



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería de Sistemas e Informática

Escuela Profesional de Ingeniería de Sistemas

**Automatización de la respuesta a incidentes de
ciberseguridad mediante XSOAR en una empresa del
rubro digital**

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Ingeniero de Sistemas

AUTOR

Jorge Luis MARQUEZ COAGUILA

ASESOR

Nilo Eloy CARRASCO ORÉ

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

Marquez, J. (2026). *Automatización de la respuesta a incidentes de ciberseguridad mediante XSOAR en una empresa del rubro digital*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Escuela Profesional de Ingeniería de Sistemas]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Jorge Luis Marquez Coaguila
Tipo de documento de identidad	DNI
Número de documento de identidad	75367135
URL de ORCID	https://orcid.org/0009-0002-4737-4870
Datos de asesor	
Nombres y apellidos	Nilo Eloy Carrasco Oré
Tipo de documento de identidad	DNI
Número de documento de identidad	09342780
URL de ORCID	https://orcid.org/0000-0001-5664-9309
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Santiago Domingo Moquillaza Henríquez
Tipo de documento	DNI
Número de documento de identidad	08280889
Miembro del jurado 1	
Nombres y apellidos	Raúl Marcelo Armas Calderón
Tipo de documento	DNI
Número de documento de identidad	07156168
Datos de investigación	
Línea de investigación	No aplica

Grupo de investigación	No aplica
Agencia de financiamiento	Sin financiamiento
Ubicación geográfica de la investigación	País: Perú Departamento: Lima
	Provincia: Lima Distrito: Cercado de Lima Jr. Carlos Amezaga No. 375 Universidad Nacional Mayor de San Marcos Latitud: -12.0564232 Longitud: -77.0843327
Año o rango de años en que se realizó la investigación	2025
URL de disciplinas OCDE	2.02.04 -- Ingeniería de sistemas y comunicaciones https://purl.org/pe-repo/ocde/ford#2.02.04



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
Escuela Profesional de Ingeniería de Sistemas

Acta Virtual de Sustentación
del Trabajo de Suficiencia Profesional

Siendo las 20:02 horas del día 02 de abril del año 2026, se reunieron virtualmente los docentes designados como Miembros de Jurado del Trabajo de Suficiencia Profesional, presidido por el Mg. Moquillaza Henríquez Santiago Domingo (Presidente), Ing. Armas Calderón Raúl Marcelo (Miembro) y el Ing. Carrasco Ore Nilo Eloy (Miembro Asesor), usando la plataforma Meet (<http://meet.google.com/hot-tmmg-afm>), para la sustentación virtual del Trabajo de Suficiencia Profesional intitulado: **“AUTOMATIZACIÓN DE LA RESPUESTA A INCIDENTES DE CIBERSEGURIDAD MEDIANTE XSOAR EN UNA EMPRESA DEL RUBRO DIGITAL”**, por el Bachiller **Marquez Coaguila Jorge Luis**; para obtener el Título Profesional de Ingeniero de Sistemas.

Acto seguido de la exposición del Trabajo de Suficiencia Profesional, el Presidente invitó al Bachiller a dar las respuestas a las preguntas establecidas por los miembros del Jurado.

El Bachiller en el curso de sus intervenciones demostró pleno dominio del tema, al responder con acierto y fluidez a las observaciones y preguntas formuladas por los señores miembros del Jurado.

Finalmente habiéndose efectuado la calificación correspondiente por los miembros del Jurado, el Bachiller obtuvo la nota de **18 (DIECIOCHO)**.

A continuación el Presidente de Jurados el Mg. Moquillaza Henríquez Santiago Domingo, declara al Bachiller **Ingeniero de Sistemas**.

Siendo las 20:55 horas, se levantó la sesión.

Presidente

Mg. Moquillaza Henríquez Santiago Domingo

Miembro

Ing. Armas Calderón Raúl Marcelo

Miembro Asesor

Ing. Carrasco Ore Nilo Eloy



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

CERTIFICADO DE SIMILITUD

Yo, Nilo Eloy Carrasco Ore en mi condición de asesor acreditado mediante Resolución Decanal N° 001268-2025-D-FISI/UNMSM y OFICIO N° 009-PTTSP-FISI-2025 del Trabajo de Suficiencia Profesional, cuyo título es Automatización de la Respuesta a Incidentes de Ciberseguridad mediante XSOAR en una empresa del rubro digital, presentado por el bachiller Marquez Coaguila Jorge Luis para optar el Título Profesional de Ingeniero de Sistemas, 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 5% 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 **TITULO PROFESIONAL DE INGENIERO DE SISTEMAS.**

Lima, 4 de junio de 2026

Firma del Asesor:

Nombres y Apellidos del asesor: Nilo Eloy Carrasco Ore

DNI: 09342780

FICHA CATALOGRÁFICA

AUTOMATIZACIÓN DE LA RESPUESTA A INCIDENTES DE CIBERSEGURIDAD MEDIANTE XSOAR EN UNA EMPRESA DEL RUBRO DIGITAL

AUTOR: MARQUEZ COAGUILA JORGE LUIS

ASESOR: CARRASCO ORÉ NILO ELOY

LIMA – PERÚ, 2025

TÍTULO PROFESIONAL: Título Profesional de Ingeniero de Sistemas.

ÁREA / PROGRAMA / LÍNEA DE INVESTIGACIÓN:

Ingenierías / Tecnología de Información y Comunicación / Ingeniería de Software

PREGRADO: Universidad Nacional Mayor de San Marcos -
Facultad de Ingeniería de Sistemas e Informática - Escuela profesional de
Ingeniería de Sistemas

Formato 21 x 29.7 cm

Páginas: viii, 79

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

**Automatización de la Respuesta a Incidentes de Ciberseguridad con XSOAR en
una empresa del rubro digital**

Autor: Marquez Coaguila, Jorge Luis

Asesor: Carrasco Oré, Nilo Eloy

Título: Trabajo de Suficiencia Profesional para optar el Título Profesional de
Ingeniero de Sistemas

Fecha: Diciembre de 2025

RESUMEN

El presente trabajo tiene como objetivo describir la implementación de un proyecto de estandarización y automatización de procesos de respuesta a incidentes de ciberseguridad mediante la plataforma Cortex XSOAR en una empresa multinacional del rubro digital dedicada al desarrollo y publicación de videojuegos. La problemática inicial se originó tras la adquisición y consolidación de diversos sellos editoriales, lo que generó diferencias en procedimientos, herramientas y flujos de trabajo en los equipos de seguridad y una sobrecarga operacional para los analistas.

Ante este contexto, se planteó como objetivo central unificar procesos en un entorno consolidado, mejorar la eficiencia operativa y reducir los tiempos de respuesta (MTTR) frente a incidentes. La metodología utilizada incluyó la revisión, documentación y adaptación de procedimientos existentes, el diseño de playbooks automatizados y la estandarización de campos y flujos en la gestión de tickets. Asimismo, se desarrollaron plantillas de comunicación para la atención de reportes de usuarios y se coordinó con equipos internos de infraestructura y seguridad de producto para integrar acciones de respuesta automatizada.

La experiencia permitió constatar que la centralización de procesos en XSOAR no solo optimizó la consistencia de la gestión de incidentes y facilitó la escala operativa del SOC, sino que también fortaleció la colaboración entre equipos globales, garantizando la capacidad de adaptación frente a un panorama de ciberamenazas en constante evolución.

Palabras claves: ciberseguridad, SOC, XSOAR, automatización, respuesta a incidentes, runbooks.

NATIONAL MAJOR UNIVERSITY OF SAN MARCOS

FACULTY OF SYSTEMS AND INFORMATICS ENGINEERING

PROFESSIONAL SCHOOL OF SYSTEM ENGINEERING

Implementation of Cortex XSOAR for the automation of cybersecurity incident management in a digital sector development company

Autor: Marquez Coaguila, Jorge Luis

Advisor: Carrasco Oré, Nilo Eloy

Title: Professional Sufficiency Work to opt for the Professional Title of Systems Engineer

Date: December 2025

ABSTRACT

The objective of this work is to describe the implementation of a project to standardize and automate cybersecurity incident response processes using the Cortex XSOAR platform in a multinational digital company dedicated to the development and publication of video games. The initial problem arose after the acquisition and consolidation of various publishing labels, which led to differences in procedures, tools, and workflows among security teams and an operational overload for analysts.

Given this context, the main objective was to unify processes in a consolidated environment, improve operational efficiency, and reduce response times (MTTR) to incidents. The methodology used included reviewing, documenting, and adapting existing procedures, designing automated playbooks, and standardizing fields and flows in ticket management. Communication templates were also developed by the soc team to address user reports, and coordination took place with internal infrastructure and product security teams to integrate automated response actions.

The experience showed that centralizing processes in XSOAR not only optimized the consistency of incident management and facilitated the operational scale of the SOC, but also strengthened collaboration between global teams, ensuring adaptability in the constantly evolving cyber threat landscape.

Keywords: cybersecurity, SOC, XSOAR, automation, incident response, runbooks.

ÍNDICE GENERAL

RESUMEN	iii
ABSTRACT	iv
ÍNDICE GENERAL	v
INTRODUCCIÓN.....	1
CAPÍTULO I – TRAYECTORIA PROFESIONAL.....	3
CAPÍTULO II - CONTEXTO EN EL QUE SE DESARROLLA LA EXPERIENCIA	6
2.1 Empresa – Actividad que realiza	6
2.2 Misión.....	7
2.3 Visión	8
2.4 Organización de la empresa	8
2.5 Área, cargo y funciones desempeñadas.....	10
2.6 Experiencia profesional realizada en la organización	11
CAPÍTULO III – ACTIVIDADES DESARROLLADAS	13
3.1 Situación problemática.....	13
Análisis de métricas operativas del SOC.....	15
3.1.1 Definición del problema.....	16
3.2 Solución.....	17
3.2.1 Objetivos	21
3.2.1.1 Objetivo General	21
3.2.1.2 Objetivos Específicos.....	21
3.2.2 Alcance.....	22
Limitaciones del alcance.....	23
3.2.3 Etapas y Metodología	23
Fundamentación de la metodología utilizada	23
Definición de conceptos clave utilizados en el proyecto	25

3.2.4 Fundamentos Utilizados.....	26
Marco normativo y de buenas prácticas	26
NIST Cybersecurity Framework (CSF).....	26
ISO/IEC 27035	27
MITRE ATT&CK Framework.....	27
Fundamentos tecnológicos	27
Security Orchestration, Automation and Response (SOAR)	27
Security Information and Event Management (SIEM)	27
Endpoint Detection and Response (EDR)	28
Gestión de tickets y comunicaciones internas	28
Estimación de complejidad en puntos de historia	28
Roles involucrados en la implementación	31
3.2.5 Implementación de las áreas, procesos, sistemas y buenas prácticas	32
3.2.5.1 Arquitectura funcional y de integraciones	33
3.2.5.2 Gobierno corporativo y roles	36
Etapas desarrolladas como sprints funcionales.....	38
3.2.5.3 Playbook de Phishing.....	43
3.2.5.4 Playbook de Malware / Endpoint Detection and Response (EDR)	48
3.2.5.5 Playbook de Accesos Sospechosos / Identidad.....	57
3.2.5.6 Observabilidad y visibilidad operativa	60
3.2.5.7 Calidad, seguridad y resiliencia de las automatizaciones.....	65
3.3 Evaluación.....	67
3.3.1 Evaluación económica	67
3.3.2 Interpretación del VAN y TIR.....	70
CAPITULO IV – REFLEXIÓN CRÍTICA DE LA EXPERIENCIA.....	73

CAPITULO V – CONCLUSIONES Y RECOMENDACIONES.....	73
5.1. Conclusiones.....	73
5.2. Recomendaciones.....	74
5.3 Fuentes de información.....	75
5.4 Glosario.....	77
ANEXOS.....	79

Figura 1 Organigrama enfocado en subárea “Centro de Operaciones de Seguridad y Ciberdefensa”	10
Figura 2 Organigrama enfocado en subárea “Centro de Operaciones de Seguridad y Ciberdefensa”	10
Figura 3 Consecuencias de la sobrecarga operativa del SOC	15
Figura 4 Consecuencias de la sobrecarga operativa del SOC	15
Figura 5 Centralización de procesos de seguridad en Cortex XSOAR...	21
Figura 6 Centralización de procesos de seguridad en Cortex XSOAR...	21
Figura 5 Centralización de procesos de seguridad en Cortex XSOAR...	21
Figura 7 Modelo propuesto por Palomino et al., 2024.....	25
Figura 8 Modelo propuesto por Palomino et al., 2024.....	25
Figura 11 Topología lógica de integraciones	34
Figura 12 Topología lógica de integraciones	34
Figura 9 Ciclo iterativo de implementación de XSOAR en el SOC	40
Figura 10 Ciclo iterativo de implementación de XSOAR en el SOC	40
Figura 13 Ejemplo de ejecución parcial del playbook de phishing.....	47
Figura 14 Ejemplo de ejecución parcial del playbook de phishing.....	47
Figura 15 Agrupación automatizada de incidentes de phishing en campañas.....	48
Figura 16 Agrupación automatizada de incidentes de phishing en campañas.....	48
Figura 17 Diagrama del Playbook Unisolate Endpoint.....	53
Figura 18 Diagrama del Playbook Unisolate Endpoint.....	53
Figura 19 Diagrama funcional del playbook Endpoint Malware Investigation – Generic.....	54
Figura 20 Diagrama funcional del playbook Endpoint Malware Investigation – Generic.....	54
Figura 21 <i>Flujo de remediación ante accesos sospechosos (SSO)</i> ...	58
Figura 22 <i>Flujo de remediación ante accesos sospechosos (SSO)</i> ...	58
Figura 23 Visualización de alertas en el dashboard de Cortex XSOAR..	62
Figura 24 Visualización de alertas en el dashboard de Cortex XSOAR..	62
Figura 25 Notificación automatizada del Demisto Bot en Slack.....	64

INTRODUCCIÓN

El presente trabajo de suficiencia profesional tiene como objetivo describir la implementación de un proyecto orientado a la mejora de procesos en el área de ciberseguridad, con especial enfoque en la gestión de alertas, el análisis de incidentes y la estandarización de procedimientos a través de la plataforma Cortex XSOAR. La experiencia se desarrolla en el contexto de un Centro de Operaciones de Seguridad (SOC) de una empresa multinacional dedicada al desarrollo y publicación de videojuegos, un sector altamente dinámico que enfrenta de manera constante riesgos asociados a ciberamenazas.

El problema principal que se identificó estuvo relacionado con la falta de homogeneidad en los procesos y herramientas empleadas por los equipos de seguridad, situación que se acentuó tras la integración de distintos sellos editoriales dentro de la compañía. Este escenario generó diferencias en los flujos de trabajo, duplicidad de esfuerzos y una sobrecarga operativa para los analistas, quienes debían adaptarse a procedimientos distintos según cada entorno. Ante ello, se consideró fundamental avanzar hacia la consolidación y centralización de los procesos de respuesta a incidentes, buscando garantizar consistencia, eficiencia y colaboración global.

El proyecto planteado tuvo como objetivo principal la optimización de la gestión de incidentes a través de la implementación de Cortex XSOAR como plataforma central de orquestación y automatización. Con este enfoque, se buscó reducir los tiempos medios de respuesta (MTTR), estandarizar la atención de incidentes y fortalecer la transferencia de conocimiento dentro del equipo. La estrategia contempló no solo la automatización de tareas técnicas mediante playbooks, sino también la elaboración de procedimientos operativos estándar (SOPs), la documentación de flujos de trabajo y la creación de plantillas de comunicación para reportes de usuarios.

El desarrollo del trabajo se realizó bajo un enfoque iterativo, ajustando las soluciones en función de la práctica diaria y de la evolución de las amenazas y necesidades del SOC. Este dinamismo permitió implementar mejoras sostenibles y

adaptables, en línea con la naturaleza cambiante de la ciberseguridad. Además, se tomaron como referencia marcos internacionales reconocidos, entre ellos el NIST Cybersecurity Framework y MITRE ATT&CK, que aportaron buenas prácticas y lineamientos para validar la efectividad de las acciones emprendidas.

El valor del proyecto no radicó únicamente en la automatización, sino también en la capacidad de centralizar la gestión de incidentes y fomentar la colaboración entre equipos distribuidos en diferentes regiones. Este aspecto resultó clave en un entorno globalizado, donde la coordinación y la estandarización de procesos se convierten en factores determinantes para mantener la resiliencia operativa frente a amenazas cada vez más sofisticadas.

La estructura del documento se organiza de la siguiente manera:

- **Capítulo I:** Presenta la trayectoria profesional del autor, describiendo la experiencia laboral, la formación académica y las certificaciones obtenidas en el campo de la ciberseguridad.
- **Capítulo II:** Expone el contexto de la organización, su misión, visión, estructura y el rol desempeñado en el área de seguridad.
- **Capítulo III:** Define la situación problemática, los objetivos del proyecto, la solución planteada, así como la metodología y fundamentos teóricos aplicados en su ejecución.
- **Capítulo IV:** Contiene la reflexión crítica de la experiencia, con los aprendizajes y limitaciones encontrados durante el desarrollo del trabajo.
- **Capítulo V:** Reúne las conclusiones y recomendaciones del proyecto, resaltando los aportes y el impacto generado en la organización.

Finalmente, se incluyen las fuentes de información consultadas y los anexos que complementan el desarrollo del trabajo.

CAPÍTULO I – TRAYECTORIA PROFESIONAL

El autor se desempeña como Analista de Ciberseguridad en una compañía internacional dedicada al desarrollo de videojuegos de alcance global, participando activamente en la implementación y optimización del SOC global. Su experiencia incluye la gestión de incidentes, análisis de alertas, automatización de procesos y desarrollo de runbooks y SOPs, así como la integración de herramientas de monitoreo y protección de endpoints. Ha trabajado también en soporte técnico y administración de redes, contribuyendo al fortalecimiento de la seguridad de la información y a la mejora continua de los procesos operativos, aplicando estándares y marcos reconocidos en la industria, como NIST y MITRE ATT&CK. Los detalles se describen en la Tabla 1:

Tabla 1

Experiencias Laborales

Empresa / Período	Descripción de actividades realizadas
Aynitech (2021 – Actualidad)	Cargo: Analista de Ciberseguridad Senior Actividades: Monitoreo y administración de alertas de seguridad en plataformas SIEM para cliente en USA. Soporte en la implementación de controles basados en ISO 27001 y políticas internas de seguridad de la información. Implementación de Palo Alto Cortex XSOAR y diseño de playbooks para la automatización de respuestas.

Gestión y análisis de incidentes de ciberseguridad.

Tivit
(enero 2021 – julio 2021)

Cargo: Practicante de Tecnologías de la Información

Actividades: Mantenimiento de laboratorios; instalación y gestión de puntos de red; soporte a oficinas administrativas en hardware, software y redes; administración del inventario de equipos.

