tinary

GUÍA · CUANDO ALGO FALLA

Qué hacer si hackearon tu sitio

Los primeros pasos para contener el daño: aislar el sitio, guardar evidencia, cambiar accesos y avisar a quien corresponde.

GUÍA · 20 MIN DE LECTURA

Descubrir que tu sitio fue atacado genera urgencia, y la urgencia empuja a borrar, reinstalar y seguir como si nada. Es la reacción más común y también la que más complica las cosas: se pierde la evidencia, el atacante conserva su acceso y el problema vuelve a las pocas semanas.

Esta guía ordena lo que conviene hacer en las primeras horas y en los días siguientes. Está pensada para sitios web, tiendas en línea y aplicaciones de empresas, y sirve aunque no tengas equipo técnico propio. Si lo tienes, compártela con él: el orden de los pasos importa tanto como cada paso.

Cómo saber si tu sitio fue hackeado

Algunos ataques son evidentes, como una portada cambiada. La mayoría no: el atacante prefiere pasar inadvertido para seguir usando tu sitio el mayor tiempo posible. Estas son las señales más frecuentes:

- Aparecen páginas, enlaces o productos que nadie de tu equipo creó, muchas veces sobre apuestas, medicamentos o préstamos.
- El sitio redirige a otras páginas, a veces solo cuando se entra desde un celular o desde un resultado de Google. Por eso puede que tú no lo veas al escribir la dirección directamente.
- El navegador o Google muestran advertencias como «Este sitio puede haber sido hackeado» o una pantalla roja de sitio peligroso.
- Hay usuarios administradores que no reconoces, o cambiaron los permisos de usuarios existentes.
- Tu proveedor de hosting suspendió la cuenta o te avisó de archivos maliciosos, envío masivo de correos o consumo anormal de recursos.
- Los correos de tu dominio empiezan a llegar a spam o a ser rechazados, porque tu servidor quedó en listas de bloqueo.
- Tus clientes reportan cobros que no reconocen, correos extraños a tu nombre o un formulario de pago distinto al habitual.

- El sitio está más lento, se cae seguido o aparecen archivos con nombres extraños o fechas de modificación que nadie explica.
- Recibes un mensaje que exige un pago a cambio de devolverte el acceso o de no publicar tus datos.

Una sola señal no confirma un ataque, pero si ves una, actúa como si lo fuera hasta descartarlo. Revisar cuesta mucho menos que dejar pasar días.

Antes de tocar nada: cuatro reglas

1. **No borres nada todavía.** Los archivos modificados, los usuarios creados por el atacante y los registros del servidor son la única forma de saber cómo entró y qué se llevó. Si los eliminas, pierdes esa respuesta.
2. **No restaures una copia de respaldo encima del sitio atacado.** Primero guarda una copia del estado actual. Después decide qué restaurar.
3. **Trabaja desde un equipo de confianza.** Si el ataque partió de una contraseña robada, el computador desde el que administras el sitio podría estar infectado. Cambia las claves desde otro equipo, actualizado y con antivirus al día.
4. **Revisa si ya corre un plazo legal.** Si tu empresa presta servicios esenciales o fue calificada como operador de importancia vital, la Ley 21.663 te da 3 horas desde que tomas conocimiento del incidente para enviar una alerta temprana a la Agencia Nacional de Ciberseguridad (ANCI). Ese aviso no puede esperar a que termine la investigación.

Además, designa a una persona a cargo de coordinar y abre una bitácora: un documento simple donde se anote la fecha y hora de cada cosa que se observa y de cada acción que se toma, y quién la hizo. Parece un detalle, pero en un incidente es lo que evita repetir trabajo, contradecirse con los clientes y perder plazos.

CUÁNDO LLAMAR A ESPECIALISTAS DESDE EL INICIO

Esta guía te sirve para dar los primeros pasos. Hay situaciones, sin embargo, en las que conviene sumar a un equipo especializado desde la primera hora, porque un error al comienzo no se puede deshacer después:

- Tu sitio procesa pagos o guarda datos personales de clientes.
- No sabes cómo entró el atacante, o el problema vuelve después de limpiarlo.
- Hay más de un sistema afectado: correo, servidores, CRM, ERP o cuentas en la nube.
- Recibiste una extorsión o una exigencia de pago.
- Tu empresa debe reportar a la ANCI o a la Agencia de Protección de Datos Personales.
- Necesitas evidencia que sirva para una denuncia, un juicio o un reclamo a tu seguro.

