Universidad Autónoma de Ciudad Juárez

Instituto de Ingeniería y Tecnología

Departamento de Ingeniería Eléctrica y Computación

Maestría en Cómputo Aplicado

"Diseño e implementación de un Centro de Operaciones de Seguridad (SOC) basado en cómputo en la nube"

Tesis para obtener el grado de:

Maestro en Cómputo Aplicado

Ing. Fredy Fernando Álvarez Sánchez

"Becado por el Consejo Nacional de Humanidades, Ciencia y Tecnología"

Bajo la dirección del

Dr. Víctor Manuel Morales Rocha

Ciudad Juárez, Chihuahua, agosto de 2026

Ciudad Juárez, Chihuahua, a 31de agosto de 2026

Asunto: Autorización de publicación

C. Fredy Fernando Alvarez Sanchez

Presente.-

En virtud de que cumple satisfactoriamente los requisitos solicitados, informo a usted que se autoriza la publicación del documento de **Diseño e implementación de un Centro de Operaciones de Seguridad (SOC) basado en cómputo en la nube**, para presentar los resultados del proyecto de titulación con el propósito de obtener el título de Maestro en Cómputo Aplicado.

Sin otro particular, reciba un cordial saludo.

Dr. Víctor Manuel Morales Rocha

Director de Tesis

Declaración de Originalidad

Yo, Fredy Fernando Álvarez Sánchez, declaro que el material contenido en esta publicación fue elaborado con la revisión de los documentos mencionados en el capítulo de Bibliografía, y que la solución obtenida es original y no ha sido copiada de ninguna otra fuente ni utilizada para obtener otro título o reconocimiento en otra institución de educación superior.

Fredy Fernando Alvarez Sanchez
Maestrante

Agradecimientos

Estimados docentes, colaboradores y amigos,

Quiero expresar mi más profundo agradecimiento por su invaluable apoyo durante el desarrollo de mi proyecto en la Maestría en Cómputo Aplicado. Culminar esta etapa no habría sido posible sin la guía técnica, el tiempo y la disposición de cada uno de ustedes.

A mis mentores, gracias por compartir su experiencia y por retarme a alcanzar la excelencia académica. A mis colegas y amigos les agradezco enormemente las horas de discusión, el intercambio de ideas y el respaldo moral en los momentos de mayor complejidad técnica. Su colaboración no solo fortaleció la calidad de mi investigación, sino que también enriqueció mi crecimiento profesional y personal.

Este logro es compartido. Me siento honrado de haber contado con un equipo tan talentoso y generoso. Gracias por creer en este proyecto y por ser parte fundamental de este camino hacia la especialización.

Con gratitud y respeto,

Dedicatoria

Para mi esposa Sara y mi hijo Kalil:

A Sara, mi compañera de vida, por ser el pilar fundamental que sostuvo este sueño. Gracias por tu paciencia infinita, por entender mis ausencias durante las largas jornadas de estudio y por recordarme siempre el propósito de mi esfuerzo. Tu amor y apoyo incondicionales son el motor que impulsa cada uno de mis pasos.

A Kalil, mi hijo. Aunque aún eres muy joven para comprender el esfuerzo que implica estudiar, también eres la razón por la que busco ser mejor cada día. Espero que este logro sea para ti un ejemplo de que, con dedicación y perseverancia, cualquier meta es alcanzable. Pronto será tu oportunidad de realizarte.

Todo este trabajo y la culminación de mi maestría se los dedico a ustedes por ser mi hogar, mi familia y mi mayor alegría.

Los amo profundamente.

Contenido

Glosario de términos

- **SOC (Security Operations Center):** Centro encargado de monitorear, detectar, responder y prevenir incidentes de ciberseguridad en tiempo real.
- **SIEM (Security Information and Event Management):** Sistema que recolecta, analiza y correlaciona eventos de múltiples fuentes para detectar amenazas y generar alertas.
- **Endpoint:** Dispositivo final dentro de una red (PC, laptop, servidor, etc.) que puede ser monitoreado o protegido por herramientas de seguridad.
- **Log:** Registro cronológico de eventos generados por sistemas, aplicaciones o dispositivos que pueden analizarse para detectar anomalías.
- **Análisis de vulnerabilidades:** Proceso de identificación, clasificación y evaluación de debilidades en sistemas o redes que pueden ser explotadas por atacantes.
- **Respuesta a incidentes:** Conjunto de acciones coordinadas para contener, erradicar y recuperarse de un evento de seguridad.
- **Threat Intelligence (Inteligencia de amenazas):** Información procesable sobre amenazas actuales o emergentes que permite prevenir o mitigar ataques.
- **MITRE ATT&CK:** Base de conocimientos sobre técnicas y tácticas usadas por atacantes, útil para clasificación y detección de amenazas.
- **IoC (Indicator of Compromise):** Evidencia observable de una posible intrusión, como direcciones IP, hashes de archivos maliciosos o URL sospechosas.
- **Honeypot:** Sistema señuelo diseñado para atraer atacantes y estudiar sus técnicas sin poner en riesgo la infraestructura real.
- **Firewall:** Sistema de filtrado de tráfico de red que permite o bloquea comunicaciones según políticas de seguridad definidas.
- **VPN (Virtual Private Network):** Tecnología que crea una conexión cifrada sobre una red pública para proteger la confidencialidad de la información.
- **CVE (Common Vulnerabilities and Exposures):** Catálogo público de vulnerabilidades conocidas en software y hardware.

- **Phishing:** Técnica de ingeniería social para obtener credenciales o datos mediante correos o sitios falsos.
- **Data Lake:** Repositorio centralizado donde se almacenan grandes volúmenes de datos, tanto estructurados como no estructurados, para su análisis.
- **Dashboard:** Interfaz gráfica que permite visualizar información relevante (como alertas o métricas) en tiempo real.
- **Playbook:** Conjunto predefinido de acciones automatizadas para responder a un incidente específico.
- **Zero Trust:** Modelo de seguridad que asume que ningún usuario o dispositivo es confiable por defecto, incluso dentro de la red.
- **Syslog:** Protocolo estándar para enviar mensajes de registro desde dispositivos a un servidor centralizado.
- **Normas ISO/IEC 27001:** Estándares internacionales para la gestión de la seguridad de la información.
- **NIST SP 800-61:** Guía del Instituto Nacional de Estándares y Tecnología de Estados Unidos de América para la gestión de incidentes de seguridad informática.
- **Alertas de seguridad:** Mensajes generados por sistemas de monitoreo que indican posibles eventos sospechosos o maliciosos.
- **Correlación de eventos:** Proceso que relaciona múltiples registros o eventos para identificar patrones de ataque o incidentes.
- **Base de datos NoSQL:** Sistema de gestión de datos no relacional utilizado para almacenar grandes volúmenes de información flexible y escalable.
- **Sysmon:** Herramienta de Microsoft que proporciona monitoreo detallado del sistema para detección avanzada de amenazas.
- **Wazuh:** Plataforma de código abierto para monitoreo de seguridad, detección de intrusos y análisis de integridad.
- **Suricata:** Motor de detección de amenazas basado en red capaz de realizar inspección profunda de paquetes.
- **AlienVault OTX:** Plataforma colaborativa de intercambio de inteligencia de amenazas en tiempo real.

- **MISP (Malware Information Sharing Platform):** Plataforma de código abierto para el intercambio de indicadores de compromiso y amenazas cibernéticas.