La educación académica del autor se detalla en la Tabla 2:

Tabla 2

Educación Académica

Período	Educación Académica
2015 - 2020	Grado Académico de Bachiller en Ingeniería de Software Escuela Académico Profesional de Ingeniería de Software Facultad de Ingeniería de Sistemas e Informática Universidad Nacional Mayor de San Marcos

Los cursos realizados por el autor se muestran en la tabla 3:

Tabla 3*Cursos realizados*

Institución	Curso
VMedu	Scrum Fundamentals
LinkedIn Learning	CompTIA Security+ (SY0-601)
ERCA	ISO 27032 Lead Cybersecurity Manager
Malwarebytes	Malwarebytes Endpoint Detection & Response Fundamentals
LACNIC	Introducción a la gestión de redes

Las certificaciones logradas por el autor se reseñan en la Tabla 4:

Tabla 4*Certificaciones del autor*

Período	Certificación	Institución
2024	Scrum Fundamentals	VMedu

2021	CompTIA Security+ (SY0-601)	CompTIA
2021	ISO 27032 Lead Cybersecurity Manager	ERCA
2021	Malwarebytes Endpoint Detection & Response Fundamentals	Malwarebytes
2021	Introducción a la gestión de redes	LACNIC

CAPÍTULO II - CONTEXTO EN EL QUE SE DESARROLLA LA EXPERIENCIA

2.1 Empresa – Actividad que realiza

La organización en la que se desarrolló la experiencia profesional es una compañía multinacional de entretenimiento digital con una presencia sólida en distintos continentes y con operaciones consolidadas en los mercados de Norteamérica, Europa, Asia y Latinoamérica. Su campo de acción principal está orientado al desarrollo, publicación y distribución de videojuegos de alcance global, los cuales abarcan desde producciones de gran presupuesto hasta títulos destinados a audiencias casuales. A través de los años, la empresa ha logrado posicionarse como referente en la industria, destacando por su capacidad de innovación, el uso de motores gráficos avanzados y la incorporación de narrativas complejas que permiten experiencias inmersivas y adaptadas a distintos públicos.

El modelo de negocio combina de manera equilibrada la venta tradicional de títulos en formato físico y digital con esquemas más recientes como las expansiones descargables, contenido adicional de pago, micropagos y servicios de suscripción, lo que

le ha permitido diversificar ingresos y asegurar la sostenibilidad de largo plazo. A esto se suma la provisión de servicios en línea, conocidos como *LiveOps*, que garantizan el funcionamiento continuo de los servidores y la generación periódica de contenido dinámico para mantener la atención de las comunidades de jugadores. Estas operaciones requieren una infraestructura tecnológica robusta y equipos especializados capaces de gestionar grandes volúmenes de usuarios simultáneos en distintas regiones del mundo. De hecho, se estima que los juegos móviles que aplican LiveOps generan en promedio 30 veces más ingresos que títulos que no utilizan ese modelo (Sensor Tower, 2023).

En el marco de su estrategia de expansión, la empresa apostó por el mercado de videojuegos móviles, reconociendo que este segmento concentra actualmente la mayor parte de la participación global en la industria. La adquisición de un desarrollador líder en este ámbito implicó una operación valorada en aproximadamente \$12 mil millones como valor empresarial, lo que incluyó pagos en acciones y efectivo, además de estimaciones de sinergias de costos de alrededor de USD 100 millones anuales durante los dos primeros años y oportunidades de ingresos adicionales superiores a los USD 500 millones con el tiempo (T2 Interactive, 2022).

Las actividades de esta envergadura, junto con el crecimiento proyectado del mercado global, donde se estima que los ingresos aumenten desde aproximadamente USD 298.98 mil millones en 2024 hasta USD 600.74 mil millones para 2030 a una tasa compuesta anual de alrededor del 12.2% (Grand View Research, 2024), demandan un enfoque estratégico en innovación tecnológica, monetización diversificada y resiliencia operativa. La magnitud de estas actividades implica también una responsabilidad elevada en términos de seguridad digital y protección de datos. Dado que los videojuegos modernos operan como ecosistemas interconectados que almacenan información sensible de millones de usuarios y procesan transacciones en tiempo real, la empresa ha invertido de manera sistemática en la consolidación de centros de operaciones de seguridad y en la implementación de soluciones de orquestación y automatización que permitan responder con rapidez a incidentes de ciberseguridad.

2.2 Misión

La misión de la empresa se centra en crear experiencias de entretenimiento interactivo de alta calidad que sean disfrutadas por jugadores de todo el mundo. Su enfoque está en desarrollar y publicar videojuegos innovadores que combinen creatividad y tecnología, asegurando que cada título ofrezca valor y diversión a los usuarios, al tiempo que mantiene estándares de excelencia en el contenido y en la entrega de sus productos (DCFmodeling, 2025).

2.3 Visión

La visión de la empresa es consolidarse como un referente global en la industria del entretenimiento interactivo, destacando por la calidad de sus videojuegos y su éxito comercial. La organización apuesta por la innovación constante, la creación de franquicias sólidas y el fortalecimiento de sus capacidades de desarrollo, para adaptarse a la evolución del mercado y generar un impacto duradero en la comunidad de jugadores (DCFmodeling, 2025).

2.4 Organización de la empresa

La empresa se estructura en diversas áreas funcionales, cada una con responsabilidades claramente definidas que contribuyen al logro de la misión y visión corporativa, que se presentará a continuación.

Entre estas áreas destacan las siguientes:

- **Dirección Estratégica:** Define la misión, visión y objetivos generales de la organización, asegurando la alineación de todas las áreas con la estrategia corporativa.
- **Recursos Humanos y Talento:** Gestiona la captación, desarrollo y retención de talento, promoviendo un entorno laboral que favorezca la colaboración y el crecimiento profesional.

- **Desarrollo de Productos:** Responsable de la concepción, desarrollo y mejora continua de los videojuegos, coordinando con múltiples equipos para garantizar la calidad y el cumplimiento de los plazos de entrega.
- **Operaciones y Tecnología:** Gestiona la infraestructura tecnológica, asegura la continuidad del negocio y mantiene la eficiencia operativa de las plataformas digitales.
- **Seguridad y Gestión de Riesgos:** Protege los activos digitales y la información crítica de la organización, gestionando amenazas, vulnerabilidades y asegurando la resiliencia operativa, incluyendo el Centro de Operaciones de Seguridad (SOC) global.
- **Finanzas:** Supervisa la gestión de los recursos financieros, asegura la sostenibilidad económica y proporciona información para la toma de decisiones estratégicas.
- **Marketing y Comunicación:** Desarrolla estrategias de comunicación y promoción de los productos, asegurando la correcta difusión de los lanzamientos y el fortalecimiento de la marca.
- **Clientes y Experiencia:** Esta área se centra en optimizar la experiencia de los jugadores y clientes, resolviendo requerimientos y manteniendo un alto nivel de satisfacción y fidelización.

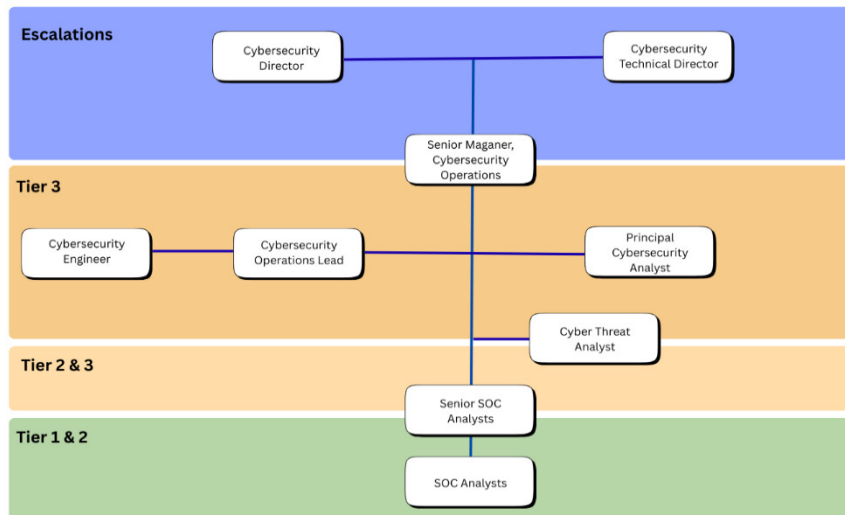
Dentro de esta estructura, el área de ciberseguridad tiene un rol esencial en la protección de activos críticos y en la garantía de la resiliencia operacional. Esta área gestiona tanto los aspectos técnicos como los normativos de la seguridad digital, asegurando el cumplimiento de estándares internacionales y la implementación de medidas preventivas frente a riesgos.

Un componente fundamental de esta división es el Centro de Operaciones de Seguridad, cuya función principal es la detección, análisis y respuesta a incidentes de seguridad en tiempo real. El SOC opera de forma jerarquizada en niveles (Tiers 1, 2 y 3), lo que permite distribuir las funciones según la complejidad de los incidentes y asegurar una adecuada escalabilidad de procesos.

Para el presente proyecto, el enfoque se centró en el área de Seguridad y Gestión de Riesgos, específicamente dentro del equipo encargado del SOC global, como se aprecia en la Figura 1.

Figura 1

Organigrama enfocado en subárea “Centro de Operaciones de Seguridad y Ciberdefensa”



Nota. Fuente: Elaboración Propia, adaptación del organigrama de la subárea SOC&CD.

2.5 Área, cargo y funciones desempeñadas

El autor se desempeñó como Analista de Ciberseguridad en el Centro de Operaciones de Seguridad global, participando activamente en la gestión de incidentes, análisis de alertas y automatización de procesos de seguridad mediante la implementación y mejora de runbooks y SOPs. Entre sus funciones se incluyen:

- Investigación y análisis de incidentes de seguridad utilizando herramientas de monitoreo, protección de endpoints y plataformas SOAR (Splunk, SentinelOne, Cortex XSOAR, etc).
- Implementación de integraciones y flujos automatizados para reducir los tiempos de atención de alertas y mejorar la eficiencia operativa del SOC.

- Coordinación con equipos internacionales para la gestión de incidentes y respuesta ante amenazas.
- Desarrollo y actualización de procedimientos operativos estándar y runbooks, promoviendo la estandarización y la transferencia de conocimiento dentro del equipo.
- Realización de simulaciones de phishing, capacitaciones internas y pruebas de concienciación de seguridad para distintos equipos.
- Apoyo en el seguimiento y reporte de métricas clave, incluyendo MTTR y MTTA, para medir el desempeño del SOC y la efectividad de los procesos implementados.

2.6 Experiencia profesional realizada en la organización

El autor del presente trabajo llevó a cabo la adaptación, documentación y estandarización de procedimientos de respuesta sobre la plataforma Cortex XSOAR como parte de la mejora operativa del área de ciberseguridad de la organización.

La experiencia profesional se desarrolló en un contexto de transformación organizacional, en el cual la compañía enfrentaba el reto de integrar nuevas líneas de negocio y garantizar la seguridad de una infraestructura tecnológica en expansión. Durante este proceso, se identificaron limitaciones en la gestión de incidentes, especialmente relacionadas con la cantidad de alertas recibidas, la falta de estandarización en los procesos de análisis y la necesidad de optimizar los tiempos de respuesta.

Esta labor incluyó la implementación, optimización y seguimiento de diversas actividades críticas para la gestión de la seguridad informática, destacando entre ellas las siguientes:

- Monitoreo y análisis de alertas de seguridad mediante la herramienta SIEM Splunk, identificando amenazas, incidentes y vulnerabilidades y asegurando la activación adecuada de los protocolos de respuesta establecidos.

- Investigación de logs de usuarios y sistemas para detectar incidentes de seguridad y vulnerabilidades reportadas, incluyendo la identificación y evaluación de phishing y otros ataques informáticos.
- Documentación y adaptación de playbooks existentes, como el Phishing Investigation Playbook, para integrarlos al entorno corporativo consolidado que abarca los sellos editoriales de la organización, incluyendo integraciones con EDR, SIEM y plataformas de correo, asegurando su correcta operación y automatización.
- Creación y mantenimiento de plantillas automáticas por tipo de reporte (spam, malicioso, legítimo o simulación) y estandarización de campos críticos en los tickets (propietario, sitio, severidad, fase) para garantizar trazabilidad y cumplimiento de auditoría en las automatizaciones.
- Colaboración con equipos de SRE, Cloud Owners y Product Security para automatizar tareas operativas como apertura de tickets, bloqueo de IPs, restricciones de acceso a la red en endpoints, etc.
- Elaboración y actualización de runbooks y SOPs para optimizar la respuesta a incidentes, asegurando eficacia, trazabilidad y cumplimiento de los protocolos de seguridad.
- Propuesta de mejoras y recomendaciones para fortalecer políticas, procedimientos y la infraestructura tecnológica, mitigando riesgos y promoviendo eficiencia en los procesos de seguridad.
- Análisis de inicios de sesión, vulnerabilidades y patrones de comportamiento de usuarios y sistemas para anticipar riesgos y reforzar la seguridad interna de la empresa.

Estas actividades permitieron al autor desarrollar competencias en gestión de incidentes, detección de phishing y demás casos de correo malicioso, automatización y optimización de procesos de seguridad informática, contribuyendo significativamente al fortalecimiento del área de ciberseguridad y al cumplimiento de los objetivos estratégicos de la organización.

CAPÍTULO III – ACTIVIDADES DESARROLLADAS

3.1 Situación problemática

En los últimos años, la empresa sobre la que se desarrolla el presente informe enfrentaba un escenario desafiante en materia de ciberseguridad. Aunque se habían realizado inversiones en infraestructura tecnológica y se disponía de procesos de monitoreo, las limitaciones en la gestión de incidentes se manifestaban de manera recurrente en la operación del Centro de Operaciones de Seguridad.

A nivel global, los ciberataques muestran un crecimiento sostenido en frecuencia y sofisticación. El IBM Cost of a Data Breach Report 2024 indicó que el costo promedio de una filtración de datos alcanzó los USD 4.88 millones, lo que representa un incremento del 10 % respecto al año anterior (IBM, 2024). Asimismo, el Verizon Data Breach Investigations Report (DBIR) 2024 señala que el 74 % de los incidentes a nivel mundial involucran un factor humano, lo que demuestra que los procesos manuales y poco estandarizados incrementan los riesgos y las pérdidas potenciales (Verizon, 2024).

En el ámbito regional, un informe de Deloitte (2023) reveló que en Latinoamérica solo el 7 % del presupuesto de TI se destina a ciberseguridad, por debajo del promedio global de 10 %. En el caso de Perú, las cifras son aún más alarmantes: durante el primer semestre de 2024 se detectaron 909,830 amenazas cibernéticas, convirtiéndolo en el país más afectado de la región (ESET, 2024). En paralelo, las denuncias por ciberdelitos ascendieron a 20,704 casos entre enero y junio de 2024, lo que significó un incremento del 61 % respecto al mismo periodo de 2023 (Ministerio Público, 2024).

A nivel local, la organización ya contaba con un SOC operativo, pero con automatizaciones limitadas, puntuales y no integradas con las distintas herramientas de seguridad. Por ejemplo, se disponía de filtros básicos para correos sospechosos y algunas plantillas para generación de reportes, pero la mayoría de los procesos continuaba siendo manual. Esta situación generaba duplicidad de tareas, inconsistencias en las respuestas de

los distintos equipos y un incremento significativo en los tiempos medios de detección y respuesta (MTTD y MTTR).

Adicionalmente, en 2022 la organización atravesaba un proceso de adquisición corporativa, lo cual incrementó las exigencias en términos de cumplimiento normativo y estandarización de procesos. Esta integración generó heterogeneidad en los procedimientos de seguridad, uso de herramientas diversas y flujos de trabajo no estandarizados, lo cual dificultaba la coordinación entre equipos globales. El SOC recibía diariamente un alto volumen de alertas provenientes de diferentes fuentes: SIEM (Splunk), soluciones EDR (CrowdStrike, SentinelOne), correo electrónico (Proofpoint, PhishER), y sistemas internos de ticketing (ServiceNow, Jira). La falta de integración entre estas plataformas obligaba a los analistas a realizar tareas manuales repetitivas, como búsquedas de indicadores de compromiso (IOCs), validación de reputación en múltiples bases de datos y generación manual de tickets para la gestión de incidentes (ASIS, 2023). Esta situación impulsó la decisión de implementar una solución más consistente y escalable, teniendo en cuenta que diversos estudios internacionales evidencian que los equipos de los Centros de Operaciones de Seguridad (SOC) enfrentan altos niveles de sobrecarga operativa y agotamiento profesional. En este contexto, se identifican factores como el incremento de la carga de trabajo, la sobrecarga de información y la complejidad operativa como principales detonantes del desgaste del personal. Esta problemática se ilustra en la Figura 2.

Figura 2

Consecuencias de la sobrecarga operativa del SOC



Nota: Tomada de "SOC team members battle with burnout, overload and chaos", Help Net Security, 2020

Como se aprecia en la Figura 2, el 75% de los encuestados señala que el incremento de la carga de trabajo es la principal causa de agotamiento, mientras que el 67% identifica la sobrecarga de información como un problema creciente, lo cual refuerza la necesidad de soluciones de automatización.

Análisis de métricas operativas del SOC

La Tabla 5 presenta una comparación de las principales métricas operativas del Centro de Operaciones de Seguridad antes y después de la automatización de los procesos de respuesta a incidentes de ciberseguridad. Los valores correspondientes al escenario previo evidencian limitaciones significativas en la gestión de incidentes, reflejadas en elevados tiempos de respuesta y resolución, así como en un porcentaje considerable de falsos positivos.

Tabla 5
Comparación de tiempos de resolución de incidentes en el SOC

Métrica	Antes de la automatización	Después de la automatización (con XSOAR)
Tiempo medio de detección (MTTD)	8 horas	2 horas
Tiempo medio de respuesta (MTTR)	12 horas	3 horas
Porcentaje de Falsos Positivos	40%	15%
Incidentes críticos resueltos en <24h	55%	90%

Nota: Fuente: elaboración propia basada en métricas operativas del SOC, 2025.

La adopción de procesos de orquestación y automatización mediante SOAR permitió reducir de manera significativa los tiempos de resolución, optimizando el ciclo de vida de los incidentes. Como se observa en la Tabla 5, el MTTD y el MTTR experimentaron mejoras sustanciales, lo cual evidencia la eficiencia de los playbooks y la reducción de la intervención manual.

3.1.1 Definición del problema

Problema general

La escasa automatización de los procesos operacionales de ciberseguridad en la empresa del rubro digital, que influye de manera negativa en la respuesta a incidentes de ciberseguridad.

Problemas específicos

- Poca integración entre las principales herramientas de seguridad de la organización (SIEM, EDR, correo, ticketing, comunicación) en un entorno centralizado.
- Falta de estandarización de los diseños y documentación de playbooks automatizados para la atención de incidentes de ciberseguridad.
- Ausencia de una definición de los campos y procedimientos en la gestión de incidentes de seguridad, asegurando consistencia entre los diferentes entornos de la organización.
- Carencia de mecanismos de comunicación directa con usuarios internos para mejorar la respuesta frente a incidencias de seguridad.

3.2 Solución

La solución propuesta se diseñó para responder de manera directa a la problemática identificada en la operación del Centro de Operaciones de Seguridad, abordando la escasa automatización, la limitada integración entre herramientas y la ausencia de estandarización en los procesos de respuesta y resolución de incidentes de ciberseguridad.

Para este fin, se planteó la implementación de una plataforma de orquestación, automatización y respuesta en seguridad (SOAR), seleccionándose Cortex XSOAR como herramienta central de la solución. La elección de esta plataforma respondió a una decisión a nivel organizacional por parte de la alta dirección, que además estuvo alineada con los lineamientos corporativos definidos tras el proceso de adquisición de la empresa, orientados a la estandarización de tecnologías de seguridad y a la adopción de soluciones con alcance global.

Adicionalmente, Cortex XSOAR fue seleccionado por su capacidad de integrar múltiples soluciones de seguridad en un entorno centralizado, su flexibilidad para el diseño de playbooks automatizados y su soporte para entornos corporativos distribuidos, características que permitieron abordar de manera efectiva los problemas específicos identificados en la gestión de incidentes de ciberseguridad (Palo Alto Networks, 2024).

La solución no solo buscó resolver problemas operativos inmediatos, sino también fortalecer la madurez del SOC frente a auditorías internacionales, optimizar el uso de los

recursos disponibles y reducir los tiempos de respuesta y resolución ante incidentes de ciberseguridad.