En cualquiera de estos casos, escríbenos a **contacto@tinary.cl**. Tomamos el caso contigo: contenemos el daño, preservamos la evidencia y nos hacemos cargo de la investigación mientras tú sigues atendiendo tu negocio.

PASO 1

Aislar el sitio

El objetivo es cortar el daño sin destruir la evidencia. Aislar no es borrar.

- Pon el sitio en modo mantenimiento o reemplaza la portada por una página simple que avise de una interrupción temporal. Si no puedes hacerlo, pide a tu proveedor de hosting que suspenda el sitio sin eliminar archivos ni bases de datos.
- Si es una tienda, desactiva el pago en línea mientras investigas. Un formulario de pago alterado puede estar copiando las tarjetas de tus clientes en este mismo momento.
- Restringe el acceso al panel de administración, por ejemplo solo desde la dirección de tu oficina, o desactívalo temporalmente.
- Pausa las integraciones que conectan el sitio con otros sistemas: CRM, ERP, inventario, automatizaciones y webhooks. Si el atacante tiene acceso al sitio, puede tener acceso a todo lo que el sitio toca.
- Si el sitio comparte servidor con otros sitios o sistemas de tu empresa, avisa a quien los administra: pueden estar expuestos por el mismo camino.
- Evita apagar o reinstalar el servidor si puedes. Hay información que solo existe mientras está encendido, como los procesos en ejecución y las conexiones activas. Si tienes un servidor propio o en la nube, una copia instantánea del disco (snapshot) antes de cualquier cambio es la mejor forma de conservarla.

PASO 2

Guardar evidencia

La evidencia sirve para tres cosas: entender cómo entró el atacante, saber qué datos fueron afectados y respaldar una denuncia, un reclamo a tu seguro o un reporte a una autoridad. Guárdala antes de limpiar.

- **Copia completa de los archivos del sitio y de la base de datos, tal como están.** Guárdala fuera del servidor afectado, en un lugar con acceso restringido, y anota la fecha y hora en que la hiciste.
- **Registros del servidor (logs).** Pide a tu hosting los registros de acceso y de error del servidor web, los accesos por FTP o SFTP, los accesos al panel del hosting y los registros de correo. Hazlo el primer día: muchos proveedores conservan los registros solo por algunos días.
- **Registros de otras plataformas.** Si usas un servicio de protección o distribución como Cloudflare, un firewall de aplicaciones o un plugin de seguridad, descarga sus eventos del período.
- **Lista de usuarios** del panel de administración, con sus permisos y fechas de creación.
- **Capturas de pantalla** de lo que se ve: páginas alteradas, advertencias, mensajes de extorsión, correos sospechosos. Que se vean la dirección, la fecha y la hora.
- **Mensajes recibidos**: avisos del hosting, de Google, de clientes o del banco. Guarda los originales, no solo un reenvío.
- **Cronología**: cuándo se notó el primer síntoma, quién lo notó y qué cambios se hicieron al sitio en las semanas anteriores, como actualizaciones, plugins nuevos, cambios de proveedor o accesos entregados a terceros.

No abras ni ejecutes archivos sospechosos para ver qué hacen, y no reenvíes el material a personas que no participan en la respuesta: la evidencia puede contener datos personales de tus clientes.

ANÁLISIS FORENSE

Si el caso puede terminar en una denuncia, un juicio o un reclamo a tu seguro, la evidencia tiene que recogerse de forma que nadie pueda cuestionarla: copias verificables con su huella digital (hash), registro de quién la tuvo y cuándo (cadena de custodia) y análisis sobre copias, nunca sobre el original.

Ese es el trabajo de un análisis forense, y es una de las formas en que te ayudamos: reconstruimos qué pasó, cómo entró el atacante, desde cuándo estaba dentro, qué hizo y qué información tocó. Todo queda documentado en un informe que sirve ante tu seguro, la Fiscalía o una autoridad.

