redcricket

Evaluación de proveedores

Plantilla de cuestionario uniforme, con ficha de clasificación y registro de evidencia.

Úsala tal cual o adáptala. No requiere cuenta ni registro.

Cómo usarla

Un cuestionario sirve si es **el mismo para todos**. Uno distinto por proveedor no se puede comparar, y lo que una auditoría quiere ver es precisamente el criterio uniforme.

1. **Levanta el inventario por acceso, no por gasto.** La lista de contabilidad ordena a los proveedores por lo que cuestan. Esta los ordena por lo que pueden ver o hacer. Empieza por los que tocan datos de clientes, sistemas productivos o correo.
2. **Clasifícalos en tres niveles, no en siete.** Crítico, relevante, marginal. Una escala más fina se ve más seria y se abandona más rápido.
3. **Manda el mismo cuestionario a todos.** El valor está en que sea igual, no en que sea largo.
4. **Guarda la respuesta con fecha y autor.** Una respuesta sin fecha no prueba nada: no se sabe si describe la situación de hoy o la de hace tres años. La fecha es la mitad de la evidencia.
5. **Define cuándo se repite.** Anual para los críticos, al renovar para el resto. Escrito, aunque sea una línea.

Ficha del proveedor

PROVEEDOR

SERVICIO QUE PRESTA

CONTACTO

CORREO

FECHA DE ALTA

RESPONSABLE INTERNO

¿A qué accede?

☐ Datos de clientes ☐ Sistemas productivos ☐ Correo ☐ Infraestructura de red ☐ Instalaciones

☐ Ninguno de los anteriores

Criterio de nivel

Nivel	Cuándo aplica
Crítico	Puede ver o modificar datos de clientes, o entrar a sistemas productivos. Si falla, la operación o la confianza se ven afectadas el mismo día.
Relevante	Accede a información interna o a sistemas de soporte. Un problema suyo se nota, pero hay margen para reaccionar.
Marginal	No toca información sensible ni sistemas. Se registra para que el inventario esté completo.

NIVEL ASIGNADO

QUIÉN LO ASIGNÓ

JUSTIFICACIÓN BREVE

Cuestionario

Este es el cuestionario que se envía al proveedor. Mándalo igual a todos: el valor está en poder comparar las respuestas.

A · Acceso: quién entra y a qué

01 ¿A qué sistemas o información nuestra tiene acceso tu equipo?

02 ¿Cuántas personas de tu equipo tienen ese acceso, y quién autoriza que se otorgue?

03 Cuando alguien deja tu empresa o cambia de puesto, ¿en cuánto tiempo se le retira el acceso a nuestros sistemas?

B · Credenciales

04 ¿El acceso a nuestros sistemas usa autenticación de múltiples factores?

05 ¿Las credenciales son individuales o se comparten entre varias personas?

06 ¿Dónde y cómo se guardan esas credenciales?

C · Protección de la información

07 ¿Nuestra información se cifra en tránsito y en almacenamiento?

08 ¿En qué país o región se almacena?

09 Al terminar el contrato, ¿qué se hace con nuestra información y en qué plazo?

D · Continuidad

10 ¿Con qué frecuencia se respalda la información relacionada con nuestro servicio?

11 ¿Se ha probado restaurar un respaldo en los últimos doce meses?

12 Si tu servicio se interrumpe, ¿en cuánto tiempo se restablece normalmente?

E · Incidentes

13 ¿Existe un procedimiento escrito de respuesta a incidentes?

14 Si ocurre un incidente que afecte nuestra información, ¿en cuánto tiempo se comprometen a avisarnos?

15 ¿Han tenido en los últimos veinticuatro meses un incidente que afectara a clientes?

> **Sobre la pregunta 15:** una respuesta afirmativa no descalifica a nadie — casi toda organización con operación real ha tenido alguno. Lo que sí es señal es no poder contestarla.

F · Cumplimiento y terceros

16 ¿Cuentan con certificación vigente, o preparación en curso, en algún marco de seguridad (ISO 27001, SOC 2, PCI DSS u otro)? Si la tienen, adjunten la constancia.

17 ¿Subcontratan a terceros que también tendrían acceso a nuestra información? ¿Cuáles?

18 ¿Quién es la persona responsable de seguridad o de protección de datos con quien podemos escalar un tema? Nombre, cargo y correo.

Para quien responde

RESPONDIDO POR

CARGO

CORREO

FECHA

Señales de atención

Ninguna de estas respuestas descalifica por sí sola. Todas ameritan una segunda conversación antes de firmar o renovar.

- No hay autenticación de múltiples factores sobre sistemas que tocan datos de clientes **(4)**.
- Credenciales compartidas entre varias personas **(5)**.
- El retiro de accesos no tiene plazo definido **(3)**.
- No se ha probado una restauración de respaldo **(11)**.
- No hay plazo comprometido para notificar un incidente **(14)**.
- Hay subcontratistas con acceso que no estaban declarados en el contrato **(17)**.
- No hay una persona con nombre a quien escalar **(18)**.

Registro de la evaluación

PROVEEDOR

NIVEL

FECHA DE ENVÍO

FECHA DE RESPUESTA

SEÑALES DE ATENCIÓN DETECTADAS

Decisión

☐ Se aprueba ☐ Se aprueba con condiciones ☐ Se pide más información ☐ No se aprueba

QUIÉN DECIDIÓ

FECHA DE PRÓXIMA REVISIÓN

Dónde encaja Red Cricket

Los cinco pasos se pueden hacer con esta plantilla y una carpeta. Lo que se rompe a mano es el sexto mes: el inventario se desactualiza, las respuestas quedan en el correo de alguien y nadie se entera hasta la siguiente auditoría.

Riesgo de Proveedores, el módulo ancla de Red Cricket Cloud, hace este mismo trabajo de forma sostenida: inventario, cuestionario que se envía por liga —el proveedor no necesita crear cuenta—, evaluación por proveedor, recordatorios de renovación y evidencia exportable. Está en el tier de entrada, dentro de la misma suscripción que los otros siete módulos.

Se prueba treinta días, sin tarjeta: cloud.redcricket.net/es/register
El método completo, en cinco pasos: redcricket.net/es/blog/como-demostrar-que-evaluaste-a-tus-proveedores

Esta plantilla es material de referencia y no constituye asesoría legal ni una evaluación de cumplimiento. Red Cricket no certifica: prepara la evidencia para quien sí lo hace.