UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
SEGURIDAD DE LA INFORMACIÓN
RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:

PROYECTO DE TITULACIÓN CON COMPONENTES DE INVESTIGACIÓN APLICADA Y/O DE DESARROLLO

TEMA:

CREACIÓN DE EQUIPOS DE RESPUESTA A INCIDENTES (SOC) PARA EL GAD MUNICIPAL DEL CANTÓN CUENCA

AUTORES:

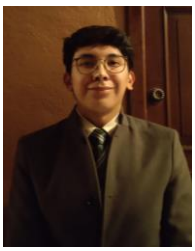
LUIS MATEO ÁLVAREZ BERMEO
RENÉ RAFAEL OCHOA CALDERÓN

DIRECTOR:

JUAN CARLOS DOMÍNGUEZ AYALA

CUENCA – ECUADOR
2025

Autores:



Luis Mateo Álvarez Bermeo
Ingeniero en Telecomunicaciones.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
lalvarezb@est.ups.edu.ec

René Rafael Ochoa Calderón
Ingeniero en Telecomunicaciones.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
rochoac2@est.ups.edu.ec

Dirigido por:

Juan Carlos Domínguez Ayala
Ingeniero de Sistemas.
Maestría en Redes de Comunicación.
jdominguez@ups.edu.ec

DEDICATORIA

Dedicatoria de Luis Mateo Álvarez Bermeo

Quiero dedicar esta tesis a mi familia, quienes son mi más grande impulso para seguir adelante. A mis padres, quienes me orientaron por el camino del bien, velaron por mi bienestar y se han sacrificado para darme un buen estilo de vida. Deseo que con esta nueva etapa de mi vida se enorgullezcan de este logro, porque es de y para ustedes. Sobre todo, estoy agradecido con Dios por tenerlos a mi lado. Los amo.

De este modo, este trabajo está dedicado a mis hermanas Gaby, Daysi y Kate, quienes se han presentado como mis consejeras personales, en quienes confío todos mis secretos y que siempre han acompañado en cada situación complicada.

También quiero nombrar a todas las personas que han sido parte fundamental en este nuevo capítulo de mi vida: familia y amigos. Este entorno de personas me ha brindado su apoyo hasta el día de hoy. Aunque no pueda nombrarlos a todos, han formado a la persona que soy, marcándome con sus palabras, acciones y enseñanzas al cruzar este camino.

Por último, pero no menos importante, quiero dedicar esta tesis a Dios, ya que Él me permitió estar aquí, junto a las personas que aprecio, sin pedir nada a cambio.

Dedicatoria de René Rafael Ochoa Calderón

Dedico este proyecto, en primer lugar, a mi familia, mi pilar más fuerte, y en especial a mis padres, quienes representan para mí los seres más importantes y queridos.

También quiero dedicar este trabajo de titulación a todas aquellas personas que me brindaron su apoyo, consejo y guía a lo largo del camino.

Este trabajo es el resultado de la constancia y el esfuerzo, por lo que deseo compartir esta dedicatoria con mi compañero de tesis, con quien enfrenté y superé este desafío académico.

AGRADECIMIENTO

Agradecimiento de Luis Mateo Álvarez Bermeo

En primer lugar, quiero exponer mis sinceros agradecimientos a mi familia, quienes con su apoyo y consejos me ayudaron a crecer como persona. A mis padres, quienes son los pilares para alcanzar mis objetivos académicos y personales. A mis hermanas, quienes me ayudaron a ver el mundo desde otras perspectivas, gracias a las experiencias que compartieron conmigo.

Quiero mencionar también a mis amigos, los que estuvieron y los que conocí en esta nueva etapa de mi vida, en especial a René, Sebastián y Santiago, con quienes comparto una amistad que viene desde la universidad, y que siempre podrán contar con mi apoyo en cualquier instante de sus vidas.

Agradezco profundamente al Ing. Juan Carlos Domínguez Ayala, quien nos guio en este proceso de titulación. Extiendo también mi gratitud a los docentes que nos entregaron sus conocimientos durante este año de maestría.

Quiero agradecer al GAD Municipal de Cuneca, por recibirnos con las puertas abiertas para el desarrollo del presente tema de titulación, al Ing. Gerardo Gordillo, quien nos brindó su ayuda, guía y conocimiento para tener un mejor entendimiento corporativo en el desarrollo de este proyecto.

Por último, pero no menos importante, estoy agradecido con Dios por mantenerme con salud, junto a las personas que quiero, además por brindarme conocimiento y la sabiduría para afrontar esta etapa de mi vida.

Agradecimiento de René Rafael Ochoa Calderón

Quiero empezar agradeciendo de todo corazón a mis padres, por haberme permitido alcanzar una de las metas más importantes de mi vida. Pero, sobre todo, por su inquebrantable apoyo para lograrlo. También estoy profundamente agradecido con mi compañero de la tesis, con él que cometimos juntos los errores y alcanzamos el éxito juntos.

También le debo mi mayor agradecimiento a los profesores que, a lo largo de este año, con su dedicación y enseñanzas, me dejaron mucho más de lo que creen que han hecho para llevarme a este punto.

Un agradecimiento especial al GAD Municipal del cantón Cuenca por permitirnos desarrollar este proyecto dentro de su institución, lo cual enriqueció mucho nuestra experiencia.

No puedo dejar de agradecer, y mencionar al ingeniero Juan Carlos Domínguez, cuyo apoyo y guía fueron fundamentales. Finalmente, debo agradecer a mis amigos y compañeros Santiago, Mateo y Sebastián. Su apoyo y amistad hicieron que el camino sea más llevadero.

Tabla de Contenido

CREACION DE EQUIPOS DE RESPUESTA A INCIDENTES (SOC) PARA EL GAD MUNICIPAL DEL CANTON CUENCA.

AUTOR(ES):

LUIS MATEO ALVAREZ BERMEO, RENE RAFAEL OCHOA CALDERON

Resumen

Este proyecto de titulación propone el diseño de un SOC (Centro de Operaciones de Seguridad) para el GAD Municipal del cantón Cuenca, con el objetivo de establecer una estructura operativa que permita monitorear y responder a los incidentes de seguridad de la información que puedan afectar a la institución.

Este trabajo parte de un análisis organizativo y tecnológico del GAD municipal. Se propone una estructura escalable, orientada a la gestión eficiente de incidentes. En esta propuesta se definieron roles para el equipo SOC, los niveles jerárquicos de escalamiento y un esquema de cobertura horaria que garantice monitoreo continuo. También se diseñaron procesos para la vigilancia constante, la contención de amenazas, la respuesta ante incidentes y la comunicación interna entre las áreas involucradas.

También se identifican herramientas, analizando soluciones de seguridad actualmente existentes en el entorno del GAD municipal, destacándose el EDR de Kaspersky, el firewall Palo Alto, la herramienta Dynatrace, y se evalúan opciones como el SIEM KUMA, que ofrece integración directa con el entorno actual. Esto permite aprovechar mejor las inversiones existentes, fortalecer la detección y respuesta a amenazas.

La propuesta incluye la arquitectura, procesos y personal, formando una base para reforzar la ciberdefensa del GAD Municipal, buscar mejorar los tiempos de respuesta ante amenazas y garantizar la continuidad operativa, promoviendo el autoaprendizaje y mejora continua de los procedimientos tras cada evento de seguridad.

Este trabajo surge del objetivo general de desarrollar un plan integral para la creación y gestión de equipos de respuesta a incidentes (SOC) en el GAD Municipal del cantón Cuenca. La propuesta se centra en la efectividad en la prevención, detección y respuesta a incidentes de ciberseguridad. Para lograrlo se planteó el

uso de tres objetivos específicos: Analizar las mejores prácticas para la creación y gestión de equipos SOC en organizaciones mediana-grandes. Diseñar la estructura organizativa, las funciones y responsabilidades del equipo SOC, considerando el tamaño, complejidad y necesidades de la organización. Establecer los procesos, procedimientos y herramientas necesarios para la operación efectiva del equipo SOC.

Con el desarrollo de este proyecto se alcanzó el planteamiento de las bases para una propuesta de una implementación futura de un equipo SOC para el GAD Municipal del Cantón Cuenca, cual mediante el trabajo en conjunto de procesos, talento humano y tecnóloga, estructurados roles y jerarquías permitirá mantener una operatividad, monitoreo, detección y respuesta ante incidentes de seguridad de la información que puede afectar a la institución, buscando herramientas compatibles con las ya implementadas dentro del sistema municipal para un fortalecimiento en su ciberdefensa.

Palabras clave:
SOC (Centro de Operaciones de Seguridad), Ciberseguridad, SIEM, EDR, Detección de incidentes, Respuesta a incidentes, GAD Municipal.

ABSTRACT

This degree project proposes the design of a SOC (Security Operations Center) for the Municipal GAD of the canton of Cuenca, with the aim of establishing an operational structure that allows for monitoring and response to information security incidents that may affect the institution.

This work is based on an organizational and technological analysis of municipal GAD. A scalable structure is proposed, geared towards efficient incident management. This proposal defines roles for the SOC team, hierarchical escalation levels, and a schedule that guarantees continuous monitoring. Processes were also designed for constant surveillance, threat containment, incident response, and internal communication between the areas involved.

Tools are also identified, analyzing existing security solutions in the municipal GAD environment, highlighting Kaspersky's EDR, the Palo Alto firewall, and the Dynatrace tool, and evaluating options such as KUMA SIEM, which offers direct integration with the current environment. This allows for better use of existing investments and strengthens threat detection and response.

The proposal includes architecture, processes, and personnel, forming a basis for strengthening the Municipal GAD's cyber defense, seeking to improve response times to threats, and ensuring operational continuity, promoting self-learning and continuous improvement of procedures after each security event.

This work stems from the overall objective of developing a comprehensive plan for the creation and management of incident response teams (SOC) in the Municipal GAD of the canton of Cuenca. The proposal focuses on effectiveness in the prevention, detection, and response to cybersecurity incidents. To achieve this, three specific objectives were proposed: Analyze best practices for the creation and management of SOC teams in medium-to-large organizations. Design the

organizational structure, functions, and responsibilities of the SOC team, considering the size, complexity, and needs of the organization. Establish the processes, procedures, and tools necessary for the effective operation of the SOC team.

With the development of this project, the foundations were laid for a proposal for the future implementation of a SOC team for the Municipal GAD of the Canton of Cuenca, which, through the joint work of processes, human and technological talent, structured roles, and hierarchies, will allow for the maintenance of operations, monitoring, detection, and response to information security incidents that may affect the institution, seeking tools compatible with those already implemented within the municipal system to strengthen its cyber defense.

Palabras clave:
SOC (Security Operations Center), Cybersecurity, SIEM, EDR, Incident detection, Incident Response, Municipal GAD.

Objetivos

Objetivo General

- Desarrollar un plan integral para la creación y gestión de equipos de respuesta a incidentes (SOC) en el GAD Municipal del cantón Cuenca, asegurando su efectividad en la prevención, detección y respuesta a incidentes de ciberseguridad.

Objetivos Específicos

- Analizar las mejores prácticas para la creación y gestión de equipos SOC en organizaciones mediana-grandes.
- Diseñar la estructura organizativa, las funciones y responsabilidades del equipo SOC, considerando el tamaño, complejidad y necesidades de la organización.
- Establecer los procesos, procedimientos y herramientas necesarios para la operación efectiva del equipo SOC.

1. Introducción

Los sistemas de información se encuentran en constante cambio. En las últimas décadas, tanto la tecnología de la información como las amenazas contra la seguridad han evolucionado de forma paralela [1]. La seguridad de la información constituye un proceso fundamental y continuo que permite prevenir, proteger y minimizar los ataques que podrían comprometer la confidencialidad, integridad y disponibilidad de los activos de información de una organización [1]. Estos tres principios son esenciales con el fin de preservar la confianza de los usuarios en los sistemas de seguridad implementados por las empresas o instituciones.

En el año 2023, según estudios realizados por Cybersecurity Ventures, se estimaron aproximadamente 2.200 ciberataques diarios, esto equivale a que cada 39 segundos se presente un ataque [2]. Los sistemas de control industrial (ICS) de Kaspersky registraron un descenso global en el porcentaje de ataques dirigidos a tecnología operativa, pasando del 34% en el primer semestre al 31% en el segundo. Sin embargo, se reportó un aumento en los bloqueos de ataques maliciosos en regiones como Europa Occidental (21,65%) y Europa Oriental (34,5%), mientras que en Latinoamérica se evidenció una leve disminución, llegando al 39% [3].

