Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ingeniería Electrónica y Eléctrica
Escuela Profesional de Ingeniería de Telecomunicaciones

Implementación de un sistema de orquestación en CyberSOC para detección y respuesta automatizada ante amenazas perimetrales de un cliente corporativo

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Ingeniero de Telecomunicaciones

AUTOR

Guillermo Alonso ACUÑA GAMARRA

ASESOR

Mg. Ana Milagros CORONEL CHAMORRO

Lima, Perú

2026



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

https://creativecommons.org/licenses/by-nc-sa/4.0/

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Acuña, G. (2026). *Implementación de un sistema de orquestación en CyberSOC para detección y respuesta automatizada ante amenazas perimetrales de un cliente corporativo*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería Electrónica y Eléctrica, Escuela Profesional de Ingeniería de Telecomunicaciones]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Guillermo Alonso Acuña Gamarra
Tipo de documento de identidad	DNI
Número de documento de identidad	73904910
URL de ORCID	No Aplica
Datos de asesor	
Nombres y apellidos	Ana Milagros Coronel Chamorro
Tipo de documento de identidad	DNI
Número de documento de identidad	09752919
URL de ORCID	https://orcid.org/0000-0003-2165-0742
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Teresa Esther Núñez Zúñiga
Tipo de documento	DNI
Número de documento de identidad	08006778
Miembro del jurado 1	
Nombres y apellidos	Celso Ysidro Geronimo Huaman
Tipo de documento	DNI
Número de documento de identidad	09191500
Miembro del jurado 2	
Nombres y apellidos	Jorge Elías Moscoso Sánchez
Tipo de documento	DNI
Número de documento de identidad	08596442
Datos de investigación	
Línea de investigación	Ciberseguridad
Grupo de investigación	No Aplica
Agencia de financiamiento	No Aplica

Ubicación geográfica de la investigación	Edificio: Ciudaris País: Perú Departamento: Lima Provincia: Lima Distrito: Santiago de Surco Dirección: Av. Encalada 1171 Latitud: -12.105324016411487 Longitud: -76.97100543981571
Año o rango de años en que se realizó la investigación	2025-2026
URL de disciplinas OCDE	Telecomunicaciones https://purl.org/pe-repo/ocde/ford#2.02.05

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMÉRICA)
FACULTAD DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA
Teléfono 619-7000 Anexo 4226
Calle Germán Amezaga 375 – Lima 1 – Perú

ACTA DE SUSTENTACIÓN

TRABAJO DE SUFICIENCIA PROFESIONAL

ACTA N°77/FIEE-PPP/2026

Los suscritos Miembros del Jurado, docentes permanentes de las Escuelas Profesionales de la Facultad de Ingeniería Electrónica y Eléctrica, reunidos en la fecha 29 de Octubre del 2026, como Presidente de Jurado la **DRA. TERESA ESTHER NUÑEZ ZUÑIGA,** integrado por el Miembro de Jurado el **DR. JORGE ELÍAS MOSCOSO SÁNCHEZ,** el Miembro de Jurado el **DR. CELSO YSIDRO GERONIMO HUAMAN** y Miembro Asesor la **MG. ANA CORONEL CHAMORRO.**

Después de escuchar la Sustentación Presencial del Trabajo de Suficiencia Profesional del Bachiller **GUILLERMO ALONSO ACUÑA GAMARRA** con código 16190247 que para optar el Título Profesional de Ingeniero de Telecomunicaciones sustentó el Trabajo de Suficiencia Profesional titulado **IMPLEMENTACIÓN DE UN SISTEMA DE ORQUESTACIÓN EN CYBERSOC PARA DETECCIÓN Y RESPUESTA AUTOMATIZADA ANTE AMENAZAS PERIMETRALES DE UN CLIENTE CORPORATIVO.**

El jurado examinador procedió a formular las preguntas reglamentarias y, luego de una deliberación en privado, decidió otorgarle el calificativo de 17 (Diecisiete)

Ciudad Universitaria, 29 de Octubre del 2026

DRA. TERESA ESTHER NUÑEZ ZUÑIGA
Presidente Jurado

DR. CELSO YSIDRO GERONIMO HUAMAN
Miembro Jurado

DR. JORGE ELÍAS MOSCOSO SÁNCHEZ
Miembro Jurado

MG. ANA CORONEL CHAMORRO
Miembro Asesor

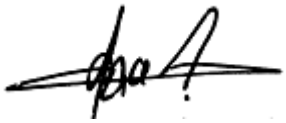
UNIVERSIDAD NACIONAL MAYOR DE
SAN MARCOS
Universidad del Perú, Decana de América

CERTIFICADO DE SIMILITUD

Yo**, ANA CORONEL CHAMORRO** en mi condición de asesor acreditado con el Dictamen N°78/FIEE-PPP/2026 del Trabajo de Suficiencia Profesional titulado **IMPLEMENTACIÓN DE UN SISTEMA DE ORQUESTACIÓN EN CYBERSOC PARA DETECCIÓN Y RESPUESTA AUTOMATIZADA ANTE AMENAZAS PERIMETRALES DE UN CLIENTE CORPORATIVO,** presentado por el bachiller GUILLERMO ALONSO ACUÑA GAMARRA, para optar el título profesional de Ingeniero de Telecomunicaciones. CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante la plataforma PIDS, el documento evaluado cuenta con el 04% de similitud, nivel PERMITIDO para continuar con los trámites correspondientes y para su publicación en el repositorio institucional.

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del título profesional de Ingeniero de Telecomunicaciones.

Lima, 29 de Octubre del 2026



Firma del Asesor

DNI: 09752919

Nombres y apellidos del asesor:
ANA CORONEL CHAMORRO

DEDICATORIA

Este trabajo está dedicado a mi madre, por su constante apoyo, fortaleza y ejemplo, que me han inspirado a alcanzar este logro profesional.

AGRADECIMIENTOS

Agradezco a mi familia, que siempre me alentó a continuar con el presente trabajo; a mis compañeros por compartir sus ideas y motivarme a seguir siempre adelante; y a mi asesora, la Mag. Ana Coronel Chamorro por apoyarme en la estructuración de mis ideas para desarrollar el presente trabajo.

RESUMEN

Este trabajo de suficiencia profesional tuvo como objetivo implementar un sistema de orquestación en el CyberSOC de MC INNOVATEC S.A.C. para automatizar la detección y respuesta ante amenazas perimetrales de un cliente corporativo cuyas alertas del SIEM IBM QRadar se gestionaban manualmente, con tiempos elevados. La implementación se organizó en cuatro etapas y catorce fases: priorización de 48 reglas de detección (23 de firewall y 25 de WAF Akamai); diseño de dos plantillas de flujo parametrizables; construcción del motor MCIA, integrado mediante API con las herramientas del CyberSOC y fuentes de inteligencia de amenazas; y validación mediante piloto controlado y pase a producción. El impacto se evaluó comparando el MTTD y MTTR del proceso manual (octubre-noviembre de 2025) con los de producción (abril de 2026). El MTTD global se redujo de 1 h 30 min a 2 min 45 s (−97.0 %) y el MTTR global, de 30 h 52 min a 1 min 16 s (−99.9 %), por debajo de las metas acordadas. La respuesta automatizada alcanzó el 98.8 % de las ofensas, con un ahorro estimado de 442.0 horas-analista mensuales. Se concluye que la orquestación mejoró sustancialmente la capacidad operativa del CyberSOC y resultó económicamente viable.

Palabras clave: orquestación de seguridad, SOAR, CyberSOC, automatización de la respuesta, amenazas perimetrales.

ABSTRACT

This professional sufficiency report aimed to implement an orchestration system in the CyberSOC of MC INNOVATEC S.A.C. to automate the detection of and response to perimeter threats for a corporate client whose IBM QRadar SIEM alerts were handled manually, with high response times. The implementation was organized into four stages and fourteen phases: prioritization of 48 detection rules (23 for firewall and 25 for the Akamai WAF); design of two parameterizable flow templates; construction of the MCIA engine, integrated through APIs with the CyberSOC tools and threat intelligence sources; and validation through a controlled pilot and production deployment. The impact was assessed by comparing the MTTD and MTTR of the manual process (October–November 2025) with those in production (April 2026). The overall MTTD decreased from 1 h 30 min to 2 min 45 s (−97.0%) and the overall MTTR from 30 h 52 min to 1 min 16 s (−99.9%), below the agreed targets. Automated response covered 98.8% of the offenses, with an estimated saving of 442.0 analyst-hours per month. It is concluded that orchestration substantially improved the operational capacity of the CyberSOC and proved economically viable.

Keywords: security orchestration, SOAR, CyberSOC, response automation, perimeter threats.

INDICE GENERAL

CARÁTULA i
RESUMEN iv
ABSTRACT v
TABLA DE CONTENIDO vi
LISTA DE FIGURAS x
LISTA DE TABLAS xii
CAPÍTULO I: INTRODUCCIÓN 1
1.1 Objetivos del informe 2
1.2 Estructura del informe 3
CAPÍTULO II: INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD 4
2.1 Institución – Actividad que desarrolla 4
2.2 Periodo de duración de la actividad 4
2.3 Finalidad y objetivos de la entidad 4
2.4 Razón social 5
2.5 Dirección postal 5
2.6 Nombre y correo electrónico del profesional a cargo 5
CAPÍTULO III: DESCRIPCIÓN DE LA ACTIVIDAD 6
3.1 Organización de la actividad 6
3.2 Finalidad y objetivos de la Actividad 8
3.2.1 Finalidad 8
3.2.2 Objetivos 8
3.3 Problemática 9
3.3.1 Problema General 11
3.3.2 Problemas Específicos 11
3.3.3 Justificación e importancia de la investigación 11
3.4 Metodología 14
3.4.1 Bases teóricas 14
3.4.2 Marco conceptual 16

3.4.2.1 Centro de Operaciones de Seguridad (SOC / CyberSOC) 16

3.4.2.2 SOAR (*Security Orchestration, Automation and Response*) 16

3.4.2.3 Red Perimetral 16

3.4.2.4 Amenazas Perimetrales 17

3.4.2.5 *Playbooks* de Respuesta ante Incidentes 17

3.4.2.6 MTTD (*Mean Time to Detect*) 17

3.4.2.7 MTTR (*Mean Time to Resolve*) 17

3.4.2.8 SIEM (*Security Information and Event Management*) 18

3.4.2.9 Ofensas, eventos y alertas de seguridad 18

3.4.2.10 Reglas de detección y casos de uso de seguridad 18

3.4.2.11 API (*Application Programming Interface*) 19

3.4.2.12 Microservicios 19

3.4.2.13 Web Application Firewall (WAF) 19

3.4.2.14 Lista Dinámica Externa (EDL) y listas de bloqueo 20

3.4.2.15 Inteligencia de amenazas (*Threat Intelligence*) e indicadores de compromiso (IoC) 20

3.4.2.16 Enriquecimiento de información 20

3.4.2.17 Inteligencia artificial generativa e ingeniería de prompts 20

3.5 Procedimiento 21

3.5.1 Etapa 1: Análisis y levantamiento de información (Fases 1 y 2) 22

3.5.1.1 Fase 1 - Iniciación y gobierno interno 22

3.5.1.2 Fase 2 - Descubrimiento y requisitos 32

3.5.2 Etapa 2: Diseño e implementación de la solución (Fases 3 a 9) 34

3.5.2.1 Fase 3 - Diseño e implementación de la arquitectura 34

3.5.2.2 Fase 4 - Provisionamiento de infraestructura 39

3.5.2.3 Fase 5 - Desarrollo del core – cybersoc-api 41

3.5.2.4 Fase 6 - Desarrollo de integraciones 42

3.5.2.5 Fase 7 - Motor de decisión y respuesta 47

3.5.2.6 Fase 8 - *Playbooks* por regla 52

3.5.2.7 Fase 9 - Sistema web y *dashboards* 53

3.5.3 Etapa 3: Piloto controlado y pase a producción (Fases 10 a 12) 55

3.5.3.1 Fase 10 - Pruebas y QA 55

3.5.3.2 Fase 11 - Piloto controlado 57

3.5.3.3 Fase 12 - Despliegue a producción 61

3.5.4 Etapa 4: Cierre de la implementación y transición a operación continua (Fases 13 y 14) 61

3.5.4.1 Fase 13 - Operación y mejora continua (estado permanente) 61

3.5.4.2 Fase 14 - Cierre de la implementación 64

3.6 Resultado de la actividad 71

3.6.1 Resultado de la implementación del sistema de orquestación en el CyberSOC 71

3.6.2 Resultado de la identificación y priorización de las reglas de detección 72

3.6.3 Resultado del diseño de los flujos de respuesta automatizada 73

3.6.4 Resultado de la implementación de los flujos en el orquestador 75

3.6.5 Resultado de la evaluación del impacto en los indicadores MTTD y MTTR 76

CAPÍTULO IV: DISCUSIÓN DE RESULTADOS 78

4.1 Descripción de la implementación 78

4.1.1 Etapa de análisis y levantamiento de información (Fases 1 y 2) 78

4.1.2 Etapa de diseño e implementación de la solución (Fases 3 a 9) 79

4.1.3 Etapa de piloto controlado y pase a producción (Fases 10 a 12) 80

4.1.4 Etapa de cierre de la implementación y transición a operación continua (Fases 13 y 14) 81

4.2 Evaluación Económica 82

4.2.1 Supuestos considerados 83

4.2.2 Inversión del proyecto 84

4.2.3 Beneficio mensual bruto 85

4.2.4 Costo mensual de afinamiento y mejora continua 85

4.2.5 Flujo de caja y evaluación económica 86

CAPÍTULO V: CONCLUSIONES 89

CAPÍTULO VI: RECOMENDACIONES 91

CAPÍTULO VII: REFERENCIAS 93

CAPÍTULO VIII: ANEXOS 97

Anexo A Cronograma detallado del proyecto (diagrama de Gantt) 97
Anexo B Evidencias de integración del orquestador MCIA 97
Anexo C Registros del periodo posterior (abril de 2026) 98
Anexo D Constancia de ejecución y conformidad del trabajo de suficiencia profesional 98

LISTA DE FIGURAS

Figura 1 Organigrama de los equipos involucrados en el desarrollo de la actividad 6
Figura 2 Firewalls FortiGate integrados en QRadar 22
Figura 3 WAF Akamai integrado en QRadar 22
Figura 4 Lista Dinámica Externa (EDL) configurada en FortiGate 23
Figura 5 Consola de Cortex XDR 24
Figura 6 Consola de Tenable 24
Figura 7 Consola del WAF Akamai 25
Figura 8 Reglas de detección de Firewall configuradas en QRadar (listado parcial) 29
Figura 9 Reglas de detección de WAF Akamai configuradas en QRadar (listado parcial) 29
Figura 10 Convocatoria a la reunión de kick-off del proyecto 32
Figura 11 Arquitectura implementada del motor de orquestación MCIA 36
Figura 12 Plantilla de flujo para las reglas de Firewall 38
Figura 13 Plantilla de flujo para las reglas de WAF Akamai 38
Figura 14 Mecanismo de no duplicación de bloqueos entre fuentes 39
Figura 15 Recursos asignados a la máquina virtual 41
Figura 16 Conectividad VPN site-to-site entre el firewall del cliente y el de la empresa 41
Figura 17 Captura parcial del conector de Inteligencia de amenazas 43
Figura 18 Captura parcial del conector de Tenable 43
Figura 19 Captura parcial del conector de Cortex 44
Figura 20 Captura parcial del conector de iTop 44
Figura 21 Captura parcial del conector de Gemini 44
Figura 22 Captura parcial del bloqueo en lista dinámica externa 45
Figura 23 Captura parcial del bloqueo en WAF Akamai 46
Figura 24 Captura parcial del inicio de recepción de las ofensas para WAF Akamai y los firewalls 47

Figura 25 Captura parcial de envío de correo dentro del flujo del playbook 47
Figura 26 Captura parcial de los niveles de reputación 49
Figura 27 Captura parcial del risk score de una IP 50
Figura 28 Reporte de bloqueos de IP en la lista dinámica externa 51
Figura 29 Envío del reporte automatizado para la rama no maliciosa 51
Figura 30 Envío del reporte automatizado de ofensa recurrente 52
Figura 31 Flujo completo de la plantilla para Firewalls 53
Figura 32 Flujo completo de la plantilla para WAF Akamai 53
Figura 33 Dashboard de tiempo promedio de detección 54
Figura 34 Dashboard de tiempo promedio de respuesta 54
Figura 35 Bitácora de ofensas 54
Figura 36 Dashboard de monitoreo en tiempo real del proceso del orquestador 55
Figura 37 Registro del CUD-154 gatillado desde el SIEM QRadar 56
Figura 38 Ejecución del flujo del CUD-154 56
Figura 39 Ejecución satisfactoria del flujo con bloqueo de IP 56
Figura 40 Registro de bloqueo de una IP maliciosa 57
Figura 41 Reporte del CUD-154 sin ejecución de bloqueo 58
Figura 42 Reporte de análisis del CUD-154 sin ejecución de bloqueo 58
Figura 43 Reporte de bloqueo de la IP 91.231.XX.XX 59
Figura 44 Acceso al EDL para desbloqueo de IPs 60
Figura 45 Agenda de reunión por correo para aprobación de autobloqueo y de pase a producción 61
Figura 46 KPI de MTTD en el orquestador MCIA 62
Figura 47 KPI de MTTR en el orquestador MCIA 62
Figura 48 Reporte de IPs bloqueadas en el EDL 63
Figura 49 Reporte de IPs bloqueadas en WAF Akamai 63
Figura 50 Registro de la información de vulnerabilidades en Tenable 64
Figura 51 Convocatoria a la reunión de comité operativo y conformidad de la puesta en operación del orquestador MCIA 70
Figura 52 Casos de uso de Firewall 73
Figura 53 Casos de uso de WAF Akamai 73
Figura 54 Comparativo del proceso manual del analista frente al paso automatizado 75

LISTA DE TABLAS

Tabla 1 Cronograma de actividades del proyecto 21
Tabla 2 Stakeholders identificados en el proyecto 26
Tabla 3 Matriz RACI de las actividades del proyecto 27
Tabla 4 Línea base del MTTD (octubre y noviembre de 2025) 30
Tabla 5 Línea base del MTTR (octubre y noviembre de 2025) 30
Tabla 6 Política de auto-respuesta acordada con el cliente 33
Tabla 7 Herramientas integradas y su propósito en el orquestador 33
Tabla 8 Comparativa de MTTD/MTTR antes y después de la implementación 65
Tabla 9 Distribución de incidentes procesados por el orquestador MCIA según rama de decisión 66
Tabla 10 Tasa de ejecución confirmada del bloqueo automático 67
Tabla 11 Reducción de carga operativa manual 68
Tabla 12 KPIs de éxito del proyecto 69
Tabla 13 Inversión del proyecto (costo de horas-hombre) 84
Tabla 14 Beneficio mensual bruto por ahorro de horas 85
Tabla 15 Costo mensual de afinamiento y mejora continua 85
Tabla 16 Flujo de caja proyectado a 12 meses 86

CAPÍTULO I:
INTRODUCCIÓN

La ciberseguridad se ha convertido en una de las principales preocupaciones de las organizaciones modernas. La acelerada transformación digital ha ampliado las infraestructuras tecnológicas y, con ellas, la superficie de exposición ante ataques informáticos. Según el panorama de amenazas de la Agencia de la Unión Europea para la Ciberseguridad (European Union Agency for Cybersecurity [ENISA], 2024), los ataques dirigidos al perímetro de red, entre ellos la denegación de servicio distribuido, las intrusiones por vulnerabilidades expuestas y las técnicas de evasión de controles, han aumentado en frecuencia y sofisticación, lo que exige respuestas cada vez más rápidas y coordinadas.

En este contexto, los Centros de Operaciones de Seguridad (SOC) enfrentan el reto de procesar grandes volúmenes de alertas en tiempo real. Cuando esa gestión se realiza de forma manual, los tiempos de detección y respuesta se prolongan, los procedimientos varían según el analista que atiende cada caso y se incrementa la probabilidad de errores u omisiones. IBM Security (2024) informa que las organizaciones que incorporan automatización y orquestación en sus operaciones de seguridad reducen en más del 30% el tiempo necesario para detectar y contener brechas frente a aquellas que mantienen procesos manuales. La automatización de la detección y la respuesta constituye, por tanto, una necesidad operativa para los CyberSOC que atienden infraestructuras expuestas de manera permanente.

Un escenario de estas características se presentaba en el CyberSOC de MC INNOVATEC S.A.C., unidad que brinda servicios de monitoreo y respuesta ante incidentes a clientes corporativos mediante la plataforma SIEM IBM QRadar. En el caso de uno de sus principales clientes, la atención de las alertas perimetrales se realizaba de forma completamente manual. El analista debía consultar el SIEM, revisar fuentes externas de inteligencia de amenazas, verificar las vulnerabilidades de los

activos asociados, registrar los hallazgos y notificar al cliente. Este procedimiento limitaba la capacidad del CyberSOC para contener oportunamente amenazas como intrusiones, escaneos maliciosos y accesos no autorizados.

La elección del tema respondió a la necesidad de mejorar esos procesos de detección y respuesta, así como a la experiencia profesional del autor en la operación e ingeniería del CyberSOC. A partir de dicha experiencia, se identificó la oportunidad de aplicar la orquestación de seguridad para estandarizar los procedimientos y reducir los tiempos de respuesta ante incidentes.

La propuesta se sustenta en los principios de la orquestación, automatización y respuesta de seguridad (SOAR), que permiten integrar las herramientas del SOC mediante interfaces de programación de aplicaciones (API) y ejecutar flujos de respuesta predefinidos (playbooks). Se consideran, asimismo, las guías de gestión de incidentes del National Institute of Standards and Technology [NIST] (Cichonski et al., 2012) y las prácticas de automatización promovidas por la Cybersecurity and Infrastructure Security Agency [CISA] (2021). Sobre esta base, se desarrolló el motor de orquestación MCIA, integrado con el SIEM, los firewalls perimetrales, el WAF Akamai, las fuentes de inteligencia de amenazas y las herramientas de gestión de vulnerabilidades y tickets, que incorpora además un motor de decisión basado en un puntaje de riesgo para determinar si cada caso se bloquea de forma automática o se deriva al análisis asistido.

1.1 Objetivos del informe

El presente informe tiene como objetivo describir la experiencia profesional del autor en la implementación de un sistema de orquestación en el CyberSOC de la empresa donde labora, orientado a automatizar la detección y respuesta ante amenazas perimetrales de un cliente corporativo. De manera específica, busca exponer el contexto operativo y la problemática que motivaron la actividad; describir el procedimiento seguido en sus cuatro etapas y catorce fases; analizar los resultados obtenidos en los indicadores MTTD y MTTR, así como la evaluación económica; por último, formular las conclusiones y recomendaciones derivadas de la implementación.

1.2 Estructura del informe

El informe se organiza de la siguiente manera: el Capítulo II describe la institución donde se desarrolló la actividad; el Capítulo III presenta la organización de la actividad, sus objetivos, la problemática, la justificación, la metodología, el procedimiento aplicado y los resultados obtenidos; el Capítulo IV discute dichos resultados y presenta la evaluación económica; el Capítulo V expone las conclusiones; el Capítulo VI, las recomendaciones. Finalmente, el Capítulo VII reúne las referencias bibliográficas y el Capítulo VIII, los anexos que complementan el trabajo.

CAPÍTULO II:
INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD

2.1 Institución – Actividad que desarrolla

La institución donde se desarrollaron las actividades correspondió a MC INNOVATEC S.A.C., empresa integradora de tecnologías de la información y telecomunicaciones.

Su actividad principal consistió en brindar soluciones integrales en ciberseguridad, *networking*, *datacenter*, redes ópticas, CCTV, *cloud*, Comunicaciones Unificadas y DevNet, garantizando la calidad, innovación y soporte especializado en cada uno de sus proyectos.

2.2 Periodo de duración de la actividad

El presente proyecto se realizó desde el 15 de diciembre del 2025 hasta el 30 de abril del 2026.

2.3 Finalidad y objetivos de la entidad

La organización tuvo como finalidad consolidarse como una empresa integradora líder en tecnologías de la información y telecomunicaciones en el Perú y a nivel internacional, ofreciendo soluciones innovadoras y de alto valor agregado.

Con más de siete años de operaciones en el mercado peruano e internacional y más de 500 proyectos implementados con éxito, la empresa impulsó la transformación digital de sus clientes mediante la optimización de la infraestructura tecnológica, el fortalecimiento de la ciberseguridad y la promoción de la eficiencia operativa.

Su misión es: "Transformar el potencial de las tecnologías más innovadoras en valor para ayudar a nuestros clientes a reducir costos, ser más productivos y competitivos, desarrollando soluciones que resuelvan sus necesidades de negocios".

Su visión es: "Ser la empresa de soluciones de tecnología de información y comunicaciones más reconocida del medio por la calidad de los servicios que brindamos a las empresas lideres en cada industria dentro y fuera del país".

Su Política de Seguridad de la Información es: “Proteger la confidencialidad, integridad y disponibilidad de la información, cumpliendo la normativa aplicable y promoviendo la mejora continua del SGSI”.

2.4 Razón social

MC INNOVATEC S.A.C. con RUC 20602823696

2.5 Dirección postal

Av. La Encalada 1171, Santiago de Surco, Lima, Perú.

2.6 Nombre y correo electrónico del profesional a cargo

Wilber Rojas – wrojas@mcinnovatec.com

CAPÍTULO III:
DESCRIPCIÓN DE LA ACTIVIDAD

3.1 Organización de la actividad

En la Figura 1 se presenta el organigrama de las áreas que participaron en el desarrollo de la actividad:

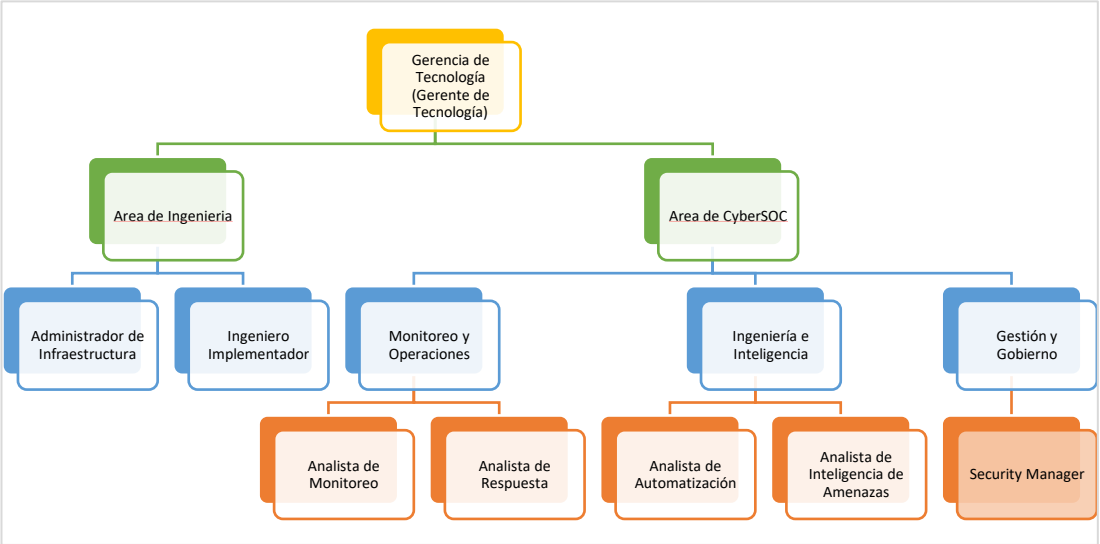


Figura 1 **Organigrama de los equipos involucrados en el desarrollo de la actividad.**
Fuente. Elaboración propia.

