

Expel opera las herramientas que tú compraste. TecnetSOC trae todo incluido y lo opera por ti, 24/7.

Con Expel, compras y renuevas las licencias de tu EDR y tu SIEM, y sus analistas reciben acceso a tus consolas y a tus equipos. TecnetSOC trae su plataforma, no pide credenciales de tus consolas y puedes probar Response 30 días.



41

capacidades donde TecnetSOC va más allá

9

capacidades en las que coincidimos

0

capacidades donde Expel supera a TecnetSOC

De las 50: 41 donde vamos más allá y 9 en las que coincidimos

Misma lista de 50 capacidades y mismo criterio para TecnetSOC y Expel: la oferta más completa publicada de cada uno, con la fuente de cada dato. [Cómo lo hicimos](#)

Pedir la prueba de Response por 30 días

o empieza gratis con Visibility, hasta 10 dispositivos

tecnetone.com/servicios/soc-as-a-service

- ✓ SOC agéntico 24/7 en LATAM, EE.UU. y Europa
- ✓ Español nativo y atención multiidioma
- ✓ Compuerta Humana en lo crítico
- ✓ Operación certificada ISO/IEC 27001:2022
- ✓ Crítico: aviso e inicio de investigación en 30 min (objetivo)

Información pública consultada al 29 de septiembre de 2026. Versión 2026.09. Comparativo informativo elaborado por TecnetOne, no afiliado a las marcas mencionadas.

— ANTES DE COMPARAR

Expel es un servicio de SOC administrado que trabaja sobre las herramientas de seguridad que ya tienes; la protección de equipos, el SIEM y el correo los pones tú. Aquí comparamos la oferta más completa publicada de cada uno, capacidad por capacidad.

— LO QUE NOS HACE DISTINTOS

Diferencias que se notan en el día a día

01
Las herramientas las pagas tú

CON EXPEL
Tú compras y renuevas las licencias de tu EDR, tu SIEM y demás herramientas; Expel se conecta por API y opera sobre lo que ya tienes. [\[1\]](#)

CON TECNETSOC
El plan más completo ya trae SIEM con correlación MITRE ATT&CK, EDR/XDR, NDR, IDS/IPS y filtrado web.

02
Te recomienda, tu equipo parchea

CON EXPEL
Recibes recomendaciones de remediación y análisis de causa raíz; aplicar y probar los parches queda en manos de tu equipo. [\[2\]](#)

CON TECNETSOC
El SOC parchea: prioriza por KEV y EPSS, valida en grupo piloto y cierra solo cuando el escáner lo confirma.

03
Sus analistas entran a tus consolas y equipos

CON EXPEL
Tu equipo entrega credenciales y da a sus analistas acceso a la consola de tu EDR y SIEM, incluida la terminal remota en tus equipos. [\[3\]](#)

CON TECNETSOC
Instalas un agente, el resto de la plataforma se despliega sola y no cedas credenciales de administrador.

04
Analistas en EE.UU. y atención en inglés

CON EXPEL
Todos sus analistas trabajan desde EE.UU. y su sitio y documentación están en inglés; no publica atención en español ni operación en LATAM. [\[4\]](#)

CON TECNETSOC
Operamos en LATAM, EE.UU. y Europa con analistas en tu zona horaria, en español nativo y multiidioma.

05
Phishing como complemento aparte

CON EXPEL
Phishing es un complemento que investiga los correos que tus empleados reportan; no publica filtro antispam propio ni simulaciones de phishing para tu personal. [\[5\]](#)

CON TECNETSOC
El plan más completo incluye seguridad de correo (spam, phishing, malware, BEC) y simulaciones de phishing para tu personal.

06
Demo, cotización y pago anticipado

CON EXPEL
Cotizas a la medida y su sitio ofrece demo, sin prueba gratuita publicada; en AWS Marketplace contratas 12 a 36 meses, pago anticipado y sin reembolsos. [\[6\]](#)

CON TECNETSOC
Pagas por dispositivo, Visibility es gratis hasta 10 dispositivos y pruebas Response 30 días en tu entorno real.