Entre los tipos de ataque más frecuentes se destacan el malware, con más de mil millones de variantes activas en 2023, y el ransomware, que presentó un incremento del 95% durante el mismo año. Asimismo, los ataques de phishing han evolucionado significativamente gracias al uso de nuevas tecnologías como la inteligencia artificial, lo que ha permitido a los ciberdelincuentes perfeccionar técnicas como el vishing y el smishing [2].

La empresa Appgate reportó en 2023 un aumento del 77% en la cantidad de incidentes a nivel global, siendo América Latina la región más afectada. En comparación con 2022, el incremento regional fue del 60% [4]. Según los ICS de Kaspersky, Latinoamérica es una de las zonas con mayor riesgo en lo que respecta

a ataques dirigidos a redes tecnológicas, donde predominan los scripts maliciosos y las páginas de phishing. Países como Ecuador, México, Nicaragua, República Dominicana y Uruguay se encuentran dentro del top 15 de naciones con mayores porcentajes de bloqueos de documentos maliciosos durante el segundo semestre de 2023 [3].

En cuanto a Ecuador, se registraron más de 12 millones de ciberataques en 2023. El país se posicionó en el quinto lugar a nivel mundial con mayor número de intentos de phishing. Además, se observó un incremento del 50% en los ataques con troyanos bancarios [5]. En 2022, la plataforma de trámites digitales perteneciente al Municipio de Quito presentó un ciberataque tipo ransomware, el cual dejó fuera de servicio al sistema temporalmente y afectó entre el 15% y 20% de la información institucional [6].

Actualmente, uno de los componentes más críticos en la estrategia de seguridad de la información es el Centro de Operaciones de Seguridad (SOC), responsable del monitoreo, detección y respuesta ante incidentes relacionados con amenazas y vulnerabilidades que afectan a la organización. El SOC está conformado por profesionales especializados que supervisan los sistemas de red, identifican comportamientos maliciosos y reaccionan ante ataques como malware y phishing [7].

Para que el SOC funcione correctamente, es indispensable contar con procesos y procedimientos bien definidos, que permitan gestionar los incidentes de forma estructurada y medir su efectividad mediante indicadores y métricas (KPIs), con el fin de minimizar los costos asociados a posibles brechas de seguridad [7].

El SOC combina personas, procesos y tecnologías para realizar un monitoreo en tiempo real, analizar los incidentes y coordinar respuestas rápidas y efectivas. Además, mantiene una colaboración activa con otras áreas de la organización, como el departamento de TI, asegurando el cumplimiento de políticas y normas internas de seguridad [7].

Tradicionalmente, la arquitectura del SOC se basa en un modelo radial, en el cual el sistema de gestión de eventos e información de seguridad (SIEM) actúa como núcleo central. Este núcleo se conecta con otros componentes de seguridad como evaluadores de vulnerabilidades, gestores de riesgos y cumplimiento, escáneres de aplicaciones, sistemas de prevención de accesos no autorizados o intrusiones, herramientas de análisis de comportamiento de usuarios y dispositivos, soluciones EDR y plataformas de inteligencia de amenazas [8].

En este sentido, y de acuerdo con lo previamente expuesto, la presencia de un Centro de Operaciones de Seguridad dentro del GAD Municipal de Cuenca se presenta como una solución ante incidentes, amenazas y vulnerabilidades que pudieran afectar a la corporación. El monitoreo, detección y respuesta ante estos eventos permitirá mantener la continuidad operativa y asegurar una imagen institucional sólida en cuanto a su capacidad de proteger la información. Este proyecto plantea la base estructurada para el establecimiento de dicho centro, con miras a una implementación futura por parte del GAD Municipal de Cuenca.

2. Determinación del Problema

Actualmente, cada persona dentro de una organización puede representar un eslabón seguro o débil dentro del campo de la seguridad de la información. El ciberespacio, donde circula todo tipo de información, se ha convertido en uno de los principales objetivos para los ciberdelincuentes. Los ciberataques, que son cualquier forma de destruir, robar o alterar información mediante acceso no autorizado a una red de datos, son considerado uno de los mayores riesgos globales. Entre los ataques más frecuentes se encuentran el malware, denegación de servicio distribuido (DDoS), la suplantación de identidad, phishing, inyección de código SQL, el scripting entre sitios (XSS), entre otros tipos de riesgos que se presentan en la red.

La Estrategia Nacional de Ciberseguridad reconoce la necesidad de implementar y fortalecer las capacidades de ciberseguridad del país. A pesar de algunos avances, el índice nacional de ciberseguridad aún se encuentra por debajo del promedio internacional, según el estudio realizado por el BID y la OEA [9], Ecuador obtuvo calificación de 3.88 sobre 5 en su índice en ciberseguridad, siendo áreas como la respuesta ante incidentes marcada como punto crítico. Esta estrategia se construye sobre pilares como la ciberdefensa, la prevención de ciberdelitos y el fortalecimiento de la resiliencia institucional. Se enfatiza la importancia de la gobernanza y la cooperación internacional para salvaguardar los derechos digitales de los ciudadanos y mejorar la confianza en el entorno digital.

La seguridad de la información es un campo enorme y esencial, con un gran impacto en las empresas a nivel global y local. Se analiza el desarrollo histórico de la seguridad de la información, partiendo desde una perspectiva amplia hasta llegar a un enfoque especifico, destacando su importancia y alcance en el entorno digital actual.

A nivel mundial, la creciente interconexión de sistemas y el aumento en la frecuencia de ataques han obligado a las organizaciones a adoptar soluciones más robustas, como los sistemas SIEM (Security Information and Event Management) y el uso de herramientas basadas en automatización e inteligencia artificial. Los cuales están siendo implementados en entornos empresariales globales, con el propósito de perfeccionar la detección y respuesta a los ataques a la información [10]. Para asegurar el ciberespacio es necesario adoptar tecnología avanzadas y colaborativas a nivel global. Observamos que en el artículo [10] con la implementación de machine learning se obtuvo una reducción significativa de falsos positivos. Demuestra un rendimiento positivo, con tasa de detección alta y una mejora de eficiencia de los analistas del SOC.

A nivel regional, los centros de operaciones de ciberseguridad (SOC) se han convertido en estructuras fundamentales para la protección de activos digitales. Un estudio [11] presento un modelo analítico de SOC para distintos sectores, como defensa, inteligencia y espacios comerciales. Esto permitió identificar áreas críticas, ajustar procesos y alcanzar mayores niveles de eficacia operativa.

En un contexto local, se ha observado que muchas organizaciones aún carecen de procesos estructurados para detectar y responder a incidentes. En investigaciones locales [12] observamos que la implementación de SOC para monitorizar, detectar y responder a incidentes de seguridad es esencial debido a que proporciona un enfoque estructurado para la respuesta a incidentes y la mitigación de amenazas. Al momento de su implementación se observó una mejora significativa en la capacidad de respuesta a incidentes y coordinación entre los distintos departamentos. Reduciendo los tiempos de respuesta y mitigando las amenazas de seguridad.

Por esta razón, este proyecto propone el diseño de un SOC para el GAD Municipal de Cuenca, Enfocado en definir procesos, procedimientos, roles operativos, niveles de escalabilidad y la jerarquía estructural necesaria para el funcionamiento eficiente del equipo de seguridad. Este desarrollo busca establecer una base sólida

que permita gestionar eficazmente los eventos e incidentes de seguridad de la información que se presenten en la institución.

Como parte de este enfoque, también se evaluarán opciones viables para la integración de un sistema SIEM, que permita correlacionar eventos y obtener visibilidad en tiempo real. Cabe resaltar que, según los antecedentes del GAD Municipal, ya se han invertido en soluciones perimetrales y herramientas de seguridad; por tanto, el siguiente paso lógico es consolidar esas inversiones a través de un SOC que potencie la detección temprana y la respuesta efectiva ante incidentes.

3. Marco teórico referencial

Este capítulo presenta los fundamentos necesarios para comprender cómo se estructura y opera un Centro de Operaciones de Seguridad (SOC). A lo largo de esta sección se abordan conceptos clave, enfoques técnicos y normativos, así como modelos operativos y herramientas que respaldan la gestión de la seguridad de la información.

El propósito es reunir información relevante que permita aplicar buenas prácticas en la implementación de un SOC, tomando como base marcos teóricos reconocidos. Se analizan aspectos esenciales como los roles del personal, los procesos y las tecnologías requeridas para su funcionamiento. Esta base conceptual busca asegurar que la propuesta planteada se ajuste tanto a los estándares internacionales como a las necesidades específicas del GAD Municipal de Cuenca.

3.1 Investigación Documental

Esta sección se basa en una revisión documental que permitió reunir y analizar información relevante sobre cómo se estructuran, organizan y operan los SOC (Centros de Operaciones de Seguridad).

A través de este análisis fue posible identificar elementos clave como los roles que los conforman, los factores críticos para su implementación y los aspectos que garantizan su funcionamiento continuo. Esta recopilación servirá de base para adaptar el diseño de nuestra propuesta del SOC a la realidad institucional del GAD Municipal de Cuenca.

3.1.1 Definición y Propósito de un SOC

Un Centro de Operaciones de Seguridad (SOC) es un área esencial dentro de cualquier organización, es la responsable de gestionar la seguridad de la información. Su principal función es la centralización y coordinación de tareas

esenciales como la monitorización, detección y respuesta ante incidentes de seguridad [13]. De acuerdo con el Instituto SANS, un SOC funciona gracias a la coordinación de personas, procesos y tecnologías avanzadas que permiten vigilar de forma constante los sistemas y actuar ante comportamientos sospechosos. [14]. FortiGuard Labs lo describe como sectores estratégicos que solo responden ante incidentes, sino que también se adelantan a posibles ataques gracias al análisis proactivo de amenazas. Este enfoque permite a los SOCs identificar patrones de riesgo y dirigir los recursos hacia los puntos más críticos, priorizando acciones en función del nivel de amenaza. [15][16].

El SOC está conformado por expertos en ciberseguridad y seguridad de la información, quienes garantizan la supervisión, análisis y salvaguarda de los sistemas, redes y datos de la empresa contra posibles amenazas digitales [14]. Para lograr esto, cuentan con herramientas como plataformas SIEM y herramientas de análisis para supervisar en tiempo real la actividad de los sistemas y redes institucionales. [15]. Este centro de operaciones es fundamental para minimizar riesgos de seguridad, con la implementación de controles efectivos y evitando que ocurran brechas que puedan afectar a la empresa [16].

El objetivo principal de un SOC es resguardar los activos más importantes de una organización mediante la combinación de procesos, tecnología y personas, bajo una estrategia coordinada [13]. Además, el SOC es fundamental para la minimización los costos relacionados con violaciones de datos y robustece la seguridad de la organización [16]. Facilitando la toma de decisiones estratégicas al ofrecer información clara sobre el estado de la seguridad y las posibles vulnerabilidades. [15]. Esto no solo protege la integridad de la información, sino que también garantiza el cumplimiento de las regulaciones de seguridad y fortalece la capacidad de la organización para mantenerse en operatividad frente a incidentes [14].

3.1.1 Triada: Procesos, Personas, Tecnologías

En esta sección se presenta la tríada fundamental, la cual se compone por la estructura de un Centro de Operaciones de Seguridad (SOC). Misma que se

encuentra conformada por tres elementos clave: procesos, personas y tecnologías. Esta tríada representa los pilares esenciales que permiten el funcionamiento coordinado y efectivo de un SOC. El análisis de estos componentes busca ofrecer una visión panorámica inicial de cómo se organiza y opera un SOC.

3.1.1.1 Procesos

La gestión de los procesos permitirá moldear el método de administración de actividades de los SOC, permitiendo estandarizar las actividades para una mejora continua, de tal manera que facilite el entendimiento de las actividades a la dirección, para contar con el apoyo corporativo y económico [14].

Se presenta el concepto de cadena de valor, lo que permite la coexistencia de instrumentos de política, reglas de gestión, procesos, procedimientos, entre otros, lo que permite el entendimiento de las actividades que serán realizadas por cada persona, debido a que se implementa de manera ordenada y jerárquica [15].

Para tener una mejora continua de los procesos, estos deberán presentar su debida documentación. Esto permitirá observar indicadores de medición y un mejor análisis sobre la mejora de estos, lo cual permita tomar mejores decisiones sobre los cambios que se deberían implementar a los procesos [16].

