

Acronis respalda y protege tus equipos. TecnetSOC es el SOC agéntico que opera toda tu seguridad por ti, 24/7.

Con Acronis, el MDR 24/7 se contrata aparte de tu respaldo y su catálogo no incluye detección en tu red interna. Con TecnetSOC, la vigilancia 24/7 es el servicio, con detección en tu red interna y resumen ejecutivo cada mañana.



32

capacidades donde TecnetSOC va más allá

18

capacidades en las que coincidimos

1

capacidad donde Acronis supera a TecnetSOC
Incluida en las 18 en que coincidimos

De las 50: 32 donde vamos más allá y 18 en las que coincidimos

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

Acronis es una plataforma de protección y respaldo que se vende a través de proveedores de TI (MSP); su servicio de SOC se contrata y se entrega por medio de ellos, y 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
Tu proveedor instala, configura y afina

CON ACRONIS
Tu proveedor de TI despliega los agentes, configura las políticas, elige los equipos críticos y resuelve las exclusiones que el SOC le pide. [\[1\]](#)

CON TECNETSOC
Instalas un agente, el resto de la plataforma se despliega solo y analistas de TecnetOne lo operan 24/7, sin proyecto de implementación.

02
La vigilancia 24/7 se contrata aparte

CON ACRONIS
El SOC 24/7 (MDR) no viene en la plataforma: se factura por separado, igual que la concientización, y tu proveedor decide si lo contrata. [\[2\]](#)

CON TECNETSOC
La operación 24/7 del SOC es el servicio mismo: no se suma aparte, se paga por dispositivo en planes acumulativos.

03
Remediar depende del nivel contratado

CON ACRONIS
En el MDR Standard el SOC recomienda y tu proveedor remedia, incluida la reversión de cambios (rollback); en el Advanced, parchear o ejecutar scripts exige licencia de gestión remota (RMM). [\[1\]](#)

CON TECNETSOC
El SOC ejecuta la respuesta y el parcheo, con RMM en la oferta más completa, y una persona aprueba cada acción crítica.

04
Tu red interna queda fuera

CON ACRONIS
El MDR parte de lo que detecta su agente EDR/XDR; su catálogo no ofrece IDS/IPS ni detección en la red interna (NDR). [\[1\]](#)

CON TECNETSOC
La oferta más completa suma IDS/IPS y detección en la red interna (NDR) a SIEM con MITRE ATT&CK, identidad, nube y correo.

05
Los avisos llegan a tu proveedor

CON ACRONIS
El SOC notifica, llama y pide aprobaciones a los contactos que registra tu proveedor de TI, y a ellos llega el reporte mensual. [\[1\]](#)

CON TECNETSOC
Lo contratas directo o con tu proveedor, y cada mañana a las 07:30 recibes un resumen ejecutivo en lenguaje de negocio.

06
Soporte del fabricante solo en inglés

CON ACRONIS
Su soporte técnico atiende solo en inglés y solo a tu proveedor de TI; tú no tienes canal directo con el fabricante. [\[3\]](#)

CON TECNETSOC
La operación y la mesa de soporte 24/7 son en español nativo, con atención multidioma y analistas en tu zona horaria.

— DÓNDE ESTÁ LA DIFERENCIA

Las tres áreas con más diferencia

Operación y servicio

TecnetSOC **14**

Acronis **5**

de 14 capacidades completas en esta área

Detección y respuesta

TecnetSOC **15**

Acronis **6**

de 15 capacidades completas en esta área

Exposición y gestión de TI

TecnetSOC **12**

Acronis **4**

de 12 capacidades completas en esta área

— CAPACIDAD POR CAPACIDAD

TecnetSOC y Acronis, lado a lado

Capacidad	TecnetSOC	Acronis Plataforma y SOC a través de proveedores de TI	Evidencia sobre Acronis
✓ Lo ofrece + Lo ofrece como complemento ✗ No forma parte de su oferta publicada	⓪ Parcial, limitado o requiere otro contrato	? Sin evidencia pública	
Operación y servicio	14 de 14	5 completas +9 parciales	
Centro de operaciones (SOC) 24/7 con analistas humanos	✓	✓	MDR 24/7 operado por el SOC de Acronis TRU desde abril de 2026, también por socios; se contrata y entrega a través del proveedor de TI [4]
Agentes de IA que investigan y filtran las alertas antes de pasarlas a un analista	✓	⓪	EDR prioriza actividad sospechosa y resume incidentes con IA; no hay agentes que filtren cada alerta [5]
Compuerta Humana: una persona aprueba cada acción crítica antes de ejecutarse	✓	⓪	Aprobación del proveedor de TI solo en equipos críticos; el resto se aísla sin aprobación previa [1]

