Propuesta de implementación de servicios de seguridad de la información bajo un modelo de outsourcing

INTEGRANTES:
JOSE IGNACIO GONZÁLEZ PABÓN

DOCENTE:
JORGE MAURICIO SEPÚLVEDA CASTAÑO

CORPORACIÓN UNIVERSITARIA REMINGTON
INGENIERIA EN SISTEMAS
OUTSOURCING EN TI
MEDELLÍN, COLOMBIA
28-03-2026

Tabla de contenido

1. Introducción 7
2. Palabras clave 7
3. Marco Conceptual y Contextual 7
3.1 Contexto actual de la ciberseguridad 7
3.2 Outsourcing en Tecnologías de la Información 8
3.3 Seguridad de la información 8
3.4 Gestión de servicios de TI 8
3.5 Acuerdos de Nivel de Servicio (ANS) 9
3.6 Infraestructura tecnológica en empresas medianas 9
3.7 Importancia del factor humano en la seguridad 9
4. Análisis De Necesidades Del Cliente 10
4.1 Perfil del cliente objetivo 10
4.2 Situación actual identificada 11
4.3 Riesgos principales del entorno 12
Riesgos sobre infraestructura 12
Riesgos sobre sistemas 12
Riesgos sobre usuarios 12
4.4 Brechas operativas detectadas 13
5. Diseño Del Servicio De Ciberseguridad 15
5.1 Objetivo del diseño del servicio 15
5.2 Componentes del servicio 15
5.2.1 Servicio de monitoreo SOC 7x24 15
5.2.2 Gestión de incidentes 16
5.2.3 Gestión de vulnerabilidades 17
5.2.4 Gestión de identidades y accesos (IAM) 17

5.2.5 Respaldo y recuperación 18
5.2.6 Capacitación y concientización 19
5.3 Enfoque por capas 19
6. Arquitectura Técnica Del Servicio 20
6.1 Arquitectura lógica del servicio 20
6.2 Integración de componentes 21
6.3 Flujo de eventos y respuesta 22
6.4 Cobertura sobre la infraestructura del cliente 23
6.5 Alta disponibilidad y continuidad 24
6.6 Escalabilidad del servicio 24
7. Modelo Operativo Del Servicio 25
7.1 Objetivo del modelo operativo 25
7.2 Estructura operativa por niveles 25
Nivel 1 (N1) – Monitoreo y atención inicial 25
Nivel 2 (N2) – Análisis especializado 25
Nivel 3 (N3) – Especialistas y arquitectura 26
7.3 Mesa de servicio y gestión de tickets 27
Herramientas sugeridas 27
7.4 Turnos y cobertura operativa 28
7.5 Flujo de atención de incidentes 28
7.6 Gobierno del servicio 28
Comité operativo semanal 29
Comité mensual de servicio 29
Comité ejecutivo trimestral 29
7.7 Gestión documental y reportes 29
Reporte técnico semanal 29
Reporte ejecutivo mensual 30

Reporte trimestral 30
7.8 Integración con usuarios y áreas del cliente 30
8. Implementación Del Servicio 30
8.2 Fase 1 – Diagnóstico y levantamiento inicial 31
8.3 Fase 2 – Diseño detallado de la solución 32
8.4 Fase 3 – Despliegue de herramientas 32
8.5 Fase 4 – Integración y pruebas piloto 33
8.6 Fase 5 – Capacitación y transferencia de conocimiento 33
8.7 Fase 6 – Puesta en producción 34
8.8 Fase 7 – Estabilización y mejora continua 34
8.9 Cronograma de implementación sugerido 35
8.10 Riesgos del proyecto y mitigación 35
9. Acuerdo De Nivel De Servicio (ANS) 36
9.1 Objetivo del ANS 36
9.2 Alcance del ANS 36
9.3 Métricas y niveles de servicio 36
Disponibilidad del servicio 36
Tiempos por severidad 37
9.4 Indicadores clave de desempeño (KPI) 38
9.5 Responsabilidades del proveedor 39
9.6 Responsabilidades del cliente 39
9.7 OLAs (Acuerdos operativos internos) 39
9.8 Capacitaciones dentro del ANS 40
9.9 Exclusiones del servicio 40
9.10 Penalizaciones y compensaciones 40

9.11 Gobierno y revisión del ANS 41
10. Gestión De Herramientas Y Stack Tecnológico 41
10.1 Enfoque de selección tecnológica 41
10.2 Comparativa general: Open Source vs Enterprise 42
10.3 Comparativa por tipo de herramienta 43
SIEM / SOC 43
Gestión de vulnerabilidades 43
IAM (Identidades) 43
Respaldo y Recuperacion 44
Gestión de incidentes 44
10.4 Estrategia Recomendada 44
Escenario 1 (Costo optimizado) 44
Escenario 2 (Balanceado) RECOMENDADO 44
Escenario 3 (Alta madurez) 45
10.5 Justificación del enfoque híbrido 45
11. Resultados Esperados Y Valor Para El Cliente 45
11.1 Objetivo del valor esperado 45
11.2 Resultados esperados a nivel técnico 45
11.3 Resultados esperados a nivel operativo 46
11.4 Resultados esperados sobre usuarios 46
11.5 Resultados esperados en continuidad del negocio 47
11.6 Valor financiero para el cliente 47
11.7 Valor estratégico del servicio 47
11.8 Indicadores de éxito esperados 48
12. Beneficios Del Modelo De Outsourcing 48
12.1 Acceso a talento especializado 48

12.2 Reducción de costos operativos 49
12.3 Escalabilidad del servicio 49
12.4 Cobertura continua 7x24 50
12.5 Adopción acelerada de mejores prácticas 50
12.6 Enfoque en el core del negocio 50
12.7 Mejora continua del servicio 51
12.8 Reducción del riesgo organizacional 51
12.9 Soporte para auditoría y cumplimiento 52
12.10 Ventaja competitiva para el cliente 52
Conclusiones 52
Referencias 53
Estándares y marcos de referencia 53
Artículo sobre riesgo humano 53
Herramientas Open Source 53
Herramientas Enterprise 54

1. Introducción

El presente informe técnico tiene como objetivo diseñar una propuesta para la implementación de servicios de seguridad de la información bajo un modelo de outsourcing. La propuesta está orientada a organizaciones que requieren fortalecer la protección de sus activos tecnológicos mediante la externalización de servicios especializados.

El modelo planteado incluye servicios de monitoreo de seguridad, gestión de incidentes, análisis de vulnerabilidades y control de accesos, complementados con un programa de capacitación continúa dirigido a los usuarios y equipos técnicos. Este enfoque integral se encuentra soportado por un Acuerdo de Nivel de Servicio (ANS) que define métricas, niveles de disponibilidad, tiempos de respuesta y sanciones.

Como resultado, se propone una solución que no solo fortalece la infraestructura tecnológica, sino que también promueve una cultura organizacional orientada a la seguridad de la información.

2. Palabras clave

Ciberseguridad, outsourcing de TI, seguridad de la información, SOC, SIEM, acuerdo de nivel de servicio (ANS), gestión de vulnerabilidades, gestión de identidades y accesos (IAM), continuidad del negocio, monitoreo 7x24.

3. Marco Conceptual y Contextual

3.1 Contexto actual de la ciberseguridad

En la actualidad, las organizaciones dependen ampliamente de los sistemas de información para el desarrollo de sus operaciones. Esta dependencia ha incrementado la exposición a amenazas cibernéticas como ataques de malware, ransomware, phishing y accesos no autorizados.

Las empresas medianas, en particular, presentan un alto nivel de vulnerabilidad debido a limitaciones en recursos tecnológicos, personal especializado y estrategias de seguridad. Esto genera la necesidad de adoptar modelos que permitan fortalecer la protección de la información sin afectar la operación del negocio.