PASO 3

Cambiar accesos

Si el atacante obtuvo una contraseña, limpiar el sitio no sirve de nada: volverá a entrar por la misma puerta. Cambia todos los accesos relacionados, en este orden y desde un equipo de confianza:

1. **Correo electrónico** de las personas que administran el sitio, el dominio y el hosting. Va primero porque la recuperación de todas las demás contraseñas llega al correo.
2. **Dominio y DNS**: la cuenta donde registraste el dominio (NIC Chile, si es un dominio .cl) y la del servicio que administra tus DNS. Quien controla el DNS decide hacia dónde van tu sitio y tu correo.
3. **Hosting o nube**: el panel del proveedor y los accesos por SSH, FTP o SFTP. Elimina las cuentas FTP que no uses.
4. **Base de datos**: cambia la contraseña y actualízala en la configuración del sitio.
5. **Panel de administración del sitio** (WordPress, WooCommerce, Shopify u otro): todos los usuarios, no solo el tuyo. Elimina las cuentas que no reconozcas, después de dejarlas registradas en la evidencia. En WordPress, cambia también las claves secretas del archivo de configuración (wp-config.php): así se cierran todas las sesiones abiertas.
6. **Pagos e integraciones**: pasarela de pago, claves de API, tokens de acceso y webhooks de tu CRM, ERP, plataforma de correo masivo y automatizaciones. Genera claves nuevas y anula las anteriores.
7. **Accesos de terceros**: agencias, desarrolladores y proveedores. Si alguien externo tenía acceso, es el momento de revisar si todavía lo necesita.

En cada acceso, usa una contraseña nueva, larga y única, guardada en un gestor de contraseñas; activa la verificación en dos pasos donde exista y cierra las sesiones abiertas. Si la misma contraseña se usaba en otros servicios, cámbiala también allí.

PASO 4

Avisar a quien corresponde

Avisar a tiempo protege a tus clientes, te permite cumplir la ley y te deja en mejor posición. Callar suele salir más caro: los clientes terminan enterándose por otro lado. A quién avisar depende de lo que pasó.

A QUIÉN	CUÁNDO Y PARA QUÉ
Dirección y equipo interno	Siempre. Incluye al área legal si existe y a quien desarrolla y mantiene el sitio. Define una sola persona que hable hacia afuera, para que no circulen versiones distintas.
Proveedor de hosting	Siempre. Puede entregar registros, aislar el sitio y revisar si otros clientes del mismo servidor fueron afectados.
Banco o procesador de pagos	Si el sitio procesa pagos y se sospecha que se alteró el formulario de pago o se robaron datos de tarjetas. Pueden bloquear operaciones y avisar a los bancos emisores.
Compañía de seguros	Si tienes una póliza de ciberriesgos. Avísale antes de contratar ayuda externa: muchas pólizas exigen aviso inmediato y trabajar con proveedores aprobados.
Agencia Nacional de Ciberseguridad (ANCI)	Obligatorio para quienes prestan servicios esenciales y para los operadores de importancia vital (Ley 21.663), cuando el incidente puede tener efectos significativos. Si tu empresa no está en esas categorías, igual puedes informar el incidente al CSIRT Nacional; ayuda a advertir a otras organizaciones.
Agencia de Protección de Datos Personales	Ley 21.719, vigente desde el 1 de diciembre de 2026. Si el ataque provocó la destrucción, filtración, pérdida o alteración de datos personales y existe un riesgo razonable para las personas afectadas.
Personas afectadas	Obligatorio cuando la filtración involucra datos sensibles, como los de salud, datos de niños y niñas menores de 14 años, o datos económicos, financieros, bancarios o comerciales (Ley 21.719). Aunque no estés obligado, avisar a tus clientes para que cambien su contraseña o revisen sus cobros es lo correcto.
PDI o Fiscalía	Para denunciar el delito. La Ley 21.459 sanciona, entre otros, el acceso ilícito a sistemas, la interceptación, el ataque a la integridad de los datos y el fraude informático. La PDI cuenta con una brigada especializada en cibercrimen. La denuncia suele ser necesaria para reclamos al banco o al seguro.