Ilustraciones

Resumen

Esta tesis presenta el diseño e implementación del Centro de Operaciones de Seguridad (SOC) para la Universidad Autónoma de Ciudad Juárez (UACJ), que utiliza computación en la nube y herramientas de código abierto. El objetivo es centralizar y mejorar las operaciones de ciberseguridad mediante la integración de la recopilación de registros de eventos, el monitoreo en tiempo real, la inteligencia de amenazas y la respuesta a incidentes. El SOC propuesto utiliza Wazuh como solución EDR, Elastic Stack como SIEM, Greenbone para la gestión de vulnerabilidades y MISP para compartir inteligencia sobre amenazas. La metodología siguió un ciclo de vida iterativo, basado en prototipos y apoyado en el análisis de riesgos (NIST SP 800-30), el modelado de la arquitectura, la definición de métricas y el despliegue piloto. Los resultados incluyen un prototipo funcional, la formalización de procedimientos operativos, la colaboración interinstitucional y la creación de un equipo de ciberseguridad capacitado. El proyecto posiciona al SOC de la UACJ como una solución escalable y replicable alineada con los marcos ISO 27001, NIST y MITRE ATT&CK.

Palabras clave: SOC, ciberseguridad, Wazuh, Elastic Stack, MISP, SIEM, EDR, vulnerabilidades, inteligencia de amenazas, NIST SP 800-30, ISO/IEC 27001, MITRE ATT&CK.

Abstract

This thesis presents the design and implementation of the Security Operations Centre (SOC) for the Autonomous University of Ciudad Juárez (UACJ), which utilises cloud computing and open-source tools. The aim is to centralise and improve cybersecurity operations by integrating event log collection, real-time monitoring, threat intelligence and incident response. The proposed SOC utilises Wazuh as an EDR solution, Elastic Stack as a SIEM, Greenbone for vulnerability management, and MISP for sharing threat intelligence. The methodology followed an iterative, prototype-based lifecycle supported by risk analysis (NIST SP 800-30), architecture modelling, the definition of metrics, and a pilot deployment. The results include a functional prototype, the formalisation of operational procedures, inter-institutional collaboration and the creation of a trained cybersecurity team. The project positions the UACJ SOC as a scalable and replicable solution aligned with the ISO 27001, NIST and MITRE ATT&CK frameworks.

Keywords: SOC, cybersecurity, Wazuh, Elastic Stack, MISP, SIEM, EDR, vulnerabilities, threat intelligence, NIST SP 800-30, ISO/IEC 27001, MITRE ATT&CK.

Introducción

En la actualidad, la adopción de servicios de cómputo en la nube es fundamental para la competitividad institucional; sin embargo, esta evolución tecnológica expone a las organizaciones a vulnerabilidades que pueden comprometer sus activos más valiosos. En la Universidad Autónoma de Ciudad Juárez (UACJ), aunque existen herramientas de monitoreo, estas operan de manera aislada y carecen de coordinación efectiva con la Dirección General de Tecnologías de la Información (DGTI). Esta falta de centralización limita la capacidad institucional para detectar y responder a incidentes de manera oportuna, lo que genera una exposición al riesgo que debe mitigarse con urgencia.

Para resolver esta problemática, el presente trabajo propone el diseño e implementación de un Centro de Operaciones de Seguridad (SOC) basado en cómputo en la nube y en herramientas de código abierto. La arquitectura técnica utiliza plataformas líderes como Wazuh para la detección y respuesta en endpoints (EDR) y Elastic Stack como sistema central de gestión de eventos (SIEM). Esta integración permite centralizar la recopilación de registros de eventos y realizar análisis inteligentes en tiempo real para mejorar la visibilidad y la defensa de la infraestructura universitaria.

La metodología empleada sigue un modelo de ciclo de vida iterativo y evolutivo basado en prototipos, lo que asegura que la solución se adapte progresivamente a los requerimientos reales de la institución. El proyecto se fundamenta en estándares internacionales de rigor industrial, académico y técnico, integrando el análisis de riesgos de NIST SP 800-30 y el marco de referencia MITRE ATT&CK para la clasificación de amenazas. Además, se establece un Acuerdo de Nivel de Servicio (SLA) con métricas claras de tiempo de detección y respuesta para garantizar la eficacia operativa del centro, así como la eficiencia de las detecciones de falsos positivos y verdaderos positivos.

Finalmente, la instauración del SOC-UACJ se posiciona como el mecanismo central para garantizar el derecho humano a la protección de los datos personales de la comunidad universitaria. Al transitar de un cumplimiento reactivo a una postura de "Privacidad por Diseño", la universidad asegura que el acceso a la información sea auditado conforme a los principios de legalidad y de lealtad. En última instancia, este centro no solo fortalece la defensa perimetral, sino que también constituye el pilar de la confianza institucional ante los órganos reguladores y ante la sociedad en general.

1. Planteamiento del problema.

1.1. Contextualización.

Hoy en día, los servicios de **cómputo en la nube** (en inglés, Cloud Computing) son elementos fundamentales para mantener la competitividad en la industria y en la economía [1]. Uno de los tres principales modelos de servicios en la **nube** es el software como servicio (SaaS, por sus siglas en inglés, Software as a Service). En este modelo, un proveedor de servicios externo aloja las aplicaciones y las pone a disposición en línea. Regularmente, para acceder a este tipo de servicio se requiere una suscripción en lugar de comprar la licencia de uso. Dado que el proveedor aloja la aplicación en la **nube**, su funcionamiento no se ve afectado [2]. No obstante, la preocupación por la seguridad de los servicios en la nube no desaparece entre los usuarios, especialmente respecto de su información [3].

En instituciones privadas y públicas donde se cuenta con servicios y tecnologías de información existen diversas vulnerabilidades que las hacen propensas a sufrir ataques maliciosos dirigidos a sus principales activos de valor [4], por lo que la necesidad de protegerse y/o actuar para mitigar riesgos y dar respuesta rápida a emergencias es primordial. Si bien dichas organizaciones suelen contar con herramientas de monitoreo subutilizadas, estas generan, en proporción a la magnitud de la organización, grandes volúmenes de datos e información que pueden encontrarse dispersos en diversas fuentes y dispositivos. En los procesos de acopio y análisis de información, el personal responsable invierte demasiado tiempo en actividades tediosas que pueden desalentarlo y no ser efectivas en cuanto a protección en tiempo real [5].

Un centro de operaciones de seguridad, o ***SOC*** (en inglés, Security Operations Center), es el punto focal para las operaciones de seguridad y defensa de la red informática de una organización [6]. El propósito del ***SOC*** es defender y supervisar de forma continua los sistemas y redes de la organización (es decir, la infraestructura cibernética). El ***SOC*** también es responsable de detectar, analizar y responder oportunamente a incidentes de ciberseguridad. La organización dota al ***SOC*** de personal técnico y operativo cualificado (p. ej., analistas de seguridad, personal de respuesta a incidentes, personal de seguridad de sistemas e ingenieros) e implementa una combinación de técnicas, gestión y operaciones. También se utilizan algunos controles (incluidas herramientas de monitoreo, escaneo y análisis forense) para monitorear, fusionar, correlacionar, analizar y responder a amenazas

[7]. Esto se logra gracias a los datos de eventos relevantes que se registran y analizan a partir de múltiples fuentes, comparándolos con los indicadores de compromiso (**IoC**) conocidos utilizados por los atacantes, para esto se aplican reglas de detección a partir de dichos indicadores.

Las fuentes antes mencionadas incluyen defensas perimetrales, dispositivos de red (por ejemplo, enrutadores, conmutadores) y fuentes de datos de punto final. El ***SOC*** proporciona una capacidad holística de conciencia situacional para ayudar a las organizaciones a determinar la postura de seguridad del sistema y de la organización [8]. Un ***SOC*** tiene la capacidad de salvaguardar todos los activos y esta capacidad puede obtenerse de varias maneras. Las organizaciones más grandes pueden implementar un ***SOC*** dedicado, mientras que las más pequeñas pueden contratar servicios de terceros para proporcionar una capa de seguridad a sus activos.

1.2. Descripción del problema.

Actualmente, en la Universidad Autónoma de Ciudad Juárez (**UACJ**) no se cuenta con un Centro de Operaciones de Seguridad formalmente establecido. Si bien existen diversas herramientas y aplicaciones para monitorear la seguridad del tráfico en la red universitaria, estas operan de forma aislada y sin una integración efectiva entre las distintas subdirecciones que conforman la Dirección General de Tecnologías de Información (**DGTI**). Esta falta de coordinación y centralización limita la capacidad institucional para detectar, analizar y responder a incidentes de manera oportuna, lo que genera una exposición a riesgos de seguridad de distintos niveles de criticidad que deben ser mitigados con urgencia.

