ZetTateK

GUÍA PARA DIRECTIVOS · 2026

¿SOC propio o administrado? Los números reales.

¿Cuánto cuesta de verdad vigilar su red las 24 horas en Latinoamérica? ¿De qué se compone cada modelo? ¿Cómo decidir con datos antes de presupuestar 2027?

Ciberseguridad · SOC 24/7 · Venezuela · México · LATAM · USA
www.zettatek.com · Segunda edición, agosto de 2026

© 2026 ZetTateK. Puede compartir este documento completo y sin modificar.
Si cita alguno de sus datos, indique la fuente: zettatek.com/guia-soc-propio-o-administrado

>_ ANTES DE EMPEZAR

¿Para quién es esta guía?

Si usted dirige la tecnología o las finanzas de una empresa con más de 100 empleados y le han pedido evaluar "algo de ciberseguridad" para el próximo presupuesto, esta guía le ahorra semanas de cotizaciones confusas.

No encontrará aquí terminología innecesaria ni advertencias alarmistas. Encontrará la aritmética: cuántas personas hacen falta para cubrir 24 horas, de qué conceptos se compone el costo de cada modelo, qué gastos aparecen después del arranque y en qué punto conviene cada camino.

Las tres preguntas que responde

1. ¿De qué se compone el costo propio?

La cuenta completa: turnos, salarios, recargos legales, licencias, formación, espacio y el tiempo hasta que el equipo funciona de verdad.

2. ¿Cómo se cobra el administrado?

Las modalidades habituales, qué debe quedar escrito en el contrato y por qué su precio no se desglosa igual.

3. ¿Cuál conviene en mi caso?

Un criterio de decisión según tamaño, sector y madurez, incluido el modelo mixto que casi nadie explica.

Y un extra

Diez preguntas para evaluar a cualquier proveedor, incluidos nosotros, y una lista de verificación final.

> **Una advertencia honesta sobre las cifras**
>
> Los montos de esta guía son **rangos de referencia para planificación**, construidos con costos de mercado en Latinoamérica a mediados de 2026. No son una cotización.
>
> Y algo más importante: **cada cuenta está atada a un escenario declarado**, porque sin decir de qué tamaño de empresa hablamos, un rango orienta menos de lo que confunde. Cuando aparece un número, aparece también el supuesto del que depende.
>
> **No encontrará aquí el precio de nuestros servicios.** Darle una cifra sin conocer su alcance sería adivinar, y usted la tomaría como compromiso. Lo que sí encontrará es qué variables mueven ese precio, para que pueda comparar propuestas con criterio.

Primero, ¿qué es exactamente un SOC?

Un SOC (Centro de Operaciones de Seguridad) es el equipo y la tecnología que vigilan de forma continua lo que ocurre en sus sistemas, distinguen lo normal de lo sospechoso y actúan cuando algo va mal.

La analogía útil es la de un centro comercial: las cámaras son los sensores instalados en su red; la sala de monitoreo con vigilantes despiertos las 24 horas es el SOC; y la brigada que baja a actuar cuando suena una alarma es la respuesta a incidentes. Un antivirus y un firewall son la cerradura y la alarma: necesarios, pero nadie los está mirando de madrugada.

> **Lo que un SOC no es:** no es un antivirus con otro nombre, no es un informe mensual en PDF, y no es una persona del equipo de TI que además revisa alertas cuando puede.

>_ CAPÍTULO 1

Las tres opciones reales

Toda empresa que se plantea esto termina en uno de tres caminos. Conviene nombrarlos bien antes de compararlos.

Opción A · SOC propio (interno)

Usted contrata analistas, compra las licencias, define los procesos y opera. Control total, costo total y responsabilidad total. Tiene sentido cuando la seguridad es parte del núcleo del negocio, hay volumen suficiente para justificar el equipo y existe capacidad de atraer y retener talento especializado.

Opción B · SOC administrado (MSSP)

Un proveedor especializado opera el servicio con su propio equipo, sus procesos y sus herramientas, bajo un contrato con niveles de servicio y una cuota mensual. Usted mantiene el control de las decisiones y delega la operación continua. Es el modelo dominante en empresas medianas y grandes que no viven de la seguridad.

Opción C · Modelo mixto (híbrido)

Su equipo interno atiende el horario laboral y el proveedor cubre noches, fines de semana y feriados. O bien el proveedor opera mientras el equipo interno madura y va asumiendo funciones. Es el camino más frecuente cuando ya existe un equipo de TI sólido pero pequeño.