La solución contempló las siguientes líneas de acción, las cuales fueron implementadas de manera progresiva mediante etapas de trabajo estructuradas en Sprints.

Sprint 0 – Planificación del proyecto

El Sprint 0 correspondió a la etapa inicial de planificación y preparación del proyecto, cuyo objetivo principal fue establecer las bases metodológicas, técnicas y operativas necesarias para la posterior implementación de los sprints orientados a la automatización de la respuesta a incidentes de ciberseguridad mediante Cortex XSOAR. A diferencia de los sprints posteriores, este sprint no estuvo enfocado en la entrega de automatizaciones funcionales, sino en la definición del alcance, coordinación entre áreas y alineamiento estratégico del proyecto.

Durante esta etapa se realizó una coordinación previa con las áreas directamente involucradas en la gestión y respuesta a incidentes de seguridad, las cuales participaron activamente en la definición de requerimientos, validación de flujos operativos y priorización de casos de uso. Las principales áreas involucradas fueron:

- Centro de Operaciones de Seguridad (SOC): responsable del análisis, triage y gestión diaria de incidentes de ciberseguridad.
- Equipo de Ingeniería de Seguridad: encargado del diseño técnico de las integraciones, automatizaciones y buenas prácticas de seguridad.
- Equipo de Infraestructura y Cloud: responsable de los entornos tecnológicos donde se ejecutan las soluciones de seguridad.
- Equipo de Product Security: encargado de validar impactos sobre plataformas y servicios digitales.
- Gestión de TI / IT Operations: involucrado en la coordinación de cambios, accesos y controles operativos.

Como resultado de esta coordinación, se definió el alcance del proyecto, estableciendo los tipos de incidentes a automatizar, las herramientas a integrar y los criterios de éxito para cada sprint posterior. Asimismo, se acordó el uso de Cortex XSOAR como plataforma central de orquestación, permitiendo consolidar la gestión de alertas, incidentes y flujos de respuesta en un único entorno.

Sprint 1 – Integración de herramientas de seguridad

Este Sprint tuvo como objetivo principal centralizar la gestión de alertas e incidentes mediante la integración de las principales herramientas de seguridad utilizadas por la organización dentro de Cortex XSOAR. Para ello, se integraron diversas herramientas de seguridad previamente desplegadas en el entorno de la organización, las cuales cumplían roles específicos dentro del proceso de detección, análisis y respuesta a incidentes. En total, el proyecto contempló la integración de múltiples soluciones de seguridad, priorizadas en función de su impacto operativo y su frecuencia de uso dentro del SOC, siendo Cortex XSOAR la plataforma central encargada de la orquestación y automatización de los flujos de respuesta.

Sprint 2 – Estandarización de procesos de gestión de incidentes

El objetivo de este Sprint fue establecer un marco común para la gestión de incidentes de ciberseguridad. Se definieron campos obligatorios, criterios de severidad, clasificaciones de incidentes y procedimientos operativos, asegurando consistencia en el tratamiento de los incidentes entre los diferentes equipos y tenants de la organización. Esta estandarización permitió mejorar la calidad de la información registrada y sentó las bases para una automatización efectiva.

Sprint 3 – Automatización mediante playbooks de respuesta

En este Sprint se desarrollaron playbooks automatizados orientados a los principales casos de uso identificados en el SOC, tales como incidentes de phishing, malware y actividad sospechosa. Los playbooks permitieron orquestar acciones de

enriquecimiento, análisis, contención y respuesta, reduciendo la intervención manual de los analistas y acelerando los tiempos de respuesta y resolución de incidentes.

Sprint 4 – Comunicación y colaboración operativa

Este Sprint estuvo orientado a mejorar la comunicación entre el SOC y los usuarios internos durante la gestión de incidentes de ciberseguridad. Se implementaron mecanismos de notificación automática y plantillas de comunicación estandarizadas a través de canales internos, lo que permitió una interacción más eficiente, trazable y oportuna frente a las incidencias de seguridad.

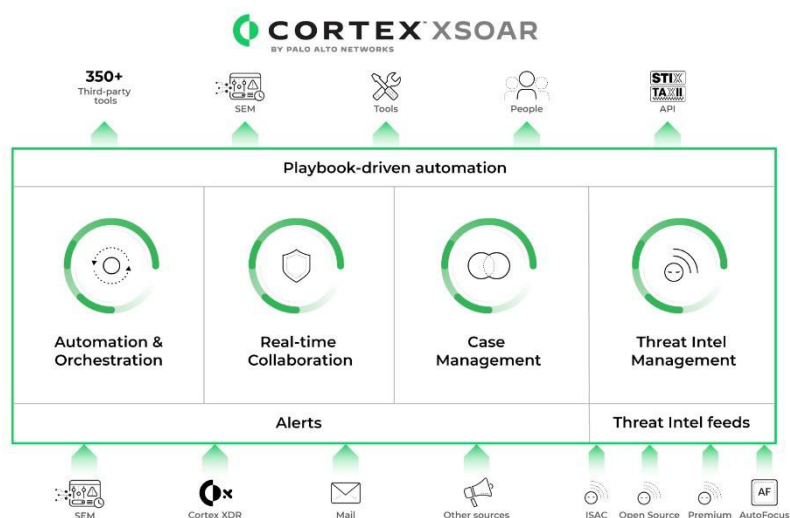
Sprint 5 – Optimización de métricas y mejora continua del SOC

Finalmente, este Sprint se enfocó en la optimización de las métricas operativas del SOC, tales como los tiempos de respuesta y resolución de incidentes (MTTR), el volumen de casos atendidos y la consistencia en la documentación generada. Los resultados obtenidos en esta etapa evidenciaron una mejora significativa en la eficiencia operativa del SOC, tal como se refleja en las métricas comparativas presentadas en la Tabla 5.

Asimismo, la solución implementada se basa en una arquitectura centralizada de orquestación y automatización que integra múltiples fuentes de información, herramientas de seguridad y equipos humanos dentro de un mismo flujo operativo. En este modelo, la plataforma actúa como centro de coordinación, permitiendo la ejecución de playbooks automatizados y la gestión unificada de incidentes. Esta arquitectura conceptual se muestra en la Figura 5.

Figura 5

Centralización de procesos de seguridad en Cortex XSOAR



Nota. Recuperado de: <https://register.paloaltonetworks.com/introducingcortexxsoar>

Esta arquitectura sirvió como base para la implementación de los casos de uso desarrollados en el presente trabajo, en concreto para la automatización de incidentes de phishing, accesos sospechosos y eventos detectados por EDR.

3.2.1 Objetivos

3.2.1.1 Objetivo General

Automatizar los procesos operacionales de ciberseguridad en la empresa del rubro digital, para la mejora de las respuestas a los incidentes de ciberseguridad, en el centro de operaciones de seguridad de la empresa.

3.2.1.2 Objetivos Específicos

- Integrar las principales herramientas de seguridad de la organización (SIEM, EDR, correo, ticketing, comunicación) en un entorno centralizado.
- Estandarizar los diseños y la documentación de playbooks automatizados para la atención de incidentes de ciberseguridad.
- Definir los campos y procedimientos en la gestión de incidentes de seguridad, asegurando consistencia entre los diferentes entornos.

- Establecer mecanismos de comunicación directa con usuarios internos para mejorar la respuesta frente a incidencias de seguridad.

3.2.2 Alcance

El alcance del proyecto de implementación de Cortex XSOAR para el Centro de Operaciones de Seguridad se delimitó tanto en términos técnicos como organizacionales, priorizando aquellos procesos y casos de uso que representaban mayor impacto para la operación del Centro de Operaciones de Seguridad.

En términos generales, el alcance incluyó los siguientes aspectos:

- Integración de herramientas críticas de seguridad
 - SIEM (Splunk): centralización de alertas y correlación de eventos.
 - EDR (CrowdStrike, SentinelOne): ejecución de acciones de contención automatizada en endpoints.
 - Correo electrónico (Proofpoint): ingestión y clasificación de reportes de mensajes de correo potencialmente malicioso.
 - Gestión de tickets (ServiceNow): generación automática y estandarizada de incidentes.
 - Comunicación corporativa (Slack): notificación de alertas y coordinación entre los distintos equipos.
- Casos de uso priorizados
 - Incidentes de correo electrónico malicioso y mensajes sospechosos: automatización de la investigación, categorización y respuesta frente a reportes de phishing y spam.
 - Malware en endpoints: integración con EDR para aislamiento inmediato de equipos comprometidos.
 - Accesos sospechosos a credenciales: validación automática de IPs, hashes y dominios contra fuentes de reputación.
- Procesos organizacionales
 - Definición de campos estándar en tickets de seguridad (severidad, propietario, estado, sitio, fase, clasificación).

- Documentación de SOPs y runbooks como parte del proceso de transferencia de conocimiento y elaboración de plantillas de comunicación interna

Limitaciones del alcance

- La implementación del proyecto se centró en incidentes de seguridad interna y no en la protección directa de usuarios finales de videojuegos.
- No se incluyeron en esta fase integraciones con herramientas de seguridad de aplicaciones ni sistemas financieros.
- La evaluación económica consideró únicamente el ahorro en horas-hombre y no los costos indirectos por incidentes evitados.

3.2.3 Etapas y Metodología

Fundamentación de la metodología utilizada

La implementación de una plataforma de orquestación y automatización de seguridad (SOAR) requiere de un enfoque metodológico iterativo e incremental, debido a que los procesos de ciberseguridad son dinámicos y requieren ajustes constantes. Adoptar una metodología rígida o de despliegue único implicaría altos riesgos técnicos y organizacionales, considerando la complejidad de las integraciones y la resistencia natural al cambio por parte de los equipos involucrados.

En este sentido, se optó por una estrategia que permita desarrollar y validar entregables de forma progresiva. Tal como señala el SANS Institute (2022), los equipos que implementan SOAR suelen comenzar automatizando tareas simples (como la creación de tickets o validaciones básicas) y luego evolucionan hacia flujos más complejos a través de ciclos de prueba, ajuste y validación continua. Este enfoque incremental no solo reduce riesgos, sino que permite evidenciar mejoras tempranas.

Asimismo, se consideró la estrategia de los *low-hanging fruits*, recomendada por proveedores como BlueVoyant (2023), que sugiere priorizar casos de uso frecuentes y

rutinarios, que al ser automatizados ofrecen un retorno rápido y tangible. Estos éxitos iniciales incrementan la aceptación del equipo, validan la metodología y allanan el camino para escenarios más sofisticados.

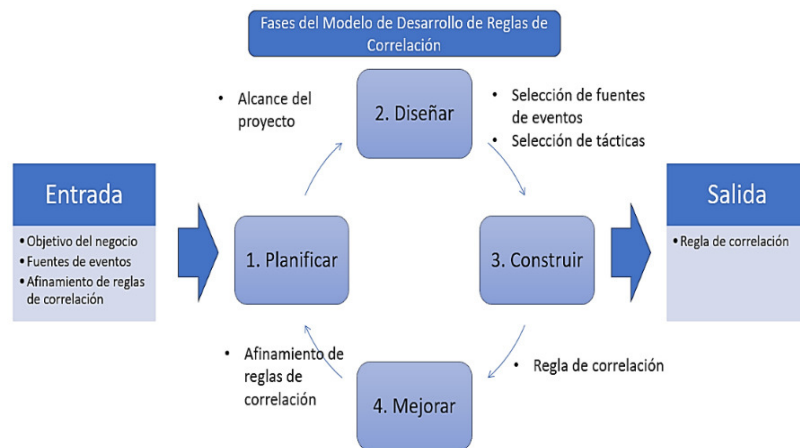
Por su parte, IBM Security (2023) define a SOAR como una plataforma cuyo principal objetivo es reducir los tiempos de detección y respuesta (MTTD y MTTR) mediante la automatización y orquestación de flujos entre distintas herramientas. Dicho impacto, sin embargo, solo se logra si se implementa mediante un enfoque iterativo, acompañado de retroalimentación constante y medición de resultados.

Desde el ámbito académico, investigaciones como Shaukat et al. (2024) plantean que los playbooks deben ajustarse progresivamente según el entorno de operación, considerando variables como falsos positivos, nuevos vectores de ataque o restricciones organizacionales. En este sentido, el proyecto adoptó un enfoque orientado a la mejora continua.

Un enfoque metodológico complementario es el propuesto por Palomino et al. (2024), quienes diseñaron un modelo para el desarrollo de reglas de correlación en entornos SIEM, orientado particularmente a la detección de ransomware. Su propuesta contempla cuatro fases cíclicas: planificar, diseñar, construir y mejorar, las cuales permiten gestionar la complejidad técnica de forma progresiva, validando resultados parciales y ajustando según la retroalimentación del entorno. Aunque el presente proyecto se centra en plataformas SOAR y en la automatización de respuestas, la lógica de fases iterativas y mejora continua resulta aplicable, especialmente en etapas de afinamiento de playbooks y en el diseño colaborativo de flujos automatizados que deben adaptarse a amenazas emergentes. Este modelo propuesto se sintetiza en la Figura 7.

Figura 7

Modelo propuesto por Palomino et al., 2024



Nota: Modelo de desarrollo de reglas de correlación para la detección y alerta de ransomware, Palomino et al. (2024)

Definición de conceptos clave utilizados en el proyecto

Luego de la descripción de la metodología empleada, se presentan los conceptos clave utilizados a lo largo del presente informe, con el propósito de facilitar la comprensión del enfoque adoptado para la automatización de los procesos de respuesta a incidentes de ciberseguridad. Estas definiciones permiten contextualizar los términos técnicos empleados durante la implementación del proyecto.

- **Centro de Operaciones de Seguridad (SOC):** unidad encargada del monitoreo continuo, análisis y gestión de eventos e incidentes de seguridad, responsable de coordinar las acciones de respuesta ante amenazas detectadas.
- **Orquestación:** proceso mediante el cual se coordinan de forma estructurada las acciones de múltiples herramientas de seguridad, permitiendo la ejecución secuencial o paralela de tareas dentro de un flujo automatizado.
- **Automatización:** uso de playbooks y reglas predefinidas para ejecutar tareas repetitivas de análisis, enriquecimiento y respuesta a incidentes sin intervención manual, reduciendo el tiempo de respuesta y la carga operativa del analista.

- **Playbook:** conjunto estructurado de acciones automatizadas que definen el flujo de respuesta ante un tipo específico de incidente de ciberseguridad, incluyendo actividades de triage, contención, erradicación y cierre.
- **Sprint:** unidad iterativa de trabajo orientada a la implementación de un conjunto específico de funcionalidades o automatizaciones, con entregables verificables al finalizar cada ciclo. En el presente proyecto, el término Sprint no se emplea en el sentido estricto de Scrum, sino como un marco operativo adaptado al contexto de automatización SOAR.
- **Mean Time to Respond (MTTR):** métrica utilizada para medir el tiempo promedio transcurrido desde la detección de un incidente hasta la ejecución de las acciones de respuesta correspondientes.
- **Definition of Ready (DoR):** conjunto de criterios mínimos que deben cumplirse antes de iniciar la implementación de un caso de uso o sprint, asegurando que los requisitos estén claramente definidos.
- **Definition of Done (DoD):** criterios que determinan cuándo una automatización o sprint puede considerarse completado, incluyendo validaciones técnicas y operativas.

3.2.4 Fundamentos Utilizados

El desarrollo e implementación del presente proyecto se basó en fundamentos teóricos y tecnológicos que responden a estándares internacionales de ciberseguridad, así como a principios operativos ampliamente aceptados en entornos de centros de operaciones de seguridad. Estos fundamentos permitieron construir una solución alineada con el contexto organizacional, especialmente tras el proceso de integración corporativa por la adquisición. A continuación, se describen los principales enfoques adoptados:

Marco normativo y de buenas prácticas

NIST Cybersecurity Framework (CSF)

Este marco de trabajo, desarrollado por el *National Institute of Standards and Technology*, plantea cinco funciones clave para una gestión integral de la ciberseguridad: Identificar, Proteger, Detectar, Responder y Recuperar (NIST, 2018). Las etapas de Detección y Respuesta fueron centrales para la estructuración

de los playbooks implementados, ya que permiten operar incidentes bajo procesos repetibles y medibles.

ISO/IEC 27035

La norma ISO 27035 establece directrices para la gestión de incidentes de seguridad de la información, considerando su detección, análisis, evaluación, tratamiento y aprendizaje posterior (ISO, 2016). Este enfoque es clave para formar la documentación de SOPs, el establecimiento de criterios de severidad, y la trazabilidad de cada respuesta automatizada.

MITRE ATT&CK Framework

MITRE ATT&CK (The Adversarial Tactics, Techniques, and Common Knowledge) es una base de conocimientos que contiene las tácticas y técnicas utilizadas por actores maliciosos. Este framework se empleó para mapear los incidentes reportados y clasificados (como spear phishing, acceso no autorizado o malware en endpoints), permitiendo estructurar los playbooks según técnicas específicas como *T1566.001 (Phishing: Spearphishing Attachment)* o *T1059 (Command and Scripting Interpreter)* (MITRE, 2023).

Fundamentos tecnológicos

Security Orchestration, Automation and Response (SOAR)

SOAR es un enfoque tecnológico que permite integrar diferentes herramientas de seguridad, automatizar tareas repetitivas y coordinar la respuesta a incidentes (IBM Security, 2023). En este proyecto se utilizó la plataforma Cortex XSOAR, que facilitó la creación de playbooks para incidentes frecuentes como correos sospechosos, accesos indebidos y amenazas detectadas por el software EDR.

Security Information and Event Management (SIEM)

La plataforma SIEM (en este caso, Splunk) cumple un rol central en la correlación de eventos y la generación de alertas. La integración de XSOAR con el SIEM permitió que estas alertas se transformaran automáticamente en tickets, con enriquecimiento de datos y ejecución de acciones definidas en los playbooks.

Endpoint Detection and Response (EDR)

Se integraron herramientas como CrowdStrike y SentinelOne para la detección y respuesta ante amenazas en endpoints. Estas plataformas proporcionaron capacidades como el aislamiento automático del equipo comprometido y el análisis de procesos sospechosos, acciones que fueron orquestadas a través de XSOAR.

Gestión de tickets y comunicaciones internas

Los sistemas de gestión de tickets (ServiceNow y Jira) fueron clave para documentar la trazabilidad del incidente. La integración con Slack permitió comunicaciones automáticas mediante la implementación de bots y en tiempo real con demás equipos encargados, garantizando la continuidad operativa y la eficiencia del proceso de respuesta.

Estimación de complejidad en puntos de historia

La estimación de complejidad del proyecto se realizó durante el Sprint 0, utilizando una aproximación basada en puntos de historia, con el objetivo de dimensionar el esfuerzo requerido para la implementación de los sprints orientados a la automatización de la respuesta a incidentes de ciberseguridad. Esta estimación fue adaptada al contexto del proyecto SOAR y se apoyó en marcos de referencia reconocidos en la industria de la seguridad de la información.

En particular, se tomó como base el modelo PICERL propuesto por el SANS Institute, el cual estructura el ciclo de respuesta a incidentes en las fases de Preparación (Preparation), Identificación (Identification), Contención (Containment), Erradicación (Eradication), Recuperación (Recovery) y Lecciones Aprendidas (Lessons Learned). Este modelo permitió identificar las etapas del proceso donde la automatización aportaba mayor valor operativo, así como aquellas que requerían validación humana debido a su impacto o criticidad (SANS Institute, 2022).

Adicionalmente, se consideró el marco MITRE ATT&CK como referencia para contextualizar los incidentes en función de las tácticas y técnicas empleadas por atacantes

informáticos. Este enfoque facilitó la priorización de los casos de uso a automatizar, alineando los playbooks con técnicas de ataque relevantes y recurrentes dentro del entorno de la organización (MITRE, 2023).