Capacidad	TecnetSOC	Acronis Plataforma y SOC a través de proveedores de TI	Evidencia sobre Acronis
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		Acronis Copilot investiga en lenguaje natural, pero sigue en acceso anticipado [5]
Operación en LATAM, EE.UU. y Europa, con analistas en tu zona horaria			Sin evidencia de SOC en LATAM; proveedor de seguridad administrada socios citados en Reino Unido, Australia, Asia y Europa [4]
Analistas, soporte y portal en español nativo			Soporte oficial a proveedores de servicio solo en inglés; el portal de la plataforma está disponible en 26 idiomas [3]
Reportes para dirección en español y en lenguaje de negocio			Reporte Executive Summary para el cliente; sin evidencia de redacción en español ni en lenguaje de negocio [6]
Tiempos de notificación e inicio de investigación publicados por severidad	Crítico: 30 min (objetivo)	15 min, promedio	Promedio de inicio de investigación: 15 min en alto y crítico, 30 min en bajo y medio; avisos al proveedor de TI [1]
Resumen ejecutivo cada mañana: lo que pasó en las últimas 24 horas	07:30		Reportes programables diarios en el portal; no hay resumen ejecutivo diario de lo ocurrido [7]
Reportes automáticos semanales, mensuales, trimestrales y anuales			Reportes programados en portal y reporte mensual MDR; sin reportes trimestrales ni anuales documentados [1]
Gerente técnico de cuenta (TAM) asignado y revisiones trimestrales			Servicio pagado de Technical Account Management de Acronis Professional Services [8]
Contacto 24/7 con personas de soporte o seguridad			Contacto 24/7 en inglés solo para el proveedor de TI; el cliente final no tiene canal directo con Acronis [9]
Certificación independiente de la operación (ISO 27001 o SOC 2 Tipo II)	ISO/IEC 27001:2022		Trust Center declara serie ISO/IEC 27000, SOC 2 y PCI DSS [10]
Arranque rápido con un agente de software: la actividad de tus dispositivos, visible en horas	Típico: 2 a 4 horas		Un solo agente y consola; MDR se activa con un clic sobre EDR o XDR [11]
Detección y respuesta	15 de 15	6 completas +5 parciales	
Monitoreo continuo y correlación de eventos (SIEM), alineado con MITRE ATT&CK (marco de referencia de técnicas de ataque)			XDR correlaciona eventos con MITRE ATT&CK; no es un SIEM de registros de terceros [5]
Protección avanzada en cada equipo (EDR/XDR): malware, ransomware y explotación de vulnerabilidades			EDR/XDR con comportamiento, prevención de explotación de vulnerabilidades y antiransomware con rollback [12]
Filtrado web en el equipo			Filtrado de URL incluido en la protección del equipo [5]
Detección de intrusos (IDS/IPS)			No ofrece IDS/IPS de red [13]
Detección de amenazas en la red interna (NDR)			Sin NDR; Device Sense solo descubre equipos sin agente [14]
Investigaciones documentadas y enriquecidas con inteligencia de amenazas			Feed de inteligencia en tiempo real, búsqueda de IoC y enriquecimiento en MDR [5]
Gestión de incidentes con bitácora y tiempo de atención medido por caso			Incidentes con ticket, estado y resolución; reportes MDR con MTTR y SLA [1]
Respuesta con aislamiento de equipos y bloqueo de direcciones IP			Aislamiento y cuarentena incluidos; sin evidencia de bloqueo de direcciones IP como acción de respuesta [12]
Respuesta a incidentes con análisis de causa raíz			Respaldo forense y análisis de causa raíz en MDR Advanced [1]
Postura de identidad: MFA, cuentas privilegiadas y acceso condicional			Postura de Microsoft 365 y acciones en Entra ID; sin postura de Google Workspace [15]
Zero Trust: DNS seguro, acceso a aplicaciones y control de aplicaciones no autorizadas (shadow IT)			Sin DNS seguro ni acceso Zero Trust; solo control de uso de GenAI por URL [12]