Las funciones de cada área fueron las siguientes:

A. Gerencia de Tecnología

Fue responsable de aprobar los cambios a nivel estratégico y presupuestal, y participó como *stakeholder* interesado en la mejora continua sobre la infraestructura de la empresa para el despliegue de la herramienta.

B. Ingeniería

Participó en la aprobación técnica y en la configuración del servicio utilizado como parte de la solución, proporcionando las especificaciones técnicas

y los permisos necesarios para su adecuada configuración. Esta área estuvo conformada por:

- **Administrador de Infraestructura:** Encargado de aprobar, a nivel técnico, el uso de los recursos de la empresa destinados al servidor.
- **Ingeniero Implementador:** Encargado de realizar la implementación del servidor, incluyendo la configuración del sistema operativo, la asignación de IP y la asignación de permisos, entre otras actividades.

C. CyberSOC

Presentó la necesidad de contar con una herramienta que apoye las actividades operativas para mejorar la detección y respuesta ante incidentes, y participó en la implementación de la solución. Dentro del CyberSOC se consideran las siguientes áreas:

1. Monitoreo y Operaciones

- **Analista de Monitoreo y Analista de Respuesta:** Equipo encargado de identificar la necesidad de una herramienta que apoyará las operaciones del CyberSOC y de proporcionar información sobre las actividades realizadas diariamente.

2. Ingeniería e Inteligencia

- **Analista de Automatización:** Encargado de implementar la herramienta de orquestación para apoyar las actividades del equipo de Monitoreo y Operaciones.
- **Analista de Inteligencia de Amenazas:** Encargado de proporcionar los accesos a las fuentes de inteligencia externas y a las herramientas del cliente, como QRadar y demás fuentes dentro del alcance del proyecto, así como de apoyar en el afinamiento de los flujos del orquestador.

3. Gestión y Gobierno

- **Security Manager:** Encargado de liderar la implementación del orquestador y actuar como punto de contacto con los *stakeholders* y con el cliente para el seguimiento y entrega de resultados.

3.2 Finalidad y objetivos de la Actividad

3.2.1 Finalidad

La finalidad del proyecto fue fortalecer la capacidad de detección y respuesta ante amenazas en la red perimetral del cliente, gestionada desde el CyberSOC, mediante la implementación de un sistema de orquestación de seguridad que automatizara los flujos de respuesta ante incidentes, redujera los tiempos de detección y contención, estandarizara los procedimientos y contribuyera a mejorar la capacidad operativa del CyberSOC frente al panorama de amenazas.

3.2.2 Objetivos

- **Objetivo General**

  Implementar un sistema de orquestación en un CyberSOC para automatizar la detección y respuesta ante amenazas perimetrales de un cliente corporativo.

- **Objetivos Específicos**

  a) Identificar las reglas de detección configuradas en el *Security Information and Event Management* (SIEM) para el WAF Akamai y los firewalls integrados con mayor frecuencia de disparo y mayor potencial de automatización en los flujos de respuesta.

  b) Diseñar los flujos de respuesta automatizada en el orquestador a partir de los elementos del proceso manual del analista y las integraciones con las herramientas del CyberSOC, con el propósito de garantizar una contención oportuna ante los principales vectores de amenaza perimetral.

c) Implementar los flujos de respuesta automatizada en el orquestador para garantizar su correcta operación sobre las herramientas del CyberSOC, desde el piloto controlado hasta el pase a producción.

d) Evaluar el impacto de la implementación del sistema de orquestación en los indicadores operativos MTTD y MTTR del CyberSOC, comparándolos con los valores obtenidos mediante el proceso manual.

3.3 Problemática

A nivel global, distintos informes del sector tecnológico muestran que los ataques dirigidos a las infraestructuras de red perimetral han aumentado tanto en frecuencia como en complejidad. La Agencia de la Unión Europea para la Ciberseguridad (ENISA, 2024), identifica entre las amenazas más comunes los ataques de denegación de servicio distribuido (DDoS), las intrusiones mediante vulnerabilidades expuestas y el uso de técnicas para evadir controles de seguridad. Estas amenazas requieren respuestas cada vez más rápidas y coordinadas. En esa misma línea, IBM Security (2024) reporta que las organizaciones que incorporan automatización y orquestación en sus operaciones de seguridad reducen en más del 30 % el tiempo necesario para detectar y contener brechas, en comparación con aquellas que mantienen procesos manuales. Estos resultados evidencian la importancia de incorporar mecanismos de automatización en los CyberSOC.

En el caso del Perú, los incidentes de ciberseguridad registrados en los últimos años evidencian el crecimiento de la exposición del ecosistema digital nacional. Asimismo, Ernst & Young Perú (EY, 2024) señala que los sectores corporativo y financiero vienen enfrentando un mayor número de intentos de intrusión y ataques dirigidos al perímetro de red, lo que plantea la necesidad de reforzar las capacidades de detección y respuesta en las organizaciones peruanas. A esto se suma que la digitalización acelerada del sector productivo, público y financiero, ha ampliado los puntos de exposición. Aunque los intentos de ataque disminuyeron de 15 mil millones en 2022 a 5 mil millones en 2023, las pérdidas económicas asociadas a delitos informáticos alcanzaron los S/ 40 millones, situación que evidencia la necesidad de contar con mecanismos de respuesta más eficientes y automatizados (Banco Central de Reserva del Perú [BCRP], 2025; Forbes Perú, 2024).

En este contexto, el crecimiento de las infraestructuras tecnológicas también ha incrementado los puntos de exposición ante posibles ataques. Los delincuentes informáticos aprovechan esta situación para desarrollar métodos cada vez más complejos y dirigidos contra los perímetros de red de empresas e instituciones. Frente a este escenario, los Centros de Operaciones de Seguridad (SOC) deben procesar grandes cantidades de alertas en tiempo real, lo que representa una dificultad cuando las actividades dependen principalmente de procedimientos manuales. Ante esta necesidad, la orquestación de seguridad permite automatizar determinadas tareas de detección y respuesta, contribuyendo a reducir los tiempos de atención y reacción ante los incidentes.

La empresa objeto de estudio ofrece servicios de Tecnologías de la Información (TI) y ciberseguridad a clientes del sector corporativo peruano. Su principal unidad operativa de servicio es el Centro de Operaciones de Ciberseguridad (CyberSOC), desde el cual se monitorean y atienden los eventos de seguridad de sus clientes a través de la plataforma SIEM, IBM QRadar. Sin embargo, esta gestión no contaba con un sistema de orquestación que articulara y automatizara los flujos de trabajo relacionados con las amenazas del perímetro de red. Los analistas gestionan manualmente las alertas generadas por el SIEM, lo que prolongaba los tiempos de atención. En promedio, el equipo atendía más de 1200 alertas al mes, considerando las diferentes plataformas integradas y los clientes a los que se brindaba servicio. De este universo, el presente trabajo se delimitó a las dos fuentes perimetrales del cliente corporativo en estudio: los firewalls *FortiGate* y el WAF Akamai. En estos casos, los tiempos de atención superaban los 60 minutos en promedio. Este modo de trabajo afectaba la capacidad del CyberSOC para detectar y atender oportunamente amenazas como intrusiones, escaneos maliciosos y accesos no autorizados.

El proceso de atención comprendía la consulta de la información proporcionada por el SIEM, la revisión de fuentes externas de inteligencia de amenazas, la verificación de vulnerabilidades explotables o de severidad alta y crítica en los activos asociados, el registro de los hallazgos en la herramienta de gestión de tickets y la elaboración del *case management* (reporte) que posteriormente era notificado al cliente. Al depender de la intervención humana en cada una de estas etapas, los tiempos de atención podían variar entre turnos y existía un mayor margen

para errores u omisiones en las acciones de respuesta, lo que afectaba la capacidad de protección de los activos digitales de los clientes.

Ante esta situación, surgió la necesidad de incorporar un sistema de orquestación en el CyberSOC que permitiera automatizar la detección y respuesta ante amenazas perimetrales, reducir los tiempos de reacción, estandarizar los procesos de contención y mejorar el seguimiento de los incidentes. De esta manera, se buscó mejorar la eficiencia operativa del equipo y fortalecer la capacidad de respuesta del servicio brindado al cliente.

3.3.1 Problema General

¿Cómo implementar un sistema de orquestación en un CyberSOC para automatizar la detección y respuesta ante amenazas perimetrales de un cliente corporativo?

3.3.2 Problemas Específicos

a) ¿Cuáles son las reglas de detección configuradas en el *Security Information and Event Management* (SIEM) para el WAF Akamai y los firewalls integrados que presentan mayor frecuencia de disparo y mayor potencial de automatización en los flujos de respuesta?

b) ¿Cómo diseñar los flujos de respuesta automatizada en el orquestador a partir de los elementos del proceso manual del analista y de las integraciones con las herramientas del CyberSOC para garantizar una contención oportuna ante los principales vectores de amenaza perimetral?

c) ¿Cómo implementar los flujos de respuesta automatizada en el orquestador para garantizar su correcta operación sobre las herramientas del CyberSOC, desde el piloto controlado hasta el pase a producción?

d) ¿Cuál es el impacto de la implementación del sistema de orquestación en los indicadores operativos MTTD y MTTR del CyberSOC, en comparación con el proceso manual?

3.3.3 Justificación e importancia de la investigación

A. Justificación Práctica

Dentro del CyberSOC de la empresa se identificó que las alertas de seguridad generadas por el SIEM eran gestionadas manualmente a partir del monitoreo de la infraestructura de los clientes. Esta situación generaba demoras en la atención y contención de los incidentes, además de diferencias en la ejecución de los procedimientos según la experiencia del analista responsable de cada caso. A medida que aumentaba el volumen de eventos, este modo de trabajo dificultaba mantener una atención eficiente y uniforme. Ante esta situación, el proyecto permitió automatizar los flujos de respuesta mediante un sistema de orquestación que estandarizó las acciones, redujo los tiempos de atención y permitió que los analistas concentraran sus actividades en los casos que requerían un mayor nivel de análisis. Asimismo, la implementación estableció una base tecnológica que permitió al CyberSOC ampliar su capacidad operativa y de atender amenazas cada vez más complejas.

B. Justificación Técnica

Uno de los principales problemas identificados fue la falta de integración entre las herramientas de seguridad utilizadas por el CyberSOC, entre ellas el SIEM IBM QRadar, el *Web Application Firewall* (WAF) y los firewalls perimetrales. Si bien el SIEM permitía detectar y generar alertas, las acciones de análisis y respuesta sobre el WAF y los firewalls se realizaban de manera independiente y manual, sin un flujo coordinado entre las diferentes herramientas.

La implementación del sistema de orquestación permitió establecer una capa de integración mediante APIs y conectores, de modo que las etapas de detección, análisis de contexto y respuesta se ejecutaran de manera coordinada y automatizada. Esto permitió, además, obtener una medición más precisa de los indicadores MTTD y MTTR del CyberSOC, los cuales anteriormente eran calculados de forma manual.

C. **Justificación Social**

La atención oportuna de los incidentes de ciberseguridad resulta importante debido a que sus consecuencias pueden afectar no solo a la organización involucrada, sino también a sus usuarios y terceros. Un incidente no atendido oportunamente puede ocasionar interrupciones de servicios, exposición de información y pérdida de confianza en los sistemas digitales.

En este contexto, el CyberSOC brinda servicios de monitoreo y respuesta a organizaciones del sector corporativo, por lo que la reducción de los tiempos de detección y contención contribuyó a fortalecer la seguridad de los clientes que dependen de estos servicios. La automatización de la respuesta ante amenazas perimetrales permitió reducir la posibilidad de que una atención tardía afectara a otros actores relacionados con los servicios monitoreados. Asimismo, la implementación del sistema evidenció la posibilidad de desarrollar capacidades de automatización y respuesta en empresas peruanas del sector tecnológico, mediante la integración de herramientas y recursos disponibles para las necesidades específicas de sus operaciones.

D. Justificación Económica

La implementación del sistema de orquestación presentó beneficios económicos relacionados principalmente con la reducción del tiempo destinado a tareas repetitivas y con la disminución del riesgo asociado a respuestas tardías ante incidentes de seguridad. La automatización permitió aprovechar mejor las horas de trabajo de los analistas y reducir el riesgo de incumplimiento de los acuerdos de nivel de servicio (SLA). Como referencia, según el informe *Cost of a Data Breach* 2025, IBM Security (2025) señaló que el costo promedio de una filtración de datos en América Latina alcanzó los USD 2.51 millones. Asimismo, identificó que las organizaciones que logran identificar y contener una filtración en menos de 200 días pueden reducir sus costos en aproximadamente USD 600 000, mientras que aquellas que emplean soluciones de inteligencia artificial y automatización pueden alcanzar ahorros de hasta USD 900 000 por incidente y reducir en 111 días el tiempo de identificación y resolución.

En el caso del CyberSOC, la reducción de los tiempos de respuesta permitió disminuir el riesgo de incumplimiento de los acuerdos de nivel de servicio (SLA) establecidos con los clientes, lo que contribuyó a evitar posibles penalidades contractuales. Asimismo, la automatización de tareas repetitivas, como el bloqueo de direcciones IP maliciosas y la gestión de alertas de bajo riesgo, permitió liberar horas de trabajo de los analistas para destinarlas al análisis de casos que requerían mayor intervención humana.

De esta manera, la solución implementada contribuyó a incrementar la capacidad operativa del CyberSOC sin requerir un aumento proporcional del personal para atender el crecimiento del volumen de alertas. Esto favoreció la escalabilidad del servicio y permitió aprovechar de manera más eficiente los recursos disponibles. En términos económicos, los principales beneficios estuvieron relacionados con la reducción de horas de trabajo destinadas a tareas repetitivas, la disminución del riesgo de penalidades por incumplimiento de los SLA y la reducción del impacto potencial asociado a una respuesta tardía ante incidentes de seguridad. Estos factores sustentaron la conveniencia de implementar el sistema de orquestación frente al mantenimiento del proceso de respuesta manual.

3.4 Metodología

El presente apartado desarrolla las bases teóricas y el marco conceptual que sustentan la solución implementada. El método aplicado para resolver el problema se detalla en el apartado 3.5 Procedimiento.

3.4.1 Bases teóricas

En esta sección se revisaron trabajos previos, tesis y publicaciones relacionadas con la implementación de plataformas SOAR, la orquestación de la seguridad y la automatización de la respuesta ante incidentes, tanto en el ámbito nacional como internacional. Esta revisión permitió identificar enfoques, marcos de referencia y resultados obtenidos en experiencias previas, que sirvieron de sustento para el diseño e implementación del sistema de orquestación desarrollado en el presente proyecto.

A. Antecedentes nacionales

En el ámbito nacional, Vilcarromero y Vilchez (2018) desarrollaron, en su tesis de maestría para la Universidad Peruana de Ciencias Aplicadas (UPC): *Una propuesta de implementación de un modelo de gestión de ciberseguridad para el Centro de Operaciones de Seguridad (SOC) de una empresa del sector telecomunicaciones, basado en el Cybersecurity Framework (CSF) del NIST (NIST, 2018)*. El modelo abordó la gestión de riesgos y la medición de controles según niveles de madurez, considerando los procesos, la tecnología y el personal involucrado en la operación del SOC. Este antecedente resulta relevante porque evidencia la aplicación de un enfoque basado en el NIST en centros de

operaciones de seguridad peruanos y respalda el enfoque por procesos adoptado en el presente proyecto.

Por su parte, Atalaya Urrutia (2023), en su tesis doctoral sustentada en la Universidad Nacional de Piura, propuso un modelo de ciberseguridad para universidades privadas del Perú basado en las normas ISO/IEC 27032 y el marco NIST. El modelo incorporó componentes de evaluación de riesgos, políticas y procedimientos de seguridad, monitoreo, detección de incidentes, y mejora continua. Aunque el ámbito de aplicación difiere del sector corporativo atendido por el CyberSOC, el estudio aporta un referente sobre la aplicación de marcos de ciberseguridad reconocidos internacionalmente en organizaciones peruanas y permite relacionarlos con las necesidades particulares de cada organización. En este caso, mediante un sistema de orquestación SOAR a las particularidades operativas de cada organización.

B. Antecedentes internacionales

En el contexto internacional, Mir y Ramachandran (2021) presentaron la implementación de una plataforma SOAR aplicada a sistemas SCADA de redes eléctricas inteligentes (*smart grids*). Los autores demostraron cómo la orquestación permitió correlacionar alertas de sistemas de control industrial y ejecutar respuestas ante amenazas dirigidas a infraestructura crítica. Aunque estos sistemas pertenecen al dominio OT y no al de TI corporativa abordado en el presente proyecto, el estudio evidencia la aplicación de plataformas SOAR en entornos que requieren respuestas rápidas y coordinadas.

Pulyala et al. (2019) realizaron un análisis del impacto de las plataformas SOAR en la eficiencia operativa de los centros de operaciones de seguridad (SOC), evidenciando reducciones significativas en los tiempos de detección y respuesta (MTTD y MTTR), así como una disminución de la carga operativa sobre los analistas de nivel 1 mediante la automatización de tareas repetitivas. Estos resultados se relacionan directamente con los indicadores que se utilizaron para evaluar la implementación del sistema de orquestación en el presente proyecto.

Finalmente, Ismail et al. (2025) propusieron un enfoque de hiperautomatización para SOC basado en inteligencia artificial agentica, integrado

a una plataforma SOAR, con el objetivo de robustecer la generación y ejecución de *playbooks* de respuesta automatizada. Si bien el presente proyecto no contempla la incorporación de agentes de inteligencia artificial, el estudio constituye un referente para posibles mejoras futuras del sistema de orquestación implementado en el CyberSOC.

3.4.2 Marco conceptual

3.4.2.1 Centro de Operaciones de Seguridad (SOC / CyberSOC)

Un Centro de Operaciones de Seguridad (SOC, *Security Operations Center*) es un equipo centralizado que monitorea, detecta, analiza y responde de forma continua a los incidentes de ciberseguridad de una o varias organizaciones, apoyándose en la integración de procesos, tecnología y personal especializado (MITRE Corporation, 2022). En el presente trabajo, el CyberSOC de la empresa constituye el entorno operativo donde se implementó el sistema de orquestación, al ser la unidad responsable del monitoreo y la respuesta sobre la infraestructura del cliente.

3.4.2.2 SOAR (*Security Orchestration, Automation and Response*)

Las plataformas SOAR son soluciones tecnológicas que integran capacidades de orquestación de herramientas de seguridad, automatización de flujos de trabajo y gestión de incidentes en un único entorno operativo (MITRE Corporation, 2022). Permiten definir *playbooks*, es decir, secuencias automatizadas de acciones de respuesta que se ejecutan ante la detección de eventos específicos, reduciendo la intervención humana en tareas repetitivas y acelerando los tiempos de contención (CISA, 2021).

3.4.2.3 Red Perimetral

La red perimetral comprende el conjunto de dispositivos y controles que delimitan el límite entre la red interna de una organización e Internet (Stallings, 2017). Sus principales componentes incluyen firewalls de próxima generación (NGFW), sistemas de detección y prevención de intrusiones (IDS/IPS), *proxies* y zonas desmilitarizadas (DMZ) (Scarfone y Hoffman, 2009).

3.4.2.4 Amenazas Perimetrales

Las amenazas perimetrales abarcan ataques de reconocimiento, explotación de vulnerabilidades en servicios expuestos, ataques de denegación de servicio (DoS/DDoS) e intentos de acceso no autorizado (Scarfone y Mell, 2007). Estos vectores representan algunos de los principales riesgos dirigidos a los controles de frontera de la red organizacional y se encuentran catalogados en marcos de referencia de uso extendido como MITRE ATT&CK (MITRE Corporation, 2023).

3.4.2.5 *Playbooks* de Respuesta ante Incidentes

Un *playbook* de respuesta ante incidentes es un conjunto de procedimientos predefinidos que describe las acciones a ejecutarse ante un tipo específico de evento de seguridad (Cichonski et al., 2012). En el contexto SOAR, los *playbooks* se implementan como flujos de trabajo automatizados que pueden incluir acciones de enriquecimiento de información, notificación a equipos, bloqueo de amenazas en dispositivos de red y documentación del incidente (CISA, 2021).

3.4.2.6 MTTD (*Mean Time to Detect*)

El tiempo medio de detección (MTTD) mide el tiempo promedio transcurrido entre la ocurrencia de un incidente de seguridad y su identificación por parte del CyberSOC (Cichonski et al., 2012). Según análisis de incidentes reales a nivel global, el MTTD puede extenderse semanas o meses cuando los procesos de monitoreo son predominantemente manuales, lo que evidencia la necesidad de mecanismos de detección automatizada (Verizon, 2024).

Dado que el momento de ocurrencia de un incidente no es observable directamente, en el presente trabajo el MTTD se define operativamente como el tiempo transcurrido desde la generación de la ofensa en QRadar hasta la notificación al cliente, en el proceso manual, o hasta la finalización del análisis y la creación del ticket, en el proceso automatizado. Esta definición incluye el triaje, el enriquecimiento y la elaboración del reporte, por lo que es más amplia que la definición conceptual de Cichonski et al. (2012). Las fórmulas se detallan en la Fase 1 (apartado 3.5.1.1).

3.4.2.7 MTTR (*Mean Time to Resolve*)

El tiempo medio de resolución (MTTR) mide el tiempo promedio entre la detección de un incidente y la ejecución de las acciones de contención o resolución (Cichonski et al., 2012). Su reducción es uno de los objetivos primarios de la implementación de plataformas SOAR, al automatizar las acciones de respuesta iniciales y eliminar la latencia asociada a los procesos manuales (Verizon, 2024).

En el presente trabajo, el MTTR se define operativamente como el tiempo transcurrido desde la notificación al cliente hasta el cierre del caso, en el proceso manual, o desde el inicio del accionable hasta el cierre del ticket, en el proceso automatizado. En los casos derivados a análisis asistido, concluye cuando el cliente indica la acción y el cierre. En ambos procesos el indicador termina con el cierre del flujo de atención, lo que permite comparar los mismos hitos antes y después de la implementación.

3.4.2.8 SIEM (*Security Information and Event Management*)

Las plataformas SIEM recopilan, normalizan y correlacionan eventos de seguridad provenientes de múltiples fuentes de la infraestructura tecnológica, generando alertas cuando se detectan patrones anómalos o comportamientos maliciosos (Kent y Souppaya, 2006). Su función consiste en centralizar la información del entorno de seguridad y facilitar la correlación de eventos para la generación de alertas (Bhatt et al., 2014). IBM QRadar, empleado en el CyberSOC, proporciona estas capacidades junto con el análisis de flujos de red y la generación de ofensas que sirven como punto de partida para los *playbooks* SOAR.

3.4.2.9 Ofensas, eventos y alertas de seguridad

En el contexto de la plataforma SIEM IBM QRadar, un evento es un registro puntual generado por una fuente monitoreada, como un firewall o un WAF, mientras que una ofensa es la agrupación de eventos correlacionados que la plataforma clasifica como un posible incidente y presenta al analista para su gestión (IBM, 2024). Las ofensas generadas por las reglas de detección priorizadas constituyen el punto de entrada de los flujos automatizados del orquestador MCIA.

3.4.2.10 Reglas de detección y casos de uso de seguridad

Las reglas de detección o de correlación definen las condiciones bajo las cuales el SIEM genera una ofensa a partir de los eventos recibidos y permiten implementar los casos de uso de seguridad que el SOC decide monitorear sobre la infraestructura (IBM, 2024). En este proyecto se priorizaron 48 reglas, 23 asociadas a eventos de firewall y 25 al tráfico web del WAF Akamai, que delimitan el universo de casos de uso automatizados por el orquestador.

3.4.2.11 API (*Application Programming Interface*)

Una interfaz de programación de aplicaciones (API) es un conjunto de definiciones y protocolos que permite que dos sistemas de software se comuniquen e intercambien datos de forma estandarizada. En las arquitecturas web modernas destaca el estilo REST, fundamentado en los principios arquitectónicos de la web (Fielding, 2000). El orquestador MCIA se integra mediante API con el SIEM, el WAF Akamai, las fuentes de reputación, la ticketera iTop y el motor de IA, lo que permite ejecutar consultas y acciones de respuesta de forma automatizada.

3.4.2.12 Microservicios

Los microservicios son un estilo arquitectónico que estructura una aplicación como un conjunto de servicios pequeños e independientes, desplegables por separado y comunicados mediante interfaces ligeras, lo que favorece la escalabilidad, disponibilidad y mantenimiento del sistema (Newman, 2021). En la solución implementada, los microservicios cybersoc-api y email-api conectan el motor de orquestación con el resto de los componentes y se encargan, respectivamente, de exponer la información y enviar las notificaciones.

3.4.2.13 Web Application Firewall (WAF)

Un *Web Application Firewall* (WAF) es un control de seguridad que inspecciona y filtra el tráfico HTTP/HTTPS dirigido a las aplicaciones web, con el fin de bloquear ataques como inyecciones de código, explotación de vulnerabilidades o accesos no autorizados (OWASP Foundation, s. f.). En este proyecto, el WAF Akamai es, a la vez, fuente de alertas correlacionadas en el SIEM y canal de respuesta sobre el cual el orquestador ejecuta los bloqueos automáticos de direcciones IP maliciosas.

3.4.2.14 Lista Dinámica Externa (EDL) y listas de bloqueo

Una lista dinámica externa (EDL, *External Dynamic List* o *external blocklist*) es un mecanismo mediante el cual un firewall consume periódicamente, desde una ubicación externa, una lista de indicadores como direcciones IP, dominios o URL, y aplica sobre ellos acciones de bloqueo de forma centralizada y dinámica, sin modificar manualmente la política de cada equipo (Fortinet, 2024). En la solución implementada, la EDL de los firewalls FortiGate es el canal mediante el cual el orquestador bloquea direcciones IP maliciosas de manera simultánea en los 21 firewalls del cliente.

3.4.2.15 Inteligencia de amenazas (*Threat Intelligence*) e indicadores de compromiso (IoC)

La inteligencia de amenazas es información sobre actores, campañas y artefactos maliciosos que, una vez procesada y contextualizada, permite anticipar, detectar y priorizar la respuesta ante ataques. Los indicadores de compromiso (IoC) son evidencias observables asociadas a actividad maliciosa, como direcciones IP, dominios o hashes de archivos (Johnson et al., 2016). El orquestador MCIA consulta fuentes de reputación como VirusTotal, AbuseIPDB, Criminal IP y OTX AlienVault para determinar la reputación de las direcciones IP involucradas en cada ofensa, información que forma parte del factor de certeza reputacional del *risk score*.

3.4.2.16 Enriquecimiento de información

El enriquecimiento de información es el proceso de agregar contexto adicional a una alerta, como el estado de vulnerabilidades del activo, la geolocalización o la reputación de una dirección IP, con el fin de mejorar el análisis y la decisión de respuesta (Cichonski et al., 2012). En los flujos del orquestador, el enriquecimiento se realiza de forma automática mediante las integraciones con Tenable, Cortex XDR, la geolocalización de IP y las fuentes de inteligencia de amenazas.

3.4.2.17 Inteligencia artificial generativa e ingeniería de prompts

Los modelos de lenguaje de gran escala son sistemas de inteligencia artificial capaces de generar texto a partir de instrucciones en lenguaje natural denominadas *prompts*; su ingeniería se basa en la práctica de diseñar dichas instrucciones para orientar la respuesta del modelo hacia una tarea específica (Liu et al., 2023). En la solución implementada, la rama no maliciosa de los flujos envía el contexto

consolidado del evento al motor de IA (Gemini) mediante *prompts* estructurados, para obtener un análisis asistido con recomendaciones sobre el tratamiento del evento.

3.5 Procedimiento

Para el desarrollo del proyecto, las actividades se organizaron en cuatro etapas, conformadas por catorce fases de trabajo. Estas fases fueron definidas de acuerdo con la secuencia necesaria para el desarrollo e implementación del sistema de orquestación. El cronograma general de actividades se presenta en la Tabla 1, mientras que el detalle de cada fase, sus actividades predecesoras y entregables se encuentra en el Anexo A.