En este contexto, la ciberseguridad deja de ser un componente opcional y se convierte en un elemento estratégico para garantizar la continuidad del negocio y la protección de los activos digitales.

3.2 Outsourcing en Tecnologías de la Información

El outsourcing en Tecnologías de la Información consiste en la delegación de procesos y servicios tecnológicos a proveedores externos especializados. Este modelo permite a las organizaciones optimizar recursos, reducir costos operativos y acceder a tecnologías avanzadas sin necesidad de realizar grandes inversiones.

En el ámbito de la ciberseguridad, el outsourcing permite implementar servicios como monitoreo continuo, gestión de incidentes y análisis de vulnerabilidades, garantizando un nivel de protección más alto frente a amenazas.

Además, este modelo facilita la escalabilidad de los servicios, adaptándose a las necesidades cambiantes de la organización.

3.3 Seguridad de la información

La seguridad de la información se fundamenta en tres principios esenciales:

- **Confidencialidad:** Garantiza que la información solo sea accesible para personas autorizadas.
- **Integridad:** Asegura que la información no sea alterada de manera indebida.
- **Disponibilidad:** Permite que la información esté accesible cuando sea requerida.

Estos principios son la base para la implementación de controles de seguridad en cualquier organización, y su adecuada gestión permite reducir riesgos asociados a incidentes de seguridad.

3.4 Gestión de servicios de TI

La gestión de servicios de Tecnologías de la Información se basa en la implementación de procesos que permiten diseñar, operar y mejorar servicios tecnológicos de manera eficiente.

Marcos de referencia como ITIL y COBIT establecen buenas prácticas para la gestión de incidentes, cambios, problemas y niveles de servicio, facilitando la alineación entre los servicios de TI y los objetivos del negocio.

En el contexto de la ciberseguridad, estos marcos permiten estructurar procesos claros para la detección, análisis y respuesta ante incidentes.

3.5 Acuerdos de Nivel de Servicio (ANS)

Un Acuerdo de Nivel de Servicio (ANS) es un documento formal que establece los compromisos entre un proveedor de servicios y un cliente. En este se definen aspectos como:

- Niveles de disponibilidad
- Tiempos de respuesta
- Métricas de desempeño
- Responsabilidades
- Penalizaciones

El ANS permite garantizar la calidad del servicio y establecer mecanismos de control y seguimiento, siendo un elemento clave en los modelos de outsourcing.

3.6 Infraestructura tecnológica en empresas medianas

Las empresas medianas suelen contar con una infraestructura tecnológica híbrida, compuesta por:

- Servidores locales (on-premise)
- Servicios en la nube (IaaS, PaaS, SaaS)
- Redes internas y externas
- Equipos de usuario final

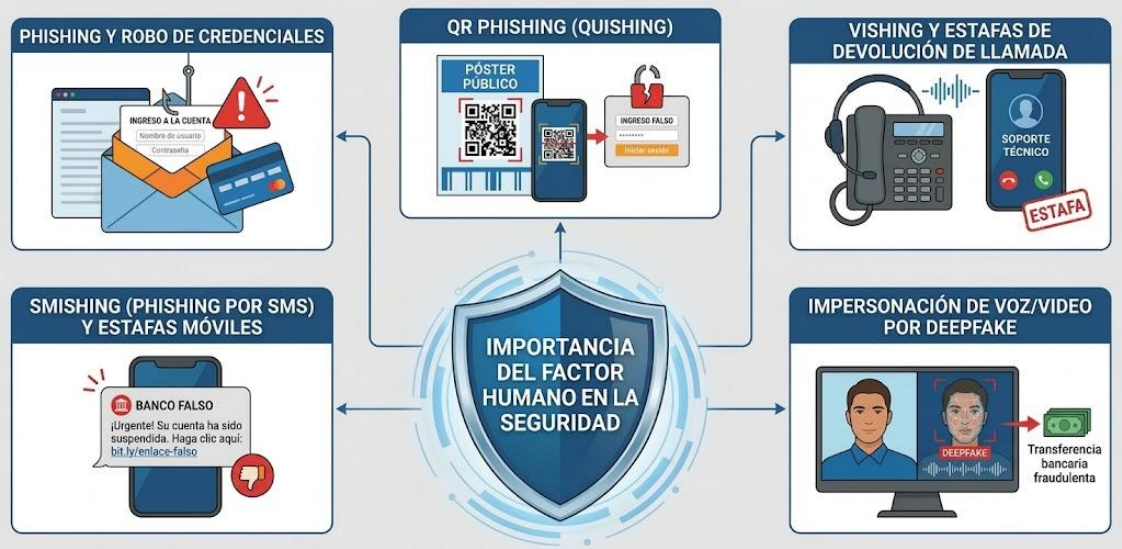
Este tipo de infraestructura presenta múltiples puntos de exposición a amenazas, lo que requiere la implementación de controles de seguridad en diferentes niveles.

3.7 Importancia del factor humano en la seguridad

Uno de los principales vectores de ataque en las organizaciones es el factor humano. Prácticas inadecuadas como el uso de contraseñas débiles, la apertura de correos maliciosos o la falta de conocimiento en seguridad incrementan el riesgo de incidentes.

Por esta razón, la implementación de programas de capacitación y concientización es fundamental para fortalecer la cultura de seguridad dentro de la organización y reducir vulnerabilidades asociadas al comportamiento de los usuarios.

Ilustración 1



Fuente: keepnetlabs - what-is-human-risk-management

3.8 Relación entre outsourcing y ciberseguridad

La integración del outsourcing con la ciberseguridad permite a las organizaciones adoptar un enfoque estratégico basado en:

- Monitoreo continuo
- Respuesta rápida ante incidentes
- Acceso a personal especializado
- Implementación de tecnologías avanzadas

Este modelo no solo mejora la protección de la información, sino que también optimiza la gestión de los servicios y reduce los riesgos operativos.

4. Análisis De Necesidades Del Cliente

4.1 Perfil del cliente objetivo

La propuesta está orientada a una **empresa mediana con infraestructura híbrida estándar**, aplicable a sectores como servicios, comercio, manufactura, logística o tecnología.

Ilustración 2

Fuente: elaboración propia.

Este tipo de organización normalmente cuenta con:

- Infraestructura local con servidores físicos o virtualizados
- Servicios en nube pública o privada
- Aplicaciones corporativas y bases de datos
- Estaciones de trabajo y dispositivos móviles
- Acceso remoto para usuarios internos y terceros
- Dependencia operativa de correo, ERP, CRM y archivos compartidos

Aunque no se trata de un sector específico, el modelo está diseñado para ser **replicable en cualquier empresa mediana que requiera fortalecer su postura de seguridad**.

4.2 Situación actual identificada

En empresas de este tipo es común encontrar debilidades como:

- Monitoreo limitado o inexistente de eventos de seguridad
- Falta de correlación centralizada de logs
- Ausencia de personal especializado 7x24

- Gestión reactiva de incidentes
- Vulnerabilidades sin seguimiento periódico
- Controles de acceso poco maduros
- Copias de seguridad sin pruebas de restauración
- Bajo nivel de capacitación del personal

Estas condiciones generan una exposición alta frente a incidentes de ciberseguridad que pueden afectar la continuidad operativa.

