

Stellar Cyber une tus herramientas en una plataforma que opera tu equipo o tu proveedor.

TecnetSOC trae las herramientas y las opera por ti, en tu idioma.

Con Stellar Cyber, la protección de equipos viene de un EDR de otro fabricante, el correo lo filtra otro producto y la licencia se mide por GB o activos al día. Con TecnetSOC, EDR, correo y parcheo van en el servicio y analistas de TecnetOne responden 24/7.



44

capacidades donde TecnetSOC va más allá

6

capacidades en las que coincidimos

0

capacidades donde Stellar Cyber 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 Stellar Cyber: 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)

— ANTES DE COMPARAR

Stellar Cyber es una plataforma abierta de operaciones de seguridad (SIEM, NDR, UEBA e ITDR) que tu equipo o un proveedor de servicios certificado opera; Stellar Cyber no ofrece un SOC propio. La protección de equipos, el filtrado de correo y el escaneo de vulnerabilidades vienen de productos de otros fabricantes integrados. Aquí comparamos la plataforma con lo que incluye TecnetSOC, capacidad por capacidad.

Diferencias que se notan en el día a día

01
La plataforma no es el servicio

CON STELLAR CYBER
Compras una plataforma: vigilar, investigar y responder a toda hora lo hace tu equipo o un proveedor de servicios (proveedor de seguridad administrada) certificado que contratas aparte; Stellar Cyber no opera un SOC propio. [\[1\]](#)

CON TECNETSOC
Analistas de TecnetOne vigilan, investigan y responden 24/7, en tu zona horaria y en español; ante un crítico, notifican e inician investigación en 30 minutos, como objetivo.

02
El EDR lo compras a otro fabricante

CON STELLAR CYBER
La protección de cada equipo viene de un EDR que compras a otro fabricante: su modelo es traer tu propio EDR e integrarlo, entre 32 opciones como CrowdStrike, SentinelOne o ESET. [\[2\]](#)

CON TECNETSOC
La protección avanzada en cada equipo (EDR/XDR) y el filtrado web van en la oferta más completa, con un agente y actividad visible por lo general en 2 a 4 horas.

03
Pagas por datos ingeridos, no por dispositivo

CON STELLAR CYBER
La licencia se mide por GB diarios ingeridos o por activos activos al día, y su documentación fija reglas de cumplimiento del límite contratado, con cobro del excedente. [\[3\]](#)

CON TECNETSOC
Pagas por dispositivo con planes que se suman; el SIEM y la retención van dentro del servicio.

04
Ve vulnerabilidades, no las parchea

CON STELLAR CYBER
Las vulnerabilidades llegan de escáneres de otros fabricantes integrados, y su licencia (SIEM, NDR, UEBA, inteligencia de amenazas, IDS, sandbox, orquestación e integridad de archivos) no incluye instalar parches. [\[4\]](#)

CON TECNETSOC
El SOC parchea por explotación real (KEV y EPSS), con plazos objetivo por severidad, valida en grupo piloto y da por cerrado solo cuando el escáner confirma.

05
Tu correo lo filtra otro producto

CON STELLAR CYBER
La IA analiza los correos que tus usuarios reportan como sospechosos; a la pregunta de si aún necesitas Mimecast o Proofpoint para el filtrado de entrada, su respuesta es sí. [\[5\]](#)

CON TECNETSOC
La protección contra spam, phishing, malware y suplantación (BEC) va dentro del servicio, con cuarentena en autoservicio y simulaciones de phishing con métricas por usuario.

06
Detecta ataques, no respalda tus datos

CON STELLAR CYBER
Su licencia sola reúne las capacidades de detección y respuesta, pero no incluye respaldo de servidores, bóveda inmutable ni recuperación ante desastres de tus sistemas. [\[4\]](#)

CON TECNETSOC
Puedes sumar TecnetProtect (costo aparte): respaldo en bóveda inmutable por cliente y recuperación ante desastres con simulacros y RTO medido.