Tabla 1 **Cronograma de actividades del proyecto**

Etapa	**Actividades**	**Mes**				
		dic-25	**ene-26**	**feb-26**	**mar-26**	**abr-26**
Etapa 1	1. Iniciación y gobierno interno					
	2. Descubrimiento y requisitos					
Etapa 2	3. Diseño de arquitectura					
	4. Provisionamiento de infraestructura					
	5. Desarrollo del core (cybersoc-api)					
	6. Desarrollo de integraciones					
	7. Motor de decisión y respuesta					
	8. *Playbooks* por regla					
	9. Sistema web y dashboards					
Etapa 3	10. Pruebas y QA					
	11. Piloto controlado					
	12. Despliegue a producción					
Etapa 4	13. Operación y mejora continua *					

14. Cierre de la implementación	

Fuente. Elaboración propia.

3.5.1 Etapa 1: Análisis y levantamiento de información (Fases 1 y 2)

3.5.1.1 Fase 1 - Iniciación y gobierno interno

A. Evaluación del entorno operativo del cliente.

1. Fuentes integradas con el QRadar que monitorea el CyberSOC.

   Se identifican las siguientes fuentes:

   a. Firewall: Se cuenta con 21 firewalls de la marca FortiGate, distribuidos en la infraestructura del cliente, como se muestra en la Figura 2.

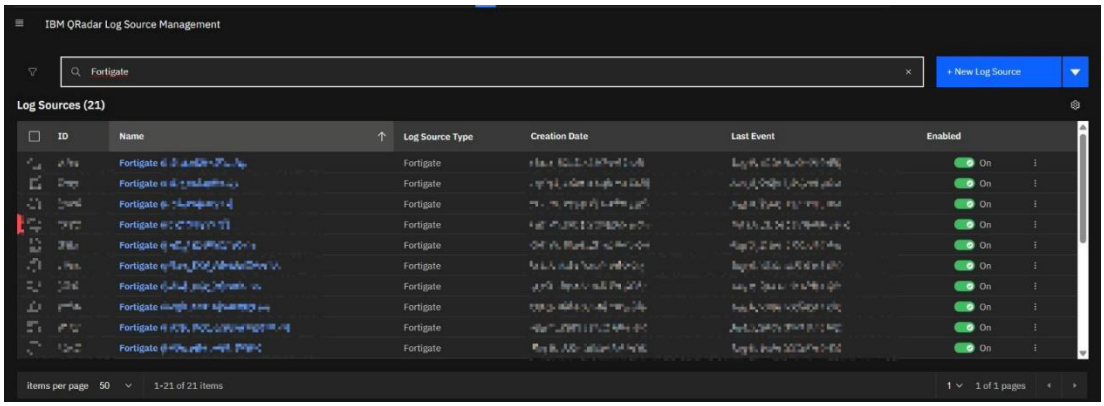


Figura 2 **Firewalls FortiGate integrados en QRadar.** Fuente. Elaboración propia, a partir de la herramienta QRadar.

   b. WAF Akamai: Servicio de *Web Application Firewall* de la marca Akamai, desplegado en la nube, como se muestra en la Figura 3.

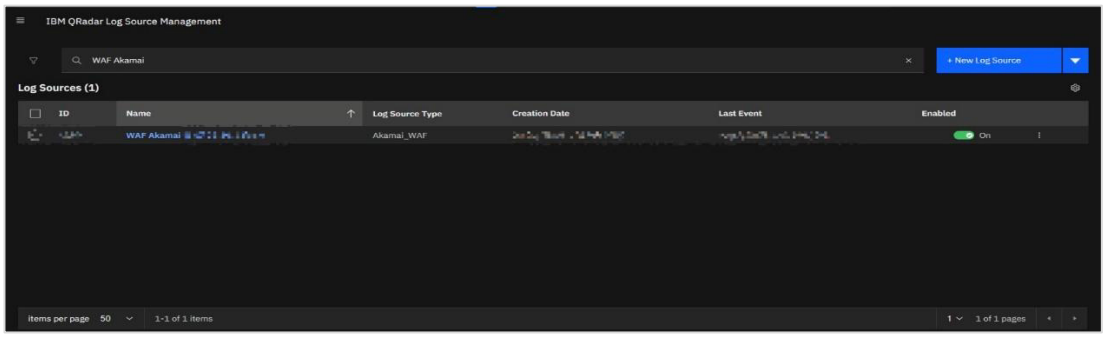


Figura 3 **WAF Akamai integrado en QRadar.** Fuente. Elaboración propia, a partir de la herramienta QRadar.

2. Herramientas de seguridad gestionada

El inventario de las herramientas identificadas comprende las siguientes:

a. Lista dinámica externa (EDL): Uso de la función nativa EDL de FortiGate para distribuir y bloquear direcciones IP maliciosas de forma centralizada en los *firewalls*, como se muestra en la Figura 4.



Figura 4 **Lista Dinámica Externa (EDL) configurada en FortiGate** Fuente. Elaboración propia

b. Cortex XDR: Plataforma de detección y respuesta extendida (XDR) que permite enriquecer la información sobre las vulnerabilidades detectadas en los *endpoints*. Proporciona datos como el CVE, la severidad, la explotabilidad y la criticidad del activo, facilitando su priorización y la respuesta ante las amenazas, como se muestra en la Figura 5.

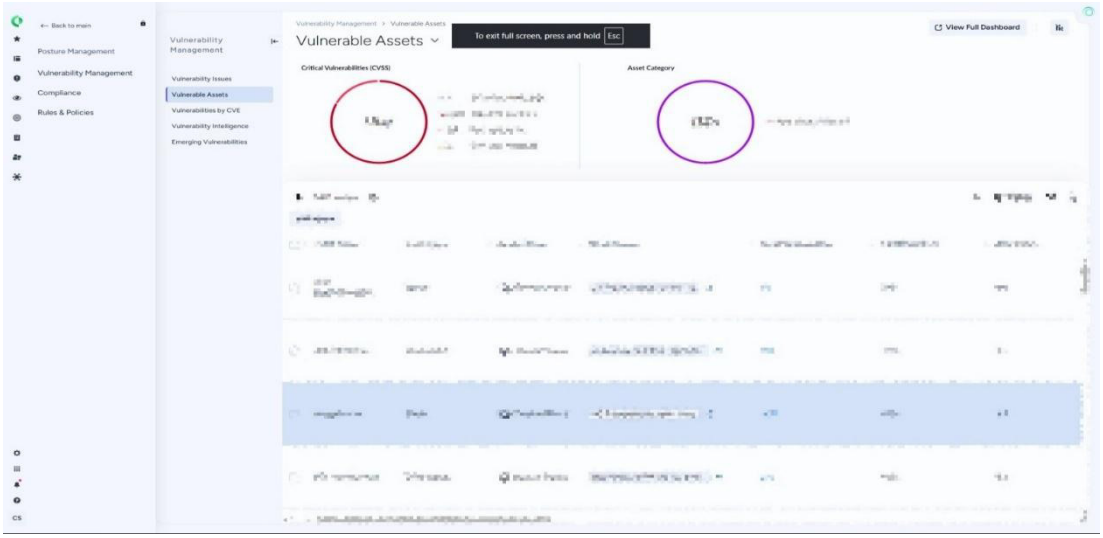


Figura 5 **Consola de Cortex XDR.** Fuente. Elaboración propia, a partir de la herramienta Cortex XDR.

c. Tenable: Plataforma de gestión de vulnerabilidades que escanea los *endpoints* para identificar las vulnerabilidades presentes. Proporciona información como el CVE, la severidad y el estado del parche, lo que permite mantener una visión actualizada del riesgo en los activos, como se muestra en la Figura 6.

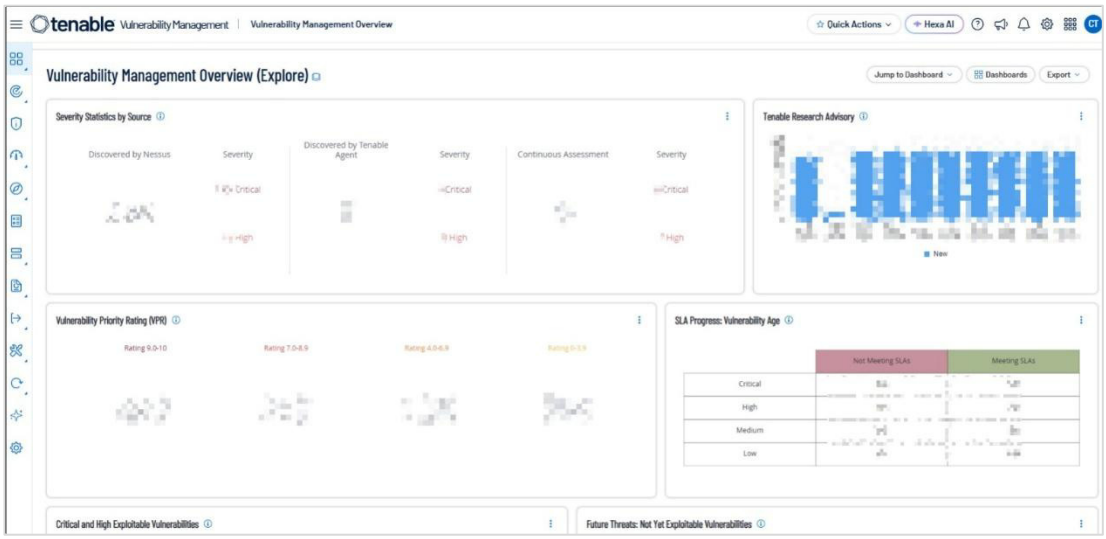


Figura 6 **Consola de Tenable.** Fuente. Elaboración propia, a partir de la herramienta Tenable.

d. *Web Application Firewall* (WAF) de Akamai: Protege las aplicaciones web mediante el filtrado del tráfico entrante y el bloqueo de direcciones

IP maliciosas identificadas, contribuyendo a prevenir ataques y accesos no autorizados a los servicios expuestos, como se muestra en la Figura 7.

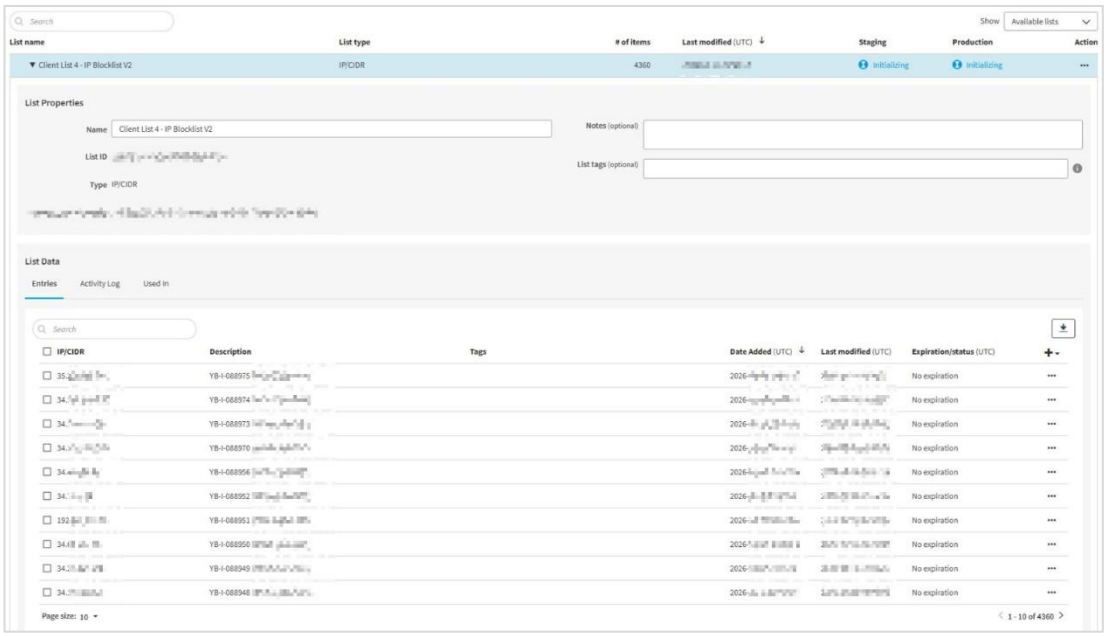


Figura 7 **Consola del WAF Akamai.** Fuente. Elaboración propia, a partir de la herramienta WAF Akamai.

3. Flujos de detección y respuesta que el CyberSOC gestiona actualmente sobre la infraestructura del cliente

   Se identificaron los siguientes flujos de detección:

   a. Como parte del levantamiento de información, se revisaron los flujos de detección y respuesta que actualmente gestiona el CyberSOC sobre la infraestructura del cliente

      Para ello, se identificaron los *stakeholders* involucrados, se establecieron sus principales responsabilidades y se elaboró una matriz RACI para definir su participación en las actividades del proyecto.

      - **Identificación de *stakeholders:*** Se identificaron las partes interesadas de la empresa y del cliente que intervienen en el desarrollo del proyecto. Se consideraron tanto los responsables de la implementación y operación del orquestador como aquellos

encargados de aprobar o participar en las acciones realizadas sobre la infraestructura del cliente. Los *stakeholders* identificados se muestran en la Tabla 2.

Tabla 2 **Stakeholders identificados en el proyecto**

Organización	Leyenda Roles	*Stakeholder*	Responsabilidad principal	Tipo de participación
EMPRESA	GT	Gerente de Tecnología	Busca optimizar recursos y ofrecer mejor calidad de servicios.	Indirecta
	SM	Gerente de seguridad	Lidera la iniciativa; es el principal responsable de la comunicación con todas las áreas; presente en todas las fases del proyecto supervisando.	Directa
	AA	Analista de Automatización	Implementa la herramienta (orquestador).	Directa
	AITA	Analista de Inteligencia de Amenazas	Comparte su aporte para el análisis de la lógica que se irá llevando (*risk score*).	Directa
	EM	Equipo de Monitoreo	Aporta sus actividades manuales para que sean automatizadas.	Directa
CLIENTE	LSI	Líder de Seguridad de la Información	Presente en el proyecto; brinda su aprobación para los pases a producción.	Directa

	AFW	Analista de Seguridad FW	Administra los firewalls del cliente; aprueba el bloqueo de IPs en el EDL bajo la lógica de risk score que ingresa el orquestador.	Directa
	AWAF	Analista de Seguridad WAF	Administra el WAF Akamai del cliente; aprueba el bloqueo de IPs en el Network List bajo la lógica de risk score que ingresa el orquestador.	Directa

Fuente. Elaboración propia.

- **Definición de responsabilidades:** A partir de los *stakeholders* identificados, se establecieron las principales responsabilidades de cada participante dentro del proyecto. Esto permitió precisar las funciones relacionadas con el diseño, configuración, pruebas, aprobación y seguimiento de los flujos de respuesta automatizada.

- **Matriz RACI:** Para complementar la definición de responsabilidades, se elaboró una matriz RACI para las principales actividades del proyecto. Esta matriz permite identificar el nivel de participación de cada *stakeholder*: **R** corresponde a quien ejecuta la actividad (*Responsible*), **A** quien asume la responsabilidad y aprobación final (*Accountable*), **C** a quien es consultado (*Consulted*) e **I** a quien debe mantenerse informado (*Informed*). La matriz RACI se presenta en la Tabla 3.

Tabla 3 **Matriz RACI de las actividades del proyecto**

Actividad	**GT**	**SM**	**AA**	**AITA**	**EM**	**LSI**	**AFW**	**AWAF**

Definición de alcance y objetivos del proyecto	C	A/R	C	I	I	C	I	I
Diseño de la lógica de risk score	I	A	C	R	I	C	I	I
Mapeo de actividades manuales de monitoreo a automatizar	I	A	R	I	R	I	I	I
Desarrollo/configuración del orquestador	I	A	R	C	I	I	I	I
Definición de reglas de integración con FW (EDL)	I	A	R	I	I	C	R	I
Definición de reglas de integración con WAF Akamai (Network List)	I	A	R	I	I	C	I	R
Pruebas del orquestador en ambiente controlado	I	A	R	I	C	I	C	C
Aprobación de pase a producción	I	R	I	I	I	A	I	I
Aprobación de bloqueo de IPs en EDL (FW)	I	I	R	I	I	I	A	I
Aprobación de bloqueo de IPs en Network List (WAF)	I	I	R	I	I	I	I	A
Monitoreo y ajuste continuo de la lógica de risk score	I	A	C	R	C	I	I	I
Gestión de excepciones / falsos positivos	I	A	R	I	I	I	C	C
Comunicación de avances y reporte de estado	I	A/R	I	I	I	I	I	I

Fuente. Elaboración propia.

4. Levantamiento y priorización de reglas de detección, se documentaron las 23 reglas de correlación configuradas en QRadar para los eventos de firewall y las 25 reglas asociadas al WAF Akamai para el tráfico web

Se identificaron las reglas de detección de firewall configuradas en QRadar, como se muestra de manera parcial en la Figura 8.



Figura 8 **Reglas de detección de Firewall configuradas en QRadar (listado parcial).** Fuente. Elaboración propia, a partir de la herramienta QRadar.

Asimismo, se identificaron las reglas de detección asociadas al WAF Akamai configuradas en QRadar, cuyo listado parcial se muestra en la Figura 9.



Figura 9 **Reglas de detección de WAF Akamai configuradas en QRadar (listado parcial).** Fuente. Elaboración propia, a partir de la herramienta QRadar.

5. Definición de la línea base de indicadores (MTTD, MTTR, intervención manual)

   a. MTTD

      Para este proyecto, corresponde al tiempo transcurrido desde la generación de la alerta en QRadar hasta el reporte de esta al cliente. Se calculó mediante la siguiente fórmula:

      MTTD = Hora de reporte al cliente − Hora de generación de la alerta en QRadar

      En la Tabla 4 se muestra la línea base del MTTD correspondiente a los meses de octubre y noviembre de 2025, calculada a partir de 236 alertas de Firewall (137 y 99 respectivamente) y 367 de WAF Akamai (182 y 185). Cada valor corresponde al promedio del tiempo de detección

de las alertas del periodo, es decir, la suma de los tiempos dividida entre la cantidad de alertas. En conjunto, el MTTD fue de 1:30:34.

Tabla 4 **Línea base del MTTD (octubre y noviembre de 2025)**

Plataforma	Oct-25	Nov-25	Promedio general
Firewall Fortigate	1:50:28	1:54:35	1:52:11
WAF Akamai	1:29:46	1:03:46	1:16:40
Promedio general	1:38:39	1:21:29	1:30:34

Fuente. Elaboración propia.

b. MTTR

Para este proyecto, el MTTR corresponde al tiempo transcurrido desde el reporte de la alerta al cliente hasta su solución. Se calculó mediante la siguiente fórmula:

MTTR = Hora de solución de la alerta − Hora de reporte al cliente

En la Tabla 5 se muestra la línea base del MTTR correspondiente a los meses de octubre y noviembre de 2025, calculada sobre las mismas 603 alertas consideradas para el MTTD. Al igual que en el caso anterior, cada valor corresponde al promedio del tiempo de resolución de las alertas del periodo. En conjunto, el MTTR fue de 30:52:55, es decir, cerca de 31 horas desde el reporte al cliente hasta la solución.

Tabla 5 **Línea base del MTTR (octubre y noviembre de 2025)**

Plataforma	Oct-25	Nov-25	Promedio general
Firewall Fortigate	39:18:11	26:06:23	33:46:02

WAF Akamai	27:47:56	30:14:03	29:01:35
Promedio general	32:44:22	28:47:43	30:52:55

Fuente. Elaboración propia.

c. Intervención manual

Antes de la implementación del orquestador, el análisis, la respuesta y la solución de las alertas se realizaban de manera manual. El analista de monitoreo revisaba la ofensa generada en QRadar y enviaba la notificación correspondiente al cliente. Cuando el caso requería una acción inmediata, se coordinaba con el cliente para obtener su confirmación. Una vez autorizado el accionable, el analista de respuesta ejecutaba la acción correspondiente y posteriormente se procedía con el cierre del caso.

Cabe precisar que la línea base considera únicamente las alertas generadas por las reglas de las dos fuentes perimetrales incluidas en el alcance del proyecto: los *firewalls* FortiGate y el WAF Akamai. Por ello, su volumen mensual es menor al total de alertas gestionadas por el CyberSOC, que considera todas las plataformas integradas y clientes y supera las 1200 alertas mensuales.

6. *Kick-off* formal de la iniciativa

Se realizó una reunión con participación de los *stakeholders* del proyecto y representantes del cliente, en la cual se presentó la iniciativa de implementación del orquestador y su finalidad de mejorar los tiempos de atención y respuesta del servicio de seguridad gestionada. Como resultado, se obtuvo la aprobación para iniciar el desarrollo de la iniciativa y se establecieron los principales acuerdos y compromisos, los cuales quedaron registrados en un acta cuya evidencia se muestra en la Figura 10. Entre los acuerdos registrados en el acta de dicha reunión, se establecieron como metas del proyecto reducir el MTTD a menos de 15 minutos y el MTTR a menos de 30 minutos.



Figura 10 **Convocatoria a la reunión de kick-off del proyecto**. Fuente. Elaboración propia, a partir del correo enviado el 15/12/2025.

3.5.1.2 Fase 2 - Descubrimiento y requisitos

A partir del inventario de fuentes, herramientas y reglas de detección levantado en la Fase 1 (Figuras 8 y 9), en esta fase se definieron el criterio de análisis por fuente, la política de auto-respuesta y los requisitos de integración del orquestador.

A. Definición del criterio de análisis por fuente

Se identifica que existen dos flujos:

1. Reglas de *firewall*

La matriz de decisión determina si el análisis debe realizarse sobre la IP de origen o de destino.

2. WAF Akamai

El destino se mantiene fijo mediante el *CEF Connector*, por lo que se analiza la IP de origen externa junto con el *request site*.

B. Definición de la política de auto-respuesta y aprobación del cliente

Se decidió qué acciones puede ejecutar el orquestador de forma automática, el umbral de riesgo que las habilita y los casos que requieren validación humana, según lo establecido en la Tabla 6.

Tabla 6 **Política de auto-respuesta acordada con el cliente**

Elemento	**Definición acordada**
Acciones automáticas permitidas	Bloqueo de IP en WAF Akamai y en la Lista Dinámica Externa
Umbral de riesgo que las habilita	Risk score ≥ 6
Tratamiento de casos por debajo del umbral (< 6)	Sin bloqueo automático; análisis asistido por IA y notificación.

Fuente. Elaboración propia.

C. Definición de requisitos de integración y conectividad

Se identificaron los APIs, conectores y mecanismo de comunicación (VPN *site-to-site*) necesarios para que el orquestador acceda de forma segura al SIEM, a los dispositivos perimetrales y a las herramientas de seguridad del cliente, según se detalla en la Tabla 7.

Tabla 7 **Herramientas integradas y su propósito en el orquestador**

Herramienta / Fuente	**Tipo de conexión prevista**	**Propósito en el orquestador**
IBM QRadar	API propio de la plataforma	Fuente de ofensas de Firewall y WAF Akamai
VPN site-to-site (Firewall del cliente – Firewall de la empresa)	Tunel VPN *site-to-site*	Acceso seguro del orquestador a la API de QRadar sobre la infraestructura del cliente
Lista Dinámica Externa (EDL)	Cuenta de servicio provista por el cliente	Bloqueo automático en los firewalls del cliente
WAF Akamai	API propio de la plataforma	Bloqueo automático de IPs maliciosas en el módulo WAF

Tenable	Carga documental (sin API en tiempo real)	Enriquecimiento con estado de vulnerabilidades
Cortex XDR	API propio de la plataforma	Enriquecimiento con información de activos en tiempo real
Geolocalización de IP	API propio de la plataforma	Enriquecimiento de contexto geográfico de la IP
AbuseIPDB	API propio de la plataforma	Reputación de IP para el cálculo de risk score
VirusTotal	API propio de la plataforma	Reputación de IP para el cálculo de risk score
CriminalIP	API propio de la plataforma	Reputación de IP para el cálculo de risk score
OTX AlienVault	API propio de la plataforma	Reputación de IP para el cálculo de risk score
Gemini	API propio de la plataforma	Apoyo de IA al triaje y recomendaciones
iTop	Cuenta de servicio de la herramienta	Gestión y trazabilidad de tickets

Fuente. Elaboración propia.

3.5.2 Etapa 2: Diseño e implementación de la solución (Fases 3 a 9)

3.5.2.1 Fase 3 - Diseño e implementación de la arquitectura

A. Definición de los componentes de la plataforma, del modelo de datos, de los microservicios y del motor de cálculo de *risk score* (gravedad global, certeza reputacional, direccionalidad del flujo y mapeo de campañas activas, en una escala de 1 a 10)

Como parte de esta fase, se diseñó e implementó el motor de orquestación MCIA (motor de orquestación con inteligencia artificial),

construido bajo una arquitectura por capas que va desde la visualización hasta el almacenamiento de datos. Esta arquitectura permite escalar el sistema y mantenerlo disponible, como se muestra en la Figura 11.

En el centro de esta arquitectura está el motor de orquestación MCIA, que programa tareas y ejecuta varios flujos de trabajo al mismo tiempo. Se conecta con el SIEM del cliente (IBM QRadar), correlaciona los eventos con apoyo de inteligencia de amenazas y calcula un puntaje de riesgo por cada alerta. Este puntaje combina cuatro factores en una escala del 1 al 10: gravedad global, certeza reputacional, direccionalidad del flujo y mapeo de campañas activas.

A partir de los eventos que recibe del SIEM y de otras herramientas del cliente, el orquestador puede actuar de forma automática y bloquear direcciones IP maliciosas tanto en los firewalls (vía lista EDL) como en el WAF de Akamai. Para reforzar este análisis, cruza información con herramientas de gestión de vulnerabilidades como Tenable y Cortex XDR, y con fuentes de inteligencia de amenazas externas como VirusTotal, AbuseIPDB, Criminal IP y OTX AlienVault. También se integra con iTop para la gestión de tickets, con IPlocation para geolocalizar direcciones IP y con Gemini, que aporta procesamiento de IA adicional para interpretar los eventos.

Por debajo, una capa de microservicios propios, *cybersoc-api* y *email-api*, ambos con alta disponibilidad, conecta el motor MCIA con el resto del sistema y se encarga de exponer la información y enviar las notificaciones correspondientes. Los datos quedan almacenados en una base de datos PostgreSQL configurada también con alta disponibilidad, lo que evita interrupciones ante fallas.

Finalmente, los operadores y analistas acceden a un sistema web donde revisan en tiempo real el estado de las alertas, consultan métricas operativas y siguen la trazabilidad de las alertas e incidentes. Ese acceso pasa primero por un firewall perimetral y luego por uno de red interna, que filtran el tráfico antes de llegar al sistema.

