CIBERLABS®

NOC

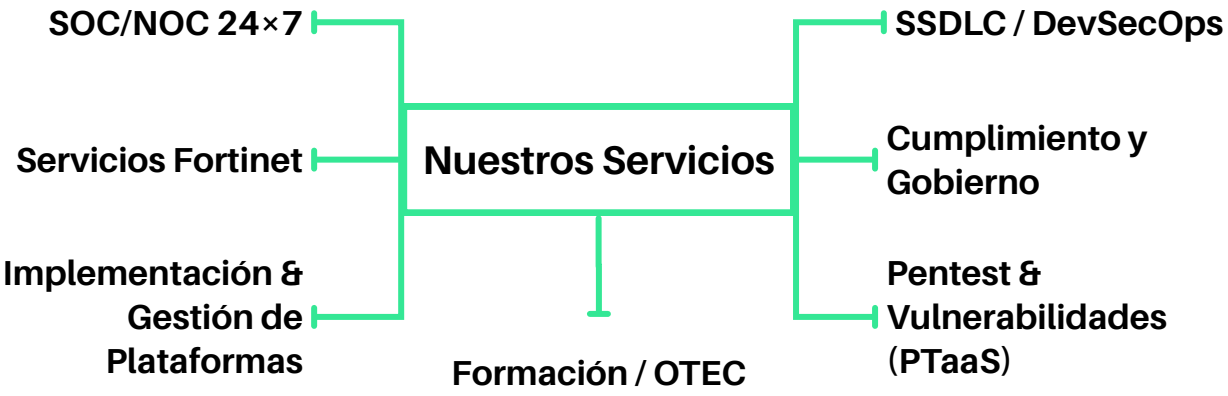
Catálogo de servicios

2025

Servicios Ciberlabs

Somos una empresa de profesionales de diferentes áreas tecnológicas, en constante capacitación y asumiendo variados desafíos con nuestros clientes, siempre enfocados en entregar un servicio de excelencia.

Cada día, nuestros clientes, nos siguen confiando tareas cruciales al minuto de tomar decisiones de inversión tecnológica o el camino a seguir en cuanto a la protección de sus activos digitales.



1. Servicio NOC

El servicio Network Operation Center (NOC) se orienta a la vigilancia, gestión y soporte operacional de la infraestructura tecnológica del cliente, con foco en la continuidad, disponibilidad y desempeño de los sistemas bajo contrato. Esta propuesta expone el alcance operativo del NOC.

2. Alcance y enfoque del servicio

Este servicio NOC se centra en la supervisión constante de parámetros de salud y disponibilidad (CPU, memoria, uso de disco, latencia, estado de servicios, conectividad, entre otros) y en la gestión operativa de los equipos contratados. Se alinea con buenas prácticas y con requisitos legales aplicables. No considera aspectos de ciberseguridad activa.

3. NOC vs. SOC

Es importante comprender la diferencia entre los servicios NOC y SOC para evitar solapamientos y expectativas incorrectas:

	NOC	SOC
Objetivo	Mantener la disponibilidad, rendimiento y operatividad de la infraestructura.	Detección, análisis y respuesta a amenazas y ataques de seguridad informática.
Actividades Tipicas	Monitoreo de sistemas, gestión de incidencias operativas, escalamiento técnico, gestión de parches operativos, reportes de disponibilidad.	Detección de intrusiones, correlación avanzada de eventos, threat hunting, análisis forense, respuesta a incidentes de seguridad y coordinación con autoridades en caso de delitos informáticos.
Alcance de respuesta	Contención operativa, reinicios controlados, coordinación con equipos de soporte técnico y escalamiento a especialistas.	Estas actividades requieren capacidades, herramientas (SIEM, EDR), procesos y experiencia especializados que no están incluidos en el servicio NOC base.

4. Condiciones sobre Almacenamiento de Logs y Evidencia

Por diseño, el servicio NOC incluye la recolección de métricas y alertas operativas necesarias para la vigilancia de salud y disponibilidad. Sin embargo, el almacenamiento centralizado de logs (retención de registros para análisis forense, cumplimiento o investigación legal) no está incluido en la modalidad base y debe ser gestionado mediante una de las siguientes opciones:

Opción A - Servicio adicional cotizable: Podemos proveer un servicio gestionado de recolección y retención de logs (capacidad, políticas de retención, acceso y análisis). Este servicio se cotiza por separado y puede incluir la provisión de infraestructura, configuraciones y paneles de tendencias.