Es importante tener en cuenta que los procesos tienen como objetivo dar un determinado servicio o producto a un área, por otro lado, los procedimientos son ejecutados por un solo individuo y describen como esa persona tiene que realizar esa actividad. Un proceso puede componerse de múltiples procedimientos, pero nunca al revés [14].

La Cisco systems propone procesos y procedimientos que pueden formar parte del SOC:

- Gestión de servicios corporativos

Encargada de garantizar que los servicios de seguridad estén alineados con los objetivos corporativos. Permite analizar las amenazas y los requerimientos

primordiales de la organización para priorizar los servicios. Además, se encarga de la supervisión del cumplimiento de estándares internos y externos [15].

- Gestión de incidentes de seguridad

Está enfocado en la detección, investigación, mitigación y respuesta ante incidentes. Este es el servicio más visible del SOC, debido a que es la reacción ante problemas cotidianos, para garantizar una respuesta eficiente ante diversos eventos [16].

- Gestión de vulnerabilidades

Permite la identificación y mitigación de los riesgos antes de que estos escalen a grandes amenazas para la corporación. Se incluye la búsqueda de documentación y corrección de vulnerabilidades en sistemas, redes y aplicaciones. Con la finalidad de mejorar los niveles de seguridad y minimizar la probabilidad de incidentes[15].

- Monitoreo de seguridad

Se encarga de la supervisión continua de los eventos en tiempo real, para identificar comportamientos inusuales. Estos pueden ser un indicador de actividades maliciosas, lo que permite generar notificaciones automáticas al equipo de seguridad con la ayuda de herramientas como plataformas SIEM y sistemas de análisis [14].

- Gestión de registros de auditoria

Encargada de la recolección y análisis de datos para implementar auditorías de cumplimiento y análisis forense, mediante la identificación de patrones de riesgo. Basado en herramientas de normalización y análisis de datos para la gestión del aumento y diversidad de eventos de seguridad [15], [17].

- Inteligencia de seguridad

Se encarga de combinar datos, servicios de reputación global y bases de amenazas para una predicción ante posibles riesgos y de tal manera que permita una coordinación de respuestas más efectivas [15].

- Generación de reportes de seguridad

Es el encargado de la comunicación del estado de la seguridad a todas las partes interesadas. Esto permite identificar áreas por mejorar y documentar respuestas ante eventos críticos [18].

- Interconexión de procesos

Para que un SOC sea exitoso se debe a la orquestación de estos procedimientos, alineándolos con las estrategias corporativas, de tal manera de asegurar una respuesta eficiente ante cualquier eventualidad [17], [18].

3.1.1.2 Personas

La tecnología sola no puede afrontar el desafío de la seguridad de la información, esta necesita estar acompañada de un personal capacitado dentro del SOC. Su función es la protección y defensa de la organización, los clientes y los activos críticos. Los periodos en un SOC pueden resumirse en:

1. **Fases de rutina prolongadas:** Realizar revisiones de seguridad, auditorías, de procesos, configuración de tecnologías y capacitación individual.
2. **Fases de crisis cortas pero intensas:** Dar una respuesta inmediata ante incidentes cuando las alarmas se activan, requiere soluciones conscientes, rápidas y efectivas bajo presión [15].

La capacitación individual es un aspecto fundamental en el perfil de un analista del SOC. Este conocimiento no se adquiere solo con ayuda de cursos o clases impartidas, esta se refuerza mediante la implementación de nuevos productos, detección de nuevas vulnerabilidades y el análisis de ataques emergentes [13].

En tiempos de crisis, la comunicación efectiva con otras áreas es clave para la solución a incidentes de manera eficiente. Por ello, se debe trabajar en conjunto con las personas, los procedimientos y las tecnologías para alinear la misión del SOC con los servicios que demanda la organización [15].

Roles dentro del SOC

Los roles determinan las aptitudes requeridas para cumplir con los servicios del SOC. Estos pueden encontrarse dentro del propio SOC o ser suministrados por otras áreas.

- Roles de liderazgo

Incluye al director y distintos niveles jerárquicos encargados de asignar órdenes al equipo de trabajo, canalizando los esfuerzos para alcanzar los objetivos planeados [13].

- Roles analíticos

Son el núcleo del SOC, abarcando la gestión de incidentes, vulnerabilidades, monitoreo, investigación forense e inteligencia de amenazas. Cada especialización aporta conocimientos específicos, fortaleciendo el SOC [13].

- Ingeniería de operaciones

Se encarga de la implementación y mantenimiento de soluciones de seguridad dentro del entorno TI. Requiere conocimientos especializados en integración y configuración de herramientas de seguridad, generalmente suministrados por proveedores tecnológicos [18].

El SOC debe agruparse en cuatro ramas principales:

1. Operaciones: Identifica los servicios prestados y es el encargado de la gestión de incidentes y vulnerabilidades. Involucra monitoreo, investigaciones y respuesta a incidentes.

2. Ingeniería de operaciones: Administra y configura equipos de seguridad dentro de la organización.
3. Inteligencia de seguridad: Monitorea amenazas externas e intercambiar información con organismos externos.
4. Gestión de soporte: En empresas grandes, esta área puede incluir servicio técnico, gestores de proyectos y auditores.

3.1.1.3 Herramientas

Las herramientas que se implementan en un SOC (centro de Operaciones de seguridad) garantizan la vigilancia y detección de amenazas. Debido a los avances tecnológicos, es necesario mantener actualizadas las herramientas y manejarlas correctamente para asegurar su efectividad [15].

Infraestructura de Redes

La red sobre la que opera el SOC define el alcance del monitoreo y las capacidades de respuesta ante los incidentes. Se consideran tres entornos básicos.

- Red interna: Resguarda sistemas críticos como bases de datos, aplicaciones y servidores.
- Red externa: Conexión a internet y tráfico de fuentes desconocidas, donde ocurren intentos de intrusión.
- DMZ (Zona desmilitarizada): Segmento donde se alojan servidores públicos, con reglas estrictas de cortafuegos [18].

En la investigación [15] se recomienda la segmentación de redes o seguridad granular, que consiste en subdividir múltiples redes para que cada una tenga un propósito específico. Esto permite contener posibles intrusiones, evitando que se extiendan a otras partes de la red.

El uso de conexiones VPN y accesos remotos seguros es otro componente importante. Estas deben contar con cifrado robusto y mecanismos de autenticación

confiables para garantizar que los accesos remotos comprometan la red de la organización [15].

Sistemas de Gestión y Monitoreo

- SIEM (Security Information and Event Management): Recopilan registros, generan alertas y ayudan a reaccionar de forma oportuna ante incidentes [18].
- EDR (Endpoint Detection and Response): Permiten vigilar los equipos finales en tiempo real, detectando comportamientos sospechosos o software malicioso [15].

Seguridad de Red

- Cortafuegos y listas de control de acceso (ACL), que filtran el tráfico no autorizado [18].
- IDS (Sistemas de Detección de Intrusiones): Identifican patrones anómalos en el tráfico de red [15].
- IPS (Sistemas de Prevención de Intrusiones): Actúan de forma automática, bloqueando las amenazas que hayan sido detectadas por el IDS o por mecanismos propios [18].

Protección de Datos y Sistemas

- DLP (Data Loss Prevention): Detecta y bloquea intentos de fuga de información [18].
- Escáneres de vulnerabilidades: Identifican y priorizan fallos en software y redes [15].

Automatización y análisis avanzado

- SOAR (Security Orchestration, Automation, and Response): Automatiza flujos de trabajo y respuestas ante incidentes [18].
- Análisis de Big Data: Identifica patrones de ataques basados en datos históricos [15].

3.1.1.4 Gestión de servicios corporativos

Estos procesos se asignan a servicios de tecnologías de la información (TI), que pueden estar basados en algún tipo de práctica para realizar esta acción, de tal manera de integrar seguridad en las operaciones corporativas, garantizando el funcionamiento de todos los sistemas con altos estándares de protección.

- Gestión de eventos: administración y monitoreo de auditorías de los dispositivos de red y sistemas informáticos, de tal amanera de proporcionar una mayor seguridad [15], [17].
- Gestión de incidentes: implantado y ejecutado por soporte técnico, administración de servidores y otras áreas operativas que manejen infraestructura tecnológica [17].
- Gestión de problemas: identificar los inconvenientes desde la raíz que generan los incidentes[17].
- Gestión de vulnerabilidades: puede ser implementado por el área operativa de TI, instalación de parches, resolución de defectos reportados, análisis de seguridad de los equipos que se encuentran administrando [15].
- Algunos SOCs tienen a su cargo el manejo de plataformas tecnológicas, donde se implementan los procesos de gestión del cambio, gestión de configuraciones, gestión de versiones [17].

3.1.1.5 Gestión de servicios de seguridad

Abarca actividades generalmente asociadas a la detección, investigación, contención y respuesta ante incidentes que se encuentren relacionados, siendo este el servicio más visible del SOC debido a la reacción que el mismo tendrá ante los incidentes presentados cotidianamente, garantizando una respuesta eficiente [17].

- Definición y estandarización para el desarrollo de procesos o procedimientos: establece quienes son los involucrados y como se desarrollarán y aprobarán nuevos documentos [19].
- Procesos de medición y soporte: recolección de métrica de los procesos y solución de los reportes periódicamente[8].
- Procesos de mejora continua: tiene la finalidad de implementar mejoras a partir del análisis de los indicadores de rendimiento [8], [19].
- Proceso de entrega de servicios de seguridad: como los usuarios acceden a los servicios [15], [17].
    - Gestión de tiques.
    - Proceso de auditoría y soporte de cumplimiento.
- Procesos como capacitaciones de la persona, continuidad de operación y procesos de recuperación a desastres conforman el mismo agrupamiento de procesos[8].

Los procesos de gestión de proveedores y de reporte financiero y operacional se encargan de informar a los directorios e interesados sobre los aspectos de estos.[8].

3.1.1.6 Ingeniería de servicios de seguridad

Procesos asociados al mantenimiento de plataformas tecnológicas, cuestiones como cambios en versiones de actualizaciones pueden tomar relevancia, pero el riesgo que implican operacionalmente y el impacto que pueden generar [13].

- Procesos de administración de ciclo de vida: analizar, planificar, despliegue, prueba y remoción de productos electrónicos.
- Proceso de gestión de versiones, migraciones y configuraciones: establecer pasos y correctas prácticas para migraciones o actualizaciones en sistemas y dispositivos.

3.1.1.7 Operación de los servicios de seguridad

Esto contiene el proceso y procedimientos para el mantenimiento de los sistemas de información utilizada por el SOC [13].

- Proceso de monitoreo de sistemas: identificar problemas que impidan alcanzar el nivel del servicio que deseamos entregar.
- Proceso de licenciamiento: identificar licencias próximas a caducar.
- Proceso de mantenimiento de la plataforma: dar soporte a la plataforma tecnológica y a aplicaciones que se utilice dentro del SOC.
- Proceso de gestión de contenido: creación de reglas, casos de usos, alertas, filtros y monitores presentes del software que se encontrara funcionando como SIEM.

Según el informe de FortiGuard Labs, los procesos dentro de un SOC deben evolucionar para abordar tácticas avanzadas como el uso de herramientas NDR y la creación de mapas de calor TTP basados en MITRE ATT&CK. Estos procesos ayudan a priorizar amenazas, reducir tiempos de respuesta y mejorar la precisión en la detección[15].

3.1.2 Estandarización

La implementación de un Centro de Operaciones de Seguridad (SOC), requiere alinearse con normativas y marcos reconocidos internacionalmente, que sirvan de guía para asegurar la protección de la información y una gestión eficaz de los incidentes. Algunos de los marcos más relevantes son [13]:

ISO/IEC 27000 Gestión de la Seguridad de la Información.

La ISO/IEC 27000 establece las bases para desarrollar y sostener un Sistema de Gestión de Seguridad de la Información (SGSI), fundamental para un SOC. Bajo una serie de procesos, como [13]:

- La formulación de políticas y procedimientos que guíen la gestión de la seguridad.
- La clasificación y gestión de los activos de información.
- La identificación y tratamiento de los riesgos de la seguridad.
- La implementación de planes de protección de la empresa contra posibles amenazas.

De esta manera se asegura que las operaciones del SOC se alineen con los criterios de confidencialidad, integridad y disponibilidad, garantizando una protección correcta frente a posibles amenazas.

NIST Enfoque para la Mejora Continua de la Ciberseguridad

El NIST proporciona un modelo para gestionar la ciberseguridad en una organización, basándose en los cinco pilares fundamentales: identificar, proteger, detectar, responder y recuperar. Para un SOC, esto implica [13]:

- Monitorear de forma constante los sistemas para identificar posibles amenazas.
- Responder rápidamente ante incidentes para minimizar su impacto.
- Implementar procesos de recuperación para restaurar rápidamente los servicios afectados.

