Checklist de cumplimiento de seguridad web

OWASP · PCI DSS · ISO 27001 · GDPR/RGPD · NIS2 — guía práctica para freelancers y agencias

---

Esta checklist ayuda a revisar, sitio por sitio, los puntos técnicos que más piden auditores y clientes al hablar de cumplimiento normativo. No sustituye asesoría legal ni una auditoría certificada — es una guía práctica para priorizar antes de esa auditoría.

1. OWASP — Configuración y hardening

Cubre control de acceso roto (A01) y errores de configuración de seguridad (A05) del OWASP Top 10.

- ■ Cabeceras presentes: HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Permissions-Policy, Referrer-Policy.
- ■ Cipher suites TLS actualizadas, sin versiones obsoletas de TLS.
- ■ Paneles administrativos (/wp-admin, phpMyAdmin) no accesibles sin protección adicional.
- ■ Sin archivos sensibles expuestos: backups, .env, configuraciones de servidor.
- ■ Redirects HTTP→HTTPS correctos, sin mixed content.

2. PCI DSS v4.0 — si procesas pagos

Aplica a cualquier negocio que procese, almacene o transmita datos de tarjetas.

- ■ Escaneo de vulnerabilidades interno y externo cada 3 meses (Requisito 11.2).
- ■ Escaneo tras cualquier cambio significativo de infraestructura.
- ■ Documentación de cada escaneo: fecha, hallazgos, puntuación.

NOTA: un escáner como IntGuard es complementario — no sustituye el escaneo ASV trimestral oficial exigido a comercios nivel 1-4.

3. ISO/IEC 27001:2022

Evidencia de medidas técnicas apropiadas para un Sistema de Gestión de Seguridad de la Información (SGSI).

- ■ Registro periódico y documentado de escaneos de vulnerabilidades.
- ■ Proceso definido de respuesta ante hallazgos críticos.
- ■ Evidencia exportable (PDF/CSV) para auditoría interna o externa.

4. GDPR / RGPD

Medidas técnicas y organizativas apropiadas (art. 32) para proteger datos personales.

- ■ Cifrado en tránsito (TLS) verificado en todos los subdominios activos.
- ■ Proceso de notificación de brechas definido (art. 33-34, plazo 72h).
- ■ DPA (Acuerdo de Encargado de Tratamiento) firmado con proveedores relevantes.

5. NIS2

Aplica a operadores de servicios esenciales e importantes en la UE (alcance ampliado respecto a NIS1).

- ■ Gestión de riesgos de ciberseguridad documentada.
- ■ Escaneo y monitorización continua de la superficie expuesta.

■ Plan de respuesta a incidentes con roles y plazos definidos.
