tinary

GUÍA · ANTES DE CONTRATAR

Cómo elegir un proveedor de ciberseguridad

Qué preguntar antes de contratar: certificaciones, cobertura 24/7, tiempos de respuesta y qué entrega cada informe.

GUÍA · 15 MIN DE LECTURA

Contratar un proveedor de ciberseguridad es entregarle a alguien externo la llave de tus sistemas y la confianza de tus clientes. Por eso la decisión no debería depender de quién presenta mejor ni de quién cobra menos, sino de lo que cada proveedor puede demostrar.

Esta guía reúne lo que conviene preguntar, cómo leer las respuestas y qué señales deberían hacerte dudar. Sirve para comparar propuestas de ethical hacking, auditoría de código, monitoreo continuo o respuesta a incidentes, y también para revisar si tu proveedor actual te está dando lo que necesitas.

01

Antes de pedir propuestas, define qué necesitas

Un proveedor solo puede ofrecerte algo a tu medida si sabe qué quieres proteger. Antes de la primera reunión, responde por escrito:

- **Qué quieres proteger**: sitio web, tienda en línea, aplicación, integraciones, correo, servidores o servicios en la nube.
- **Por qué ahora**: un lanzamiento, un incidente, un requisito de un cliente o de una licitación, una ley, o simplemente que no sabes cómo estás.
- **Qué te exigen**: la Ley 21.719 de datos personales, la Ley 21.663 de ciberseguridad si prestas servicios esenciales, contratos con clientes o auditorías.
- **Con quién cuentas**: equipo técnico propio, un proveedor de desarrollo o nadie.
- **Qué esperas recibir**: un informe para decidir, acompañamiento para corregir o vigilancia permanente.

Si no tienes claro qué tipo de revisión necesitas, la guía «Qué revisión necesita tu empresa» te ayuda a definirlo. Llevar estas respuestas por escrito te permite comparar propuestas sobre la misma base.

02

Quién hará el trabajo

La empresa que vende no siempre es la que ejecuta. Pregunta:

- ¿Quiénes harán el trabajo y qué experiencia y certificaciones tienen esas personas?
- ¿Son parte del equipo del proveedor o subcontratados? Si hay subcontratistas, ¿quiénes son y qué acuerdos de confidencialidad los cubren?
- ¿Han trabajado con sistemas como los tuyos: WordPress, tiendas en línea, aplicaciones a medida, APIs, Microsoft 365, Google Workspace, CRM o ERP?
- ¿Pueden darte referencias de clientes de un tamaño y un rubro parecidos al tuyo?

La experiencia en tu tipo de tecnología pesa tanto como la experiencia en seguridad. Un equipo que entiende cómo funcionan tus integraciones encuentra fallas que un análisis genérico no ve.

03

Certificaciones: qué significan y cómo verificarlas

Hay dos tipos de certificaciones, y conviene no confundirlas.

Las de la empresa

Muestran cómo el proveedor gestiona la seguridad de su propia operación, incluida la información que le vas a entregar.

- **ISO/IEC 27001**: norma internacional de gestión de seguridad de la información. Pide el certificado y fíjate en tres cosas: que esté vigente, quién lo emitió (debe ser un organismo de certificación acreditado) y cuál es su alcance. Un certificado que cubre solo un área administrativa no dice nada sobre el servicio que vas a contratar.
- **Informes SOC 2**: no son una certificación, sino el informe de un auditor independiente sobre los controles del proveedor. El Tipo I revisa el diseño de los controles en una fecha; el Tipo II revisa que funcionaron durante un período, normalmente de varios meses. Si te lo ofrecen, pregunta de qué tipo es y qué período cubre.
- **Alianzas con fabricantes**: indican que el proveedor conoce a fondo una tecnología. Son útiles si coinciden con lo que tú usas.