— DÓNDE ESTÁ LA DIFERENCIA

Las tres áreas con más diferencia

Detección y respuesta

TecnetSOC **15**

Expel **3**

de 15 capacidades completas en esta área

Exposición y gestión de TI

TecnetSOC **12**

Expel **1**

de 12 capacidades completas en esta área

Operación y servicio

TecnetSOC **14**

Expel **5**

de 14 capacidades completas en esta área

— CAPACIDAD POR CAPACIDAD

TecnetSOC y Expel, lado a lado

Capacidad	TecnetSOC	Expel SOC	Evidencia sobre Expel
✓ Lo ofrece ⊕ Lo ofrece como complemento ⓪ Parcial, limitado o requiere otro contrato ? Sin evidencia pública ✗ No forma parte de su oferta publicada			
Operación y servicio	14 de 14	5 completas +6 parciales	
Centro de operaciones (SOC) 24/7 con analistas humanos	✓	✓	SOC 24×7×365 con analistas humanos y acceso directo a ellos [1]
Agentes de IA que investigan y filtran las alertas antes de pasarlas a un analista	✓	✓	Ruxie y sus agentes de triaje y correlación investigan alertas antes del analista [7]
Compuerta Humana: una persona aprueba cada acción crítica antes de ejecutarse	✓	✓	Analistas validan la amenaza antes de que Ruxie ejecute la contención [1]
Asistente de investigación con IA en el portal, que cita sus fuentes	✓ Neo	⓪	Ruxie como "AI SOC manager"; sin evidencia de asistente conversacional bajo demanda que cite fuentes [8]

Capacidad	TecnetSOC	Expel SOC	Evidencia sobre Expel
Lo ofrece Lo ofrece como complemento No forma parte de su oferta publicada Parcial, limitado o requiere otro contrato Sin evidencia pública			
Operación en LATAM, EE.UU. y Europa, con analistas en tu zona horaria			SOC centrado en Norteamérica; sin operación en LATAM [9]
Analistas, soporte y portal en español nativo			Sin evidencia de analistas ni soporte en español [10]
Reportes para dirección en español y en lenguaje de negocio			Reportes en inglés; sin versión en español [1]
Tiempos de notificación e inicio de investigación publicados por severidad	Crítico: 30 min (objetivo)		Tiempo medio de respuesta de 14 min y objetivo de 5 min citados por terceros; sin compromiso contractual publicado [11]
Resumen ejecutivo cada mañana: lo que pasó en las últimas 24 horas	07:30		Sin evidencia de resumen ejecutivo diario [1]
Reportes automáticos semanales, mensuales, trimestrales y anuales			Solo reporte mensual de métricas; sin semanal, trimestral ni anual publicados [1]
Gerente técnico de cuenta (TAM) asignado y revisiones trimestrales			Gerente de relación dedicado en Premium; revisiones trimestrales sin confirmar [2]
Contacto 24/7 con personas de soporte o seguridad			Atención 24×7 desde la puesta en marcha hasta las preguntas del día a día, con acceso directo a expertos del SOC [2]
Certificación independiente de la operación (ISO 27001 o SOC 2 Tipo II)	ISO/IEC 27001:2022		Certificada ISO 27001, ISO 27701 y SOC 2 Tipo II (Trust Center) [12]
Arranque rápido con un agente de software: la actividad de tus dispositivos, visible en horas	Típico: 2 a 4 horas		Conexión por API en minutos sin agente, pero requiere que el cliente tenga sus propias herramientas [13]
Detección y respuesta	15 de 15	3 completas +9 parciales	
Monitoreo continuo y correlación de eventos (SIEM), alineado con MITRE ATT&CK (marco de referencia de técnicas de ataque)			Correlación en Workbench y Managed SIEM sobre Sentinel o Splunk del cliente [14]
Protección avanzada en cada equipo (EDR/XDR): malware, ransomware y explotación de vulnerabilidades			Sin EDR propio; opera sobre CrowdStrike, Defender, SentinelOne del cliente [11]
Filtrado web en el equipo			Sin filtrado web propio en el equipo [1]
Detección de intrusos (IDS/IPS)			Monitorea alertas de red de firewalls o sensores de terceros; sin IDS propio [1]
Detección de amenazas en la red interna (NDR)			Cobertura de red solo mediante herramientas de terceros integradas [1]
Investigaciones documentadas y enriquecidas con inteligencia de amenazas			Investigaciones enriquecidas con inteligencia y trazabilidad completa en Workbench [1]
Gestión de incidentes con bitácora y tiempo de atención medido por caso			Workbench registra cada acción; reporte mensual con MTTD y MTTR [1]
Respuesta con aislamiento de equipos y bloqueo de direcciones IP			Remediación automática: aislar equipo, deshabilitar cuenta y bloquear, mediante las herramientas del cliente [11]
Respuesta a incidentes con análisis de causa raíz			Respuesta forense completa aparte o por contrato previo, según un directorio independiente; sin confirmación oficial [9]
Postura de identidad: MFA, cuentas privilegiadas y acceso condicional			Detección en identidad (Okta, Entra); sin gestión de postura ni cuentas privilegiadas [1]
Zero Trust: DNS seguro, acceso a aplicaciones y control de aplicaciones no autorizadas (shadow IT)			Sin DNS seguro, acceso Zero Trust ni control de shadow IT [1]
Seguridad en la nube: alertas y postura			Detección en Azure, AWS, GCP y OCI; postura de nube no evidenciada [1]
Seguridad de correo: spam, phishing, malware y fraude por suplantación (BEC)			Triaje del buzón de phishing reportado; sin antispam ni cuarentena propios [5]
Concientización: simulaciones de phishing y entrenamiento con métricas			Sin simulaciones de phishing ni entrenamiento de usuarios [5]