Las tres áreas con más diferencia

Operación y servicio

TecnetSOC **14**

Stellar Cyber **1**

de 14 capacidades completas en esta área

Exposición y gestión de TI

TecnetSOC **12**

Stellar Cyber **0**

de 12 capacidades completas en esta área

Detección y respuesta

TecnetSOC **15**

Stellar Cyber **5**

de 15 capacidades completas en esta área

TecnetSOC y Stellar Cyber, lado a lado

Capacidad	TecnetSOC	Stellar Cyber Open XDR	Evidencia sobre Stellar Cyber
✓ Lo ofrece + Lo ofrece como complemento Ⓜ Parcial, limitado o requiere otro contrato ? Sin evidencia pública ✗ No forma parte de su oferta publicada ● Lo pone tu equipo			
Operación y servicio	14 de 14	1 completa +7 parciales	
Centro de operaciones (SOC) 24/7 con analistas humanos	✓	Lo pone tu equipo	Sin SOC propio; la vigilancia 24/7 la pone tu equipo o un proveedor de servicios certificado que contratas aparte [1]
Agentes de IA que investigan y filtran las alertas antes de pasarlas a un analista	✓	Ⓜ	Auto Triage prioriza y filtra alertas; el analista que decide lo pone tu equipo o tu proveedor [6]

Capacidad	TecnetSOC	Stellar Cyber Open XDR	Evidencia sobre Stellar Cyber
☒ Lo ofrece ☒ Lo ofrece como complemento ☐ Parcial, limitado o requiere otro contrato ☐ Sin evidencia pública ☐ No forma parte de su oferta publicada ☐ Lo pone tu equipo			
Compuerta Humana: una persona aprueba cada acción crítica antes de ejecutarse	☒	☐	Playbooks automáticos o con una persona en el ciclo, a tu elección; los opera tu equipo o tu proveedor [7]
Asistente de investigación con IA en el portal, que cita sus fuentes	☒ Neo	☐	AI Investigator responde en lenguaje natural con consultas editables; en acceso anticipado, sin citas de fuentes documentadas [8]
Operación en LATAM, EE.UU. y Europa, con analistas en tu zona horaria	☒	Lo pone tu equipo	Sin analistas propios; según Stellar Cyber, proveedores de LATAM operan su plataforma y tú eliges uno [9]
Analistas, soporte y portal en español nativo	☒	☐	Sitio en español; idioma de consola y soporte no publicado; los analistas los pone tu equipo o tu proveedor [10]
Reportes para dirección en español y en lenguaje de negocio	☒	☐	Reportes personalizables que arma tu equipo o tu proveedor; reportes ejecutivos en español no documentados [11]
Tiempos de notificación e inicio de investigación publicados por severidad	☒ Crítico: 30 min (objetivo)	Lo pone tu equipo	Solo tiempos de soporte de la plataforma (de una hora a días hábiles); los de seguridad dependen de tu proveedor [12]
Resumen ejecutivo cada mañana: lo que pasó en las últimas 24 horas	☒ 07:30	Lo pone tu equipo	Sin resumen ejecutivo diario documentado; lo arma tu equipo o tu proveedor [13]
Reportes automáticos semanales, mensuales, trimestrales y anuales	☒	☐	Reportes programados semanales o mensuales que configura tu equipo o tu proveedor; trimestrales y anuales no documentados [13]
Gerente técnico de cuenta (TAM) asignado y revisiones trimestrales	☒	Lo pone tu equipo	Gerente de éxito del cliente asignado para la plataforma; TAM y revisiones trimestrales no documentados [14]
Contacto 24/7 con personas de soporte o seguridad	☒	☐	Soporte 24x7 de la plataforma por portal; el contacto de seguridad 24/7 lo pone tu equipo o tu proveedor [15]
Certificación independiente de la operación (ISO 27001 o SOC 2 Tipo II)	☒ ISO/IEC 27001:2022	☒	Su centro de confianza publica ISO/IEC 27001 y SOC 2, con informe SOC 2 disponible [16]
Arranque rápido con un agente de software: la actividad de tus dispositivos, visible en horas	☒ Típico: 2 a 4 horas	☐	Sensor propio solo para Windows Server y Linux; en equipos de trabajo depende de un EDR de otro fabricante [17]
Detección y respuesta	15 de 15	5 completas +6 parciales	
Monitoreo continuo y correlación de eventos (SIEM), alineado con MITRE ATT&CK (marco de referencia de técnicas de ataque)	☒	☒	Correlaciona alertas en casos y las ordena en su XDR Kill Chain, basada en MITRE ATT&CK [18]
Protección avanzada en cada equipo (EDR/XDR): malware, ransomware y explotación de vulnerabilidades	☒	☐	Sin EDR propio: integra 32 EDR de otros fabricantes, como CrowdStrike, SentinelOne y ESET [2]
Filtrado web en el equipo	☒	☐	Sin evidencia de filtrado web en el equipo [4]
Detección de intrusos (IDS/IPS)	☒	☒	El sensor detecta intentos de intrusión en archivos y tráfico de red (IDS); el bloqueo pasa por tu firewall [19]
Detección de amenazas en la red interna (NDR)	☒	☒	NDR propio: sensor modular con análisis de tráfico de red, IDS y sandbox de malware [19]
Investigaciones documentadas y enriquecidas con inteligencia de amenazas	☒	☒	Plataforma de inteligencia de amenazas integrada que enriquece registros y casos con indicadores [20]
Gestión de incidentes con bitácora y tiempo de atención medido por caso	☒	☒	Casos con bitácora de actividad y registro de creación, reconocimiento y cierre [21]
Respuesta con aislamiento de equipos y bloqueo de direcciones IP	☒	☐	Bloquea IP con tu firewall y contiene equipos con tu EDR, ambos de otros fabricantes conectados [22]
Respuesta a incidentes con análisis de causa raíz	☒	Lo pone tu equipo	Herramientas para investigar; la respuesta con análisis de causa raíz la pone tu equipo o tu proveedor [23]

