

Heimdal te vende la plataforma. TecnetSOC te entrega el servicio: seguridad operada por personas e IA, 24/7.

Con Heimdal, lo que su SOC puede hacer se fija al firmar y solo alcanza los módulos que licencias. En TecnetSOC, analistas responden 24/7 en todas las capas de tu plan y una persona aprueba cada acción crítica.



41

capacidades donde TecnetSOC va más allá

9

capacidades en las que coincidimos

0

capacidades donde Heimdal 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 Heimdal: 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 multidioma

✓ 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

Heimdal es una plataforma de seguridad con un servicio de SOC; cada módulo se licencia por separado. 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
Si solo notifica, la contención te toca a ti

CON HEIMDAL
Lo que su SOC puede hacer se pacta por adelantado en MXDR Adapt: si solo autorizas notificar o aconsejar, contener te toca a ti. [\[1\]](#)

CON TECNETSOC
Analistas propios de TecnetOne investigan y responden 24/7; una persona aprueba cada acción crítica antes de ejecutarla, caso por caso.

02
El SOC ve solo lo licenciado

CON HEIMDAL
El SOC solo vigila y contiene dentro de los módulos que licencies y despliegues; cada módulo se paga por separado. [\[1\]](#)

CON TECNETSOC
Pagas por dispositivo con planes acumulativos: cada plan suma capas al anterior y el SOC opera todas las de tu plan 24/7.

03
Otras capas, otros proveedores

CON HEIMDAL
Su catálogo no incluye simulaciones de phishing, superficie de ataque externa, pentesting, monitoreo de disponibilidad ni respaldo: cada uno es otro proveedor y otro contrato. [\[2\]](#)

CON TECNETSOC
La oferta más completa suma phishing simulado, superficie de ataque externa, pentesting anual y NOC; el respaldo inmutable es complemento aparte.

04
Que llegue el parche no es cerrar la vulnerabilidad

CON HEIMDAL
Sus 4 horas miden cuánto tarda el parche del fabricante en llegar a tu equipo; no publica priorización por explotación real (KEV o EPSS). [\[3\]](#)

CON TECNETSOC
El SOC prioriza por KEV y EPSS, valida en piloto y da por cerrada la vulnerabilidad solo cuando el escáner confirma la corrección.

05
SOC en Europa, distribuidor en LATAM

CON HEIMDAL
Su SOC opera desde Europa y en LATAM la relación comercial pasa por un distribuidor, no por el equipo que vigila tus dispositivos. [\[4\]](#)

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

06
Sin normativa mexicana ni plataforma de cumplimiento

CON HEIMDAL
Los reportes de cumplimiento se mapean a marcos como NIS2, DORA e ISO 27001; no incluye plataforma GRC ni normas mexicanas como CNBV o NOM-024. [\[5\]](#)

CON TECNETSOC
Puedes sumar TecnetGRC, con costo aparte por norma: ISO 27001, SOC 2, PCI DSS, CNBV, LFPDPPP, NOM-024 y portal del auditor.

— DÓNDE ESTÁ LA DIFERENCIA

Las tres áreas con más diferencia

Operación y servicio

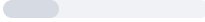
TecnetSOC  **14**

Heimdal  **3**

de 14 capacidades completas en esta área

Detección y respuesta

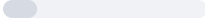
TecnetSOC  **15**

Heimdal  **4**

de 15 capacidades completas en esta área

Exposición y gestión de TI

TecnetSOC  **12**

Heimdal  **2**

de 12 capacidades completas en esta área

— CAPACIDAD POR CAPACIDAD

TecnetSOC y Heimdal, lado a lado

Capacidad		TecnetSOC	Heimdal Plataforma y SOC	Evidencia sobre Heimdal
 Lo ofrece	 Lo ofrece como complemento	 Parcial, limitado o requiere otro contrato	 Sin evidencia pública	
 No forma parte de su oferta publicada				
Operación y servicio		14 de 14	3 completas	
			+8 parciales	
Centro de operaciones (SOC) 24/7 con analistas humanos			MXDR incluye SOC propio 24/7 con analistas, operado desde Europa [5]	
Agentes de IA que investigan y filtran las alertas antes de pasarlas a un analista			AI Wingman Triage anunciado abr 2026, liberación por etapas; sin evidencia de filtrar cada alerta [6]	
Compuerta Humana: una persona aprueba cada acción crítica antes de ejecutarse			MXDR Adapt fija por contrato si el SOC notifica, aconseja o actúa; sin aprobación por acción [7]	