La estimación se realizó considerando cuatro criterios clave, definidos durante el Sprint 0 y alineados con las fases del modelo PICERL:

1. Complejidad de integración: asociada principalmente a las fases de Preparación e Identificación.
2. Nivel de automatización: vinculada a las fases de Identificación y Contención.
3. Impacto operativo: evaluado especialmente en las fases de Contención y Erradicación.
4. Validaciones y controles: relacionados con Recuperación y Lecciones Aprendidas.

Este enfoque permitió asignar puntos de historia de manera más objetiva, considerando tanto la complejidad técnica como el impacto operativo y el riesgo asociado a cada automatización.

Cabe precisar que la estimación de complejidad del presente proyecto no se realizó mediante técnicas formales de planificación ágil, tales como Planning Poker. En su lugar, se definió una escala base de puntos de historia, empleada como una referencia interna para orientar la priorización y planificación de tareas dentro de cada sprint, de acuerdo con la complejidad técnica y el impacto operativo de las automatizaciones implementadas.

Esta escala fue diseñada considerando el contexto específico del proyecto de automatización SOAR, tomando en cuenta factores como el número de herramientas involucradas, la cantidad de decisiones condicionales dentro de los playbooks y el nivel de riesgo asociado a las acciones automatizadas.

En función de estos criterios, se estructuró una escala interna de puntos de historia para clasificar la complejidad de las automatizaciones desarrolladas, la cual se presenta en la Tabla 6:

Tabla 6

Escala de puntos de historia y criterios de complejidad de las automatizaciones

Puntos de historia	Tipo de tarea o playbook asociado	Criterios de complejidad considerados	Justificación práctica
1	Consulta de reputación de IP o dominio	Una integración, lógica lineal, sin ramificaciones ni impacto operativo directo	Automatizaciones de bajo riesgo, resueltas mediante una única llamada API y respuesta booleana.
2	Triage básico de correos sospechosos (phishing de baja severidad)	Integración con correo electrónico, parsing de contenido, clasificación inicial sin acciones destructivas	Incluyó análisis de encabezados, búsquedas simples en inteligencia de amenazas y cierre automático sin escalamiento.
3	Automatización de casos de spam con creación de ticket	Uso de al menos dos sistemas (correo y ticketing), trazabilidad requerida	Requirió documentación del incidente, notificación al usuario y registro formal en el sistema de gestión de incidentes.
5	Aislamiento condicional de endpoint tras detección de malware	Integración con EDR, validaciones condicionales y posible autorización manual	Involucró múltiples condiciones de entrada, validación de indicadores y, en algunos casos, intervención de analistas de nivel avanzado.
8	Detección y escalamiento de accesos anómalos en múltiples herramientas (IDP, SIEM, SSO)	Integración entre IDP, SIEM y SSO, múltiples ramas de decisión	Requirió correlación entre fuentes, evaluación de riesgo y ejecución de acciones como forzado de MFA o suspensión temporal de sesiones.
13	Playbooks complejos de respuesta a ransomware o amenazas críticas	Alto riesgo operativo, múltiples integraciones (SIEM, EDR, correo, AD, ticketing)	Incluyó acciones de contención críticas, validaciones adicionales y monitoreo posterior a la ejecución.

Nota: Elaboración propia, basada en el análisis interno de la complejidad técnica y el impacto operativo de las automatizaciones implementadas durante el proyecto.

Como se apreciaba en la tabla, la asignación de puntos de historia aumenta progresivamente en función del número de integraciones involucradas, la cantidad de ramas condicionales dentro del playbook y el impacto operativo potencial de las acciones automatizadas. Esta clasificación permitió priorizar el desarrollo de automatizaciones críticas y distribuir el esfuerzo técnico de manera estructurada a lo largo de los sprints del proyecto.

Roles involucrados en la implementación

El proyecto de automatización se desarrolló en coordinación con distintos perfiles técnicos y operativos del Centro de Operaciones de Seguridad y Ciberdefensa, además de otros equipos. En la Tabla 7 se resumen los roles involucrados en el proyecto y sus funciones respectivas:

Tabla 7

Definición de roles del proyecto

Rol	Descripción	Cantidad estimada
Director de Ciberseguridad	Supervisión estratégica y alineamiento global del área de seguridad.	1
Director Técnico de Ciberseguridad	Coordinación de arquitectura de seguridad, aprobaciones técnicas y validación de soluciones.	1
Líder de Operaciones de Ciberseguridad	Gestión operativa del equipo de analistas, monitoreo y cumplimiento de SLA.	1
Gerente Senior de Operaciones	Coordinación de roadmap de automatización y soporte a decisiones técnicas y operativas.	1
Ingeniero de Ciberseguridad (Tier 3)	Resolución de incidentes complejos y apoyo en el diseño de respuestas automatizadas.	1–2
Analista Principal	Liderazgo técnico en la gestión de incidentes y soporte en el diseño de flujos automatizados.	1
Analista de Amenazas (Cyber Threat Analyst)	Correlación de inteligencia de amenazas e integración con MITRE ATT&CK.	1
Analistas Senior del SOC	Revisión de alertas críticas, validación de flujos, entrenamiento de nuevos analistas.	2–3
Analistas Tier 1 & 2	Triaje inicial, ejecución de tareas automatizadas, monitoreo y documentación.	8–15

Nota. Fuente: Elaboración propia, basada en la estructura del Centro de Operaciones de Seguridad y Ciberdefensa de la organización.

3.2.5 Implementación de las áreas, procesos, sistemas y buenas prácticas

La implementación del proyecto se estructuró en seis fases operativas que reflejan el ciclo completo de transformación del proceso de respuesta a incidentes, que va desde la evaluación inicial hasta la fase de mejora continua. Cada una de estas etapas se desarrolló bajo un enfoque incremental, colaborativo y alineado con las buenas prácticas del área de ciberseguridad, priorizando la automatización de tareas críticas, la estandarización de procedimientos y la integración de las herramientas tecnológicas clave.

A lo largo del proyecto se generaron múltiples entregables, entre ellos, playbooks automatizados, plantillas operativas, SOPs documentados, integraciones funcionales y dashboards de métricas, que demuestran el valor progresivo de cada fase. Estos entregables fueron desarrollados y validados por el equipo de seguridad interna, en conjunto con los responsables técnicos del entorno de orquestación, y supervisados por líderes de operaciones de ciberseguridad (SOC leads).

La Tabla 8 resume las seis fases que guiaron la implementación, detallando su propósito y los principales productos generados en cada una.

Tabla 8

Fases de implementación del proyecto y entregables desarrollados

Fase	Descripción	Entregables principales
Levantamiento de información y diagnóstico inicial	Evaluación de flujos operativos, tiempos de respuesta, herramientas existentes y puntos de dolor en la operación.	Línea base de métricas (MTTD, MTTR), inventario de alertas,

Fase	Descripción	Entregables principales
		análisis de flujos manuales.
Priorización de casos de uso	Selección de incidentes de mayor frecuencia e impacto; análisis de automatización para primera iteración de playbooks.	Matriz de priorización, fichas de casos de uso, listado inicial de flujos seleccionados.
Diseño y prototipado de playbooks	Modelado visual en Cortex XSOAR; definición de lógica condicional, integraciones por paso y validación en sandbox.	Prototipos de playbooks, flujogramas, estructura modular de tareas automatizadas.
Implementación gradual en producción	Despliegue progresivo de playbooks validados, pruebas funcionales e integración con herramientas activas.	Playbooks en producción, registro de ejecuciones, historial de versiones por playbook.
Medición y retroalimentación	Comparación de métricas pre y post automatización, revisión de resultados y validación con equipo operativo.	Dashboards de XSOAR, reportes de mejora de MTTR, comentarios de usuarios, iteraciones.
Ciclo de mejora continua	Revisión continua de casos, documentación de SOPs, actualización de campos estándar y retroalimentación de incidentes.	SOPs estandarizados, plantillas de tickets, lista de lecciones aprendidas, mejoras por fase.

Nota: Elaboración propia basada en el enfoque operativo del proyecto.

A continuación, se describe cada una de estas fases con mayor detalle, destacando las herramientas utilizadas, los flujos diseñados, las buenas prácticas aplicadas y los beneficios obtenidos tras su implementación.

3.2.5.1 Arquitectura funcional y de integraciones

La arquitectura de integración desarrollada como parte de este proyecto respondió a la necesidad de centralizar y orquestar las distintas fuentes de eventos de seguridad dentro del entorno del SOC. La plataforma SOAR fue configurada como núcleo del sistema, permitiendo la automatización de tareas críticas y la coordinación de flujos de trabajo entre herramientas dispares.

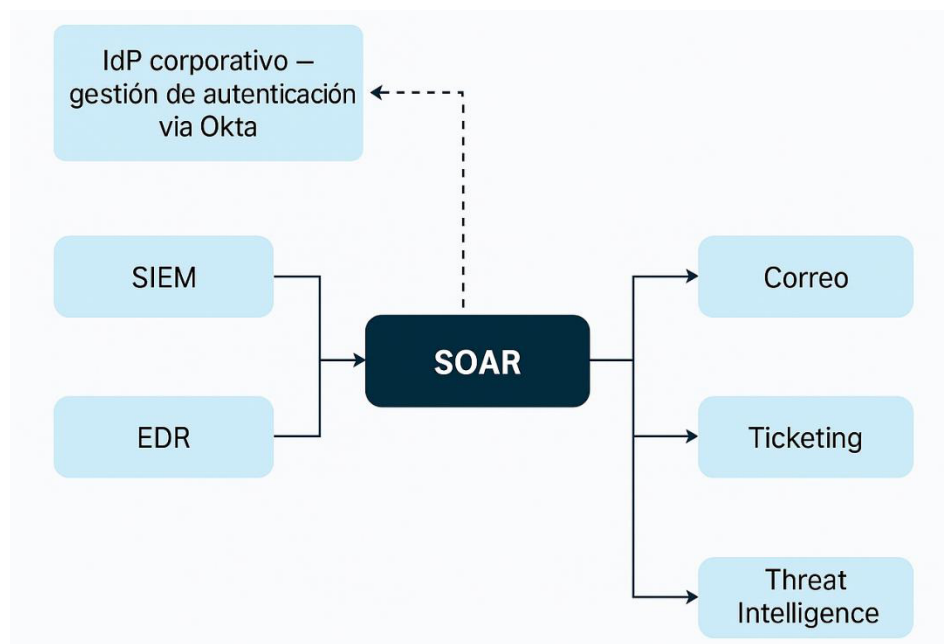
Durante la implementación, se integraron sistemas como el SIEM corporativo, el EDR, la plataforma de correo electrónico, el gestor de tickets (ITSM), el sistema de identidad (SSO/IDP) y servicios de inteligencia de amenazas. La conectividad se realizó mediante métodos seguros (API Keys, OAuth, SAML), garantizando autenticación robusta y control de permisos por integración.

Estas integraciones permitieron recibir alertas en tiempo real, enriquecer eventos con datos contextuales, disparar acciones automatizadas como aislamiento de endpoints o cierre de tickets, y generar documentación completa para auditoría. El diseño se basó en una arquitectura tipo hub-and-spoke, con XSOAR como centro operativo y canales bidireccionales con cada sistema fuente o destino.

La arquitectura de integración implementada se representa en la Figura 11, donde se observa a XSOAR como nodo central de orquestación y los distintos sistemas conectados mediante integraciones autenticadas y controladas.

Figura 9

Topología lógica de integraciones



Nota. Fuente: Elaboración propia.

La conectividad con las distintas plataformas se realizó de forma segura, utilizando autenticación gestionada a través de Okta, el sistema corporativo de identidad (IdP). Dependiendo del tipo de sistema, se habilitaron métodos como OAuth 2.0 federado, SAML assertions o tokenización temporal con expiración controlada, todos ellos autorizados y auditados mediante la consola de gestión de accesos de Okta. Esto permitió aplicar el principio de mínimo privilegio, rotación periódica de credenciales, y trazabilidad completa sobre qué integraciones fueron activadas, por quién, y en qué contexto.

La Tabla 9 resume las principales características técnicas de las integraciones implementadas:

Tabla 9

Conectores y parámetros técnicos de integración

Sistema	Tipo de autenticación	Frecuencia de consulta	Límites de consultas por hora	Fallback en caso de error
SIEM	OAuth 2.0 federado (via Okta)	Tiempo real	10,000	Sí
EDR	OAuth 2.0 federado (via Okta)	Cada 5 min	6,000	Sí
Correo	OAuth 2.0 federado (via Okta)	Cada 2 min	5,000	Sí
Ticketing	API Token gestionado con Okta SSO	Cada 1 min	3,000	No
SSO/IdP	Okta (SAML SSO)	Cada login	1,000	Sí
Threat Intelligence	API Key tradicional	Cada 15 min	2,000	Sí

Nota. Fuente: Elaboración propia.

Asimismo, se aplicaron controles de seguridad y clasificación de datos. Algunos tipos de información, como direcciones de correo o credenciales de sesión, fueron tratados como confidenciales y sujetos a enmascaramiento, no persistencia o control de acceso auditado. La Tabla 10 presenta un resumen de estas políticas:

Tabla 10*Clasificación y control de datos manejados por la plataforma*

Tipo de dato	Clasificación	Control aplicado
Correo electrónico	Confidencial	Enmascaramiento + logging
IP de origen	Uso interno	Registro con hash
Hash de archivo	Uso interno	Registro sin persistencia
Credenciales de sesión	Confidencial	Vencimiento automático + no persistencia
Nombre de usuario	Uso interno	Auditoría de acceso
Registro de ticket	Público	Sin restricción

Nota. Fuente: Elaboración propia.

Además, se diseñaron mecanismos de resiliencia para garantizar que las fallas de un sistema externo (como caída de EDR o timeouts de SIEM) no afectaran el flujo global. Esto incluyó implementación de *rate limiting*, *circuit breakers*, separación de ambientes dev/prod, y alertas automáticas por fallos de conexión o errores en autenticación, esto con coordinación con el equipo de SRE (Site Reliability Engineering).

3.2.5.2 Gobierno corporativo y roles

La implementación del proyecto no solo implicó el diseño técnico de integraciones y playbooks, sino también el establecimiento de un marco de gobernanza operativa que asegure la sostenibilidad, calidad y escalabilidad del sistema a lo largo del tiempo.

Este marco se construyó con base en principios de responsabilidad compartida, control de cambios, calidad continua y mejora iterativa. Para ello, se definieron roles operativos, flujos de revisión y aprobación, criterios para validar la madurez de cada playbook y controles que permitieran asegurar la alineación con los objetivos del área de ciberseguridad.

Responsabilidad sobre el ciclo de vida de los playbooks

Cada playbook desarrollado dentro de XSOAR tiene un ciclo de vida estructurado, que va desde su conceptualización hasta su despliegue en producción, incluyendo etapas de validación, pruebas, documentación y actualización. Para asegurar que cada fase fuera

adecuadamente gestionada, se estableció un esquema RACI (Responsible, Accountable, Consulted, Informed), asignando responsables por rol y actividad, que se presenta en la Tabla 11:

Tabla 11

Matriz RACI para el ciclo de vida de un playbook

Actividad	Responsable (R)	Aprobador (A)	Consultado (C)	Informado (I)
Identificación del caso de uso	Analista Principal	Líder de Operaciones de Ciberseguridad	Analistas Tier 1 & 2	SOC completo
Diseño del flujo de playbook	Analistas Senior del SOC	Gerente Senior de Operaciones de Ciberseguridad	Analista de Amenazas (Cyber Threat Analyst)	Equipo de TI
Revisión técnica y QA	Ingeniero de Ciberseguridad (Tier 3)	Director Técnico de Ciberseguridad	Analistas Senior del SOC	SOC completo
Despliegue en entorno productivo	Gerente Senior de Operaciones de Ciberseguridad	Director de Ciberseguridad	Ingeniero de Ciberseguridad (Tier 3)	Cumplimiento / Auditoría
Documentación operativa y SOP	Analista de Amenazas (Cyber Threat Analyst)	Director Técnico de Ciberseguridad	Gerente Senior de Operaciones de Ciberseguridad	Operaciones Globales
Revisión post-producción y mejora	Líder de Operaciones de Ciberseguridad	Director de Ciberseguridad	Ingeniero de Ciberseguridad (Tier 3)	Todos los stakeholders

Nota. Fuente: Elaboración propia.

Criterios de aceptación y despliegue (DoR / DoD)

Para estandarizar la calidad mínima esperada de cada playbook antes de su paso a producción, se definieron criterios de Definition of Ready (DoR) y Definition of Done (DoD). Estos requisitos no solo funcionaron como checklist para el equipo técnico, sino también como mecanismos de control ante potenciales auditorías y revisiones, como se ve en la Tabla 12.

Tabla 8*Criterios de aceptación para automatizaciones en SOAR*

Fase	Criterios requeridos	Rol responsable
Definition of Ready (DoR)	Caso de uso validado por impacto y frecuencia	Analista Principal
	Integraciones disponibles y autenticadas	Analistas Senior del SOC
	Diagrama de flujo lógico aprobado	Analista Principal
	Escenarios de prueba definidos (normal, excepción, fallo)	Ingeniero de Ciberseguridad (Tier 3)
	Revisión técnica preliminar completada	Ingeniero de Ciberseguridad (Tier 3)
Definition of Done (DoD)	Playbook desplegado en entorno productivo	Gerente Senior de Operaciones de Ciberseguridad
	Logging activo y trazabilidad validada	Analistas Tier 1 & 2
	Validación post-despliegue ejecutada	Analistas Senior del SOC
	Evidencias generadas en ticketing o CMDB	Analista de Amenazas (Cyber Threat Analyst)
	Documentación formal publicada (SOP, guías)	Gerente Senior de Operaciones de Ciberseguridad

Nota. Fuente: Elaboración propia.

Estos criterios permitieron al equipo evitar automatizaciones incompletas, riesgos por flujos mal validados, o despliegues prematuros. Además, facilitaron el control de versiones, la planificación de mejoras incrementales y la evaluación del impacto de cada automatización sobre el entorno operativo.

Etapas desarrolladas como sprints funcionales

Antes de adoptar formalmente el enfoque iterativo basado en sprints funcionales, el proyecto fue inicialmente estructurado en una serie de fases secuenciales, cada una con entregables específicos y objetivos definidos. Este enfoque permitió ordenar las primeras actividades de diagnóstico, priorización y diseño, así como validar técnicamente la viabilidad del entorno de automatización y las integraciones que eran requeridas.

A continuación, se presenta un resumen de las etapas originales:

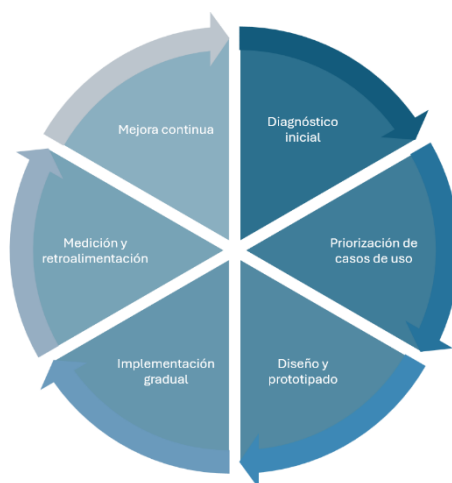
- Levantamiento de información y diagnóstico inicial: Se recopilaron y documentaron los procedimientos existentes en la operación diaria, identificando puntos de fricción, tareas repetitivas y diferencias entre entornos. Se construyó una línea base de métricas como el tiempo medio de detección (MTTD) y el tiempo medio de respuesta (MTTR), además de identificar duplicidad de esfuerzos y fragmentación en los flujos operativos heredados tras la adquisición corporativa.
- Priorización de casos de uso: Con base en el diagnóstico previo, se seleccionaron los incidentes de mayor frecuencia e impacto para la organización. Se priorizaron casos que presentaban alto volumen y buena factibilidad técnica de automatización, tales como: gestión de correos sospechosos (phishing, spam, smishing), alertas de malware en endpoints, y eventos críticos detectados por el SIEM.
- Diseño y prototipado de playbooks: Se desarrollaron los primeros playbooks en Cortex XSOAR, replicando de forma estructurada los procedimientos manuales del equipo operativo. Estos flujos fueron testeados en ambientes controlados, evaluando su eficacia y adaptándolos con base en los resultados obtenidos. La fase incluyó definición de condiciones, lógica de decisión, tareas automáticas e integraciones iniciales.