4.3 Riesgos principales del entorno

Con base en el análisis del perfil de empresa objetivo, los principales riesgos identificados son:

Riesgos sobre infraestructura

- Ataques a servidores on-premise y máquinas virtuales
- Exposición de servicios en nube sin controles suficientes
- Movimientos laterales dentro de la red
- Falta de segmentación

Riesgos sobre sistemas

- Vulnerabilidades en aplicaciones internas
- Bases de datos expuestas
- Falta de parchado
- Integraciones inseguras entre plataformas

Riesgos sobre usuarios

- Phishing
- Robo de credenciales
- Uso indebido de privilegios
- Dispositivos no administrados

4.4 Brechas operativas detectadas

Desde la perspectiva del servicio, las brechas más comunes son:

- No existe un SOC o centro de monitoreo formal
- Los eventos no se analizan en tiempo real
- No hay métricas claras de tiempo de respuesta
- No existe ANS definido con terceros
- No hay simulaciones de ataque ni pruebas de phishing
- La respuesta depende del conocimiento puntual del equipo interno

Estas brechas afectan directamente la capacidad de prevención y respuesta.

4.5 Necesidades del cliente

A partir del análisis realizado, se identifican las siguientes necesidades estratégicas:

Necesidades técnicas

- Monitoreo centralizado de infraestructura, nube y endpoints
- Gestión de vulnerabilidades continua
- Integración SIEM + SOC
- Protección de identidades
- Gestión de backups y restauración

Necesidades operativas

- Cobertura 7x24
- Escalamiento por niveles
- Gestión de tickets
- Reportes ejecutivos y técnicos
- Métricas SLA

Necesidades humanas

- Capacitaciones periódicas
- Campañas de concientización

- Simulaciones de phishing
- Evaluaciones técnicas

4.6 Justificación del servicio propuesto

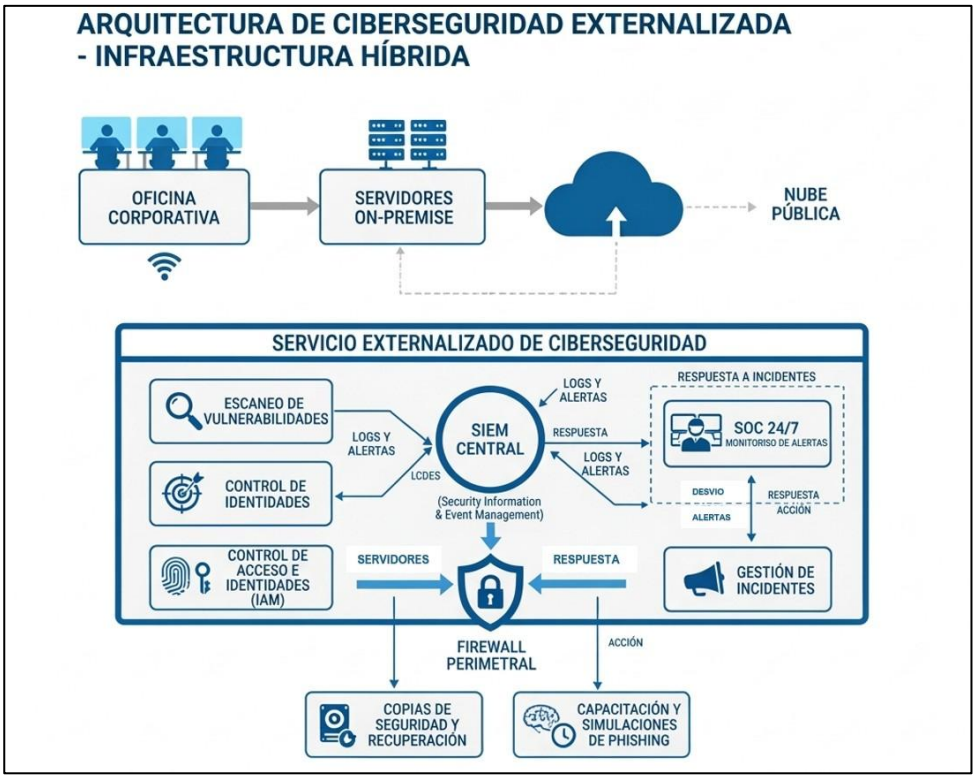
La contratación de un servicio de ciberseguridad bajo outsourcing responde a la necesidad de **cerrar brechas técnicas, operativas y humanas**, mediante un modelo especializado que combine:

- herramientas avanzadas
- personal experto
- procesos definidos
- métricas medibles
- mejora continua

Este enfoque permite a la empresa cliente fortalecer su seguridad sin necesidad de crear una operación interna compleja y costosa.

5. Diseño Del Servicio De Ciberseguridad

Ilustración 3



Fuente: Elaboración Propia.

5.1 Objetivo del diseño del servicio

El diseño del servicio de ciberseguridad tiene como propósito establecer una solución integral que permita a una empresa mediana proteger su infraestructura tecnológica, sistemas de información y usuarios, mediante un modelo de outsourcing especializado.

La propuesta está estructurada bajo un enfoque por capas, cubriendo infraestructura, aplicaciones, identidades, continuidad del negocio y factor humano.

5.2 Componentes del servicio

5.2.1 Servicio de monitoreo SOC 7x24

Descripción

Se implementa un Centro de Operaciones de Seguridad (SOC) encargado del monitoreo continuo de la infraestructura tecnológica, con capacidad de detección temprana de amenazas y respuesta inicial.

Aplicación

- **Infraestructura:** servidores físicos, virtuales y nube
- **Usuarios:** detección de accesos inusuales
- **Sistemas:** logs de aplicaciones críticas

Herramientas

Software libre

- Wazuh
- ELK Stack
- Graylog

Software comercial

- Splunk Enterprise Security
- IBM QRadar
- Microsoft Sentinel

5.2.2 Gestión de incidentes

Descripción

Proceso estructurado para la identificación, clasificación, contención, erradicación y recuperación de incidentes.

Aplicación

- Eventos críticos de infraestructura
- Compromiso de cuentas
- Malware
- indisponibilidad de servicios

Herramientas

Libre

- TheHive
- Cortex

Comercial

- ServiceNow SecOps
- Palo Alto Cortex XSOAR

5.2.3 Gestión de vulnerabilidades

Descripción

Servicio orientado a la identificación proactiva de vulnerabilidades en infraestructura, aplicaciones y nube.

Aplicación

- servidores
- sistemas operativos
- aplicaciones web
- bases de datos
- nube

Herramientas

Libre

- OpenVAS / Greenbone
- Nmap

Comercial

- Tenable Nessus
- Qualys
- Rapid7

5.2.4 Gestión de identidades y accesos (IAM)

Descripción

Protección de usuarios, privilegios y autenticación.

Aplicación

- usuarios administrativos
- accesos VPN
- aplicaciones SaaS
- nube

Herramientas

Libre

- FreeIPA
- Keycloak

Comercial

- Okta
- Azure AD
- CyberArk

5.2.5 Respaldo y Recuperación

Descripción

Garantiza la continuidad operativa ante incidentes como ransomware o pérdida de datos.

Aplicación

- servidores
- bases de datos
- nube
- endpoints críticos

Herramientas

Libre

- Bacula
- UrBackup

Comercial

- Veeam
- Acronis

5.2.6 Capacitación y concientización

Descripción

Programa permanente para reducir el riesgo humano.

Aplicación

- usuarios finales
- líderes
- administradores TI
- terceros

Actividades

- campañas de phishing
- charlas
- talleres
- pruebas técnicas
- ejercicios tabletop

Herramientas

Libre

- GoPhish
- Moodle

Comercial

- KnowBe4
- Proofpoint Security Awareness

5.3 Enfoque por capas

El diseño se implementa en cinco capas:

1. Perímetro
2. Infraestructura
3. Aplicaciones
4. Identidades
5. Usuario final

Este modelo garantiza una defensa en profundidad alineada con estándares de seguridad.

