

Cyrebro vigila las herramientas que ya tienes. TecnetSOC trae las suyas y opera tu seguridad completa, en tu idioma.

Con Cyrebro, tus sistemas los conecta un integrador certificado, dejas una máquina dedicada como recolector y el parcheo no está en el servicio. Con TecnetSOC instalas un agente, ves actividad en 2 a 4 horas y el SOC parchea.



44

capacidades donde TecnetSOC va más allá

6

capacidades en las que coincidimos

0

capacidades donde Cyrebro supera a TecnetSOC

De las 50: 44 donde vamos más allá y 6 en las que coincidimos

Misma lista de 50 capacidades y mismo criterio para TecnetSOC y Cyrebro: 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

Cyrebro es un servicio de SOC que se conecta a las herramientas que ya tienes; no incluye su propia protección de equipos. 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

Integración solo con tercero certificado

CON CYREBRO
Tus sistemas solo los puede conectar un integrador certificado de su lista, y debes dejar una máquina dedicada como recolector de eventos. [1]

CON TECNETSOC
Instalas un agente y el resto se despliega solo: actividad en el portal en 2 a 4 horas, sin proyecto de implementación ni servidores.

02

Parcheo y vulnerabilidades quedan fuera

CON CYREBRO
El servicio publicado es detección y respuesta; no documenta gestión de vulnerabilidades ni parcheo de sistemas, así que cerrar esas brechas queda en tu equipo. [2]

CON TECNETSOC
El SOC parchea priorizando por KEV y EPSS, valida en grupo piloto y da por cerrado solo cuando el escáner lo confirma.

03

Un SOC, una sola región

CON CYREBRO
El SOC opera desde Israel en una sola región y sin turnos que sigan la zona horaria del cliente (follow-the-sun), según un directorio independiente de proveedores MDR. [3]

CON TECNETSOC
Analistas propios operan en LATAM, EE.UU. y Europa, en tu zona horaria y en español nativo.

04

Más datos, más costo

CON CYREBRO
Extender la retención de registros en almacenamiento frío tiene costo adicional, y un directorio independiente advierte que el volumen ingerido puede subir el precio. [1]

CON TECNETSOC
Pagas por dispositivo con planes acumulativos, y la plataforma es un servicio en la nube que no instalas ni mantienes.

05

Correo y phishing no están en el servicio

CON CYREBRO
M365 Protect vigila accesos, apps y privilegios en tu suite, pero no documenta filtrado de spam o phishing ni simulaciones para tu personal. [4]

CON TECNETSOC
La seguridad de correo (spam, phishing, malware, BEC) y las simulaciones de phishing vienen en la oferta más completa.

06

Los reportes los pides tú

CON CYREBRO
Los reportes los generas tú con un asistente cuando los necesitas; no publica envíos automáticos ni plataforma de cumplimiento para tu auditoría. [5]

CON TECNETSOC
Recibes un resumen ejecutivo cada mañana y reportes automáticos en PDF; TecnetGRC se suma como complemento para tu auditoría.

— DÓNDE ESTÁ LA DIFERENCIA

Las tres áreas con más diferencia

Detección y respuesta

TecnetSOC 15

Cyrebro 3

de 15 capacidades completas en esta área

Exposición y gestión de TI

TecnetSOC 12

Cyrebro 0

de 12 capacidades completas en esta área

Operación y servicio

TecnetSOC 14

Cyrebro 3

de 14 capacidades completas en esta área

— CAPACIDAD POR CAPACIDAD

TecnetSOC y Cyrebro, lado a lado

Capacidad	TecnetSOC	Cyrebro SOC	Evidencia sobre Cyrebro
✓ Lo ofrece + Lo ofrece como complemento ⓧ No forma parte de su oferta publicada	ⓧ Parcial, limitado o requiere otro contrato	? Sin evidencia pública	
Operación y servicio	14 de 14	3 completas +6 parciales	
Centro de operaciones (SOC) 24/7 con analistas humanos	✓	✓	Monitoreo 24/7/365 con analistas de nivel 1 a 4 [6]
Agentes de IA que investigan y filtran las alertas antes de pasarlas a un analista	✓	ⓧ	Se presenta como "AI-native"; la IA lleva solo investigaciones de baja severidad [2]
Compuerta Humana: una persona aprueba cada acción crítica antes de ejecutarse	✓	ⓧ	Acción automática por playbook o escalamiento para aprobación, según un directorio independiente, sin documentación oficial [3]

