PUDAZ

Informe de cierre de rescate
Entregado el 30 de septiembre de 2026

Ejemplo. El negocio, el sitio y los datos son de ejemplo. Es el formato del informe que entregamos al terminar un rescate.

Rescate de sitio WordPress

Tu sitio está limpio y la puerta por donde entraron, cerrada.

Te entregamos www.ejemplo.test funcionando el miércoles 30 de septiembre a las 16:00, dentro del plazo de 1 a 2 días hábiles. Abajo está el detalle del trabajo y lo que te recomendamos para que no se repita.

NEGOCIO	SITIO	SERVICIO	ENTREGA
Hostal Los Coigües de ejemplo	www.ejemplo.test WordPress	Rescate de sitio WordPress $89.990 + IVA, precio fijo	30-09-2026, 16:00 Equipo Pudaz

1 Qué pasó

El lunes 28 de septiembre nos escribiste porque, al buscar el hostal en Google desde el celular, el sitio llevaba a una página de apuestas. Desde el computador se veía normal, y además habían dejado de llegar consultas por el formulario.

1. **Lun 28-09, 11:20** — Nos escribes por el formulario.
2. **Lun 28-09, 16:00** — Diagnóstico gratis desde afuera. El caso calza con el precio fijo.
3. **Mar 29-09, 10:30** — Pago confirmado y accesos funcionando. Ahí empieza el plazo.
4. **Mié 30-09, 16:00** — Te entregamos el sitio limpio y este informe.

2 Qué encontramos

1. **La vía de entrada.** Un plugin de galería que llevaba 19 meses sin actualizar. Esa versión tenía una falla conocida que permitía subir archivos sin iniciar sesión, y por ahí entraron el 21 de septiembre.
2. **Archivos y código maliciosos.** 11 archivos escondidos en la carpeta de imágenes y código agregado al final de 2 archivos del tema.
3. **Dos administradores desconocidos.** "soporte-wp" y "admin2", creados el mismo 21 de septiembre.
4. **1.240 páginas falsas de apuestas** en la base de datos, y Google alcanzó a mostrar 312 en sus resultados. La redirección solo se activaba en visitas que llegaban desde Google en el celular. Por eso, al entrar directo, todo se veía normal.
5. **Respaldos que no servían.** El hosting guardaba 7 días de respaldos y todos eran posteriores al 21 de septiembre, así que ya venían infectados.

3 Qué hicimos

- Antes de tocar nada, guardamos un respaldo completo del sitio tal como estaba.
- Borramos los 11 archivos maliciosos y sacamos el código agregado al tema.
- Reinstalamos WordPress y los plugins desde sus copias oficiales.
- Limpiamos la base de datos. Borramos las 1.240 páginas falsas y 2 tareas programadas que volvían a crear los archivos.
- Eliminamos los 2 administradores desconocidos y cerramos todas las sesiones abiertas.
- Cambiamos la galería vulnerable por la que trae WordPress. Los 6 álbumes de fotos quedaron iguales.
- Bloqueamos la ejecución de programas en la carpeta de imágenes.
- Pedimos a Google, desde Search Console, que revise el sitio y saque las páginas falsas de sus resultados. Cuándo responde depende de Google.
- Al final pasamos dos escáneres de malware, y ninguno encontró nada.

4 Qué cambiamos

QUÉ	ANTES	AHORA
WordPress	6.4.3	7.0.3
Tema del sitio	3.9.4	4.12.4
Plugins	12, de ellos 7 desactualizados	10, todos al día. Sacamos la galería y uno que estaba desactivado.
Administradores	4, dos desconocidos	2, los que reconoces
Contraseñas de WordPress y de la base de datos	Las mismas desde 2023	Nuevas. Las tuyas te las mandamos por un enlace seguro.
Claves de seguridad del sitio	Las de la instalación original	Nuevas
Programas en la carpeta de imágenes	Se podían ejecutar	Bloqueados
PHP del servidor	7.4	7.4, sin cambio (ver recomendación 2)

5 Respaldo entregado

Archivo. ejemplo-test-limpio-2026-09-30.zip

Contenido. Archivos del sitio (612 MB) y base de datos (38 MB), ya limpios, del 30-09 a las 15:10.

Dónde está. Guardado fuera del servidor. El 30-09 te mandamos el enlace de descarga por correo. Bájalo y guárdalo en tu computador o en tu nube.

Si algo vuelve a fallar, este es el punto limpio desde donde partir.

6 Garantía

Garantía: 30 días hábiles sobre lo reparado.

Corre desde la entrega, del 30 de septiembre al jueves 12 de noviembre de 2026 (de lunes a viernes, sin feriados). Si el mismo problema vuelve por la misma causa, lo corregimos sin costo.

No cubre una falla con otra causa (por ejemplo, una falla nueva en otro plugin), lo que se instale o cambie después sin coordinarlo con nosotros, las recomendaciones críticas que no se sigan ni las fallas del proveedor de hosting. El detalle está en pudaz.cl/terminos/.

7 Recomendaciones

1 Cambia la clave del hosting y la del correo — Crítica, esta semana

Nosotros cambiamos las de WordPress y la base de datos. Las del panel del hosting y del correo no las tenemos, y conviene cambiarlas por precaución.

2 **Pide a tu hosting pasar a PHP 8.3** — Este mes

Tu sitio funciona con PHP 7.4, que no recibe parches de seguridad desde noviembre de 2022. Tu plan de hosting no nos deja cambiarlo desde el panel, así que hay que pedirlo al soporte del proveedor. Si quieres, te dejamos el mensaje escrito.

3 **Activa la verificación en dos pasos** — Este mes

En WordPress, para los dos administradores. Así, una clave robada no basta para entrar.

4 **Mantén los plugins al día** — Siempre

Todo partió por un plugin que pasó 19 meses sin actualizar. Puedes hacerlo tú cada semana o dejárnoslo con el Plan Sitio ($49.990 + IVA al mes).

Equipo Pudaz
contacto@pudaz.cl

Si tienes dudas sobre este informe, escríbenos a contacto@pudaz.cl. Te respondemos en 1 día hábil.