- Implementación gradual en producción: Con los playbooks validados, se procedió a su despliegue progresivo en el entorno productivo. Se definieron criterios de activación, controles de ejecución, rutas de escalamiento y mecanismos de auditoría. Las integraciones clave incluyeron herramientas como Splunk, SentinelOne, CrowdStrike, Proofpoint, ServiceNow y Slack.
- Medición y retroalimentación: Durante esta etapa se recopilaban métricas como MTTR, MTTD, volumen de alertas automatizadas y tasa de falsos positivos. Estas métricas se contrastaron con la línea base y sirvieron como insumo para refinar los flujos, ajustar parámetros y mejorar la experiencia del analista.
- Ciclo de mejora continua: Finalmente, se estableció un modelo de revisión y mejora continua. A través de la retroalimentación directa del equipo y del análisis de nuevos incidentes, se ajustaron los flujos, se documentaron SOPs y se estandarizaron plantillas. Este proceso aseguró que las automatizaciones se mantuvieran alineadas con las necesidades reales del entorno y buenas prácticas.

La siguiente figura sintetiza este ciclo de mejora continua en el SOC:

Figura 11

Ciclo iterativo de implementación de XSOAR en el SOC



Nota. Fuente: Elaboración propia.

Aunque el enfoque secuencial fue útil en las etapas iniciales, conforme avanzó el proyecto se evidenció la necesidad de adoptar una metodología más iterativa, que permitiera integrar desarrollo, pruebas, validación y ajustes dentro de unidades funcionales completas. Esta necesidad dio lugar a una reorganización del trabajo en Sprints funcionales, entendidos como bloques de implementación centrados en un caso de uso específico, con entregables claros y validados por el equipo técnico.

Dicho modelo facilitó la trazabilidad de resultados, permitió evidenciar mejoras desde las primeras entregas y fomentó la colaboración entre los distintos niveles operativos del área de ciberseguridad, tal como se recomienda en entornos de automatización avanzada (BlueVoyant, 2023; MITRE, 2023). Con el fin de evidenciar la alineación entre las fases originalmente planteadas para el proyecto y la estructura adoptada bajo el enfoque por sprints, se estableció una correspondencia metodológica que se sintetiza en la Tabla 13:

Tabla 13
Correspondencia entre fases originales y Sprints funcionales

Fase original del proyecto	Ubicación dentro del modelo de Sprints
Levantamiento de información y diagnóstico inicial	Sprint 1 – Planificación y contexto operativo
Priorización de casos de uso	Sprint 1 – Justificación y selección de flujos iniciales
Diseño y prototipado de playbooks	Sprint 1 (desarrollo) y siguientes – según caso de uso
Implementación gradual en producción	Sprint 1 y siguientes – Incremento e integración por caso
Medición y retroalimentación	Todos los Sprints – Validación de métricas y mejora
Ciclo de mejora continua	Sprint 6 – Revisión global y ajustes en flujos/SOPs

Nota: Elaboración propia

La implementación de la automatización del SOC requirió la integración coordinada de diversas herramientas tecnológicas, cada una con funciones específicas dentro del ciclo de detección, análisis y respuesta a incidentes. La Tabla 14 resume las principales plataformas utilizadas, su rol operativo, ventajas relevantes y los playbooks asociados en el contexto del proyecto.

Tabla 14

Herramientas utilizadas en la automatización del SOC con sus funciones, ventajas y playbooks asociados

Herramienta	Función en el SOC	Ventajas destacadas	Casos de uso / Playbooks
Cortex XSOAR	Orquestación de alertas y automatización de respuesta mediante playbooks.	Integración con más de 700 herramientas; trazabilidad; visualización clara de flujos.	Mensajes sospechosos, accesos anómalos, malware, clasificación de alertas.
Splunk	Correlación de eventos y generación de alertas a partir de logs.	Alta personalización; dashboards; reglas de correlación personalizadas.	Envío de alertas a XSOAR, soporte al análisis inicial.
SentinelOne	Detección y contención de amenazas en endpoints, respuesta autónoma.	Respuesta inmediata; bajo consumo; excelente detección basada en inteligencia artificial.	Aislamiento de endpoint comprometido, recolección de evidencia.
CrowdStrike Falcon	Análisis profundo de amenazas y persistencia en endpoints críticos.	Cobertura completa del ciclo de ataque; integración con inteligencia de amenazas.	Análisis de amenazas persistentes, validación de IOC y ejecución de bloqueos.
Proofpoint	Clasificación y análisis de mensajes sospechosos recibidos por correo.	Sandboxing de adjuntos y enlaces; alta precisión en detección de phishing.	Análisis de encabezados, URLs, adjuntos y clasificación automatizada.

Herramienta	Función en el SOC	Ventajas destacadas	Casos de uso / Playbooks
ServiceNow, Jira	Gestión de tickets y trazabilidad de incidentes de ciberseguridad.	Automatización de creación y cierre de tickets; cumplimiento de SLA.	Creación y asignación de incidentes de seguridad, cierre automático.
Slack	Canal de notificación y coordinación en tiempo real con los equipos SOC.	Notificaciones inmediatas a canales críticos y a responsables específicos.	Notificación automatizada al Slack del SOC según criticidad del caso.

Nota. Fuente: Elaboración propia.

En conjunto, los fundamentos conceptuales y tecnológicos descritos en esta sección fueron decisivos para garantizar que el proyecto de automatización del SOC no se limitara a solo una adopción de herramientas, sino que sea una solución estructurada, alineada a estándares internacionales, adaptable al contexto organizacional y orientada a resultados tangibles.

La integración entre diversos frameworks como NIST CSF, ISO/IEC 27035 y MITRE ATT&CK, junto con la implementación de plataformas como Cortex XSOAR, Splunk, SentinelOne, CrowdStrike, Proofpoint, ServiceNow, Slack, entre otras permitió construir una arquitectura que no solo fortaleció la capacidad de respuesta ante incidentes, sino que también permitió estandarizar procedimientos, mejoró la trazabilidad de acciones y fomentó una cultura de mejora continua dentro del SOC.

Estos fundamentos sentaron las bases técnicas, organizacionales y estratégicas necesarias para ejecutar de forma ordenada el despliegue de playbooks y SOPs, lo cual será detallado en el siguiente apartado.

3.2.5.3 Playbook de Phishing

La gestión de incidentes por phishing constituyó uno de los casos de uso prioritarios para la automatización debido a su elevada frecuencia, repetitividad operativa y riesgo de compromiso inicial de credenciales. El objetivo del playbook fue estandarizar y acelerar el triaje inicial, mejorar la calidad de la evidencia recopilada, y reducir el tiempo medio de respuesta (MTTR) sin eliminar controles humanos en situaciones de alto riesgo. La

implementación se realizó en la plataforma Cortex XSOAR, integrando información de correo corporativo, fuentes de threat intelligence, EDR y el sistema de gestión de incidentes (ServiceNow), con autenticación a través de Okta.

El diseño se guió por los principios de menor privilegio, reversibilidad y “fail-safe”: las acciones destructivas (aislamiento de endpoints, bloqueo de cuentas) requieren confirmación o son restringidas para cuentas VIP. Para definir la lógica de decisión se utilizó una matriz de riesgo basada en reputación de IOC, correlación con detecciones en endpoints y contexto de la cuenta (usuario normal vs cuenta crítica). Los criterios de aceptación (DoR/DoD) y la gobernanza del ciclo de vida quedan especificados en las secciones 3.2.5.2 y Tabla 12.

Se definieron los siguientes objetivos operativos del playbook:

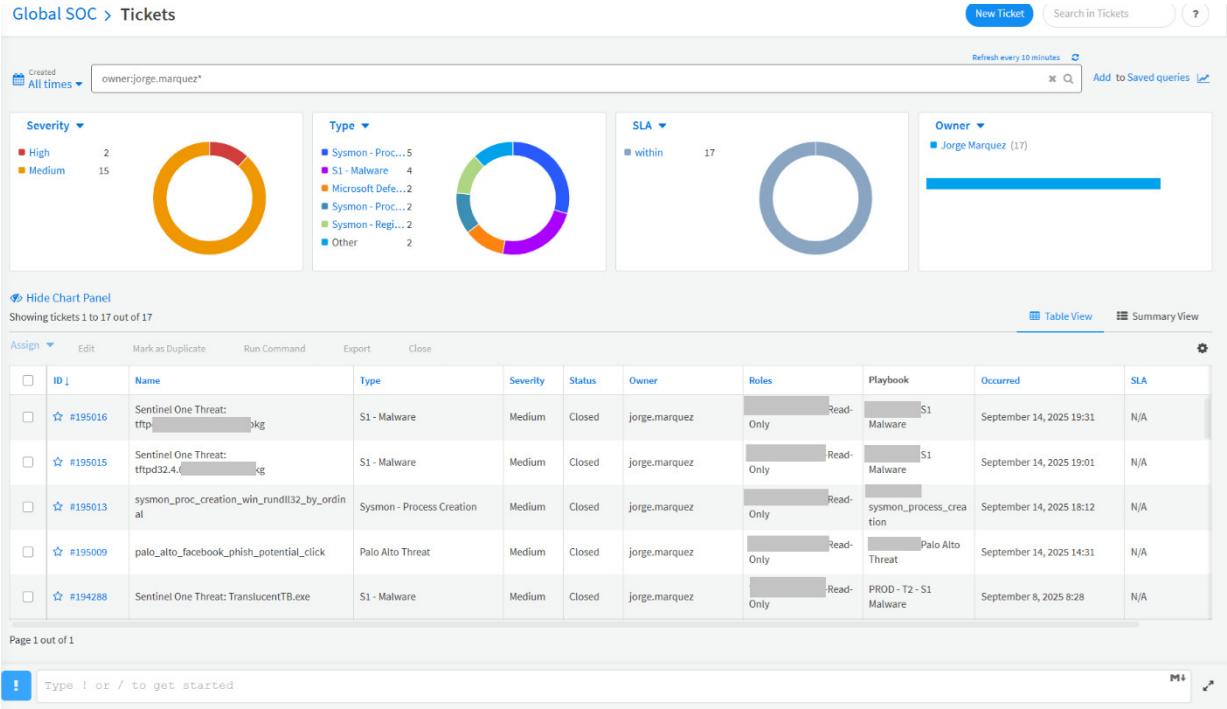
1. Automatizar el triage inicial y el enriquecimiento de artefactos para reducir la carga de analistas T1.
2. Estandarizar las acciones de contención para incidentes de riesgo alto con trazabilidad completa.
3. Generar evidencia y documentación automática en ServiceNow para cumplir requisitos de auditoría.
4. Mantener puntos de intervención manual en escenarios de excepciones (cuentas VIP, detección ambigua).

Flujo lógico (resumen)

El flujo del playbook inicia al recibir una alerta generada cuando un usuario reporta manualmente un correo sospechoso mediante el botón “Report Phishing”, habilitado en el cliente Outlook corporativo a través del complemento “Proofpoint PhishAlarm”. Esta integración permite que, con un solo clic, se genere una alerta estandarizada que es automáticamente ingerida por Cortex XSOAR, clasificándose como incidente de potencial phishing. La Figura 7 muestra la interfaz del cliente de correo con dicho botón habilitado. En la figura 8 se pueden ver las alertas integradas en el dashboard de XSOAR:

Figura 8

Visualización de alertas de phishing en el dashboard de Cortex XSOAR



Nota. Fuente: Captura del dashboard de XSOAR

Adicionalmente, el flujo lógico general de este playbook se resume en la Tabla 14:

Tabla 9

Resumen del flujo lógico del playbook de phishing

Paso	Acción	Fuente / Integración	Resultado esperado	Responsable
1	Recepción automática de reporte enviado por el usuario desde Outlook (botón “Report phishing”)	Correo corporativo / botón "Report phishing"	Alerta de <i>Phishing Reported</i> ingestada y clasificada automáticamente	Analistas T1/T2 (operación inicial)
2	Extracción automática de artefactos (remitente, IP, URLs, attachments)	XSOAR (parsers)	Artefactos listos para enriquecer	XSOAR (automatización)

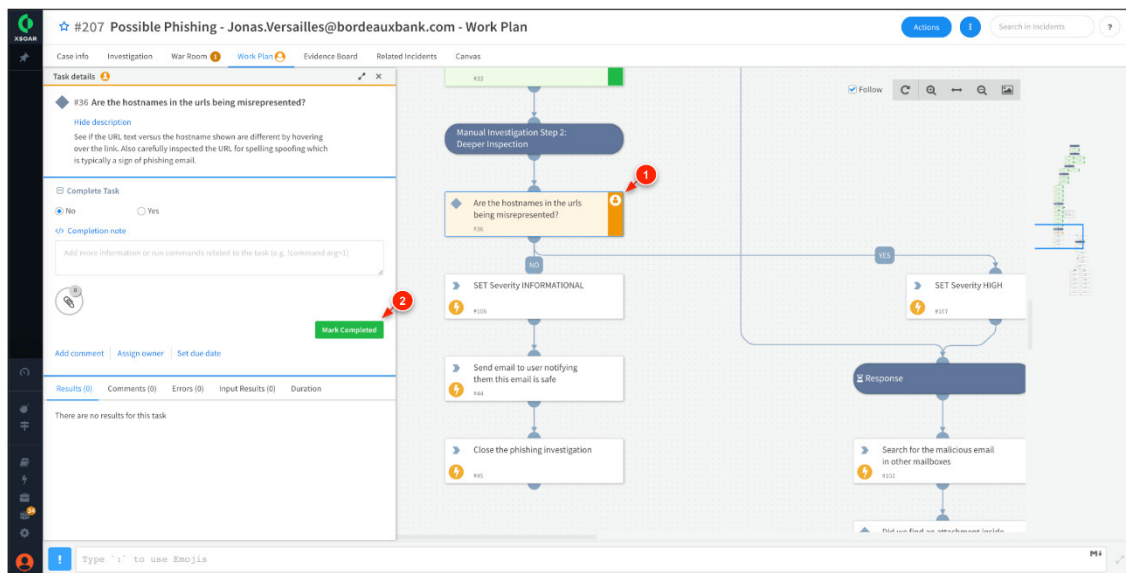
Paso	Acción	Fuente / Integración	Resultado esperado	Responsable
3	Enriquecimiento TI (VT, Hybrid Analysis)	Threat Intelligence	Score de reputación	Analista Principal (revisión)
4	Correlación con EDR/SIEM	EDR, SIEM	Detección de actividad en endpoints / búsquedas históricas	Analistas Senior / Ingeniero T3
5	Evaluación de riesgo (reglas)	XSOAR (motor de decisiones)	Clasificación: Bajo / Medio / Alto	Analistas Senior
6	Acción automática o escalamiento	EDR / Mail gateway / ServiceNow	Bloqueo, aislamiento o ticket	Ingeniero T3 (acción crítica) / T1 para cierres automáticos
7	Notificación y documentación	ServiceNow / correo de usuario	Registro completo y comunicación	Analistas T1/T2 (notificación)
8	Revisión post-incidente	Dashboard KPI	Ajustes en playbook si es necesario	Líder de Operaciones / Gerente Senior

Nota. Fuente: elaboración propia.

Para presentar gráficamente la implementación práctica del flujo descrito en la Tabla 14, se presenta en la Figura 13 un ejemplo de ejecución parcial del playbook de phishing dentro de la plataforma XSOAR.

Figura 13

Ejemplo de ejecución parcial del playbook de phishing

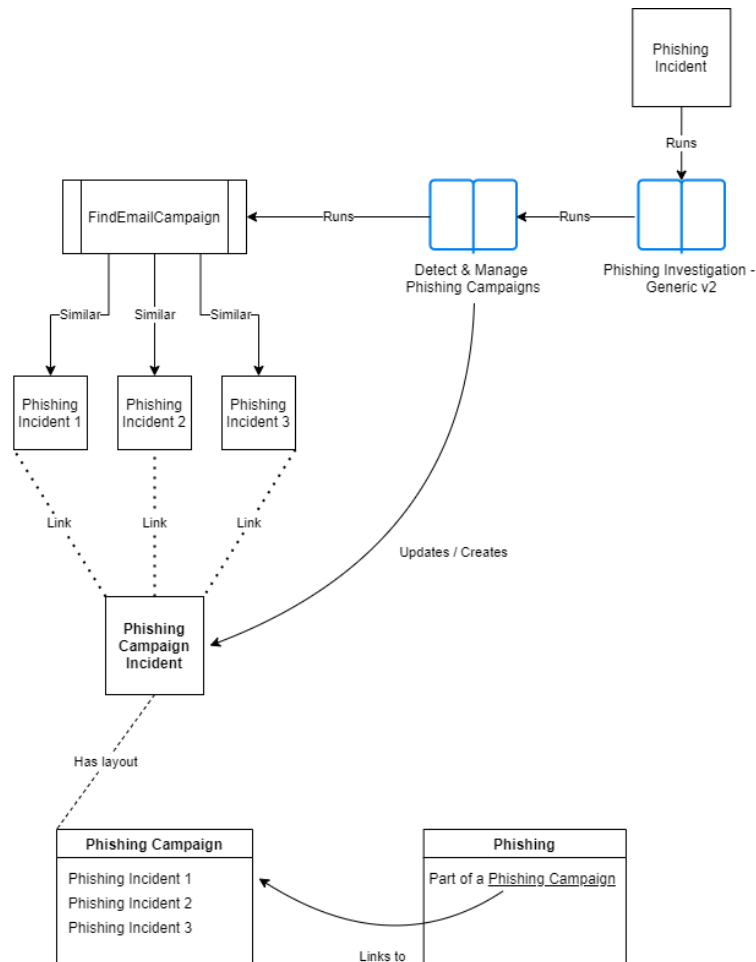


Nota. Fuente: Captura anonimizada – plataforma Cortex XSOAR (2025). Recuperado de <https://cdn.qwiklabs.com/>

Como parte de las iteraciones posteriores del playbook de phishing, se habilitó el módulo de gestión de campañas, que permite correlacionar múltiples incidentes individuales bajo un incidente maestro. Esta funcionalidad se apoya en mecanismos automatizados de detección de similitud entre indicadores, remitentes, asuntos de correo y estructuras comunes en los mensajes reportados. Cuando se identifican patrones repetitivos, XSOAR agrupa los eventos mediante el submódulo “FindEmailCampaign”, generando un “Phishing Campaign Incident” que permite gestionar de forma centralizada la investigación, contención y respuesta del incidente. Esta capacidad de orquestación avanzada no solo mejora la eficiencia operativa del SOC, sino que permite anticipar movimientos de campañas activas, documentar su alcance, y aplicar medidas preventivas de forma más estratégica. La Figura 14 presenta el flujo lógico de esta agrupación automatizada.