Capacidad	TecnetSOC	Stellar Cyber Open XDR	Evidencia sobre Stellar Cyber
☒ Lo ofrece ☒ Lo ofrece como complemento ☐ Parcial, limitado o requiere otro contrato ☐ Sin evidencia pública ☐ No forma parte de su oferta publicada ☐ Lo pone tu equipo			
Postura de identidad: MFA, cuentas privilegiadas y acceso condicional	☒	☐	ITDR detecta abuso de identidades en AD, Entra ID y Okta; postura (MFA, acceso condicional) no documentada [24]
Zero Trust: DNS seguro, acceso a aplicaciones y control de aplicaciones no autorizadas (shadow IT)	☒	☐	Sin evidencia de DNS seguro, acceso Zero Trust ni control de shadow IT [25]
Seguridad en la nube: alertas y postura	☒	☐	Ingiera registros de AWS, Azure, Google Cloud y OCI; la postura llega integrando CSPM de otros fabricantes [26]
Seguridad de correo: spam, phishing, malware y fraude por suplantación (BEC)	☒	☐	Analiza los correos que reportan tus usuarios; el filtrado de entrada sigue en Mimecast o Proofpoint [5]
Concientización: simulaciones de phishing y entrenamiento con métricas	☒	☐	Sin simulaciones de phishing ni entrenamiento de usuarios en las capacidades de su licencia [4]
Recomendaciones de seguridad priorizadas con flujo de aprobación	☒	☐	Su analizador de cobertura MITRE sugiere dónde invertir para ampliar la detección; sin flujo de aprobación [27]
Exposición y gestión de TI	12 de 12	0 completas +2 parciales	
Inventario unificado de activos y de software	☒	☐	Descubre activos por IP y MAC y permite importar tu inventario; inventario de software no documentado [28]
Vulnerabilidades priorizadas por gravedad y probabilidad de explotación (CVSS, EPSS)	☒	☐	Sin escáner propio: integra Tenable, Qualys y Rapid7; uso de EPSS no documentado [29]
Prioridad a las fallas que ya se están explotando (catálogo KEV de CISA)	☒	☐	Sin evidencia de priorización por catálogo KEV de CISA [28]
Parcheo de sistema operativo y aplicaciones de terceros	☒	☐	Sin evidencia de parcheo; las capacidades de su licencia no incluyen instalar parches [4]
Parcheo operado por el proveedor, con plazos publicados por severidad	☒ Críticos: 48 h (objetivo)	Lo pone tu equipo	Sin parcheo operado por Stellar Cyber; lo pone tu equipo o tu proveedor [23]
Verificación de cierre: el escáner confirma que la vulnerabilidad desapareció	☒	☐	Sin evidencia de verificación de cierre de vulnerabilidades [4]
Validación de parches en grupo piloto antes del despliegue	☒	☐	Sin evidencia de validación de parches en grupo piloto [4]
Superficie de ataque externa: lo que tu empresa expone en Internet, con puntaje de riesgo	☒ Puntaje 0 a 100	☐	Sin evidencia de monitoreo de lo que tu empresa expone en Internet [25]
Alertas de dominios que imitan tu marca y de credenciales o claves expuestas	☒	☐	Sin evidencia de alertas de dominios que imitan tu marca ni de credenciales expuestas [25]
Prueba de penetración (pentest) anual	☒ Anual	Lo pone tu equipo	Sin pentest como servicio propio; lo pone tu equipo o tu proveedor [23]
Gestión remota de equipos (RMM)	☒	☐	Sin evidencia de gestión remota de equipos (RMM) [29]
Monitoreo de disponibilidad (NOC)	☒	☐	Sin evidencia de monitoreo de disponibilidad de tus sistemas (NOC) [25]
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 propio; las capacidades de su licencia sola no incluyen respaldo [4]
Bóveda de respaldo inmutable (no se puede alterar ni borrar), aislada por cliente	☒ Complemento	☐	Sin bóveda de respaldo propia [4]
Recuperación ante desastres con simulacros y tiempo de recuperación (RTO) medido	☒ Complemento RTO medido	☐	Sin recuperación ante desastres de tus sistemas; en sitio, la de la plataforma corre por tu cuenta [30]