Este ciclo de mejora continua permite que el SOC se adapte de forma dinámica a las amenazas emergentes y evolucione con los cambios tecnológicos.

ITIL (Information Technology Infrastructure Library)

ITIL es un marco ampliamente adoptado para la gestión de servicios de TI, que también es aplicable a la seguridad. Su implementación en un SOC ayuda en [13]:

- Integrar los procesos de seguridad en los servicios de TI.
- Definir procedimientos claros para escalar y resolver incidentes críticos de seguridad.
- Mejorar la eficiencia operativa mediante un enfoque basado en la calidad y la mejora constante.

COBIT5 para la Seguridad de la Información

El estándar COBIT5 establece una conexión directa entre los objetivos de seguridad y las metas. Su aplicación dentro de un SOC implica [13]:

- Alinear las estrategias de seguridad con los objetivos estratégicos de la organización.
- Evaluar de manera continua los riesgos y asegurar el cumplimiento de las normativas.
- Medir el desempeño del SOC con indicadores clave de rendimiento (KPI) que permitan optimizar los recursos y la efectividad del centro.

3.1.3 Tecnologías emergentes

Sistemas AIS

Los sistemas Inmunes Artificiales son herramientas computacionales diseñadas a partir del sistema inmunológico humano. Estas técnicas copian los mecanismos como la identificación y neutralización de enfermedades, aplicándolos al ámbito de ciberseguridad. Su funcionamiento se basa en aprender y adaptarse de manera continua, esto permite identificar patrones inusuales y responder a amenazas emergentes. Esta tecnología está basada en la capacidad biológica de distinguir entre lo propio y lo externo, aplicando este principio para detectar anomalías en los sistemas digitales. Integran enfoques avanzados, como la detección de señales de peligro, para reforzar su capacidad de reaccionar ante situaciones que podrían representar riesgos potenciales (Falowo et al., 2024).

Inteligencia general artificial

El AGI se define como un sistema avanzado capaz de aprender, comprender y aplicar conocimientos de manera autónoma en diversas áreas sin requerir una supervisión constante. En la ciberseguridad, la AGI ofrece una manera de potenciar significativamente las capacidades de los sistemas inmunes artificiales (AIS), permitiendo detectar patrones complejos con mayor precisión y reducir errores

como falsos positivos o negativos. Su capacidad para analizar datos, comprender texto, y adaptarse rápida y continuamente a nuevas amenazas resulta útil para optimizar el funcionamiento de los SOCs. A pesar de la etapa inicial de AGI de su desarrollo, su utilidad en la funcionalidad de los AIS es una apuesta prometedora en las estrategias de defensa digital [16].

Ndr (network detection and response)

La tecnología NDR permite observar y reaccionar ante actividades sospechosas en redes internas mediante el uso de análisis sofisticados. Esta solución identifica flujos de tráfico inusuales asociados a posibles ciberamenazas y ofrece métodos automáticos para responder y manejar riesgos de manera inmediata[15], [16] .

Sandboxing

La técnica de sandboxing implica la evaluación de programas o archivos en un espacio virtual seguro, diseñado para observar su funcionalidad. Este método ayuda a descubrir actividades maliciosas en aplicaciones nuevas o sospechosas sin riesgo para los sistemas reales [17].

Mapas de calor ttp basados en mitre att&ck

Los mapas de calor basados en MITRE ATT&CK destacan tácticas y métodos frecuentes de adversarios. Al visualizar estas técnicas, las organizaciones pueden priorizar sus defensas y ajustar estrategias de respuesta ante las amenazas más recurrentes [15].

Análisis de indicadores de compromiso (iocs)

El uso de indicadores de compromiso ayuda a detectar brechas de seguridad mediante la identificación de elementos como URLs o archivos maliciosos. Este análisis facilita la contención rápida de amenazas en etapas iniciales.

ElasticStack (elk)

Una de las tecnologías más utilizadas en SIEM modernos, permite la recolección, transformación y visualización de registros de eventos. La implementación de ELK en laboratorios virtuales, como se describe en [20], permite simular y analizar ataques reales, mejorando la capacidad de detección de los SIEM.

Sysmon y winlogbear

Herramientas destacadas para capturar eventos del sistema y enviarlos al SIEM para análisis avanzado.

3.2 Análisis comparativo

En esta sección se comparan los diferentes enfoques de diseño, implementación y operaciones de SOCs, analizando dos modelos referenciales.

3.2.1 SOC Corporativo en firma de consultoría.

Este modelo, basado en el diseño desarrollado por [14], propone el SOC con características bien definidas, perfiles técnicos especializados y una clara estructura jerárquica. Se basa en estándares internacionales como ISO 27001 y se centra en grandes empresas.

- **Ventajas:** Madurez estructural, claridad en roles, formalización de procesos y escalamiento.
- **Desventajas:** Altos costos de implementación y mantenimiento; dependencia de personal altamente calificado.

3.2.2 SOC basado en herramientas de código abierto

La propuesta de [8] muestra la viabilidad de la introducción funcional de SOC, utilizando tecnologías de bajo costo, como las herramientas flexibles de pila, docker, suricata y alarma gratuita.

- **Ventajas:** Reducción de costos, independencia de licencias comerciales, escalabilidad técnica.
- **Desventajas:** Requiere personal capacitado en software libre y una infraestructura base sólida.

3.3 Entrevista con expertos

Como parte del enfoque cualitativo, se realizó una entrevista al encargado de la infraestructura del GAD Municipal de Cuenca con el objetivo de entender las capacidades actuales y limitaciones para la implementación de un SOC.

3.4 Análisis de respuestas

Riesgos e Incidentes Identificados

- El problema más recurrente que se identifica es el phishing debido a la falta de capacitación del personal.
- Se identifica la necesidad de proteger el entorno físico debido a incidentes de seguridad física.

Recursos humanos y capacitación

- Se registra la necesidad de personal exclusivo en ciberseguridad, actualmente se depende del soporte de un software.
- No se dispone de un plan de capacitación ni de contratación específica para roles del SOC.

Herramientas y presupuesto

- Se dispone de presupuesto mixto, con posibilidad de combinar herramientas comerciales y open source.

Gobernanza y escalamiento

- Las decisiones críticas de seguridad no cuentan con participación técnica directa, todo recae en el director municipal y responsables por dependencia.

4. Estructura organizativa del equipo SOC

En el presente capítulo se abarca un estudio sobre el contexto institucional que formará parte del proyecto del SOC. A la par de esto, se indagará sobre la infraestructura tecnológica de la institución, junto a los sistemas de seguridad implementados, con el fin de tener un mejor encaminamiento hacia los requerimientos reales del GAD Municipal de Cuenca.

Al evaluar el tamaño y la complejidad del grupo de empresas que forman parte de este proyecto, se pudo observar que actualmente cuentan con firewalls, tecnología Check Point y un sistema EDR como parte de sus métodos de seguridad. Considerando esta base ya implementada, el enfoque del proyecto se orientó hacia el monitoreo de los eventos de seguridad que se presenten, integrando la operación de estos elementos dentro del SOC.

Teniendo todo esto en cuenta, se definirán los roles y la jerarquía del equipo SOC, junto al proceso de escalamiento a aplicar en caso de que se presente un incidente de seguridad. Adicionalmente, se presentarán las opciones de herramientas a implementar dentro del centro, así como un horario operativo establecido para el funcionamiento del equipo y sus componentes tecnológicos.

4.1 Análisis Organizativo

Para la planificación de este proyecto, es necesario realizar un análisis previo del estado actual y el tamaño de la organización, ya que esto permitirá moldear el proyecto de forma adecuada a los requerimientos reales del GAD Municipal de Cuenca.

Una vez estudiado el contexto corporativo, resulta indispensable comprender con claridad el despliegue de la infraestructura de red institucional, así como los

sistemas de seguridad actualmente implementados. Este entendimiento permitirá definir una base sólida sobre la cual desarrollar la estructura del SOC.

4.1.1 Evaluación del tamaño y complejidad de la empresa

El GAD Municipal del Cantón Cuenca, junto a las empresas ETAPA EP, EMOV, EMAC EP, FARMASO, Bomberos Cuenca, Registro de la Propiedad, Consejo de Seguridad Ciudadana Cuenca, Hospital Municipal de Cuenca, EMURPLAG EP, EMUCE EP, EMUVI EP, GUARDIA CIUDADANA DE CUENCA, Fundación Turismo Cuenca, CORPAC, EDEC EP, Fundación Bienal de Cuenca. Mediante el presente proyecto de titulación buscan centralizar y monitorear la seguridad de la información dentro de este ámbito municipal.

En base a lo antes mencionado se define un alcance con la centralización de una futura instalación de centro de monitoreo centralizado, adicionando una mayor atención en la detección y mitigación de ataque de phishing, siendo estos los dos puntos más vulnerables de las empresas. Esto es debido a que este grupo de empresas municipales adquirieron nuevos equipos de seguridad, afrontando limitaciones como la ausencia de herramientas de monitoreo y seguridad como las antes mencionada. Esto impide tener una visión en tiempo real del estado de la seguridad de los sistemas, lo que reduce la capacidad de respuesta ante incidentes.

Este proyecto incluirá 17 de las 24 empresas municipales, siendo enfocada a las que manejan una mayor concentración de volumen de tráfico de datos y servicios, representando esto una mayor necesidad para el control y monitorio continuo de los sistemas, sus datos y servicios.

Las complejidades presentadas por el momento son las diversidades tecnológicas en sus estructuras de red, aunque esta se encuentre segmentada estas tecnologías pueden diferenciarse en versiones, marcas, configuraciones, puertas traseras e incluso vulnerabilidades. Se tiene en cuenta que al ser empresas municipales estas se encuentran trabajando bajo la red que provee ETAPA EP, es decir que no cuentan

con un segundo ISP de respaldo en caso de fallas de servicio, adicionando la falta de un servidor de backup.

Esto no solo se deberá enfocar en monitoreo y en la detección de amenazas, se debe implementar una concientización al personal sobre los riesgos que pueden tener la información del usuario corporativo y de los clientes en caso de algún ataque, en estos casos siendo los más mencionados los intentos de phishing hacia las entidades municipales.

4.1.2 Estructura de la red del GAD Municipal

La infraestructura de red del GAD Municipal de Cuenca está diseñada para garantizar una conectividad eficiente y segura entre sus distintas dependencias y servicios. Su estructura se basa en un data center principal, que centraliza los servidores críticos y los sistemas de gestión institucional. De esta manera, la red se distribuye a través de una serie de switches y firewalls, cuales regulan el tráfico de datos y salvaguardan la seguridad perimetral. Esta distribución permite mantener la conectividad de diversas empresas municipales y dependencias, tanto de manera interna como externa, segmentándola en una red pública, siendo destinada para servicios abiertos a la ciudadanía. Aplicando una red privada la cual es dedicada a la gestión interna y los sistemas administrativos. En la Ilustración 1, se puede apreciar un croquis del sistema de red que se encuentra presente en el GAD Municipal.

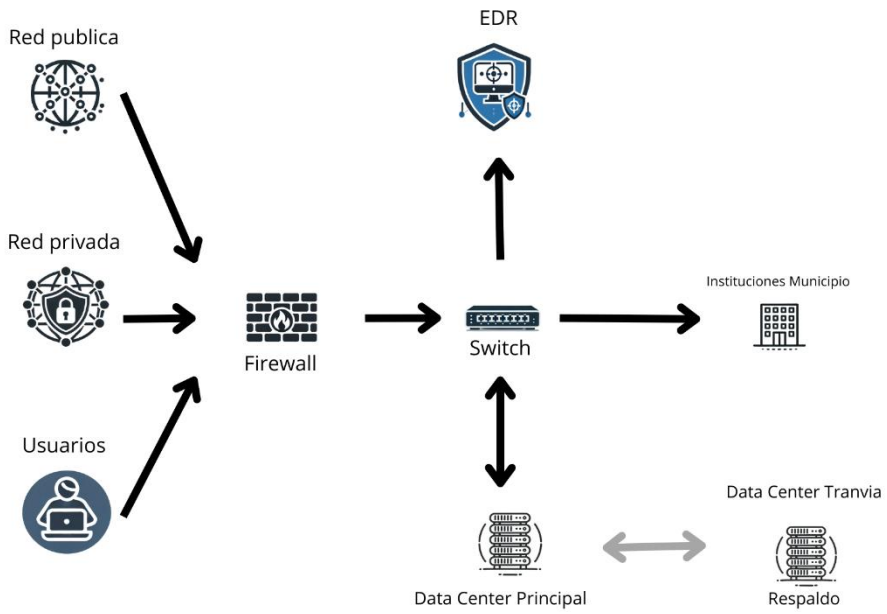


Ilustración 1 Replica simulada de la estructura de red

Para realizar una estrategia de modernización y expansión de la infraestructura de la red corporativa, se plantea el uso de un nuevo data center que servirá como backup, mismo que se encontraría ubicado en la estación central del tranvía. Esto permitirá una mejora en la disponibilidad y redundancia de los servicios digitales, atomizando la toma de decisiones, gestión de información y fortalecimiento de la ciberseguridad a la municipalidad.

