tinary

GUÍA · ANTES DE LANZAR

Qué revisión necesita tu empresa

Ethical hacking, auditoría de código o monitoreo continuo: cómo elegir según lo que tienes y lo que vas a lanzar.

GUÍA · 13 MIN DE LECTURA

No existe una revisión de seguridad que sirva para todo. Cada una mira tus sistemas desde un ángulo distinto y responde una pregunta distinta. Elegir bien depende de dos cosas: lo que ya tienes funcionando y lo que estás por lanzar.

Esta guía explica las tres revisiones más comunes, cuándo conviene cada una y cómo combinarlas a lo largo del año, con ejemplos de situaciones frecuentes en empresas.

Las tres revisiones, en una frase

ETHICAL HACKING

¿Qué podría hacer hoy un atacante contra lo que ya está publicado?

Mira tus sistemas desde afuera, como lo haría un intruso, pero con tu permiso.

AUDITORÍA DE CÓDIGO Y DEPENDENCIAS

¿Qué fallas hay dentro de tu aplicación y de las librerías que usa?

Mira tus sistemas desde adentro, antes de que lleguen a tus clientes.

MONITOREO CONTINUO

¿Alguien está intentando entrar, o ya entró?

Mira tus sistemas todo el año, mientras operas.

Las dos primeras son una fotografía: muestran cómo estás en un momento determinado. El monitoreo es una cámara encendida: muestra lo que pasa todos los días.

	ETHICAL HACKING	AUDITORÍA DE CÓDIGO	MONITOREO CONTINUO
Qué responde	Qué puede hacer un atacante hoy.	Qué fallas hay dentro del código y sus dependencias.	Si alguien está atacando ahora.
Cómo mira	Desde afuera, como un atacante.	Desde adentro, leyendo el código.	Todo el tiempo, sobre la operación real.
Cuándo conviene	Antes de lanzar, después de cambios importantes y al menos una vez al año.	Mientras desarrollas y antes de lanzar o recibir una aplicación.	Desde que el sistema está en producción, de forma permanente.
Qué entregas	Alcance, autorización firmada y, según el tipo, cuentas de prueba.	Acceso de lectura al repositorio y documentación.	Acceso a los registros de tus sistemas y contactos de escalamiento.
Qué recibes	Hallazgos comprobados, priorizados y con su corrección.	Hallazgos con archivo y línea, dependencias vulnerables y cómo corregir.	Alertas analizadas, respuesta a incidentes e informes periódicos.
Qué no hace	No vigila lo que pasa después de la prueba.	No ve fallas de configuración del servidor ni de la operación.	No corrige las fallas de fondo de tu sistema.

01

Ethical hacking

Un equipo especializado ataca tus sistemas con tu autorización y con las mismas técnicas que usaría un intruso, para encontrar las fallas que se pueden aprovechar de verdad. A diferencia de un escaneo automático, cada hallazgo se comprueba y se explica: qué permite hacer, qué tan grave es para tu negocio y cómo se corrige.

Qué puede cubrir: sitios web y tiendas en línea, aplicaciones web y móviles, APIs e integraciones, la infraestructura expuesta a internet y, si se pide, la red interna o los servicios en la nube.

Tres formas de hacerlo, según cuánta información entregas

- **Caja negra**: el equipo parte sin información, como un atacante externo. Muestra lo que cualquiera puede encontrar, pero puede dejar fuera funciones que requieren una cuenta.

- **Caja gris**: el equipo recibe cuentas de prueba con distintos perfiles, como cliente, vendedor o administrador. Es la opción más usada en aplicaciones, porque permite responder preguntas como «¿un cliente puede ver los pedidos de otro?».
- **Caja blanca**: el equipo recibe además documentación y acceso al código. Es la más profunda y se acerca a una auditoría de código.

Conviene cuando

- Vas a lanzar un sitio, una tienda o una aplicación, o una versión con cambios importantes.
- Tu sistema lleva tiempo funcionando y nunca se revisó, o la última revisión fue hace más de un año.
- Un cliente, una licitación o una auditoría te pide demostrar que revisaste tu seguridad.
- Tuviste un incidente y quieres confirmar que la puerta quedó cerrada.