Capacidad	TecnetSOC	Stellar Cyber Open XDR	Evidencia sobre Stellar Cyber
☒ Lo ofrece ☒ Lo ofrece como complemento ☒ Parcial, limitado o requiere otro contrato ☒ Sin evidencia pública			
☒ No forma parte de su oferta publicada ☒ Lo pone tu equipo			
Cumplimiento	6 de 6	0 completas	+2 parciales
Evidencia mensual lista para auditores y aseguradoras	☒ Mensual	☒	Reportes listos de PCI y HIPAA, personalizables; sin paquete de evidencia mensual [11]
Preparación para ISO 27001, SOC 2 y PCI DSS con controles compartidos	☒ Complemento	☒	Reportes de PCI DSS listos; preparación ISO 27001 o SOC 2 no documentada [11]
Preparación normativa mexicana: CNBV Fintech, protección de datos (LFPDPPP) y NOM-024	☒ Complemento	☒	Sin evidencia de normativa mexicana [11]
Gestión de riesgos, controles, declaración de aplicabilidad y auditorías internas	☒ Complemento	☒	Sin gestión de riesgos, controles ni auditorías internas para tu empresa [11]
Portal para tu auditor con sala de evidencias y página pública de confianza (trust center)	☒ Complemento	☒	Centro de confianza propio de Stellar Cyber; sin portal para tu auditor ni página de confianza tuya [16]
Continuidad de negocio, riesgo de proveedores y gestión de brechas de datos	☒ Complemento	☒	Sin evidencia de continuidad de negocio, riesgo de proveedores ni gestión de brechas [11]
Cómo se contrata	No suma al conteo		
Precio por dispositivo, con planes que se suman	☒ Por dispositivo	☒	Licencia por activos activos al día o por GB diarios ingeridos; sin planes que se suman [31]
Plan gratuito para empezar	☒ Hasta 10 dispositivos	☒	Sin plan gratuito publicado [4]
Prueba gratuita en tu entorno real	☒ 30 días	☒	Prueba de concepto con tus datos y en tu entorno; duración y costo no publicados [32]
Disponible con la marca de tu proveedor de TI	☒	☒	Plataforma multiempresa para proveedor de seguridad administrada, con reportes con la marca del proveedor [11]
Cobertura completa	50	6	+17 parciales

Lo que tu equipo tendría que poner para operarla 24/7: personas, turnos, tiempos de respuesta, resumen diario, respuesta a incidentes y parcheo operado. TecnetSOC los incluye en el servicio.

SIGUIENTE PASO

De la herramienta al servicio, sin proyecto de implementación

Instalas un solo agente, ves la actividad de tus dispositivos en horas y nuestros analistas operan 24/7 en tu idioma.

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

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

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

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 Stellar Cyber: Stellar Cyber, oferta más completa publicada (plataforma Open XDR con NG-SIEM, NDR con IDS y sandbox, UEBA, ITDR, inteligencia de amenazas, Auto Triage, AI Investigator y respuesta automatizada; sin SOC propio: la operación la pone tu equipo o un proveedor de servicios certificado), consulta 14 oct 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.