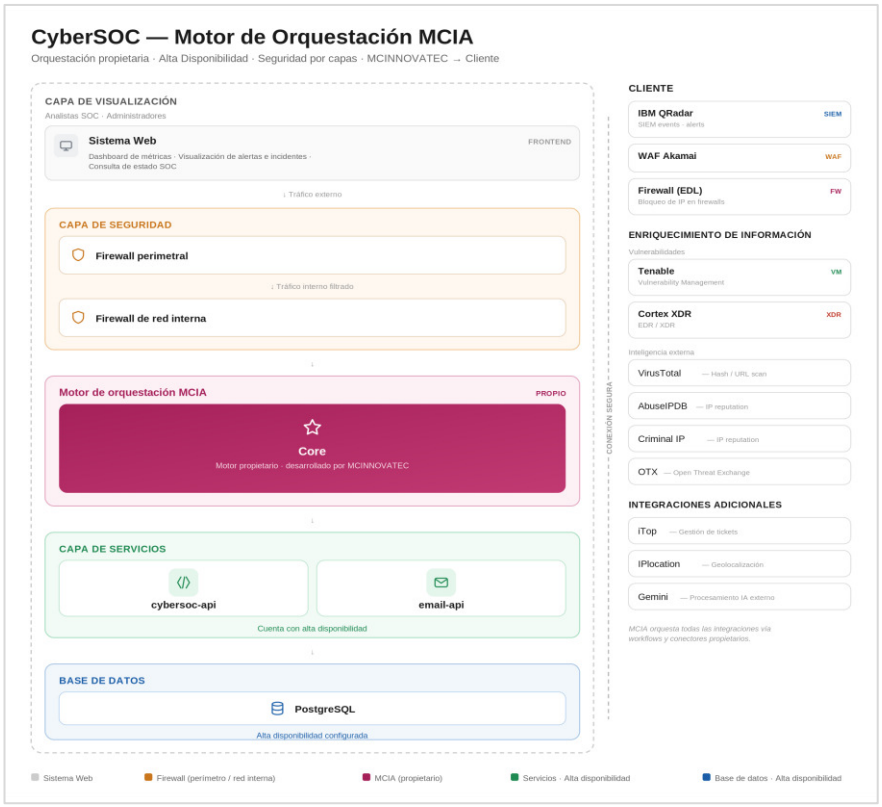


Figura 11 **Arquitectura implementada del motor de orquestación MCIA.**
Fuente. Elaboración propia.

B. Diseño de plantillas de flujo por fuente

Plantilla por defecto para eventos de firewall (Lista Dinámica Externa, con enriquecimiento de Tenable y Cortex XDR) y plantilla específica para WAF Akamai (orden WAF→EDL, con historial por *request site*).

El diseño de los *playbooks* del sistema SOAR sigue una arquitectura modular. En lugar de construir una lógica independiente para cada una de las 48 reglas priorizadas (23 de Firewall y 25 de WAF Akamai), se definieron dos plantillas de flujo que comparten una misma secuencia de etapas y se parametrizan según la regla que las dispara. Esta forma de trabajo reduce el esfuerzo de mantenimiento, ya que un cambio en la lógica de enriquecimiento o de respuesta se aplica a todas las reglas de la fuente correspondiente sin tener que modificar cada *playbook* de forma individual.

1. Plantillas de flujo por fuente

Ambas plantillas ejecutan una misma secuencia de etapas, que se adaptan según la fuente:

a. Ingesta

Recepción del evento (ofensa de un Firewall o alerta de WAF Akamai) y extracción de los campos relevantes: IP origen o destino según la matriz de decisión para Firewall, o IP origen externa junto con el *request site* para WAF Akamai.

b. Enriquecimiento

Consulta a fuentes de contexto, Tenable y Cortex XDR para obtener información sobre las vulnerabilidades del activo en el caso de Firewall; para WAF Akamai, se consulta el historial de eventos previos asociados al *request site*.

c. Cálculo de *risk score*:

Cálculo del puntaje considerando la gravedad global, certeza reputacional, direccionalidad del flujo y mapeo de campañas activas, en una escala de 1 a 10.

d. Decisión

Clasificación según el umbral de riesgo: ≥6 corresponde a malicioso y <6 sospechoso, benigno o neutral.

e. Respuesta

Para eventos clasificados como maliciosos, se ejecuta el bloqueo automático (Lista Dinámica Externa para Firewall; WAF→EDL para WAF Akamai) y se genera un ticket en iTop. Para los eventos no maliciosos, se realiza un análisis asistido por IA (Gemini) y, si el resultado es sospechoso, benigno o neutral, se envía un reporte por correo.

f. Registro

Trazabilidad de cada etapa, incluyendo los tiempos de ingesta, enriquecimiento, decisión y respuesta, en el log de auditoría del orquestador, visible en el sistema web.

La Figura 12 muestra la plantilla de flujo para las reglas de Firewall.

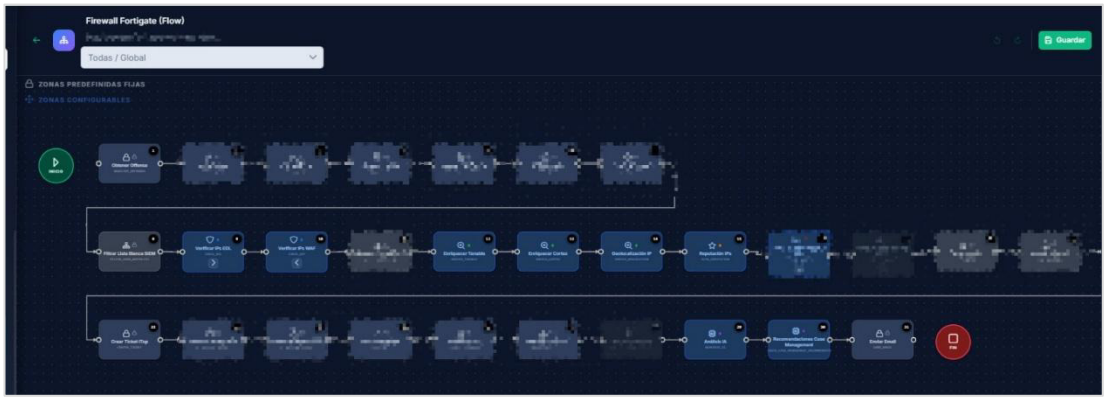


Figura 12 **Plantilla de flujo para las reglas de Firewall.** Fuente. Elaboración propia, a partir del orquestador MCIA.

La Figura 13 describe la plantilla de flujo para las reglas de WAF Akamai.

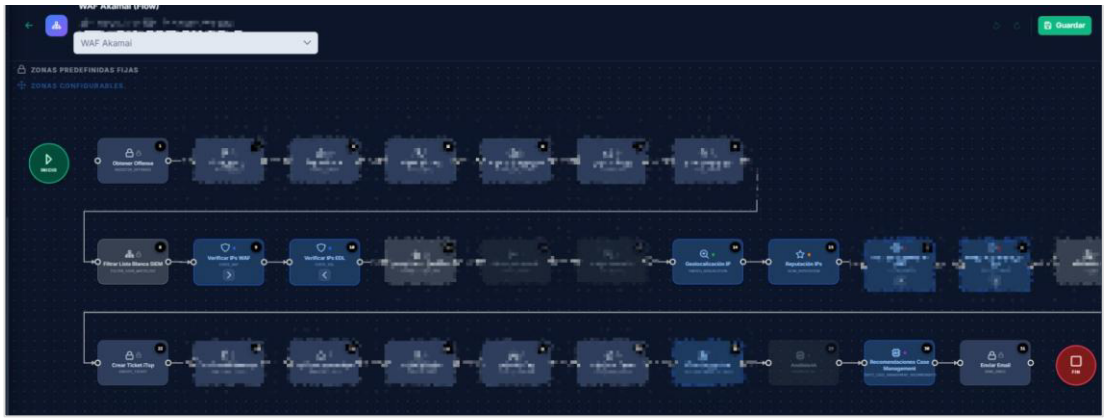


Figura 13 **Plantilla de flujo para las reglas de WAF Akamai.** Fuente. Elaboración propia, a partir del orquestador MCIA.

C. Diseño de no duplicación entre fuentes

Mecanismo para evitar un doble bloqueo o ticket cuando una misma IP es detectada simultáneamente en diferentes fuentes.

1. El orquestador verifica, antes de ejecutar el bloqueo o generar el ticket, si la misma IP (Firewall) o la misma IP y *request site* (WAF Akamai) ya fueron gestionadas en una ejecución previa. De esta manera, se evita un doble bloqueo o ticket cuando una misma amenaza es detectada por más de una fuente, como se evidencia en la Figura 14.

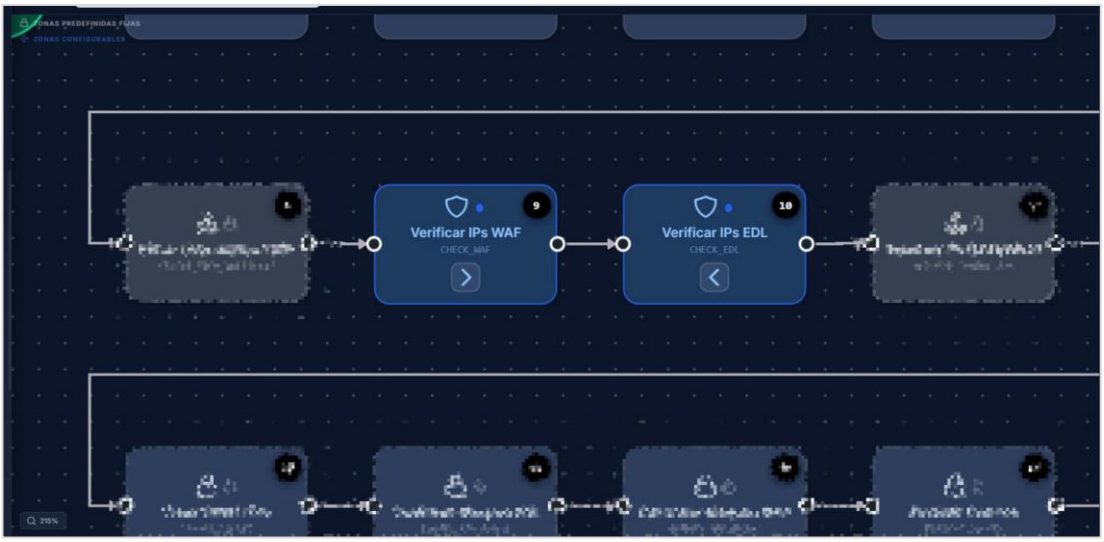


Figura 14 **Mecanismo de no duplicación de bloqueos entre fuentes.** Fuente. Elaboración propia, a partir del orquestador MCIA.

3.5.2.2 Fase 4 - Provisionamiento de infraestructura

A. Aprovisionamiento de la VM sobre la infraestructura del CyberSOC (no del cliente), *hardening* del sistema operativo, despliegue de contenedores (Docker/Nginx) y bases de datos (PostgreSQL, Redis)

Para el despliegue de los servicios sobre la VM aprovisionada en la infraestructura del CyberSOC, se optó por una arquitectura basada en contenedores (Docker), proxy reverso (Nginx) y bases de datos especializadas (PostgreSQL y Redis), por las siguientes razones:

1. Docker (contenedores)

Los contenedores permiten aislar cada componente (aplicación, base de datos, caché y proxy) en entornos independientes, evitando conflictos de dependencias y facilitando el despliegue y la administración de servicios. Además, facilitan el escalamiento y la recuperación rápida ante fallos, y mejoran la seguridad al limitar el alcance de cada proceso, aspecto clave en un entorno de CyberSOC.

2. Nginx (proxy reverso)

Funciona como punto de entrada único hacia los servicios, encargándose del cifrado TLS/SSL, el balanceo de carga y la limitación de peticiones (*rate limiting*) ante posibles ataques. Al ser el único componente expuesto públicamente, permite reducir la superficie de ataque de la VM y oculta la topología interna de la infraestructura.

3. PostgreSQL (base de datos relacional)

Se eligió por ser un motor de base datos por su robustez y de código abierto y por las garantías ACID que ofrece para asegurar la integridad y confiabilidad de los datos críticos, como usuarios, alertas e incidentes. Además, brinda un soporte avanzado de seguridad (cifrado, roles y auditoría), lo cual permite mantener la trazabilidad de las operaciones.

4. Redis (caché / almacenamiento en memoria)

Se utilizó como capa de caché en memoria para acelerar consultas frecuentes, gestionar sesiones y manejar notificaciones en tiempo real. Esto permitió reducir la carga sobre PostgreSQL y mejora los tiempos de respuesta.

5. Dimensionamiento de recursos

Para soportar estos servicios de forma simultánea, se dimensionaron los recursos de la VM (RAM, CPU y disco) de acuerdo con la carga esperada, garantizando estabilidad y margen de crecimiento. En la Figura 15 se muestra la configuración de recursos asignados a la máquina virtual.

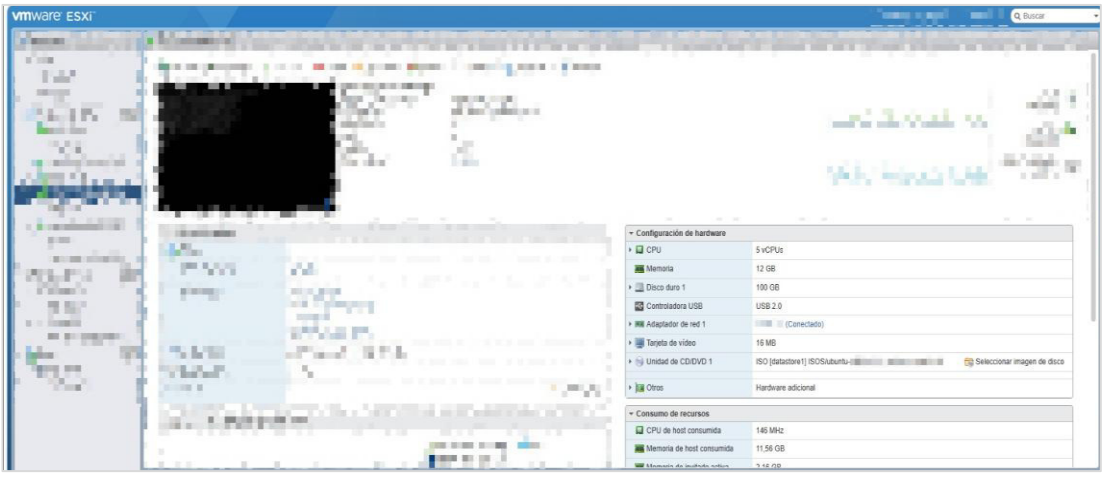


Figura 15 **Recursos asignados a la máquina virtual.** Fuente. Elaboración propia, a partir de los datos del VMware ESXi.

B. Habilitación de la VPN *site-to-site* entre el firewall del cliente y el de la empresa, y validación de la conectividad hacia la API de IBM QRadar

Se habilitó la conexión VPN *site-to-site* entre el firewall del cliente y el de la empresa. La evidencia de la conectividad VPN se muestra en la Figura 16.

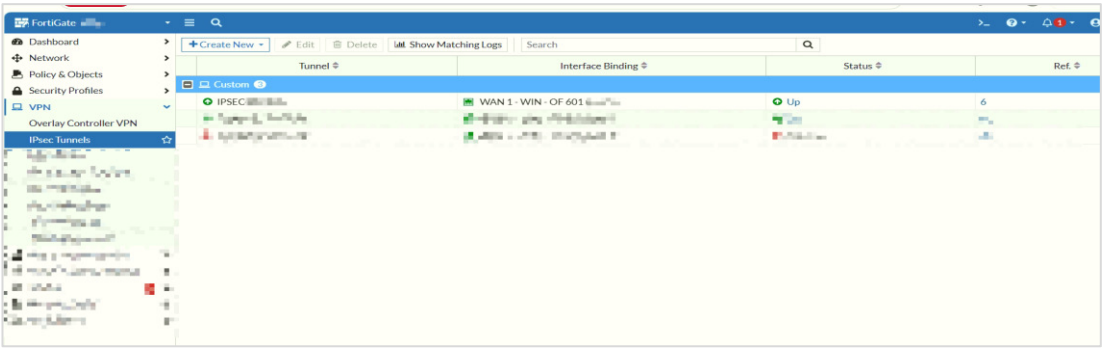


Figura 16 **Conectividad VPN site-to-site entre el firewall del cliente y el de la empresa.** Fuente. Elaboración propia a partir del firewall perimetral.

3.5.2.3 Fase 5 - Desarrollo del core – cybersoc-api

A. Construcción de los módulos de ingesta y cierre de ofensas de QRadar, gestión de contexto y caché, lista blanca y resolución de IP

El módulo de ingesta obtiene las ofensas desde QRadar, valida su estado y las cierra en el SIEM para evitar la acumulación de eventos y mantener la visibilidad sobre su ciclo de vida. A continuación, recupera los

eventos asociados y registra los *logs sources* correspondientes. Estos datos se almacenan temporalmente en Redis antes de consolidarse en un objeto de contexto único que sirve de insumo para el resto del flujo. Sobre ese contexto, el orquestador filtra las IPs contra la lista blanca del SIEM y verifica si ya fueron gestionadas previamente en WAF Akamai o en la Lista Dinámica Externa, evitando una doble acción sobre una misma IP.

La resolución de IP se realiza de forma modular. Cada ofensa de QRadar está asociada a una regla identificada por su categoría CUD-XXX (por ejemplo, CUD-154), y el módulo consulta una configuración administrable por regla que define, para cada CUD-XXX, si el campo a analizar es la IP origen o la IP destino. Esta configuración materializa la matriz de decisión definida en la Fase 2, sin necesidad de codificar una lógica particular para cada una de las 23 reglas de firewall (ver Anexo B).

B. Desarrollo de la lógica de plantillas de flujo de WAF Akamai, incluyendo el análisis de IPs y del *request site*.

Se desarrolló la lógica de la plantilla de flujo de WAF Akamai, a partir de la plantilla de Firewall descrita anteriormente. En este caso se reemplazó el paso de resolución de IP origen/destino por el análisis del *request site*. Debido a que en WAF Akamai el destino es fijo (el activo protegido), la plantilla analiza la IP origen externa junto con el dominio o página al que intentó conectarse, construyendo el historial correspondiente para el enriquecimiento y el cálculo de *risk score*.

3.5.2.4 Fase 6 - Desarrollo de integraciones

A. Construcción de conectores hacia fuentes de inteligencia de amenazas, Tenable y Cortex XDR (enriquecimiento), la ticketera iTop y el motor de IA (Gemini) para la rama de análisis asistido.

Cada conector se desarrolló como un módulo independiente dentro de la capa de microservicios del motor MCIA, encargado de consumir las API correspondientes a las fuentes de inteligencia de amenazas (VirusTotal, AbuseIPDB, Criminal IP y OTX), así como a Tenable y Cortex XDR para el

enriquecimiento de vulnerabilidades, como se evidencia en las Figuras 17, 18 y 19.

La integración con iTop se implementó mediante su API REST para la creación y actualización de tickets, como se muestra en la Figura 20. Por su parte, la integración con Gemini se construyó mediante su API, utilizando *prompt engineering* sobre el contexto consolidado del evento para obtener una recomendación en lenguaje natural como apoyo al análisis, asistido por IA, como se muestra en la Figura 21. Cabe precisar que el consumo de este servicio se realiza mediante una API provista por el tenant propio, con licenciamiento empresarial (enterprise), y que al motor de IA solo se envía información no confidencial del evento, cuyo alcance es de conocimiento del cliente. Con ello se buscó resguardar la confidencialidad de la información procesada durante la implementación.

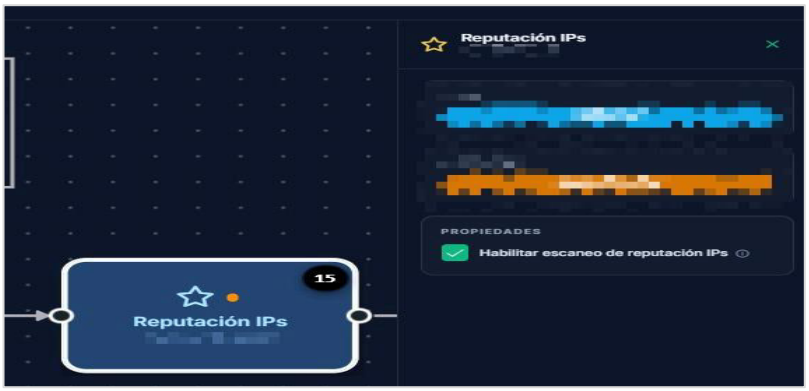


Figura 17 **Captura parcial del conector de Inteligencia de amenazas**.
Fuente. Elaboración propia a partir del orquestador MCIA.



Figura 18 **Captura parcial del conector de Tenable**.
Fuente. Elaboración propia a partir del orquestador MCIA.

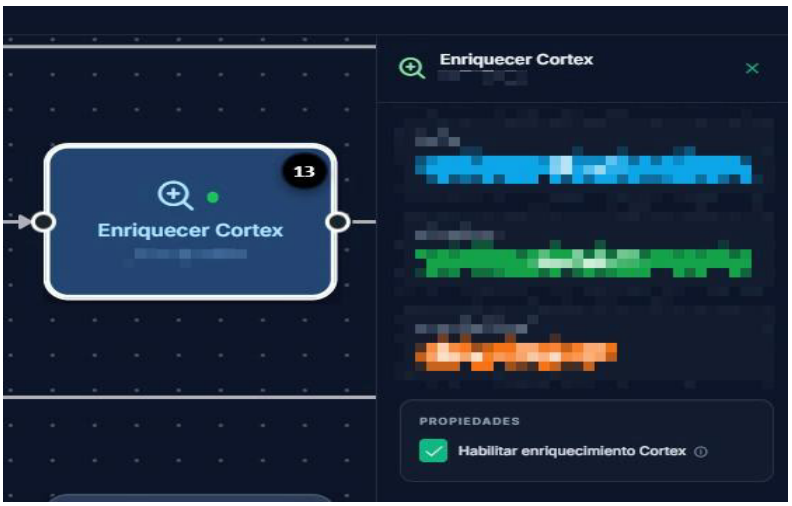


Figura 19 **Captura parcial del conector de Cortex.**
Fuente. Elaboración propia a partir del orquestador MCIA.

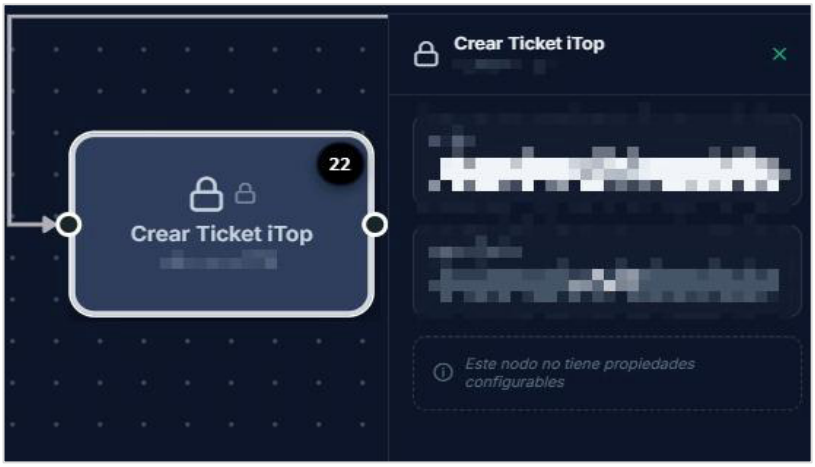


Figura 20 **Captura parcial del conector de iTop.**
Fuente. Elaboración propia a partir del orquestador MCIA.

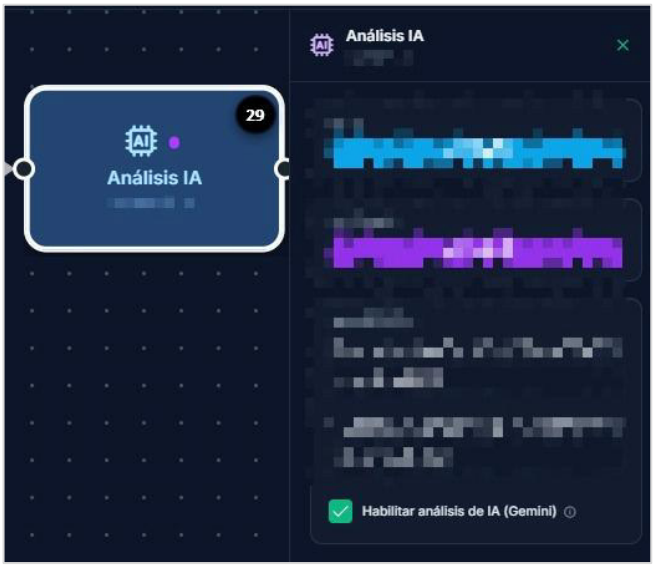


Figura 21 **Captura parcial del conector de Gemini**.
Fuente. Elaboración propia a partir del orquestador MCIA.

B. Integración con la Lista Dinámica Externa y con WAF Akamai, como canal de respuesta.

La integración con la Lista Dinámica Externa se desarrolló mediante una cuenta de servicio provista por el cliente, con acceso a la ruta donde reside la lista dinámica externa, para insertar direcciones IP de forma centralizada en los 21 firewalls. Por su parte, la integración con WAF Akamai se construyó sobre su API de gestión de listas de control de acceso, permitiendo bloquear la IP de origen a nivel del servicio web.

Ambos conectores se integraron como nodos de bloqueo dentro del mismo flujo del motor de decisión. Cada uno cuenta con una validación previa mediante una propiedad configurable a nivel de plantilla que permite habilitar o deshabilitar el canal correspondiente, como se muestra en la Figura 22 para EDL y en la Figura 23 para WAF Akamai.

Esto permite activar selectivamente cada canal según el tipo de plantilla: en la plantilla de Firewall solo se habilita el bloqueo hacia la Lista Dinámica Externa, mientras que en la plantilla de WAF Akamai se habilitan ambos canales (EDL y WAF), dado que el activo protegido responde a las dos superficies. En ambos casos, la acción de bloqueo puede revertirse de forma independiente sin afectar el resto del flujo.

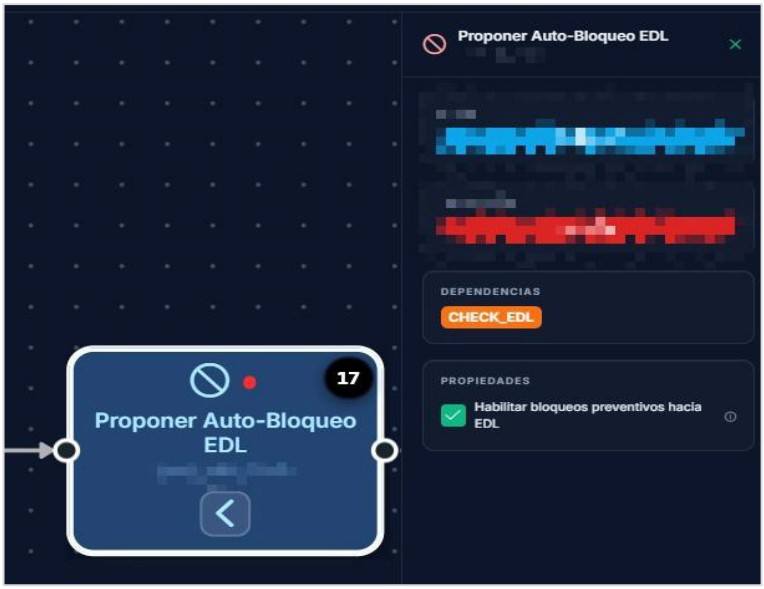


Figura 22 **Captura parcial del bloqueo en lista dinámica externa.**
Fuente. Elaboración propia a partir del orquestador MCIA.



Figura 23 *Captura parcial del bloqueo en WAF Akamai.*
Fuente. Elaboración propia a partir del orquestador MCIA.

C. Configuración de la recepción de eventos de WAF Akamai y de los firewalls desde QRadar y las acciones de respuesta sobre el WAF y la Lista Dinámica Externa, respetando la política de auto-respuesta pactada.

La recepción de eventos desde QRadar se configuró mediante su API REST, consultando en tiempo real las ofensas abiertas asociadas a las reglas priorizadas, según se muestra en la Figura 24. De esta manera, las ofensas de WAF ingresan al orquestador por el mismo canal que las de firewall.