1.3. Antecedentes.

Existen antecedentes bien documentados de algunos proyectos realizados siguiendo metodologías orientadas a la integración de distintos sistemas. En ellos se muestra la importancia de automatizar los procesos de almacenamiento de información y se describen algunos análisis sistemáticos realizados para definir los mejores procedimientos para mitigar los riesgos informáticos [9]. También se denota la importancia de tener personal asignado a las diversas funciones de operaciones de seguridad, como pueden ser:

- La planificación, el diseño y la coordinación de la operación de los elementos que sostienen los sistemas de comunicaciones.
- El establecimiento de métodos y procedimientos orientados al uso de los sistemas de red (hardware, software y dispositivos de comunicación).
- El desarrollo de proyectos de mejora continua de redes y tecnologías de la información para optimizar el desempeño de la red.
- El mantenimiento de la documentación de los sistemas (hardware, software y procedimientos operativos).
- El desarrollo e implementación de procedimientos de recuperación ante desastres para los sistemas de información y las comunicaciones.
- La administración de los sistemas de seguridad en centros de datos, tanto principales como secundarios (firewall, IDS, sistemas de acceso, etc.).
- El aseguramiento del cumplimiento de las normas, políticas y procedimientos de seguridad de la información.

En [10], el autor resalta la importancia del análisis de triaje (priorización), pues constituye una etapa fundamental en las operaciones cibernéticas de los ***SOC,*** dado que las fuentes masivas de datos generan grandes exigencias en la capacidad de procesamiento de la información y en el razonamiento analítico de los analistas de ciberseguridad. Además, en su mayoría, los analistas de seguridad inexpertos actúan con menor eficacia que los analistas expertos al decidir qué operaciones de triaje a realizar. Para mejorar el rendimiento de los analistas, se diseñan métodos (Playbooks) que describan las operaciones de respuesta que fueron diseñados por los analistas de seguridad expertos a partir de un análisis histórico de casos investigados [11]. En su tesis, el autor investiga diferentes métodos de recuperación de datos basados en redes neuronales recurrentes, incluyendo también la recuperación basada en reglas y en el contexto de las operaciones de triage de datos. Al mismo tiempo, analiza las nuevas orientaciones para solucionar el problema de la recuperación de las operaciones de triaje de datos.

Para los autores de [12], con la introducción de los ***SOC*** alrededor del año 2005, la importancia de estos ha crecido significativamente, especialmente a partir de 2015. Esto se debe a la necesidad primordial de prevenir incidentes cibernéticos graves y a la adopción de operaciones de seguridad centralizadas en las empresas. En su documento realizan un estudio bibliográfico para recopilar diversos puntos de vista. Utilizando la bibliografía descubierta para determinar el estado que, en su momento, regulaba la técnica de los ***SOC,*** se derivaron

los bloques de construcción primarios. También se identificaron los retos temporales de un ***SOC***. También detectaron una deficiencia muy notable en la investigación académica, ya que esta se centraba en los aspectos humanos y tecnológicos de un ***SOC,*** mientras que se descuidaba la conexión entre ambas áreas mediante procesos muy específicos (no técnicos).

El progresivo uso de los ***SOC*** por parte de la mayoría de las grandes organizaciones como parte de su estrategia de ciberseguridad, ha propiciado varios estudios enfocados en comprender y mejorar las operaciones de los ***SOC***. Sin embargo, hasta donde se sabe, no existía ninguna revisión bibliográfica sistemática sobre los retos a los que se enfrentan los analistas de ***SOC*** ni sobre las métricas de rendimiento de estos. En [13], los autores realizaron una "Revisión Sistemática de la Literatura" (***SLR***, por sus siglas en inglés), apegados a las directrices para la elaboración de ***SLR,*** y analizaron los artículos publicados sobre los ***SOC*** entre 2008 y 2018. Facilitaron una visión global de los obstáculos identificados por los analistas de los ***SOC, así*** como de los mecanismos de medición sugeridos en la bibliografía. Además, presentaron un mapeo de los retos y las métricas de rendimiento existentes que muestra cómo medir la eficacia de un analista al abordar un reto concreto, identifica ciertos inconvenientes y sugiere mejoras. Sus conclusiones han permitido a los analistas y gestores del ***SOC***, así como a la comunidad académica, una mejor comprensión de los retos que obstaculizan un mayor rendimiento de los analistas.

1.4. Objetivos.

Para el desarrollo del presente proyecto, se plantean un objetivo general y cinco objetivos particulares, basados en el alcance y las limitaciones de este.

1.4.1. Objetivo general.

Diseñar e implementar un Centro de Operaciones de Seguridad en la Universidad Autónoma de Ciudad Juárez (**UACJ**), basado en tecnologías de cómputo en la nube y en herramientas de código abierto, que permita la recolección y la correlación de registros de eventos (logs) para mejorar la visibilidad, la detección y la respuesta ante amenazas cibernéticas, promoviendo la protección integral de los activos informáticos institucionales.

1.4.2. Objetivos particulares.

1. **Establecer una arquitectura técnica para el SOC-UACJ**, basada en tecnologías de código abierto y de cómputo en la nube, que permita la recopilación, el procesamiento y la visualización centralizada de eventos de seguridad generados por los sistemas y dispositivos de la red institucional.
2. **Implementar una plataforma de monitoreo y análisis de seguridad que utilice herramientas de código abierto** e integre funciones de detección de intrusiones, análisis de logs, evaluación de vulnerabilidades, respuesta activa y correlación de eventos en tiempo real.
3. **Definir políticas y procedimientos para la gestión de incidentes de seguridad,** incluyendo la clasificación de eventos, la respuesta ante amenazas, el análisis forense y la documentación de actividades, en conformidad con marcos como NIST, ISO 27001 y MITRE ATT&CK.
4. **Capacitar al personal responsable de las operaciones del SOC en el uso de herramientas de inteligencia de amenazas,** la gestión de eventos de seguridad, el análisis de comportamiento y la respuesta automatizada, fomentando un enfoque proactivo y coordinado.
5. **Realizar una prueba de concepto del SOC-UACJ,** incluyendo la identificación y protección de activos críticos, la recolección de logs de múltiples fuentes, el monitoreo del tráfico de red y la validación de alertas, para evaluar la viabilidad técnica y operativa del modelo propuesto (ver Anexos 5 y 8).

1.4.3. Alcance.

- El proyecto tendrá como principal alcance el diseño e implementación de un sistema centralizado de recopilación, almacenamiento y análisis de registros de eventos (***logs***) generados por los sistemas informáticos, aplicaciones y dispositivos conectados a la red de la Universidad Autónoma de Ciudad Juárez, con el objetivo de fortalecer la capacidad institucional de detección, respuesta y toma de decisiones ante amenazas de ciberseguridad.
- Se incorporará la supervisión del tráfico de red mediante herramientas de código abierto, lo que permitirá realizar análisis detallados orientados a la detección de amenazas, la evaluación del rendimiento, la identificación de anomalías, con el fin de mejorar la visibilidad del comportamiento de la RedUACJ.