Los plazos de la Ley 21.663

Si tu empresa está obligada a reportar a la ANCI, estos son los plazos, contados desde que tomas conocimiento del incidente:

REPORTE	PLAZO
Alerta temprana	Dentro de 3 horas.
Segundo reporte, con la información actualizada	Dentro de 72 horas. Si eres operador de importancia vital y el incidente afecta la prestación de tu servicio esencial, dentro de 24 horas.
Plan de acción	Solo operadores de importancia vital: dentro de 7 días corridos.
Informe final	Dentro de 15 días corridos.

La Ley 21.719, por su parte, pide reportar a la Agencia de Protección de Datos Personales «por los medios más expeditos posibles y sin dilaciones indebidas». En la práctica, eso significa apenas tengas información suficiente, sin esperar a cerrar la investigación.

Cómo avisar a tus clientes

Di lo que sabes, lo que todavía no sabes y lo que estás haciendo. No minimices ni especules: si después descubres que el alcance fue mayor, una primera comunicación que restó importancia al problema te quitará credibilidad. Este modelo sirve como punto de partida:

Asunto: Información importante sobre la seguridad de tus datos en `[EMPRESA]`

Estimado/a `[NOMBRE]`,

El `[FECHA]` detectamos un acceso no autorizado a `[nuestro sitio web / nuestra tienda en línea]`. Apenas lo supimos, aislamos el sitio, cambiamos los accesos y comenzamos una investigación con especialistas en ciberseguridad.

Según lo que sabemos hasta ahora, la información que podría haberse visto afectada es: `[DATOS AFECTADOS: por ejemplo, nombre, correo, dirección e historial de compras]`.

`[Si corresponde: Los datos de tarjetas de pago no se almacenan en nuestro sitio.]`

Te recomendamos:

- Cambiar tu contraseña en `[SITIO]` y en cualquier otro servicio donde uses la misma.
- Desconfiar de correos, mensajes o llamadas que digan venir de `[EMPRESA]` y te pidan claves, códigos o pagos.
- [Si corresponde:] Revisar los movimientos de tu tarjeta y avisar a tu banco si ves algo que no reconoces.

Si tienes dudas, escríbenos a `[CORREO]` o llámanos al `[TELÉFONO]`. Te mantendremos informado si sabemos algo nuevo.

Saludos cordiales,

`[NOMBRE Y CARGO]`

`[EMPRESA]`

TE ACOMPAÑAMOS CON LOS REPORTES

Qué informar, a quién y en qué plazo es una de las preguntas más difíciles en las primeras horas. Te ayudamos a preparar los reportes a la ANCI y a la Agencia de Protección de Datos Personales con la información técnica que piden, la información para tu seguro y el mensaje para tus clientes, para que lo que digas sea preciso y no haya que corregirlo después.

PASO 5

Encontrar por dónde entró

Antes de limpiar, hay que entender cómo entró el atacante. Si no se cierra esa puerta, el sitio limpio vuelve a infectarse, a veces en cuestión de horas. Estas son las causas más comunes en sitios de empresas:

- Plugins, temas o módulos desactualizados con fallas conocidas. Es la causa más frecuente en WordPress y WooCommerce.
- Plugins o temas descargados de sitios no oficiales, como versiones gratuitas de productos pagados, que muchas veces traen una puerta trasera incluida.
- Contraseñas débiles, reutilizadas o filtradas en otro servicio, sobre todo en cuentas sin verificación en dos pasos.
- Computadores infectados con programas que roban las contraseñas guardadas en el navegador.
- Formularios o funciones que no validan lo que reciben y permiten subir archivos o ejecutar comandos.
- Accesos de agencias, desarrolladores o exempleados que nunca se eliminaron.
- Claves de API o contraseñas expuestas en el código, en un repositorio público o en un archivo de configuración accesible desde internet.
- Un servidor compartido con otro sitio vulnerable.