Las acciones de respuesta sobre el WAF y la Lista Dinámica Externa se establecieron para ejecutarse únicamente dentro de los límites definidos en la política de auto-respuesta acordada con el cliente (Tabla 6). El bloqueo automático se restringió a los casos que cumplen el umbral de riesgo establecido, mientras que los demás casos derivan a la rama de análisis asistido, cuyo reporte se remite al cliente para su revisión.



Figura 24 **Captura parcial del inicio de recepción de las ofensas para WAF Akamai y los firewalls.** Fuente. Elaboración propia a partir del orquestador MCIA.

D. Desarrollo del microservicio de correo, independiente del núcleo, para el envío de reportes y alertas.

El microservicio de correo (*email-api*) se desarrolló de forma independiente del núcleo *cybersoc-api*, siguiendo el mismo criterio aplicado a los demás componentes de la arquitectura (Figura 11). Este microservicio recibe la plantilla y el contenido del reporte generado por el orquestador y gestiona su envío a los destinatarios configurados para cada tipo de alerta. Dentro de la plantilla de flujo, este envío se representa como un nodo independiente (Figura 25). Al llegar la ejecución al nodo "Enviar Email", el orquestador invoca el microservicio de correo y la plantilla de flujo finaliza.

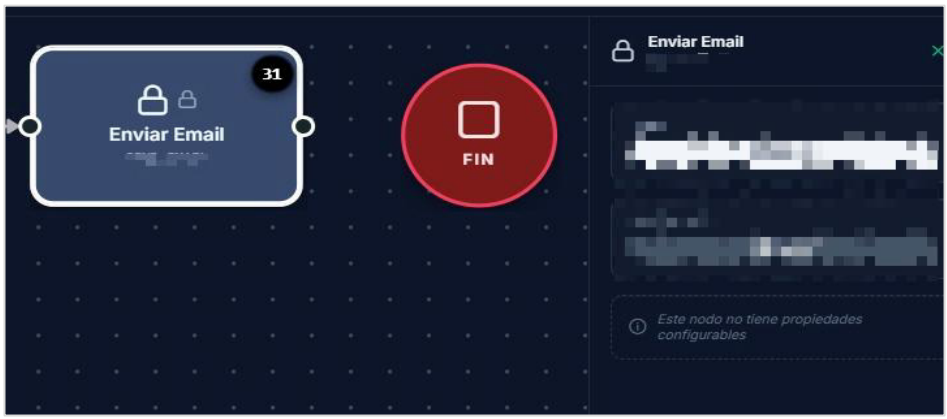


Figura 25 **Captura parcial de envío de correo dentro del flujo del playbook.** Fuente. Elaboración propia a partir del orquestador MCIA.

3.5.2.5 Fase 7 - Motor de decisión y respuesta

A. Implementación del cálculo de *risk score* y del umbral de decisión (≥6 = malicioso, <6 = no malicioso).

El cálculo del *risk score* se implementó como un módulo del motor MCIA que combina los cuatro factores definidos en la Fase 3 (gravedad global, certeza reputacional, direccionalidad del flujo y mapeo de campañas activas) en una escala de 1 a 10. En la Figura 26 se muestran los niveles de reputación. Cada factor corresponde a una fuente de inteligencia con un peso diferenciado según su cobertura y confiabilidad:

1. VirusTotal (gravedad global - máx. 4 pts)

Consenso de 94 motores antivirus. Otorga 0 pts si no hay detecciones; 1 pt si al menos un *engine* la marca como sospechosa sin confirmación maliciosa; 2 pts con 1–3 *engines* maliciosos; 3 pts con 4–10 *engines* maliciosos; y 4 pts con más de 10 *engines* maliciosos.

2. AbuseIPDB (certeza reputacional - máx. 3 pts)

Reportes comunitarios de equipos SOC y CERTs globales, ponderados mediante el *abuseConfidenceScore* (0–100 %). Otorga 0 pts con score de 0 %; 1 pt entre 1–25 %; 2 pts entre 26–60 %; y 3 pts superando el 60 %. Se aplica una regla de bonus que eleva automáticamente al máximo de 3 pts cuando la IP acumula más de 100 reportes provenientes de más de 20 fuentes distintas, permitiendo identificar IP con actividad masiva activa cuyo porcentaje de *confidence* puede resultar moderado.

3. OTX AlienVault (campañas activas - máx. 2 pts)

Considera la presencia en campañas de amenazas documentadas globalmente. Otorga 0 pts sin *pulses* registrados; 1 pt con 1–10 pulses; y 2 pts con más de 10 pulses. Se aplica una excepción de *bypass* para rangos de infraestructura global reconocida (AWS, Google, Azure, entre otros), estableciendo el *score* en 0 pts para evitar falsos positivos por su alta visibilidad pública.

4. CriminalIP (dirección de flujo - máx. 1 pt)

Considera el perfil de riesgo del tráfico entrante (*scoreInbound*). Otorga 0 pts con nivel SAFE o LOW, y 1 pt con nivel MEDIUM, HIGH o CRITICAL. Actúa como señal de contexto complementaria y recibe el

menor peso del modelo, debido a que puede subestimar IP con actividad ofensiva saliente intensa.

Sobre ese puntaje se implementó el umbral de decisión pactado con el cliente: los eventos con *risk score* igual o mayor a 6 se clasifican como maliciosos y activan la rama de auto-respuesta, mientras que los eventos con un puntaje menor a 6 no activan el bloqueo automático y pasan a la rama de análisis asistido. El valor del umbral se definió en consenso con el cliente, optando por un nivel intermedio-alto para reducir la probabilidad de bloquear automáticamente direcciones IP legítimas (falsos positivos). Para estos casos, el análisis asistido permite realizar una validación adicional antes de determinar la acción correspondiente. En la Figura 27 se muestra un ejemplo de la evaluación del *risk score* de una IP maliciosa.

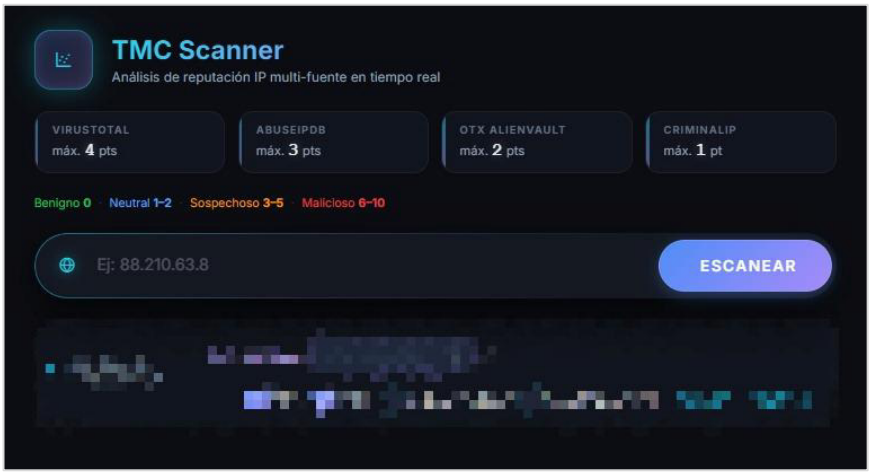


Figura 26 **Captura parcial de los niveles de reputación**
Fuente. Elaboración propia, a partir del orquestador MCIA.

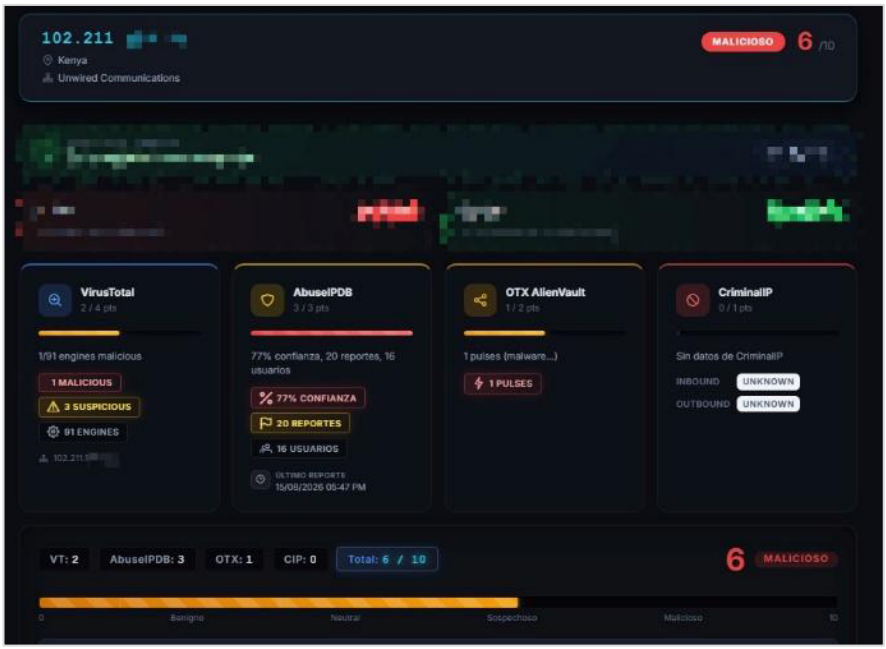


Figura 27 **Captura parcial del risk score de una IP**. Fuente. Elaboración propia, a partir del orquestador MCIA.

B. Rama maliciosa: autobloqueo en la Lista Dinámica Externa y en WAF Akamai, y generación automática de ticket.

Para la rama maliciosa, se implementó el bloqueo en la Lista Dinámica Externa o en WAF Akamai, según la fuente que originó el evento, seguido de la generación automática de un ticket en iTop con el detalle del evento. De esta manera, el analista cuenta con la trazabilidad de la acción ejecutada por el orquestador sin intervención manual, como se muestra en la Figura 28.

La ejecución del bloqueo incluye un paso de comprobación. Una vez enviada la dirección IP a la Lista Dinámica Externa o al WAF Akamai, según la fuente del evento, el flujo vuelve a consultar el destino para confirmar que el bloqueo quedó registrado; si no lo confirma, lo envía nuevamente y repite la consulta hasta verificarlo. De esta manera, el estado que reporta el orquestador refleja lo que ocurrió realmente en la infraestructura y no solo el envío de la instrucción. Este paso se ejecuta después del bloqueo y es distinto del paso "Verificar IPs EDL" descrito en el apartado 3.5.2.1, que ocurre antes y solo consulta si la IP ya fue tratada, sin ejecutar ninguna acción. Ambos se observan en la Figura 39.

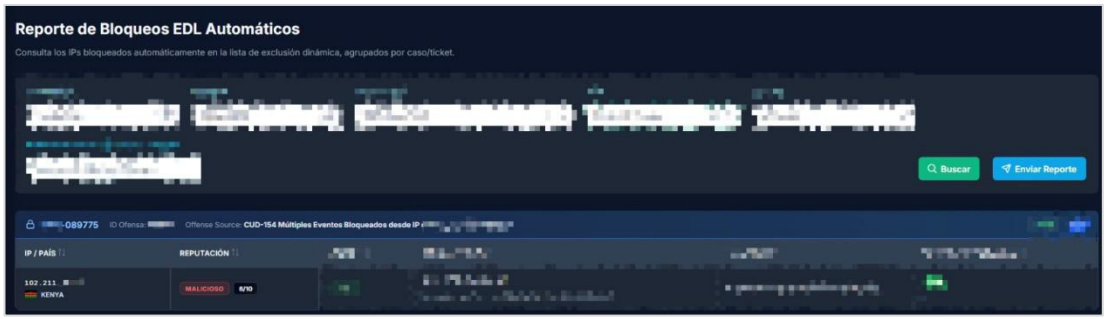


Figura 28 **Reporte de bloqueos de IP en la lista dinámica externa**. Fuente. Elaboración propia, a partir del orquestador MCIA.

C. Rama no maliciosa: análisis asistido por IA con recomendaciones y, solo si el resultado es sospechoso, benigno o neutral, envío de un reporte por correo.

Para la rama no maliciosa, se implementó el envío del contexto del evento a Gemini para obtener un análisis asistido con recomendaciones. Cuando el resultado corresponde a un caso sospechoso, benigno o neutral, se genera y envía por correo un reporte al cliente con el contexto del evento y la recomendación, como se muestra en la Figura 29.

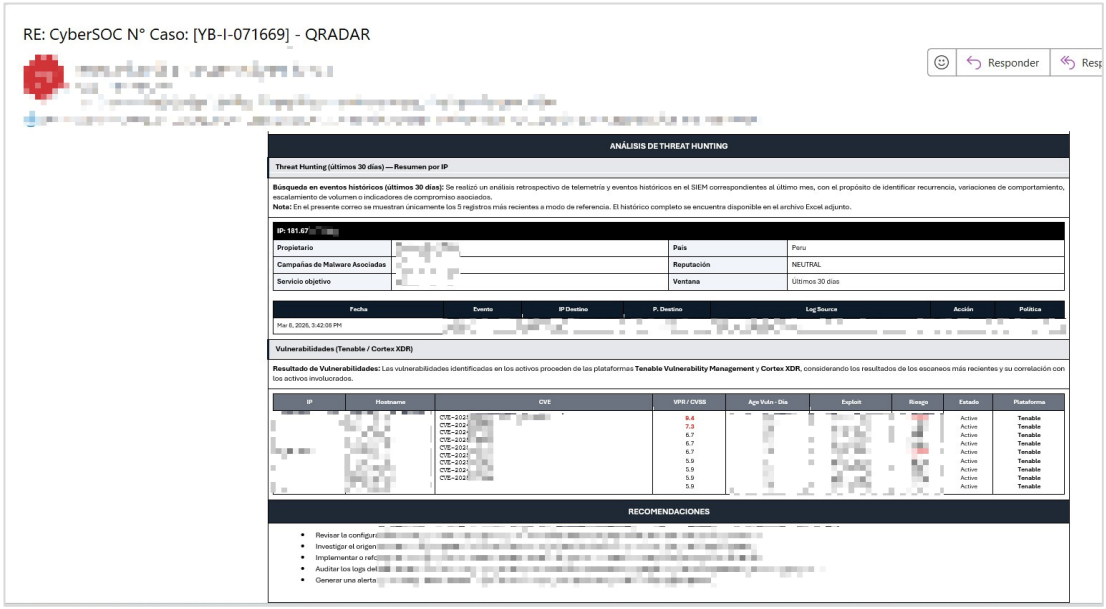


Figura 29 **Envío del reporte automatizado para la rama no maliciosa**. Fuente. Elaboración propia, a partir del buzón del CyberSOC.

D. Botón de apagado para desactivar el autobloqueo.

En las Figuras 22 y 23 se evidencia la deshabilitación de esta función.

E. No duplicación entre fuentes y detección de ofensa recurrente por IP y *request site*.

Se implementó también la lógica de no duplicación entre fuentes descrita en la Fase 3 (Figura 14). También se agregó la detección de ofensas recurrentes por IP y por IP más *request site*, que identifica cuándo una misma IP vuelve a generar eventos después de haber sido reportada, permitiendo escalar su prioridad de tratamiento, como se muestra en la Figura 30.



Figura 30 **Envío del reporte automatizado de ofensa recurrente.** Fuente. Elaboración propia, a partir del buzón del CyberSOC.

3.5.2.6 Fase 8 - *Playbooks* por regla

A. Diseño e implementación de los flujos de trabajo para las 48 reglas priorizadas, cada una parametrizada según su plantilla de flujo.

El diseño e implementación de los flujos de trabajo para las 48 reglas priorizadas se realizó mediante la parametrización de cada regla según la plantilla correspondiente a su fuente. Las 23 reglas de firewall se configuraron sobre la plantilla de firewall FortiGate, que se muestra en la Figura 31, y las 25 reglas de WAF Akamai sobre la plantilla correspondiente, mostrada en la Figura 32. La parametrización se realizó mediante la configuración por regla definida en la Fase 5, utilizando el identificador CUD-XXX para firewall y su equivalente para WAF Akamai, el cual determina para cada regla el campo que debe ser analizado.



Figura 31 **Flujo completo de la plantilla para Firewalls.** Fuente. Elaboración propia, a partir del orquestador MCIA.



Figura 32 **Flujo completo de la plantilla para WAF Akamai.** Fuente. Elaboración propia, a partir del orquestador MCIA.

3.5.2.7 Fase 9 - Sistema web y *dashboards*

A. Desarrollo de la interfaz de indicadores, trazabilidad de acciones del orquestador y KPIs operativos segmentados por fuente (Firewall y WAF Akamai).

Como evidencia de esta fase, la Figura 33 muestra el *dashboard* de MTTD para las plataformas WAF Akamai y Firewall, y la Figura 34 el correspondiente al MTTR, permitiendo al equipo de Monitoreo visualizar los tiempos de detección y respuesta de cada fuente. Adicionalmente, se incorporó una bitácora de los tickets generados desde el propio sistema web, mostrada en la Figura 35, que permite centralizar el seguimiento de los casos atendidos por el orquestador. Finalmente, se implementó un *dashboard* de monitoreo en tiempo real del proceso del orquestador, mostrado en la Figura 36, que permite visualizar el estado de las acciones ejecutadas a medida que ocurren.



Figura 33 **Dashboard de tiempo promedio de detección.** Fuente. Elaboración propia, a partir del orquestador MCIA.



Figura 34 **Dashboard de tiempo promedio de respuesta.** Fuente. Elaboración propia, a partir del orquestador MCIA.

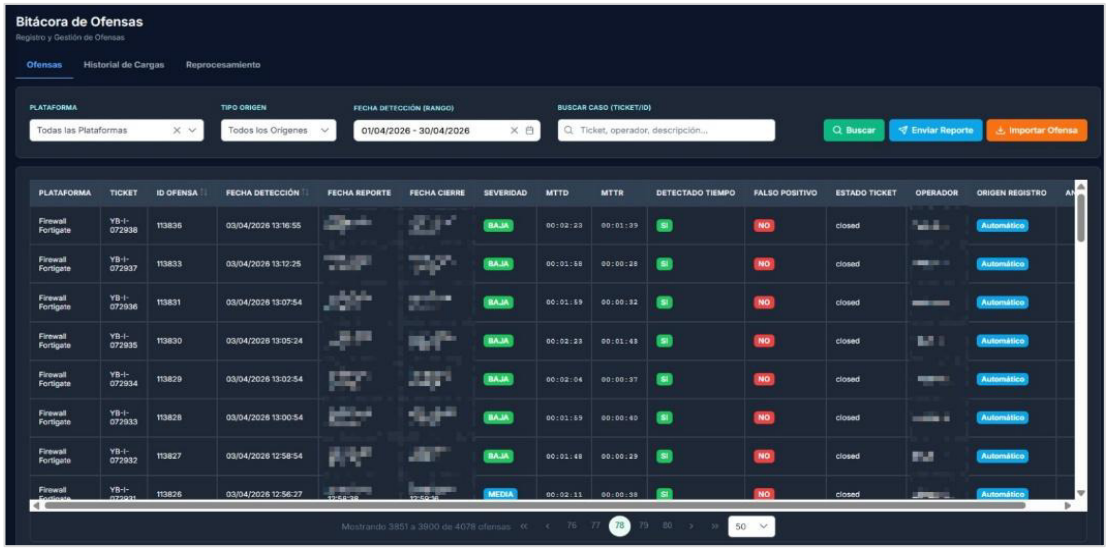


Figura 35 **Bitácora de ofensas.** Fuente. Elaboración propia, a partir del orquestador MCIA.

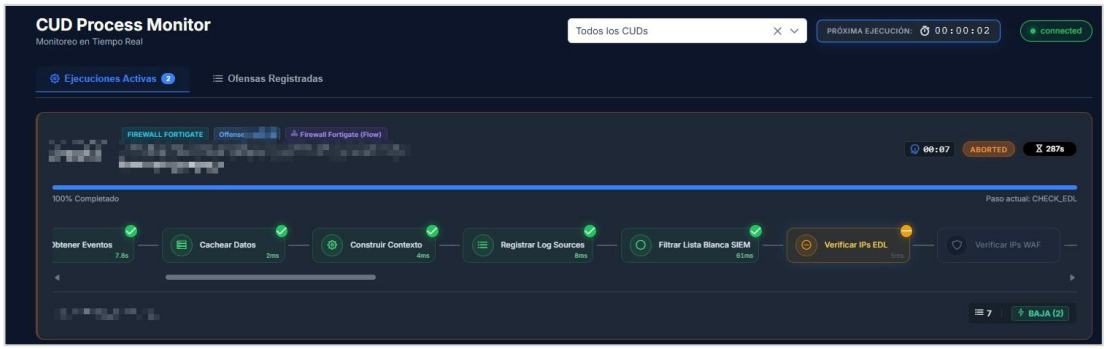


Figura 36 **Dashboard de monitoreo en tiempo real del proceso del orquestador.** Fuente. Elaboración propia, a partir del orquestador MCIA.

3.5.3 Etapa 3: Piloto controlado y pase a producción (Fases 10 a 12)

3.5.3.1 Fase 10 - Pruebas y QA

A. Pruebas unitarias, de integración, de volumen de eventos y de reversión de bloqueos, incluyendo falsos positivos y no duplicación para WAF Akamai y Firewall.

Como evidencia de esta validación, se toma de manera representativa la fuente de firewall. La Figura 37 muestra el listado de ofensas registradas en el orquestador, donde se identifica la regla CUD-XXX asociada a cada ofensa. En este caso, corresponde a la regla CUD-154, asociada a la fuente firewall, con estado PENDING y a la espera de iniciar su procesamiento. Durante un periodo de un minuto se acumulan los eventos asociados, evitando concentrar un volumen excesivo de información y facilitando su análisis.

A partir de este identificador, el orquestador inicia el flujo y verifica si la IP ya fue objeto de una acción previa. La Figura 38 muestra la misma ofensa CUD-154 durante su ejecución. Luego de completar el paso "Filtrar Lista Blanca SIEM", el flujo se detiene en "Verificar IPs EDL" y finaliza con estado ABORTED, debido a que la IP ya se encontraba registrada en la Lista Dinámica Externa (EDL) como resultado de un tratamiento previo. Esta verificación evita que se realice un bloqueo duplicado o se genere un ticket adicional sobre una IP que ya fue gestionada, dando soporte a la prueba de no duplicación entre fuentes.

En la Figura 39 se muestra un flujo ejecutado satisfactoriamente sobre la ofensa #192815 correspondiente a la regla CUD-154, con 224 eventos asociados. La captura permite seguir el recorrido del orquestador: luego de la clasificación, el flujo crea el ticket en iTop y envía la dirección IP a la Lista Dinámica Externa mediante el paso "Confirmar Bloqueo EDL"; a continuación, el paso "Validación Final" vuelve a consultar la lista para confirmar que el bloqueo quedó registrado, y el flujo cierra con "Auto-Cerrar Ticket". Finalmente, la Figura 40 muestra la IP bloqueada correctamente, con un *risk score* de 7, cumpliendo con el umbral establecido para la ejecución del bloqueo automático.



Figura 37 **Registro del CUD-154 gatillado desde el SIEM QRadar**. **Fuente**. Elaboración propia, a partir del orquestador MCIA.



Figura 38 **Ejecución del flujo del CUD-154.** Fuente. Elaboración propia, a partir del orquestador MCIA.



Figura 39 **Ejecución satisfactoria del flujo con bloqueo de IP.** Fuente. Elaboración propia, a partir del orquestador MCIA.



Figura 40 **Registro de bloqueo de una IP maliciosa.** Fuente. Elaboración propia, a partir del orquestador MCIA.

3.5.3.2 Fase 11 - Piloto controlado

A. Despliegue en modo observación: ejecución de *playbooks* de ambas fuentes sin autobloqueo activo, para calibrar *risk score* y lista blanca antes de intervenir la infraestructura del cliente.

Como evidencia del despliegue en modo observación, la Figura 41 muestra el caso 069279, generado a partir de 500 eventos de bloqueo que activaron la regla CUD-154 (Detección de Múltiples Eventos de Bloqueo desde una misma IP origen). En las columnas EDL y WAF del reporte se observa el valor "NO" para las IP involucradas, lo que indica que el orquestador identificó y clasificó el caso sin ejecutar acciones de bloqueo sobre la infraestructura.

La Figura 42 complementa esta evidencia con el análisis de Threat Hunting realizado sobre la IP 91.231.XX.XX, en el que se confirmó una reputación “MALICIOSO”, validando que el criterio de riesgo aplicado durante la observación correspondía a una amenaza real. Estas evidencias corresponden al piloto ejecutado en modo observación, con el autobloqueo deliberadamente desactivado, y no forman parte del periodo de evaluación en producción reportado en el apartado 3.6.5.

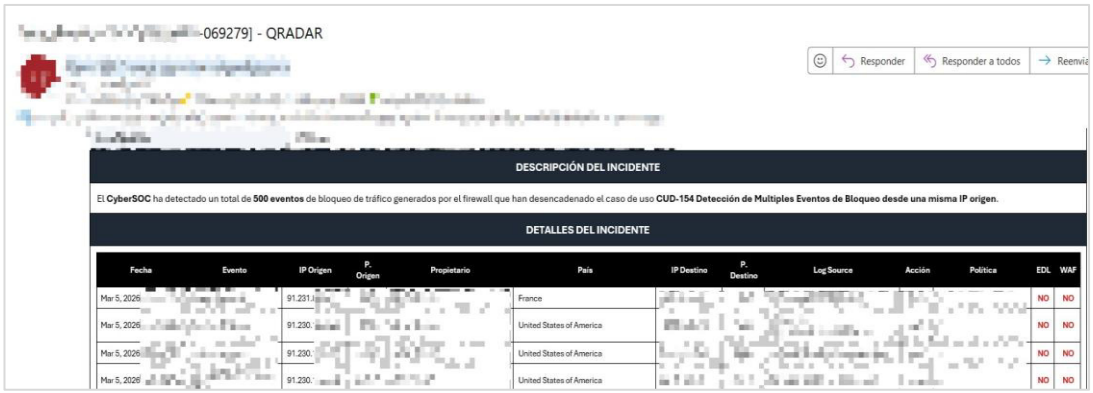


Figura 41 **Reporte del CUD-154 sin ejecución de bloqueo.** Fuente. Elaboración propia, a partir del buzón del CyberSOC.



Figura 42 **Reporte de análisis del CUD-154 sin ejecución de bloqueo.** Fuente. Elaboración propia, a partir del buzón del CyberSOC.

B. Ajuste de umbrales y mecanismo de reversión: afinamiento del umbral con retroalimentación del analista y habilitación de *rollback*.

Con la calibración del umbral realizada a partir de los casos observados durante el piloto, la Figura 43 muestra que, ante una reincidencia posterior de la misma IP (91.231.XX.XX), registrada en el ticket 069324, el orquestador ejecutó el bloqueo automático en la Lista Dinámica Externa, quedando reflejado con estado "OK" en el reporte de bloqueos automáticos. Esto se realizó luego de activar el bloqueo para IPs maliciosas.

El mecanismo de reversión se sustenta en el acceso directo del operador de Monitoreo a la ruta de red donde se encuentra el archivo de la Lista Dinámica Externa (threatfeeds_IP_QRADAR.txt), consumido de forma centralizada por los 21 firewalls FortiGate. La Figura 44 muestra dicho archivo, en el que cada IP bloqueada queda registrada junto con el número de caso de

CyberSOC que la originó, como se observa para el caso 069324 y la IP 91.231.XX.XX.

Al retirar manualmente la línea correspondiente, el operador puede revertir el bloqueo de forma centralizada sobre los 21 firewalls, sin necesidad de intervenir cada uno de manera individual. El orquestador continúa operando de forma continua (24/7), pero no cuenta con un mecanismo de reversión automática.

Por criterio de seguridad operativa, la reversión no se ejecutó sobre la IP mostrada en la evidencia, debido a que corresponde a una IP con reputación maliciosa confirmada. La validación se limitó a comprobar el acceso a la ruta y el formato de registro utilizado por el orquestador.