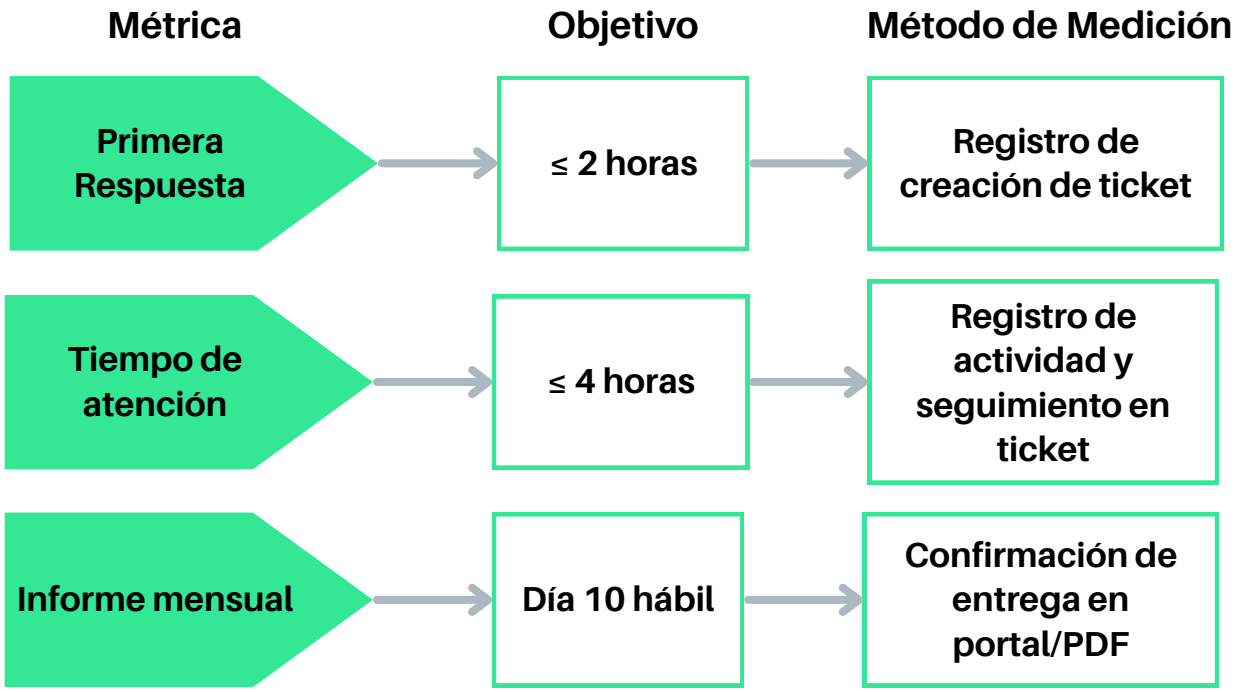
Opción B - Infraestructura aportada por el cliente: El cliente provee un servidor o plataforma con las capacidades necesarias (almacenamiento, CPU, conectividad y acceso) para que nuestros sistemas recolecten y analicen los registros. En este caso, la implementación y pruebas de integración se consideran parte del onboarding.

Importante: *La ausencia de almacenamiento centralizado de logs puede limitar la capacidad de cumplir ciertos requerimientos legales o realizar análisis forenses detallados. Si el cliente requiere cumplir obligaciones de conservación de registros (por ejemplo, para investigaciones legales según Ley 21.459 o requisitos de auditoría), debe considerar expresamente la opción de retención de logs o garantizar infraestructura propia adecuada.*

5. Alcances Operativos

Modalidades	**Básico** 9×5: Lun–Vie 09:00–18:00
	Extendido 12×5: Horarios diurnos a convenir
	Full 24×7
Equipos cubiertos	Pack base desde 50 dispositivos (upgrade disponible)
Sensores por equipo	Hasta **20** sensores base por equipo (sensores adicionales cotizables)
On-Call Emergencias	**Horario hábil**: Ingeniero disponible. **Horario No hábil**: Ingeniero disponible hasta 10 HH/mes fuera de horario (no acumulables)
Reportes Infraestructura y Servicios	**Mensual**, en PDF y portal web (Entrega: Día 10 hábil) **On Demand,** en PDF y portal web (Entrega: en 5 hábiles)
Nota	El servicio NOC no incluye seguridad especializada (SIEM gestionado, threat hunting, análisis forense avanzado o respuesta avanzada a incidentes de seguridad). Estas capacidades se ofrecen como servicios adicionales (SOC).