Lo que necesitas preparar: la lista de lo que entra en la prueba (dominios, aplicaciones y APIs), una autorización firmada, cuentas de prueba para cada perfil, las fechas y horarios permitidos, y un contacto técnico disponible durante la prueba. Si puedes, habilita un ambiente de pruebas igual al de producción: permite probar más a fondo sin arriesgar tu operación.

Lo que no es: un ethical hacking no garantiza que no existan otras fallas, y su resultado vale para el momento en que se hizo. Cada cambio importante puede abrir puertas nuevas.

02

Auditoría de código y dependencias

Se revisa el código fuente de tu aplicación, con herramientas automáticas y lectura manual, para encontrar fallas antes de que lleguen a producción. Incluye las librerías de terceros que usa tu aplicación, que suelen ser la mayor parte del código y una de las principales fuentes de vulnerabilidades conocidas.

Qué revisa

- **Código propio**: validación de los datos que ingresan, control de permisos, manejo de sesiones, consultas a la base de datos y carga de archivos.
- **Dependencias**: librerías y componentes con vulnerabilidades publicadas, abandonados o con licencias problemáticas.
- **Secretos**: contraseñas, claves de API o tokens escritos en el código o en el historial del repositorio.
- **Configuración**: archivos de despliegue, contenedores e infraestructura definida como código.

Conviene cuando

- Desarrollas tu propio software, con un equipo interno o con un proveedor.
- Vas a recibir una aplicación desarrollada por un tercero. Revisarla antes de aceptarla y pagarla es mucho más barato que corregirla después. Si puedes, deja en el contrato que la entrega debe aprobar una revisión de seguridad.
- Vas a lanzar una aplicación que maneja pagos, datos personales o información sensible.
- Quieres incorporar la seguridad al ciclo de desarrollo, para que cada cambio se revise antes de publicarse.

Lo que necesitas preparar: acceso de solo lectura al repositorio, una explicación de la arquitectura y alguien del equipo de desarrollo que pueda responder preguntas.

Cuándo no es lo primero: si tu sitio está hecho con WordPress, WooCommerce u otra plataforma estándar y no tiene desarrollos propios, una auditoría de código completa rara vez es la mejor inversión. En ese caso conviene más un ethical hacking y una revisión de los plugins, los temas y su configuración.

03

Monitoreo continuo

Se recogen los registros de actividad de tus sistemas (sitio, servidores, correo, cuentas en la nube, firewall e integraciones) y se analizan de forma permanente, con reglas de detección y analistas que revisan las alertas. Cuando ocurre algo sospechoso, se investiga, se te avisa y, si está acordado, se actúa para contenerlo.

Qué detecta

- Intentos de acceso repetidos, accesos desde lugares o en horarios inusuales y cuentas comprometidas.
- Cambios no autorizados en archivos, configuraciones o permisos.
- Programas maliciosos y comportamientos anómalos en servidores y equipos.
- Ataques contra tu sitio o tus APIs mientras ocurren.

Conviene cuando

- Tu operación depende de sistemas en línea y una interrupción te cuesta ventas.
- Guardas datos personales de clientes. Detectar un ataque a tiempo reduce lo que se filtra y te permite cumplir los plazos de aviso de la ley.
- No tienes un equipo que revise registros y alertas todos los días.
- Ya tuviste un incidente.

Lo que necesitas preparar: acceso a los registros de los sistemas que se van a vigilar (a veces requiere instalar un agente en los servidores), una lista de contactos para escalar alertas a cualquier hora y una definición previa de qué acciones puede tomar el proveedor sin consultarte.

Lo que no es: el monitoreo detecta y responde, pero no corrige las fallas de fondo de tu sistema. Por eso se complementa con revisiones periódicas.

