AEGIS PYME

CYBERSECURITY INTELLIGENCE

Evaluación de seguridad digital

Informe ejecutivo y técnico preliminar

DOMINIO EVALUADO	empresa-ficticia.example
ESTADO DE EVALUACIÓN	Completado
FORMATO DEL INFORME JSON	1.2
DISEÑO DEL PDF	1.4
FECHA DE GENERACIÓN	13/11/2026 18:47
CONCLUSIÓN DE SEGURIDAD	No determinada

Documento preliminar automatizado. La finalización de las comprobaciones no certifica la seguridad de la empresa.

01 | Resumen ejecutivo

Las comprobaciones solicitadas finalizaron.

AEGIS PYME ha procesado 4 modulos de evaluacion para empresa-ficticia.example. Se han registrado 6 observaciones de configuracion. Estas observaciones no constituyen vulnerabilidades confirmadas.

El resultado describe las comprobaciones realizadas y sus limitaciones. No certifica que la organizacion sea segura.

4	0	6
MÓDULOS COMPLETADOS	MÓDULOS PARCIALES	OBSERVACIONES

Índice ACI orientativo: C · 64/100

Hay vías de ataque baratas que conviene cerrar.

Vía de ataque más barata observada: Acceder a la base de datos expuesta a internet (coste para el atacante: trivial).

Reglas ACI aci-1.0-preliminar, pendientes de calibrar con pilotos. Índice orientativo de exposición basado en información pública. No es una certificación ni una conclusión de seguridad.

02 | Alcance y cobertura

La cobertura describe qué módulos fueron solicitados y cuáles pudieron ejecutarse. No representa el porcentaje de seguridad.

Seguridad web	Completado
Seguridad del correo	Completado
Exposición externa	Completado
Servicios expuestos	Completado

03 | Observaciones técnicas

03.1 — Cabecera HSTS no observada

La respuesta HTTPS examinada no incluia la cabecera HSTS. Su conveniencia debe evaluarse segun la arquitectura del servicio.

Prioridad de revisión: Revisión ordinaria

Identificador: web:HSTS_NOT_OBSERVED

Observación preliminar; no es una vulnerabilidad confirmada.

Evidencia registrada

header	Strict-Transport-Security
observed	False
url	https://empresa-ficticia.example/

03.2 — El certificado de la web caduca en 12 dias

Si no se renueva a tiempo, los navegadores mostraran el aviso de sitio no seguro. Conviene confirmar la renovacion automatica.

Prioridad de revisión: Revisión recomendada

Identificador: web:CERT_EXPIRING_SOON

Observación preliminar; no es una vulnerabilidad confirmada.

Evidencia registrada

certificate_expiry	Nov 24 23:59:59 2026 GMT
days_left	12

03.3 — La web publica el software y la version que utiliza

Conocer la version exacta permite buscar en segundos fallos conocidos de ese software. No confirma que existan.

Prioridad de revisión: Revisión recomendada

Identificador: web:SOFTWARE_VERSION_DISCLOSED

Observación preliminar; no es una vulnerabilidad confirmada.

Evidencia registrada

disclosed	["Server: Apache/2.4.41 (Ubuntu)", "X-Powered-By: PHP/7.4.3"]

03.4 — Faltan protecciones basicas del navegador

La respuesta no activa varias cabeceras que dificultan ataques contra los visitantes de la web.

Prioridad de revisión: Revisión ordinaria

Identificador: web:BROWSER_PROTECTIONS_MISSING

Observación preliminar; no es una vulnerabilidad confirmada.

Evidencia registrada

not_observed	["Content-Security-Policy", "X-Content-Type-Options"]
url	https://empresa-ficticia.example/

03.5 — DMARC solo en modo observacion (p=none)

La politica DMARC existe pero no pide bloquear los mensajes que suplantan el dominio; solo genera informes.