Figura 14

Agrupación automatizada de incidentes de phishing en campañas



Nota. Fuente: Cortex XSOAR Phishing Campaign

La agrupación automática de incidentes en campañas se implementó utilizando las capacidades descritas en la documentación oficial de XSOAR para el *Phishing Campaign Pack*, que permiten detectar similitudes entre mensajes, vincular incidentes relacionados y crear un incidente maestro para la gestión centralizada de campañas (Palo Alto Networks, 2025).

3.2.5.4 Playbook de Malware / Endpoint Detection and Response (EDR)

La automatización del análisis y respuesta ante amenazas detectadas en endpoints representa también uno de los pilares fundamentales en la mejora del tiempo de contención (MTTC) dentro del SOC. Particularmente, los incidentes relacionados con archivos maliciosos, procesos anómalos o actividades sospechosas en estaciones de trabajo y servidores fueron priorizados para la construcción de un playbook dedicado en Cortex XSOAR.

Este flujo de automatización fue diseñado para integrarse directamente con la plataforma EDR desplegada en la organización, CrowdStrike Falcon, en coordinación con el sistema de ticketing (ServiceNow), el SIEM (Splunk) y herramientas complementarias de threat intelligence y sandboxing.

El principal objetivo fue reducir el tiempo entre detección, aislamiento y análisis forense inicial, especialmente en aquellos casos en los que el malware es detectado por firmas genéricas, heurísticas o comportamientos que requieren acción inmediata antes de escalar.

Este playbook se desarrolló a partir del paquete *Endpoint Malware Investigation* de Cortex XSOAR, adaptado a las integraciones y flujos específicos de la organización.

Flujo funcional (adaptado desde XSOAR)

El flujo completo se divide en cinco fases principales:

1. Enriquecimiento inicial: Se ejecutan sub-playbooks para enriquecer información sobre el endpoint afectado y sobre el archivo sospechoso. Sub-playbooks: *Endpoint Enrichment - Generic*, *File Enrichment - Generic v2*.
2. Detonación y análisis del archivo: Si el archivo está disponible, se recupera automáticamente desde el endpoint; de lo contrario, se solicita carga manual. Luego, se ejecuta la detonación (es decir, la ejecución de archivos o URL sospechosos dentro de un entorno seguro y aislado) en sandbox para evaluar su comportamiento.

3. Evaluación y contención: Se calcula el nivel de severidad y se evalúa si se aplica un aislamiento automático del host o si se requiere intervención manual para la aprobación. En escenarios confirmados, se ejecuta el sub-playbook *Isolate Endpoint - Generic* y se actualiza el incidente.
4. Hunting y respuesta ampliada: Se inicia una búsqueda de endpoints adicionales comprometidos. Si se detectan, se aíslan automáticamente y se notifica al equipo. Esto permite anticipar movimientos laterales o propagación del malware en la red interna de la organización.
5. Remediación y cierre: Se bloquean los indicadores relacionados, se genera el resumen técnico de investigación, se realiza el *un-isolation* si corresponde, y se cierra el caso.

Con base en el flujo funcional descrito previamente, se realizó un mapeo detallado entre las fases operativas, las acciones ejecutadas, las integraciones involucradas y los responsables asignados dentro del SOC. Este mapeo permite visualizar de manera estructurada la distribución de responsabilidades y los componentes técnicos activados en cada etapa del proceso automatizado, tal como se presenta en la Tabla 15:

Tabla 10

Mapeo del flujo operativo y responsables

Fase	Acción principal	Integración	Responsable	Sub-playbook / módulo
1	Enriquecimiento del endpoint	CrowdStrike Falcon	Analista de Amenazas	Endpoint Enrichment - Generic
1	Enriquecimiento del hash	VirusTotal, fuentes internas	Analista Principal	File Enrichment - Generic

Fase	Acción principal	Integración	Responsable	Sub-playbook / módulo
2	Detonación del archivo	Sandboxing (ej. WildFire)	T3 / SOC Senior	Detonate File - Generic
3	Aislamiento automático o condicional	EDR	Ingeniero de Ciberseguridad (Tier 3)	Isolate Endpoint - Generic
4	Hunting de endpoints adicionales	CrowdStrike RTR / Splunk	Analista Senior SOC	Manual - Hunt for infected endpoints
5	Remediación automatizada	Firewall / EDR	Gerente de Operaciones	Block Indicators - Generic
5	Cierre y documentación	ServiceNow / CMDB	T1 + QA	Generate Investigation Summary Report

Nota. Fuente: elaboración propia en base al flujo estándar de XSOAR

Umbrales y condiciones de automatización

El playbook cuenta con múltiples nodos condicionales que aseguran control en puntos críticos:

- Si no se logra recuperar el archivo automáticamente
 - Paso a modo manual.
- Si *auto isolation* = true y el IOC tiene reputación maliciosa
 - Se ejecuta el sub-playbook *Isolate Endpoint*.
- Si múltiples endpoints presentan comportamientos similares en < 15 minutos
 - Se ejecuta notificación y aislamiento en paralelo.
- Si el analista clasifica el incidente como falso positivo
 - Se ejecuta el cierre automático con etiquetas.

Buenas prácticas aplicadas

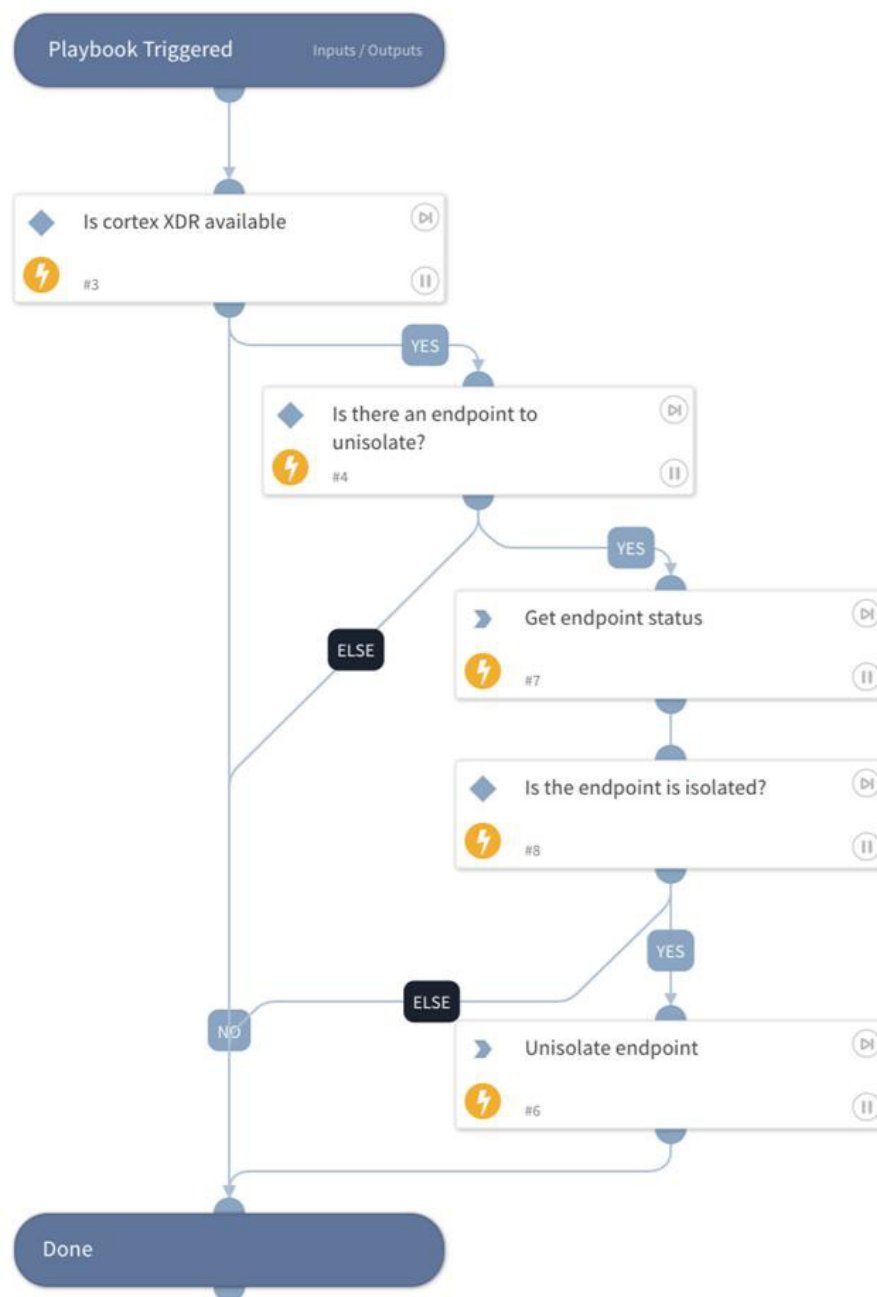
- Rollback planificado, es decir, las acciones de aislamiento pueden revertirse mediante la ejecución del sub-playbook *Unisolate Endpoint*.

- La validación previa en sandbox para evitar que la automatización ejecute acciones destructivas sin contexto.
- Documentación automatizada en ServiceNow y generación de resumen técnico para cada incidente.
- Separación de lógica en sub-playbooks reutilizables (enriquecimiento, bloqueo, hunting).
- Aprobación manual opcional para casos sin IOC confirmado o con comportamiento ambiguo.

Como parte de la fase de remediación y cierre del incidente, se diseñó un playbook específico orientado a revertir el aislamiento aplicado previamente a un endpoint comprometido. Este flujo automatizado permite restaurar la conectividad del equipo una vez validada la contención de la amenaza, asegurando que el proceso se realice de manera controlada y documentada. El diagrama correspondiente se presenta en la Figura 15.

Figura 16

Diagrama del Playbook Unisolate Endpoint



Nota. Fuente: Cortex XDR - Unisolate Endpoint Playbook (2025)

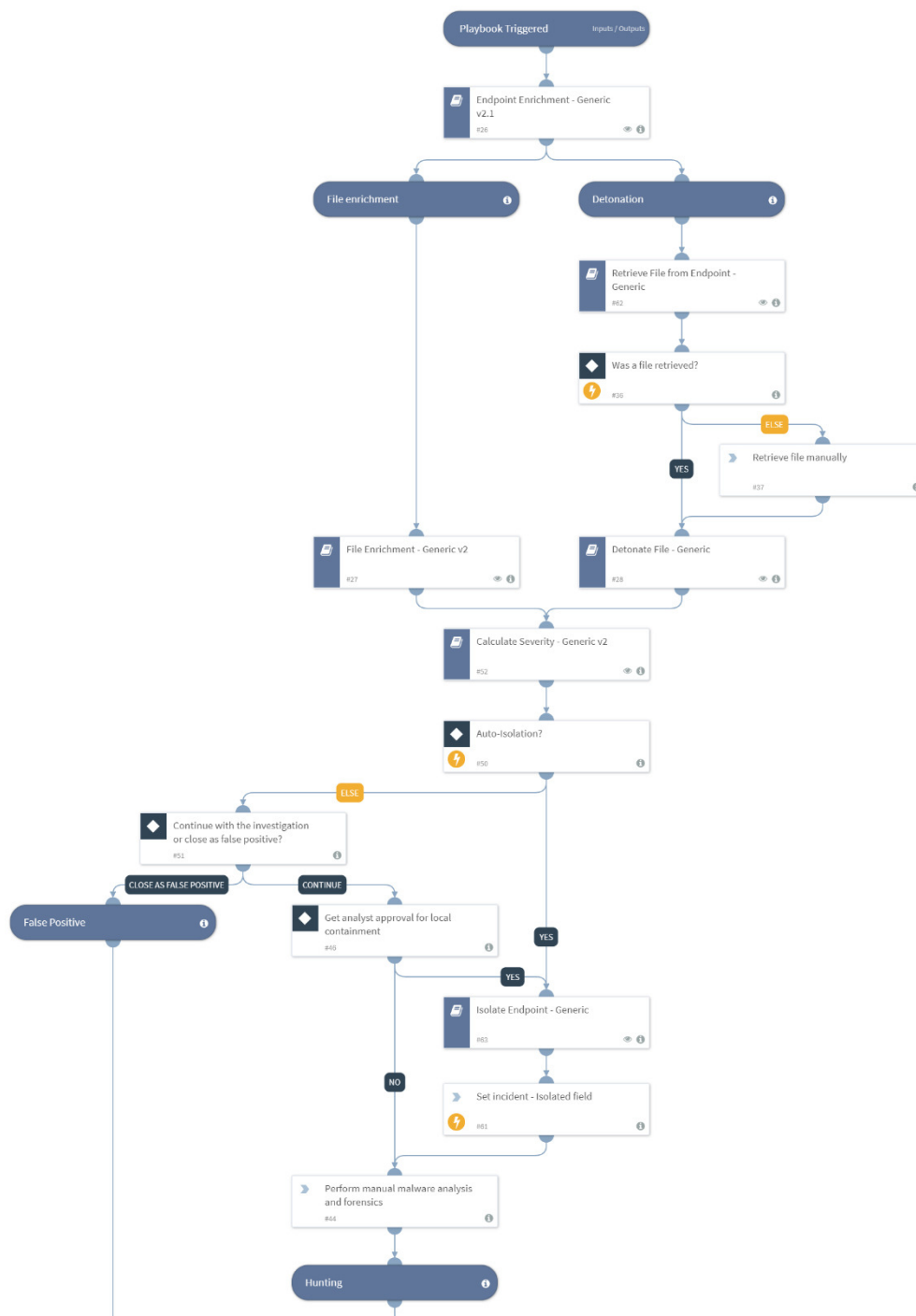
Resultados observados

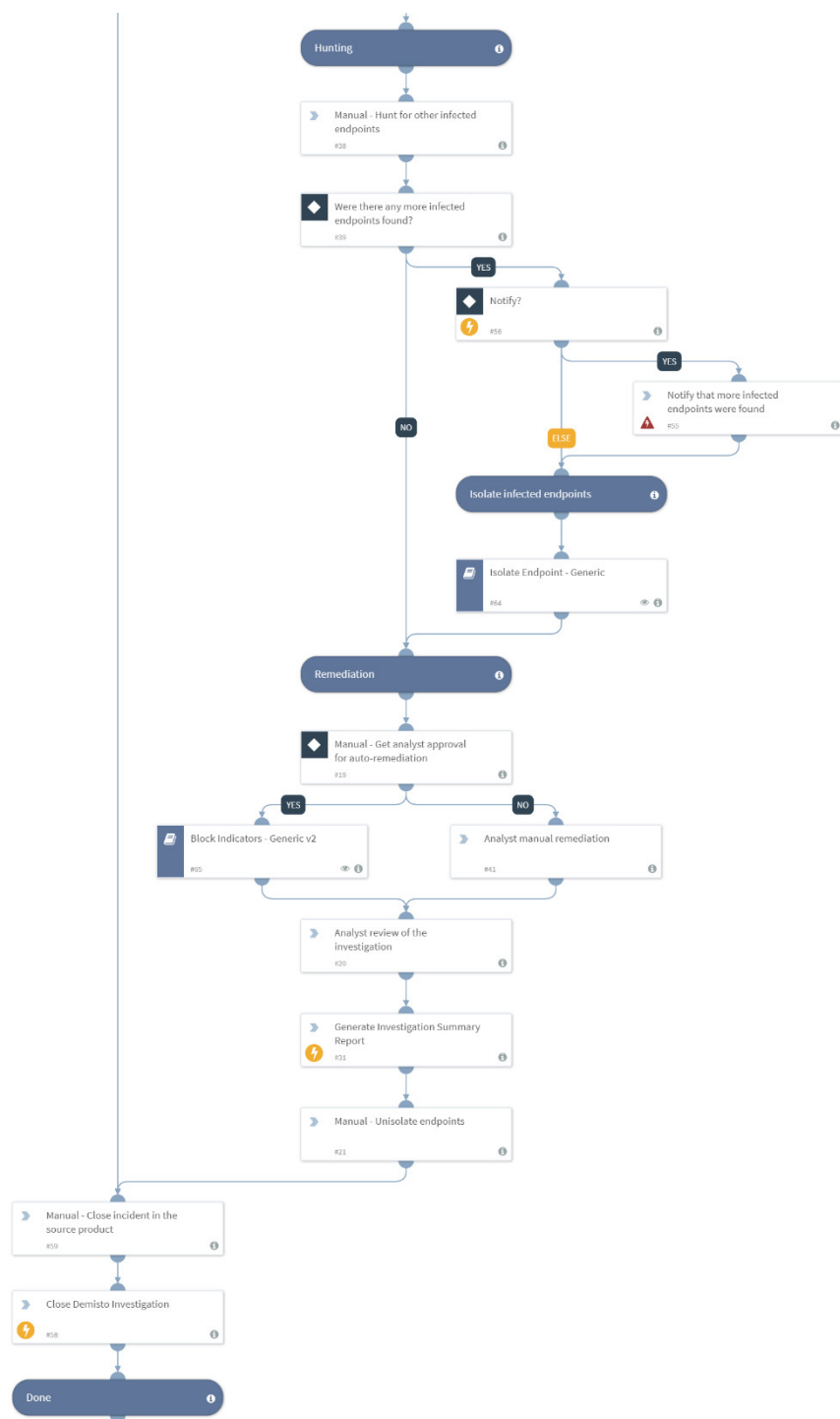
- Reducción del MTTC (Mean Time To Contain) de 1.8 h a 10–15 min para casos confirmados.
- Automatización parcial o total en > 70 % de los incidentes tipo malware genérico.
- Disminución de reingresos del mismo IOC en la red interna en un 60 % por bloqueo preventivo.
- Mejora en el nivel de confianza del SOC al tener visibilidad centralizada del proceso.

Para la gestión de incidentes asociados a posibles infecciones en endpoints, se utilizó el playbook Endpoint Malware Investigation – Generic, el cual concentra las principales etapas de análisis y respuesta automatizada. Este flujo integra tareas de enriquecimiento, análisis del archivo sospechoso y decisiones de contención dentro de una misma secuencia operativa. Su estructura funcional se presenta en la Figura 16.

Figura 16

Diagrama funcional del playbook Endpoint Malware Investigation – Generic





Nota. Flujo automatizado en Cortex XSOAR adaptado para la investigación de malware en endpoints, integrando sub-playbooks de enriquecimiento, detonación, aislamiento, hunting y remediación. Fuente: Documentación oficial de Palo Alto Networks (2025) y entorno operativo del SOC.

3.2.5.5 Playbook de Accesos Sospechosos / Identidad

Introducción

En entornos corporativos que operan con proveedores de identidad como Azure AD y Okta, este último siendo la solución SSO para la presente organización, la detección de intentos de acceso sospechosos representa una prioridad estratégica dentro del SOC. Estos eventos, que incluyen inicios de sesión desde ubicaciones anómalas, patrones inconsistentes de autenticación o manipulación del segundo factor (MFA), son indicativos comunes de fases iniciales de intrusión o abuso de credenciales.

El playbook desarrollado en Cortex XSOAR automatiza la respuesta ante este tipo de incidentes, integrando herramientas como el SIEM (Splunk), el proveedor de identidad federado (Okta), y módulos de enriquecimiento de IPs y usuarios. La lógica se basa en decisiones condicionadas por el tipo de anomalía, el perfil del usuario y el nivel de riesgo detectado.

Activación y flujo lógico

El playbook se activa automáticamente ante:

- Alertas del SIEM clasificadas como *SuspiciousAuthenticationAttempt*.
- Inicios de sesión riesgosos detectados por Okta.
- Eventos de login desde regiones no permitidas o inusuales, o desde IPs identificadas como maliciosas.