Capacidad	TecnetSOC	Cyrebro SOC	Evidencia sobre Cyrebro
Lo ofrece Lo ofrece como complemento 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		Sin evidencia de analista de IA conversacional en el portal que cite fuentes [1]
Operación en LATAM, EE.UU. y Europa, con analistas en tu zona horaria			SOC operado desde Israel; sin follow-the-sun documentado [3]
Analistas, soporte y portal en español nativo			En LATAM el español lo pone el partner local (niveles 1 y 2); el nivel 3 atiende desde Tel Aviv [7]
Reportes para dirección en español y en lenguaje de negocio			Reportes en inglés sencillo; sin evidencia de reportes en español [5]
Tiempos de notificación e inicio de investigación publicados por severidad	Crítico: 30 min (objetivo)		No publica SLA de notificación ni de respuesta [5]
Resumen ejecutivo cada mañana: lo que pasó en las últimas 24 horas	07:30		Sin evidencia de resumen ejecutivo diario [5]
Reportes automáticos semanales, mensuales, trimestrales y anuales			Asistente de reportes bajo demanda; sin cadencia automática documentada [5]
Gerente técnico de cuenta (TAM) asignado y revisiones trimestrales			Menciona gerente de cuenta; sin revisiones trimestrales documentadas [6]
Contacto 24/7 con personas de soporte o seguridad			Analistas disponibles 24/7 para asistencia [5]
Certificación independiente de la operación (ISO 27001 o SOC 2 Tipo II)	ISO/IEC 27001:2022		Declara ISO 27001, SOC 2 e ISO 22301 [5]
Arranque rápido con un agente de software: la actividad de tus dispositivos, visible en horas	Típico: 2 a 4 horas		Requiere un recolector de eventos e integraciones; un directorio independiente habla de horas, sin confirmación oficial [3]
Detección y respuesta	15 de 15	3 completas +8 parciales	
Monitoreo continuo y correlación de eventos (SIEM), alineado con MITRE ATT&CK (marco de referencia de técnicas de ataque)			Repositorio de datos propio (data lake), más de 1,500 detecciones, mapeo MITRE ATT&CK [1]
Protección avanzada en cada equipo (EDR/XDR): malware, ransomware y explotación de vulnerabilidades			Sin EDR propio; se integra con SentinelOne, CrowdStrike, Defender; add-on Managed EDR [2]
Filtrado web en el equipo			Sin filtrado web propio en el equipo [2]
Detección de intrusos (IDS/IPS)			Solo ingiere alertas de IDS/IPS de firewalls de terceros [8]
Detección de amenazas en la red interna (NDR)			Sin NDR propio; depende de logs de red de terceros [8]
Investigaciones documentadas y enriquecidas con inteligencia de amenazas			Inteligencia de amenazas y enriquecimiento incluidos en investigaciones [1]
Gestión de incidentes con bitácora y tiempo de atención medido por caso			Gestión de incidentes en plataforma; sin MTTR por incidente documentado [1]
Respuesta con aislamiento de equipos y bloqueo de direcciones IP			Aislamiento y bloqueo vía EDR o firewall de terceros [3]
Respuesta a incidentes con análisis de causa raíz			Respuesta a incidentes y forense digital incluidos [1]
Postura de identidad: MFA, cuentas privilegiadas y acceso condicional			M365 Protect detecta escalamiento de privilegios; no evalúa postura de identidad [4]
Zero Trust: DNS seguro, acceso a aplicaciones y control de aplicaciones no autorizadas (shadow IT)			Sin oferta Zero Trust, DNS seguro ni shadow IT [2]
Seguridad en la nube: alertas y postura			Monitorea logs de Azure, AWS, GCP; sin postura de nube documentada [1]
Seguridad de correo: spam, phishing, malware y fraude por suplantación (BEC)			M365 Protect monitorea accesos y apps; no filtra spam ni phishing [4]
Concientización: simulaciones de phishing y entrenamiento con métricas			Sin oferta de concientización ni simulaciones de phishing [2]