- stellarcyber.ai/partners/find-mssp/ (Diferencias que se notan en el día a día)
- stellarcyber.ai/platform/universal-endpoint-detection-and-response-... (Diferencias que se notan en el día a día)
- docs.stellarcyber.ai/6.6.x/Configure/Adm-in-Licensing-Compliance.htm (Diferencias que se notan en el día a día)
- stellarcyber.ai/resources/stellar-cyber-pricing/ (Diferencias que se notan en el día a día)
- stellarcyber.ai/automatically-triage-phishing-emails-with-stellar-c-... (Diferencias que se notan en el día a día)
- stellarcyber.ai/platform/capabilities-autonomous-soc/ (Agentes de IA que investigan y filtran las alertas...)
- stellarcyber.ai/platform/automated-threat-hunting/ (Compuerta Humana: una persona aprueba cada acción...)
- stellarcyber.ai/ai-investigator-natural-language-threat-hunting/ (Asistente de investigación con IA en el portal, que...)
- stellarcyber.ai/news/press-releases/stellar-cyber-becomes-a-platfor... (Operación en LATAM, EE.UU. y Europa, con analistas en...)
- stellarcyber.ai/es/ (Analistas, soporte y portal en español nativo)
- stellarcyber.ai/enterprise/compliance-and-reporting/ (Reportes para dirección en español y en lenguaje de...)
- success.stellarcyber.ai (Tiempos de notificación e inicio de investigación...)
- docs.stellarcyber.ai/6.6.x/Using/Respond/Reports-Scheduled.htm (Resumen ejecutivo cada mañana: lo que pasó en las...)
- stellarcyber.ai/customer-success/ (Gerente técnico de cuenta (TAM) asignado y revisiones...)
- stellarcyber.ai/customer-support/ (Contacto 24/7 con personas de soporte o seguridad)
- security.stellarcyber.ai/ (Certificación independiente de la operación (ISO 27001...))
- docs.stellarcyber.ai/prod-docs/6.5.x/Installation/Server-Sensor-OS.htm (Arranque rápido con un agente de software: la actividad...)
- docs.stellarcyber.ai/6.6.x/Common/Home-XDR-Kill-Chain-Understanding... (Monitoreo continuo y correlación de eventos (SIEM),...)
- docs.stellarcyber.ai/6.6.x/Installation/Sensor-Types-Introduction.htm (Detección de intrusos (IDS/IPS))
- stellarcyber.ai/threat-intelligence-built-in-not-bolted-on/ (Investigaciones documentadas y enriquecidas con...)
- docs.stellarcyber.ai/6.6.x/Using/Cases/Cases-Main.htm (Gestión de incidentes con bitácora y tiempo de atención...)
- docs.stellarcyber.ai/6.6.x/Using/Cases/Cases-Detail-Response-Tab.htm (Respuesta con aislamiento de equipos y bloqueo de...)
- stellarcyber.ai/stellar-cyber-services/ (Respuesta a incidentes con análisis de causa raíz)
- stellarcyber.ai/identity-threat-detection-response-itdr/ (Postura de identidad: MFA, cuentas privilegiadas y...)
- stellarcyber.ai/platform/ (Zero Trust: DNS seguro, acceso a aplicaciones y control...)
- stellarcyber.ai/uc/multi-cloud-security/ (Seguridad en la nube: alertas y postura)
- stellarcyber.ai/mitre-attck-coverage-analyzer/ (Recomendaciones de seguridad priorizadas con flujo de...)
- docs.stellarcyber.ai/6.6.x/Using/Investigate/Asset-Analytics-Main.htm (Inventario unificado de activos y de software)
- docs.stellarcyber.ai/6.6.x/Configure/Connectors/1-Connectors-List.htm (Vulnerabilidades priorizadas por gravedad y...)
- docs.stellarcyber.ai/6.4.xs/Common/Stellar-Description.htm (Recuperación ante desastres con simulacros y tiempo de...)
- docs.stellarcyber.ai/6.6.x/Configure/System-Licensing.htm (Precio por dispositivo, con planes que se suman)
- stellarcyber.ai/schedule-proof-of-concept/ (Prueba gratuita en tu entorno real)

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.