Las de las personas

Acreditan los conocimientos de quienes harán el trabajo. Estas son algunas de las más reconocidas:

CERTIFICACIÓN	QUÉ ACREDITA
OSCP / OSCP+ (OffSec)	Pruebas de intrusión, con un examen práctico en que el candidato debe comprometer sistemas reales en un tiempo limitado.
OSWE (OffSec)	Ataque a aplicaciones web a partir de la revisión de su código fuente.
eWPT / eWPTX (INE Security)	Pruebas de intrusión en aplicaciones web, con examen práctico.
GPEN / GWAPT (GIAC)	Pruebas de intrusión en redes y en aplicaciones web.
CEH (EC-Council)	Conocimiento general de técnicas de ataque. Es más teórica, aunque tiene una variante práctica.
CompTIA Security+, CySA+ y PenTest+	Fundamentos de seguridad, análisis y monitoreo, y pruebas de intrusión.
CISSP (ISC2) / CISM (ISACA)	Gestión y gobierno de la seguridad. Útiles para planes, políticas y cumplimiento.
ISO/IEC 27001 Lead Auditor o Lead Implementer	Auditoría o implementación de sistemas de gestión de seguridad de la información.

Tres advertencias:

- Una certificación demuestra que alguien aprobó un examen, no que tenga experiencia en sistemas como los tuyos. Pide las dos cosas.
- Verifica las certificaciones. La mayoría de los emisores tiene un registro público o insignias digitales que se pueden comprobar en línea.
- Pregunta si las personas certificadas son las que van a trabajar en tu proyecto, o si solo aparecen en la presentación comercial.

04

Cobertura 24/7: qué hay detrás de la promesa

«Monitoreo 24/7» puede significar cosas muy distintas: desde analistas que revisan cada alerta en turnos, todos los días del año, hasta un sistema que envía correos automáticos que alguien lee el lunes. Para saber qué te están ofreciendo, pregunta:

- ¿Hay personas en turno las 24 horas, incluidos fines de semana y festivos, o fuera del horario de oficina solo hay alertas automáticas?

- Si a las 3 de la mañana de un domingo se detecta un ataque, ¿quién lo ve, cuánto tarda en revisarlo y quién te llama?
- ¿El equipo de turno es propio o subcontratado? ¿Desde dónde opera?
- ¿Pueden actuar para contener el ataque, por ejemplo bloqueando una dirección o desactivando una cuenta, o solo avisan? ¿Qué autorización necesitan de tu parte para hacerlo?
- ¿Qué sistemas vigilan exactamente: tu sitio, tus servidores, tu correo, tus cuentas en la nube, tus integraciones?
- ¿Cómo descartan las falsas alarmas? Un servicio que te reenvía cientos de alertas sin analizar te traspasa el trabajo a ti.
- ¿Qué necesitan de ti? Normalmente, una lista de contactos de escalamiento con teléfonos disponibles a cualquier hora.

Pide que te muestren cómo se ve una alerta real, con los datos ocultos, y cómo te llegaría. Y pregúntate si de verdad necesitas cobertura las 24 horas: si tu tienda vende de noche, si guardas datos de clientes o si un día sin sistema te cuesta caro, probablemente sí.

05

Tiempos de respuesta: que queden por escrito

Los tiempos de respuesta son la parte más concreta de un servicio y, a la vez, la que más se presta a confusión. Distingue entre:

- **Tiempo de detección**: cuánto pasa entre que algo ocurre y que el proveedor lo identifica.
- **Tiempo de notificación**: cuánto tarda en avisarte después de identificarlo.
- **Tiempo de respuesta**: cuánto tarda en empezar a actuar.
- **Tiempo de contención**: cuánto tarda en detener el daño.
- **Tiempo de resolución**: cuánto tarda en cerrar el caso.