- El sistema propuesto integrará plataformas especializadas, como Wazuh, para la gestión de eventos, la detección de intrusiones y la evaluación de vulnerabilidades, así como herramientas complementarias para la visualización y el análisis, en concordancia con las mejores prácticas de ciberseguridad.
- Se identificarán los sistemas críticos y aplicaciones relevantes que generen información de seguridad y se configurarán para enviar sus registros al sistema centralizado, asegurando la compatibilidad, el control de formatos y la consistencia temporal de los logs.
- Se establecerán políticas y procedimientos técnicos para garantizar la integridad, confidencialidad y disponibilidad de los registros recopilados, alineados con marcos normativos como NIST SP 800-53, ISO 27001:2022 y las recomendaciones del MITRE ATT&CK.
- Se definirán métricas de desempeño y calidad para evaluar la eficacia del sistema de recolección y análisis de logs, incluyendo indicadores de cobertura, correlación de eventos, generación de alertas y tiempos de respuesta ante incidentes.
- Finalmente, se documentarán los resultados del proyecto mediante informes técnicos que incluyan estadísticas de operación, casos de prueba, análisis de eventos relevantes, hallazgos clave y recomendaciones para la mejora continua del sistema, dejando sentadas las bases para la consolidación futura de un ***SOC*** completo y funcional en la **UACJ**.

1.4.4. Limitaciones.

Las siguientes son las principales limitaciones del proyecto:

- El proyecto no contempla la gestión directa de incidentes detectados mediante sistemas de alerta temprana o plataformas de prevención de intrusiones (IPS), ya que su enfoque se centra exclusivamente en la recopilación, el análisis y la correlación de registros de eventos.
- No se incluirá la gestión de logs provenientes de sistemas o infraestructuras que no pertenezcan a la UACJ, tales como servicios administrados por terceros, proveedores externos o socios tecnológicos, por lo que la trazabilidad quedará restringida al entorno institucional.

- Quedan excluidos del alcance los sistemas y dispositivos que no se encuentren conectados a la RedUACJ, como estaciones de trabajo o servidores que operen en redes segmentadas, en redes privadas no integradas o fuera del dominio institucional.
- Tampoco se considerará la integración de equipos que, por limitaciones técnicas o de antigüedad, no sean compatibles con la infraestructura de recolección de logs, ya sea por no contar con soporte para agentes de monitoreo, protocolos estándar de exportación de registros, o interfaces remotas habilitadas.
- No se abordará la automatización de acciones correctivas o de contención (playbooks) ni el uso de plataformas avanzadas de orquestación (SOAR), dado que esta fase del proyecto se enfoca en establecer los cimientos para un SOC operativo y no en la madurez plena de la respuesta automatizada.
- El presente proyecto representa una fase inicial de implementación del SOC, por lo que no se cubrirá la operación continua bajo esquemas 24x7 ni la integración con servicios de inteligencia de amenazas en tiempo real tipo TIP (Threat Intelligence Platform), aunque se sientan las bases para su incorporación futura.

1.5. Justificación.

En la actualidad existe una serie de riesgos de "Seguridad Informática" que enfrentan las empresas u organizaciones, ya que reciben todo tipo de intentos y/o ataques maliciosos a sus sistemas de información. Según Kasperky [14], México es uno de los países que sufren más ataques informáticos por segundo a nivel mundial, por lo que los servicios de "Seguridad Informática" son una herramienta fundamental para salvaguardar los activos de las instituciones.

Un ***SOC*** puede proporcionar a la **UACJ** una capa adicional de seguridad cibernética y ayudar a proteger sus sistemas y datos contra amenazas externas e internas, lo que puede contribuir a garantizar la privacidad y la confidencialidad de los datos de los estudiantes, profesores y empleados de la universidad (ver Anexo 3). También puede garantizar la integridad y disponibilidad de los sistemas de información de la universidad a través de la implementación de controles de seguridad, la detección y respuesta rápida a amenazas de seguridad y la capacitación del personal en mejores prácticas de seguridad cibernética [15], [16].

Un centro de operaciones de seguridad informática puede ayudar desde la **DGTI** a la **UACJ** de diversas maneras, incluyendo:

- Monitoreo constante de la seguridad: El ***SOC*** puede supervisar en tiempo real la red y los sistemas de la universidad para detectar y responder rápidamente ante cualquier amenaza de seguridad. Esto puede ayudar a prevenir intrusiones no autorizadas, robos de datos y otros ataques.
- Investigación de incidentes de seguridad: Si se produce un incidente de seguridad, el ***SOC*** puede investigar su causa y proporcionar información valiosa sobre cómo evitar incidentes similares en el futuro. También puede ayudar a la universidad a determinar la magnitud del incidente y a tomar medidas para remediarlo.
- Protección contra amenazas externas: El ***SOC*** puede implementar medidas de seguridad adicionales para proteger la **UACJ** frente a amenazas externas, como ataques de ***phishing***, ***malware*** y otros tipos de ciberataques.
- Cumplimiento normativo: El ***SOC*** puede ayudar a la universidad a cumplir con las regulaciones y normativas de seguridad de la información, la Ley de Protección de Datos Personales de Sujetos Obligados [17] y otras regulaciones similares. También contribuiría a cumplir los acuerdos de los consorcios universitarios, así como las normativas vigentes de la Guardia Nacional.

Privacidad y Cumplimiento Legal como Pilar de Confianza Institucional

La implementación del **SOC-UACJ** no debe percibirse únicamente como una medida de defensa perimetral, sino como el mecanismo central para garantizar el derecho humano a la protección de los datos personales de la comunidad universitaria, conformada por alumnos, docentes y personal administrativo. En un entorno donde la **UACJ** procesa grandes volúmenes de información sensible en infraestructuras híbridas y en la nube, la vigilancia y la respuesta centralizadas se vuelven imperativas para cumplir con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados [17], [18], [19], [20].

Un ***SOC*** formalmente establecido permite a la Dirección General de Tecnologías de Información (**DGTI**) transitar de un cumplimiento normativo reactivo a una postura de "Privacidad por Diseño", alineada con los controles de seguridad y privacidad del marco NIST SP 800-53. Esta capacidad de monitoreo continuo asegura que los activos de información no solo estén disponibles e íntegros, sino que su acceso esté estrictamente auditado conforme a los principios de legalidad y lealtad.

Estratégicamente, la protección profunda de estos datos es el cimiento de la confianza institucional ante órganos reguladores como la Contraloría General y el Abogado General,

así como para fortalecer la reputación de la universidad ante consorcios académicos y organismos de seguridad nacional, como la Guardia Nacional. En última instancia, la instauración de este centro operativo posiciona a la UACJ como un referente en transparencia y seguridad de la información en el ámbito de las Instituciones de Educación Superior en México.

2. Marco teórico.

El presente marco teórico proporciona un contexto conceptual para la investigación realizada. El marco teórico establece una base sólida de conocimiento y ofrece un marco conceptual para la investigación. En la introducción de este documento se presentan algunos antecedentes, por lo que se exponen el marco conceptual, la revisión de la literatura, las teorías y las hipótesis que se utilizarán en la investigación [21].

2.1. Seguridad de los datos.

La seguridad de los datos se refiere a la protección de la información almacenada en sistemas informáticos o en cualquier medio digital, con el fin de evitar el acceso no autorizado, el uso indebido, la modificación o la destrucción de la información. Esto implica implementar medidas de seguridad, tanto físicas como lógicas, para garantizar la privacidad, la integridad y la disponibilidad de los datos.

Entre las medidas de seguridad más comunes se incluyen el uso de contraseñas robustas, la encriptación de la información, la autenticación de usuarios [22], la realización de copias de seguridad, la implementación de firewalls y sistemas de detección de intrusiones, así como la capacitación y concienciación de los usuarios sobre la importancia de la seguridad de los datos [23]. La seguridad de los datos es fundamental en cualquier organización para garantizar la protección de la información sensible y evitar consecuencias negativas, como pérdidas financieras, daños reputacionales y sanciones legales, entre otras [24].

2.2. Tríada CID.

La confidencialidad, integridad y disponibilidad, también conocida como la tríada de la **CID** (*CIA Triad*, en inglés), es un modelo diseñado para guiar las políticas de seguridad de la información dentro de una organización; ver la Ilustración 1.

- La confidencialidad se refiere a la protección de la información mediante la limitación del acceso a las personas autorizadas. Esto se logra mediante la implementación de

medidas de seguridad y de control de acceso que garantizan la privacidad y el secreto de la información o de los recursos sensibles.