A partir de este trigger, se ejecutan tareas de análisis, enriquecimiento y contención. El usuario afectado es evaluado mediante llamadas a la API de Okta y fuentes externas como VirusTotal o IP reputation services. Si se confirma un comportamiento anómalo, se procede a forzar el reinicio del segundo factor (2FA), limpiar sesiones activas o bloquear temporalmente al usuario.

Diagrama del flujo de remediación

La lógica del playbook sigue el modelo propuesto por Palo Alto Networks en su entrada “*Playbook of the Week: Suspicious SSO*”, adaptado al entorno del SOC, como se detalla en la figura 17:

Figura 17

Flujo de remediación ante accesos sospechosos (SSO)

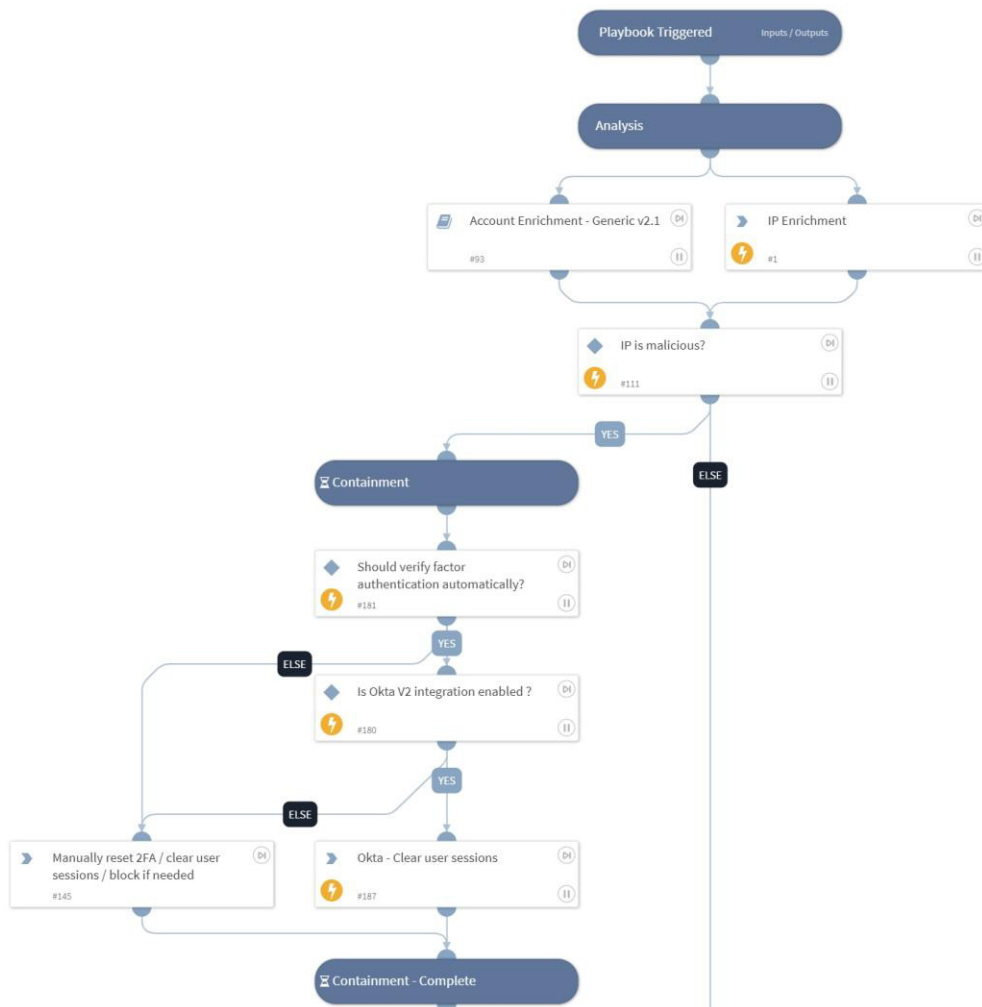


Diagrama del playbook Suspicious SSO adaptado en Cortex XSOAR. Tras detectar un inicio de sesión con una IP sospechosa, se realiza el enriquecimiento del usuario y la IP, y se decide automáticamente si se restablece el segundo factor de autenticación o si se eliminan sesiones activas mediante la integración con Okta. Fuente: Adaptado de Palo Alto Networks (2025). Blog oficial: Playbook of the Week – Suspicious SSO

Para la gestión de accesos sospechosos se implementó un playbook específico orientado a eventos de autenticación anómala detectados en el entorno de identidad. Este flujo integra tareas de enriquecimiento de cuenta e IP, así como evaluación de riesgo y ejecución de acciones correctivas en función de reglas predefinidas.

El detalle del flujo operativo, junto con las integraciones involucradas y los responsables en cada etapa, se presenta en la Tabla 16.

Tabla 11

Flujo operativo del playbook de accesos sospechosos

Paso	Acción	Integración	Resultado	Responsable
1	Recepción de alerta por login sospechoso	Splunk /Okta	Incidente ingestado en XSOAR	Automático
2	Enriquecimiento de cuenta	Okta API	Score de riesgo, historial de sesiones	Analista de Amenazas
3	Enriquecimiento de IP	VirusTotal / AbuseIPDB / MaxMind	Clasificación de IP maliciosa	Analista Senior
4	Evaluación condicional de riesgo	Reglas XSOAR	Decisión: bloquear / forzar 2FA / limpiar sesiones	Ingeniero Tier 3
5	Ejecución de acción automatizada	Okta (vía API)	Sesiones cerradas, MFA reiniciado	Gerente / Tier 3
6	Notificación operativa	Demisto bot (Slack #xsoar-alerts)	Alerta al SOC con detalles del caso	Analistas T1/T2

Nota. Fuente: Elaboración propia.

Umbrales y decisiones automáticas

- Si la IP del login está listada como maliciosa, se procede a limpiar sesiones activas y suspender temporalmente al usuario, se evalúa abrir un ticket para efectuar la rotación de credenciales.
- Si hay login simultáneo desde múltiples ubicaciones, se procede a forzar reinicio del segundo factor de autenticación.
- Si el usuario es VIP o cuenta crítica, solo notificación y revisión manual, con posible escalamiento a un analista senior o lead.
- Si el score de riesgo es bajo y sin historial, se clasifica como falso positivo y se cierra automáticamente.

Resultados observados

- Tiempo promedio de contención reducido a <12 minutos.

- Automatización total en el 75 % de los accesos sospechosos no críticos.
- Reducción significativa de riesgo por sesiones prolongadas sin supervisión.
- Mayor eficiencia en la gestión de MFA y limpieza de sesiones a través de Okta.

Buenas prácticas aplicadas

- Validación manual obligatoria para cuentas privilegiadas.
- Logging completo de acciones automatizadas con trazabilidad en ServiceNow.
- Integración nativa con Slack a través del Demisto bot (bot que permite integrar XSOAR con Slack) para alertas inmediatas.
- Priorización de incidentes basada en combinación de score de IP, comportamiento de usuario y ubicación.
- Separación de escenarios de respuesta para cuentas VIP, cuentas normales y cuentas de servicio.

3.2.5.6 Observabilidad y visibilidad operativa

La observabilidad en un entorno de operaciones de seguridad no se limita a visualizar eventos, sino que implica la capacidad de interpretar el estado de los sistemas, procesos y respuestas automatizadas en tiempo real. Según Gartner (2023), la implementación de mecanismos de visibilidad y alertamiento inmediato es clave para reducir el tiempo de permanencia de un atacante en la red y mitigar el impacto de los incidentes. En el marco de este proyecto, se priorizó el desarrollo de una capa de visibilidad transversal, tanto a nivel de interfaz como de comunicación, que permitiera al SOC actuar con eficiencia y contexto ante incidentes críticos sin depender exclusivamente de interfaces manuales o revisiones periódicas.

Dashboards operativos en XSOAR

La primera capa de observabilidad se habilitó directamente en la consola de XSOAR, donde se diseñó un dashboard operativo personalizado. Este panel se estructuró

en base a widgets filtrados por tipo de incidente, nivel de severidad, estado de ejecución del playbook y origen de la alerta.

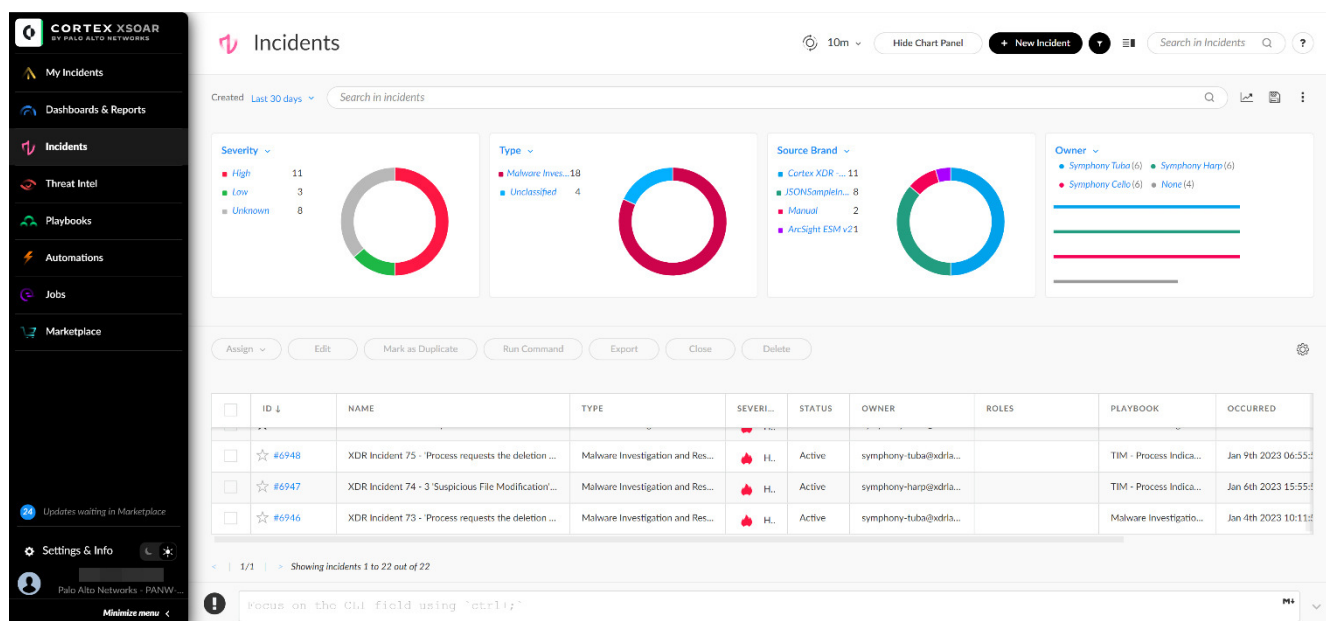
Cada widget muestra visualmente:

- La cantidad total de incidentes abiertos por categoría
- El número de ejecuciones exitosas, fallidas o en espera
- El tiempo promedio de resolución por tipo de alerta
- El desglose de incidentes activos por responsable asignado

Esta interfaz permite al analista del SOC no solo identificar incidentes pendientes, sino también obtener una visión operativa del comportamiento del ecosistema de automatizaciones en su conjunto. Se convierte así en un punto de referencia durante reuniones de coordinación diaria (daily standup), así como en revisiones semanales del equipo de liderazgo. La configuración de este panel permitió centralizar la información operativa en una sola vista, facilitando la supervisión continua del estado de los incidentes y del desempeño de los playbooks automatizados. Un ejemplo de esta visualización se muestra en la Figura 23.

Figura 20

Visualización de alertas en el dashboard de Cortex XSOAR



Nota. Captura del panel principal de XSOAR donde se reflejan incidentes en curso, clasificados por tipo, severidad y estado del playbook asociado. Recuperado de: <https://www.sjutra.com/services/palo-alto-cortex-xsoar/>

Notificación proactiva mediante Demisto Bot

La segunda capa de observabilidad fue implementada a través de una integración con Slack, diseñada para emitir notificaciones estructuradas mediante un bot llamado Demisto Bot, el cual actúa como un canal de alerta en tiempo real para el SOC.

El canal asignado fue #xsoar-alerts, creado específicamente para consolidar todas las alertas generadas por incidentes gestionados en XSOAR, y configurado con políticas de acceso restringido solo al equipo de seguridad y respuesta. Esta integración se basó en el principio de visibilidad inmediata sin intervención, y fue particularmente útil durante turnos remotos, nocturnos o en contextos de carga alta.

Cada vez que se genera una alerta crítica (por ejemplo, reportes de correo malicioso, inicios de sesión sospechosos, detección de malware), el Demisto Bot publica automáticamente un mensaje con los siguientes elementos:

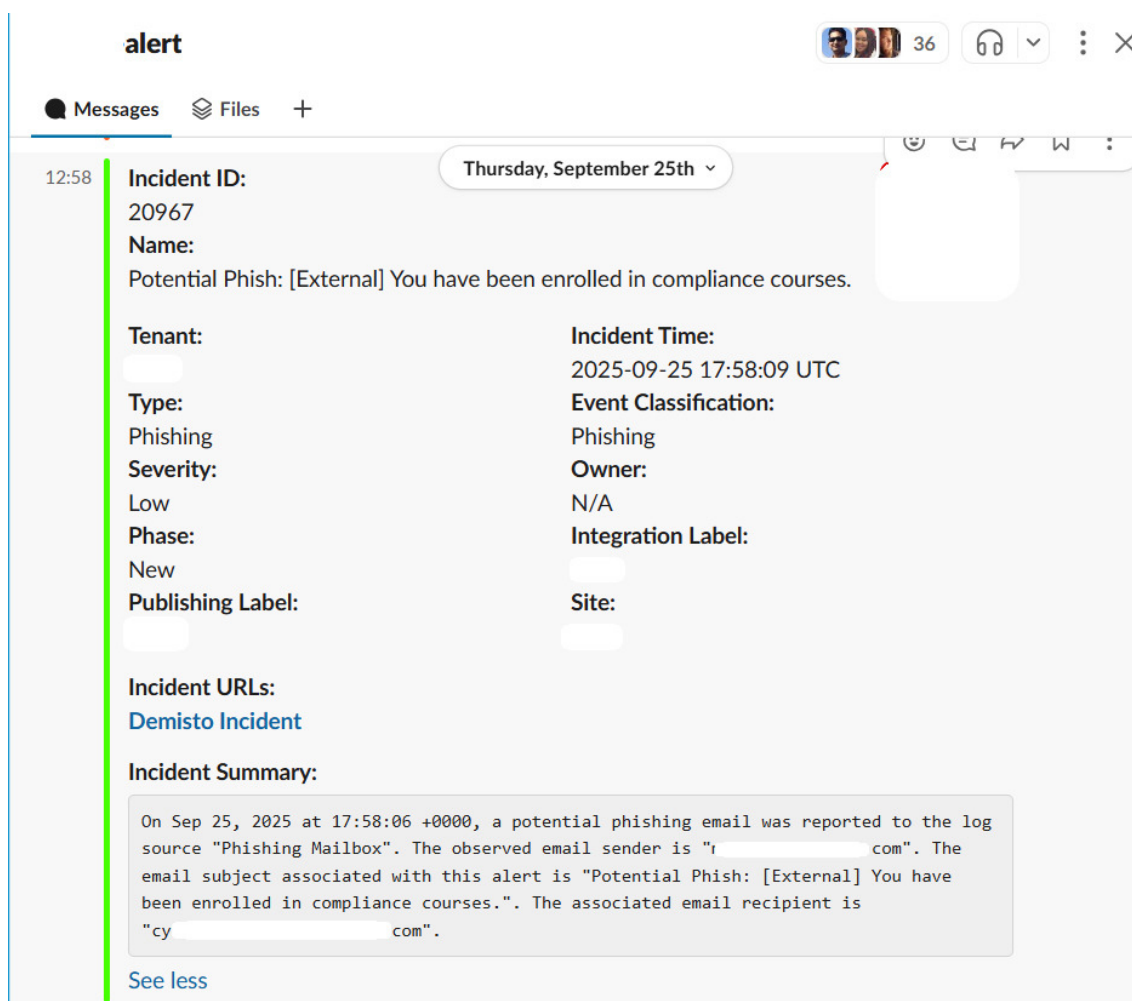
- Tipo de incidente (phishing, malware, acceso sospechoso, etc.)
- Severidad calculada por el playbook
- Indicador de compromiso involucrado (IP, hash, URL, usuario)

- Acción tomada por la automatización (bloqueo, cierre, escalamiento)
- Enlace directo al incidente en XSOAR

Esta configuración permitió que el equipo reciba información contextualizada en tiempo real, sin necesidad de monitorear constantemente la consola principal. Un ejemplo de estas notificaciones automatizadas se muestra en la Figura 24.

Figura 22

Notificación automatizada del Demisto Bot en Slack



Nota. Notificación automatizada emitida por XSOAR tras la ejecución del playbook de phishing. El mensaje incluye detalles del incidente y un enlace directo al panel de respuesta.

Este canal no sustituye el monitoreo clásico del dashboard, sin embargo, permite reducir significativamente el tiempo medio hasta el reconocimiento de un incidente (MTTA), al enviar alertas estructuradas al instante y permitir una revisión directa desde cualquier dispositivo móvil o estación de trabajo. Este tipo de integración está alineada con las buenas prácticas recomendadas por el SANS Institute (2022), que resalta el uso de plataformas de colaboración como Slack para mejorar la coordinación en tiempo real de los equipos de seguridad.

Diseño del canal y políticas de seguridad

El canal #xsoar-alerts fue implementado siguiendo políticas internas que contemplan:

- Acceso solo para personal del SOC, Ingenieros de Seguridad y Seguridad de Producto (prodsec)
- Registro de todos los mensajes generados por el bot en logs persistentes
- Prohibición de respuestas manuales al bot
- Separación lógica de canales por función: #xsoar-alerts (alertas), #xsoar-dev (desarrollo)

Esta segmentación favorece la gobernanza y evita discordancias operativas entre flujos informativos, de análisis y de ingeniería. Tal como señala Sridharan (2018), “un sistema observable es un sistema accionable”; es decir, la visibilidad no debe ser solo un punto de monitoreo sino una herramienta para actuar con inmediatez y contexto. En este proyecto, se diseñaron ambas modalidades como complementarias.

Resultados observables tras su implementación

- Reducción del MTTA (Mean Time To Acknowledge) de eventos críticos: de ~28 minutos promedio a menos de 8 minutos.
- Mayor involucramiento del equipo de respuesta incluso fuera de la consola principal de XSOAR.
- Alertas uniformes, estructuradas y sin ambigüedad, con trazabilidad y acceso directo.
- Validación satisfactoria durante simulacros de respuesta rápida, en donde el 100 % de los analistas respondió vía Slack en <10 minutos.

3.2.5.7 Calidad, seguridad y resiliencia de las automatizaciones

A medida que se despliegan procesos automatizados en ambientes críticos como lo es un SOC, se vuelve indispensable implementar prácticas que aseguren la calidad del código, la seguridad de las acciones ejecutadas y la resiliencia del sistema ante errores o escenarios no previstos. Este punto describe los mecanismos adoptados durante el proyecto para garantizar que los playbooks desarrollados no solo cumplieran su función operativa, sino que lo hicieran de forma confiable, segura y auditable.

Validación técnica y gobernanza

Cada automatización fue desplegada bajo un proceso formal de validación en entorno controlado. Antes de ser promovidos a producción, los playbooks debían cumplir con:

- Criterios de aceptación definidos (DoR/DoD) ya documentados en la sección 3.2.5.2.
- Revisión entre pares (peer review) realizada por un analista senior.
- Pruebas unitarias de cada sub-playbook o bloque condicional.
- Validación funcional por parte del equipo de ingeniería de ciberseguridad.
- Aprobación técnica del equipo de Liderazgo.