Un proveedor que promete «respuesta en 15 minutos» puede referirse a que en 15 minutos te llega un correo automático. Pide que cada tiempo quede definido:

- **Por nivel de gravedad**, con ejemplos concretos de qué situación corresponde a cada nivel.
- **Con un punto de partida claro**: desde que ocurre el evento, desde que se genera la alerta o desde que tú lo reportas.
- **Con su horario**: si rige las 24 horas o solo en horario hábil.
- **Con medición y consecuencias**: cómo se informa el cumplimiento cada mes y qué pasa si no se cumple, como descuentos o término del contrato.

Así debería verse, como mínimo, el anexo de niveles de servicio de una propuesta de monitoreo o de respuesta:

NIVEL	EJEMPLO DE SITUACIÓN	DEBE QUEDAR DEFINIDO
Crítico	Ataque en curso, sitio caído por un ataque, datos de clientes saliendo de tus sistemas.	Tiempos de notificación, inicio de la respuesta y contención, válidos a cualquier hora.
Alto	Cuenta de administrador comprometida, archivo malicioso detectado en un servidor.	Tiempos de notificación y de respuesta, válidos a cualquier hora.
Medio	Intentos repetidos de acceso, vulnerabilidad nueva en un componente que usas.	Tiempo de notificación y plazo sugerido de corrección.
Bajo	Configuración mejorable, hallazgo informativo.	Inclusión en el informe periódico.

06

Qué entrega cada informe

El informe es lo que te queda cuando el proveedor termina. Antes de contratar, pide un informe de ejemplo con los datos del cliente ocultos. Si no pueden mostrarlo, es una señal de alerta. Esto es lo que debería traer cada tipo de servicio.

Ethical hacking

- Resumen ejecutivo en lenguaje de negocio: qué tan expuesto estás, qué es lo más urgente y qué decisiones se necesitan.
- Alcance exacto: qué se probó y qué no, desde dónde, en qué fechas y con qué tipo de acceso.
- Metodología reconocida, como la guía de pruebas de OWASP (WSTG), el estándar de verificación OWASP ASVS, PTES o NIST SP 800-115.
- Cada hallazgo con una descripción clara, evidencia que permita reproducirlo, gravedad según un criterio explícito (por ejemplo, CVSS) ajustada a tu contexto, impacto para el negocio y una recomendación concreta para corregirlo.
- Lo que se probó y resistió. Saber qué está funcionando bien también es información.
- Limitaciones de la prueba: lo que no se pudo probar y por qué.
- Una nueva prueba (retest) para verificar las correcciones. Pregunta si está incluida en el precio y por cuánto tiempo.

Auditoría de código y dependencias

- Qué partes del código se revisaron y con qué combinación de herramientas automáticas y revisión manual.
- Hallazgos depurados, sin falsas alarmas, con el archivo y la línea, una explicación y un ejemplo de cómo corregirlo.
- Librerías y dependencias con vulnerabilidades conocidas, con la versión que las corrige.
- Contraseñas, claves o tokens encontrados en el código o en el historial del repositorio.
- Idealmente, un inventario de componentes (SBOM) y una revisión de licencias.

Monitoreo continuo

- Informe periódico, normalmente mensual: qué se vigiló, qué alertas hubo, cuáles fueron incidentes reales y qué se hizo con cada uno.
- Cumplimiento real de los tiempos comprometidos, caso por caso y no solo en promedio.
- Tendencias y recomendaciones: qué se repite y qué conviene cambiar.
- Acceso a un panel o portal para ver el estado en cualquier momento.

Respuesta a incidentes y análisis forense

- Cronología de lo ocurrido, desde el ingreso del atacante hasta la recuperación.
- Causa raíz: cómo entró y por qué fue posible.
- Alcance: qué sistemas y qué datos fueron afectados.
- Evidencia preservada con su cadena de custodia, si el caso puede llegar a una denuncia, un juicio o un reclamo al seguro.
- Acciones tomadas y pendientes.
- Indicadores de compromiso: direcciones, archivos y otros rastros que sirvan para detectar un nuevo intento.
- Información lista para los reportes que la ley te exija.

Desconfía de un informe que es solo la exportación de una herramienta automática, de hallazgos sin evidencia, de todo marcado como crítico o de un documento que tu equipo no puede entender sin el proveedor al lado.