6. Arquitectura Técnica Del Servicio

6.1 Arquitectura lógica del servicio

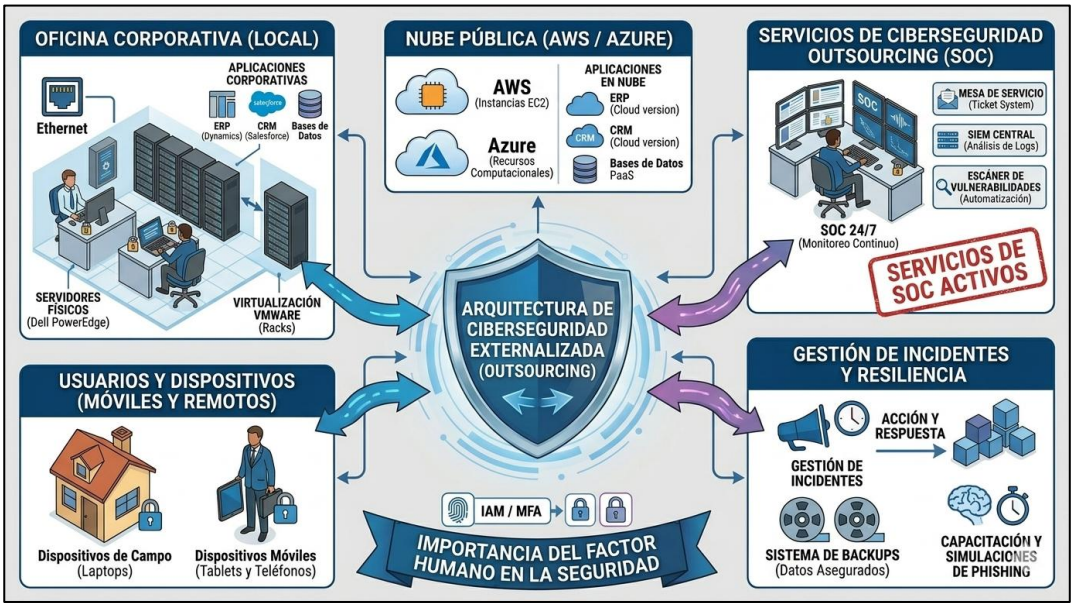
La arquitectura técnica propuesta se basa en un modelo centralizado y escalable que integra la infraestructura local del cliente con servicios en la nube y plataformas de seguridad gestionadas por el proveedor.

El objetivo principal es garantizar visibilidad, correlación de eventos y capacidad de respuesta sobre todos los activos críticos de la organización.

La arquitectura contempla los siguientes dominios:

- Capa de usuario final
- Capa de red y perímetro
- Capa de servidores y virtualización
- Capa de aplicaciones y bases de datos
- Capa de nube pública
- Capa de monitoreo y correlación
- Capa de respaldo y recuperación

Ilustración 4



Fuente: Elaboración Propia.

6.2 Integración de componentes

La solución integra diferentes tecnologías de seguridad dentro de un ecosistema único de monitoreo y respuesta.

Capa de captura

Se instalan agentes o conectores en:

- servidores Windows y Linux
- máquinas virtuales
- equipos de usuario
- aplicaciones críticas
- firewalls
- servicios cloud

Estos componentes envían eventos hacia el SIEM.

Capa de análisis

El SIEM centraliza:

- logs
- eventos
- autenticaciones
- cambios críticos
- alertas de endpoint
- eventos cloud

Posteriormente se aplican reglas de correlación, casos de uso y detección de anomalías.

Capa de operación

El SOC recibe las alertas procesadas y activa el flujo de:

- validación
- clasificación
- severidad
- respuesta
- escalamiento

6.3 Flujo de eventos y respuesta

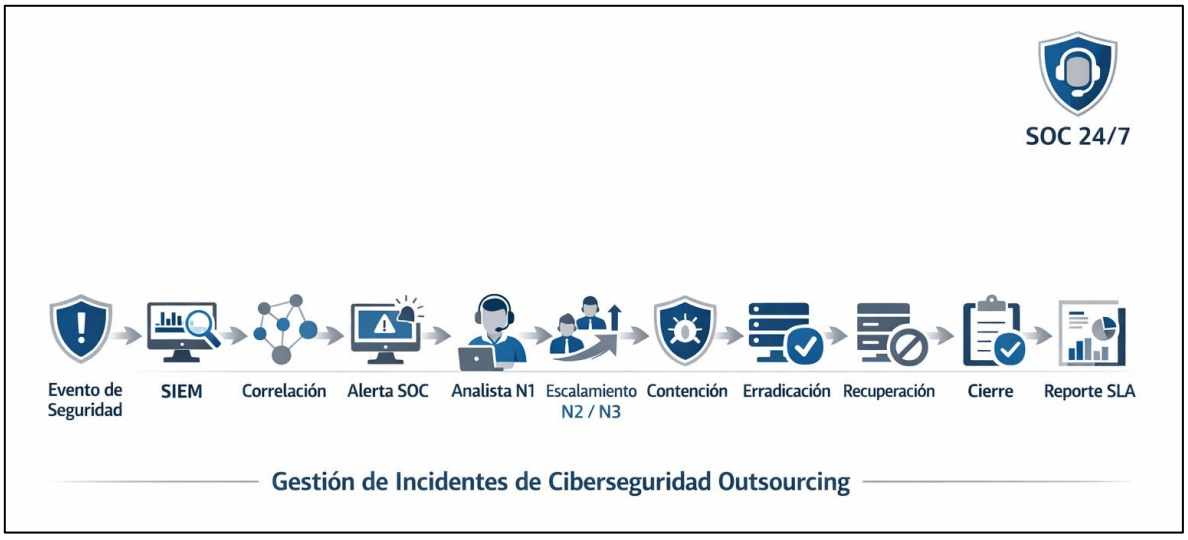
El flujo operativo del servicio sigue la siguiente secuencia:

1. Generación del evento
2. Recolección por agente o syslog
3. Ingesta en SIEM
4. Correlación y clasificación
5. Generación de alerta
6. Atención por analista N1
7. Escalamiento a N2 o N3
8. Contención

9. Recuperación
10. Cierre con documentación SLA

Este flujo garantiza trazabilidad completa del incidente.

Ilustración 5



Fuente: Elaboración Propia.

6.4 Cobertura sobre la infraestructura del cliente

La arquitectura cubre:

Infraestructura

- servidores físicos
- virtualización
- switches
- firewalls
- VPN

Sistemas

- ERP
- CRM
- correo

- bases de datos
- aplicaciones web

Usuarios

- accesos remotos
- MFA
- privilegios
- endpoints

Nube

- workloads AWS / Azure
- buckets
- IAM cloud
- logs cloud

6.5 Alta disponibilidad y continuidad

La arquitectura debe soportar:

- redundancia de SIEM
- respaldo de configuraciones
- failover de componentes críticos
- backup de logs
- DRP de herramientas SOC

Esto garantiza continuidad incluso ante incidentes mayores.

6.6 Escalabilidad del servicio

El modelo permite crecimiento por:

- nuevos usuarios
- nuevas sedes
- nuevos servicios cloud

- nuevas aplicaciones
- mayor volumen de logs

Esto es clave para empresas medianas en expansión.

7. Modelo Operativo Del Servicio

7.1 Objetivo del modelo operativo

El modelo operativo define la forma en que el proveedor prestará el servicio de ciberseguridad outsourcing, estableciendo procesos, roles, responsabilidades, niveles de soporte, turnos de atención y mecanismos de escalamiento.

Su propósito es garantizar una operación continua, controlada y alineada con los niveles de servicio acordados con el cliente.

7.2 Estructura operativa por niveles

La prestación del servicio se organiza mediante un esquema de soporte escalonado que permite responder de manera eficiente a incidentes y requerimientos.