Capacidad	TecnetSOC	Acronis Plataforma y SOC a través de proveedores de TI	Evidencia sobre Acronis
Lo ofrece Lo ofrece como complemento Parcial, limitado o requiere otro contrato Sin evidencia pública No forma parte de su oferta publicada			
Seguridad en la nube: alertas y postura			Sin monitoreo de alertas ni postura de Azure; Azure solo como destino de DR [16]
Seguridad de correo: spam, phishing, malware y fraude por suplantación (BEC)			Email Security con marca Acronis, con motor de un tercero; se licencia por usuario aparte de la protección de equipos [17]
Concientización: simulaciones de phishing y entrenamiento con métricas			SAT propio con simulaciones de phishing, cursos y consola multi-cliente [18]
Recomendaciones de seguridad priorizadas con flujo de aprobación			Líneas base de postura M365 y CyberFit Score; sin flujo de aprobación documentado [15]
Exposición y gestión de TI	12 de 12	4 completas +4 parciales	
Inventario unificado de activos y de software			Inventario de hardware y software con RMM, más descubrimiento Device Sense [14]
Vulnerabilidades priorizadas por gravedad y probabilidad de explotación (CVSS, EPSS)			Evaluación de vulnerabilidades de sistema y aplicaciones de terceros; sin priorización por EPSS documentada [19]
Prioridad a las fallas que ya se están explotando (catálogo KEV de CISA)			Sin evidencia pública de priorización por catálogo KEV de CISA [19]
Parcheo de sistema operativo y aplicaciones de terceros			Parcheo de sistema y aplicaciones de terceros con RMM [14]
Parcheo operado por el proveedor, con plazos publicados por severidad	 Críticos: 48 h (objetivo)		MDR Advanced puede ejecutar parches como remediación; sin tiempos publicados de parcheo [11]
Verificación de cierre: el escáner confirma que la vulnerabilidad desapareció			Escaneos programados reflejan el estado; no hay verificación explícita de cierre [19]
Validación de parches en grupo piloto antes del despliegue			Aprobación automática de parches con prueba: si se instalan bien en los equipos de prueba, se despliegan al resto [20]
Superficie de ataque externa: lo que tu empresa expone en Internet, con puntaje de riesgo	 Puntaje 0 a 100		No ofrece EASM [13]
Alertas de dominios que imitan tu marca y de credenciales o claves expuestas			No detecta typosquatting ni secretos expuestos [13]
Prueba de penetración (pentest) anual	 Anual		No ofrece pentesting; servicios profesionales cubren auditoría de su propia solución [5]
Gestión remota de equipos (RMM)			RMM propio con escritorio remoto, scripting y automatización [14]
Monitoreo de disponibilidad (NOC)			Monitoreo de sistema y hardware con alertas; Acronis no opera un NOC [14]
Respaldo y continuidad	3 de 3	3 completas +0 parciales	
Respaldo de servidores, archivos, bases de datos, máquinas virtuales y Microsoft 365	 Complemento		Respaldo de servidores, VM, aplicaciones, archivos y Microsoft 365 [2]
Bóveda de respaldo inmutable (no se puede alterar ni borrar), aislada por cliente	 Complemento		Almacenamiento inmutable en Acronis Cloud, aislado por tenant de cliente [21]
Recuperación ante desastres con simulacros y tiempo de recuperación (RTO) medido	 Complemento RTO medido		DR con runbooks y pruebas de failover automáticas mensuales [16]

Capacidad	TecnetSOC	Acronis	Evidencia sobre Acronis
✓ Lo ofrece + Lo ofrece como complemento ⓪ Parcial, limitado o requiere otro contrato ? Sin evidencia pública ✗ No forma parte de su oferta publicada			
Cumplimiento	6 de 6	0 completas	+1 parcial
Evidencia mensual lista para auditores y aseguradoras	✓ Mensual	⓪	Reportes de cumplimiento de postura M365 y ejecutivos; no es paquete de evidencia mensual [15]
Preparación para ISO 27001, SOC 2 y PCI DSS con controles compartidos	+ Complemento	✗	Sin plataforma GRC; solo guías de apoyo para ISO 27001 [22]
Preparación normativa mexicana: CNBV Fintech, protección de datos (LFPDPPP) y NOM-024	+ Complemento	✗	Sin marcos mexicanos (CNBV, LFPDPPP, NOM-024) [10]
Gestión de riesgos, controles, declaración de aplicabilidad y auditorías internas	+ Complemento	✗	No gestiona riesgos, SoA ni auditorías internas [13]
Portal para tu auditor con sala de evidencias y página pública de confianza (trust center)	+ Complemento	✗	Trust Center es de Acronis, no para el cliente final [23]
Continuidad de negocio, riesgo de proveedores y gestión de brechas de datos	+ Complemento	✗	DR técnico sí, pero sin módulos GRC de continuidad, proveedores o brechas [13]
Cómo se contrata	No suma al conteo		
Precio por dispositivo, con planes que se suman	✓ Por dispositivo	⓪	Por carga de trabajo (workload), usuario o GB según el servicio, o por paquetes; sin planes acumulativos por dispositivo [2]
Plan gratuito para empezar	✓ Hasta 10 dispositivos	⓪	Funciones esenciales de seguridad sin costo, pero dentro de un contrato con compromiso mínimo [13]
Prueba gratuita en tu entorno real	✓ 30 días	✓	Prueba gratuita de 30 días [24]
Disponible con la marca de tu proveedor de TI	✓	✓	Se vende solo vía proveedores de servicio con marca propia (marca blanca) [25]
Cobertura completa	50	18	+19 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