4.2 Estructura organizativa propuesta

Al haberse evaluado el tamaño y la complejidad del proyecto, se definirán los roles que formarán al equipo SOC, de tal manera que se establecerán las responsabilidades de cada integrante. Con esto se asegurará que cada miembro se encuentra con su debido proceso definido, permitiendo actuar con mayor agilidad y caridad frente a los diferentes eventos de seguridad que puedan presentarse. La estructura presentada buscará optimizar la coordinación y eficiencia operativa dentro del centro de seguridad, facilitando la detección, el análisis, escalamientos y la resolución de incidentes de una manera más ordenada y oportuna.

4.2.1 Roles Principales

A continuación, se definirán los roles presentes dentro del equipo SOC, detallando la función específica que cumple cada uno dentro de la operación del centro. Esta identificación permite establecer una estructura clara de responsabilidades, facilitando la asignación de tareas, la comunicación interna y la eficacia en la respuesta ante incidentes de seguridad.

4.2.1.1 Coordinador del SOC

Esta persona será quien liderará y gestione el equipo, garantizando que el centro de operaciones se mantenga operando de manera eficiente. El encargado será el responsable de definir una estrategia de seguridad que se encuentre alineada con los objetivos del GAD Municipal de Cuenca. En este rol se gestionarán los presupuestos y la adquisición de nuevas herramientas para el uso dentro del SOC. Por último, realizará supervisiones de la gestión de los incidentes y el cumplimiento de las normativas de seguridad establecidas, garantizando la ejecución de procesos de cumplimiento y auditorias.

4.2.1.2 Analista nivel 1 (Monitoreo y Detección)

Este rol se encargará del proceso de monitoreo de seguridad, donde se supervisará en tiempo real las alertas generadas por el SIEM y otras herramientas de monitoreo. En el momento de que una alerta sea detectada, el encargado deberá identificar y calificar la amenaza según su criticidad. Antes de que produzca un escalamiento de incidente se deberá realizar un análisis previo, de tal manera de descartar un falso positivo. Esto asegurara que se cumpla con un proceso de calificación y escalamiento según criterios preestablecidos para la determinación de la severidad del evento.

4.2.1.3 Analista nivel 2 (Investigación y Respuesta)

Este rol será el responsable del proceso de investigación de incidentes de seguridad, se encargará del análisis de los registros de actividad (logs), tráfico de red y comportamiento anómalo de los usuarios. Se aplicarán aún procesos de análisis forense mediante el uso de herramientas de almacenamiento, revisión de disco y un análisis del tráfico de la red para definir el origen y alcance de la vulnerabilidad.

El analista nivel 2 se encontrará encargado de la contención y la mitigación de amenazas, ejecutando procesos de respuesta ante incidentes mediante la aplicación de medidas correctivas y recomendaciones post-incidentes, adicionalmente, desarrollará reglas y alertas que facilitarán la detección de futuras amenazas.

4.2.1.4 Analista nivel 3 (Threat Hunter)

El Threat Hunter se encargará de la identificación de amenazas persistentes avanzadas APT y ataques dirigidos directamente a la estructura municipal. Debido a la constante evolución de las amenazas, este rol tendrá la responsabilidad del proceso de inteligencia de seguridad, mediante el uso de fuentes internas y externas para la investigación de tácticas, técnicas y procedimientos de ataque.

Adicionalmente se aplicarán procesos de simulación de ataques, permitiendo evaluar la seguridad actual con la ayuda de entornos controlados. Esto permitirá la capacitación de los miembros del equipo SOC para el cumplimiento de los procesos de reglas avanzadas y la mejora de detecciones basadas en el comportamiento de amenazas.

4.2.1.5 Ingeniero de Seguridad

Este rol se encargará de la gestión de la infraestructura del SOC, incluyendo tareas como la configuración y mantenimiento del hardware y software de seguridad. También será quien lleva a cabo la implementación de actualizaciones y parches de

seguridad, garantizando la protección de los sistemas contra vulnerabilidades conocidas.

El encargado de este rol liderará las pruebas de seguridad y pentesting, asegurando que se cumplan los estándares de protección esperados por los parches y actualizaciones realizadas. Por último, optimizará las herramientas de detección, garantizando el correcto funcionamiento entre la correlación de eventos.

4.2.1.6 Responsable de respuesta a incidentes CSIRT

El responsable de Respuesta a Incidentes es el encargado en gestionar los ataques cibernéticos críticos, realizará la tarea de coordinar con los demás equipos para mitigar los efectos del ataque. Será el encargado del desarrollo de los planes de contingencia y continuidad operativa de los servicios del GAD Municipal, mediante la implementando procesos de contención y mitigación para la minimización del impacto antes de la erradicación de la amenaza. También será el encargado del proceso de erradicación y recuperación, garantizando que los sistemas afectados sean restaurados correctamente y eliminando cualquier rastro de la amenaza.

Al finalizar la recuperación de la información y el servicio de los equipos se implementará un proceso de post-mortem y aprendizaje, donde se evaluará lo ocurrido para plantear mejoras en los planes de seguridad y tomas de decisiones, con la finalidad de reducir tiempos y vulnerabilidades futuras. Este rol tendrá la potestad de informar los incidentes a la Dirección de TICs y la Alcaldía en caso de una crisis de seguridad critica para la empresa.

4.2.1.7 Encargado de cumplimiento y auditoria

En este rol el responsable estará a cargo de las auditorias de los procesos de seguridad, con la finalidad de evaluar el cumplimiento de las normativas y regulaciones bajo directrices internacionales. Mediante auditorias periódicas se verificará la eficiencia y seguridad de los procesos del SOC, permitirá la gestión de

la documentación de informes, políticas y procedimientos de seguridad, con la finalidad de cumplir los estándares establecidos.

Esta persona mantendrá actualizado los marcos regulatorios, mediante la alineación de políticas y procedimientos con estándares internacionales. Adicionalmente se validará el desempeño de los controles de seguridad en función de los eventos detectados.

4.2.2 Flujo de Trabajo y Escalamiento

En esta sección se especificará el proceso que tendrá la gestión de los incidentes de seguridad dentro del SOC, desde su momento de detección inicial hasta su resolución final, con la finalidad de asegurar un flujo de trabajo claro y bien definido para cada uno de los roles involucrados. Adicionalmente se determinarán los casos para realizar un escalamiento a niveles superiores, según su criticidad y capacidad de resolución del equipo de nivel inicial. De esta manera se busca establecer una respuesta organizada y efectiva ante la presencia de cualquier evento de seguridad que puede comprometer la operatividad del GAD Municipal de Cuenca.

4.2.2.1 Primer Nivel: Detección y Monitoreo

Responsable: Analista Nivel 1.

Las funciones básicas de este nivel incluirán el monitoreo de eventos ante cualquier alerta emitida por el SIEM o el EDR. El analista realizará una clasificación inicial de los incidentes, con la finalidad de descartar falsos positivos, eventos severos o de alto impacto. Adicionalmente aplicará respuestas básicas como el bloqueo de IPs maliciosas, negación de acceso sospechosos y contención de malware. En caso de que el incidente requiera un mayor análisis o acciones de mitigación se escalará a segundo nivel.

4.2.2.2 Segundo Nivel: Investigación y Respuesta

Responsable: Analista Nivel 2.

Este nivel se encargará de realizar un análisis más detallado de los ataques escalados, mediante la revisión de logs, correlación de eventos y datos de almacenamiento. Se mantendrá el contacto con diferentes áreas para la mitigación del ataque. En caso de que el evento sea crítico o de alto impacto, se escalará al tercer nivel.

4.2.2.3 Respuesta Avanzada y Contención

Responsable: Analista Nivel 3 (Threat Hunter).

Este nivel será responsable de la identificación de ataques avanzados y amenazas persistentes. En caso de ataques de mayor impacto, como filtraciones de datos o ataques internos, el personal encargado gestionará la contención de la amenaza. Mantendrá coordinación con el responsable de Respuesta a Incidentes (CSIRT) para una mejor toma de decisiones estratégicas.

Si es necesario, el caso se escalará al coordinador del SOC para la intervención de la Alta Dirección.

4.2.2.4 Gestión Estratégica y Decisiones Críticas

Responsable: Responsable de Respuesta a Incidentes (CSIRT).

Este rol evaluará la necesidad de notificar a organismos externos o a la Alta Dirección, dependiendo del impacto del ataque en la organización.

Si la amenaza afecta los servicios críticos del GAD Municipal, podrá declarar un estado de crisis y aplicar protocolos de recuperación para restaurar la operatividad del sistema.

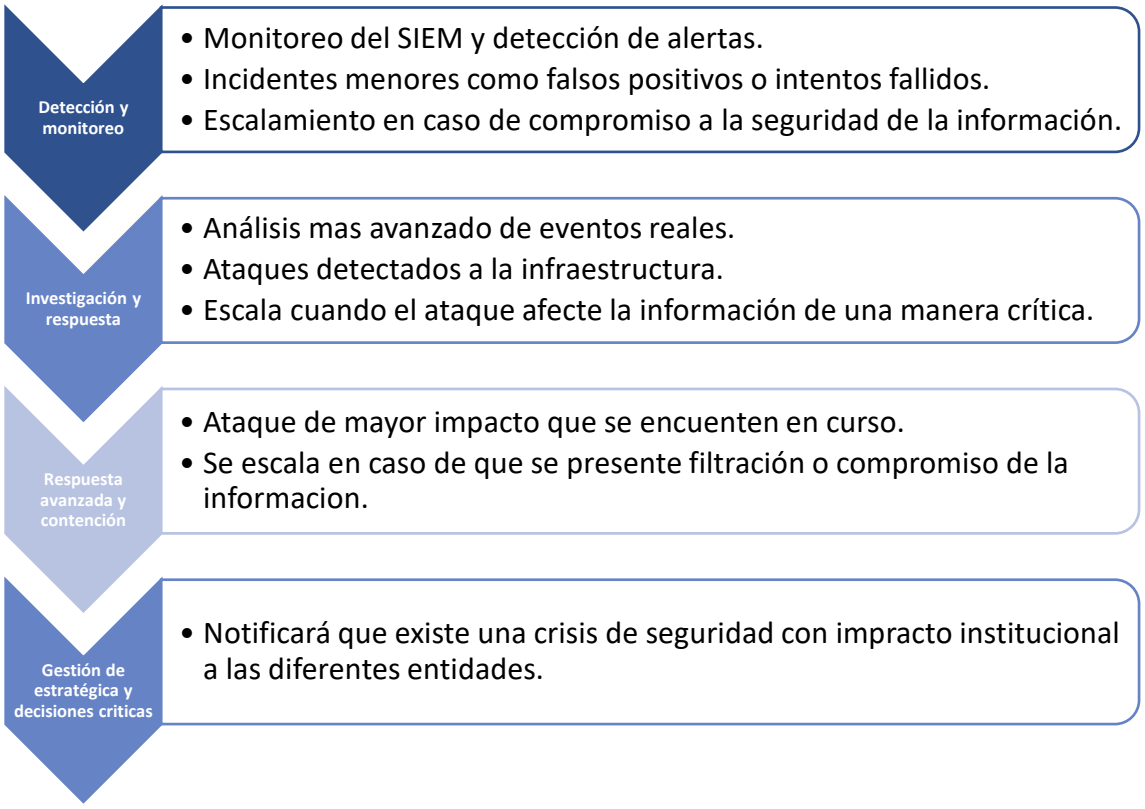


Ilustración 2 Resumen de la Jerarquía en Caso de Incidentes

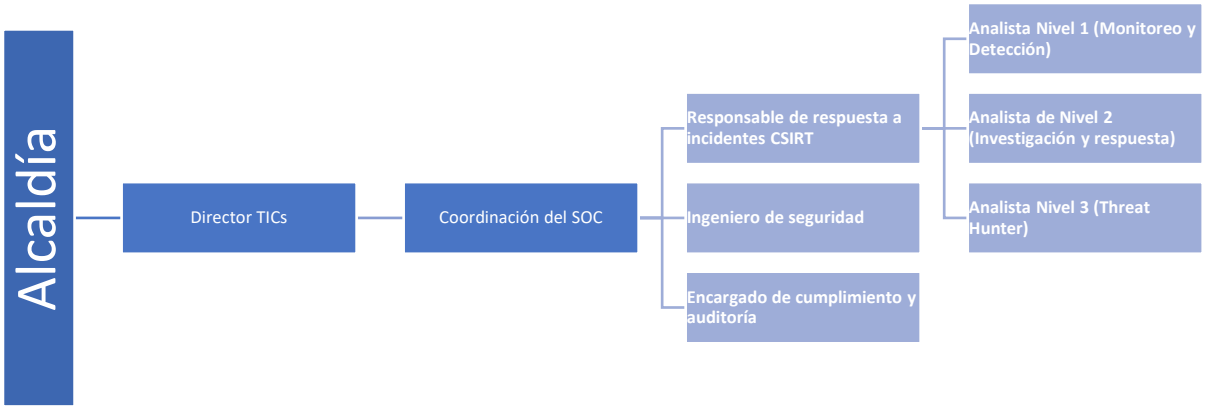


Ilustración 3 Resumen Jerárquico de la Estructura del SOC

En la Ilustración 2 se presenta la jerarquización de los incidentes de seguridad en función de su complejidad y criticidad sobre el sistema. Asimismo, en la Ilustración