Los registros que guardaste en el paso 2 son la principal pista: muestran desde dónde se conectaron, a qué archivos accedieron y cuándo. Ojo con las fechas: el primer síntoma visible suele aparecer días o semanas después del ingreso real.

Cuando los registros no alcanzan, o el ataque es más elaborado, se necesita una investigación más profunda: análisis de los archivos maliciosos, revisión de los servidores y de las cuentas involucradas, y búsqueda de rastros en otros sistemas de la empresa. Es el tipo de trabajo que hacemos en nuestro servicio de respuesta y recuperación.

PASO 6

Limpiar y recuperar

Hay dos caminos, y muchas veces se combinan.

Restaurar una copia de respaldo limpia

Es el camino más rápido si tienes respaldos y sabes cuándo empezó el ataque. Elige una copia anterior a la fecha del ingreso, no solo anterior al primer síntoma. Después de restaurar, aplica de inmediato las actualizaciones y los cambios de acceso: la copia tiene la misma falla que permitió el ataque. Considera también lo que se pierde, como pedidos, registros o contenidos creados después de esa fecha, que habrá que recuperar aparte.

Limpiar el sitio actual

Es necesario si no hay respaldos confiables. Incluye:

- Reinstalar el núcleo del sistema (por ejemplo, WordPress), los plugins y los temas desde sus fuentes oficiales, en vez de corregir archivo por archivo.
- Revisar los archivos que no se reemplazan, como imágenes y documentos subidos: no deberían contener programas ejecutables, como archivos .php dentro de la carpeta de cargas.
- Revisar la base de datos: usuarios, configuraciones y contenidos con código o enlaces insertados.
- Buscar tareas programadas, usuarios ocultos y archivos de configuración modificados que le permitan al atacante volver.
- Eliminar los plugins, temas, cuentas y servicios que no se usan. Lo que no existe no se puede atacar.
- Actualizar todo: sistema, plugins, temas y la versión de PHP o del lenguaje que use tu sitio.

Si el sitio maneja pagos o datos sensibles, o si no se logró determinar por dónde entró el atacante, la opción más segura es reconstruir en un servidor nuevo y migrar solo los contenidos revisados.

PASO 7

Volver a operar y vigilar

- Antes de reabrir, comprueba que el sitio no redirige (prueba desde un celular y desde un resultado de búsqueda), que no hay usuarios desconocidos, que los formularios y el pago funcionan como deben y que todo está actualizado.
- Reabre de forma controlada y mantén el panel de administración restringido algunos días.
- Si Google marcó el sitio como peligroso, solicita una revisión desde Google Search Console, en la sección de problemas de seguridad. Mientras la advertencia siga activa, perderás la

mayoría de tus visitas. Si tu dominio quedó en listas de bloqueo de correo, pide la exclusión en cada una una vez resuelto el problema.

- Reactiva las integraciones una por una, con las claves nuevas.
- Vigila con atención las semanas siguientes: cambios de archivos, usuarios nuevos, accesos al panel desde lugares inusuales. Volver a infectarse es común cuando quedó una puerta trasera sin detectar.

PASO 8

Aprender de lo que pasó

Cuando todo esté estable, reúne a quienes participaron y deja por escrito qué pasó, cómo entró el atacante, qué datos se vieron afectados, qué se hizo y en cuánto tiempo, y qué funcionó y qué no. Termina con una lista de mejoras con responsables y fechas. Ese documento es útil para tu equipo y tu seguro, y para demostrar diligencia ante una autoridad o un cliente.

Un ethical hacking después de la recuperación confirma que la puerta quedó cerrada y que no hay otras abiertas.

Si te piden un rescate

Algunos ataques terminan con un mensaje que exige un pago, normalmente en criptomonedas, a cambio de devolverte el acceso o de no publicar tus datos. Antes de hacer cualquier cosa:

- No respondas ni negocies por tu cuenta. Guarda el mensaje como evidencia.
- Busca asesoría especializada y, si corresponde, avisa a tu seguro y haz la denuncia.
- Ten presente que pagar no garantiza que recuperes la información ni que tus datos no se publiquen o se vendan igual, y te identifica como una empresa dispuesta a pagar.
- Revisa si tienes respaldos que el ataque no alcanzó. Los que se guardan fuera del servidor y sin acceso desde él suelen ser los que se salvan.