> **La opción que nadie declara pero muchos eligen**
>
> La cuarta alternativa es no hacer nada y confiar en que el antivirus y el firewall alcanzan. Es gratuita hasta el día en que deja de serlo. Este documento no busca asustar a nadie, pero omitirla sería deshonesto: es, con diferencia, la decisión más común y la más costosa a mediano plazo.

¿Qué debe cubrir cualquiera de los tres?

Función	Significado en la práctica
Monitoreo 24/7	Alguien observa los eventos de seguridad todo el tiempo, no solo en horario de oficina.
Detección	Separar el ruido de lo relevante: de miles de eventos diarios, identificar los que importan.
Respuesta	Actuar: aislar un equipo comprometido, bloquear una cuenta, cortar una conexión.
Gestión de vulnerabilidades	Saber qué puertas están abiertas antes de que alguien entre por ellas.
Cacería de amenazas	Buscar activamente al intruso que ya está dentro y aún no ha hecho ruido.
Evidencia y reportes	Demostrar ante auditores, casa matriz o aseguradora que el control existe y funciona.

Si una propuesta no cubre las seis, no está comparando lo mismo.

>_ CAPÍTULO 2

De qué se compone el costo propio

Casi todas las cuentas fallan en lo mismo: se calcula el costo de las herramientas y se subestima el de la cobertura continua. Empecemos por ahí.

La aritmética de las 24 horas

Cubrir 24 horas los 7 días exige tres turnos diarios. Un año tiene 8.760 horas y una persona trabaja alrededor de 1.800 horas efectivas, descontando vacaciones, feriados, capacitación y ausencias.

8.760 ÷ 1.800 = 4,9 personas

Solo para tener un puesto ocupado de forma permanente

Con relevos, vacaciones simultáneas y rotación, la cifra realista es de **seis analistas más un responsable** con experiencia que dirija el equipo y escale los casos graves.

Ese es el piso, y no es una recomendación de proveedor: es una división. Es el único número de esta guía que no depende de su país, su tamaño ni su sector.

Los ocho conceptos del costo propio

Cuando alguien dice que un SOC propio cuesta los salarios, se queda en la mitad. La lista completa es esta:

#	Concepto	Razón por la que no se recorta
1	Siete salarios	Seis analistas por turnos más un responsable senior
2	Recargos por horario	El trabajo nocturno y en festivos tiene recargos legales en México y Venezuela. No son negociables
3	Licenciamiento de plataforma	Correlación de eventos. Se paga por volumen de datos o por equipo, así que crece con la empresa
4	Herramientas complementarias	Inteligencia de amenazas, análisis, orquestación de respuesta
5	Formación y certificaciones	Las técnicas de ataque cambian cada trimestre. Sin actualizar, el equipo detecta lo del año pasado
6	Almacenamiento de registros	La retención que exige una auditoría cuesta, y sube todos los meses
7	Espacio e infraestructura	Sala, pantallas, energía respaldada y más de un enlace. Un centro que se queda sin luz deja de monitorear
8	Suplencias y rotación	Vacaciones, incapacidades y renuncias. Alguien cubre esas horas, y el reemplazo tarda meses en conocer la red

> Los conceptos **2, 6, 7 y 8** casi nunca aparecen en una comparación. Y son justo los que no se pueden negociar: el primero es ley, el segundo lo exige la auditoría, el tercero es física y el cuarto es la vida.

La cuenta anual, con su escenario declarado

Lea esto antes de la tabla

La cuenta de abajo corresponde a **un escenario concreto: una empresa de 300 a 600 empleados, con entre 250 y 500 equipos y servidores monitoreados, sin operación en varios países.**

Si su empresa es más pequeña, las líneas 3, 4 y 6 bajan porque dependen del volumen. Si es más grande o tiene sedes en varios países, suben, y probablemente necesite más de siete personas. **Las líneas 1 y 2 no bajan nunca**, porque el año siempre tiene 8.760 horas.

