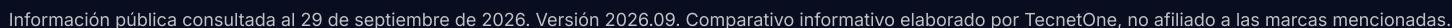


Con Vicarius, tu equipo arma grupos, reglas y reportes, responde por los plazos y necesita su propio EDR y SIEM; nadie del fabricante vigila tu entorno. **TecnetSOC es un servicio: el SOC parchea, críticos en 48 horas como objetivo.**



Vicarius es una herramienta de remediación de vulnerabilidades que tu equipo opera; no es un servicio de SOC administrado. Lo demás que necesitarías (EDR, SIEM, RMM, respaldo) se compra y se opera por separado, y no todo se integra de forma nativa. Este comparativo muestra, capacidad por capacidad, qué parte de lo que incluye TecnetSOC cubre Vicarius por sí sola y qué tendrías que sumar en productos, contratos y personal.

— LO QUE NOS HACE DISTINTOS

Diferencias que se notan en el día a día

01
Compras software, tú lo operas

CON VICARIUS
Compras una plataforma: tu equipo crea grupos, reportes y automatizaciones en cada cliente, según sus requisitos y acuerdos de nivel de servicio (SLA), y los mantiene. [\[1\]](#)

CON TECNETSOC
Contratas un servicio: analistas propios de TecnetOne operan 24/7 y el SOC ejecuta el parcheo, no tu equipo.

02
Nadie vigila a las 3 a.m

CON VICARIUS
No hay analistas del fabricante vigilando tu entorno: es software de remediación y su equipo entra después del incidente, para recuperar y endurecer. [\[2\]](#)

CON TECNETSOC
Analistas en tu zona horaria operan 24/7; en crítico, notificación e inicio de investigación en 30 minutos, como objetivo.

03
EDR y SIEM corren por tu cuenta

CON VICARIUS
Necesitas tu propio EDR y tu propio SIEM: la plataforma toma sus señales sin reemplazar ninguno, y cada uno se licencia y opera por separado. [\[3\]](#)

CON TECNETSOC
El plan más completo incluye EDR/XDR en cada equipo y SIEM con correlación MITRE ATT&CK, operados por el SOC.

04
El plazo de parcheo es tuyo

CON VICARIUS
Eliges parchear bajo demanda, por ventana o por regla; el fabricante no publica plazos de instalación y cumplirlos depende de tu equipo. [\[4\]](#)

CON TECNETSOC
El SOC aplica parches con objetivos escritos: críticos en 48 h, importantes 7 días, rutina 30 días, dentro de tus ventanas.

05
Correo, identidad y red: fuera

CON VICARIUS
Cubres vulnerabilidades y parches; correo, phishing, identidades, red interna y superficie externa quedan fuera, y cada frente pide otro producto y otra consola. [\[3\]](#)

CON TECNETSOC
El plan más completo suma seguridad de correo, simulaciones de phishing, identidad, NDR y superficie externa en un servicio.

06
Normas mexicanas, fuera del mapa

CON VICARIUS
La remediación se mapea a marcos como NIST, CIS e ISO 27001; CNBV, LFPDPPP o NOM-024 no figuran y no se presenta como plataforma GRC. [\[5\]](#)

CON TECNETSOC
El complemento TecnetGRC (costo aparte, se contrata por cada norma) cubre ISO 27001, SOC 2, PCI DSS, CNBV, LFPDPPP y NOM-024 con portal del auditor.

— DÓNDE ESTÁ LA DIFERENCIA

Las tres áreas con más diferencia

Detección y respuesta

TecnetSOC **15**

Vicarius **0**

de 15 capacidades completas en esta área

Operación y servicio

TecnetSOC **14**

Vicarius **1**

de 14 capacidades completas en esta área

Exposición y gestión de TI

TecnetSOC **12**

Vicarius **6**

de 12 capacidades completas en esta área

— CAPACIDAD POR CAPACIDAD

TecnetSOC y Vicarius, lado a lado

Capacidad	TecnetSOC	Vicarius Remediación	Evidencia sobre Vicarius
☒ 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 +2 parciales	
Centro de operaciones (SOC) 24/7 con analistas humanos	☒	Lo pone tu equipo	Software que opera el proveedor de TI; no es SOC ni MDR [3]
Agentes de IA que investigan y filtran las alertas antes de pasarlas a un analista	☒	☒	Su IA prioriza vulnerabilidades y genera scripts; no investiga alertas [6]
Compuerta Humana: una persona aprueba cada acción crítica antes de ejecutarse	☒	☒	Sin servicio con aprobación humana; el proveedor de TI configura la remediación [7]
Asistente de investigación con IA en el portal, que cita sus fuentes	☒ Neo	☒	Sin analista de guardia con IA en el portal [3]