Errores que conviene evitar

- Borrar todo y reinstalar sin guardar evidencia ni entender cómo entró el atacante.
- Restaurar un respaldo que ya estaba infectado.
- Cambiar las contraseñas desde el mismo equipo que pudo haber sido comprometido.
- Olvidar las integraciones: el atacante puede seguir entrando por una clave de API o un webhook.
- Dar por cerrado el problema porque el sitio «se ve bien». Muchos ataques están diseñados para no verse.

- Avisar tarde, o avisar algo que después hay que corregir.
- Pagar un rescate sin asesoría.

Lista de verificación de las primeras 24 horas

N.°	ACCIÓN	HECHO
01	Persona a cargo designada y bitácora abierta.	
02	Revisado si la empresa debe reportar a la ANCI. Si es así, alerta temprana enviada dentro de 3 horas.	
03	Sitio en mantenimiento o suspendido, sin borrar nada.	
04	Pago en línea e integraciones pausados.	
05	Copia completa de archivos y base de datos guardada fuera del servidor.	
06	Registros pedidos al hosting y descargados de las demás plataformas.	
07	Capturas y mensajes guardados con fecha y hora.	
08	Contraseñas cambiadas desde un equipo de confianza, empezando por el correo.	
09	Verificación en dos pasos activada y sesiones abiertas cerradas.	
10	Usuarios desconocidos documentados y desactivados.	
11	Hosting, banco o procesador de pagos y seguro informados, según corresponda.	
12	Evaluado si hubo datos personales afectados y si corresponde reportar a la Agencia de Protección de Datos Personales y a los afectados.	
13	Decidido si se hará la denuncia en la PDI o la Fiscalía.	
14	Decidido si se necesita análisis forense o apoyo especializado.	

Cómo reducir el riesgo de que vuelva a pasar

- Actualiza el sistema, los plugins y los temas apenas haya versiones nuevas, y elimina lo que no uses.
- Instala componentes solo desde fuentes oficiales.
- Activa la verificación en dos pasos en todas las cuentas de administración, correo, dominio y hosting.
- Usa cuentas personales para cada persona, con el permiso mínimo necesario, y elimínalas apenas alguien deja de trabajar contigo.
- Programa respaldos automáticos guardados fuera del servidor, y prueba de vez en cuando que se pueden restaurar.
- Haz una revisión de seguridad antes de cada lanzamiento o cambio importante.
- Activa el monitoreo continuo, para detectar el próximo intento en minutos y no en semanas.
- Deja un plan simple por escrito: quién decide, a quién se llama, dónde están las claves y los contactos. Esta guía puede ser el punto de partida.

Cómo te ayuda Tinary

SERVICIO	QUÉ HACEMOS
Respuesta y recuperación	Contenemos el daño, limpiamos o reconstruimos el sitio y te ayudamos a volver a operar.
Análisis forense e investigación	Determinamos cómo entró el atacante, desde cuándo estaba dentro, qué hizo y qué datos tocó, con la evidencia preservada y su cadena de custodia.
Reportes y comunicaciones	Preparamos contigo los reportes a las autoridades, la información para tu seguro y el mensaje a tus clientes.
Ethical hacking	Después de la recuperación, confirmamos que la puerta quedó cerrada y que no hay otras abiertas.
Monitoreo continuo	Vigilamos tus sistemas para detectar el próximo intento antes de que crezca.

CUANDO ALGO FALLA

¿Te está pasando ahora?

Escríbenos de inmediato con tu nombre, tu empresa, un teléfono de contacto y lo que estás viendo. No necesitas tener todo claro para escribirnos: ordenar el caso es parte de nuestro trabajo.

Escríbenos a contacto@tinary.cl →

Esta guía es informativa y no reemplaza la asesoría legal ni técnica para un caso concreto. Las referencias legales corresponden a la normativa chilena a noviembre de 2026: Ley 21.663 Marco de Ciberseguridad, Ley 21.719 de Protección de Datos Personales y Ley 21.459 de Delitos Informáticos.