MI TICKET · UBIKUA · SEGURIDAD

Informe de seguridad y cumplimiento ENS

Generado: 05/11/2026 03:30 · Entorno: Local y produccion · Alcance: Auditoria automatica de codigo, configuracion y superficie HTTP de Mi Ticket. Entornos: local y production. Comprobaciones no destructivas.

Estado global: **Con observaciones** · Riesgo: medio

COMPROBACIONES	CORRECTAS	AVISOS	CRITICAS
37	**32**	**5**	**0**

Cumplimiento ENS BASICO: 70 %

15 medidas revisadas. El porcentaje cuenta solo las medidas en estado "cumple".

Resumen ejecutivo

Este informe público resume el estado de seguridad de Mi Ticket y las medidas de cumplimiento ENS revisadas en la última auditoría. Los detalles técnicos y las evidencias sensibles se mantienen en el informe interno.

Comprobaciones

Comprobacion	Estado	Detalle
Directorios internos protegidos por .htaccess	**OK**	
Carpeta security/ bloqueada por HTTP	**OK**	
Secretos fuera del repositorio	**OK**	
Funciones peligrosas en src/	**OK**	
Consultas SQL construidas con interpolacion	**OK**	
Cookies de sesion	**OK**	
Hash de contrasenas	**OK**	
Proteccion CSRF global	**OK**	
Dependencias PHP fijadas	**OK**	
Registro de actividad de la aplicacion	**OK**	
Copias de seguridad verificables	**Aviso**	
Fichero security.txt	**OK**	
Disponibilidad de la portada	**OK**	
Formulario de acceso	**OK**	
Token CSRF en login	**OK**	

Comprobacion	Estado	Detalle
Rechazo de POST sin CSRF	**OK**	
Pagina publica de seguridad	**OK**	
Pagina de cumplimiento ENS	**OK**	
Cabeceras HTTP de seguridad	**OK**	
Politica CSP	**Aviso**	
Banner del servidor	**Aviso**	
Flags de cookie de sesion	**OK**	
Exposicion de ficheros internos	**OK**	
Disponibilidad de la portada	**OK**	
Formulario de acceso	**OK**	
Token CSRF en login	**OK**	
Rechazo de POST sin CSRF	**OK**	
Pagina publica de seguridad	**OK**	
Pagina de cumplimiento ENS	**OK**	
Cabeceras HTTP de seguridad	**OK**	
Politica CSP	**Aviso**	
HSTS (produccion)	**Aviso**	
Banner del servidor	**OK**	
Flags de cookie de sesion	**OK**	
Exposicion de ficheros internos	**OK**	
Redireccion HTTP a HTTPS (produccion)	**OK**	
Certificado TLS (produccion)	**OK**	

Hallazgos y recomendaciones

Severidad	Hallazgo	Detalle y recomendación
Medio	Copias de seguridad verificables	**Recomendación:** Configura y prueba copias de base de datos y ficheros.
Medio	Sin politica de seguridad de contenido (CSP)	**Recomendación:** Define una CSP compatible con los assets locales y sin scripts inline innecesarios.
Bajo	Banner del servidor (Local)	**Recomendación:** Minimiza la version del servidor en la configuracion web.

Severidad	Hallazgo	Detalle y recomendación
Medio	HSTS no configurado	**Recomendación:** Activa HSTS cuando el certificado TLS sea valido y estable.

Medidas ENS

Código	Medida	Estado	Evidencia
org.1	Politica de seguridad y responsabilidades	**parcial**	Roles separados y documentacion en docs/; falta aprobacion formal anual.
op.acc.1	Control de acceso a la aplicacion	**cumple**	Middleware de autenticacion y autorizacion por rol en routes.php.
op.acc.2	Gestion de usuarios y permisos	**cumple**	Altas, bajas y roles por organizacion; sesiones por usuario.
op.acc.4	Contrasenas y autenticacion	**cumple**	password_hash/password_verify y recuperacion con token.
op.acc.5	Proteccion frente a ataques de autenticacion	**parcial**	Rate limiting en login, registro y escaneo; sin MFA.
op.exp.2	Configuracion segura	**parcial**	HTTPS forzado y cabeceras parciales; certificado de produccion pendiente.
op.exp.4	Actualizaciones y dependencias	**parcial**	composer.lock presente; auditoria de dependencias pendiente de automatizar.
op.exp.7	Registro de actividad	**cumple**	Registro de errores y actividad de aplicacion en storage/logs.
op.mon.1	Deteccion y registro de incidentes	**parcial**	Alertas basicas y revision periodica; sin SIEM.
op.cont.1	Continuidad del servicio	**parcial**	Control de acceso offline en PWA; plan de continuidad no formalizado.
op.cont.3	Copias de seguridad	**parcial**	Procedimiento local; falta verificar copia externa y restauracion.
mp.info.1	Proteccion de datos personales	**cumple**	Minimizacion, consentimiento, baja RGPD y aislamiento por organizacion.
mp.info.4	Cifrado de informacion	**parcial**	TLS en produccion dependiente de certificado valido; datos en reposo sin cifrado adicional.
mp.si.2	Integridad de entradas	**cumple**	Firma HMAC-SHA256 de QR y validacion de estado en servidor.
mp.com.1	Perimetro y exposicion de servicios	**parcial**	Directorios internos protegidos; revisar CSP y hardening del servidor.

Alcance y limitaciones

Auditoria automatica de codigo, configuracion y superficie HTTP de Mi Ticket. Entornos: local y production. Comprobaciones no destructivas.

Este documento refleja controles técnicos y organizativos revisados automáticamente y mediante revisión manual. No constituye una certificación oficial del ENS ni sustituye una auditoría de conformidad independiente. Para el informe interno completo, accede al panel de superadministración.