Concepto	Rango anual (USD)	Supuesto del que depende
6 analistas de seguridad por turnos	150.000 a 240.000	Costo cargado de 25 a 40 mil por analista
1 líder o especialista senior	45.000 a 70.000	Perfil escaso en la región
Licenciamiento de plataforma	25.000 a 90.000	Volumen de datos ingeridos
Herramientas complementarias	12.000 a 35.000	Alcance de inteligencia y orquestación
Formación y certificaciones	8.000 a 20.000	Tamaño del equipo
Infraestructura y almacenamiento	6.000 a 25.000	Retención exigida por su auditoría
Total anual estimado	**246.000 a 480.000**	**Sin rotación ni puesta en marcha**

El número que debe verificar usted

Todo el total cuelga de un solo supuesto: **el costo cargado de 25 a 40 mil dólares por analista al año.** Ese dato no es igual en Monterrey que en Caracas, y usted lo conoce mejor que nosotros.

Tome el costo cargado real de un perfil equivalente en su empresa, multiplíquelo por siete, y sume las cuatro líneas de tecnología. **Ese número le va a servir mucho más que el nuestro, porque es el suyo.**

La distinción que decide, y no es el monto

Hay una diferencia que pesa más que cualquier cifra, y es contable. Un SOC propio es **inversión más gasto corriente**: la sala, las pantallas, la energía respaldada y las licencias iniciales son capital; los salarios y las suscripciones son gasto. Van por dos vías distintas del presupuesto. Un SOC administrado es **solo gasto corriente**: una cuota, una línea.

Y no se aprueban igual. La inversión de capital exige comité, ciclo presupuestario anual y competir con la ampliación de la planta o la renovación de la flota. Si el ciclo del próximo año ya se cerró, el proyecto espera doce meses por calendario, no por falta de voluntad.

Ahí está la explicación de algo que confunde a mucha gente: los 12 a 18 meses del modelo propio no son solo formación del equipo. Buena parte de ese tiempo se va en conseguir la aprobación, ejecutar la compra y montar el espacio, antes de que el primer analista se siente a mirar una pantalla.

Y lo que casi nunca se presupuesta

El tiempo hasta que funciona
Entre 12 y 18 meses desde la contratación hasta que el equipo detecta con precisión en una red concreta. Ese período se paga completo y protege poco.

La rotación
El analista de seguridad es de los perfiles más disputados del mercado. Cada salida cuesta reclutamiento, meses de vacío y conocimiento que se va con la persona.

La fatiga de alertas
Sin afinamiento constante, el equipo recibe miles de avisos irrelevantes. Termina ignorándolos, y ahí es donde se pierden los incidentes reales.

La dependencia de una persona
En equipos pequeños el conocimiento se concentra en quien lleva más tiempo. Si esa persona renuncia, la capacidad real cae de golpe.

Conclusión del capítulo

Para el escenario declarado (300 a 600 empleados, 250 a 500 equipos), **un SOC propio con cobertura continua difícilmente baja de 250.000 dólares anuales en Latinoamérica, y no protege plenamente hasta el segundo año.**

Es una decisión perfectamente válida. Pero debe tomarse sabiendo esto, y habiendo hecho la cuenta con los costos reales de su propia nómina.

Antes de pasar de página, haga este ejercicio

No hace falta pedir una cotización para saber en qué punto está hoy. Responda tres cosas:

1. **¿Cuántas personas de su equipo pueden atender una alerta de seguridad de madrugada?** No recibir el correo: atenderla, entender qué pasa y decidir qué hacer.
2. **Multiplique por 1.800.** Ese es el total de horas que su equipo puede cubrir al año.
3. **Compare con 8.760.**

Si su respuesta a la primera pregunta es	Su cobertura real al año es
1 persona	20%
2 personas	41%
3 personas	61%
5 personas	Más del 100%, y ahí la pregunta cambia: ¿están afinando la detección o solo apagando fuegos?

La diferencia entre lo que uno cree cubrir y lo que cubre de verdad es exactamente el hueco por donde entra el problema.

>_ CAPÍTULO 3

El costo de un SOC administrado

El modelo administrado reparte entre muchos clientes el costo del equipo, las licencias y los procesos. Por eso la cuota mensual es una fracción del costo de construirlo.

¿Cómo se cobra habitualmente?

Modalidad	Funcionamiento	Referencia
Por equipos monitoreados	Cuota por servidor y estación protegida	La más común
Por volumen de datos	Según los registros que ingiere la plataforma	Frecuente en grandes
Cuota fija mensual	Alcance definido, precio predecible	Recomendada

¿Por qué este capítulo no trae un desglose como el anterior?