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 Acronis: Acronis Cyber Protect Cloud en su oferta más completa (Ultimate Protection o servicios sueltos: EDR, XDR, MDR Advanced by Acronis TRU, Email Security, Collaboration Security, Security Posture Management, SAT, DLP, RMM, PSA, Backup, Backup M365, Disaster Recovery). Se vende solo a proveedores de servicio (proveedor de TI), con licencia por workload, por usuario o por GB y compromiso mínimo mensual; la plataforma la opera el proveedor de TI y el MDR lo opera el SOC de Acronis (TRU) o un proveedor de seguridad administrada socio. 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.

- go.acronis.com/mdr-service-definition (Diferencias que se notan en el día a día)
- www.acronis.com/en/products/cloud/cyber-protect/pricing/ (Diferencias que se notan en el día a día)
- www.acronis.com/en/support/serviceproviderscope/ (Diferencias que se notan en el día a día)
- www.acronis.com/en/pr/2026/acronis-launches-mdr-by-acronis-tru-to-p... (Centro de operaciones (SOC) 24/7 con analistas humanos)
- www.acronis.com/en/products/cloud/cyber-protect/extended-detection-... (Agentes de IA que investigan y filtran las alertas...)
- www.acronis.com/en/resource-center/resource/executive-summary-repor... (Reportes para dirección en español y en lenguaje de...)
- www.acronis.com/en/support/documentation/AcronisCyberCloud/reportin... (Resumen ejecutivo cada mañana: lo que pasó en las...)
- www.acronis.com/en/services/technical-account-management/ (Gerente técnico de cuenta (TAM) asignado y revisiones...)
- www.acronis.com/en/support/serviceproviderguidelines/ (Contacto 24/7 con personas de soporte o seguridad)
- www.acronis.com/en/trust-center/compliance/ (Certificación independiente de la operación (ISO 27001...))
- www.acronis.com/en/products/cloud/cyber-protect/managed-detection-a... (Arranque rápido con un agente de software: la actividad...)
- www.acronis.com/en/products/cloud/cyber-protect/security-edr/ (Protección avanzada en cada equipo (EDR/XDR): malware,...)
- www.acronis.com/en/products/cloud/cyber-protect/ (Detección de intrusos (IDS/IPS))
- www.acronis.com/en/products/cloud/cyber-protect/rmm-solution/ (Detección de amenazas en la red interna (NDR))
- www.acronis.com/en/solutions/cloud/microsoft-365-security-posture-m... (Postura de identidad: MFA, cuentas privilegiadas y...)
- www.acronis.com/en/products/cloud/cyber-protect/disaster-recovery/ (Seguridad en la nube: alertas y postura)
- www.acronis.com/en/products/cloud/cyber-protect/email-security/ (Seguridad de correo: spam, phishing, malware y fraude...)
- www.acronis.com/en/products/cloud/cyber-protect/security-awareness-... (Concientización: simulaciones de phishing y...)
- www.acronis.com/en/solutions/cloud/vulnerability-assessments/ (Vulnerabilidades priorizadas por gravedad y...)
- www.acronis.com/en-us/support/documentation/CyberProtectionService/.. (Validación de parches en grupo piloto antes del...)
- www.acronis.com/en/products/cloud/cyber-protect/backup/ (Bóveda de respaldo inmutable (no se puede alterar ni...))
- www.acronis.com/en/compliance/iso-27001/ (Preparación para ISO 27001, SOC 2 y PCI DSS con...)
- www.acronis.com/en/trust-center/ (Portal para tu auditor con sala de evidencias y página...)
- www.acronis.com/en/products/cloud/trial/ (Prueba gratuita en tu entorno real)
- www.acronis.com/en/partners/service-providers/ (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.