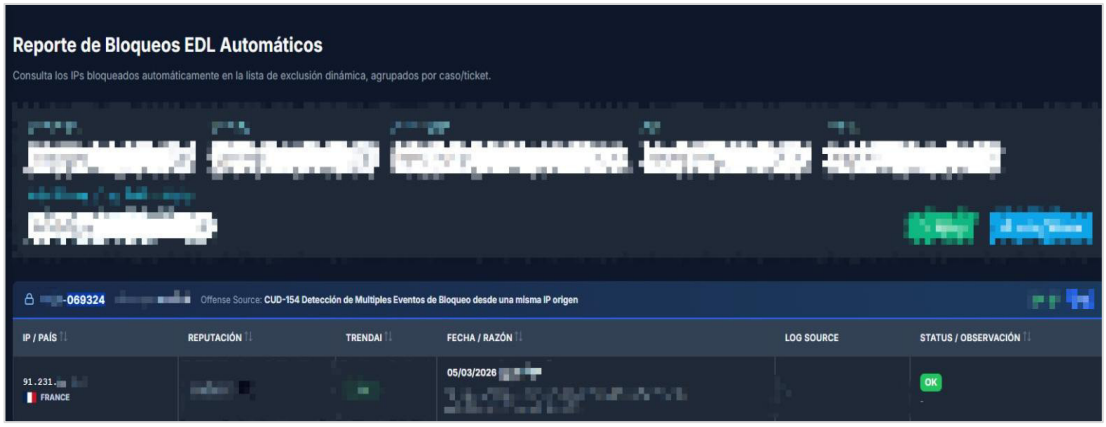


Figura 43 **Reporte de bloqueo de la IP 91.231.XX.XX.** Fuente. Elaboración propia, a partir del orquestador MCIA.

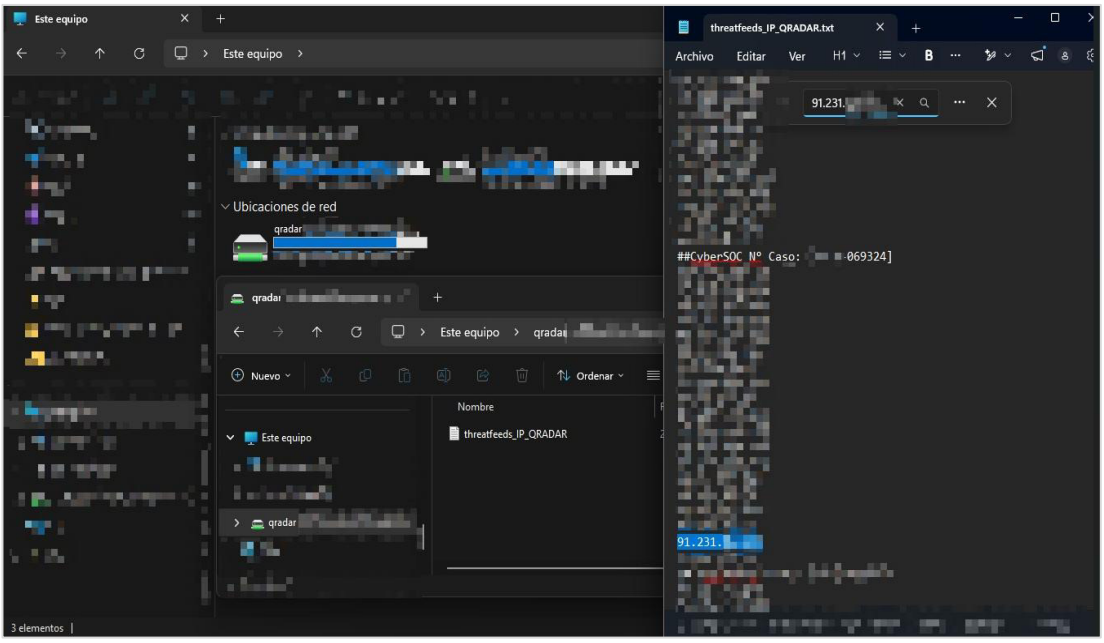


Figura 44 **Acceso al EDL para desbloqueo de IPs.** Fuente. Elaboración propia, a partir del orquestador MCIA.

C. Aprobación del cliente: validación conjunta de los resultados del piloto como condición previa para activar el autobloqueo en producción para todos los casos.

La aprobación del cliente se obtuvo de forma verbal durante la reunión de revisión de resultados sostenida por Microsoft Teams, en la que se presentaron los resultados y el funcionamiento del piloto como sustento para autorizar el pase a producción. La Figura 45 muestra la convocatoria de dicha reunión como evidencia de su realización.



Figura 45 **Agenda de reunión por correo para aprobación de autobloqueo y de pase a producción. Fuente. Elaboración propia, a partir de datos de correo corporativo.**

3.5.3.3 Fase 12 - Despliegue a producción

A. Aprobación del autobloqueo, activación gradual del bloqueo de la lista dinámica externa y WAF, validación post-despliegue y seguimiento continuo por el equipo de Monitoreo.

Con la aprobación del cliente formalizada durante la reunión mostrada en la Figura 45, la activación se realiza de forma gradual, habilitando primero las reglas de mayor volumen y menor complejidad de análisis, y ampliando progresivamente la cobertura hasta cubrir las 48 reglas priorizadas. Cada etapa de activación se acompaña de una validación post-despliegue sobre los primeros eventos bloqueados de forma automática. El seguimiento continuo de la operación quedó a cargo del equipo de Monitoreo, que utiliza el sistema web de la Fase 9 para verificar el estado de los bloqueos y escalar cualquier caso que requiera intervención manual.

3.5.4 Etapa 4: Cierre de la implementación y transición a operación continua (Fases 13 y 14)

3.5.4.1 Fase 13 - Operación y mejora continua (estado permanente)

A. Monitoreo recurrente de KPIs por fuente, gobernanza de reglas y reportería periódica.

Como evidencia del monitoreo recurrente de los KPI establecido en esta fase, las Figuras 46 y 47 presentan el comportamiento del MTTD y del MTTR registrados en el panel de indicadores del orquestador MCIA (Fase 9), correspondientes al periodo de operación continua iniciado en abril de 2026. Este panel permite al equipo de Monitoreo realizar el seguimiento de ambos indicadores de forma segmentada por fuente (Firewall y WAF Akamai), verificar los tiempos de detección y respuesta alcanzados tras el pase a

producción (Fase 12) y detectar cualquier desviación que requiera un ajuste en las reglas o en el umbral de riesgo del motor de decisión.

Como evidencia de la reportería periódica, las Figuras 48 y 49 muestran los reportes de direcciones IP bloqueadas distribuidos mediante el microservicio de correo (Fase 6) hacia los *stakeholders* identificados en la Tabla 2, correspondientes a la Lista Dinámica Externa (EDL) y al WAF Akamai, respectivamente. Estos reportes consolidan las direcciones IP bloqueadas automáticamente por el orquestador durante el periodo reportado y permiten al equipo de Monitoreo y al cliente mantener visibilidad sobre la operación del autobloqueo sin necesidad de acceder directamente al sistema web.



Figura 46 **KPI de MTTD en el orquestador MCIA.** Fuente. Elaboración propia, a partir del orquestador MCIA.



Figura 47 **KPI de MTTR en el orquestador MCIA.** Fuente. Elaboración propia, a partir del orquestador MCIA.



Figura 48 **Reporte de IPs bloqueadas en el EDL.** Fuente. Elaboración propia, a partir de datos de correo corporativo.

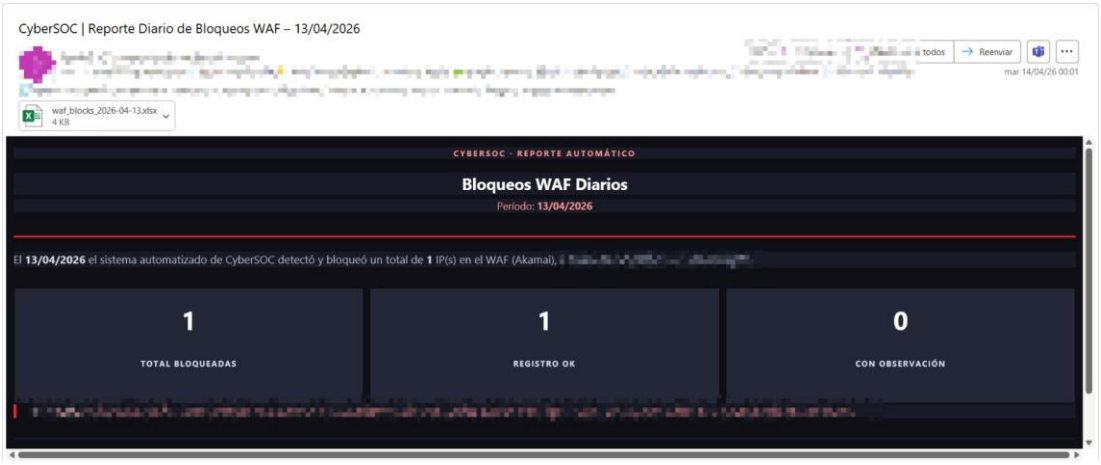


Figura 49 **Reporte de IPs bloqueadas en WAF Akamai.** Fuente. Elaboración propia, a partir de datos de correo corporativo.

B. Carga semanal de vulnerabilidades (Tenable), conforme a la periodicidad del escaneo

El operador actualiza semanalmente la información de vulnerabilidades en Tenable, de acuerdo con la periodicidad del escaneo. El orquestador MCIA integra esta información al flujo de trabajo cada vez que se actualiza. La Figura 50 muestra el registro de la información de vulnerabilidades en Tenable.

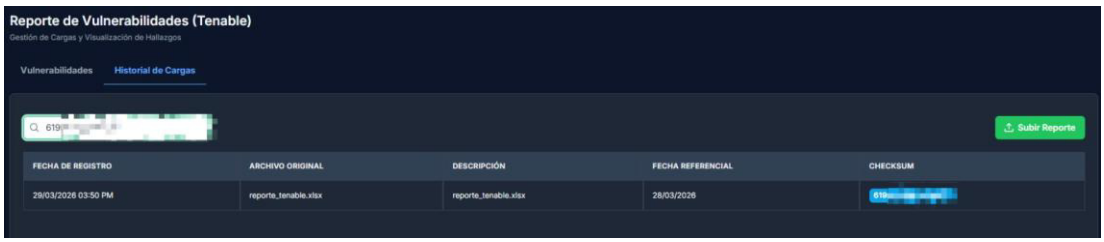


Figura 50 **Registro de la información de vulnerabilidades en Tenable.** *Fuente.* Elaboración propia, a partir del orquestador MCIA.

C. Redefinición del rol del analista CyberSOC: transición de ejecutor manual a supervisor y validador de excepciones

La redefinición del rol del analista CyberSOC se realizó de manera progresiva conforme el orquestador asumió la ejecución de las acciones de bloqueo y registro. El analista de Monitoreo y Operaciones pasó de ejecutar manualmente cada paso del proceso a supervisar la operación del orquestador, validar las excepciones derivadas para revisión humana y atender los casos que, de acuerdo con la política de auto-respuesta, requieren aprobación antes de su ejecución.

Como parte de la mejora continua, en los casos derivados a análisis asistido el CyberSOC contacta de forma proactiva a los responsables del cliente (líder de Firewall y líder de WAF). Cuando la aprobación se obtiene por llamada, el CyberSOC la deja registrada mediante un correo de confirmación antes del cierre del caso desde el orquestador, lo que asegura la trazabilidad en la ticketera iTop.

Esta fase inició en abril de 2026 y continúa de forma indefinida, en paralelo al cierre formal de la implementación (Fase 14).

3.5.4.2 Fase 14 - Cierre de la implementación

- Medición final de indicadores, MTTD y MTTR globales y por fuente, tasa de ejecución confirmada del bloqueo automático y reducción de intervención manual, comparados con la línea base.
- Transferencia de conocimiento y capacitación del equipo de operación, para mantener la plataforma sin dependencia de una persona clave.

- Documentación de resultados y lecciones aprendidas, generando lineamientos que puedan ser replicados en otros clientes del CyberSOC.
- Conformidad del cliente sobre la puesta en operación.

A continuación, se compara el periodo previo a la implementación del orquestador MCIA (01/10/2025 – 30/11/2025) con el periodo posterior a su puesta en operación (del 01/04/2026 al 30/04/2026), correspondiente al primer mes completo de operación en producción. Las cifras de línea base corresponden al proceso manual previo al orquestador.

A. Comparativa de tiempos de detección y resolución (MTTD/MTTR)

La Tabla 8 compara los tiempos promedio de detección (MTTD) y de resolución (MTTR) antes y después de la implementación, por fuente de eventos.

Tabla 8 **Comparativa de MTTD/MTTR antes y después de la implementación**

Métrica	**N.° de incidentes (antes / después)**	**Antes (línea base)**	**Después (con MCIA)**	**Variación (%)**
MTTD promedio – Firewall	118 / 4031	1 h 52 min.	2 min. 47 s.	-97.5%
MTTD promedio – WAF Akamai	184 / 143	1 h 16 min.	1 min. 54 s.	-97.5%
MTTR promedio – Firewall	118 / 4031	33 h 46 min.	1 min. 13 s.	-99.9%
MTTR promedio – WAF Akamai	184 / 143	29 h 1 min.	2 min. 32 s.	-99.9%
MTTD global	302 / 4174	1 h 30 min.	2 min. 45 s.	-97.0%
MTTR global	302 / 4174	30 h 52 min.	1 min. 16 s.	-99.9%

Fuente. Elaboración propia.

Los valores globales de la Tabla 8 corresponden al promedio ponderado por el número de casos de cada fuente. En el periodo posterior, los firewalls concentran el 96.6 % de los casos (4031 de 4174), por lo que el MTTD y el MTTR globales resultan cercanos a los valores de esa fuente. Asimismo, el MTTR posterior considera la totalidad de los casos del periodo: tanto los 4123 que activaron el bloqueo automático como los 51 derivados a la rama de análisis asistido por IA. En estos últimos, el indicador concluye cuando el cliente indica la acción a ejecutar y el cierre, y el operador cierra el caso desde el orquestador MCIA. El detalle de los registros del periodo posterior se presenta en el Anexo C.

En esta comparación, el cliente pasó de ejecutar cada acción a revisar únicamente los casos derivados por el propio orquestador a la rama de análisis asistido, que representaron el 1.2 % de los eventos del periodo evaluado y que llegan al cliente con el enriquecimiento y la recomendación ya generados. De esta manera, el orquestador ejecutó automáticamente las acciones que anteriormente requerían la aprobación del cliente, reduciendo la carga operativa tanto del cliente como de los analistas de Monitoreo y Respuesta del CyberSOC.

B. Volumen de eventos por rama de decisión

La Tabla 9 presenta el volumen de incidentes ingeridos por el orquestador y su distribución entre las dos ramas del motor de decisión definidas en el apartado 3.5.2.5. La totalidad de alertas fue procesada automáticamente en las etapas de ingesta, enriquecimiento y clasificación; la diferencia entre ambas ramas radica en el desenlace: los eventos con *risk score* ≥6 activan el bloqueo automático, mientras que los de puntaje menor a 6 concluyen con un reporte de análisis asistido por IA.

Tabla 9 **Distribución de incidentes procesados por el orquestador MCIA según rama de decisión**

Fuente	**Incidentes totales ingeridos**	**Rama de auto-respuesta (score ≥6)**	**Rama de análisis asistido**	**Tasa de respuesta automatizada**

			por IA (score <6)	
Firewall	4031	3988	43	98.9%
WAF Akamai	143	135	8	94.4%
Total	4174	4123	51	98.8%

Fuente. Elaboración propia.

C. Tasa de ejecución confirmada del bloqueo automático

La tasa de ejecución confirmada del bloqueo automático mide el porcentaje de incidentes clasificados como maliciosos, aquellos con *risk score* igual o mayor a 6 que activan la rama de auto-respuesta, cuyo bloqueo quedó registrado en la Lista Dinámica Externa o en el WAF Akamai. El indicador no incluye los incidentes con puntaje menor a 6, que por diseño derivan a la rama de análisis asistido y terminan con el envío de un reporte, sin ejecución de bloqueo. El registro de cada bloqueo se confirma mediante el paso de validación final descrito en el apartado 3.5.2.5. La Tabla 10 presenta el resultado por fuente.

Tabla 10 **Tasa de ejecución confirmada del bloqueo automático**

Fuente	**Incidentes con risk score ≥6 (rama auto-respuesta)**	**Bloqueos ejecutados y confirmados**	**Tasa de ejecución confirmada (%)**
Firewall	3988	3988	100%
WAF Akamai	135	135	100%
Global	4123	4123	100%

Fuente. Elaboración propia.

Cada bloqueo se da por ejecutado solo después de que el paso de validación final confirma que la dirección IP quedó registrada en la Lista Dinámica Externa o en el WAF Akamai, según la fuente del caso. Por ello, el

resultado refleja bloqueos verificados sobre la infraestructura y no únicamente instrucciones enviadas. En consecuencia, el indicador mide la ejecución técnica confirmada del bloqueo automático y no la efectividad en la contención de amenazas, dado que no evalúa el desempeño sobre los 51 casos que, por diseño, derivaron a la rama de análisis asistido.

D. Reducción de carga operativa manual

La Tabla 11 muestra una estimación del ahorro operativo a partir del tiempo de gestión por incidente antes y después de la automatización, aplicado sobre la carga de referencia del proceso manual (302 incidentes mensuales). El tiempo de gestión se asume igual al MTTD, tramo que corresponde a las actividades del CyberSOC, y la comparabilidad de volúmenes se sustenta en el apartado 4.2.1. Este cálculo se retoma en el apartado 4.2 (Evaluación Económica).

Tabla 11 **Reducción de carga operativa manual**

Métrica	**Antes (proceso manual)**	**Después (con MCIA)**	**Variación (%)**	**Ahorro**
Tiempo de gestión por incidente (MTTD)	1 h 30 min 34 s	2 min 45 s	−97.0	1 h 27 min 49 s
Incidentes de referencia por mes	302	302	—	—
Horas-analista equivalentes por mes	455.9 h	13.8 h	−97.0	442.0 h

Fuente. Elaboración propia.

En la Tabla 11 se puede observar que, con el MCIA, el tiempo de gestión por incidente se reduce en 97.0 %. Cabe precisar que, de forma conservadora, a las 13.8 horas del periodo posterior se les asignó el tiempo de procesamiento del orquestador como si fuera tiempo de

analista, mientras que las horas de supervisión y afinamiento se valorizan por separado en la Tabla 15.

E. Cumplimiento de los KPIs de éxito

La Tabla 12 contrasta los resultados obtenidos con las metas acordadas en el kick-off. Las metas se evalúan sobre el promedio global y por fuente.

Tabla 12 **KPIs de éxito del proyecto**

KPI	Línea base	Meta	Resultado	Estado
MTTD global	1 h 30 min	< 15 min	2 min 45 s	Cumple
MTTR global	30 h 52 min	< 30 min	1 min 16 s	Cumple
MTTD / MTTR Firewall	1 h 52 min / 33 h 46 min	< 15 / < 30 min	2 min 47 s / 1 min 13 s	Cumple
MTTD / MTTR WAF Akamai	1 h 16 min / 29 h 1 min	< 15 / < 30 min	1 min 54 s / 2 min 32 s	Cumple
Reglas en producción	0/48	—	48/48	Seguimiento
Tasa de respuesta automatizada	0 %	—	98.8 %	Seguimiento
Tasa de ejecución confirmada del bloqueo	—	—	100 %	Seguimiento

Fuente. Elaboración propia.

Para sostener la plataforma sin depender de una sola persona, se documentaron los procedimientos y configuraciones necesarios para el correcto funcionamiento del orquestador. Asimismo, se capacitó al equipo de operación mediante sesiones prácticas y se designó un

responsable de respaldo para operar la plataforma en ausencia del líder técnico del proyecto.

Del proyecto se identificaron cinco lecciones aprendidas que quedaron documentadas: validar la calidad de una fuente antes de integrarla, debido a que los logs no normalizados reducen la automatización; calibrar los umbrales de forma progresiva para evitar falsos positivos; documentar y capacitar al equipo durante el cierre y no después, para evitar la dependencia de una sola persona; mantener una comunicación periódica con el cliente para que la conformidad final no sea una sorpresa; y redactar los procedimientos pensando en su reutilización, de modo que puedan aplicarse a otros clientes sin rehacer la documentación.

Como cierre de esta fase, en la Figura 51 se presenta el correo remitido al cliente el 28 de abril de 2026, mediante el cual se convocó al comité operativo. En dicho comité quedó registrada la conformidad sobre la puesta en operación del orquestador MCIA. Adicionalmente, la empresa emitió una constancia de ejecución y conformidad del trabajo, en la que acredita la participación del autor en el análisis, diseño, implementación y puesta en operación del sistema de orquestación entre diciembre de 2025 y abril de 2026 (ver Anexo D). Los resultados correspondientes a esta fase se detallan en el apartado 3.6.



Figura 51 **Convocatoria a la reunión de comité operativo y conformidad de la puesta en operación del orquestador MCIA.** Fuente. Elaboración propia, a partir del correo enviado el 28/04/2026.

3.6 Resultado de la actividad

Como resultado de las actividades realizadas, se implementó el sistema de orquestación del CyberSOC para la detección y respuesta automatizada ante amenazas perimetrales de un cliente corporativo.

3.6.1 Resultado de la implementación del sistema de orquestación en el CyberSOC

Al finalizar la implementación, el sistema de orquestación MCIA quedó operativo en producción, cubriendo las 48 reglas de detección priorizadas (23 de Firewall y 25 de WAF Akamai) mediante los flujos de respuesta automatizada. Al comparar el periodo posterior a la puesta en operación (del 01/04/2026 al 30/04/2026) con la línea base del periodo previo (01/10/2025 – 30/11/2025), los resultados evidenciaron una reducción del tiempo medio de detección (MTTD) global de 1 h 30 min a 2 min 45 s (-97.0 %), y del tiempo medio de resolución (MTTR) global de 30 h 52 min a 1 min 16 s (-99.9 %). Por fuente, el MTTD de Firewall bajó de 1 h 52 min a 2 min 47 s y el de WAF Akamai de 1 h 16 min a 1 min 54 s (ambos -97.5 %); mientras que el MTTR de Firewall bajó de 33 h 46 min a 1 min 13 s y el de WAF Akamai de 29 h 1 min a 2 min 32 s (ambos -99.9 %).

Ambos indicadores se ubicaron por debajo de las metas de 15 y 30 minutos acordadas con el cliente (Tabla 12).

El orquestador procesó de forma automática la totalidad de los 4174 eventos ingeridos durante el periodo evaluado (4031 de Firewall y 143 de WAF Akamai) en las etapas de ingesta, enriquecimiento y clasificación. De ellos, el 98.8 % (4123 eventos) superó el umbral de risk score ≥6 y activó la rama de auto-respuesta con bloqueo automático, mientras que el 1.2 % (51 eventos) obtuvo un puntaje menor a 6 y derivó a la rama de análisis asistido por IA, concluyendo con un reporte de recomendación, sin ejecución de bloqueo. Sobre los 4123 eventos de la rama de auto-respuesta, el bloqueo fue ejecutado y verificado en su totalidad mediante el paso de validación final del flujo, con una tasa de ejecución confirmada del bloqueo automático del 100 %.

En cuanto a la carga operativa, el tiempo de gestión por incidente se redujo de 1 h 30 min 34 s a 2 min 45 s (−97.0 %). Sobre la carga de referencia del proceso manual (302 incidentes mensuales), ello representa un ahorro estimado de 442.0 horas-analista

equivalentes al mes (Tabla 11). El mayor número de ofensas procesadas por el orquestador (4174) no es comparable con esa carga, debido a que el orquestador cierra cada ofensa en minutos y QRadar genera nuevas ofensas con mayor frecuencia (apartado 4.2.1).

El cliente validó los resultados y aprobó el pase a producción del autobloqueo, culminando con la transferencia de conocimiento al equipo de operación del CyberSOC.

3.6.2 Resultado de la identificación y priorización de las reglas de detección

De acuerdo con lo descrito en la Etapa 1: Análisis y levantamiento de información (Fases 1 y 2), se identificaron las reglas de detección configuradas en el SIEM (IBM QRadar) para los 21 firewalls FortiGate integrados y para el WAF Akamai, y se priorizaron considerando su frecuencia de alertas y su potencial de automatización.

La priorización operó en dos niveles. A nivel de fuentes, se seleccionaron los firewalls FortiGate y el WAF Akamai por ser, entre las plataformas del cliente integradas al SIEM, las que mayor volumen de alertas perimetrales generaban y mayor carga operativa representaban para el equipo de monitoreo. Además, ambas contaban con una acción de respuesta que podía ser automatizada: el bloqueo de direcciones IP.

Como resultado, se levantaron 48 reglas de detección, de las cuales 23 corresponden a eventos de firewall y 25 a tráfico web del WAF Akamai, que constituyeron el universo de casos de uso a automatizar. La frecuencia de las alertas se obtuvo del histórico de tickets registrados en la ticketera iTop durante los meses de octubre y noviembre de 2025, contabilizando el número de incidentes generados por cada regla. Sobre este conteo se aplicaron los criterios de priorización: volumen de alertas generadas en el SIEM durante el periodo, tipo de acción de respuesta requerida (bloqueo de IP), disponibilidad del dato necesario para la decisión (IP origen o destino para firewall; IP origen externa y *request site* para WAF Akamai) y existencia de un procedimiento manual realizado por el analista de manera diaria.

En la Figura 52 se presentan los casos de uso de firewall y en la Figura 53 los del WAF Akamai, indicando en ambos casos el nombre de la regla, la cantidad de alertas en el periodo y el criterio de análisis asignado.

Nombre del caso de uso	¿Qué evalua la regla?	¿Quién aplica para Vulnerabilidades?	N° de alertas
CUD-154 Detección de	IP origen	IP Destino	177
CUD-149 Detección de	IP Destino	IP Origen	36
CUD-152 Detección de	IP origen	IP Destino	13
CUD-158 Exploit/Malwar	IP Destino	IP origen	5
CUD-156 Deteccion de	IP origen	IP Destino	4
CUD-140 Detección de	IP origen	IP Destino	1
CUD-162 Excessive Fire	IP Destino	IP origen	0
CUD-141 Detección de	IP origen	IP Destino	0
CUD-142 Detección de	IP origen	IP Destino	0
CUD-143 Detección de	IP origen	IP Destino	0
CUD-144 Detección de	IP origen	IP Destino	0
CUD-145 Detección de	IP origen	IP Destino	0
CUD-146 Detección de	IP origen	IP Destino	0
CUD-147 Detección de	IP origen	IP Destino	0
CUD-148 Detección de	IP origen	IP Destino	0
CUD-150 Detección de	IP origen	IP Destino	0
CUD-151 Detección de	IP origen	IP Destino	0
CUD-153 Detección de	IP origen	IP Destino	0
CUD-155 Detección de	IP Destino	IP Origen	0
CUD-157 Detección de	IP origen	IP Destino	0
CUD-159 Microsoft Win	IP origen	IP Destino	0
CUD-160 Detección de	IP Destino	IP origen	0
CUD-164 Detección de	IP Destino	IP origen	0

Figura 52 **Casos de uso de Firewall.** Fuente. Elaboración propia.

