

ALERTA

CIBERSEGURIDAD Y DATOS PERSONALES

Fallas críticas en PHP: cada día sin actualizar debilita tu *defensa* *legal*.

PHP opera casi 7 de cada 10 sitios web, incluido todo WordPress. Dos fallas críticas ya se explotan.

01 · QUÉ PASÓ

Tres fallas en *cuatro días*.

CRÍTICA · CVSS 9.2

EN EXPLOTACIÓN

PHP2Shell

CVE-2026-109618 · CVE-2026-109619

Corregida el 21 de octubre en PHP 8.5.12, 8.4.27, 8.3.36 y 8.2.35.

PHP 8.1 y anteriores no recibirán corrección: hay que migrar.

ACOTADA · 23 DE OCTUBRE

SIN PARCHE

CVE-2026-115560

Sin corrección hasta la próxima versión regular. Se bloquea a nivel servidor con

```
session.upload_progress.enabled=0
```

02 · EL RIESGO

Sin actualizar, un atacante *puede:*

01 Entrar sin contraseña

Ejecutar su propio código en tu servidor.

02 Leer tus bases de datos

Expedientes de clientes, datos de empleados y contraseñas almacenadas.

03 Quedarse *dentro*

Dejar accesos ocultos que siguen activos después de actualizar.

04 Usar tu sitio contra otros

Infectar a tus visitantes, tumbar tu sitio o atacar a terceros desde tu servidor.

03 · TU EXPOSICIÓN LEGAL · LFPDPPP

Si la corrección es gratuita y está disponible,
no aplicarla es *difícil de justificar*.

Deber de seguridad (art. 18): medidas acordes con el riesgo y el desarrollo tecnológico.

MULTA DE HASTA

\$37.5
millones de pesos

320,000 UMA por vulnerar la seguridad de tus bases de datos, cuando te sea imputable (arts. 58, fr. XI, y 59).

×2

con datos sensibles

+

multa adicional si la infracción persiste

Además de la *multa*:

Verificación de oficio

ART. 54

La Secretaría Anticorrupción y Buen Gobierno puede iniciarla si presume fundadamente una violación a la ley.

Aviso inmediato a titulares

ART. 19

Si la vulneración afecta de forma significativa sus derechos patrimoniales o morales.

Indemnización

ART. 53

Las personas afectadas pueden reclamar los daños.

Responsabilidad civil o penal

ART. 61

Las sanciones administrativas no la excluyen.

Qué hacer *esta semana*

1 Confirma por escrito

Pide a quien administra tus servidores que confirme que actualizó PHP (o migró a 8.2 o superior) y aplicó el cambio de configuración.

2 Conserva las bitácoras

Solicita que se revisen y conserven desde el 17 de octubre, fecha del primer intento de explotación detectado.

3 Evalúa el aviso a titulares

Si hay indicios de acceso no autorizado, decide de inmediato si debes notificarlos.

4 Documenta cada paso

Ese registro es tu evidencia de diligencia.

¿Necesitas evaluar tu exposición
o revisar tus contratos con
proveedores?

cyber@lipp.legal