Capacidad	TecnetSOC	Cyrebro SOC	Evidencia sobre Cyrebro
✓ 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	✓	●	Pasos de mitigación accionables; sin flujo de aprobación documentado [2]
Exposición y gestión de TI	12 de 12	0 completas +0 parciales	
Inventario unificado de activos y de software	✓	✗	Sin inventario de activos y software documentado [2]
Vulnerabilidades priorizadas por gravedad y probabilidad de explotación (CVSS, EPSS)	✓	✗	Sin módulo de gestión de vulnerabilidades documentado [2]
Prioridad a las fallas que ya se están explotando (catálogo KEV de CISA)	✓	✗	Sin priorización por KEV documentada [2]
Parcheo de sistema operativo y aplicaciones de terceros	✓	✗	No ofrece parcheo [2]
Parcheo operado por el proveedor, con plazos publicados por severidad	✓ Críticos: 48 h (objetivo)	✗	No ofrece parcheo operado con tiempos [2]
Verificación de cierre: el escáner confirma que la vulnerabilidad desapareció	✓	✗	Sin escáner de verificación de cierre [2]
Validación de parches en grupo piloto antes del despliegue	✓	✗	Sin parcheo, sin grupo piloto [2]
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 [2]
Alertas de dominios que imitan tu marca y de credenciales o claves expuestas	✓	✗	Sin detección de typosquatting ni secretos expuestos [2]
Prueba de penetración (pentest) anual	✓ Anual	✗	Sin pentesting documentado [2]
Gestión remota de equipos (RMM)	✓	✗	No ofrece RMM [2]
Monitoreo de disponibilidad (NOC)	✓	✗	No ofrece NOC ni monitoreo de disponibilidad [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 y consultas al data lake sirven de evidencia; sin entrega mensual [5]
Preparación para ISO 27001, SOC 2 y PCI DSS con controles compartidos	+ Complemento	✗	Sin plataforma GRC [2]
Preparación normativa mexicana: CNBV Fintech, protección de datos (LFPDPPP) y NOM-024	+ Complemento	✗	Sin cobertura de normativa mexicana [2]
Gestión de riesgos, controles, declaración de aplicabilidad y auditorías internas	+ Complemento	✗	Sin gestión de riesgos, controles ni SoA [2]

Capacidad	TecnetSOC	Cyrebro SOC	Evidencia sobre Cyrebro
✓ 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	✗	Sin portal de auditor ni Trust Center para clientes [2]
Continuidad de negocio, riesgo de proveedores y gestión de brechas de datos	+ Complemento	✗	Sin módulos de continuidad, proveedores ni brechas [2]
Cómo se contrata	No suma al conteo		
Precio por dispositivo, con planes que se suman	✓ Por dispositivo	✗	Cotización a la medida; sin precios ni planes públicos [2]
Plan gratuito para empezar	✓ Hasta 10 dispositivos	✗	Sin plan gratuito [2]
Prueba gratuita en tu entorno real	✓ 30 días	ⓘ	Sin prueba gratuita pública; prueba de valor bajo solicitud, según un directorio independiente [3]
Disponible con la marca de tu proveedor de TI	✓	✓	"Your brand, powered by CYREBRO": el partner vende con su marca [6]
Cobertura completa	50	6 +15 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: 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 Cyrebro: CYREBRO AI-Native MDR (plataforma SOC completa + M365/Workspace Protect + Managed EDR + programa proveedor de TI co-branded), 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. www.cyrebro.io/why-cyrebro/solution-description/ (Diferencias que se notan en el día a día)

2. www.cyrebro.io/ (Diferencias que se notan en el día a día)

3. mdrproviders.io/providers/cyrebro (Diferencias que se notan en el día a día)
4. www.cyrebro.io/cyrebro-m365-protect/ (Diferencias que se notan en el día a día)

5. www.cyrebro.io/faqs/ (Diferencias que se notan en el día a día)

6. www.cyrebro.io/partners/ (Centro de operaciones (SOC) 24/7 con analistas humanos)
7. tiinside.com.br/en/03/12/2025/cyrebro-chega-ao-brasil-com-apoio-da-... (Analistas, soporte y portal en español nativo)

8. www.cyrebro.io/integrations/ (Detección de intrusos (IDS/IPS))

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.](#)