Capacidad	TecnetSOC	Expel SOC	Evidencia sobre Expel
☒ Lo ofrece ☒ Lo ofrece como complemento ☐ No forma parte de su oferta publicada ☐ Parcial, limitado o requiere otro contrato ☐ Sin evidencia pública			
Recomendaciones de seguridad priorizadas con flujo de aprobación	☒	☐	Recomendaciones de resiliencia en Workbench; sin flujo de aprobación evidenciado [1]
Exposición y gestión de TI	12 de 12	1 completa +1 parcial	
Inventario unificado de activos y de software	☒	☐	Sin inventario propio de activos y software [15]
Vulnerabilidades priorizadas por gravedad y probabilidad de explotación (CVSS, EPSS)	☒	☐	Prioriza con datos de Qualys, Tenable o Rapid7 del cliente; no escanea [15]
Prioridad a las fallas que ya se están explotando (catálogo KEV de CISA)	☒	☒	Vulnerability Prioritization evalúa cada actualización del catálogo KEV y EPSS [16]
Parcheo de sistema operativo y aplicaciones de terceros	☒	☐	No parchea; solo recomienda, el cliente ejecuta [15]
Parcheo operado por el proveedor, con plazos publicados por severidad	☒ Críticos: 48 h (objetivo)	☐	Sin parcheo operado ni tiempos publicados [15]
Verificación de cierre: el escáner confirma que la vulnerabilidad desapareció	☒	☐	Sin verificación de cierre propia [15]
Validación de parches en grupo piloto antes del despliegue	☒	☐	Sin validación de parches en grupo piloto [15]
Superficie de ataque externa: lo que tu empresa expone en Internet, con puntaje de riesgo	☒ Puntaje 0 a 100	☐	Sin superficie de ataque externa (EASM) ni puntaje de exposición [10]
Alertas de dominios que imitan tu marca y de credenciales o claves expuestas	☒	☐	Sin detección de typosquatting ni secretos expuestos [10]
Prueba de penetración (pentest) anual	☒ Anual	☐	Sin pentesting [10]
Gestión remota de equipos (RMM)	☒	☐	Sin RMM [10]
Monitoreo de disponibilidad (NOC)	☒	☐	Sin NOC ni monitoreo de disponibilidad [10]
Respaldo y continuidad	3 de 3	0 completas +0 parciales	
Respaldo de servidores, archivos, bases de datos, máquinas virtuales y Microsoft 365	☒ Complemento	☐	Sin respaldo [10]
Bóveda de respaldo inmutable (no se puede alterar ni borrar), aislada por cliente	☒ Complemento	☐	Sin bóveda inmutable [10]
Recuperación ante desastres con simulacros y tiempo de recuperación (RTO) medido	☒ Complemento RTO medido	☐	Sin recuperación ante desastres [10]
Cumplimiento	6 de 6	0 completas +0 parciales	
Evidencia mensual lista para auditores y aseguradoras	☒ Mensual	☐	Sin evidencia mensual para auditores o aseguradoras [10]
Preparación para ISO 27001, SOC 2 y PCI DSS con controles compartidos	☒ Complemento	☐	Sin plataforma GRC para el cliente [10]
Preparación normativa mexicana: CNBV Fintech, protección de datos (LFPDPPP) y NOM-024	☒ Complemento	☐	Sin normativa mexicana [10]
Gestión de riesgos, controles, declaración de aplicabilidad y auditorías internas	☒ Complemento	☐	Sin gestión de riesgos, SoA ni auditorías internas [10]