- La disponibilidad se refiere a la capacidad de un sistema para estar en funcionamiento y disponible cuando se necesite. Esto significa que el sistema debe estar disponible para su uso en todo momento y que no debe haber interrupciones en el acceso a la información o a los datos [25].
- La integridad [26] se refiere a la precisión y la consistencia de los datos e información almacenados en un sistema. La integridad implica garantizar que los datos no sean alterados de manera no autorizada y que se mantengan precisos y confiables.[1]

En conjunto, la confidencialidad, la disponibilidad y la integridad se consideran los tres pilares de la seguridad informática y son elementos fundamentales que deben abordarse en la protección de los sistemas de información y en la gestión de la seguridad de los datos.

ILUSTRACIÓN 1. TRIADA CID (IMAGEN TOMADA DE LINKEDIN[1]).

2.3. Amenazas.

Las amenazas en seguridad informática son cualquier tipo de acción malintencionada cuyo objetivo sea comprometer la confidencialidad, la integridad o la disponibilidad de la

[1] https://www.linkedin.com/pulse/confidencialidad-integridad-y-disponibilidad-martinez-ramirez/?originalSubdomain=es

información almacenada en sistemas informáticos [27]. Algunas de las amenazas más comunes en seguridad informática incluyen:

- Virus y *malware*: programas maliciosos que se instalan en un sistema para dañar o robar información.
- Phishing: técnicas de ingeniería social que utilizan correos electrónicos o mensajes de texto falsos para engañar a los usuarios y obtener información personal o financiera.
- Ransomware: un tipo de programa malicioso que cifra los datos del usuario y exige un rescate para descifrarlos.
- Ataques de denegación de servicio (en inglés, Denial of Service, o ***DoS***): una técnica utilizada para saturar un sitio web o un servidor con tráfico para impedir el acceso de los usuarios legítimos.
- Ataques de Denegación de Servicio Distribuido (en inglés, Distributed Denial of Service o ***DDoS***) [28]: son un tipo de ciberataque que intenta impedir que un sitio web o recurso de red esté disponible, colapsándolo con tráfico malintencionado para que no pueda funcionar correctamente.
- Ataques de fuerza bruta: intentos repetitivos para descubrir contraseñas o claves de acceso a un sistema, probando diferentes combinaciones hasta encontrar la correcta.
- Ingeniería social: técnicas que emplean la persuasión o el engaño para obtener información confidencial de los usuarios.
- Robo de identidad: usurpación de la identidad de una persona para cometer actividades fraudulentas.
- Actores maliciosos: Ciberdelincuentes

En la Ilustración 2 se muestran algunas de las amenazas de seguridad informática más comunes, pero existen muchas otras técnicas y estrategias que los atacantes pueden emplear para comprometer la seguridad de los sistemas informáticos.

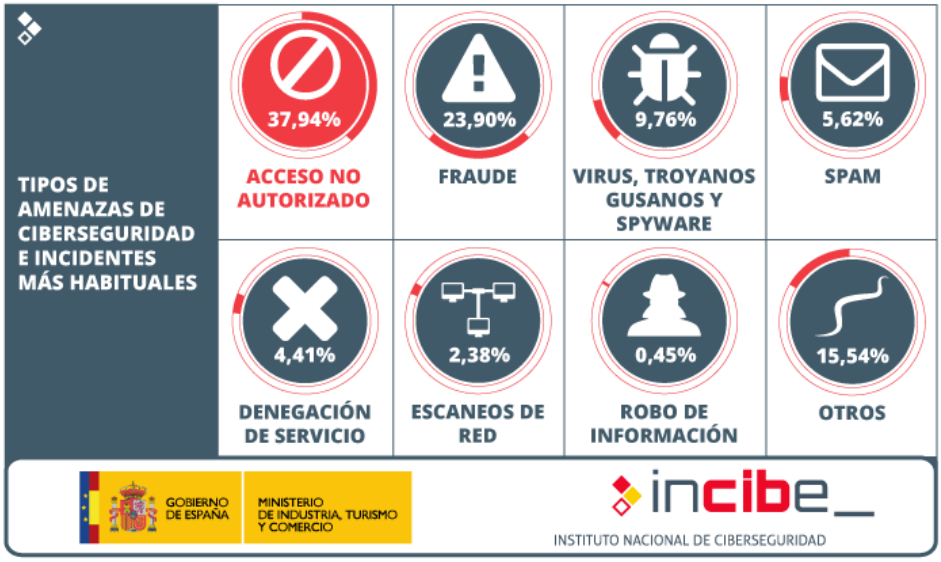


ILUSTRACIÓN 2. AMENAZAS DE SEGURIDAD MÁS FRECUENTES (IMAGEN TOMADA DE INTERNET[2]).

2.4. Vulnerabilidades.

Las vulnerabilidades de seguridad informática son puntos débiles o fallas en sistemas informáticos que pueden ser explotadas por atacantes para comprometer la integridad, la confidencialidad o la disponibilidad de la información almacenada en ellos [29]. Estas vulnerabilidades pueden ser el resultado de errores en el diseño o la implementación de software, de configuraciones incorrectas de hardware o software, de problemas en la gestión de contraseñas y credenciales, de la falta de actualizaciones de seguridad, entre otros factores [30].

Las vulnerabilidades pueden ser explotadas de diversas maneras, como la ejecución de código malicioso, la obtención de información sensible, el acceso no autorizado a sistemas, entre otras [31]. Es importante identificar y mitigar las vulnerabilidades de seguridad informática para garantizar la protección de la información y prevenir ataques cibernéticos. La gestión de

[2] Incibe. Instituto Nacional de Ciberseguridad. Gobierno de España. https://www.incibe.es/

vulnerabilidades es un proceso fundamental para la protección de los activos de ***IT***; véase la Ilustración 3.

ILUSTRACIÓN 3. GESTIÓN DE VULNERABILIDADES (IMAGEN TOMADA DE INTERNET[3]).

2.5. Registros de eventos.

Los ***logs*** son registros detallados de los eventos que ocurren en un sistema informático, una aplicación o un dispositivo [32]. Estos registros pueden incluir información como la fecha y hora, el tipo, la fuente y los detalles específicos de un evento. Los ***logs*** son útiles para los administradores de sistemas y los desarrolladores, ya que pueden utilizarse para solucionar problemas y resolver errores del sistema. También pueden utilizarse para realizar análisis de seguridad y detectar patrones y tendencias en el comportamiento del sistema. Los ***logs*** pueden generarse automáticamente por el sistema o crearse manualmente por un usuario. Algunos ejemplos de logs incluyen los registros de eventos del sistema operativo, los de errores de una aplicación y los de tráfico de red.

[3] Proceso de Gestión de Vulnerabilidades. Gigadefense. https://gigadefense.com.mx/gestion-de-vulnerabilidades/

2.5.1. Archivos de eventos.

Este es un tipo de archivo en el que se acumulan los registros de eventos (***logs***) que ocurren en un sistema. Se generan y se alojan en un directorio específico, de modo que resultan fáciles de encontrar para analizarlos; véase la ilustración 4.

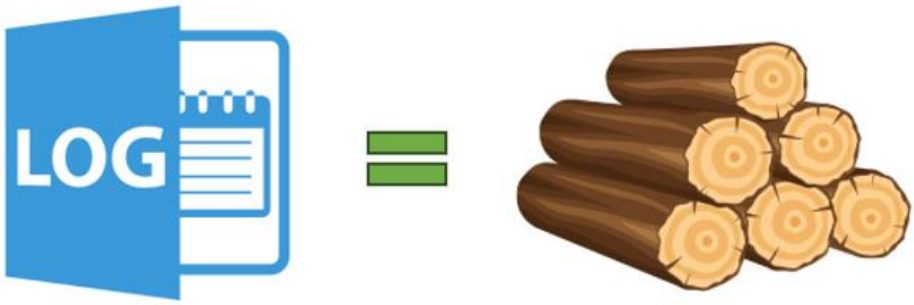


ILUSTRACIÓN 4. ARCHIVOS DE EVENTOS (PROPIA).