Nombre del caso de uso	¿Qué evalua la regla?	N° de alertas
CUD-299 Detección de Unknown	Source IP	196
CUD-301 Detección de ataques D	Source IP	71
CUD-290 Detección de Local File	Source IP	48
CUD-303 Detección de intentos d	Source IP	15
CUD-309 Detección de Unknown	Source IP	9
CUD-312 Detección de Unknown	Source IP	7
CUD-294 Detección de Ataques d	Source IP	5
CUD-307 Detección de Impersona	Source IP	5
CUD-306 Detección de Unknown	Source IP	3
CUD-292 Detección de Cross-site	Source IP	2
CUD-304 Detección de intentos d	Source IP	2
CUD-311 Detección de Unknown	Source IP	2
CUD-315 Detección de ataques V	Source IP	2
CUD-291 Detección de SQL Injec	Source IP	0
CUD-293 Detección Potential Rer	Source IP	0
CUD-295 Detección de ataques d	Source IP	0
CUD-296 Detección de Ataques d	Source IP	0
CUD-297 Detección de intento de	Source IP	0
CUD-298 Detección intento de ata	Source IP	0
CUD-300 Detección de ataques d	Source IP	0
CUD-305 Detección de Unknown	Source IP	0
CUD-308 Detección de Unknown	Source IP	0
CUD-310 Detección de Unknown	Source IP	0
CUD-313 Detección de ataques re	Source IP	0
CUD-316 Detección de Unknown	Source IP	0

Figura 53 **Casos de uso de WAF Akamai.** Fuente. Elaboración propia.

3.6.3 Resultado del diseño de los flujos de respuesta automatizada

De acuerdo con lo descrito en la **Etapa 2: Diseño e implementación de la solución (Fase 3)**, se diseñaron los flujos de respuesta automatizada del orquestador a

partir de las actividades que realizaba manualmente el analista y de las integraciones disponibles con las herramientas del CyberSOC.

Como resultado, se obtuvieron dos plantillas de flujo, una para las reglas de firewall y otra para WAF Akamai. Ambas comparten una secuencia de seis etapas: ingesta, enriquecimiento, cálculo de risk score, decisión, respuesta y registro. La etapa de respuesta incluye una validación final que confirma que el bloqueo quedó registrado en el canal correspondiente. Ambas plantillas se parametrizan según la regla que las activa, evitando construir una lógica independiente para cada una de las 48 reglas priorizadas. Las etapas del flujo automatizan actividades que anteriormente realizaba el analista, como la consulta a fuentes de inteligencia, Tenable y Cortex XDR para el enriquecimiento; la clasificación mediante el risk score, basado en gravedad global, certeza reputacional, direccionalidad del flujo y mapeo de campañas activas, en una escala de 1 a 10 y con un umbral igual o mayor a 6; y la ejecución de la respuesta mediante el bloqueo en la Lista Dinámica Externa o en el WAF Akamai y la generación del ticket en iTop. Adicionalmente, se implementó el mecanismo de no duplicación entre fuentes y se definió con el cliente la política de auto-respuesta, estableciendo qué acciones podían ejecutarse automáticamente y cuáles requerían validación humana.

Las plantillas diseñadas se presentan en la Figura 12 (firewall) y la Figura 13 (WAF Akamai), el mecanismo de no duplicación en la Figura 14, la política de auto-respuesta en la Tabla 6 y las integraciones habilitadas en la Tabla 7. La Figura 54 presenta la correspondencia entre cada paso del proceso manual del analista y su equivalente automatizado en el orquestador.

Con ello, se atendió el segundo objetivo específico, al establecer un diseño de flujos necesarios para automatizar la respuesta ante los principales vectores de amenaza perimetral.

N°	Paso del proceso	Quién lo ejecutaba (proceso manual)	Tiempo aproximado (proceso manual)	Componente del orquestador que lo reemplaza
1	Recepción y análisis inicial de la ofensa generada en el SIEM (IBM QRadar)	Analista de Monitoreo	≈1:50 - 1:55 h (Firewall) / ≈1:03 - 1:29 h (WAF Akamai) — línea base MTTD, oct-nov 2025	Módulo de Ingesta (cybersoc-api): consulta periódica a la API REST de QRadar y extracción automática de los campos relevantes (IP origen/destino o IP origen + request site)
2	Consulta de contexto adicional del activo y del histórico del evento (vulnerabilidades, eventos previos)	Analista de Monitoreo (consulta manual a otras herramientas)	Incluido dentro del tiempo de análisis (MTTD)	Módulo de Enriquecimiento automático: Tenable y Cortex XDR (Firewall); historial por request site (WAF Akamai); fuentes de inteligencia externas (VirusTotal, AbuseIPDB, Criminal IP, OTX)
3	Determinación de la severidad y priorización del evento (criterio de riesgo)	Analista de Monitoreo (criterio experto manual)	Incluido dentro del tiempo de análisis (MTTD)	Motor de cálculo de risk score: combina gravedad global, certeza reputacional, direccionalidad del flujo y mapeo de campañas activas en una escala de 1 a 10
4	Envío de la notificación al cliente sobre la ofensa detectada	Analista de Monitoreo	Minutos, dentro del tiempo total de reporte al cliente	Microservicio de correo (email-api): generación y envío automático del reporte según la plantilla configurada por tipo de alerta
5	Llamada al cliente para una acción inmediata y espera de la confirmación del accionable	Analista de Monitoreo / Cliente	≈26 - 39 h (Firewall) / ≈27 - 30 h (WAF Akamai) — línea base MTTR, oct-nov 2025 (principal componente del tiempo de respuesta)	Política de auto-respuesta acordada con el cliente (Tabla 6): umbral de risk score ≥ 6 habilita la acción automática sin esperar confirmación telefónica
6	Ejecución del bloqueo de la IP maliciosa sobre el firewall o el WAF	Analista de Respuesta	Incluido dentro del tiempo de respuesta (MTTR)	Bloqueo automático en la Lista Dinámica Externa (EDL, para Firewall) y/o en WAF Akamai (canal WAF→EDL)
7	Registro y cierre documental del caso	Analista de Respuesta	Minutos, dentro del tiempo de cierre del caso	Generación automática de ticket en iTop con el detalle del evento, el resultado del enriquecimiento y el risk score; registro en el log de auditoría del orquestador (trazabilidad visible en el Sistema Web)

Figura 54 **Comparativo del proceso manual del analista frente al paso automatizado.**
Fuente. Elaboración propia.

3.6.4 Resultado de la implementación de los flujos en el orquestador

De acuerdo con lo descrito en la Etapa 2: Diseño e implementación de la solución (Fases 4 a 9) y la Etapa 3: Piloto controlado y pase a producción (Fases 10 a 12), se implementaron los flujos de respuesta automatizada diseñados en el apartado anterior sobre las herramientas del CyberSOC.

Como resultado, se construyó el motor de orquestación MCIA sobre una arquitectura por capas (Figura 11), desplegado en contenedores Docker con proxy Nginx y bases de datos PostgreSQL y Redis (Figura 15), y conectado al SIEM del cliente mediante una VPN *site-to-site* (Figura 16). Sobre esta base se desarrollaron los módulos del núcleo cybersoc-api (ingesta y cierre de ofensas, gestión de contexto, lista blanca y resolución de IP) y el microservicio independiente email-api para el envío de reportes (Figura 25), además de los conectores hacia las fuentes de inteligencia de amenazas, Tenable, Cortex XDR, iTop y Gemini (Figuras 17 a 24), y los canales de bloqueo hacia la Lista Dinámica Externa y el WAF Akamai (Figuras 22 y 23).

El motor de decisión se implementó con el cálculo de *risk score* y el umbral de clasificación, igual o mayor a 6 como malicioso (Figura 26), habilitando la rama de autobloqueo con validación final y generación de ticket (Figura 28) y la rama de análisis asistido por IA con envío de reporte (Figura 29), junto con la lógica de no duplicación y detección de ofensa recurrente (Figura 30). Con esta base se

parametrizaron los flujos de trabajo de las 48 reglas priorizadas, 23 de Firewall y 25 de WAF Akamai, sobre las dos plantillas definidas (Figuras 31 y 32), y se desarrolló el sistema web con los *dashboards* de MTTD, MTTR, bitácora de tickets y monitoreo en tiempo real (Figuras 33 a 36).

La correcta operación de los flujos implementados se validó mediante pruebas unitarias, de integración y de no duplicación, evidenciadas en el caso CUD-154 (Figuras 37 y 38). Posteriormente, se ejecutó un piloto controlado en modo observación, sin autobloqueo activo, que permitió calibrar el umbral de riesgo y la lista blanca (Figuras 41 y 42), antes de habilitar el bloqueo automático de forma progresiva, conforme se confirmaba la reincidencia de amenazas reales (Figura 43), y validar el mecanismo de reversión sobre la Lista Dinámica Externa (Figura 44). Con la aprobación del cliente (Figura 45), se realizó el pase a producción de forma gradual hasta cubrir las 48 reglas priorizadas, bajo seguimiento continuo del equipo de Monitoreo.

Con ello, se atendió el tercer objetivo específico, al implementar y poner en operación los flujos de respuesta automatizada sobre las herramientas del CyberSOC, desde el piloto controlado hasta el pase a producción.

3.6.5 Resultado de la evaluación del impacto en los indicadores MTTD y MTTR

De acuerdo con lo descrito en la Etapa 4: Cierre de la implementación y transición a operación continua (Fase 14), se evaluó el impacto de la implementación del sistema de orquestación en los indicadores operativos MTTD y MTTR del CyberSOC, comparando el periodo previo a la implementación (01/10/2025 al 30/11/2025) con el periodo posterior a su puesta en operación (01/04/2026 al 30/04/2026).

Como se muestra en la Tabla 8, el tiempo medio de detección (MTTD) global se redujo de **1 h 30 min a 2 min 45 s (-97.0%)**, y el tiempo medio de resolución (MTTR) global de **30 h 52 min a 1 min 16 s (-99.9%)**. Por fuente, el MTTD de Firewall bajó de 1 h 52 min a 2 min 47 s y el de WAF Akamai de 1 h 16 min a 1 min 54 s, ambos con una reducción de 97.5%; el MTTR de Firewall bajó de 33 h 46 min a 1 min 13 s y el de WAF Akamai de 29 h 1 min a 2 min 32 s, ambos con una reducción

de 99.9%. Ambos indicadores se ubicaron por debajo de las metas de 15 y 30 minutos (Tabla 12).

En cuanto al volumen de eventos, la Tabla 9 muestra que el orquestador procesó automáticamente los 4174 eventos ingeridos durante el periodo evaluado (4031 de Firewall y 143 de WAF Akamai). De ellos, el 98.8 % (4123 eventos) activó la rama de auto-respuesta por alcanzar un risk score ≥6, y el 1.2 % (51 eventos) derivó a la rama de análisis asistido por IA, cuyo desenlace es el envío de un reporte con recomendación y no la ejecución de un bloqueo. Asimismo, la Tabla 10 evidencia una tasa de ejecución confirmada del bloqueo automático del 100 % sobre los 4123 eventos con risk score ≥6, verificada mediante el paso de validación final que confirma que cada bloqueo quedó registrado.

Finalmente, la Tabla 11 muestra que el tiempo de gestión por incidente se redujo de 1 h 30 min 34 s a 2 min 45 s (−97.0 %). Sobre la carga de referencia del proceso manual (302 incidentes mensuales), ello representa un ahorro estimado de 442.0 horas-analista equivalentes al mes. El mayor número de ofensas procesadas por el orquestador (4174) no es comparable con esa carga, debido a que el orquestador cierra cada ofensa en minutos y QRadar genera nuevas ofensas con mayor frecuencia (apartado 4.2.1). Este ahorro operativo se retoma en el apartado 4.2, Evaluación Económica.

Con ello, se atendió el cuarto objetivo específico, al evidenciar una mejora en los indicadores operativos MTTD y MTTR del CyberSOC frente al proceso manual previo.

CAPÍTULO IV:
DISCUSIÓN DE RESULTADOS

4.1 Descripción de la implementación

El presente capítulo discute los resultados obtenidos durante el desarrollo e implementación del sistema de orquestación MCIA, organizándolos en las cuatro etapas descritas en el Capítulo III, que agrupan de manera consolidada los hitos alcanzados a lo largo de las catorce fases del proyecto. En cada etapa se presentan brevemente los principales resultados y se contrastan con los antecedentes expuestos en el apartado 3.4.1, identificando las coincidencias y diferencias.

4.1.1 Etapa de análisis y levantamiento de información (Fases 1 y 2)

A. Identificación y caracterización de fuentes de datos

Se consolidó el inventario de fuentes integradas con el SIEM QRadar, 21 firewalls FortiGate y el WAF Akamai, validando su disponibilidad y las herramientas de enriquecimiento asociadas, Tenable y Cortex XDR, lo que permitió determinar la viabilidad técnica del flujo de detección y respuesta.

B. Definición del gobierno del proyecto

Se identificaron los stakeholders y se formalizó una matriz RACI que delimitó responsabilidades entre la empresa y el cliente, reduciendo ambigüedades en la operación del orquestador.

C. Levantamiento y priorización de reglas de detección

Se documentan y priorizan 48 reglas de correlación, 23 de firewall y 25 de WAF Akamai, a partir del histórico de tickets, delimitando el universo de casos de uso a automatizar.

D. Establecimiento de la línea base de indicadores

Se calcularon el MTTD y el MTTR del proceso manual durante octubre y noviembre de 2025, constituyendo el punto de comparación para medir el impacto de la automatización.

E. Contraste con los antecedentes nacionales

Los resultados de esta etapa coinciden con Vilcarromero y Vilchez (2018), quienes plantearon para un SOC un modelo de gestión basado en el NIST CSF que considera los procesos, la tecnología y el personal. El presente trabajo abordó esas tres dimensiones: los procesos, mediante la política de auto-respuesta y el levantamiento del proceso manual; la tecnología, mediante la integración de fuentes y herramientas; y el personal, mediante la matriz RACI. La diferencia radica en el enfoque de evaluación: dicho antecedente mide niveles de madurez de los controles, mientras que este trabajo mide el impacto con indicadores operativos (MTTD y MTTR). En la misma línea, Atalaya Urrutia (2023) resalta la necesidad de adaptar marcos como ISO/IEC 27032 y NIST a las particularidades de cada organización. Este trabajo coincide con ese planteamiento, pues la priorización de las 48 reglas se realizó a partir del histórico propio del cliente. Se diferencia en el ámbito (sector universitario frente a cliente corporativo) y en el nivel de intervención: el antecedente propone un modelo de gestión, mientras que aquí se ejecutó una implementación técnica en producción.

4.1.2 Etapa de diseño e implementación de la solución (Fases 3 a 9)

A. Definición de la arquitectura del orquestador

Se diseñó e implementó el motor MCIA bajo una arquitectura por capas, con microservicios, base de datos y sistema web, permitiendo la escalabilidad y disponibilidad del servicio.

B. Diseño modular de las plantillas de flujo

Se estructuraron dos plantillas parametrizables, una para firewall y otra para WAF Akamai, que comparten una misma secuencia de etapas, reduciendo el esfuerzo de mantenimiento frente a la construcción de una lógica independiente para cada regla.

C. Desarrollo del motor de decisión y de las integraciones

Se implementó el cálculo de *risk score*, el umbral de autorespuesta y los conectores hacia las fuentes de inteligencia de amenazas, Tenable, Cortex XDR, iTop y Gemini, integrando el flujo de detección, enriquecimiento y respuesta.

D. Implementación de los 48 playbooks y del sistema web

Se parametrizaron las reglas priorizadas sobre las plantillas definidas y se desarrolló el sistema web con dashboards de MTTD, MTTR y trazabilidad de tickets, proporcionando visibilidad operativa al equipo de Monitoreo.

E. Contraste con el antecedente de inteligencia artificial

Ismail et al. (2025) propusieron un enfoque de hiperautomatización con inteligencia artificial agéntica integrada a una plataforma SOAR. El presente trabajo coincide en incorporar IA al flujo de respuesta, pero con un alcance distinto. En el MCIA, la IA generativa (Gemini) solo emite recomendaciones en la rama de análisis asistido, mientras que la decisión de bloqueo se mantiene determinista, basada en el *risk score*, y con validación humana en los casos no maliciosos. Este diseño prioriza la trazabilidad y el control sobre la autonomía, y deja el enfoque agéntico como una posible evolución (Recomendación 6).

4.1.3 Etapa de piloto controlado y pase a producción (Fases 10 a 12)

A. Validación funcional mediante pruebas de QA

Se confirmó el correcto funcionamiento de los flujos, incluyendo la lógica de no duplicación entre fuentes, antes de intervenir la infraestructura del cliente.

B. Ejecución del piloto en modo observación

Se desplegó el orquestador sin autobloqueo activo, lo que permitió calibrar el umbral de riesgo y la lista blanca con evidencia real, reduciendo el riesgo de falsos positivos en producción.

C. Aprobación del cliente y pase a producción gradual

Se obtuvo la conformidad del cliente sobre los resultados del piloto y se activó el autobloqueo de forma progresiva hasta cubrir las 48 reglas priorizadas, asegurando una transición controlada hacia la operación automatizada.

D. Contraste con el antecedente en entornos OT

Mir y Ramachandran (2021) aplicaron SOAR en sistemas SCADA de redes eléctricas inteligentes, lo que evidencia que la orquestación permite respuestas coordinadas en entornos críticos. El presente trabajo coincide en ese beneficio, pero difiere en el dominio. En entornos OT, donde la disponibilidad de los procesos físicos es prioritaria, la contención automática suele requerir mayores restricciones. En el perímetro de TI corporativa, en cambio, la acción de respuesta (el bloqueo de IP externas) es acotada y reversible, y se habilitó solo después de calibrar el umbral en el piloto. Estas condiciones permitieron automatizar la respuesta sobre el 98.8 % de los casos.

4.1.4 Etapa de cierre de la implementación y transición a operación continua (Fases 13 y 14)

A. Medición del impacto en los indicadores operativos

Se compararon los valores de MTTD y MTTR del periodo posterior a la puesta en operación con la línea base, evidenciando una reducción de 97.0 % en el MTTD y de 99.9 % en el MTTR, por debajo de las metas establecidas.

B. Transferencia de conocimiento y redefinición de roles

Se capacitó al equipo de operación y se documentaron los procedimientos del orquestador, redefiniendo el rol del analista de ejecutor manual a supervisor y validador de excepciones, lo que redujo la dependencia de una persona clave.

C. Cierre formal con conformidad del cliente

Se obtuvo la conformidad del cliente sobre la puesta en operación del orquestador, así como la conformidad de la empresa respecto a lo ejecutado (Anexo D), dejando establecidos lineamientos de gobierno para su posible réplica en otros clientes del CyberSOC.

D. Contraste con los resultados reportados en la literatura

Los resultados coinciden con lo reportado por Pulyala et al. (2019) respecto a la reducción de los tiempos de detección y respuesta y de la carga operativa de los analistas mediante la automatización de tareas repetitivas; en este

trabajo, dicha reducción se tradujo en un ahorro estimado de 442.0 horas-analista equivalentes al mes.

Los resultados de la medición descrita superan las referencias que sirvieron de base al proyecto. IBM Security (2024) reporta que las organizaciones que incorporan automatización y orquestación reducen en más del 30% los tiempos de detección y contención de brechas, mientras que en el presente trabajo la reducción del MTTD y del MTTR fue de 97.0 % y 99.9 %, respectivamente. Esta diferencia puede explicarse por el alcance acotado de la implementación: la automatización se aplicó únicamente sobre dos fuentes perimetrales, los firewalls FortiGate y el WAF Akamai, con una acción de respuesta claramente delimitada, el bloqueo de direcciones IP. En este escenario, la orquestación puede alcanzar un mayor efecto; en un entorno con un mayor número de fuentes y casos de uso más heterogéneos, los porcentajes de mejora podrían ser menores.

Como limitaciones de la evaluación, la medición corresponde al primer mes completo de operación en producción (abril de 2026), periodo que coincide con el cierre del proyecto (apartado 2.2), y a un único cliente corporativo. Asimismo, en los casos derivados a análisis asistido, la reducción del MTTR también se ve favorecida por el contacto proactivo con el cliente descrito en la Fase 13.

Finalmente, el MTTD se definió operativamente a partir de la generación de la ofensa en QRadar (apartado 3.4.2.6), por lo que no considera el tiempo transcurrido entre la ocurrencia real del ataque y su registro en el SIEM.

4.2 Evaluación Económica

En la evaluación económica se analizan los ingresos y egresos monetarios asociados con la implementación del sistema de orquestación MCIA, contrastando la inversión realizada durante su desarrollo con los beneficios derivados de la reducción de horas de gestión manual de los incidentes del CyberSOC, así como con el costo mensual de mantener y afinar la herramienta. A partir de este contraste se calculan los indicadores de Relación Beneficio/Costo (B/C), Valor Actual Neto (VAN), Tasa Interna de Retorno (TIR) y Periodo de Recuperación simple, con el fin de determinar la viabilidad económica del proyecto.

4.2.1 Supuestos considerados

Dado que el orquestador se implementó sobre infraestructura propia del CyberSOC y con personal que ya forma parte de la planilla de la empresa, el proyecto no representó la compra de equipos o licencias ni la contratación de personal adicional. Para efectos de esta evaluación, la inversión se valoriza como el costo de oportunidad de las horas que el equipo del proyecto dedicó al desarrollo del orquestador, mientras que el beneficio se valoriza a partir del ahorro de horas de gestión manual generado en el equipo de Monitoreo y Respuesta. Asimismo, se considera un costo mensual de horas para el afinamiento y la mejora continua de la herramienta. Se consideraron los siguientes supuestos:

- **Periodo de desarrollo:** 5 meses (diciembre de 2025 a abril de 2026), según el cronograma del proyecto (Tabla 1).

- **Horas dedicadas al desarrollo:** Analista de Automatización, 400 h (20 h/semana); Analista de Inteligencia de Amenazas, 200 h (10 h/semana); Security Manager, 200 h (10 h/semana); y, dada su participación también en el levantamiento y las pruebas, Analista de Monitoreo y Analista de Respuesta, 100 h (5 h/semana) cada uno.

- **Ahorro mensual:** 442.0 horas-analista equivalentes (Tabla 11), distribuido en 70% para el Analista de Monitoreo y 30% para el Analista de Respuesta, en función de su participación en el proceso manual descrito en la Fase 1.

- **Horas mensuales reservadas para afinamiento y mejora continua:** una vez puesto en producción el orquestador, se consideran 10 h del Analista de Automatización, 5 h del Analista de Inteligencia de Amenazas, 5 h del Security Manager, 3 h del Analista de Monitoreo y 2 h del Analista de Respuesta.
- **Costos no incluidos:** no se consideran costos de infraestructura, dado que el orquestador se desplegó sobre recursos ya existentes del CyberSOC, ni el consumo del motor de IA, cuyo licenciamiento empresarial es asumido por la empresa de forma transversal a otros proyectos y cuyo costo es variable. Por ello, los indicadores económicos corresponden al costo incremental del proyecto, expresado en horas-hombre.

- **Tiempo de gestión por incidente:** se asume igual al MTTD (1 h 30 min 34 s antes; 2 min 45 s después), dado que este tramo corresponde a las actividades ejecutadas por el CyberSOC (triaje, enriquecimiento, análisis y reporte), mientras que el tramo del MTTR corresponde principalmente al tiempo de respuesta del cliente.

- **Comparabilidad de volúmenes:** el aumento de ofensas en el periodo posterior (4174 frente a 302 mensuales) no refleja un aumento de amenazas atendidas. En el proceso manual, el operador mantenía la ofensa abierta alrededor de una hora y en ella se acumulaban los eventos de la regla; el orquestador cierra la ofensa minutos después de su generación, por lo que QRadar genera nuevas ofensas con mayor frecuencia. Por ello, el ahorro se estima sobre la carga de referencia del proceso manual (302 casos/mes).

- **Tasa de descuento:** 12% anual, correspondiente al costo de oportunidad del capital.

- **Horizonte de evaluación:** 12 meses de operación, a partir de la puesta en producción del orquestador.

4.2.2 Inversión del proyecto

La inversión del proyecto corresponde al costo de oportunidad de las horas dedicadas por el equipo del proyecto —Analista de Automatización, Analista de Inteligencia de Amenazas, Security Manager, Analista de Monitoreo y Analista de Respuesta— durante las cuatro etapas del desarrollo, como se muestra en la Tabla 13. No se incurrió en un desembolso adicional por parte de la empresa, dado que todos los roles pertenecen a su planilla.

Tabla 13 **Inversión del proyecto (costo de horas-hombre)**

Rol	**Tarifa horaria (S/)**	**Horas dedicadas**	**Costo total (S/)**
Analista de Automatización	30.70	400	12,280.00
Analista de Inteligencia de Amenazas	34.92	200	6,984.00
Security Manager	43.37	200	8,674.00

Analista de Monitoreo	13.80	100	1,380.00
Analista de Respuesta	16.13	100	1,613.00
Total		1,000	30,931.00

Fuente. Elaboración propia.

4.2.3 Beneficio mensual bruto

El beneficio bruto se estima a partir de las 442.0 horas-analista equivalentes ahorradas mensualmente mediante la automatización (Tabla 11), distribuidas entre el Analista de Monitoreo y el Analista de Respuesta según su participación en el proceso manual previo y valorizadas de acuerdo con su tarifa horaria, como se muestra en la Tabla 14.

Tabla 14 **Beneficio mensual bruto por ahorro de horas**

Rol	% del ahorro	Horas ahorradas / mes	Tarifa horaria (S/)	Beneficio mensual (S/)
Analista de Monitoreo	70%	309.41 h	13.80	4,269.82
Analista de Respuesta	30%	132.60 h	16.13	2,138.89
Total	100%	442.01		6,408.71

Fuente. Elaboración propia.

4.2.4 Costo mensual de afinamiento y mejora continua

Puesto en producción, el orquestador requiere mantenimiento continuo, ajuste de reglas, corrección de incidencias menores y mejoras en la lógica de *risk score*. Por ello, se reserva un bloque de horas mensuales del propio equipo del proyecto para estas actividades. Este costo se descuenta del beneficio bruto para obtener el flujo neto mensual, como se muestra en la Tabla 15.

Tabla 15 **Costo mensual de afinamiento y mejora continua**

Rol	Horas reservadas / mes	Tarifa horaria (S/)	Costo mensual (S/)

Analista de Automatización	10	30.70	307.00
Analista de Inteligencia de Amenazas	5	34.92	174.60
Security Manager	5	43.37	216.85
Analista de Monitoreo	3	13.80	41.40
Analista de Respuesta	2	16.13	32.26
Total	25		772.11

Fuente. Elaboración propia.

4.2.5 Flujo de caja y evaluación económica

Con la inversión inicial, el beneficio bruto mensual y el costo mensual de afinamiento se obtiene el flujo neto mensual, a partir del cual se proyecta el flujo de caja para un periodo de 12 meses. Cada flujo se descuenta utilizando la tasa mensual equivalente a una tasa anual de 12% (0.9489% mensual), lo que permite calcular el VAN, la TIR y la relación B/C del proyecto, como se muestra en la Tabla 16.

Tabla 16 **Flujo de caja proyectado a 12 meses**

Mes	Inversión (S/)	Beneficio bruto (S/)	Costo afinamiento (S/)	Flujo neto (S/)	Flujo descontado 12% anual (S/)	Flujo acumulado descontado (S/)
0	-30,931.00	0.00	0.00	-30,931.00	-30,931.00	-30,931.00
1	0.00	6,408.71	772.11	5,636.60	5,583.62	−25,347.38
2	0.00	6,408.71	772.11	5,636.60	5,531.13	−19,816.25
3	0.00	6,408.71	772.11	5,636.60	5,479.14	−14,337.10
4	0.00	6,408.71	772.11	5,636.60	5,427.64	−8,909.46
5	0.00	6,408.71	772.11	5,636.60	5,376.62	−3,532.84
6	0.00	6,408.71	772.11	5,636.60	5,326.09	1,793.25
7	0.00	6,408.71	772.11	5,636.60	5,276.02	7,069.27

8	0.00	6,408.71	772.11	5,636.60	5,226.43	12,295.70
9	0.00	6,408.71	772.11	5,636.60	5,177.30	17,473.01
10	0.00	6,408.71	772.11	5,636.60	5,128.64	22,601.65
11	0.00	6,408.71	772.11	5,636.60	5,080.43	27,682.08
12	0.00	6,408.71	772.11	5,636.60	5,032.68	32,714.74
				TOTAL:	63,645.74	

Fuente. Elaboración propia.