Sería fácil poner aquí una tabla de seis líneas y sumarlas. Pero sería falso, y conviene explicar por qué.

El precio de un servicio administrado **no es la suma de los costos del proveedor**. Es un precio de mercado que refleje que la infraestructura, las licencias y el equipo se reparten entre muchos clientes a la vez. Nadie fuera del proveedor puede desglosarlo con honestidad, y quien le presente ese desglose probablemente se lo esté inventando.

Lo que sí puede exigir es que el precio venga con el alcance escrito: cuántos equipos, qué horario, qué significa responder, qué tiempos de compromiso y qué pasa si no se cumplen. Un precio sin alcance no se puede comparar con nada.

¿Qué determina el precio que le van a cotizar?

Aquí tampoco encontrará una cifra, y por la misma razón: cualquier número que le diéramos sin conocer su alcance sería adivinar, y usted lo tomaría como compromiso. Lo que sí le sirve es saber de qué depende, para que pueda negociar con criterio:

Variable	Efecto en el precio
Cantidad de equipos y servidores	Es el factor principal en la modalidad más común. Cuéntelos antes de pedir propuestas
Horario contratado	Cubrir 24/7 no cuesta lo mismo que cubrir noches y fines de semana sobre un equipo interno que atiende el día
Alcance de la respuesta	Avisarle cuesta menos que actuar por usted. Es la diferencia más grande y la que menos se lee en los contratos
Retención de registros	Guardar seis meses no cuesta lo mismo que guardar dos años. Lo define su auditoría, no el proveedor
Duración del compromiso	Contratos de 12 a 36 meses. A más plazo, mejor precio, y menos flexibilidad si algo no funciona

Pida siempre propuesta escrita para su caso. Si un proveedor le da un precio antes de preguntarle cuántos equipos tiene y qué horario necesita, ese precio va a cambiar después. El nuestro se calcula al terminar el diagnóstico, cuando ya sabemos de qué estamos hablando.

Comparación lado a lado

Criterio	SOC propio	SOC administrado
Naturaleza del gasto	**Inversión más gasto corriente**	**Solo gasto corriente**
Vía de aprobación	Comité y ciclo anual de capital	Partida existente del área
Personas en su nómina	7	0
Lo que determina el monto	Siete salarios, volumen de datos y retención exigida	Cantidad de equipos, horario y alcance de la respuesta
Tiempo hasta operar	12 a 18 meses	2 a 6 semanas
Cobertura nocturna	Depende de su plantilla	Incluida por contrato
Riesgo por rotación	Alto, recae en usted	Lo asume el proveedor
Control de decisiones	Total	Total, con operación delegada
Conocimiento del negocio	Máximo desde el inicio	Se construye en el arranque
Evidencia para auditoría	Debe construirla	Suele venir incluida
Escalar a otro país o sede	Repetir la inversión	Ampliar el contrato

La cuenta del modelo propio, con su escenario declarado, está en el capítulo 2. El precio del modelo administrado depende de las variables del capítulo 3 y se cotiza por caso.

¿Cuándo conviene cada uno?

Conviene el propio si

La seguridad es parte del producto que vende, maneja información sujeta a restricciones que impiden delegar, tiene más de mil empleados y puede sostener un equipo especializado a largo plazo.

Conviene el administrado si

Tiene entre 100 y 1.000 empleados, un área de TI pequeña, presión de auditoría o de su casa matriz, y necesita cobertura continua este trimestre y no el año próximo.

Y el punto medio, que suele ser la mejor decisión

El modelo mixto permite empezar con cobertura completa desde el primer mes mientras su equipo interno se forma. Si más adelante decide internalizar, lo hará con procesos probados y con su gente ya entrenada, en lugar de aprender a costa de incidentes reales.

> Tiene además una ventaja presupuestaria que casi nadie menciona: **permite empezar sin pedir inversión de capital**. Se arranca como gasto corriente, se demuestra el valor con operación real, y la conversación sobre invertir en un equipo propio se tiene el año siguiente con datos en la mano en lugar de con una presentación.

Tres errores que vemos repetirse

1. **Comparar propuestas con alcances distintos.** Una cubre horario laboral y la otra 24 horas, y se comparan los precios como si fueran lo mismo.
2. **Presupuestar solo el primer año.** El modelo propio es más caro en el año dos y tres, cuando llegan la rotación y las renovaciones de licencia.
3. **Contratar por miedo y no por criterio.** Después de un susto se firma rápido y mal. La decisión buena se toma cuando todavía no hace falta.