Capacidad	TecnetSOC	Vicarius Remediación	Evidencia sobre Vicarius
☒ 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 en LATAM, EE.UU. y Europa, con analistas en tu zona horaria	☒	Lo pone tu equipo	Sin operación ni enfoque LATAM visible [3]
Analistas, soporte y portal en español nativo	☒	☐	Soporte y material en inglés [3]
Reportes para dirección en español y en lenguaje de negocio	☒	☐	Dashboards técnicos en inglés, no reportes de negocio en español [8]
Tiempos de notificación e inicio de investigación publicados por severidad	☒ Crítico: 30 min (objetivo)	Lo pone tu equipo	Sin compromisos de notificación por severidad; no es servicio [3]
Resumen ejecutivo cada mañana: lo que pasó en las últimas 24 horas	☒ 07:30	Lo pone tu equipo	Sin resumen ejecutivo diario [3]
Reportes automáticos semanales, mensuales, trimestrales y anuales	☒	☐	Reportes de la herramienta; cadencias automáticas no confirmadas [8]
Gerente técnico de cuenta (TAM) asignado y revisiones trimestrales	☒	Lo pone tu equipo	Sin TAM ni revisiones trimestrales publicadas [3]
Contacto 24/7 con personas de soporte o seguridad	☒	☐	Sin evidencia pública de soporte 24/7 [3]
Certificación independiente de la operación (ISO 27001 o SOC 2 Tipo II)	☒ ISO/IEC 27001:2022	☒	Declara SOC 2 Tipo II; sin certificación ISO 27001 propia publicada [9]
Arranque rápido con un agente de software: la actividad de tus dispositivos, visible en horas	☒ Típico: 2 a 4 horas	☐	SaaS con agente de despliegue rápido; sin tiempo de arranque publicado [3]
Detección y respuesta	15 de 15 	0 completas +2 parciales	
Monitoreo continuo y correlación de eventos (SIEM), alineado con MITRE ATT&CK (marco de referencia de técnicas de ataque)	☒	☐	No es SIEM [3]
Protección avanzada en cada equipo (EDR/XDR): malware, ransomware y explotación de vulnerabilidades	☒	☐	vShield protege en memoria contra explotación; no es EDR ni antimalware [10]
Filtrado web en el equipo	☒	☐	Sin filtrado web [3]
Detección de intrusos (IDS/IPS)	☒	☐	Sin IDS/IPS [3]
Detección de amenazas en la red interna (NDR)	☒	☐	Sin NDR [3]
Investigaciones documentadas y enriquecidas con inteligencia de amenazas	☒	☐	Inteligencia aplicada a vulnerabilidades, no a investigación de incidentes [6]
Gestión de incidentes con bitácora y tiempo de atención medido por caso	☒	☐	Sin gestión de incidentes [3]
Respuesta con aislamiento de equipos y bloqueo de direcciones IP	☒	☐	Sin aislamiento de equipos ni bloqueo de IP [3]
Respuesta a incidentes con análisis de causa raíz	☒	Lo pone tu equipo	Sin respuesta a incidentes ni forense [3]
Postura de identidad: MFA, cuentas privilegiadas y acceso condicional	☒	☐	Sin postura de identidad [3]
Zero Trust: DNS seguro, acceso a aplicaciones y control de aplicaciones no autorizadas (shadow IT)	☒	☐	Sin Zero Trust [3]
Seguridad en la nube: alertas y postura	☒	☐	Sin seguridad de Azure [3]
Seguridad de correo: spam, phishing, malware y fraude por suplantación (BEC)	☒	☐	Sin seguridad de correo [3]
Concientización: simulaciones de phishing y entrenamiento con métricas	☒	☐	Sin concientización [3]
Recomendaciones de seguridad priorizadas con flujo de aprobación	☒	☐	Cola de remediación priorizada por vScore; sin flujo de aprobación documentado [6]