Capacidad	TecnetSOC	Heimdal Plataforma y SOC	Evidencia sobre Heimdal
✓ Lo ofrece + Lo ofrece como complemento ⓪ Parcial, limitado o requiere otro contrato ? Sin evidencia pública ✗ No forma parte de su oferta publicada			
Asistente de investigación con IA en el portal, que cita sus fuentes	✓ Neo	⓪	AI Wingman Assist guía en consola; en despliegue por etapas, sin evidencia de citar fuentes [6]
Operación en LATAM, EE.UU. y Europa, con analistas en tu zona horaria	✓	⓪	SOC en Europa; LATAM solo mediante distribuidor Aufiero, sin operación SOC local [4]
Analistas, soporte y portal en español nativo	✓	⓪	Soporte en español vía distribuidor Aufiero; sin evidencia de analistas SOC en español [8]
Reportes para dirección en español y en lenguaje de negocio	✓	?	Reportes de cumplimiento en inglés; sin evidencia de reportes ejecutivos en español [5]
Tiempos de notificación e inicio de investigación publicados por severidad	✓ Crítico: 30 min (objetivo)	✗	Su blog indica que no publica SLA del SOC [4]
Resumen ejecutivo cada mañana: lo que pasó en las últimas 24 horas	✓ 07:30	?	Sin evidencia pública de un resumen ejecutivo diario [5]
Reportes automáticos semanales, mensuales, trimestrales y anuales	✓	⓪	Reportes centralizados en consola multiempresa; sin evidencia de cadencia semanal a anual [9]
Gerente técnico de cuenta (TAM) asignado y revisiones trimestrales	✓	⓪	Account managers dedicados para partners; sin evidencia de TAM ni revisiones trimestrales [9]
Contacto 24/7 con personas de soporte o seguridad	✓	✓	Su ficha oficial de MXDR incluye soporte al cliente 24x7 como servicio clave, aparte del monitoreo continuo [10]
Certificación independiente de la operación (ISO 27001 o SOC 2 Tipo II)	✓ ISO/IEC 27001:2022	✓	Certificada SOC 2 Tipo II (ISAE 3000); sin ISO 27001 propia publicada [11]
Arranque rápido con un agente de software: la actividad de tus dispositivos, visible en horas	✓ Típico: 2 a 4 horas	⓪	Un solo agente en la nube; no publica tiempo de arranque de datos de actividad [2]
Detección y respuesta	15 de 15	4 completas +10 parciales	
Monitoreo continuo y correlación de eventos (SIEM), alineado con MITRE ATT&CK (marco de referencia de técnicas de ataque)	✓	⓪	XDR correlaciona datos de actividad y mapea MITRE ATT&CK; no es SIEM propio de logs [12]
Protección avanzada en cada equipo (EDR/XDR): malware, ransomware y explotación de vulnerabilidades	✓	✓	Next-Gen Antivirus, EDR/XDR y Ransomware Encryption Protection propios [2]
Filtrado web en el equipo	✓	✓	DNS Security Endpoint filtra tráfico web en el equipo [2]
Detección de intrusos (IDS/IPS)	✓	⓪	Firewall en el módulo antivirus; sin IDS/IPS dedicado publicado [2]
Detección de amenazas en la red interna (NDR)	✓	⓪	DNS Security Network cubre la red a nivel DNS; no es NDR de tráfico [2]
Investigaciones documentadas y enriquecidas con inteligencia de amenazas	✓	✓	XDR con inteligencia de amenazas, datos de actividad y detalles forenses [12]
Gestión de incidentes con bitácora y tiempo de atención medido por caso	✓	⓪	Threat Hunting & Action Center gestiona casos; sin evidencia de MTTR por incidente [12]
Respuesta con aislamiento de equipos y bloqueo de direcciones IP	✓	⓪	El SOC puede aislar equipos; bloqueo de IP solo vía firewalls integrados (Meraki, Palo Alto) [7]
Respuesta a incidentes con análisis de causa raíz	✓	⓪	MXDR menciona análisis forense; sin servicio de respuesta forense a incidentes definido [5]
Postura de identidad: MFA, cuentas privilegiadas y acceso condicional	✓	⓪	ITDR detecta inicios de sesión sospechosos en M365 y PASM gestiona cuentas privilegiadas; sin postura de MFA [5]
Zero Trust: DNS seguro, acceso a aplicaciones y control de aplicaciones no autorizadas (shadow IT)	✓	⓪	DNS seguro y contención de IA de terceros; sin acceso Zero Trust a aplicaciones [6]
Seguridad en la nube: alertas y postura	✓	⓪	Cubre M365 y Google Workspace; sin evidencia de postura ni alertas de Azure [12]
Seguridad de correo: spam, phishing, malware y fraude por suplantación (BEC)	✓	✓	Seguridad de correo propia: antispam, antiphishing, filtrado avanzado de malware y prevención de fraude por suplantación (BEC) [13]