3 se detalla la estructura jerárquica mediante la cual se comunicará cada evento, junto con los roles específicos que intervendrán dentro del SOC durante su gestión.

4.3 Cobertura Horaria

Para garantizar respuestas efectivas ante incidentes de seguridad, en el SOC del GAD Municipal de Cuenca se planteará un esquema de cobertura horaria optimizada, en el cual se combinará el uso de herramientas de monitoreo y seguridad las 24 horas del día, los 7 días de la semana, con la presencia de personal en turnos de 8 horas diarias, junto a un modelo de rotación fuera del horario laboral.

4.3.1 Monitoreo 24/7 Mediante el Uso de Herramientas

Sistemas como SIEM, EDR, IDS y Firewalls operarán de manera continua, sin interrupciones. Estas herramientas permitirán el análisis y detección de eventos en tiempo real, generando alertas en eventos fuera de lo normal. Además, se establecerá un sistema de notificaciones que informe de inmediato a los técnicos encargados en caso de que ocurra un evento relevante.

4.3.2 Turnos de Ocho Horas Diarias

El personal asignado al SOC trabajará en jornadas de ocho horas diarias, conforme a las políticas internas del GAD Municipal. Durante estos turnos, cada miembro del equipo deberá cumplir con sus procesos, roles y tareas asignadas, validando alertas, respondiendo a incidentes, registrando hallazgos y manteniendo actualizado el monitoreo del entorno.

4.3.3 Atención Rotatoria Fuera del Horario Laboral

Fuera del horario laboral, se designará un técnico de manera rotativa para la atención de las notificaciones de incidentes recibidas. En caso de que se genere un incidente, el técnico deberá atenderlo de inmediato se establecerá una rotación entre los miembros del equipo para que, de forma alternada, exista siempre un

técnico disponible ante cualquier incidente que requiera atención urgente y, si es necesario, escalarlo según el protocolo establecido.

4.4 Herramientas y tecnologías

Para implementar el Centro de Operaciones de Seguridad (SOC) en el GAD Municipal de Cuenca, se han evaluado múltiples herramientas que permiten la administración de eventos, la identificación y el manejo de incidentes, también la seguridad de los correos electrónicos. La selección de estas herramientas ha sido analizada según su habilidad para integrarse, su capacidad de crecimiento y su precio, con la finalidad de asegurar una defensa sólida contra las amenazas digitales.

4.4.1 Sistemas de gestión de información y eventos de seguridad (SIEM)

En el caso de los SIEM, se han considerado diferentes opciones que facilitan la identificación y la relación de eventos en tiempo real. Entre las más destacadas mencionamos:

- IBM QRadar que se destaca por incorporar inteligencia artificial y por su habilidad para automatizar la correlación de eventos, con precios anuales entre $10,000 y $30,000, que fluctúan dependiendo de la cantidad de datos que se deban procesar.
- Splunk Enterprise Security, que ofrece análisis en tiempo real y automatización avanzada de alertas, con una tarifa que parte de los $150 por gigabyte procesado al día, lo cual puede elevar el costo anual significativamente en entornos con alto volumen de datos.
- LogRhythm SIEM es otra opción efectiva en cuanto a automatización y análisis forense, con un costo aproximado de $20,000 por año.
- Graylog Enterprise representa una alternativa económica. Ofrece una versión gratuita de código abierto y una versión de pago con precios que van de $1,500 a $5,000 anuales.

Como alternativa alineada al entorno actual, se propone el uso de KUMA (Kaspersky Unified Monitoring and Analysis Platform), cuyo rango de precios es más accesible (entre $3.000 y $7.000 anuales) y que presenta una integración nativa con el EDR de Kaspersky, ya existente en la institución. Además, soporta múltiples formatos de logs como Syslog, CEF y JSON, lo que facilita la correlación de eventos de distintas fuentes.

En la Tabla 1 se puede visualizar una comparación entre los diferentes SIEMs propuestos según el contexto empresarial y sus sistemas de seguridad actualmente implementados.

Criterio	Kaspersky KUMA	Graylog Enterprise	IBM QRadar	Splunk Enterprise	LogRhythm	ArcSight (Micro Focus)
Costo estimado anual (USD)	3.000 – 7.000	1.500 – 5.000 (o gratis OSS)	25.000 – 40.000	25.000 – 50.000	20.000 – 40.000	25.000 – 50.000
Compatibilidad con Kaspersky EDR	Muy alta	Media	Alta	Alta	Alta	Alta
Compatibilidad con Dynatrace	Limitada	Media	Alta	Alta	Alta	Media
Compatibilidad con Palo Alto	Media	Alta	Alta	Alta	Alta	Alta
Notificación de eventos	Correo, consola	Correo, Webhook, API	Correo, SNMP, integraciones	Correo, Webhook, Apps	Correo, Syslog, SNMP	Correo, SNMP, herramientas
Facilidad de integración	Muy alta	Baja	Alta	Alta	Alta	Media
Soporte técnico	Alto	Limitado en OSS	Muy alto	Alto	Alto	Alto
Escalabilidad	Media	Baja	Muy alta	Muy alta	Alta	Muy alta
Relación costo-beneficio	Excelente	Buena con personal capacitado	Potente pero costoso	Flexible pero elevado	Equilibrada	Robusta, pero exige experiencia

Tabla 1 Comparación de los diferentes SIEMs propuestos

4.4.2 Soluciones de detección y respuesta en ENDPOINTS (EDR)

Para la protección de los dispositivos finales, se consideraron alternativas que garantizan una defensa contra ataques informáticos.

- Kaspersky Endpoint Detection and Response (KEDR) brinda una seguridad integral analizando los comportamientos y la información sobre amenazas. Entre sus funcionalidades más destacadas se encuentran el aislamiento remoto de dispositivos y un análisis forense detallado.
- SentinelOne basado inteligencia artificial para detectar malware y ataques sin archivos, con un precio que fluctúa entre $6 y $9 por dispositivo mensual, lo que se traduce en un costo anual de entre $72 y $108 por dispositivo.
- CrowdStrike Falcon, que destaca por su análisis continuo, tiene un precio estimado que varía de $8 a $15 por dispositivo al mes, lo que equivale a un gasto anual de entre $96 y $180.
- Fortinet FortiEDR se presenta como una opción rentable, con precios que van de $5 a $10 por dispositivo al mes, es decir, entre $60 y $120 anuales por cada unidad.
- Microsoft Defender for Endpoint, que se conecta con el paquete de Microsoft 365, comienza en $5. 20 por usuario al mes dentro del plan de suscripción Microsoft 365 E5 Security, alcanzando aproximadamente $62 anuales por usuario.

4.4.3 Seguridad en correo electrónico

Para proteger el correo electrónico de ataques, se han considerado opciones que mejoran la seguridad contra riesgos como phishing, software malicioso y ataques específicos, entre las herramientas se analizaron:

- Microsoft 365 Defender, junto con Exchange Online Protection, brinda un filtrado avanzado de amenazas y automatización en las respuestas, con precios entre los $2 a $8 por usuario cada mes, de acuerdo con el nivel de protección que se elija.

- Proofpoint Email Protection, cuyos costos se encuentran entre $30 y $50 por usuario al año, ofreciendo una defensa eficaz contra ataques complejos.
- Barracuda Email Security Gateway proporciona una protección amplia contra spam, malware y fraudes de ingeniería social, con tarifas que oscilan entre $1.50 y $4 por usuario mensualmente, lo que equivale a entre $18 y $48 anualmente.
- Google Workspace Security, que refuerza la protección en Gmail, ofrece un filtrado avanzado de amenazas con precios que van de $6 a $18 por usuario al mes, dependiendo del plan elegido.

5. Procesos, procedimientos y herramientas de monitoreo para la operación del SOC

En esta sección se presentará la recomendación de la herramienta de monitoreo de eventos a utilizar dentro de la corporación. Para ello, se consideran dos opciones principales: por un lado, el uso de Dynatrace, el cual ya se encuentra con un contrato vigente dentro de la institución, y por otro, la posibilidad de contratar un SIEM específicamente orientado al monitoreo de eventos de seguridad, siendo en este caso KUMA, debido a su alta compatibilidad con el EDR actualmente implementado de Kaspersky.

Se expondrán las ventajas y desventajas de ambas opciones, considerando el contexto operativo y técnico previamente analizado en la empresa, con el objetivo de seleccionar la solución más adecuada para garantizar la visibilidad y control de los eventos relacionados con la seguridad.

Además, se detallarán los procesos y procedimientos operativos que cada integrante del equipo SOC deberá seguir, de acuerdo con el rol que desempeñe. Esta estructura permitirá que la respuesta ante incidentes se realice de forma organizada y coherente, promoviendo una coordinación efectiva entre los niveles de análisis y asegurando que cada evento sea tratado conforme a su criticidad. Esto ayudará a mantener una respuesta coordinada y organizada, mejorando los tiempos de reacción y asegurando la continuidad operativa ante posibles amenazas.

5.1 Herramienta de Monitoreo

Para fortalecer la vigilancia y el análisis de seguridad en los dispositivos finales del GAD Municipal de Cuenca, se ha optado por priorizar el uso del EDR de Kaspersky como herramienta principal de monitoreo. Esta solución ha demostrado ser efectiva frente a amenazas avanzadas, además de ofrecer una integración fluida con

plataformas SIEM gracias a su compatibilidad con formatos de log como Syslog, CEF, LEEF y JSON. Esto facilita su implementación en arquitecturas de seguridad diversas.

En este sentido, también se podría considerar usar Dynatrace, que es compatible con el EDR de Kaspersky, sobre todo por su habilidad para recibir registros en formato Syslog, que es el formato que utiliza el EDR para el envío de sus datos. Esta opción es aún más factible porque la institución ya tiene Dynatrace en funcionamiento, por lo que solo sería necesario configurarlo correctamente y activar la conexión para la obtención de registros.

No obstante, se detectó una limitación técnica respecto a los registros del firewall Palo Alto, puesto que estos no pueden ser procesados directamente por Dynatrace sin una API de integración o un proceso intermedio de adaptación. Una opción sería crear una solución basada en una API (como la de ChatGPT o similar) que reciba los eventos de Palo Alto, los procese y los almacene en un servidor que funcione como un respaldo. Aunque esta opción es posible, su complejidad y los requisitos de mantenimiento son altos, además, no están enfocados directamente en la detección de amenazas o la correlación de eventos como lo haría un SIEM.

Frente a esta situación, se recomienda como solución principal el despliegue de Kaspersky Unified Monitoring and Analysis Platform (KUMA), un SIEM que comparte fabricante con el EDR implementado, lo que garantiza una integración directa y eficiente. KUMA tiene la capacidad de consolidar eventos desde múltiples fuentes, incluyendo Palo Alto mediante Syslog, brindando una visibilidad centralizada de los incidentes de seguridad.