Capacidad	TecnetSOC	Vicarius Remediación	Evidencia sobre Vicarius
☒ 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			
Exposición y gestión de TI	12 de 12	6 completas +0 parciales	
Inventario unificado de activos y de software	☒	☒	Inventario de activos y aplicaciones con agente [11]
Vulnerabilidades priorizadas por gravedad y probabilidad de explotación (CVSS, EPSS)	☒	☒	vScore combina CVSS, EPSS, KEV y contexto del activo [12]
Prioridad a las fallas que ya se están explotando (catálogo KEV de CISA)	☒	☒	Usa el catálogo KEV de CISA en la priorización [12]
Parcheo de sistema operativo y aplicaciones de terceros	☒	☒	vPatch: SO y miles de apps de terceros (cifra de Vicarius) [7]
Parcheo operado por el proveedor, con plazos publicados por severidad	☒ Críticos: 48 h (objetivo)	Lo pone tu equipo	El proveedor de TI ejecuta el parcheo; sin tiempos publicados [3]
Verificación de cierre: el escáner confirma que la vulnerabilidad desapareció	☒	☒	Revalida cada corrección y confirma que la vulnerabilidad desapareció [13]
Validación de parches en grupo piloto antes del despliegue	☒	☒	Grupos de activos para probar remediaciones antes del despliegue general [8]
Superficie de ataque externa: lo que tu empresa expone en Internet, con puntaje de riesgo	☒ Puntaje 0 a 100	☐	Considera exposición a Internet en el score; sin EASM ni score externo [14]
Alertas de dominios que imitan tu marca y de credenciales o claves expuestas	☒	☐	Sin alertas de dominios imitadores ni de secretos expuestos [3]
Prueba de penetración (pentest) anual	☒ Anual	Lo pone tu equipo	Sin pentesting [3]
Gestión remota de equipos (RMM)	☒	☐	No es RMM [3]
Monitoreo de disponibilidad (NOC)	☒	☐	Sin monitoreo de disponibilidad ni NOC [3]
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 [3]
Bóveda de respaldo inmutable (no se puede alterar ni borrar), aislada por cliente	☒ Complemento	☐	Sin bóveda inmutable [3]
Recuperación ante desastres con simulacros y tiempo de recuperación (RTO) medido	☒ Complemento RTO medido	☐	Sin recuperación ante desastres [3]
Cumplimiento	6 de 6	0 completas +2 parciales	
Evidencia mensual lista para auditores y aseguradoras	☒ Mensual	☐	vComply genera reportes CIS, PCI DSS, HIPAA, CMMC; no evidencia mensual integral [5]
Preparación para ISO 27001, SOC 2 y PCI DSS con controles compartidos	☒ Complemento	☐	Mapea controles de vulnerabilidades a marcos; no es plataforma GRC [5]
Preparación normativa mexicana: CNBV Fintech, protección de datos (LFPDPPP) y NOM-024	☒ Complemento	☐	Sin normativa mexicana [3]
Gestión de riesgos, controles, declaración de aplicabilidad y auditorías internas	☒ Complemento	☐	Sin gestión de riesgos, SoA ni auditorías internas [3]

Capacidad	TecnetSOC	Vicarius Remediación	Evidencia sobre Vicarius
☒ 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			
Portal para tu auditor con sala de evidencias y página pública de confianza (trust center)	☒ Complemento	☒	Tiene Trust Center propio, no para clientes del proveedor de TI [9]
Continuidad de negocio, riesgo de proveedores y gestión de brechas de datos	☒ Complemento	☒	Sin continuidad, proveedores ni brechas [3]
Cómo se contrata	No suma al conteo		
Precio por dispositivo, con planes que se suman	☒ Por dispositivo	☒	Por activo con cotización a la medida; sin planes acumulativos publicados [15]
Plan gratuito para empezar	☒ Hasta 10 dispositivos	☒	Sin plan gratuito permanente [16]
Prueba gratuita en tu entorno real	☒ 30 días	☒	Ofrece prueba gratis; duración no publicada [17]
Disponible con la marca de tu proveedor de TI	☒	☒	Consola multiempresa y programa de partners; sin marca blanca documentada [18]
Cobertura completa	50	7 +6 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.

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 Vicarius: Vicarius vRx (plataforma completa: vPatch, vShield, vScore, vScript y ScriptAI, vComply, vIntelligence; edición proveedor de TI multiempresa), 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. customer-portal.vicarius.io/vrx-for-mssps (Diferencias que se notan en el día a día)
2. www.vicarius.io/articles/vrx-for-incident-response (Diferencias que se notan en el día a día)
3. www.vicarius.io/ (Diferencias que se notan en el día a día)
4. www.vicarius.io/features/patch-management (Diferencias que se notan en el día a día)
5. [www.vicarius.io/articles/from-vulnerability-management-to-compliance...](https://www.vicarius.io/articles/from-vulnerability-management-to-compliance) (Diferencias que se notan en el día a día)
6. www.vicarius.io/features/vrx-analysis (Agentes de IA que investigan y filtran las alertas...)
7. www.vicarius.io/solution/vulnerability-remediation (Compuerta Humana: una persona aprueba cada acción...)
8. customer-portal.vicarius.io/vrx-user-guide (Reportes para dirección en español y en lenguaje de...)
9. www.vicarius.io/trust (Certificación independiente de la operación (ISO 27001...))
10. www.vicarius.io/articles/virtual-patching-legacy-software (Protección avanzada en cada equipo (EDR/XDR): malware,...)
11. customer-portal.vicarius.io/assets (Inventario unificado de activos y de software)
12. www.vicarius.io/articles/cvss-vs-epss-vs-kev-which-score-actually-matters (Vulnerabilidades priorizadas por gravedad y...)
13. [www.vicarius.io/articles/introducing-vrx-2-0-the-platform-that-scans...](https://www.vicarius.io/articles/introducing-vrx-2-0-the-platform-that-scans) (Verificación de cierre: el escáner confirma que la...)
14. www.vicarius.io/solution/continuous-exposure-management (Superficie de ataque externa: lo que tu empresa expone...)
15. www.vicarius.io/pricing (Precio por dispositivo, con planes que se suman)
16. www.g2.com/products/vrx-by-vicarius/pricing (Plan gratuito para empezar)
17. www.capterra.com/p/201047/vrx/ (Prueba gratuita en tu entorno real)
18. www.vicarius.io/solution/vicarius-vrx-for-teams-secops-and-vulnerability (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.