**YOORshop SAS**

RCS 817 466 147 — 254 Rue Vendôme, 69003 Lyon, France — yoorhosting.com

`[datos de la empresa por completar]`

**Ref. informe:** YH-DEMO-2026-01
**Fecha de auditoría:** 27 de octubre de 2026

**CONFORME Y SEGURO**

**INFORME DE INGENIERÍA DE SEGURIDAD E INTEGRIDAD • ENTREGABLE N.º 1**

# Auditoría de seguridad de un sitio web

Control de integridad del núcleo PrestaShop, detección de malware, hermetismo de secretos y auditoría de módulos.

**CLIENTE DESTINATARIO**

**Sociedad:** SARL Moto Pièces Express (Ficticio)
**Plataforma objetivo:** https://boutique-moto.example (PrestaShop 8.2.3)
**Servidor host:** srv-demo.yoorhosting.com (PHP 8.1 FPM / MariaDB)
**Alcance:** 28 274 archivos analizados • 90 módulos instalados

**INTEGRIDAD NÚCLEO PRESTASHOP**
**23 770**
20 126 idénticos · 9 adaptaciones revisadas

**BÚSQUEDA DE MALWARE**
**0 archivos**
Ninguna webshell ni script sospechoso

**MÓDULOS TERCEROS AUDITADOS**
**90 módulos**
0 fallos críticos explotables

**PROTECCIÓN DE SECRETOS**
**100 % hermético**
parameters.php, .env, .git en 403/404

**SOLICITUD DEL CLIENTE**

«Con motivo de la preparación de las campañas comerciales de fin de año y tras alertas de seguridad en el sector del comercio electrónico, la gerencia solicitó una **auditoría de integridad completa e independiente** de la tienda `boutique-moto.example`. Los objetivos fijados fueron garantizar la ausencia total de puertas traseras (webshells), verificar la estricta conformidad del núcleo PrestaShop 8.2.3, asegurar la inaccesibilidad pública de los datos sensibles y controlar las vulnerabilidades de los módulos de terceros instalados.»

**CONCLUSIÓN EJECUTIVA**

**No se ha identificado ninguna vulnerabilidad crítica explotable de forma inmediata en su tienda.** El código de PrestaShop es estrictamente conforme a la huella oficial, los permisos de archivos respetan las recomendaciones (directorios 755, archivos 644), no se encontró ningún archivo malicioso y ningún dato sensible es accesible desde Internet.

## 1 Cuadro exhaustivo de controles de integridad

| ÁMBITO DE CONTROL | METODOLOGÍA Y HERRAMIENTAS DESPLEGADAS | RESULTADO Y CONSTATACIÓN |
|---|---|---|
| **Integridad del núcleo PrestaShop** | Comparación hash SHA-256 de cada archivo con la huella oficial de PrestaShop 8.2.3 (23 770 archivos de referencia). | **Conforme** 20 126 archivos idénticos; 9 adaptaciones de negocio revisadas (albaranes, cálculos). |
| **Búsqueda de archivos maliciosos** | Escaneo de firmas de webshell (código oculto, evaluación dinámica, ejecución remota) en todo el sitio. | **Limpio** Ningún archivo malicioso detectado en el alojamiento. |
| **Carpetas de subida (upload, img)** | Búsqueda de scripts PHP ejecutables en `/img/`, `/upload/`, `/download/`. | **Protegido** Ningún script; reglas `.htaccess` de bloqueo activas. |
| **Permisos de archivos** | Inventario completo de propietario y permisos comparado con las normas de PrestaShop. | **Conforme** Carpetas 755, archivos 644, ningún archivo modificable por terceros. |
| **Archivos de configuración y secretos** | Intentos de acceso HTTP desde Internet a `parameters.php`, `settings.inc.php`, `.env`, `.git` y copias. | **Inaccesible** Todos bloqueados (respuestas HTTP 403 Forbidden o 404 Not Found). |
| **Secretos en el código fuente** | Análisis automático profundo (gitleaks) sobre 28 274 archivos. | **Hermético** Claves de módulos en archivos PHP no legibles desde Internet. |
| **Módulos instalados (90)** | Cruce de cada versión con bases de vulnerabilidades (Friends of Presta, NVD, OpenCVE). | **Actualizado** Ningún módulo en versión vulnerable explotable (Monetico, Checkout OK). |

## 2 Puntos de vigilancia a medio plazo (sin acción urgente)

Estos elementos no son explotables hoy dada la estructura del código y los controladores activos; deben integrarse durante el próximo mantenimiento programado:

| COMPONENTE Y VERSIÓN | AVISO PÚBLICO / CVE | ANÁLISIS DE IMPACTO Y POR QUÉ NO SUPONE RIESGO HOY |
|---|---|---|
| **Twig 3.4.3** | CVE-2026-46633 | Requiere un nombre de plantilla proporcionado por el atacante: ningún uso de este tipo en el código. |
| **PhpSpreadsheet 1.19.0** | CVE-2026-45034<br>CVE-2026-34084 | Requiere un archivo elegido por el atacante: la función afectada nunca se invoca en la tienda. |
| **Smarty 4.3.4** | CVE-2024-35226 | Requiere una plantilla controlada por el atacante: solo se ejecutan las plantillas del tema oficial. |
| **Módulo psgdpr 1.4.3** | CVE-2026-92809 (gravedad media) | Un cliente conectado podría añadir un registro falso de consentimiento; ningún dato leído ni modificado; parche pendiente. |
| **Archivos de instalación en raíz** | Documentación residual | Archivos `INSTALL.txt`, `Makefile`, página de instalación: documentación sin datos sensibles, a retirar por higiene. |

## 3 Metodología de investigación y pruebas de aislamiento

### CONTROL DE AISLAMIENTO POSIX

Todos los directorios están bloqueados en `0755` y los scripts PHP en `0644` bajo el UID aislado `motodemo`. El servidor web opera bajo una cuenta sin privilegios y sin permisos de escritura sobre el núcleo aplicativo.

### PROTECCIÓN WAF Y SONDAS HTTP

Las peticiones de prueba dirigidas a `/.git/config`, `/app/config/parameters.php` y `/vendor/` devolvieron estados de bloqueo herméticos **403 Forbidden** aplicados en la pasarela frontal Nginx.

## 4 Recomendaciones y calendario de mantenimiento

**RECOMENDACIÓN ESTRATÉGICA: CICLO REGULAR DE ACTUALIZACIÓN**

No se requiere ninguna acción correctiva de urgencia. El sitio puede afrontar las campañas comerciales con total seguridad. Recomendamos planificar la actualización a la última versión PrestaShop 8.2.x en la próxima ventana de mantenimiento, que integra de forma nativa las bibliotecas Twig y PhpSpreadsheet corregidas.

**Visado técnico de validación:**
Departamento de Seguridad de los Sistemas de Información (CISO) — YOORshop SAS

✓ **Informe Certificado Conforme**