Estas etapas aseguraban la correcta comprensión del flujo, la gestión adecuada de excepciones y la documentación completa para cada decisión automatizada.

Seguridad en la ejecución

Para garantizar que ninguna automatización pudiera afectar la disponibilidad o integridad de sistemas críticos, se adoptaron las siguientes medidas:

- Entornos independientes para desarrollo, pruebas en sandbox y producción.
- Restricción de privilegios mediante API Tokens de uso limitado y autenticación federada vía Okta.
- Control de ejecución crítica: las acciones sensibles (como aislamiento de endpoints o cierre de sesiones activas) solo se ejecutan si el nivel de riesgo excede un umbral predefinido.
- Exclusión de cuentas VIP mediante listas blancas dinámicas integradas a los flujos.
- Fail-safe automático en caso de error en una integración, se registra el fallo y se deriva el incidente al analista.

Mecanismos de resiliencia y continuidad operativa

Con el fin de minimizar el impacto de fallos inesperados y garantizar la recuperación, se implementaron controles de resiliencia como:

- Plan de rollback documentado para cada acción destructiva.

- Retención de versiones anteriores de los playbooks (con logs de cambios).
- *Kill switch* manual disponible en la interfaz de XSOAR, que permite desactivar un playbook ante comportamiento anómalo.
- Alertas ante fallos: cualquier error de ejecución (por ejemplo, token expirado, API caída, timeout) genera automáticamente una notificación en el canal #xsoar-alerts vía Demisto Bot.
- Revisión de métricas de fallos por parte del equipo de automatización.

3.3 Evaluación

3.3.1 Evaluación económica

La evaluación económica del proyecto se centra en el análisis de los costos y beneficios asociados a la implementación de la plataforma de automatización Cortex XSOAR dentro del Centro de Operaciones de Seguridad. Esta solución permitió orquestar la respuesta ante incidentes cibernéticos frecuentes mediante flujos automáticos, reduciendo significativamente los tiempos de atención, la carga operativa del personal y los errores humanos asociados al manejo manual de alertas.

El proyecto fue desarrollado a lo largo de seis Sprints distribuidos en aproximadamente seis meses. Durante ese periodo se automatizaron casos de uso como análisis de mensajes sospechosos, contención de malware en endpoints, validación de accesos anómalos, clasificación de alertas del SIEM y estandarización de procesos en el manejo de tickets.

La presente evaluación se estructura en tres rubros principales:

- Costos del personal operativo y técnico involucrado.
- Costos de licenciamiento de herramientas necesarias.
- Costos de soporte y mantenimiento de los flujos desarrollados.

El detalle se presenta en la Tabla 17:

Tabla 12*Costos del personal asignado al proyecto*

Rol	Costo mensual (USD)	Meses involucrados	Costo total (USD)
Ingeniero de SOAR	\$5,000	6	\$30,000
Analista Principal de Seguridad	\$4,000	6	\$24,000
Analistas SOC (Tier 1–2–3)	\$6,000	6	\$36,000
Integrador de plataformas	\$4,000	6	\$24,000
Coordinador / Product Owner	\$2,800	6	\$16,800
Total	—	—	\$130,800

Nota. Costos estimados en función de dedicación parcial durante el desarrollo del proyecto.

Fuente: Elaboración propia, con base en promedios salariales en ciberseguridad (Payscale, 2024; ZipRecruiter, 2024).

Los costos de personal presentados corresponden a una valorización del esfuerzo del equipo interno del SOC durante la fase de implementación del proyecto. Dichos recursos ya formaban parte de la estructura organizacional y no implicaron una contratación adicional ni un desembolso incremental atribuible exclusivamente al proyecto. Por tanto, estos costos no fueron considerados dentro del flujo de caja utilizado para el cálculo del VAN y TIR, sino que se consideran únicamente los costos incrementales relacionados con licenciamiento, mantenimiento y mejora continua de los playbooks implementados.

En función de los costos incrementales asociados directamente a la operación y sostenibilidad de la solución, se estimaron los gastos anuales de licenciamiento de las herramientas involucradas. El detalle se presenta en la Tabla 18.

Tabla 13*Costos de licencias de software*

Descripción	Cantidad de licencias	Costo anual (USD)	Costo total (USD)
Licencia Cortex XSOAR	1	\$20,000	\$20,000
Licencia ServiceNow	5	\$2,000	\$10,000
Integración Proofpoint	1	\$5,000	\$5,000
Slack API	1	\$0 (versión gratuita)	\$0
Total	—	—	\$35,000

Nota. Costos anuales estimados. Incluyen solo los componentes utilizados directamente en los flujos automatizados.

Adicionalmente, la organización destinó un presupuesto inicial aproximado de \$90,000 para la ejecución del proyecto, el cual incluyó costos asociados a configuración inicial, puesta en producción, ajustes técnicos y horas dedicadas específicamente a la implementación. Este monto se considera la inversión inicial del proyecto y se registra en el Año 0 del flujo de caja.

Una vez desplegados los playbooks y estabilizadas las integraciones principales, se estimaron los costos asociados a su mantenimiento operativo y mejora continua. Estos montos consideran actividades de actualización, ajustes ante cambios en herramientas externas y revisión periódica de métricas de desempeño. El detalle se presenta en la Tabla 19:

Tabla 149*Costos anuales de mantenimiento y mejora continua de la solución*

Descripción	Costo mensual (USD)	Meses estimados	Costo total (USD)
Mantenimiento de playbooks	\$500	12	\$6,000
Ajustes de integraciones	\$500	12	\$6,000

Descripción	Costo mensual (USD)	Meses estimados	Costo total (USD)
Revisión y pruebas de métricas	\$400	12	\$4,800
Total anual	—	—	\$16,800

Nota. Estimación de soporte técnico y ajustes funcionales posteriores al despliegue.

Fuente: Elaboración propia.

3.3.2 Interpretación del VAN y TIR

Para determinar la viabilidad financiera del proyecto, se calculó el Valor Actual Neto (VAN) y la Tasa Interna de Retorno (TIR) a partir del flujo de caja proyectado durante un horizonte de cinco años, periodo que además permite evaluar la estabilidad operativa de la solución en el mediano plazo. El análisis considera como beneficios los ahorros derivados de la reducción de horas-hombre en los procesos automatizados, de acuerdo con las métricas estimadas para cada caso de uso. Para el cálculo del VAN se adoptó una tasa de descuento del 10 %, valor referencial utilizado en la evaluación de proyectos tecnológicos con riesgo moderado, representando el costo de oportunidad del capital para la organización.

La Tabla 20 presenta una estimación teórica del beneficio operativo potencial derivado de la automatización de distintos casos de uso, calculada a partir del ahorro de horas operativas del equipo SOC. No obstante, para el análisis financiero se adoptó un enfoque que considera únicamente una fracción de dicho beneficio potencial, con el fin de evitar sobreestimaciones y reflejar un escenario realista de adopción gradual de la automatización.

Tabla 20*Beneficios operativos estimados por caso de uso*

Caso de uso	Horas ahorradas/año	Costo/hora (USD)	Beneficio anual (USD)
Análisis de mensajes sospechosos	2,000 hrs	\$50	\$100,000
Contención de malware	1,200 hrs	\$50	\$60,000
Accesos inusuales	900 hrs	\$50	\$45,000
Clasificación de alertas SIEM	800 hrs	\$50	\$40,000
Total anual estimado	4,900 hrs	—	\$245,000

Nota. Fuente: Elaboración propia, basado en estimaciones del SOC y valores de mercado (IBM, 2024; Forrester, 2023).

A diferencia de un modelo de comercialización directa, el presente proyecto no genera ingresos por venta de producto, sino beneficios económicos indirectos derivados de la optimización operativa. Estos beneficios se traducen en reducción de horas-hombre, disminución de reprocesos y mitigación temprana de incidentes, los cuales impactan directamente en la eficiencia del área de ciberseguridad.

Si bien el beneficio operativo potencial anual asciende a \$245,000, para efectos del análisis financiero se adoptó un enfoque conservador, considerando únicamente una fracción de dicho beneficio durante los primeros años de operación. Esto responde a una adopción progresiva de la automatización dentro del SOC y a la posibilidad de ajustes iniciales en los playbooks antes de alcanzar su máxima eficiencia. El detalle se presenta en la Tabla 21:

Tabla 15*Flujo de caja del proyecto*

Año	Costos (USD)	Beneficios (USD)	Flujo neto (USD)
0	– \$90,000	\$0	– \$90,000
1	–51,800	\$ 80,000	\$28,200
2	–51,800	\$ 84,000	\$32,200
3	–51,800	\$ 88,200	\$36,400
4	–51,800	\$ 92,610	\$40,810
5	–51,800	\$ 97,240	\$45,440

Nota. Fuente: Elaboración propia.

Resultado financiero del proyecto

- VAN estimado: \$45,698
- TIR estimado: 23 %
- Recuperación de la inversión: 4 años

Los resultados muestran que el proyecto es rentable y financieramente viable, incluso bajo estimaciones conservadoras. El VAN positivo indica que, descontando el valor del dinero en el tiempo, el proyecto genera un retorno neto significativo. La TIR, superior a la tasa de descuento del 10 %, demuestra que la inversión en automatización no solo se recupera rápidamente, sino que multiplica su valor a lo largo del horizonte de cinco años.

La recuperación de la inversión inicial se alcanza aproximadamente en el tercer año de operación, lo que resulta razonable para proyectos tecnológicos de transformación operativa. Tanto el VAN como la TIR superan ampliamente los valores mínimos de aceptación, lo que justifica la inversión desde el punto de vista financiero.

CAPITULO IV – REFLEXIÓN CRÍTICA DE LA EXPERIENCIA

El desarrollo del presente Trabajo de Suficiencia Profesional permitió aplicar de manera práctica los conocimientos de ciberseguridad en un entorno real de operación SOC, evidenciando el impacto positivo de la automatización en la eficiencia operativa y la reducción de tiempos de respuesta ante incidentes. La implementación de playbooks automatizados contribuyó a estandarizar procesos, mejorar la trazabilidad de los incidentes y fortalecer la toma de decisiones basada en métricas como MTTR, demostrando el valor estratégico de la automatización en la gestión de la seguridad.

Desde el punto de vista técnico, el proyecto facilitó el uso e integración de herramientas especializadas como Cortex XSOAR, Splunk, soluciones de EDR y plataformas de gestión de identidades, ticketing y comunicación interna. Asimismo, la adopción de un enfoque basado en Sprints orientados a casos de uso permitió aplicar una metodología iterativa que favoreció la mejora continua y la adaptación progresiva de las automatizaciones a las necesidades reales del entorno operativo, combinando marcos teóricos con prácticas flexibles.

Finalmente, esta experiencia permitió fortalecer habilidades de liderazgo y gestión al asumir funciones de coordinación con equipos multidisciplinarios ubicados en diferentes zonas horarias, promoviendo una comunicación efectiva y una adecuada alineación entre los objetivos técnicos y operativos. No obstante, se identificaron limitaciones asociadas a la dependencia de información externa y a la necesidad de ajustes continuos en los playbooks, lo que reafirma que la automatización de la respuesta a incidentes es un proceso evolutivo que requiere revisión y madurez constante.

CAPITULO V – CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

El proyecto de automatización de la respuesta a incidentes de ciberseguridad mediante la implementación de Cortex XSOAR permitió abordar de manera efectiva el problema de la baja estandarización y la alta carga operativa existente en el Centro de Operaciones de Seguridad. A través de la centralización de alertas, la orquestación de

acciones de respuesta y la definición de flujos automatizados, el proyecto logró la mejora en la automatización de procesos, la eficiencia operativa, reducción en los tiempos de respuesta y fortalecer la capacidad de la organización para enfrentar incidentes de seguridad en el entorno.

Se logró la integración de las principales herramientas de seguridad en una plataforma SOAR centralizada, lo que permitió unificar la gestión de incidentes y reducir la dependencia de procesos manuales, facilitando una respuesta coordinada, trazable y alineada con las buenas prácticas del SOC.

La definición y ejecución de playbooks automatizados contribuyó a establecer procedimientos consistentes y repetibles para la atención de incidentes de seguridad, disminuyendo la variabilidad operativa entre analistas y asegurando una aplicación homogénea de los criterios de severidad y escalamiento.

Mediante la normalización de campos, estados y métricas dentro de la gestión de incidentes se mejoró la trazabilidad de cada caso, lo cual facilitó el análisis posterior y permitió habilitar una medición objetiva del desempeño operativo, especialmente en términos de MTDD y MTTR.

La integración de mecanismos de notificación y comunicación automática con los equipos internos fortaleció la coordinación durante la respuesta a incidentes, mejoró la visibilidad del estado de cada evento y contribuyó a una operación más eficiente y alineada entre las distintas áreas involucradas.

5.2. Recomendaciones

En base a los resultados obtenidos durante el desarrollo del proyecto, se recomienda mantener un proceso continuo de revisión y actualización de los playbooks implementados, considerando la evolución constante de las amenazas y los cambios en el entorno tecnológico de la organización. En particular, se sugiere realizar una evaluación anual de los flujos automatizados e integraciones con el fin de asegurar su vigencia y efectividad.

Asimismo, se recomienda extender el enfoque metodológico basado en Sprints orientados a casos de uso a otras áreas del ámbito de ciberseguridad, tales como la gestión de vulnerabilidades, la respuesta a incidentes de identidad. Este enfoque permitiría escalar

progresivamente la automatización, reduciendo riesgos y facilitando la validación incremental de resultados.

Finalmente, como trabajo futuro, se recomienda evaluar la implementación progresiva de capacidades basadas en inteligencia artificial orientadas al análisis y parsing de contenido (correos, logs y descripciones de alertas), así como ampliar el uso de fuentes externas de información de amenazas, con el objetivo de mejorar la eficiencia y madurez operativa del SOC.

5.3 Fuentes de información

- Deloitte. (2023). *Cybersecurity in Latin America: regional insights and challenges*. Deloitte Insights. <https://www2.deloitte.com>
- ESET. (2024). *ESET Security Report 2024: amenazas en Latinoamérica*. ESET Latinoamérica. <https://www.eset.com>
- IBM. (2024). *Cost of a Data Breach Report 2024*. Ponemon Institute – IBM Security. <https://www.ibm.com/reports/data-breach>
- Ministerio Público del Perú. (2024). *Estadísticas de denuncias por delitos informáticos – primer semestre 2024*. Lima: Ministerio Público. <https://www.mpf.n.gob.pe>
- Verizon. (2024). *Data Breach Investigations Report (DBIR) 2024*. Verizon Enterprise. <https://www.verizon.com/business/resources/reports/dbir>
- Take-Two Interactive y Zynga. (2022, 10 de enero). Take-Two to acquire all outstanding shares of Zynga in a cash and stock transaction valued at \$9.86 per share, total enterprise value approximately \$12.7 billion. Business Wire. <https://www.businesswire.com/news/home/20220110005389>
- Grand View Research. (2024). *Video Game Market Size, Share and Growth Report, 2030*. Grand View Research. <https://www.grandviewresearch.com/industry-analysis/video-game-market>
- Trade Policy and Analysis Branch, U.S. Department of Commerce. (2024). *Media & Entertainment: Video Games Sector*. <https://www.trade.gov/media-entertainment-video-games-sector>

- ASIS. (2023). *Automatización del SIEM mediante tecnología SOAR: Simplificando la ciberseguridad*. ASIS Perú.
<https://www.asis.org.pe/blog/item/252-automatizacion-del-siem-mediante-tecnologia-soar-simplificando-la-ciberseguridad>
- Palo Alto Networks. (2024). *Cortex XSOAR: Security Orchestration, Automation and Response*. Palo Alto Networks.
<https://www.paloaltonetworks.com/cortex/xsoar>
- BlueVoyant. (2023). *What is SOAR and how does it work?*
<https://www.bluevoyant.com>
- Shaukat, K., Alam, T. M., Hameed, I. A., Luo, S., & Li, J. (2024). IC-SECURE: “Intelligent system for assisting security experts in generating playbooks for automated incident response.” *arXiv:2401.12345*.
<https://arxiv.org/abs/2401.12345>
- Palomino Cárdenas, J. M., Cuneo Torres, A. M. E., & Gutiérrez Arana, E. J. (2024). *Modelo de desarrollo de reglas de correlación para la detección y alerta de ransomware* [Tesis de maestría, Universidad Peruana de Ciencias Aplicadas]. Repositorio Institucional UPC. <http://hdl.handle.net/10757/683792>
- Palo Alto Networks. (s.f.). *Phishing campaign pack — Cortex XSOAR documentation*. <https://xsoar.pan.dev/docs/reference/packs/phishing-campaign>
- Sridharan, C. (2018). *Distributed systems observability*. Sebastopol, CA: O’Reilly Media.
- Investopedia. (s. f.-a). *Net Present Value (NPV)*.
<https://www.investopedia.com/terms/n/npv.asp>
- Investopedia. (s. f.-b). *Internal Rate of Return (IRR)*.
<https://www.investopedia.com/terms/i/irr.asp>
- LibreTexts. (2024). *Internal Rate of Return (IRR)*. <https://biz.libretexts.org/>
- Payscale. (2024). *Cybersecurity Analyst Hourly Pay*. <https://www.payscale.com>
- ZipRecruiter. (2024). *Cyber Security Analyst Salary*.
<https://www.ziprecruiter.com>
- Forrester. (2023). *Total Economic Impact of IBM SOAR*.
<https://www.onexte.com/wp-content/uploads/2023/02/Forrester-Report-The-Total-Economic-Impact-of-IBM-Security-SOAR.pdf>
-

5.4 Glosario

Alerta: Notificación generada por una herramienta de seguridad que indica un evento potencialmente anómalo o malicioso y que requiere análisis.

Caso de uso: Escenario específico de seguridad que describe una situación recurrente susceptible de ser automatizada mediante un playbook.

Correlación de eventos: Proceso mediante el cual se relacionan múltiples eventos de distintas fuentes para identificar un posible incidente de seguridad.

EDR (Endpoint Detection and Response): Solución de seguridad orientada a la detección, análisis y respuesta ante amenazas en equipos finales.

IOC (Indicator of Compromise): Evidencia técnica que indica la posible presencia de una actividad maliciosa, como direcciones IP, hashes o dominios.

MTTD (Mean Time to Detect): Métrica que mide el tiempo promedio que transcurre desde que ocurre un incidente hasta que es detectado.

MTTR (Mean Time to Respond): Métrica que mide el tiempo promedio necesario para contener y responder a un incidente de seguridad.

Orquestación: Coordinación automatizada de acciones entre múltiples herramientas de seguridad para ejecutar una respuesta integrada.

Parsing: Proceso de extracción y estructuración de información relevante a partir de contenido no estructurado, como correos electrónicos o logs.

Playbook: Flujo automatizado que define las acciones, decisiones e integraciones necesarias para responder a un tipo específico de incidente.

Sandbox: Entorno aislado utilizado para analizar archivos o comportamientos sospechosos sin afectar sistemas productivos.

SIEM (Security Information and Event Management): Plataforma que centraliza, correlaciona y analiza eventos de seguridad provenientes de múltiples fuentes.

SOC (Security Operations Center): Unidad organizacional encargada del monitoreo, análisis y respuesta a incidentes de ciberseguridad.

SOAR (Security Orchestration, Automation and Response): Enfoque tecnológico que integra orquestación y automatización para mejorar la respuesta a incidentes.

Sprint: Unidad iterativa de trabajo orientada a la automatización de un caso de uso específico, con entregables verificables.

Tenant: Entorno lógico independiente dentro de una plataforma compartida, utilizado para separar configuraciones y datos.

Triage: Proceso inicial de clasificación y priorización de alertas o incidentes según su impacto y criticidad.

ANEXOS