Otras revisiones que pueden servirte

- **Publicación segura**: revisión de configuración, permisos y accesos justo antes de salir al aire. Es breve y evita los errores más comunes de un lanzamiento, como paneles expuestos, archivos de respaldo accesibles desde internet o cuentas de prueba que siguen activas.
- **Integraciones y APIs**: revisión de cómo se conectan tu CRM, tu ERP, tu tienda y tus automatizaciones: qué permisos tiene cada clave, quién puede llamar a cada API y qué datos viajan entre sistemas.
- **Automatizaciones e IA**: revisión de los flujos, bots y herramientas con IA que mueven datos sin supervisión: qué pueden ver, qué pueden hacer y quién más podría usarlos.
- **Diagnóstico de datos personales (Ley 21.719)**: qué datos guardas, dónde están, quién accede a ellos y qué tienes que cambiar para cumplir la ley.
- **Revisión de compromiso**: responde una pregunta distinta a todas las anteriores: ¿ya hay alguien adentro? Se buscan rastros de un atacante en tus servidores, cuentas y registros. Conviene si notas comportamientos extraños, si un proveedor o exempleado tuvo accesos que no controlaste o antes de comprar o integrar otra empresa.

Elige según tu situación

01 Vas a lanzar un sitio, una tienda o una aplicación

Empieza por una auditoría de código si hay desarrollo propio, sigue con un ethical hacking sobre la versión casi final y cierra con una revisión de publicación segura antes de salir al aire. Desde el primer día en producción, activa el monitoreo.

02 Tienes un sitio WordPress o una tienda que funciona hace años

Un ethical hacking de caja gris, con foco en los plugins, los temas, el panel de administración y los pagos. Si vendes en línea, suma monitoreo continuo: estos sitios son blanco frecuente de ataques automatizados.

03 Desarrollas tu propio software o plataforma

Integra la auditoría de código al desarrollo, para que cada cambio importante se revise. Haz un ethical hacking antes de cada versión mayor y al menos una vez al año, y mantén el monitoreo en producción.

04 Un proveedor te está desarrollando una aplicación

Pide una auditoría de código y un ethical hacking antes de aceptar la entrega, y deja por escrito que las fallas graves se corrigen como parte del trabajo contratado.

05 Conectas tu tienda, tu CRM, tu ERP y tus automatizaciones

Revisa las integraciones y APIs: los permisos de cada clave, los webhooks y los datos que viajan entre sistemas. Complementa con un ethical hacking de las APIs expuestas y monitoreo de los accesos.

06 Un cliente, una licitación o una auditoría te pide demostrar tu seguridad

Antes de contratar, pregunta exactamente qué te piden. Muchas veces es un ethical hacking reciente, con informe formal y la verificación de que las fallas se corrigieron. Ese requisito define el alcance.

07 Guardas datos personales de tus clientes

Parte por un diagnóstico de qué datos tienes y dónde están, y revisa con un ethical hacking los sistemas que los contienen. El monitoreo te permite detectar una filtración a tiempo para avisar como exige la Ley 21.719.

08 Sospechas que algo no anda bien, pero no tienes pruebas

Cuentas que se bloquean solas, cobros extraños, clientes que reciben correos falsos a tu nombre o un exempleado que tenía demasiados accesos. Una revisión de compromiso o una investigación a medida te dice si hay alguien adentro, desde cuándo y qué ha tocado.

09 Ya te atacaron

Primero, respuesta y recuperación: contener, investigar y volver a operar (revisa la guía «Qué hacer si hackearon tu sitio»). Si necesitas saber exactamente qué pasó, o el caso puede terminar en una denuncia o en un reclamo al seguro, suma un análisis forense. Después, un ethical hacking para confirmar que no quedan puertas abiertas y monitoreo para detectar un nuevo intento.

10 No sabes cómo estás

Un diagnóstico inicial ordena el panorama: qué tienes expuesto, qué es lo más crítico y por dónde conviene partir. Es la forma más económica de no gastar en la revisión equivocada.