Entre sus beneficios se destacan:

- Compatibilidad nativa con Kaspersky EDR.
- Capacidad para almacenar eventos localmente, sin depender de la nube.
- Notificaciones automatizadas vía correo o consola.
- Licenciamiento accesible y adaptable a entornos públicos.

Además, al ya contar con licencias del EDR, el GAD podría negociar un paquete conjunto, optimizando los costos y el soporte técnico. A diferencia de Dynatrace, que está más enfocado en la observación del rendimiento de servicios y aplicaciones, KUMA cumple completamente con las funciones típicas de un SIEM, como la correlación de eventos de seguridad, generación de alertas, análisis forense y trazabilidad. Estas funciones son vitales para el SOC propuesto funcione correctamente. Además, su modelo de licenciamiento es accesible y flexible, lo que lo convierte en una opción ideal para una entidad pública como el GAD Municipal de Cuenca, que necesita una herramienta confiable, centralizada y sostenible a largo plazo.

Al analizar el caso en el cual, por decisiones internas, el GAD Municipal no opte por la adquisición del software KUMA, la institución se vería limitada a realizar un monitoreo básico de eventos mediante la herramienta Dynatrace. Sin embargo, al no tratarse de una herramienta diseñada específicamente para la gestión de eventos de seguridad como lo es un SIEM, Dynatrace presentaría limitaciones en la detección de amenazas complejas, así como en la capacidad de generar correlaciones avanzadas de eventos. Por otra parte, esto podría derivar en el incumplimiento de normativas como la detección y reporte de eventos, el análisis de incidentes y la correlación de información relevante para toma de decisiones descritas en la norma ISO/IEC 27035 [21]. La falta de un SIEM formal incrementaría la dependencia en el análisis manual, lo que podría afectar negativamente los tiempos de respuesta y aumentar la posibilidad de falsos positivos.

5.2 Procesos y Procedimientos del equipo SOC

A continuación, se presentan los procesos y procedimientos que deberá cumplir cada uno de los miembros del equipo SOC, los cuales han sido definidos en función de su rol dentro de la estructura operativa. Esta organización permite que cada integrante actúe de forma eficiente ante la ocurrencia de eventos de seguridad, siguiendo un flujo de trabajo claro y previamente establecido.

Adicionalmente, en la Ilustración 4 se pueden visualizar los diferentes tipos de eventos que podrían presentarse en la organización, los mismos que han sido clasificados según su nivel de criticidad. Esta clasificación permite determinar hasta qué nivel deben escalarse los eventos, garantizando una respuesta proporcional al impacto y facilitando la toma de decisiones por parte del equipo en cada fase del incidente.

PROCESOS DE DETECCIÓN Y MONITOREO DE EVENTOS	
Objetivo	Implementar un monitoreo dinámico, continuo y en tiempo real para la identificación de eventos presentes en las redes, equipos y endpoints mediante herramientas como SIEM, EDR e IDS.
Responsable	Analista de SOC Nivel 1
Procedimientos • Supervisar continuamente el dashboard del SIEM. • Detectar comportamientos anormales, como intentos fallidos de acceso o conexiones a direcciones de listas negras. • Clasificar los eventos como falso positivo o incidentes. • Registrar en la bitácora de eventos de seguridad y escalar según la criticidad.	

Tabla 2 PROCESOS DE DETECCIÓN Y MONITOREO DE EVENTOS

PROCESO DE ANALISIS E INVESTIGACIÓN DE INCIDENTES	
Objetivo	Confirmar los incidentes de seguridad mediante la revisión de registros, tráfico de red y herramientas del sistema.
Responsable	Analista de SOC Nivel 2
Procedimientos • Analizar los logs del sistema, del SIEM y del endpoint. • Revisar el tráfico de la red. • Identificar la ruta de infección o su fuente. • Determinar el alcance e impacto. • Documentar los hallazgos e implementar acciones para la mitigación o escalamiento.	

Tabla 3 PROCESO DE ANALISIS E INVESTIGACIÓN DE INCIDENTES

PROCESO DE CONTENCIÓN Y RESPUESTA	
Objetivo	Detener la propagación de las amenazas para preservar la integridad de los sistemas.
Responsable	Analista de SOC Nivel 3 (Threat Hunter)
Procedimientos • Aislar los equipos comprometidos. • Restringir los accesos o credenciales comprometidas. • Implementar reglas de firewall o bloqueos de proxy. • Comunicar internamente el inconveniente a los responsables de sistemas.	

Tabla 4 PROCESO DE CONTENCIÓN Y RESPUESTA

PROCESO DE ERRADICACIÓN Y REPARACIÓN	
Objetivo	Eliminar la amenaza por completo y restablecer los servicios de manera segura.
Responsable	Analista de SOC Nivel 3 (Threat Hunter)
Procedimientos • Uso de herramientas forenses para verificar que no quede rastro del ataque. • Reinstalar el sistema. • Restaurar los datos a partir de los respectivos backups. • Validar el funcionamiento y la conectividad segura antes de reincorporarlo. • Documentar los hallazgos e implementar acciones para la mitigación o escalamiento.	

Tabla 5 PROCESO DE ERRADICACIÓN Y REPARACIÓN

PROCESO DE ANALISIS POST INCIDENTE	
Objetivo	Evaluar el incidente ocurrido e implementar mejoras en el protocolo y en el sistema de seguridad.
Responsable	Responsable de Respuesta a Incidentes
Procedimientos • Elaboración del informe con la línea de tiempo, causas raíz y fallas detectadas. • Modificar los parámetros de detección y corrección en el SIEM. • Establecer nuevas normativas o políticas de acceso. • Actualizar el plan de respuesta ante incidentes. • Implementar nuevas capacitaciones para el personal.	

Tabla 6 PROCESO DE ANALISIS POST INCIDENTE

PROCESO DE CUMPLIMIENTO Y AUDITORIA	
Objetivo	Garantizar que las actividades del SOC se encuentren alineadas con normativas internacionales y políticas nacionales.
Responsable	Oficial de cumplimiento y auditoria
Procedimientos • Auditorías periódicas de los procesos, registros y tiempos de respuesta. • Validar que los controles estén basados en las normativas ISO. • Implementar simulacros y documentar los incidentes. • Emitir reportes a la dirección de TICs y al Coordinador del SOC.	

Tabla 7 PROCESO DE CUMPLIMIENTO Y AUDITORIA

PROCESO DE GESTION DE COBERTURA HORARIA	
Objetivo	Establecer una atención continua e inmediata mediante turnos rotativos fuera del horario laboral.
Responsable	Coordinador del SOC. Todos los analistas SOC.
Procedimientos • Establecer un horario rotativo para jornadas nocturnas y fines de semana. • Configuración de alertas automáticas. • Registrar todas las actividades de la jornada extra. • Planificar la rotación de los turnos con el equipo de analistas.	

Tabla 8 PROCESO DE GESTION DE COBERTURA HORARIA

PROCESO DE COMUNICACIÓN INTERNA Y ESCALAMIENTO	
Objetivo	Facilitar una comunicación clara y eficaz ante incidentes de seguridad.
Responsable	Responsable de Respuestas a Incidentes. Todos los analistas SOC.
Procedimientos • Establecer un horario rotativo para jornadas nocturnas y fines de semana. • Configurar alertas automáticas. • Registrar todas las actividades de la jornada extra. • Planificar la rotación de los turnos con el equipo de analistas.	

Tabla 9 PROCESO DE COMUNICACIÓN INTERNA Y ESCALAMIENTO

Nivel de Criticidad	Tipo de Incidente	Descripción	Responsable (Nivel)
Baja	Actividad inusual sin impacto	Comportamiento fuera de lo común sin consecuencias identificadas.	Nivel 1
Baja	Software no autorizado sin riesgo	Instalación de software no crítico ni malicioso.	Nivel 1
Baja	Phishing detectado sin interacción	Correo/mensaje fraudulento detectado, sin que el usuario interactúe.	Nivel 1
Media	Phishing con interacción sin compromiso	Usuario accede a contenido fraudulento pero no compromete datos.	Nivel 1 (con escalamiento a N2 si se repite)
Media	Malware inactivo o contenido malicioso bloqueado	Detección sin ejecución, controlado por sistemas defensivos.	Nivel 1
Media	Uso indebido de privilegios leves	Accesos no autorizados menores sin intención maliciosa.	Nivel 1 o 2
Media	Smishing o vishing sin compromiso	Mensajes o llamadas fraudulentas sin entrega de información.	Nivel 1
Alta	Phishing exitoso con compromiso de credenciales	Usuario entrega información sensible por engaño.	Nivel 2
Alta	Malware ejecutado pero contenido	Ejecución parcial o controlada de código malicioso.	Nivel 2
Alta	Acceso no autorizado significativo	Acceso indebido a sistemas sensibles o con datos críticos.	Nivel 2
Alta	Fuga parcial de información	Exfiltración de datos no críticos o internos.	Nivel 2
Crítica	Compromiso total de sistemas	El atacante obtiene control completo de activos.	Nivel 3
Crítica	Spear phishing dirigido con impacto	Ataque personalizado y exitoso a personal clave.	Nivel 3
Crítica	Fuga de información sensible o regulada	Robo de datos protegidos legalmente.	Nivel 3
Crítica	Ataques persistentes avanzados (APT)	Infiltración prolongada con técnicas sofisticadas.	Nivel 3
Crítica	Interrupción de servicios esenciales	Caída o denegación de servicios fundamentales.	Nivel 3

Ilustración 4 Tipos de Eventos

El modelo de Centro de Operaciones de Seguridad (SOC) propuesto ha sido diseñado de forma modular, permitiendo su implementación progresiva, comenzando por el GAD Municipal de Cuenca y posteriormente expandiéndose

hacia las demás empresas que forman parte del proyecto de la municipalidad. Este enfoque modular y escalable permite que otras entidades públicas, municipios u organizaciones gubernamentales puedan adoptar estructuras similares adaptadas a su contexto operativo y tecnológico.

Al presentar una arquitectura basada en herramientas compatibles, se facilita la escalabilidad y configuración del sistema de monitoreo, especialmente en entornos donde las entidades comparten tecnologías comunes, como un mismo EDR, firewall y endpoint. En este escenario, la implementación inicial se realizaría en el GAD Municipal, donde se optimizaría la configuración y los procesos del SOC, para luego replicar el modelo en el resto de las entidades municipales involucradas en el proyecto.

Este enfoque permitiría establecer un esquema pionero para la centralización de sistemas de seguridad en instituciones públicas, sirviendo como ejemplo para que otros municipios a nivel nacional puedan adoptar e implementar sus propios SOCs, fortaleciendo así la ciberdefensa gubernamental en el país.

5.3 Cotización general

En esta sección se abarca una un resumen general de la cotización, de tal manera de tener un amplio panorama del costo de la implementación del SOC de manera anual, mencionando las herramientas que serán de uso, junto al personal que formara parte del equipo. Esto permitirá mantener una visión del costo-beneficio de la implementación del SOC para el GAD municipal de Cuenca.

Categoría	Unidad/ Volumen	Costo unitario (USD)	Costo anual estimado (USD)
Seguridad de correo electrónico (Defender for O365 Plan 1)	1.569 usuarios	24 / usuario/año	**37.656**
EDR – Kaspersky EDR Optimum	1.250 endpoints	14,50 / endpoint/año	**18.125**
SIEM – KUMA (estimado 5–10 GB/día)	subscripción anual	12.000 aproximado	**12.000**
Soporte y capacitación	costo anual	—	**8.000**
Servidor físico	Costo anual x 5 años	—	**2.000 – 3.000**
Total, estimado anual	—	—	**68.781**

Tabla 10 Cotización general

En base a la información que se recompilo de [22], se realizó un aproximamiento de los costos anuales del despliegue y operación del SOC dentro del GAD Municipal de Cuenca demostrados en la Tabla 10. En el mismo que abarca las necesidades más urgentes del core corporativo, como la protección de los correos electrónicos institucionales, teniendo capacidad para 1569 empleados, según el dataset de los funcionarios públicos. Para lo cual se tomaron como referencia 1250 endpoints para el uso del EDR, un SIEM de monitoreo y centralización (KUMA), junto al trabajo de empleadores del área y capacitaciones el total redondea la cifra de $68.781.