Capacidad	TecnetSOC	Heimdal Plataforma y SOC	Evidencia sobre Heimdal
 Lo ofrece  Lo ofrece como complemento  No forma parte de su oferta publicada  Parcial, limitado o requiere otro contrato  Sin evidencia pública			
Concientización: simulaciones de phishing y entrenamiento con métricas			Sin simulaciones de phishing ni entrenamiento de concientización en su catálogo [2]
Recomendaciones de seguridad priorizadas con flujo de aprobación			AI Wingman Assist sugiere configuraciones de buenas prácticas; sin flujo de aprobación [6]
Exposición y gestión de TI	12 de 12	2 completas +4 parciales	
Inventario unificado de activos y de software			Patch & Asset Management con inventario de activos y software [3]
Vulnerabilidades priorizadas por gravedad y probabilidad de explotación (CVSS, EPSS)			Vulnerabilidades por severidad y CVE dentro del parcheo; sin EPSS ni escáner independiente [3]
Prioridad a las fallas que ya se están explotando (catálogo KEV de CISA)			Sin evidencia de priorización por catálogo KEV de CISA [3]
Parcheo de sistema operativo y aplicaciones de terceros			Windows, macOS, Linux y 350+ aplicaciones de terceros; Infinity para apps propias [3]
Parcheo operado por el proveedor, con plazos publicados por severidad	 Críticos: 48 h (objetivo)		MXDR lista parcheo y remediación de vulnerabilidades entre sus casos de uso; el parcheo lo configura el cliente y no publica plazos por severidad [10]
Verificación de cierre: el escáner confirma que la vulnerabilidad desapareció			Su proceso de gestión de vulnerabilidades incluye una etapa de verificación, sin indicar que la haga el escáner [10]
Validación de parches en grupo piloto antes del despliegue			Calendarios configurables, pero sin flujo publicado de grupo piloto [3]
Superficie de ataque externa: lo que tu empresa expone en Internet, con puntaje de riesgo	 Puntaje 0 a 100		Sin oferta de superficie de ataque externa (EASM) [2]
Alertas de dominios que imitan tu marca y de credenciales o claves expuestas			Sin detección de typosquatting ni de secretos o código expuestos [2]
Prueba de penetración (pentest) anual	 Anual		Sin oferta de pentesting [2]
Gestión remota de equipos (RMM)			Escritorio remoto, parcheo e inventario; no es RMM completo, integra ConnectWise RMM [2]
Monitoreo de disponibilidad (NOC)			Sin monitoreo de disponibilidad ni NOC [2]
Respaldo y continuidad	3 de 3	0 completas +0 parciales	
Respaldo de servidores, archivos, bases de datos, máquinas virtuales y Microsoft 365	 Complemento		No ofrece respaldo [2]
Bóveda de respaldo inmutable (no se puede alterar ni borrar), aislada por cliente	 Complemento		No ofrece bóveda inmutable [2]
Recuperación ante desastres con simulacros y tiempo de recuperación (RTO) medido	 Complemento RTO medido		No ofrece recuperación ante desastres [2]
Cumplimiento	6 de 6	0 completas +1 parcial	
Evidencia mensual lista para auditores y aseguradoras	 Mensual		Reportes de cumplimiento mapeados a NIS2, ISO 27001 y otros; no evidencia mensual formal [5]
Preparación para ISO 27001, SOC 2 y PCI DSS con controles compartidos	 Complemento		Mapea controles en reportes; no ofrece plataforma GRC [5]
Preparación normativa mexicana: CNBV Fintech, protección de datos (LFPDPPP) y NOM-024	 Complemento		Sin cobertura de normativa mexicana [2]