A. Relación Beneficio/Costo (B/C)

El valor presente de los beneficios netos (S/ 63,645.74) se dividió entre la inversión (S/ 30,931.00), obteniéndose una relación B/C de 2.06. Esto significa que por cada sol invertido en el desarrollo del orquestador se generan S/ 2.06 en beneficios netos, considerando el costo mensual de afinamiento. Por tanto, al ser mayor que 1, el proyecto resulta económicamente viable.

B. Valor Actual Neto (VAN)

Con una tasa de descuento de 12% anual, el VAN a 12 meses es de S/ 32,714.74. Al ser positivo, indica que el proyecto genera valor por encima del costo de oportunidad del capital considerado, incluso después de incluir el costo mensual de afinamiento y mejora continua.

C. Tasa Interna de Retorno (TIR)

La TIR es la tasa que hace que el VAN del proyecto sea cero: $30{,}931.00 = 5{,}636.60 \times [1 - (1 + TIR)^{-12}] / TIR$. Resolviendo por iteración se obtiene TIR = 14.71 % mensual ($5{,}636.60 \times [1 - (1.1471)^{-12}] / 0.1471 = 30{,}935.89 \approx 30{,}931.00$), equivalente a una TIR anual efectiva de 419.26 %. Este valor supera la tasa de descuento anual de 12% utilizada como referencia, lo que indica que la inversión resulta conveniente aun considerando el gasto recurrente de afinamiento.

D. Periodo de Recuperación simple

Al dividir la inversión (S/ 30,931.00) entre el flujo neto mensual (S/ 5,636.60), se obtiene un periodo de recuperación simple de 5.49 meses, equivalente

aproximadamente a 5 meses y 15 días. Esto indica que el orquestador recupera la inversión correspondiente a las horas dedicadas a su desarrollo dentro del primer año de operación, incluso considerando el costo mensual de afinamiento.

En conjunto, los cuatro indicadores muestran que la implementación del sistema de orquestación MCIA es económicamente viable: la inversión se recupera antes de los seis meses de operación y se obtiene un beneficio neto positivo después de considerar el costo mensual de afinamiento y mejora continua.

CAPÍTULO V:
CONCLUSIONES

A partir de los objetivos señalados para esta investigación se arribó a las siguientes conclusiones:

1. La implementación del orquestador MCIA permitió automatizar la detección y respuesta ante amenazas perimetrales del cliente, cubriendo las 48 reglas priorizadas (23 de Firewall y 25 de WAF Akamai) y realizando el pase de piloto a producción con aprobación del cliente, lo que permitió redefinir el rol del analista del CyberSOC, de ejecutor manual a supervisor y validador de excepciones.

2. La identificación de las reglas de detección configuradas en el SIEM, aplicando criterios de volumen de alertas, acción de respuesta automatizable y disponibilidad del dato de decisión, permitió priorizar 48 reglas de correlación (23 de Firewall FortiGate y 25 de WAF Akamai) como el universo de casos de uso a automatizar.

3. El diseño modular de dos plantillas de flujo parametrizables, una para Firewall y otra para WAF Akamai, permitió estandarizar la respuesta automatizada sobre las 48 reglas priorizadas sin requerir una lógica independiente para cada una, orientado a garantizar una contención oportuna ante los principales vectores de amenaza perimetral.

4. La implementación de los flujos diseñados sobre las herramientas del CyberSOC, validada mediante un piloto controlado y consolidada en su pase a producción, permitió procesar automáticamente la totalidad de los 4174 eventos del periodo evaluado y ejecutar la respuesta automatizada sobre el 98.8 % de ellos (4123 eventos con risk score ≥6), con una tasa de ejecución confirmada del

bloqueo automático del 100 % sobre dichos eventos; el 1.2 % restante derivó a la rama de análisis asistido por IA.

5. La evaluación del impacto evidenció una reducción del MTTD global de 97.0 % y del MTTR global de 99.9 % frente al proceso manual, con valores inferiores a las metas de 15 y 30 minutos acordadas con el cliente, tanto a nivel global como por fuente. Esta reducción del tiempo de gestión se tradujo en un ahorro estimado de 442.0 horas-analista equivalentes al mes.

CAPÍTULO VI:
RECOMENDACIONES

1. En línea con la reducción del MTTD y MTTR obtenida, se recomienda monitorear de manera periódica la disponibilidad de las fuentes de logs integradas, a fin de evitar que una interrupción en el envío de eventos afecte los tiempos de detección alcanzados.

2. Dado que la respuesta automatizada cubrió el 98.8% de los eventos de red, pero no incluyó los de *endpoint* e identidad, se recomienda evaluar la extensión de la orquestación a Cortex XDR, *Active Directory* y soluciones PAM, con el propósito de ampliar la cobertura de respuesta automatizada.

3. Para sostener la tasa de respuesta automatizada del 98.8%, se recomienda realizar revisiones periódicas de los casos de uso priorizados y de sus reglas asociadas, evitando que queden estáticas frente a nuevos patrones de amenaza y cambios en el entorno del cliente.

4. Considerando la reducción de la carga operativa lograda, se recomienda evaluar la incorporación de mecanismos de notificación directa al usuario final ante eventos que requieran comunicación, manteniendo al equipo de seguridad informado y evitando, en lo posible, generar actividades manuales adicionales para el analista.

5. Debido a la viabilidad económica obtenida, se recomienda evaluar la réplica del modelo de orquestación en otros clientes del CyberSOC, aprovechando la arquitectura modular y las plantillas parametrizables desarrolladas durante el proyecto.

6. Dado que la tasa de ejecución confirmada del bloqueo automático no evalúa los casos derivados a la rama de análisis asistido, se recomienda registrar, para dichos

casos, la decisión final adoptada por el cliente frente a la recomendación generada por el motor de IA, a fin de medir el grado de concordancia entre ambas y contar con evidencia para afinar la ingeniería de *prompts* y el umbral de *risk score*.

CAPÍTULO VII:
REFERENCIAS BIBLIOGRÁFICAS

[1] Atalaya Urrutia, C. W. (2023). *Modelo de ciberseguridad en universidades privadas en el Perú* [Tesis doctoral, Universidad Nacional de Piura]. Repositorio Institucional UNP. https://repositorio.unp.edu.pe/handle/20.500.12676/4865

[2] Banco Central de Reserva del Perú. (2025). *Memoria 2024*. https://www.bcrp.gob.pe/publicaciones/memoria-anual/memoria-2024.html

[3] Bhatt, S., Manadhata, P., y Zomlot, L. (2014). The operational role of security information and event management systems. *IEEE Security & Privacy*, *12*(5), 35-41. https://doi.org/10.1109/MSP.2014.103

[4] Cichonski, P., Millar, T., Grance, T., y Scarfone, K. (2012). *Computer security incident handling guide* (NIST Special Publication 800-61 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

[5] Cybersecurity and Infrastructure Security Agency. (2021). *Federal government cybersecurity incident and vulnerability response playbooks*. U.S. Department of Homeland Security. https://www.cisa.gov/resources-tools/resources/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks

[6] Ernst & Young Perú. (2024). *Nuevos horizontes de la madurez digital en el Perú 2024*. https://www.ey.com/es_pe/insights/technology/nuevos-horizontes-madurez-digital-peru

[7] European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[8] Fielding, R. (2000). *Architectural styles and the design of network-based software architectures* [Tesis doctoral, University of California, Irvine]. UCI Information and Computer Science. https://ics.uci.edu/~fielding/pubs/dissertation/fielding_dissertation.pdf

[9] Forbes Perú. (2024, 25 de marzo). *El Perú sufrió 5.000 millones de intentos de ciberataques en 2023, reportó Fortinet*. https://forbes.pe/tecnologia/2024-03-25/el-peru-sufrio-5-000-millones-de-intentos-de-ciberataques-en-2023-reporto-fortinet/

[10] Fortinet. (2024). *FortiOS administration guide: External blocklist (threat feed)*. Fortinet Document Library. https://docs.fortinet.com/

[11] IBM. (2024). *IBM QRadar SIEM documentation*. IBM Documentation. https://www.ibm.com/docs/en/qsip

[12] IBM Security. (2024). *Cost of a Data Breach Report 2024.* IBM Corporation. https://www.ibm.com/reports/data-breach

[13] IBM Security. (2025, 4 de septiembre). *La seguridad impulsada por IA y automatización reduce los costos de las filtraciones de datos en Latinoamérica*. IBM Newsroom. https://latam.newsroom.ibm.com/2025-09-04-IBM-La-seguridad-impulsada-por-IA-y-automatizacion-reduce-los-costos-de-las-filtraciones-de-datos-en-Latinoamerica

[14] Ismail, I., Kurnia, R., Brata, Z., Nelistiani, G., Heo, S., Kim, H., y Kim, H. (2025). Toward robust security orchestration and automated response in security operations centers with a hyper-automation approach using agentic artificial intelligence. *Information*, *16*(5), 365. https://doi.org/10.3390/info16050365

[15] Johnson, C., Badger, L., Waltermire, D., Snyder, J., y Skorupka, C. (2016). *Guide to cyber threat information sharing* (NIST Special Publication 800-150). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-150

[16] Kent, K., y Souppaya, M. (2006). *Guide to computer security log management* (NIST Special Publication 800-92). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-92

[17] Liu, P., Yuan, W., Fu, J., Jiang, Z., Hayashi, H., y Neubig, G. (2023). Pre-train, prompt, and predict: A systematic survey of prompting methods in natural language processing. *ACM Computing Surveys*, *55*(9), 1-35. https://doi.org/10.1145/3560815

[18] Mir, A., y Ramachandran, R. (2021). Implementation of security orchestration, automation and response (SOAR) in smart grid-based SCADA systems. *In Proceedings of the Sixth International Conference on Intelligent Computing and Applications* (Advances in Intelligent Systems and Computing, Vol. 1369). Springer. https://doi.org/10.1007/978-981-16-1335-7_14

[19] MITRE Corporation. (2022). *11 strategies of a world-class cybersecurity operations center*. https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

[20] MITRE Corporation. (2023). *MITRE ATT&CK: Adversarial tactics, techniques & common knowledge* [Base de datos]. https://attack.mitre.org/

[21] Newman, S. (2021). *Building microservices: Designing fine-grained systems* (2.a ed.). O'Reilly Media.

[22] NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

[23] OWASP Foundation. (s. f.). *Web application firewall*. OWASP. https://owasp.org/www-community/Web_Application_Firewall

[24] Pulyala, S., Desetty, A., y Jangampet, V. (2019). The impact of Security Orchestration, Automation, and Response (SOAR) on Security Operations Center (SOC) efficiency: A comprehensive analysis. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *10*(3), 1545-1549. https://doi.org/10.61841/turcomat.v10i3.14323

[25] Scarfone, K., y Hoffman, P. (2009). *Guidelines on firewalls and firewall policy* (NIST Special Publication 800-41 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-41r1

[26] Scarfone, K., y Mell, P. (2007). *Guide to intrusion detection and prevention systems (IDPS)* (NIST Special Publication 800-94). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-94

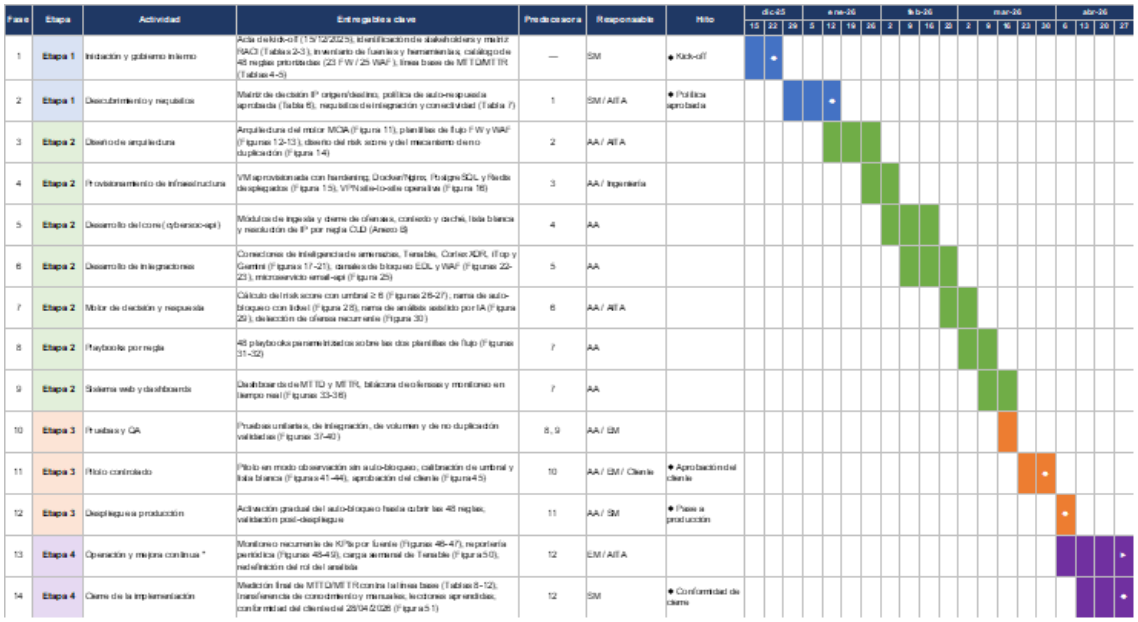
[27] Stallings, W. (2017). *Network security essentials: Applications and standards* (6.a ed.). Pearson Education.

[28] Verizon. (2024). *2024 data breach investigations report*. Verizon Communications. https://www.verizon.com/business/resources/reports/dbir/

[29] Vilcarromero, L., y Vilchez, E. (2018). *Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones* [Tesis de maestría, Universidad Peruana de Ciencias Aplicadas (UPC)]. Repositorio Académico UPC. http://hdl.handle.net/10757/624832

CAPÍTULO VIII:
ANEXOS

Anexo A
Cronograma detallado del proyecto (diagrama de Gantt)



Fase	Etapa	Actividad	Entregables clave	Predecesora	Responsable	Hito
1	Etapa 1	Iniciación y gobierno interno	Acta de kick-off (15/12/2025), identificación de stakeholders y matriz RACI (Tablas 2-3), inventario de fuentes y herramientas, catálogo de 48 reglas priorizadas (23 FW / 25 WAF), líneas base de MTTD/MTTR (Tablas 4-5)	—	SM	◆ Kick-off
2	Etapa 1	Descubrimiento y requisitos	Matriz de decisión IP origen/destino, política de auto-exposición aprobada (Tabla 6), requisitos de integración y conectividad (Tabla 7)	1	SM / AITA	◆ Política aprobada
3	Etapa 2	Diseño de arquitectura	Arquitectura del motor MCIA (Figura 11), plantillas de flujo FW y WAF (Figuras 12-13), diseño del risk score y del mecanismo de duplicación (Figura 14)	2	AA / AITA	
4	Etapa 2	Aprovisionamiento de infraestructura	VM aprovisionada con hardening, Docker/Nginx, Postgre SQL y Redis desplegados (Figura 15), VPN site-to-site operativa (Figura 16)	3	AA / Ingeniería	
5	Etapa 2	Desarrollo del core (cybersoc-api)	Módulos de ingesta y cierre de ofensas, contexto y caché, lista blanca y resolución de IP por regla CLD (Anexo B)	4	AA	
6	Etapa 2	Desarrollo de integraciones	Conectores de inteligencia de amenazas, Tenable, Cortex XDR, iTop y Gemini (Figuras 17-21), canales de bloqueo EDL y WAF (Figuras 22-23), microservicio email-api (Figura 25)	5	AA	
7	Etapa 2	Motor de decisión y respuesta	Cálculo del risk score con umbral ≥ 8 (Figuras 26-27), regla de auto-bloqueo con lista! (Figura 28), regla de análisis asistido por IA (Figura 29), detección de ofensa recurrente (Figura 30)	6	AA / AITA	
8	Etapa 2	Playbooks por regla	48 playbooks parametrizados sobre las dos plantillas de flujo (Figuras 31-32)	7	AA	
9	Etapa 2	Sistema web y dashboards	Dashboards de MTTD y MTTR, bitácora de ofensas y monitoreo en tiempo real (Figuras 33-36)	7	AA	
10	Etapa 3	Pruebas y QA	Pruebas unitarias, de integración, de volumen y de no duplicación validadas (Figuras 37-40)	8, 9	AA / SM	
11	Etapa 3	Piloto controlado	Piloto en modo observación sin auto-bloqueo, calibración de umbral y lista blanca (Figuras 41-44), aprobación del cliente (Figura 45)	10	AA / SM / Cliente	◆ Aprobación del cliente
12	Etapa 3	Despliegue a producción	Activación gradual del auto-bloqueo hasta cubrir las 48 reglas; validación post-despliegue	11	AA / SM	◆ Pase a producción
13	Etapa 4	Operación y mejora continua *	Monitoreo recurrente de KPIs por fuente (Figuras 46-47), reportería periódica (Figuras 48-49), carga semanal de Tenable (Figura 50), redefinición del rol del analista	12	SM / AITA	
14	Etapa 4	Cierre de la implementación	Medición final de MTTD/MTTR contra líneas base (Tablas 8-12), transferencia de conocimiento y manuales, lecciones aprendidas, conformidad del cliente del 28/04/2026 (Figura 51)	12	SM	◆ Conformidad de cierre

Figura A.1 **Diagrama de Gantt.** Fuente. Elaboración propia.

Anexo B
Evidencias de integración del orquestador MCIA

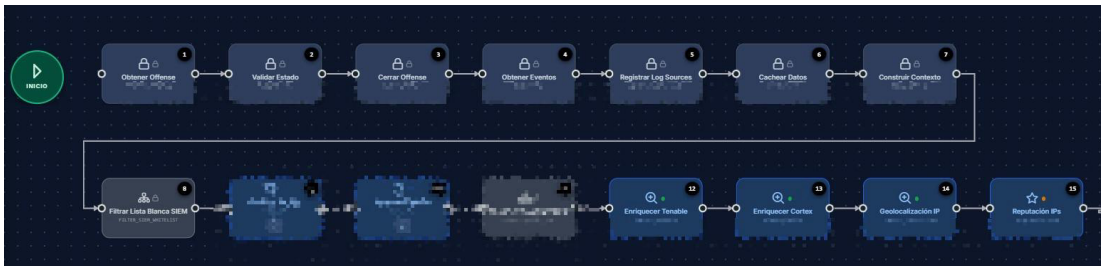


Figura B.1 **Flujo interno del módulo cybersoc-api (ingesta, contexto, caché y lista blanca).** Fuente. Elaboración propia a partir del orquestador MCIA. Datos sensibles anonimizados.

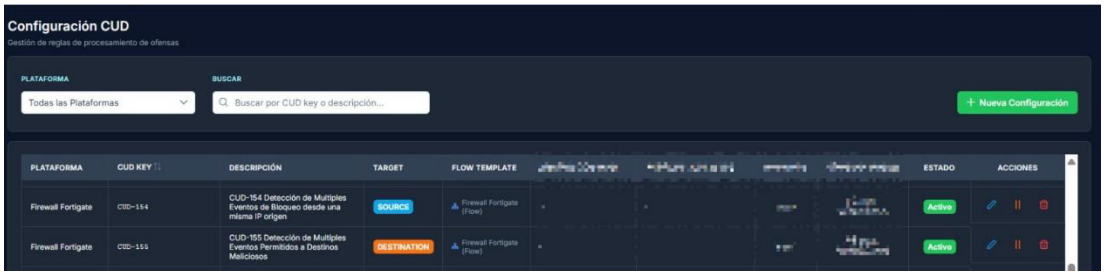


Figura B.2 **Panel de configuración CUD — matriz de decisión de IP origen/destino.**

Fuente. Elaboración propia a partir del orquestador MCIA. Datos sensibles anonimizados.

Anexo C
Registros del periodo posterior (abril de 2026)

El presente anexo muestra un extracto de la exportación de registros del orquestador MCIA correspondiente al periodo evaluado (abril de 2026). Los registros presentados son representativos del total de casos procesados en dicho periodo: 4031 de Firewall y 143 de WAF Akamai, sobre los cuales se calcularon los promedios de MTTD y MTTR reportados en la Tabla 8. Por cada caso se registra la fuente, el ticket, las fechas de detección, reporte y cierre, la severidad, los tiempos de MTTD y MTTR, y el tipo de gestión.

Plataforma	Ticket	ID Ofensa	Fecha Detección	Fecha Reporte	Fecha Cierre	Severidad	MTTD	MTTR	tectado Tiem	Falso Positivo	Impacto	Estado Ticket	Operador	Tipo de Reporte	Estado Gestión	Cierre Final
Firewall Forti	I-078231		30/04/26	30/04/26	30/04/26	MEDIA	0:01:54	0:00:48	SI	NO	NO	closed		Automático	Automático	SI
Firewall Forti	I-078230		30/04/26	30/04/26	30/04/26	MEDIA	0:01:58	0:00:45	SI	NO	NO	closed		Automático	Automático	SI
Firewall Forti	I-078229		30/04/26	30/04/26	30/04/26	BAJA	0:02:03	0:00:49	SI	NO	NO	closed		Automático	Automático	SI
Firewall Forti	I-078228		30/04/26	30/04/26	30/04/26	BAJA	0:01:53	0:01:04	SI	NO	NO	closed		Automático	Automático	SI
Firewall Forti	I-078227		30/04/26	30/04/26	30/04/26	BAJA	0:02:04	0:00:39	SI	NO	NO	closed		Automático	Automático	SI
Firewall Forti	I-078225		30/04/26	30/04/26	30/04/26	BAJA	0:01:58	0:00:53	SI	NO	NO	closed		Automático	Automático	SI
Firewall Forti	I-078224		30/04/26	30/04/26	30/04/26	BAJA	0:01:58	0:00:44	SI	NO	NO	closed		Automático	Automático	SI
Firewall Forti	I-078223		30/04/26	30/04/26	30/04/26	BAJA	0:02:13	0:01:00	SI	NO	NO	closed		Automático	Automático	SI
Firewall Forti	I-078222		30/04/26	30/04/26	30/04/26	BAJA	0:01:57	0:00:41	SI	NO	NO	closed		Automático	Automático	SI

Figura C.1 **Datos de la plataforma Firewall de abril 2026.** Fuente. Elaboración propia a partir del reporte del orquestador MCIA. Datos sensibles anonimizados.

Plataforma	Ticket	ID Ofensa	Fecha Detección	Fecha Reporte	Fecha Cierre	Severidad	MTTD	MTTR	tectado Tiem	Falso Positivo	Impacto	Estado Ticket	Operador	Tipo de Reporte	Estado Gestión	Cierre Final
WAF Akamai	I-077974		29/04/26	29/04/26	29/04/26	BAJA	0:01:37	0:01:06	SI	NO	NO	closed		Automático	Automático	SI
WAF Akamai	I-077971		29/04/26	29/04/26	29/04/26	MEDIA	0:01:24	0:01:15	SI	NO	NO	closed		Automático	Automático	SI
WAF Akamai	I-077968		29/04/26	29/04/26	29/04/26	BAJA	0:01:28	0:01:17	SI	NO	NO	closed		Automático	Automático	SI
WAF Akamai	I-077964		29/04/26	29/04/26	29/04/26	BAJA	0:01:13	0:01:16	SI	NO	NO	closed		Automático	Automático	SI
WAF Akamai	I-077947		29/04/26	29/04/26	29/04/26	BAJA	0:01:01	0:01:15	SI	NO	NO	closed		Automático	Automático	SI
WAF Akamai	I-077942		29/04/26	29/04/26	29/04/26	BAJA	0:01:50	0:01:23	SI	NO	NO	closed		Automático	Automático	SI
WAF Akamai	I-077633		28/04/26	28/04/26	28/04/26	BAJA	0:02:05	0:01:12	SI	NO	NO	closed		Automático	Automático	SI
WAF Akamai	I-077597		28/04/26	28/04/26	28/04/26	BAJA	0:02:02	0:01:13	SI	NO	NO	closed		Automático	Automático	SI

Figura C.2 **Datos de la plataforma WAF Akamai de abril 2026.** Fuente. Elaboración propia a partir del reporte del orquestador MCIA. Datos sensibles anonimizados.

Anexo D
Constancia de ejecución y conformidad del trabajo de suficiencia profesional

El presente anexo muestra la constancia emitida por la empresa el 11 de noviembre de 2026, en la cual se acredita la participación del autor en el análisis, diseño, implementación y puesta en operación del sistema de orquestación descrito en este informe, y se otorga la conformidad respecto a lo ejecutado. El documento se incluye con su autorización y se han ofuscado los datos sensibles.



INNOVATEC
Innovación en Tecnologías de Información

CONSTANCIA DE EJECUCIÓN Y CONFORMIDAD
DEL TRABAJO DE SUFICIENCIA PROFESIONAL

MC INNOVATEC S.A.C., con **RUC N° 20602823696**, debidamente representado por su Gerente General Sr. Ivor Mirko Cuba Cisneros,

por medio de la presente deja constancia que el señor:

ACUÑA GAMARRA GUILLERMO ALONSO

Identificado con , labora en la empresa desde el 19 de marzo de 2025 hasta la actualidad, cumpliendo las funciones de **SERVICE SECURITY MANAGER**, a cargo del equipo CyberSOC.

Durante el periodo comprendido entre diciembre 2025 y abril 2026, el Sr. Acuña participó en el análisis, diseño, implementación y puesta en operación en la empresa del trabajo titulado:

"IMPLEMENTACIÓN DE UN SISTEMA DE ORQUESTACIÓN EN CYBERSOC PARA DETECCIÓN Y RESPUESTA AUTOMATIZADA ANTE AMENAZAS PERIMETRALES DE UN CLIENTE CORPORATIVO"

Dicho trabajo consistió en la orquestación y automatización de procesos de monitoreo, detección y respuesta del CyberSOC, comprendiendo principalmente la integración de la plataforma SIEM de un cliente corporativo con el orquestador MCIA, la implementación de 48 reglas de detección con respuesta automatizada para las alertas del firewall y del WAF (Web Application Firewall), el bloqueo automático de direcciones IP maliciosas y el registro de los casos en la herramienta de gestión de tickets.

El trabajo fue culminado satisfactoriamente y se encuentra en operación, habiéndose obtenido como resultados la reducción del tiempo medio de detección (MTTD) a menos de 15 minutos y del tiempo medio de resolución (MTTR) a menos de 30 minutos, optimizando el tiempo del personal del CyberSOC y permitiendo reasignarlo a nuevas actividades que requieren mayor análisis. En consecuencia, MC INNOVATEC S.A.C. otorga su **CONFORMIDAD** respecto a lo ejecutado.

Se emite la presente a solicitud del interesado, para los fines que estime convenientes.

Lima, 11 de noviembre del 2026.

Atentamente,

Firmado digitalmente por:
CUBA CISNEROS IVOR MIRKO
RUC:20602823090
Motivo: Soy el autor del documento
Fecha: 11/11/2026 10:32:35-0500

LA EMPRESA
MC INNOVATEC SAC

Documento propiedad de MC INNOVATEC. Prohibido su reproducción total o parcial sin autorización.
El ejemplar impreso es copia No controlada de los sistemas de gestión de MC INNOVATEC.
Documento de uso confidencial
www.mcinnovatec.com / (511) 5548072 - (51)999192664 / Av. La Encalada 1163 - 1171 Of. 602 Santiago de Surco-Lima, Perú

Figura D.1 **Constancia de ejecución y conformidad del trabajo de suficiencia profesional.** Fuente. MC INNOVATEC S.A.C. (2026). Datos sensibles anonimizados.