Capacidad	TecnetSOC	Expel SOC	Evidencia sobre Expel
✓ Lo ofrece + Lo ofrece como complemento ✗ No forma parte de su oferta publicada	● Parcial, limitado o requiere otro contrato	? Sin evidencia pública	
Portal para tu auditor con sala de evidencias y página pública de confianza (trust center)	+ Complemento	✗	Trust Center es de Expel, no un servicio para el cliente [12]
Continuidad de negocio, riesgo de proveedores y gestión de brechas de datos	+ Complemento	✗	Sin continuidad de negocio ni gestión de proveedores [10]
Cómo se contrata	No suma al conteo		
Precio por dispositivo, con planes que se suman	✓ Por dispositivo	✗	Cotización a la medida por integraciones y volumen, no por dispositivo [17]
Plan gratuito para empezar	✓ Hasta 10 dispositivos	✗	Sin plan gratuito [6]
Prueba gratuita en tu entorno real	✓ 30 días	✗	Solo demo en línea; sin prueba gratuita publicada [18]
Disponible con la marca de tu proveedor de TI	✓	✗	Sin marca del proveedor de TI ni consola multicliente; anunciado como plan futuro según proveedor de seguridad administrada Alert [19]
Cobertura completa	50	9 +16 parciales	

SIGUIENTE PASO

Compruébalo en tu operación

Pruébalo en un entorno real, sin cambiar lo que ya te funciona.

El primer SOC agéntico en español: plataforma, analistas y soporte.

Pedir la prueba de Response por 30 días

Empezar gratis con Visibility (hasta 10 dispositivos)

O habla con un especialista

tecnetone.com/servicios/soc-as-a-service

ASÍ FUNCIONA LA PRUEBA DE RESPONSE

1

Instalas un solo agente

2

Recibes el resumen ejecutivo cada mañana

3

Decides con datos de tu entorno

ANEXO

Metodología y fuentes

Quién y con qué

Lo preparamos en TecnetOne y te mostramos la fuente de cada dato. La lista de capacidades parte del catálogo de TecnetSOC. Evaluamos la oferta más completa publicada de cada proveedor, con sus complementos propios, y la nuestra con el mismo rigor. Usamos solo información pública (sitios oficiales, documentación y comunicados) consultada al 29 de septiembre de 2026.

Qué significa cada estado

Lo ofrece: el proveedor lo entrega, lo opera y responde por ello dentro de su servicio, venga de donde venga la tecnología. Complemento: disponible con costo aparte. Parcial: alcance limitado o que requiere otro contrato u otro operador. Sin evidencia pública: no hay información pública que lo confirme al momento de la consulta; no significa que el proveedor no lo ofrezca. No forma parte de su oferta publicada: su documentación indica que no lo incluye. Lo pone tu equipo: en una herramienta, esa capacidad depende de tu personal, tus turnos y tus tiempos de respuesta, no del proveedor. Si dudamos entre dos valores, elegimos el más conservador.

Cómo corregimos

Un proveedor puede ofrecer algo que no publica: confirmarlo directamente con él. Si ves un dato desactualizado o incorrecto, escríbenos por nuestro formulario de contacto y lo corregimos en la siguiente versión. Revisamos este comparativo cada trimestre y cada vez que cambia la oferta publicada de un proveedor o nuestro catálogo.