Capacidad	TecnetSOC	Heimdal Plataforma y SOC	Evidencia sobre Heimdal
✓ Lo ofrece + Lo ofrece como complemento ⓪ Parcial, limitado o requiere otro contrato ? Sin evidencia pública ✗ No forma parte de su oferta publicada			
Gestión de riesgos, controles, declaración de aplicabilidad y auditorías internas	+ Complemento	✗	Sin gestión de riesgos, SoA ni auditorías internas [2]
Portal para tu auditor con sala de evidencias y página pública de confianza (trust center)	+ Complemento	✗	Sin portal del auditor ni Trust Center para el cliente [2]
Continuidad de negocio, riesgo de proveedores y gestión de brechas de datos	+ Complemento	✗	Sin módulos de continuidad, proveedores ni gestión de brechas [2]
Cómo se contrata	No suma al conteo		
Precio por dispositivo, con planes que se suman	✓ Por dispositivo	⓪	Cobro por dispositivo al año, pero cada módulo se licencia aparte, no acumulativo [14]
Plan gratuito para empezar	✓ Hasta 10 dispositivos	✗	Sin plan gratuito permanente publicado [14]
Prueba gratuita en tu entorno real	✓ 30 días	✓	Prueba gratis de 30 días sin tarjeta, según ficha de XDR [12]
Disponible con la marca de tu proveedor de TI	✓	⓪	Programa NEXUS para proveedores de TI con marca compartida; producto y SOC siguen siendo Heimdal [9]
Cobertura completa	50	9 +23 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

TecnetSOC frente a Heimdal · Comparativo 2026.09

tecnetone.com/servicios/soc-as-a-service · Pág. 5 de 6

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: confírmalo 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 Heimdal: Heimdal Security (Heimdal), plataforma completa con todos sus módulos más servicio MXDR (SOC 24/7), consulta 29 sep 2026

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. heimdalsecurity.com/wp-content/themes/heimdal/product-sheets/Heimda... (Diferencias que se notan en el día a día)
2. heimdalsecurity.com/ (Diferencias que se notan en el día a día)
3. heimdalsecurity.com/enterprise-security/products/patch-management-s... (Diferencias que se notan en el día a día)
4. heimdalsecurity.com/blog/best-managed-edr-services/ (Diferencias que se notan en el día a día)
5. heimdalsecurity.com/enterprise-security/products/managed-extended-d... (Diferencias que se notan en el día a día)
6. heimdalsecurity.com/blog/heimdal-expands-ai-strategy-with-ai-wingma... (Agentes de IA que investigan y filtran las alertas...)
7. heimdalsecurity.com/blog/heimdals-mxdr-adapt-worlds-first-tailored-... (Compuerta Humana: una persona aprueba cada acción...)
8. www.heimdalsecurity-la.com/en/heimdal-security-businesses-msps/ (Analistas, soporte y portal en español nativo)
9. heimdalsecurity.com/channel-partners (Reportes automáticos semanales, mensuales, trimestrales...)
10. support.heimdalsecurity.com/hc/en-us/articles/10792316864669-Manage... (Contacto 24/7 con personas de soporte o seguridad)
11. heimdalsecurity.com/blog/category/heimdal-announcements/ (Certificación independiente de la operación (ISO 27001...))
12. heimdalsecurity.com/enterprise-security/products/extended-detection... (Monitoreo continuo y correlación de eventos (SIEM),...)
13. support.heimdalsecurity.com/hc/en-us/articles/360007435238-Email-Se... (Seguridad de correo: spam, phishing, malware y fraude...)
14. heimdalsecurity.com/enterprise/request-pricing (Precio por dispositivo, con planes que se suman)

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.