Nivel 1 (N1) – Monitoreo y atención inicial

Responsable de:

- Monitoreo continuo del SIEM y herramientas SOC
- Validación inicial de alertas
- Clasificación de severidad
- Registro y documentación del incidente
- Escalamiento cuando aplique

Este nivel opera como primer filtro operativo.

Nivel 2 (N2) – Análisis especializado

Responsable de:

- Investigación técnica avanzada
- Análisis forense inicial

- Revisión de indicadores de compromiso (IoC)
- Ajuste de reglas de correlación
- Gestión de incidentes medios y altos

Este nivel se enfoca en la contención y análisis detallado.

Nivel 3 (N3) – Especialistas y arquitectura

Responsable de:

- Casos críticos y ataques avanzados
- Respuesta a ransomware
- Amenazas persistentes
- Rediseño de controles
- Hardening y arquitectura

Este nivel involucra especialistas senior y arquitectos de seguridad.

Ilustración 6

Fuente: Elaboración Propia.

7.3 Mesa de servicio y gestión de tickets

Toda interacción con el cliente se centraliza mediante una **mesa de servicio**, que permite:

- Registro de incidentes
- solicitudes
- cambios
- escalamiento
- trazabilidad
- métricas SLA

Herramientas sugeridas

Libre

- GLPI
- Zammad

Comercial

- ServiceNow
- Jira Service Management

7.4 Turnos y cobertura operativa

Dado que el servicio es de seguridad administrada, la operación se establece bajo un esquema:

- **Cobertura 7x24**
- Turnos rotativos
- Guardia para casos críticos
- Escalamiento fuera de horario
- Atención priorizada por severidad

Esto garantiza monitoreo continuo de infraestructura, nube y usuarios.

7.5 Flujo de atención de incidentes

El flujo operativo estándar es:

1. Detección del evento
2. Ingreso al SIEM
3. Validación por N1
4. Escalamiento N2/N3
5. Comunicación con cliente
6. Contención
7. Erradicación
8. Recuperación
9. Cierre y lecciones aprendidas

Este flujo debe integrarse con el ANS.

7.6 Gobierno del servicio

El servicio incluye mecanismos formales de seguimiento:

Comité operativo semanal

Revisión de:

- incidentes
- tendencias
- alertas críticas
- vulnerabilidades

Comité mensual de servicio

Revisión de:

- SLA
- cumplimiento ANS
- indicadores
- planes de mejora
- roadmap

Comité ejecutivo trimestral

Orientado a:

- resultados estratégicos
- riesgo
- madurez
- nuevas inversiones

7.7 Gestión documental y reportes

El proveedor debe entregar:

Reporte técnico semanal

- incidentes
- casos abiertos
- vulnerabilidades
- IOC detectados

Reporte ejecutivo mensual

- KPIs
- SLA
- disponibilidad
- cumplimiento de capacitaciones
- nivel de riesgo

Reporte trimestral

- madurez
- tendencias
- roadmap
- recomendaciones

7.8 Integración con usuarios y áreas del cliente

El servicio se conecta con:

- área TI
- seguridad
- infraestructura
- mesa de ayuda
- líderes de proceso
- usuarios finales

Esto es importante porque aterriza el servicio a la operación del negocio.

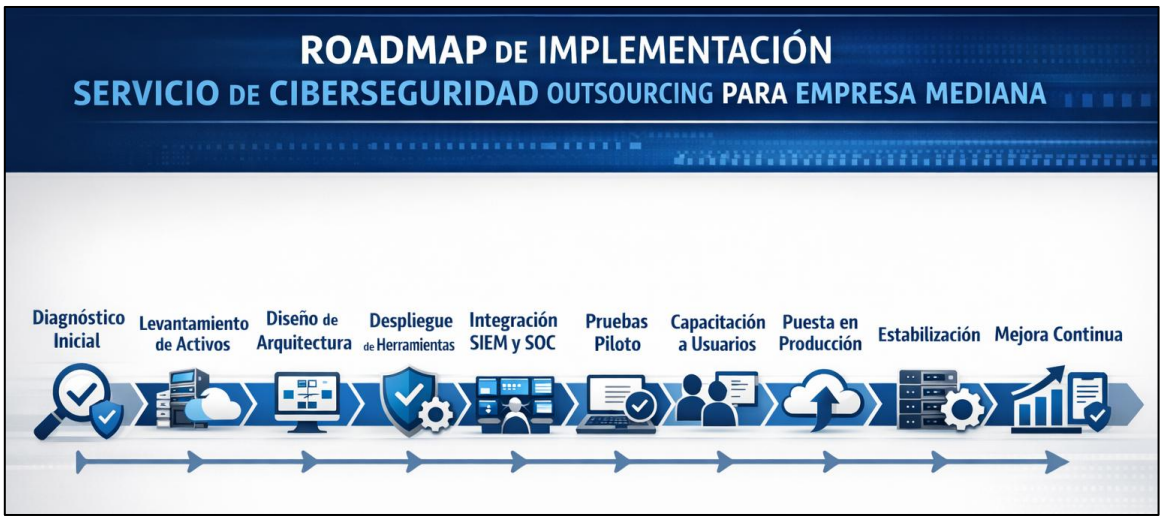
8. Implementación Del Servicio

8.1 Estrategia de implementación por fases

La implementación del servicio se desarrollará mediante un enfoque por fases, con el objetivo de minimizar el impacto sobre la operación del cliente y garantizar una transición controlada hacia el modelo de outsourcing.

Este enfoque permite gestionar riesgos, validar resultados tempranos y ajustar la arquitectura antes de la operación definitiva.

Ilustración 7



Fuente: Elaboración Propia.

8.2 Fase 1 – Diagnóstico y levantamiento inicial

En esta fase se realiza el entendimiento del entorno del cliente.

Actividades

- Inventario de activos tecnológicos
- Identificación de aplicaciones críticas
- Descubrimiento de topología de red
- Levantamiento de servicios cloud
- Identificación de usuarios privilegiados
- Revisión de backups
- Evaluación de madurez actual

Entregables

- Documento de descubrimiento
- Matriz de activos
- Matriz de riesgos inicial
- Priorización de criticidad

8.3 Fase 2 – Diseño detallado de la solución

Con base en el diagnóstico se define la arquitectura final.

Actividades

- Diseño de arquitectura SOC + SIEM
- Selección de herramientas (open source y enterprise)
- Casos de uso de seguridad
- Diseño de conectividad híbrida
- Integración con IAM
- Diseño de backups y DRP

Entregables

- Documento HLD / LLD
- Casos de uso
- Matriz de integración
- Plan de despliegue

8.4 Fase 3 – Despliegue de herramientas

En esta etapa se implementan los componentes técnicos.

Componentes

- SIEM
- agentes
- conectores

- escáner de vulnerabilidades
- IAM
- backups
- ticketing

Actividades

- instalación
- hardening
- conectividad
- pruebas
- alta disponibilidad

8.5 Fase 4 – Integración y pruebas piloto

Antes de pasar a producción se ejecuta una etapa controlada.

Actividades

- Simulación de incidentes
- pruebas de phishing
- escaneo de vulnerabilidades
- recuperación de backups
- validación de tiempos SLA
- afinamiento de correlaciones

Objetivo

Validar que el servicio responda conforme al ANS definido.

8.6 Fase 5 – Capacitación y transferencia de conocimiento

Esta fase es clave por el componente humano.

Público objetivo

- usuarios finales

- líderes
- TI
- seguridad
- terceros

Actividades

- talleres de buenas prácticas
- phishing awareness
- ejercicios tabletop
- sesiones con líderes
- documentación operativa

8.7 Fase 6 – Puesta en producción

Una vez validadas las pruebas piloto, se habilita el servicio completo.