>_ CAPÍTULO 4

Diez preguntas para evaluar a cualquier proveedor

Incluidos nosotros. Si una respuesta es vaga, insista. Un buen proveedor responde estas diez sin incomodarse.

1. ¿Quién vigila a las tres de la mañana y desde dónde?

Confirme si es personal propio o subcontratado, y en qué idioma y huso horario opera.

2. ¿En cuánto tiempo detectan y en cuánto responden?

Pida los compromisos por escrito y qué ocurre si no se cumplen.

3. ¿Qué significa exactamente "responder" en su contrato?

No es lo mismo avisarle que actuar por usted. Que quede explícito.

4. ¿Qué tecnología usan y quién es dueño de la licencia?

Si el servicio termina, ¿se queda usted sin plataforma?

5. ¿Dónde se almacenan mis registros y por cuánto tiempo?

Relevante para auditoría y para requisitos de su sector.

6. ¿Qué información mía ven y cuál no?

Debe estar delimitado por escrito y respaldado por confidencialidad.

7. ¿Cómo es el arranque y cuánto demora?

Un servicio serio detalla las etapas de puesta en marcha.

8. ¿Qué reportes recibo y con qué frecuencia?

Pida ver un informe real, anonimizado, antes de firmar.

9. ¿Puedo hablar con un cliente actual de mi sector?

La respuesta a esta pregunta dice mucho, cualquiera que sea.

10. ¿Qué pasa si quiero terminar el contrato?

Permanencias, penalizaciones y devolución de información.

Lista de verificación antes de decidir

Si puede marcar las diez, está listo para comparar propuestas de verdad. Si le faltan tres o más, todavía no está comparando: está adivinando.

- [ ] Sé cuántos equipos y servidores hay que monitorear
- [ ] Sé qué exige mi regulador, mi auditor o mi casa matriz, por escrito
- [ ] Calculé cuánto cuesta una hora de operación detenida en mi empresa
- [ ] Hice la cuenta de las 8.760 horas con el costo real de mi propia nómina
- [ ] Comparé al menos dos propuestas con el mismo alcance
- [ ] Verifiqué quién cubre noches, fines de semana y feriados
- [ ] Tengo los tiempos de detección y respuesta por escrito
- [ ] Sé qué ocurre con mis registros si termina el contrato
- [ ] Definí quién decide internamente ante un incidente grave
- [ ] Sé si mi presupuesto admite inversión de capital este año o solo gasto corriente

> **La última pregunta es la que más suele cambiar la decisión**
> Muchas empresas descubren, al llegar a ese punto, que el debate técnico entre modelos era secundario: la respuesta la definía el calendario presupuestario, no la arquitectura.

>_ EL SIGUIENTE PASO

Antes de presupuestar, conviene saber dónde está hoy

Nuestro diagnóstico ejecutivo es gratuito y no invasivo: no instalamos nada ni accedemos a sus sistemas.

Incluye: revisión externa de su superficie expuesta, 30 minutos con un especialista y un informe con los cinco riesgos principales, entregado en siete días.

zettatek.com/diagnostico-seguridad

Y si prefiere hacer primero su propia cuenta

Tome el costo cargado real de un analista en su empresa, multiplíquelo por siete, sume las cuatro líneas de tecnología del capítulo 2, y compare con lo que le cuesta hoy no tener a nadie mirando de madrugada. Ese número es el suyo, y vale más que cualquiera de los nuestros.



ZetTateK · Ciberseguridad y SOC administrado 24/7 · Venezuela · México · LATAM · USA.
Segunda edición, agosto de 2026. Las cifras del capítulo 2 corresponden al costo de operar un SOC propio y son rangos de referencia para planificación, atados al escenario declarado en ese capítulo (empresa de 300 a 600 empleados con 250 a 500 equipos monitoreados), construidos con costos de mercado en Latinoamérica a mediados de 2026. No constituyen una cotización ni asesoría financiera, y varían según país, tamaño de la red, nivel de servicio y regulación aplicable. Esta guía no publica precios de nuestros servicios: se cotizan por caso, con alcance escrito, al terminar el diagnóstico. Trabajamos alineados a marcos como ISO/IEC 27001 y MITRE ATT&CK.