6. Métricas y SLA



7. Cumplimiento Legal y Notas sobre Evidencia

El servicio NOC incorpora controles y procesos que contribuyen al cumplimiento de:

- Ley 21.459: Delitos informáticos (detección inicial y conservación de registros cuando aplica).
- Ley 21.663: Marco de ciberseguridad (gestión de disponibilidad y resiliencia).
- Ley 21.719: Protección de datos personales (medidas de disponibilidad y clasificación básica).

Sin embargo, para aspectos que dependen de la conservación a largo plazo de registros (logs) o análisis forense profundo, es imprescindible considerar el servicio adicional de retención de logs o proveer infraestructura adecuada, tal como se describe en la sección Condiciones sobre Almacenamiento de Logs y Evidencia.

8. Servicio vs. Cumplimiento

Tópico de Servicio	Ley 21.459	Ley 21.663	Ley 21.719	NIST CSF	ISO 27001 (Anexo A)
Monitoreo y Detección (salud/disp.)	Contribuye a detección inicial	Reporte de incidentes infraestructuras críticas	-	Detect (DE)	A.12.4; A.16
Gestión de Incidentes (operativos)	-	Gestión de continuidad y escalamiento	-	Respond (RS)	A.16.1.4; A.17
Vulnerabilidades y Parcheo	-	Identificación de vulnerabilidades operativas	-	Identify (ID)	A.12.6; A.18
Control de Accesos (operativo)	Prevención accesos no autorizados	-	Acceso restringido; trazabilidad	Protect (PR)	A.9; A.9.4
Encriptación y Protección de Datos	-	-	Confidencialidad de datos personales	Protect (PR)	A.10; A.8.2
Gestión de Logs	Conservación cuando aplica (ver sección 4)	-	Registro de tratamientos de datos	Detect (DE)	A.12.4; A.18.1.4
Privacidad y Datos Personales	-	-	Apoya principios de proporcionalidad y finalidad	Identify (ID)	A.18.1.3
Continuidad y Recuperación	-	Resiliencia infraestructuras críticas	-	Recover (RC)	A.17.1; A.17.2

9. Beneficios y Limitaciones

Beneficios:

- Visibilidad operacional y reducción de tiempos de respuesta.
- Cumplimiento operativo de requisitos legales relacionados con disponibilidad y resiliencia.
- Flexibilidad para ampliaciones y contratación de servicios de seguridad especializados.

Limitaciones:

- No incluye servicios de SOC (detección avanzada de amenazas, threat hunting, análisis forense avanzado, SIEM gestionado).
- Almacenamiento y retención de logs para fines forenses o regulatorios requieren contratación adicional o infraestructura aportada por el cliente.

Referencias legales:

- Ley 21.459: https://www.bcn.cl/leychile/navegar?idNorma=1177743
- Ley 21.663: https://www.bcn.cl/leychile/navegar?i=1202434
- Ley 21.719: https://www.bcn.cl/leychile/navegar?idNorma=1209272

Condiciones Comerciales

Servicio NOC

- Este servicio está pensado para apoyar el registro de salud de sus servidores/servicios.
- Gestión telefónica de solicitudes.
- Modalidad de atención 24x7 o 9x5 remota.
- Soporte de Gestión y Administración compartida del networking.
  - Soporte N1 modalidad 24x7 o 9x5 .
  - Soporte N2 y N3 actividades programadas modalidad 12x5.
  - Soporte Emergencias N2 y N3, según criticidad.
- Reportería Infraestructura y Servicios.
- Reunión mensual de coordinación y entrega de informes.

Este servicio contempla la implementación de los sistemas de monitoreo y aprendizaje de aplicativos/cliente/equipo críticos de continuidad operativa del cliente :

- Entrega en 2-3 semanas.
- Dashboards y alertas base.
- Handover + documentación.
- Reunión Inicio de servicio (máximo 2 horas).

Contáctanos para obtener tu cotización

CIBERLABS®

Contáctenos:

contacto@ciberlabs.cl

+56947017161

Guardia Vieja 181 Oficina 204, Providencia, Santiago.

www.ciberlabs.cl

linkedin.com/company/ciberlabs/