Seis preguntas para decidir

1. **¿Ya está publicado o está por lanzarse?** Si está por lanzarse, revisa antes de salir. Si ya está publicado, un ethical hacking te dice cómo estás hoy.
2. **¿Tienes código propio?** Si la respuesta es sí, la auditoría de código entra en el plan. Si usas una plataforma estándar sin desarrollos propios, probablemente no.
3. **¿Cuánto te cuesta un día sin sistema o una filtración de datos?** Si la respuesta es «mucho», necesitas monitoreo continuo.
4. **¿Alguien revisa hoy las alertas y registros de tus sistemas?** Si nadie lo hace, un ataque puede pasar semanas sin que lo notes.
5. **¿Cuándo fue la última revisión y qué cambió desde entonces?** Más de un año, o cambios importantes desde la última, justifican una nueva.
6. **¿Alguien te exige una revisión?** Si es así, el requisito define el tipo de revisión y el informe que necesitas.

Cómo se combinan a lo largo del año

MOMENTO	QUÉ HACER
Antes de lanzar	Auditoría de código si hay desarrollo propio, ethical hacking y revisión de publicación segura.
Al salir al aire	Monitoreo continuo activo desde el primer día.
Con cada cambio importante	Revisión del código nuevo y prueba enfocada en lo que cambió.
Una vez al año, como mínimo	Ethical hacking completo y revisión de integraciones y accesos.
Todo el año	Monitoreo, actualizaciones y control de quién tiene acceso a qué.
Cuando algo falla	Respuesta y recuperación, análisis forense si hace falta, y una revisión final para confirmar que quedó cerrado.

Qué preparar antes de pedir una revisión

- Una lista de lo que tienes: dominios y subdominios, aplicaciones, APIs, integraciones y plataformas en la nube.
- Quién es responsable de cada sistema, dentro de tu empresa o en tus proveedores.
- Qué maneja cada sistema: pagos, datos personales o información confidencial.
- Si tienes un ambiente de pruebas y qué tan parecido es al de producción.
- Los horarios en que no se puede afectar la operación.
- Los informes de revisiones anteriores y lo que se corrigió desde entonces.
- Los requisitos que te imponen tus clientes, tus contratos o la ley.

Con esa información, cualquier proveedor serio puede proponerte un alcance concreto y un precio responsable. Si te cuesta reunirla, eso ya dice algo, y es un buen punto de partida para un diagnóstico.

Ideas que conviene descartar

- **«Mi empresa es chica, a nadie le interesa atacarla.»** La mayoría de los ataques son automáticos: buscan fallas conocidas en miles de sitios a la vez, sin mirar de quién son.
- **«Mi hosting ya incluye seguridad.»** El proveedor protege su infraestructura, no la configuración de tu sitio, tus plugins, tus contraseñas ni tus integraciones.
- **«Un escaneo gratuito es lo mismo que un ethical hacking.»** Un escaneo encuentra fallas conocidas y genera falsas alarmas. No prueba si un cliente puede ver los datos de otro ni si un usuario común puede actuar como administrador.
- **«Ya hicimos una revisión, estamos cubiertos.»** Cada revisión es una fotografía de un momento. Cada cambio en tu sistema, cada plugin nuevo y cada vulnerabilidad recién descubierta cambian el resultado.
- **«El desarrollador ya se preocupó de la seguridad.»** Puede ser, pero quien construye no es la mejor persona para revisar su propio trabajo. Una mirada independiente encuentra lo que el equipo da por sentado.

CUANDO TU CASO NO CALZA EN NINGUNA CASILLA

Hay situaciones que ninguna revisión estándar resuelve por sí sola: una filtración de datos sin explicación, un fraude que parece salir de tus propios sistemas, un proveedor que dejó de responder y del que no sabes qué accesos conserva, o un incidente que necesitas reconstruir paso a paso para una denuncia o un reclamo al seguro.

Para eso hacemos investigaciones a medida y análisis forense: buscamos los rastros, reconstruimos lo que pasó, te decimos qué hacer y lo dejamos documentado. Escríbenos a **contacto@tinary.cl** y lo conversamos.

ELIGE POR DÓNDE EMPEZAR

¿Aún no sabes qué revisión necesitas?

Agenda un diagnóstico. Revisamos lo que tienes y lo que vas a lanzar, y te decimos qué revisión necesitas, en qué orden y qué puedes dejar para después.

Escríbenos a contacto@tinary.cl →

Esta guía es informativa. La revisión adecuada para cada empresa depende de su operación, sus sistemas y sus obligaciones; un diagnóstico permite definirla con precisión.