Incluye

- monitoreo 7x24
- escalamiento
- tickets
- dashboards
- SLA
- comités

Aquí inicia formalmente la operación contractual.

8.8 Fase 7 – Estabilización y mejora continua

Durante las primeras semanas se realiza una etapa de ajuste fino.

Actividades

- tuning SIEM
- ajuste de alertas

- optimización de casos de uso
- revisión de falsos positivos
- actualización de playbooks
- mejoras de cobertura

Esta fase permite madurar el servicio según el comportamiento real del cliente.

8.9 Cronograma de implementación sugerido

Tiempo estimado para una empresa mediana:

- Diagnóstico: 2 semanas
- Diseño: 2 semanas
- Despliegue: 3 semanas
- Piloto: 2 semanas
- Capacitación: 1 semana
- Producción: 1 semana
- Estabilización: 2 semanas

Total estimado:

13 semanas

8.10 Riesgos del proyecto y mitigación

Riesgos

- falta de inventario actualizado
- resistencia al cambio
- conectividad híbrida
- ruido de eventos
- baja adopción de usuarios

Mitigación

- talleres iniciales

- pilotos controlados
- comité de proyecto
- gestión del cambio
- plan de comunicaciones

9. Acuerdo De Nivel De Servicio (ANS)

9.1 Objetivo del ANS

El Acuerdo de Nivel de Servicio (ANS) establece los compromisos formales entre el proveedor del servicio de ciberseguridad y la empresa cliente, definiendo métricas, tiempos, disponibilidad, responsabilidades, exclusiones y mecanismos de seguimiento.

Su propósito es garantizar transparencia, control y mejora continua del servicio.

9.2 Alcance del ANS

El ANS aplica a los siguientes servicios contratados:

- Monitoreo SOC 7x24
- Gestión de incidentes
- Vulnerabilidades
- IAM
- Respaldo y recuperación
- Mesa de servicio
- Capacitaciones y concientización
- Reportes y comités

9.3 Métricas y niveles de servicio

Disponibilidad del servicio

- SOC y SIEM: **99,7%**
- Mesa de servicio: **99,5%**

- Consola de reportes: **99,0%**

Tiempos por severidad

Incidente crítico

- Detección: **≤ 5 minutos**
- Atención inicial: **≤ 15 minutos**
- Escalamiento N2/N3: **≤ 30 minutos**
- Contención: **≤ 1 hora**
- Resolución: **≤ 4 horas**

Incidente alto

- Detección: **≤ 15 minutos**
- Atención: **≤ 30 minutos**
- Resolución: **≤ 8 horas**

Incidente medio

- Atención: **≤ 2 horas**
- Resolución: **≤ 24 horas**

Incidente bajo

- Atención: **≤ 4 horas**
- Resolución: **≤ 48 horas**

Ilustración 8

Acuerdo de Nivel de Servicio (SLA)

Severidad	Tiempo de Detección	Tiempo de Respuesta	Tiempo de Escalamiento	Tiempo de Resolución	Disponibilidad del Servicio	KPI Clave
Critica	≤ 5 minutos	≤ 15 minutos	≤ 30 minutos	≤ 4 horas	• SOC / SIEM 99.7%	▸ MTTD < 10 min
Alta	≤ 15 minutos	≤ 30 minutos	≤ 1 hora	≤ 8 horas	• Mesa de Servicio 99.5%	▸ MTTR < 2 horas
Media	≤ 30 minutos	≤ 2 horas	N/A	≤ 24 horas	• Consola de Reportes 99.0%	▸ % Falsos Positivos < 5%
Baja	≤ 1 hora	≤ 4 horas	N/A	≤ 48 horas		▸ % Cumplimiento SLA > 99%
						▸ Incidentes Criticos Resueltos

Disponibilidad del Servicio					
	▸ Detección	≤ 15 minutos	≤ 30 minutos	≤ 24 horas	≤ 4 horas
	▸ Atención	≤ 30 minutos	≤ 1 hora	N/A	N/A
	▸ Resolución	N/A	N/A	N/A	N/A

Fuente: Elaboración Propia.

9.4 Indicadores clave de desempeño (KPI)

El proveedor deberá reportar mensualmente:

- MTTD (tiempo medio de detección)
- MTTR (tiempo medio de respuesta)
- porcentaje de falsos positivos
- cumplimiento SLA
- incidentes por severidad
- vulnerabilidades corregidas
- usuarios capacitados
- efectividad phishing simulation

Estos indicadores se revisarán en comité mensual.

9.5 Responsabilidades del proveedor

El proveedor se compromete a:

- monitoreo continuo 7x24
- atención por niveles
- escalamiento oportuno
- generación de reportes
- cumplimiento de playbooks
- custodia de evidencias
- respaldo de configuraciones
- actualización de reglas SIEM

9.6 Responsabilidades del cliente

La empresa cliente deberá garantizar:

- acceso controlado a infraestructura
- contactos de escalamiento
- ventanas de mantenimiento
- aprobación de cambios
- participación en comités
- asistencia a capacitaciones
- actualización de inventario

9.7 OLAs (Acuerdos operativos internos)

Además del SLA externo, se establecen OLAs internos entre equipos:

N1 → N2

- máximo **15 minutos**

N2 → N3

- máximo **30 minutos**

SOC → Infraestructura cliente

- máximo **20 minutos**

Esto garantiza coordinación operativa.

9.8 Capacitaciones dentro del ANS

El servicio incluye compromisos sobre formación:

- 1 capacitación trimestral general
- 1 simulación phishing trimestral
- 1 taller semestral técnico
- cobertura mínima 85% usuarios
- reporte de madurez semestral

Esto es diferencial en tu propuesta.

9.9 Exclusiones del servicio

No están cubiertos:

- cambios no aprobados
- proyectos fuera de alcance
- desarrollo seguro de software
- adquisiciones de licencias
- incidentes causados por terceros no autorizados
- fallas eléctricas o físicas del cliente

9.10 Penalizaciones y compensaciones

En caso de incumplimiento:

Disponibilidad

- 1% por cada 0,1% por debajo del SLA

Respuesta crítica

- 3% por incumplimiento en incidentes críticos

Reportes

- 2% por no entrega de reportes

Capacitaciones

- 2% por incumplimiento del plan trimestral

9.11 Gobierno y revisión del ANS

El ANS será revisado:

- mensualmente → operación
- trimestralmente → estrategia
- anual → renovación contractual

Permitiendo ajustes por crecimiento del cliente.

10. Gestión De Herramientas Y Stack Tecnológico

10.1 Enfoque de selección tecnológica

La selección de herramientas para la prestación del servicio de ciberseguridad se basa en un enfoque híbrido que contempla tanto soluciones de **software libre (open source)** como herramientas **comerciales (enterprise)**.

Este enfoque permite adaptarse a diferentes escenarios del cliente, considerando factores como presupuesto, nivel de madurez, escalabilidad y soporte técnico.

Las soluciones open source ofrecen alta flexibilidad y bajo costo, mientras que las soluciones enterprise proporcionan capacidades avanzadas, soporte especializado y mayor nivel de automatización.