2.5.2. Registro de eventos.

Es un registro detallado de los eventos relacionados con el sistema, la seguridad y las aplicaciones almacenadas en un sistema operativo (ver Ilustración 5). Los registros de eventos se pueden utilizar para rastrear problemas del sistema y de algunas aplicaciones y para pronosticar problemas futuros.

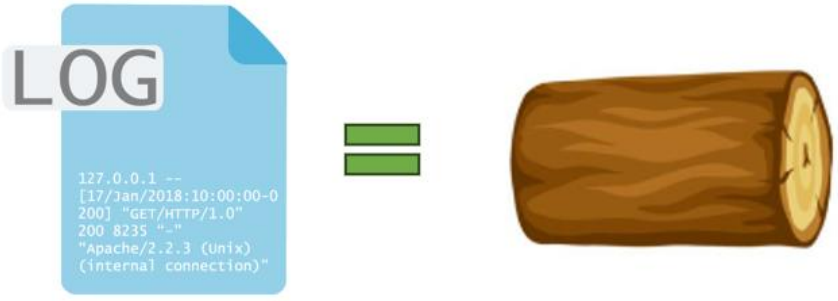


ILUSTRACIÓN 5. REGISTRO DE EVENTO (PROPIA).

2.5.3. Detalles de la información en un ***log***.

Estos proporcionan una descripción detallada de lo que ha estado haciendo un sistema, capturando una amplia gama de eventos, como inicios de sesión de usuarios, accesos a archivos, errores del sistema, conexiones de red y cambios en los datos o en la configuración

del sistema. Si bien los detalles específicos pueden variar según el tipo de registro, una entrada de registro suele incluir la información descrita en la Ilustración 6.

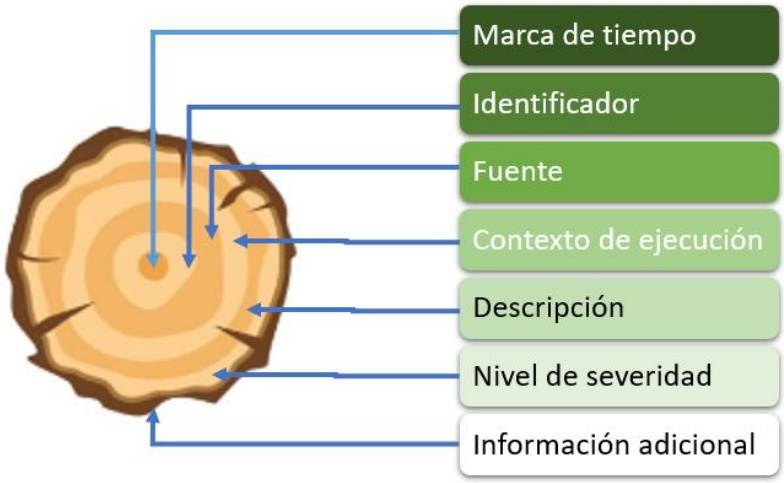


ILUSTRACIÓN 6. INFORMACIÓN CONTENIDA EN UN LOG (PROPIA).

2.5.4. Tipos de *logs.*

Los componentes de un entorno informático generan varios tipos de registros, cada uno con un propósito distinto. Estos tipos de registros incluyen, entre otros:

- **Registros de aplicaciones:** mensajes de aplicaciones específicas que proporcionan información sobre su estado, errores, advertencias y otros detalles operativos.
- **Registros de auditoría:** eventos, acciones y cambios que ocurren dentro de un sistema o aplicación, y que proporcionan un historial de las actividades del usuario y del comportamiento del sistema.
- **Registros de seguridad:** eventos relacionados con la seguridad, como inicios de sesión, modificaciones de permisos, actividades del firewall y otras acciones que afectan la seguridad del sistema.
- **Registros del servidor:** registros del sistema, de eventos, de errores y de acceso, cada uno de los cuales ofrece información distinta sobre las operaciones del servidor.
- **Registros del sistema:** actividades del kernel, errores del sistema, secuencias de inicio y estado del hardware, lo que ayuda a diagnosticar problemas del sistema.
- **Registros de red:** comunicación y actividad en una red, que capturan información sobre eventos, conexiones y transferencias de datos.

- **Registros de base de datos:** actividades dentro de un sistema de base de datos, como consultas, acciones y actualizaciones.
- **Registros del servidor web:** solicitudes procesadas por el servidor, incluidas la URL, las direcciones IP de origen, los tipos de solicitud, los códigos de respuesta y más.

Cada tipo de registro ofrece una única perspectiva de las actividades en un entorno, y analizar estos registros en su contexto entre sí es fundamental para la investigación de seguridad cibernética y la detección efectiva de amenazas.

2.5.5. Herramientas de gestión de ***logs.***

Existen diversas herramientas de gestión de logs que pueden ser utilizadas para recolectar, almacenar, procesar y analizar logs de diferentes sistemas y aplicaciones [33], véase la Ilustración 7.

ILUSTRACIÓN 7. HERRAMIENTAS DE GESTIÓN DE LOGS (IMAGEN TOMADA DE INTERNET[4]).

[4] https://blog.hackmetrix.com/centralizador-de-logs-para-cumplimiento/

Algunas de las herramientas más comunes son:

- Elasticsearch [34]: Es una herramienta de búsqueda y análisis distribuido que puede utilizarse para recolectar y almacenar logs. Permite realizar búsquedas en tiempo real, crear visualizaciones y generar alertas a partir de los logs recolectados (véase el Anexo 7).
- Logstash [35]: Es una herramienta de procesamiento de logs que puede utilizarse para recolectar, transformar y enviar logs a distintos destinos, como Elasticsearch. Logstash cuenta con una amplia gama de plugins que permiten procesar logs de distintas fuentes y formatos.
- Kibana [36]: Es una herramienta de visualización de datos que permite crear visualizaciones y dashboards a partir de los logs almacenados en Elasticsearch. Kibana permite crear gráficos, tablas y mapas interactivos para analizar los datos de los logs.
- Fluentd [37]: Es una herramienta de recolección y procesamiento de logs que puede utilizarse para enviarlos a distintos destinos, como Elasticsearch. Fluentd cuenta con una amplia gama de plugins que permiten procesar logs de distintas fuentes y formatos.
- Graylog [38]: Es una herramienta de gestión de logs que permite recolectar, almacenar, procesar y analizar dichos logs. Graylog permite realizar búsquedas en tiempo real, crear alertas y generar informes a partir de los logs recolectados.
- Splunk [39]: Es una herramienta de gestión de ***logs*** y análisis de datos que permite recolectar, almacenar y analizar logs de distintos sistemas y aplicaciones. Splunk cuenta con una amplia gama de funciones y características avanzadas para el análisis de datos.
- Nxlog [40]: La plataforma NXLog es una solución local para la gestión centralizada de registros, con un procesamiento versátil que constituye la columna vertebral de la supervisión de la seguridad. Tiene experiencia como líder en el sector en la recopilación de registros y la gestión de agentes, abordando de forma integral las tareas relacionadas con los registros de seguridad, entre las que se incluyen: recopilación, análisis sintáctico, procesamiento, enriquecimiento, almacenamiento, gestión, análisis. Su compatibilidad con los principales sistemas operativos, arquitecturas de hardware y formatos de registro, incluidas las integraciones con las principales herramientas empresariales y los principales sistemas SIEM.

Estas son solo algunas de las herramientas de gestión de logs disponibles en el mercado. La elección de la herramienta adecuada dependerá de las necesidades específicas de la **UACJ** en cuanto a la recolección, el almacenamiento, el procesamiento y el análisis de los logs (ver Anexos 4, 5 y 6).