07

Confidencialidad, permisos y contrato

Tu proveedor va a ver cómo funcionan tus sistemas y, muchas veces, datos de tus clientes. Antes de empezar debería quedar firmado:

- **Un acuerdo de confidencialidad** que cubra al proveedor y a cualquier subcontratista.
- **Una autorización escrita para las pruebas**, con el alcance exacto (dominios, direcciones y aplicaciones), las fechas y horarios, lo que está prohibido hacer y los contactos de emergencia. Un proveedor serio no empieza sin ella: atacar sistemas sin autorización es un delito.
- **Las condiciones de tratamiento de datos personales.** Si el proveedor accede a datos de tus clientes, los trata por cuenta tuya, y la Ley 21.719 exige que el contrato regule qué puede hacer con ellos, qué medidas de seguridad aplica y qué pasa con los datos al terminar.
- **Dónde y cómo guarda tu información** el proveedor, por cuánto tiempo y cómo la elimina al cerrar el servicio.
- **Gestión de accesos**: cuentas personales para cada integrante del proveedor, verificación en dos pasos y eliminación de todos los accesos al terminar.
- **Responsabilidades y seguros**: qué pasa si una prueba provoca una interrupción y si el proveedor tiene un seguro de responsabilidad profesional.
- **Qué hace si encuentra algo grave a mitad del trabajo**: debería avisarte de inmediato, sin esperar el informe final.
- **Cómo termina el contrato**: plazos, devolución de la información y traspaso ordenado si cambias de proveedor.

08

Cómo trabajará con tu equipo

- ¿Quién será tu contacto y cómo te comunicarás con esa persona durante el servicio?
- ¿Explican los hallazgos en una reunión, además de enviar el informe?
- ¿Acompañan a tu equipo o a tu proveedor de desarrollo durante la corrección, o solo entregan el informe?
- ¿Se adaptan a tu operación, por ejemplo haciendo las pruebas fuera de tus horarios de mayor venta?
- ¿Hablan en un lenguaje que tu dirección entienda?

El valor de una revisión no está en la lista de fallas, sino en que se corrijan. Un proveedor que acompaña la corrección vale más que uno que entrega un documento extenso y desaparece.

09

Precio: qué estás comparando

Las propuestas de seguridad son difíciles de comparar porque pocas veces incluyen lo mismo. Para compararlas sobre la misma base, revisa:

- **Qué incluye el precio**: alcance, número de aplicaciones o direcciones, días de trabajo, reuniones, nueva prueba de verificación e informe ejecutivo.
- **Qué se cobra aparte**: horas adicionales, atención de incidentes fuera del contrato, análisis forense, ampliaciones de alcance.
- **Plazo mínimo y condiciones de salida**, en los servicios mensuales.
- **Cómo se calculó**: un proveedor que no entendió tu alcance no puede darte un precio responsable.

Cuidado con las ofertas muy por debajo del resto: a veces corresponden a un escaneo automático presentado como ethical hacking. Un escaneo es útil, pero no reemplaza el trabajo de una persona que piensa como atacante.

10

Señales de alerta

- Promete seguridad total o sistemas «imposibles de hackear».
- Quiere empezar sin una autorización por escrito ni un alcance definido.
- No puede decirte quién hará el trabajo ni mostrarte un informe de ejemplo.
- Vende con miedo y urgencia en vez de explicar riesgos concretos.
- Pide accesos de administrador amplios sin explicar para qué.
- Su «24/7» es un correo automático o un formulario de contacto.
- No tiene un procedimiento para avisarte si encuentra algo crítico durante el trabajo.
- Se niega a dejar por escrito los tiempos de respuesta o las condiciones de confidencialidad.
- No pregunta nada sobre tu negocio y ofrece lo mismo a todos.
- No tiene a quién recurrir si el caso se complica: un incidente serio puede requerir análisis forense, investigación a fondo y apoyo con los reportes legales, y conviene saber desde antes si tu proveedor puede hacerlo.