10.2 Comparativa general: Open Source vs Enterprise

A continuación, se presenta una matriz comparativa de los factores más relevantes:

Tabla 1

Factor	Open Source	Enterprise
Costo	Sin costo de licenciamiento	Alto costo (licencias, consumo, suscripción)
Implementación	Requiere configuración manual avanzada	Implementación guiada y más rápida
Soporte	Comunidad, foros, documentación	Soporte oficial, SLA, fabricante
Escalabilidad	Depende de arquitectura propia	Alta escalabilidad nativa
Facilidad de uso	Curva de aprendizaje alta	Interfaces amigables y dashboards avanzados
Automatización	Limitada o manual	Alta (SOAR, IA, playbooks)
Integración	Flexible pero requiere desarrollo	Integraciones nativas listas
Seguridad y actualizaciones	Depende de la comunidad	Actualizaciones controladas y certificadas
Personal requerido	Alto nivel técnico interno	Menor dependencia técnica interna
Vendor lock-in	No existe	Dependencia del proveedor
Tiempo de despliegue	Mayor	Menor
Personalización	Muy alta	Limitada a capacidades del fabricante
Cumplimiento normativo	Requiere configuración manual	Incluye frameworks (ISO, NIST, etc.)
Monitoreo avanzado (IA, UEBA)	Limitado	Integrado
Costo total (TCO)	Bajo en licencias, alto en operación	Alto en licencias, menor en operación

Fuente: generación propia

10.3 Comparativa por tipo de herramienta

SIEM / SOC

El componente SIEM / SOC es el núcleo del servicio de ciberseguridad administrada, ya que permite la recolección, normalización, correlación y análisis centralizado de eventos de seguridad provenientes de infraestructura, aplicaciones, nube y usuarios.

Su función principal es facilitar la detección temprana de amenazas, la generación de alertas y la respuesta operativa por parte del SOC.

Tipo	Open Source	Enterprise
SIEM	Wazuh, ELK, Graylog	Splunk, QRadar, Sentinel

Las soluciones open source permiten monitoreo sin costo de licencia, pero requieren mayor esfuerzo de configuración, mientras que las enterprise incluyen capacidades avanzadas como análisis con inteligencia artificial y automatización.

Gestión de vulnerabilidades

La gestión de vulnerabilidades permite **identificar, clasificar, priorizar y dar seguimiento a debilidades de seguridad** presentes en sistemas operativos, aplicaciones, bases de datos, redes y servicios cloud.

Este componente es fundamental para reducir la superficie de ataque y prevenir incidentes derivados de fallas no corregidas.

Tipo	Open Source	Enterprise
Vulnerabilidades	OpenVAS	Nessus, Qualys

IAM (Identidades)

El componente IAM está orientado a la **administración centralizada de usuarios, roles, privilegios y mecanismos de autenticación**, garantizando que cada usuario tenga acceso únicamente a los recursos autorizados.

Incluye funcionalidades como autenticación multifactor, control de privilegios, federación y auditoría de accesos.

Tipo	Open Source	Enterprise
IAM	Keycloak, FreeIPA	Okta, Azure AD

Respaldo y Recuperacion

La capa de respaldo garantiza la protección, retención y recuperación de la información crítica frente a incidentes como ransomware, fallos humanos, corrupción de datos o indisponibilidad de infraestructura.

Su alcance cubre servidores, bases de datos, archivos corporativos y servicios en nube.

Tipo	Open Source	Enterprise
Backups	Bacula	Veeam, Acronis

Gestión de incidentes

La gestión de incidentes corresponde al proceso mediante el cual se **detectan, clasifican, analizan, contienen, erradican y documentan eventos de seguridad**, asegurando trazabilidad y cumplimiento del ANS.

Este componente se integra con el SOC, SIEM, playbooks y mesa de servicio.

Tipo	Open Source	Enterprise
IR / SOAR	TheHive, Cortex	ServiceNow, XSOAR

10.4 Estrategia Recomendada

Para una empresa mediana, se recomienda un enfoque:

Escenario 1 (Costo optimizado)

- Open source + equipo técnico interno
- Ideal para organizaciones con bajo presupuesto

Escenario 2 (Balanceado) RECOMENDADO

- SIEM enterprise + herramientas open source complementarias
- Ejemplo:
    - SIEM: Splunk / Sentinel

- Vulnerabilidades: OpenVAS
- Capacitación: GoPhish

Escenario 3 (Alta madurez)

- Todo enterprise
- Alta automatización
- SOC avanzado

10.5 Justificación del enfoque híbrido

El uso combinado de herramientas permite:

- Optimizar costos
- Aprovechar lo mejor de cada tecnología
- Reducir dependencia de un solo proveedor
- Adaptarse al crecimiento del cliente

11. Resultados Esperados Y Valor Para El Cliente

11.1 Objetivo del valor esperado

La implementación del servicio de ciberseguridad bajo un modelo de outsourcing busca generar resultados medibles en la operación del cliente, fortaleciendo la protección de sus activos de información y reduciendo la exposición a amenazas.

El valor esperado no se limita a la detección de incidentes, sino que abarca la continuidad del negocio, la madurez operativa, la confianza de los usuarios y la optimización de costos.

11.2 Resultados esperados a nivel técnico

Desde la perspectiva tecnológica, se espera alcanzar los siguientes resultados:

- Monitoreo centralizado de eventos de seguridad en infraestructura híbrida
- Reducción del tiempo medio de detección (MTTD)

- Disminución del tiempo medio de respuesta (MTTR)
- Identificación temprana de amenazas internas y externas
- Gestión continua de vulnerabilidades
- Mayor visibilidad sobre accesos privilegiados
- Mejor cobertura sobre activos cloud y on-premise
- Validación periódica de respaldos y recuperación

Estos resultados permiten elevar la capacidad de defensa de la organización.

11.3 Resultados esperados a nivel operativo

En la operación diaria, el servicio debe traducirse en mejoras tangibles como:

- Cobertura continua 7x24
- Trazabilidad completa de incidentes
- Escalamiento técnico estructurado
- Mayor control de tickets y solicitudes
- Reportes ejecutivos y técnicos periódicos
- Comités de seguimiento y mejora continua
- Disminución de falsos positivos
- Afinamiento progresivo de casos de uso

Esto permite una operación más predecible y controlada.

11.4 Resultados esperados sobre usuarios

El componente humano es uno de los ejes de mayor impacto del servicio.

Se espera:

- Reducción de incidentes por phishing
- Mejora en prácticas de uso de contraseñas
- Mayor adopción de MFA
- Disminución del uso indebido de privilegios

- Incremento de la cultura de seguridad
- Mejor respuesta de usuarios ante eventos sospechosos

La capacitación continua debe reflejarse en una reducción progresiva del riesgo humano.

11.5 Resultados esperados en continuidad del negocio

Uno de los principales beneficios del servicio es su impacto sobre la disponibilidad operativa.

Se espera:

- Menor indisponibilidad por incidentes de seguridad
- Mayor resiliencia ante ransomware
- Recuperación rápida de servicios críticos
- Protección de información sensible
- Mayor confianza en planes de contingencia
- Pruebas periódicas de restauración exitosas

Esto protege procesos críticos del negocio.

11.6 Valor financiero para el cliente

Desde el punto de vista económico, el outsourcing permite:

- Reducir costos de contratación de personal especializado
- Evitar inversiones altas en licenciamiento inicial
- Optimizar gastos operativos
- Escalar según crecimiento
- Disminuir pérdidas por incidentes
- Reducir impacto financiero de indisponibilidad

Esto transforma la ciberseguridad en un gasto controlado y predecible.

11.7 Valor estratégico del servicio

Más allá de la operación, el cliente obtiene valor estratégico mediante:

- Acceso a expertos especializados
- Alineación con estándares internacionales
- Mejora de la postura de riesgo
- Soporte para auditorías y cumplimiento
- Escalabilidad del modelo
- Visibilidad ejecutiva del riesgo

Este punto es muy fuerte porque vende la propuesta como **servicio estratégico**, no solo técnico.