2.5.6. Técnicas de análisis de ***logs.***

Las diferentes técnicas de análisis de ***logs*** son métodos o prácticas que se utilizan con regularidad para interpretar y extraer información de los ***logs***. Estas técnicas pueden ir desde las más simples hasta las más complejas y son vitales para identificar patrones, anomalías y conocimientos. A continuación, se muestran algunas técnicas comunes:

- **Reconocimiento de patrones:** identificar secuencias o tendencias recurrentes en los ***logs***. Este puede descubrir el comportamiento habitual del sistema o identificar acciones poco comunes que podrían representar una amenaza para la seguridad.
- **Detección de anomalías:** se centra en identificar puntos en los datos que se desvían del patrón esperado. Es primordial detectar posibles dificultades o actividades maliciosas desde su origen.
- **Análisis de correlación:** la correlación entre las diferentes entradas de ***logs*** ayuda a comprender la relación entre múltiples eventos. Puede mostrar causalidad y dependencias entre los elementos del sistema y es trascendental en el análisis de la causa raíz.
- **Análisis de línea de tiempo:** el análisis de ***logs*** a lo largo del tiempo auxilia a comprender tendencias, estacionalidades y comportamientos periódicos. Puede ser esencial para monitorear el rendimiento y pronosticar las cargas del sistema.
- **Aprendizaje automático e inteligencia artificial:** aprovechar los modelos de aprendizaje automático existentes puede automatizar y mejorar algunas técnicas de análisis de ***logs***, como la clasificación y el enriquecimiento de datos. La IA puede proveer información predictiva y contribuir a automatizar las respuestas ante eventos específicos.
- **Visualización:** la representación de los datos de ***logs*** mediante gráficos y tablas permite una comprensión intuitiva y genera conocimientos rápidamente. La visualización hace que los datos complejos obtenidos sean más accesibles y ayuden a identificar patrones y relaciones clave entre eventos ocurridos.

- **Análisis estadístico:** el uso de métodos estadísticos en el análisis de datos de ***logs*** proporciona información cuantitativa y ayuda a tomar decisiones basadas en evidencia. El uso del análisis de regresión y de las pruebas de hipótesis permite inferir relaciones y validar suposiciones.

Las técnicas mencionadas anteriormente pueden aplicarse de forma individual o en combinación, según los requisitos específicos y la complejidad de la tarea de análisis de registros. Comprender y utilizar estas técnicas puede mejorar significativamente la eficacia del análisis de *logs*, lo que se traduce en decisiones más informadas y en la toma de medidas de seguridad sólidas y eficientes.

2.5.7. Líneas de tiempo**.**

El uso de líneas de tiempo en el análisis de *logs* es fundamental por varias razones, especialmente en el contexto de la seguridad informática, la administración de sistemas, y el análisis de rendimiento de aplicaciones y redes. Este enfoque aporta claridad y perspectiva al complejo flujo de datos generados por sistemas y aplicaciones, facilitando la identificación de patrones, anomalías y eventos críticos. Los siguientes son algunos puntos clave sobre la importancia de utilizar líneas de tiempo en este contexto:

- **Comprensión de la secuencia de eventos:** Permite a los analistas y administradores de sistemas visualizar la secuencia exacta en que ocurren los eventos, lo cual es crucial para entender la causalidad en incidentes de seguridad, fallos de sistemas y problemas de rendimiento.
- **Detección de anomalías y patrones:** Al observar los eventos en una línea de tiempo, es más fácil identificar patrones de comportamiento, tanto legítimos como maliciosos, y anomalías que podrían indicar problemas o ataques en curso, como el acceso a recursos en horarios inusuales o una cantidad inusualmente alta de solicitudes a un servidor.
- **Análisis forense y de seguridad:** En el caso de un incidente de seguridad, las líneas de tiempo permiten a los investigadores seguir el rastro de los atacantes a través de los sistemas, identificando cómo se obtuvo el acceso, qué vulnerabilidades se explotaron y qué datos se vieron comprometidos.
- **Correlación de eventos entre diferentes fuentes de datos:** Los logs de distintos sistemas y aplicaciones pueden correlacionarse en una única línea de tiempo para

ofrecer una visión integral de la actividad a lo largo de toda la infraestructura, lo que permite comprender cómo los eventos en un sistema pueden afectar a otros.

- **Optimización del rendimiento y la disponibilidad:** Al analizar las líneas de tiempo de los logs, los administradores pueden identificar tendencias que indican cuellos de botella de rendimiento o patrones que preceden a fallos del sistema, lo que les permite tomar acciones correctivas antes de que los problemas se vuelvan críticos.
- **Mejora de la capacidad de respuesta:** Frente a incidentes, las líneas de tiempo facilitan una respuesta más rápida y efectiva, ya que ayudan a identificar cuándo comenzó un problema y cómo ha evolucionado, lo que permite focalizar los esfuerzos de resolución donde más se necesitan.
- **Cumplimiento y auditoría:** Las líneas de tiempo también juegan un papel importante en la demostración del cumplimiento de normativas y en los procesos de auditoría, al proporcionar un registro claro y ordenado de la actividad del sistema, accesos a datos sensibles, y cambios en la configuración.

El uso de líneas de tiempo en el análisis de logs transforma un conjunto de datos, a menudo voluminoso y complejo, en una narrativa coherente y comprensible, facilitando la identificación rápida de problemas, la comprensión de la secuencia de eventos y la toma de decisiones basada en evidencia.

Las marcas de tiempo en los registros de eventos tienen gran importancia, especialmente cuando provienen de múltiples fuentes con distintas zonas horarias. El principal desafío es mantener la consistencia de las marcas de tiempo para el análisis preciso de registros y la correlación entre diferentes fuentes. Una solución que automatiza la detección de la zona horaria y la conversión de marcas de tiempo a un formato UNIX estándar es una gran herramienta que simplifica la visualización y el análisis de datos al convertirlos a la zona horaria local del usuario, eliminando la necesidad de ajustes manuales y permitiendo un análisis y reportes más eficientes.

Las súper líneas de tiempo son herramientas de análisis forense digital que ofrecen una visión completa de los eventos en diversos sistemas y aplicaciones, lo que facilita la investigación de incidentes de seguridad que involucran múltiples elementos. Integran datos de varias fuentes de registro para revelar correlaciones y patrones, lo cual sería complejo y laborioso de realizar manualmente. Existen herramientas que facilitan este proceso al automatizar la creación de líneas de tiempo unificadas a partir de múltiples fuentes de registro.

2.6. Análisis inteligente de amenazas.

El análisis inteligente de amenazas ***CTI*** (o Cyber Threat Intelligence en inglés) es el proceso de recopilar, analizar y utilizar información sobre posibles amenazas a la seguridad de una organización. Esta información se obtiene de una variedad de fuentes, incluidas ***feeds*** públicos (datos estructurados), grupos de inteligencia de amenazas, redes de sensores y herramientas de monitoreo de seguridad [41].

El objetivo del análisis inteligente de amenazas es proporcionar una comprensión profunda de las amenazas a la seguridad y ayudar a las organizaciones a tomar medidas proactivas para prevenirlas. Esto implica el uso de técnicas de análisis avanzadas, como el análisis de ***malware*** (programas malignos), de vulnerabilidades, de redes y de comportamiento.

Al utilizar el análisis inteligente de amenazas, las organizaciones pueden identificar y prevenir ataques cibernéticos antes de que ocurran, lo que contribuye a mejorar la seguridad y a proteger los datos críticos. Además, el análisis inteligente de amenazas puede ayudar a las organizaciones a cumplir con las regulaciones de seguridad y a mantener una postura de seguridad sólida y proactiva.