Al comparar este monto con los activos críticos del GAD Municipal y el resto de las 15 corporaciones que participan en el proyecto, esta inversión de fortalecimiento en la ciberseguridad presenta una justificación ante posibles ataques, denegaciones de servicio, secuestro de información. Manteniendo una imagen a la ciudad de cuenca como pionera en la implicación e implementación ante temas de seguridad

de la información. La implementación del SOC propuesto debe ser tomado como una decisión estratégica y financieramente sostenible para salvaguardar la información y servicios proporcionados, según el análisis costo-beneficio analizado.

6. Conclusiones

- La implementación de un Centro de Operaciones de Seguridad (SOC) dentro del GAD Municipal de Cuenca se considera viable y necesaria, debido al crecimiento sostenido de las amenazas cibernéticas, al contexto organizativo de la entidad y al manejo de información crítica que esta gestiona de forma permanente.
- La estructura organizativa que se propone toma en cuenta los recursos técnicos y humanos del GAD, definiendo una jerarquía funcional clara y un modelo de gestión que permite cubrir horarios híbridos. Y así garantizar una vigilancia continua, sin sobrecargar al equipo SOC, gracias a una distribución equilibrada de responsabilidades.
- Los procesos y procedimientos definidos aseguran una operación escalable y adaptable del SOC. Se incluyen mecanismos de respuesta ante incidentes, monitoreo en tiempo real, análisis forense, comunicación interna efectiva y cumplimiento normativo, todo esto apoyado por herramientas tecnológicas disponibles o integrables en el entorno actual.
- El enfoque propuesto fue diseñado en base a entrevistas y validaciones con el personal del GAD, lo cual permitió estructurar un proyecto adaptado a la realidad institucional, alineado con las tecnologías de seguridad actualmente en uso y con proyección a futuros escenarios de mejora.
- Para las herramientas de monitoreo, se plantea iniciar con Dynatrace, complementado con una API que permita leer los registros del firewall. Como alternativa estratégica y más completa, se plantea la adquisición del SIEM KUMA de Kaspersky, el cual puede operar de forma directa con los logs de todas las herramientas de seguridad utilizadas por la institución. Ambas opciones responden al contexto actual del GAD, una orientada al monitoreo básico y otra con enfoque especializado en la gestión de eventos de seguridad.

7. Anexos

7.1 Programa de Formación para el Equipo SOC

Se desarrollará un programa de formación especializado, orientado a fortalecer las capacidades técnicas y operativas del personal que integrará el equipo SOC del GAD Municipal de Cuenca. Este programa busca garantizar que el equipo tenga las habilidades requeridas para detectar, analizar, responder y documentar correctamente los eventos de seguridad de la información, garantizando así un trabajo enfocado en las mejores prácticas y normas internacionales en gestión de incidentes.

En la Tabla 11 se presenta el contenido del programa de capacitación en el que participará todo el equipo del SOC. Esta capacitación podrá ser implementada de forma anual, permitiendo que, mediante el uso de evaluaciones y laboratorios simulados, el personal adquiera un conocimiento práctico y contextualizado sobre los distintos tipos de eventos de seguridad que podrían presentarse en el entorno institucional según su rol en el equipo.

La ejecución continua de auditorías internas y la aplicación de mejoras en los procesos del SOC permitirán que cada año el programa de formación se actualice conforme a las nuevas normativas, procedimientos y tecnologías adoptadas por el SOC, asegurando así un proceso de mejora continua en las capacidades del equipo operativo.

Estructura del Contenido del Programa de Capacitación		
Modulo	Contenido	Roles Obligados a Participar
Primer Módulo	Introducción al SOC, roles, normativas, procesos y procedimientos.	Analista Nivel 1, 2 y 3, CSIRT, Ingeniero de Seguridad y Cumplimiento y Auditoría
Segundo Módulo	Identificación, análisis, escalamiento y respuestas a incidentes.	Analista Nivel 1, 2 y 3, CSIRT
Tercer Módulo	Uso de las herramientas presentes en el SOC como: SIEM, EDR, Dynartrace, Palo Alto, etc.	Analista Nivel 1, 2 y 3, CSIRT, Ingeniero de Seguridad
Cuarto Módulo	Análisis forenses en entornos Linux y Windows.	Analista Nivel 2 y 3, CSIRT, Ingeniero de Seguridad
Quinto Módulo	Gestión de comunicación y documentación de incidentes.	Analista Nivel 1, 2 y 3, CSIRT, Cumplimiento y Auditoría
Sexto Módulo	Simulacro de la operación del SOC.	CSIRT, Cumplimiento y Auditoría

Tabla 11 Estructura del Contenido del Programa de Capacitación

7.2 Simulación de gestión de incidente de seguridad: Caso Phishing

Con el objetivo de validar la arquitectura propuesta del SOC, se plantea una simulación teórica basado en un ataque de phishing dirigido a un usuario del GAD municipal de Cuenca.

El escenario simulado se enfoca en un empleado recibe un correo con asunto “Actualización de credenciales institucionales”. El mensaje incluye un enlace a una página falsa de inicio de sesión. El usuario, sin sospechar, accede al enlace e introduce sus credenciales institucionales.

Fase 1 – Detección y Monitoreo (Nivel 1)

Responsable: Analista SOC Nivel 1

El SIEM identifica de manera automática un clic en una URL con etiqueta de categoría maliciosa gracias a su conexión con las bases de datos de inteligencia sobre amenazas. Al recibir la alerta, el analista de seguridad procede a confirmar el incidente examinando los logs de red y de navegación correspondientes, asegurándose de que no se trate de un falso positivo. Tras verificar la amenaza, clasifica el evento como un incidente de phishing y rápidamente inicia las acciones de contención. Como acción prioritaria, se bloquea la dirección IP del dominio malicioso a través del firewall, para evitar que otros usuarios tengan acceso al dominio comprometido. Una vez contenido, el incidente se escala al Nivel 2 para que el equipo especializado realice una investigación más profunda sobre el posible compromiso del equipo afectado.

Fase 2 – Análisis e Investigación (Nivel 2)

Responsable: Analista SOC Nivel 2

Usando la consola del EDR de Kaspersky, el analista examina el historial del dispositivo del usuario afectado. Identifica que las credenciales institucionales fueron ingresadas en el sitio fraudulento, lo cual representa una exposición crítica. También analiza los logs y flujos de red posteriores al ingreso, para verificar si hubo intentos de conexión con infraestructura externa. Ante la gravedad del caso, lo eleva al Nivel 3 para una investigación más profunda y acciones de contención.

Fase 3 – Respuesta Avanzada y Contención (Nivel 3)

Responsable: Analista Nivel 3 (Threat Hunter)

El analista de Nivel 3 lleva a cabo una revisión forense completa del equipo comprometido. Se valida que no hubo instalación de malware persistente, pero se procede al aislamiento temporal del endpoint, modificación de credenciales del usuario y bloqueo de cualquier dirección sospechosa registrada en las últimas 24

horas. Además, se preparan nuevas reglas de correlación en el SIEM para detectar eventos similares con mayor rapidez.

Fase 4 – Proceso de análisis Post incidente

Responsable: Responsable de Respuesta a Incidentes

Una vez neutralizado el incidente, se informa a la Dirección de TICs y a la Alta Dirección. Se documenta todo el ciclo del evento, incluyendo tiempos de respuesta, causa raíz, fallos en la cadena de detección y acciones implementadas. Como medida preventiva, se organiza una jornada de capacitación para el personal, enfocada en ingeniería social y verificación de correos sospechosos. Finalmente, se ajustan los procedimientos de respuesta a incidentes con base en las lecciones aprendidas.

Referencias

[1] R. Torres, M. J. director, R. Blanco, and J. Antonio, “Proceso para Definir y Establecer un Centro de Operaciones de Seguridad (SOC) en una Organización Financiera,” Jan. 2019, Accessed: May 19, 2025. [Online]. Available: https://reunir.unir.net/handle/123456789/8169

[2] “Ciberataques en 2023 | WatchGuard Blog.” Accessed: May 18, 2025. [Online]. Available: https://www.watchguard.com/es/wgrd-news/blog/cada-39-segundos-se-produjo-un-ciberataque-en-2023

[3] “El promedio de ciberataques a equipos OT en 2023 fue del 38.6%.” Accessed: May 18, 2025. [Online]. Available: https://latam.kaspersky.com/about/press-releases/el-promedio-de-ciberataques-a-equipos-ot-en-2023-fue-del-386

[4] “Ataques cibernéticos crecen un 60% en América Latina - DCD.” Accessed: May 18, 2025. [Online]. Available: https://www.datacenterdynamics.com/es/noticias/ataques-ciberneticos-crecen-un-60-en-america-latina/

[5] “El phishing creció 6X en América latina en el 2023 y Ecuador es uno de los países de mayor cantidad de ataques | Netlife.” Accessed: May 18, 2025. [Online]. Available: https://www.netlife.ec/phishing-2023-ecuador-america-latina/

[6] “El Municipio de Quito, víctima de ciberataque que afectó el 15 % de sus datos - SWI swissinfo.ch.” Accessed: May 18, 2025. [Online]. Available: https://www.swissinfo.ch/spa/el-municipio-de-quito-v%C3%ADctima-de-ciberataque-que-afect%C3%B3-el-15-de-sus-datos/47525602

[7] A. A. Mughal, “Building and securing the modern security operations center (soc),” *International Journal of Business Intelligence and Big Data Analytics*, vol. 5, pp. 1–15, 2022.

[8] M. Martínez Gómez, J. Enrique, and L. Patiño, “Implementación de un centro de operaciones de seguridad (SOC) de código abierto con elementos de red para sistemas industriales.” [Online]. Available: www.etsit.upv.es

[9] I. A. D. Bank and O. of A. States, “Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe,” Jul. 2020, doi: 10.18235/0002513.

[10] Xiaolong. Zheng, *IEEE ISI 2017 : IEEE International Conference on Intelligence and Security Informatics: Security and Big Data : July 22-24, 2017 - Beijing, China*. IEEE, 2017.

[11] . IEEE Staff, *2012 IEEE Conference on Technologies for Homeland Security (HST)*. IEEE, 2012.

[12] N. Miloslavskaya, “Security Operations Centers for Information Security Incident Management,” in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, 2016, pp. 131–136. doi: 10.1109/FiCloud.2016.26.

[13] R. Torres, M. J. Director, R. Blanco, and J. Antonio, “Trabajo Fin de Máster.”

[14] E. Kpmg, E. N. La, S. De Bogota, -Colombia Jorge, and E. C. Rodriguez, “DISEÑO DEL ESQUEMA DE IMPLEMENTACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) DE LA INFORMACIÓN EN LA,” 2021.
[15] Fortinet, “Un informe semestral de FortiGuard Labs Informe global del panorama de amenazas.” Accessed: Mar. 19, 2025. [Online]. Available: https://www.fortinet.com/blog/threat-research
[16] O. I. Falowo, L. Botsyoe, K. Koshoedo, and M. Ozer, “Enhancing Cybersecurity with Artificial Immune Systems and General Intelligence: A New Frontier in Threat Detection and Response,” *IEEE Access*, 2024, doi: 10.1109/ACCESS.2024.3454543.
[17] P. Hernán, B. Director, : Raúl, and H. Saroka, “Centro de operaciones de seguridad : estrategia, diseño y gestión,” 2018.
[18] A. Yushko, R. Shevchuk, K. Lopacinski, M. Leszczynska, O. Yashchyk, and T. Yurchyshyn, “Shielding Web Application against Cyber-Attacks using SIEM,” in *Proceedings - International Conference on Advanced Computer Information Technologies, ACIT*, 2023, pp. 393–396. doi: 10.1109/ACIT58437.2023.10275630.
[19] “Diseño e implantación de un centro de operaciones de seguridad (en el MINISDEF).” Accessed: May 19, 2025. [Online]. Available: http://calderon.cud.uvigo.es/items/acf3c6c5-a2ec-4a34-a222-9265269a07e7
[20] A. A. Zakharov, A. M. Shabalin, and K. S. Kruchkovsky, “Features of Creating a Virtual Laboratory for Developing and Applying Correlation Rules in Modern SIEM-Systems when Training Security Operation Center Analysts (by the Example of Microsoft Windows),” in *Proceedings - 2024 International Russian Smart Industry Conference, SmartIndustryCon 2024*, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 367–372. doi: 10.1109/SmartIndustryCon61328.2024.10515421.
[21] “Microsoft Word - Proyecto Yesid Tibaquira - Final | Enhanced Reader.”
[22] “Error 404 - Cuenca en Datos.” Accessed: Aug. 24, 2025. [Online]. Available: https://cuencaendatos.cuenca.gob.ec/dataset/funcionarios-publicos-2025%20realizamos