Evaluado en TecnetSOC: TecnetSOC en su oferta más completa (plan Compliance, con complementos TecnetProtect y TecnetGRC), catálogo de plataforma soc.catalogo.tecnetone.com y tecnetone.com/servicios/soc-as-a-service, consulta 29 sep 2026. Mismo estándar que los demás. Los complementos con costo aparte cuentan como parte de la oferta, igual que los complementos propios de los demás proveedores.

1. [expel.com/services/managed-detection-response/](#) (Diferencias que se notan en el día a día)

2. [expel.com/mdr-packages/](#) (Diferencias que se notan en el día a día)

3. [docs.expel.io/connect-your-technology/about-integrations/why-expel-...](#) (Diferencias que se notan en el día a día)

4. [expel.com/meet-the-soc-experts/](#) (Diferencias que se notan en el día a día)

5. [expel.com/services/phishing/](#) (Diferencias que se notan en el día a día)

6. [aws.amazon.com/marketplace/pp/prodview-65wyj23v3b3ea](#) (Diferencias que se notan en el día a día)

7. [expel.com/blog/what-we-built-july-2026/](#) (Agentes de IA que investigan y filtran las alertas...)
8. [expel.com/blog/new-ruxie-power-up-ai-detection-agent/](#) (Asistente de investigación con IA en el portal, que...)

9. [mdrproviders.io/providers/expel](#) (Operación en LATAM, EE.UU. y Europa, con analistas en...)

10. [expel.com/](#) (Analistas, soporte y portal en español nativo)

11. [expertinsights.com/endpoint-security/expel-mdr-par](#) (Tiempos de notificación e inicio de investigación...)

12. [security.expel.com/](#) (Certificación independiente de la operación (ISO 27001...))

13. [expel.com/resource/expel-mdr-onboarding-get-up-and-running-in-7-min...](#) (Arranque rápido con un agente de software: la actividad...)
14. [www.prnewswire.com/news-releases/expel-launches-managed-siem-to-hel...](#) (Monitoreo continuo y correlación de eventos (SIEM),...)

15. [expel.com/services/vulnerability-prioritization/](#) (Inventario unificado de activos y de software)

16. [expel.com/blog/mdr-insights-using-vulnerability-data-to-inform-reme...](#) (Prioridad a las fallas que ya se están explotando...)

17. [mdrcost.com/expel-pricing](#) (Precio por dispositivo, con planes que se suman)

18. [expel.com/on-demand-mdr-demo/](#) (Prueba gratuita en tu entorno real)

19. [www.msspalert.com/news/expel-expands-mdr-coverage-across-the-ai-att...](#) (Disponible con la marca de tu proveedor de TI)

Fuentes y fecha. Este comparativo es informativo y lo elabora TecnetOne para que compares, capacidad por capacidad, qué incluye TecnetSOC frente a la oferta más completa publicada de cada proveedor mencionado. La lista de capacidades es un catálogo propio de TecnetOne y puede no incluir todas las funciones de cada proveedor. Usamos solo información pública (sitios oficiales, documentación técnica y comunicados) consultada al 29 de septiembre de 2026; versión 2026.09, con revisión trimestral. "Sin evidencia pública" significa que no hay información pública que lo confirme al momento de la

consulta, no que el proveedor no pueda ofrecerlo de otra forma: confirma cada detalle directamente con él. Las fuentes de cada dato están en el comparativo individual de cada proveedor, enlazado al pie de la tabla.

Marcas. Los nombres y las marcas de terceros pertenecen a sus respectivos dueños y se usan solo para identificarlos y comparar de forma informativa. Ninguno de esos proveedores está afiliado a TecnetOne ni patrocina o avala este documento.

Alcance de TecnetSOC. El respaldo y la plataforma de cumplimiento (TecnetGRC) son complementos con costo aparte. Nuestros tiempos son objetivos de servicio de notificación e inicio de investigación, no de resolución (crítico: 30 minutos, como objetivo). El parcheo está sujeto a las ventanas de mantenimiento acordadas contigo y a las aplicaciones incluidas en tu perfil. El cumplimiento se entrega como preparación y evidencia, no como certificación. TecnetSOC es un servicio de TecnetOne, con operación certificada ISO/IEC 27001:2022, disponible de forma directa o a través de tu proveedor de TI.



Un SOC que habla tu idioma.

[¿Ves un dato desactualizado o inexacto? Escríbenos y lo corregimos.](#)