Prioridad de revisión: Revisión recomendada

Identificador: email:DMARC_POLICY_NONE

Observación preliminar; no es una vulnerabilidad confirmada.

Evidencia registrada

dmarc	v=DMARC1; p=none; rua=mailto:dmarc@empresa-ficticia.example

03.6 — Base de datos accesible desde internet

Un servicio de base de datos responde desde internet. Si la autenticacion es debil o no existe, los datos quedan al alcance de cualquiera.

Prioridad de revisión: Revisión recomendada

Identificador: services:DATABASE_EXPOSED

Observación preliminar; no es una vulnerabilidad confirmada.

Evidencia registrada

exposed	[{"ip": "198.51.100.20", "port": 3306, "service": "MySQL"}]
source	InternetDB (Shodan)

04 | Plan de recomendaciones

04.1 — Evaluar la implantacion de HSTS

Revisar si procede habilitar HSTS. Comprobar primero la disponibilidad HTTPS y el impacto sobre subdominios. No activar includeSubDomains o preload sin validar sus consecuencias.

Motivo: HSTS puede ayudar a reducir conexiones HTTP posteriores en navegadores compatibles.

Observación de referencia: web:HSTS_NOT_OBSERVED

Validar con personal responsable antes de aplicar cambios.

04.2 — Confirmar la renovacion del certificado

Comprobar con el proveedor web que la renovacion automatica esta activa.

Motivo: Un certificado caducado muestra avisos de seguridad a todos los visitantes.

Observación de referencia: web:CERT_EXPIRING_SOON

Validar con personal responsable antes de aplicar cambios.

04.3 — Ocultar versiones y mantener el software actualizado

Revisar que el software indicado este actualizado y configurar el servidor para no publicar la version.

Motivo: Publicar la version facilita localizar fallos conocidos.

Observación de referencia: web:SOFTWARE_VERSION_DISCLOSED

Validar con personal responsable antes de aplicar cambios.

04.4 — Activar las cabeceras de seguridad del navegador

Valorar con el proveedor web Content-Security-Policy, X-Content-Type-Options y X-Frame-Options, probando antes su efecto.

Motivo: Son protecciones gratuitas para los visitantes de la web.

Observación de referencia: web:BROWSER_PROTECTIONS_MISSING

Validar con personal responsable antes de aplicar cambios.

04.5 — Avanzar la politica DMARC

Revisar los informes DMARC y, cuando el correo legitimo pase los controles, cambiar a p=quarantine y despues a p=reject.

Motivo: Con p=none los correos que suplantan el dominio no se bloquean.

Observación de referencia: email:DMARC_POLICY_NONE

Validar con personal responsable antes de aplicar cambios.

04.6 — Retirar la base de datos de internet

Limitar el acceso a la base de datos a la red interna o a IP concretas y revisar su autenticacion.

Motivo: Una base de datos accesible desde internet expone directamente los datos.

Observación de referencia: services:DATABASE_EXPOSED

Validar con personal responsable antes de aplicar cambios.

05 | Metodología y límites

AEGIS PYME realiza una evaluación automatizada preliminar sobre las comprobaciones solicitadas. Las conclusiones se limitan a la evidencia obtenida durante esta ejecución.

- Informe de EJEMPLO generado con datos ficticios para mostrar el formato del informe AEGIS.
- Evaluacion preliminar automatizada, no auditoria integral.
- Las observaciones no son vulnerabilidades confirmadas.
- La huella SHA-256 no demuestra autenticidad ni autoria.

06 | Integridad documental

El informe JSON original incorpora una huella SHA-256. Esta permite comprobar la coherencia del contenido con su huella almacenada, pero no acredita la autoría del documento.

Huella SHA-256 del JSON:

abf10d62f2adfa077d9ad3dc57f176d2

195ba82f99cfaed60a90ebba12042c58

Esta huella corresponde al contenido del informe JSON, no al archivo PDF. No constituye firma digital ni acredita identidad del emisor.