Preguntas para la primera reunión

1. ¿Qué entendieron de lo que necesitamos y qué nos proponen?
2. ¿Quiénes harán el trabajo y qué experiencia tienen en sistemas como los nuestros?
3. ¿Trabajan con subcontratistas?
4. ¿Qué certificaciones tiene la empresa y cuál es su alcance?
5. ¿Qué certificaciones tienen las personas asignadas a nuestro proyecto?
6. ¿Qué metodología usan?
7. ¿Pueden mostrarnos un informe de ejemplo?

8. ¿Está incluida la nueva prueba para verificar las correcciones?
9. Si el servicio es 24/7, ¿quién está mirando a las 3 de la mañana y qué puede hacer?
10. ¿Cuáles son los tiempos de notificación, respuesta y contención por nivel de gravedad, y cómo se miden?
11. ¿Qué pasa si no cumplen esos tiempos?
12. ¿Qué hacen si encuentran algo crítico durante el trabajo?
13. Si tenemos un incidente grave, ¿pueden hacer el análisis forense y acompañarnos con los reportes a las autoridades?
14. ¿Cómo protegen la información que les entregamos y qué hacen con ella al terminar?
15. ¿Qué necesitan de nuestro equipo y cuánto tiempo nos va a tomar?
16. ¿Nos acompañan durante la corrección?
17. ¿Qué incluye el precio y qué se cobra aparte?
18. ¿Pueden darnos referencias de clientes parecidos a nosotros?

Tabla para comparar propuestas

Califica cada propuesta de 1 a 5 en cada criterio, multiplica por el peso y suma. Ajusta los pesos a tu caso: si contratas monitoreo, la cobertura y los tiempos de respuesta deberían pesar más; si contratas una revisión puntual, el equipo y el informe.

CRITERIO	PESO	PROV. A	PROV. B	PROV. C
Comprensión de tu necesidad y alcance propuesto	10 %			
Experiencia del equipo asignado en sistemas como los tuyos	20 %			
Certificaciones de la empresa y de las personas, verificadas	10 %			
Calidad del informe de ejemplo	15 %			
Cobertura y tiempos de respuesta por escrito	10 %			
Capacidad de respuesta ante incidentes graves y análisis forense	5 %			
Confidencialidad, tratamiento de datos y contrato	5 %			
Acompañamiento en la corrección y nueva prueba incluida	10 %			
Precio total, comparado sobre el mismo alcance	15 %			
Total	**100 %**			

Cómo trabajamos en Tinary

Escribimos esta guía con las mismas preguntas que esperamos que nos hagas a nosotros:

- **Alcance claro desde el inicio.** Acordamos por escrito qué se revisa, los entregables, los plazos y la autorización antes de empezar.
- **Hallazgos comprobados y priorizados.** Recibes un informe claro para decidir, una guía paso a paso para tu equipo técnico y la prueba de que quedó corregido.
- **Acompañamiento real.** Trabajamos con tu dirección y tus equipos técnicos, o junto a tus proveedores, hasta que las fallas quedan cerradas.
- **Vigilancia todo el año.** Monitoreo SOC 24/7, con certificación ISO 27001 y Wazuh Gold Partner.

- **Respaldo cuando el caso se complica.** Respuesta a incidentes, análisis forense e investigación a fondo, con apoyo en los reportes a las autoridades y en la comunicación con tus clientes.

ANTES DE CONTRATAR

Haznos estas mismas preguntas.

Cuéntanos qué necesitas proteger y te respondemos con un primer diagnóstico y los siguientes pasos.

Escríbenos a contacto@tinary.cl →

Esta guía es informativa y no reemplaza la asesoría legal para la contratación de un servicio. Las referencias legales corresponden a la normativa chilena a noviembre de 2026. Los nombres de certificaciones y metodologías pertenecen a sus respectivos emisores.