NEXO VIRTUAL

Checklist de emergencia

Web WordPress hackeada: qué revisar antes de tocar nada

Marca cada punto y evita errores que pueden empeorar la recuperación.

Dominio: _____ Fecha del incidente: _____

Antes de tocar nada

No borres archivos sin copia, no restaures cualquier backup y no pidas revisión a Google hasta comprobar que la web está limpia.

1. Contener el problema

- ☐ Poner la web en mantenimiento si muestra malware, redirecciónes o errores extraños.
- ☐ Evitar que usuarios o clientes sigan navegando por una web comprometida.
- ☐ No seguir haciendo cambios directamente sobre la web infectada en producción.
- ☐ Avisar al hosting si ha detectado malware, bloqueo o consumo anormal.

2. Hacer copia antes de tocar nada

- ☐ Guardar una copia completa de los archivos.
- ☐ Exportar la base de datos.
- ☐ Conservar wp-config.php y .htaccess.
- ☐ Guardar wp-content completo: plugins, tema, uploads y mu-plugins si existe.
- ☐ Descargar logs del servidor si están disponibles.

3. Revisar accesos

- ☐ Comprobar todos los usuarios administradores de WordPress.
- ☐ Cambiar la contraseña del hosting o panel de control.
- ☐ Cambiar o eliminar accesos FTP/SFTP antiguos.
- ☐ Cambiar contraseña de base de datos si hay sospecha de compromiso.
- ☐ Revisar correos asociados y accesos de proveedores o colaboradores.

4. Buscar señales de infección

- ☐ Redirecciones a páginas raras, casinos, descargas o dominios desconocidos.
- ☐ Archivos PHP sospechosos dentro de wp-content/uploads.
- ☐ Usuarios administradores desconocidos o creados recientemente.
- ☐ Plugins vulnerables, abandonados, desactivados pero aun instalados.
- ☐ URLs extrañas indexadas en Google con site:tudominio.com.
- ☐ Avisos en Search Console sobre problemas de seguridad.

5. Recuperar y proteger

- [ ] Restaurar una copia limpia solo si es anterior al hackeo.
- [ ] Actualizar WordPress, tema, constructor visual y plugins.
- [ ] Eliminar plugins y temas innecesarios o abandonados.
- [ ] Regenerar las claves SALT de WordPress para cerrar sesiones antiguas.
- [ ] Instalar o configurar seguridad después de limpiar, no como único remedio.
- [ ] Comprobar que no quedan redirecciónes, páginas spam ni errores críticos.

6. Revisar Google y el SEO

- [ ] Comprobar Search Console y la sección de problemas de seguridad.
- [ ] Usar Inspeccion de URL en home, servicios, categorias, productos y páginas clave.
- [ ] Solicitar revisión solo cuando la web este realmente limpia.
- [ ] Valorar retirada temporal de URLs spam si aparecen resultados peligrosos.
- [ ] Volver a pedir indexación de las páginas importantes cuando proceda.

7. Si es una tienda WooCommerce

- [ ] Pausar pedidos si hay riesgo en checkout, redirecciónes o pagos.
- [ ] Revisar pasarelas de pago, claves API y cuentas conectadas.
- [ ] Comprobar pedidos recientes, usuarios, cupones y correos automáticos.
- [ ] Revisar productos, enlaces, precios, métodos de envio y métodos de pago.
- [ ] No volver a vender hasta verificar que el proceso de compra es seguro.

8. Cuando pedir ayuda profesional

- [ ] Si la web genera ventas, leads o contactos importantes.
- [ ] Si Google muestra aviso de sitio peligroso.
- [ ] Si el malware vuelve después de limpiarlo.
- [ ] Si hay muchas URLs raras en Google.
- [ ] Si no sabes diferenciar archivos legítimos de archivos sospechosos.

Consejo final

Que la web vuelva a cargar no significa que el problema esté resuelto. Revisa por dónde pudo entrar el ataque y deja la instalación más protegida que antes.

¿Tu web WordPress está hackeada? Podemos ayudarte a revisarla y recuperarla con seguridad.
nexovirtual.net · info@nexovirtual.net

Recurso creado por Nexo Virtual para usuarios y empresas con webs WordPress.