11.8 Indicadores de éxito esperados

Para medir el valor generado, se proponen indicadores como:

- Reducción del 60% en incidentes por phishing en 6 meses
- Disminución del 40% en vulnerabilidades críticas
- Cumplimiento SLA > 99,5%
- Participación > 85% en capacitaciones
- MTTR menor a 4 horas en incidentes críticos
- 100% de respaldos críticos validados trimestralmente

Estos indicadores servirán como línea base para medir retorno del servicio.

12. Beneficios Del Modelo De Outsourcing

12.1 Acceso a talento especializado

Uno de los principales beneficios del outsourcing es el acceso inmediato a personal especializado en ciberseguridad, sin que la empresa tenga que asumir procesos extensos de reclutamiento, formación y retención.

El proveedor pone a disposición perfiles como:

- Analistas SOC N1, N2 y N3
- Especialistas en vulnerabilidades

- Arquitectos de seguridad
- Consultores IAM
- Especialistas en respaldo y recuperación
- Líderes de gobierno y cumplimiento

Esto permite a la empresa cliente contar con capacidades de alto nivel desde el inicio del servicio.

12.2 Reducción de costos operativos

La operación interna de un servicio de ciberseguridad requiere inversiones considerables en:

- Personal especializado
- Licencias
- Infraestructura
- Turnos 7x24
- Capacitación continua
- Herramientas de monitoreo

Mediante outsourcing, estos costos se transforman en un **modelo predecible basado en servicio**, facilitando la planeación financiera y reduciendo el costo total de propiedad.

12.3 Escalabilidad del servicio

El modelo permite crecer de acuerdo con la evolución del cliente.

Esto incluye:

- nuevas sedes
- nuevos usuarios
- nuevos servicios cloud
- más aplicaciones
- mayor volumen de logs
- nuevas campañas de capacitación

La escalabilidad es uno de los mayores diferenciales frente a una operación interna rígida.

12.4 Cobertura continua 7x24

Implementar una operación interna con cobertura permanente implica alta complejidad administrativa y financiera.

El outsourcing permite:

- monitoreo continuo
- guardias especializadas
- escalamiento inmediato
- cobertura en festivos y fines de semana
- atención por severidad

Esto garantiza capacidad de respuesta en cualquier momento.

12.5 Adopción acelerada de mejores prácticas

El proveedor transfiere experiencia adquirida en múltiples clientes y sectores, facilitando la adopción de:

- ITIL
- COBIT
- ISO 27001
- NIST
- CIS Controls

Esto acelera la madurez de la empresa cliente sin necesidad de largos procesos internos.

12.6 Enfoque en el core del negocio

Uno de los beneficios estratégicos más importantes es que la empresa puede enfocar sus recursos internos en actividades directamente relacionadas con su negocio principal.

Mientras el proveedor asume la operación de ciberseguridad, el cliente concentra esfuerzos en:

- productividad

- innovación
- crecimiento
- clientes
- procesos clave

Este enfoque mejora la eficiencia organizacional.

12.7 Mejora continua del servicio

El outsourcing incorpora mecanismos formales de evolución:

- revisión de KPIs
- tuning de reglas
- actualización de playbooks
- nuevas integraciones
- mejora de casos de uso
- nuevas campañas de awareness

Esto convierte la seguridad en un servicio vivo y en constante optimización.

12.8 Reducción del riesgo organizacional

La combinación de monitoreo, respuesta, IAM, backups y capacitación permite reducir riesgos asociados a:

- ransomware
- phishing
- fuga de información
- abuso de privilegios
- indisponibilidad
- pérdida de datos

Este beneficio conecta directamente con continuidad del negocio.

12.9 Soporte para auditoría y cumplimiento

El servicio facilita:

- trazabilidad de incidentes
- evidencias de monitoreo
- reportes históricos
- cumplimiento ANS
- métricas SLA
- evidencias de capacitación

Esto es muy valioso en auditorías internas, externas y regulatorias.

12.10 Ventaja competitiva para el cliente

Al contar con una postura de seguridad más madura, la empresa mejora:

- reputación
- confianza de clientes
- cumplimiento contractual
- protección de datos
- capacidad de crecimiento seguro

Esto convierte la ciberseguridad en un habilitador de negocio.

Conclusiones

La implementación de un servicio de ciberseguridad bajo un modelo de outsourcing representa una estrategia integral y escalable para empresas medianas que operan en entornos híbridos. A través del desarrollo del presente informe técnico se evidenció que la externalización de estos servicios permite combinar herramientas especializadas, procesos maduros y talento experto, reduciendo la exposición a amenazas y fortaleciendo la continuidad del negocio.

El diseño propuesto demuestra que la seguridad no debe limitarse únicamente al monitoreo de eventos, sino que debe abarcar de forma estructurada la protección de infraestructura, sistemas, identidades, respaldos y usuarios. La incorporación de componentes

como SOC, SIEM, gestión de vulnerabilidades, IAM, respaldo y capacitación continua permite construir una estrategia de defensa en profundidad, alineada con las necesidades reales de una empresa mediana estándar.

Desde la perspectiva operativa, la definición de un modelo por niveles, un plan de implementación por fases y un Acuerdo de Nivel de Servicio robusto garantizan que la prestación del servicio sea medible, controlable y orientada a resultados. Esto convierte la propuesta en una alternativa viable tanto técnica como financieramente frente a la construcción de una operación interna de alta complejidad.

Finalmente, se concluye que el outsourcing de ciberseguridad no solo reduce costos y mejora tiempos de respuesta, sino que se consolida como un habilitador estratégico para el negocio, al permitir a la organización enfocarse en su actividad principal mientras delega la protección de sus activos críticos a un proveedor especializado.

Referencias

Estándares y marcos de referencia

AXELOS. (2019). *Fundamentos de ITIL® 4*. AXELOS. ITIL Official Site

Organización Internacional de Normalización. (2022). *ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad*. ISO.

ISACA. (2019). *COBIT 2019: Marco de gobierno y gestión de TI*. ISACA.

Instituto Nacional de Ciberseguridad (INCIBE). (2021). *Guía de gestión de incidentes de ciberseguridad*. Gobierno de España.

Artículo sobre riesgo humano

Keepnet Labs. (2026). *What Is Human Risk Management in Cybersecurity? Definition & Benefits*.

Herramientas Open Source

Wazuh. (2026). *Wazuh – Open Source SIEM y XDR*.
Sitio oficial Wazuh

StrangeBee (TheHive Project). (2026). *TheHive – Plataforma de respuesta a incidentes*.
Sitio oficial TheHive

Greenbone. (2026). *Greenbone / OpenVAS – Gestión de vulnerabilidades*.
Sitio oficial Greenbone

Keycloak. (2026). *Keycloak – Gestión de identidades y accesos*.
Sitio oficial Keycloak

Bacula Systems. (2026). *Bacula – Software de respaldo empresarial*.
Sitio oficial Bacula

Herramientas Enterprise

Splunk Inc. (2026). *Splunk Enterprise Security Platform*.
Sitio oficial Splunk

IBM. (2026). *IBM QRadar SIEM*.
Sitio oficial QRadar

Microsoft. (2026). *Microsoft Sentinel – SIEM en la nube*.
Documentación oficial Sentinel

Tenable. (2026). *Nessus Vulnerability Scanner*.
Sitio oficial Nessus

Qualys. (2026). *Plataforma de gestión de riesgos y vulnerabilidades*.
Sitio oficial Qualys

Okta. (2026). *Gestión de identidades y accesos (IAM)*.
Sitio oficial Okta

Veeam. (2026). *Soluciones de respaldo y recuperación de datos*.
Sitio oficial Veeam

ServiceNow. (2026). *Security Operations (SecOps)*.
Sitio oficial ServiceNow SecOps

Palo Alto Networks. (2026). *Cortex XSOAR – Orquestación y automatización*.
Sitio oficial Cortex XSOAR