) auditoría del par perfil-CSR en `audit_log`
Estado	**Mitigada**
Justificación	Las plantillas estáticas y la validación servidor-side del perfil impiden que el solicitante influya en las extensiones críticas del certificado emitido.

G.9 Conclusiones del análisis

G.9.1 Síntesis cuantitativa

De las 32 amenazas identificadas siguiendo la taxonomía STRIDE:

- **23 (72 %) se consideran mitigadas**: cuentan con al menos dos controles independientes y el riesgo residual es despreciable en el contexto operativo del sistema.
- **7 (22 %) se consideran parcialmente mitigadas**: el sistema mitiga el vector más probable, pero queda una superficie residual documentada que se traslada al apartado 8.4 (limitaciones del despliegue) o al apartado

9.4 del TFG (líneas futuras): SP-03, SP-05, TA-05, RE-03, ID-02, ID-04 y DO-02.

- **2 (6 %) se consideran riesgo residual asumido**: SP-02 (*phishing* avanzado sobre TOTP) y DO-05 (DoS volumétrico de red). En ambos casos, ningún control puramente técnico bajo decisión del proyecto puede mitigarlas por completo.

G.9.2 Reproducción de la matriz de riesgo residual

La figura G.1 reproduce y amplía la figura 7.9 del TFG con la posición cualitativa de las amenazas representativas tras aplicar las mitigaciones:

Amenaza	Categoría	Probabilidad residual	Impacto	Cuadrante
SP-02 *Phishing* AiTM sobre TOTP	Spoofing	Media	Alto	Crítico
SP-03 Certificado cliente robado	Spoofing	Baja	Medio	Improbable
SP-05 Robo de JWT	Spoofing	Media	Medio	Latente
TA-05 Manipulación de auditoría	Tampering	Baja	Medio	Improbable
RE-03 Borrado de logs	Repudiation	Baja	Medio	Improbable

Amenaza	Categoría	Probabilidad residual	Impacto	Cuadrante
ID-02 Claves privadas de CA	Information disclosure	Muy baja	Alto	Improbable pero costoso
ID-04 *Token leak*	Information disclosure	Media	Medio	Latente
DO-02 Inundación OCSP	Denial of service	Media	Medio	Latente
DO-05 DoS volumétrico de red	Denial of service	Media	Alto	Crítico

Tabla G.2. Posicionamiento cualitativo de las amenazas con mayor riesgo residual.

G.9.3 Conclusiones por categoría

Spoofing. La mitigación es robusta para los vectores controlables por el sistema (contraseña, MITM, JWT, RP). El riesgo residual se concentra en el *phishing* avanzado (SP-02), inherente a cualquier sistema que dependa de un segundo factor basado en código de un solo uso; el sistema documenta `CertificateAuth` como vía preferente y la migración a WebAuthn como vía futura.

Tampering. Es la categoría con mejor cobertura técnica: cinco de seis amenazas plenamente mitigadas con controles canónicos (PDO, CSP, CSRF tokens, `HttpOnly`). La única parcial (TA-05) atañe a la integridad de los logs frente a un atacante con privilegios *root*, escenario que requiere un *append-only log* externo para mitigación completa.

Repudiation. El registro nominal en `sso_audit_log` combinado con la política de cuentas individuales asegura no repudio en operaciones administrativas y de

emisión. La amenaza parcial (RE-03) coincide con TA-05 en su naturaleza (privilegio *root* sobre BD) y comparte la vía futura recomendada.

Information disclosure. Las mitigaciones cubren los vectores habituales (BD, mensajes de error, *path traversal*, enumeración). Las dos parciales (ID-02 claves CA, ID-04 *token leak*) corresponden a riesgos cuya mitigación completa requiere componentes externos al alcance actual del proyecto: HSM/TPM para custodiar la clave maestra (ID-02) y DPoP o *tokens* vinculados al dispositivo (ID-04). Ambas se reclasifican como prioridades para la siguiente iteración.

Denial of service. Las mitigaciones aplicación-céntricas (rate limiting, caché OCSP, *pool* de conexiones, cuotas) cubren los vectores controlables. El residual (DO-05) y la parcial (DO-02) comparten naturaleza volumétrica y dependen de infraestructura *upstream* (proveedor IaaS, CDN *anycast*), externa al sistema.

Elevation of privilege. Es la categoría con cobertura más completa: cinco mitigadas, ninguna parcial. La combinación de RBAC centralizado, plantillas estáticas, separación de permisos en BD y auditoría sobre cambios de rol elimina las vías razonables de escalada bajo el modelo de amenazas considerado.

G.9.4 Trazabilidad con las limitaciones y vías futuras del TFG

Amenaza	Estado	Documentada en
SP-02 *Phishing* AiTM	Residual	TFG apartado 9.4 (WebAuthn / FIDO2)
SP-03 Cert. cliente robado	Parcial	TFG apartado 8.4 (limitación de almacenamiento *software*)
SP-05 Robo de JWT	Parcial	TFG apartado 9.4 (DPoP, RFC 9449)
TA-05 Manipulación auditoría	Parcial	TFG apartado 9.4 (*append-only log*)

Amenaza	Estado	Documentada en
RE-03 Borrado de logs	Parcial	TFG apartado 9.4 (*append-only log*)
ID-02 Claves CA	Parcial	TFG apartado 9.4 (HSM / TPM)
ID-04 *Token leak*	Parcial	TFG apartado 9.4 (DPoP, RFC 9449)
DO-02 Inundación OCSP	Parcial	TFG apartado 9.4 (CDN *anycast*)
DO-05 DoS volumétrico	Residual	TFG apartado 9.4 (CDN *anycast*)

Tabla G.3. Trazabilidad de cada amenaza con riesgo no totalmente mitigado hacia los apartados de limitaciones y vías futuras del TFG.

G.9.5 Cierre

El análisis confirma que el sistema integrado PKI + SSO mitiga la mayor parte de las amenazas STRIDE relevantes para su contexto operativo y que los riesgos residuales restantes están documentados de forma explícita, trazables a controles concretos y referidos al plan de evolución del sistema. Ninguna amenaza queda en el cuadrante de probabilidad alta e impacto alto tras aplicar las mitigaciones, y las dos amenazas residuales (SP-02 y DO-05) se sitúan fuera del alcance técnico mitigable por el propio sistema, lo que constituye una declaración explícita y trazable del perímetro de seguridad técnicamente mitigable por el propio sistema.