2.6.1. Ciclo de inteligencia sobre amenazas.

El "Ciclo de inteligencia sobre amenazas" es un proceso organizado y continuo que las organizaciones y agencias de seguridad cibernética utilizan para recopilar, analizar y comprender las amenazas en el ámbito digital. Está diseñado para ayudar a identificar y anticipar posibles ataques cibernéticos, lo que permite a las organizaciones tomar medidas proactivas para protegerse (ver ilustración 8). El ciclo consta de varias etapas clave, que son las siguientes:

- **Análisis de amenazas**: En esta etapa inicial, se identifican y definen las amenazas cibernéticas potenciales. Esto implica el seguimiento de tendencias en el ciberespacio, el monitoreo de foros y comunidades de hackers, y la revisión de incidentes anteriores para comprender los métodos y tácticas utilizados por los atacantes.
- **Recopilación**: Una vez identificadas las amenazas potenciales, se recopila la información relevante. Esto implica la recolección de datos de diversas fuentes, como

registros de red, registros de eventos de seguridad, inteligencia abierta y cerrada, y cualquier otra fuente que pueda proporcionar información sobre las amenazas.

- **Procesamiento**: En esta etapa, los datos recopilados se organizan, filtran y preparan para su análisis. Esto puede incluir la normalización de datos, la eliminación de información redundante y la preparación de los datos para su análisis posterior.
- **Análisis y producción**: Aquí se llevan a cabo la evaluación y el análisis de la información recopilada. Los analistas de amenazas cibernéticas examinan los datos procesados para identificar patrones, tendencias y posibles indicadores de amenazas. También se generan informes y reglas de detección a partir de este análisis para informar a las partes interesadas (**stakeholders**) sobre las amenazas identificadas.
- **Validación**: Antes de difundir información sobre las amenazas, es esencial verificarla. Esto implica verificar la precisión y la confiabilidad de los datos y de los análisis realizados. La validación ayuda a garantizar que las decisiones se basen en información precisa.
- **Difusión**: Una vez validada la información y generados los informes y alertas, se difunde a las partes interesadas relevantes. Esto puede incluir equipos de seguridad cibernética, tomadores de decisiones, otros organismos gubernamentales y socios del sector privado. La difusión oportuna es fundamental para tomar medidas rápidas.
- **Proyección**: consiste en prever cómo las amenazas cibernéticas podrían evolucionar en el futuro. Los analistas de inteligencia de amenazas evalúan cómo podrían cambiar las tácticas y técnicas de los atacantes y proporcionan recomendaciones para prepararse ante amenazas futuras.

ILUSTRACIÓN 8. CICLO DE INTELIGENCIA DE AMENAZAS (PROPIA)

Este ciclo de inteligencia sobre amenazas es fundamental para fortalecer la ciberseguridad y la resiliencia de las organizaciones, permitiéndoles estar mejor preparadas para enfrentar y mitigar las amenazas cibernéticas en un entorno en constante evolución [42].

2.6.2. Proveedores de inteligencia sobre amenazas.

Los proveedores de inteligencia sobre amenazas (TIP, por sus siglas en inglés) son empresas u organizaciones que recopilan, analizan y comparten información sobre amenazas a la seguridad cibernética. Su objetivo es proporcionar a sus clientes información oportuna y precisa sobre amenazas emergentes, vulnerabilidades de seguridad, *malware* y otros tipos de ciberataques.

Estos proveedores suelen utilizar una variedad de técnicas para recopilar información, como el análisis de registros de eventos, el monitoreo de redes y el análisis de amenazas en tiempo real. La información que recopilan se utiliza para desarrollar inteligencia de amenazas, que luego se comparte con los clientes en formatos como informes, alertas y actualizaciones de seguridad.

Los clientes de los proveedores de inteligencia sobre amenazas suelen ser empresas y organizaciones que buscan fortalecer su postura de seguridad cibernética y proteger sus activos y datos. Al recibir información actualizada y precisa sobre amenazas, los clientes pueden tomar medidas proactivas para mitigar los riesgos de seguridad cibernética y fortalecer sus defensas. Algunos de los principales proveedores son:

- IBM X-Force Exchange
- FireEye
- Recorded Future

2.6.3. Intercambio de inteligencia de amenazas.

El intercambio de inteligencia sobre amenazas (***CTI***, por sus siglas en inglés) se refiere al intercambio de información y conocimientos relacionados con la ciberseguridad y las amenazas en línea [6]. En términos simples, es el proceso de compartir información sobre amenazas cibernéticas entre organizaciones, empresas y entidades gubernamentales para mejorar la capacidad de todas las partes para prevenir, detectar y responder a dichas amenazas. El ***CTI*** puede incluir información sobre vulnerabilidades de seguridad, ataques

cibernéticos recientes, herramientas y técnicas utilizadas por los ciberdelincuentes, así como cualquier otra información relevante sobre amenazas; véase la Ilustración 9.

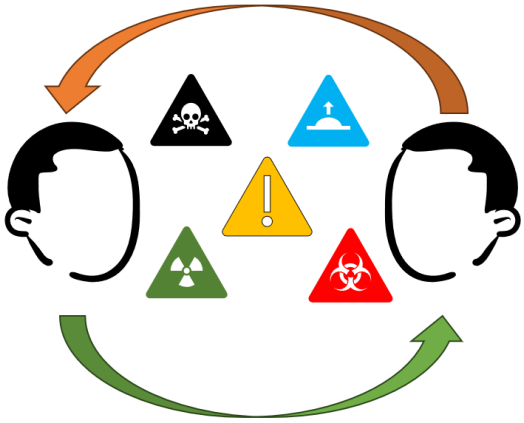


ILUSTRACIÓN 9. INTERCAMBIO DE INTELIGENCIA SOBRE AMENAZAS (PROPIA).

El intercambio de información de ***TI*** es una práctica importante en la industria de la ciberseguridad, ya que permite a las organizaciones estar mejor preparadas para proteger sus sistemas y datos contra posibles ataques y minimizar el riesgo de brechas de seguridad. Además, el intercambio de información de ***TI*** puede mejorar la capacidad de los organismos encargados de hacer cumplir la ley para combatir el cibercrimen y capturar a los delincuentes cibernéticos.

2.6.4. Marco de referencia MITRE ATT&CK.

MITRE ATT&CK[43] es una base de conocimiento globalmente accesible sobre tácticas y técnicas adversarias basadas en observaciones del mundo real. La base de conocimientos de ATT&CK se utiliza como base para el desarrollo de modelos y metodologías de amenazas específicas en los sectores privado público, y gobierno y en la comunidad de productos y servicios de ciberseguridad.

Con la creación de ATT&CK, MITRE está cumpliendo su misión de resolver problemas para un mundo más seguro, uniendo a las comunidades para desarrollar una ciberseguridad más eficaz. ATT&CK está abierto y disponible para que cualquier persona u organización lo utilice sin costo alguno. Así, ha creado proyectos e investigaciones para la organización sin fines de lucro MITRE Corporation, con sede en EE. UU., específicamente para la comunidad de ciberseguridad:

- Marco ATT & CK ® (Tácticas adversarias, técnicas y conocimiento común)
- Base de conocimiento de CAR (Repositorio de análisis cibernético)
- ENGAGE (Enfrentamiento con adversarios)
- D3FEND (Marco de detección, denegación y disrupción que potencia la defensa de la red)
- AEP (Planes de emulación de ATT &C)

ATT&CK se utiliza para comprender cómo los atacantes comprometen sistemas y redes, lo que permite a las organizaciones identificar brechas de seguridad, evaluar amenazas y mejorar sus defensas. Diferentes procedimientos para aplicar el marco de referencia (en inglés, *framework*) han sido estudiados con buenos resultados, pero en esencia se resumen a los siguientes pasos:

- **Mapeo de incidentes**: relacionar las técnicas empleadas en un ataque con las tácticas de la matriz ATT&CK.

- **Evaluación de seguridad**: Comparar la capacidad de defensa actual con las técnicas documentadas para identificar debilidades.

- **Red Teaming**: simular ataques para evaluar la efectividad de las defensas.

- **Respuesta a incidentes**: Facilitar la investigación mediante la categorización de las técnicas de ataque observadas.

Es cierto que el *framework* (Ilustración 10) es de gran utilidad para mejorar la ciberseguridad, comprender los patrones de ataque y fortalecer las defensas de cualquier organización.

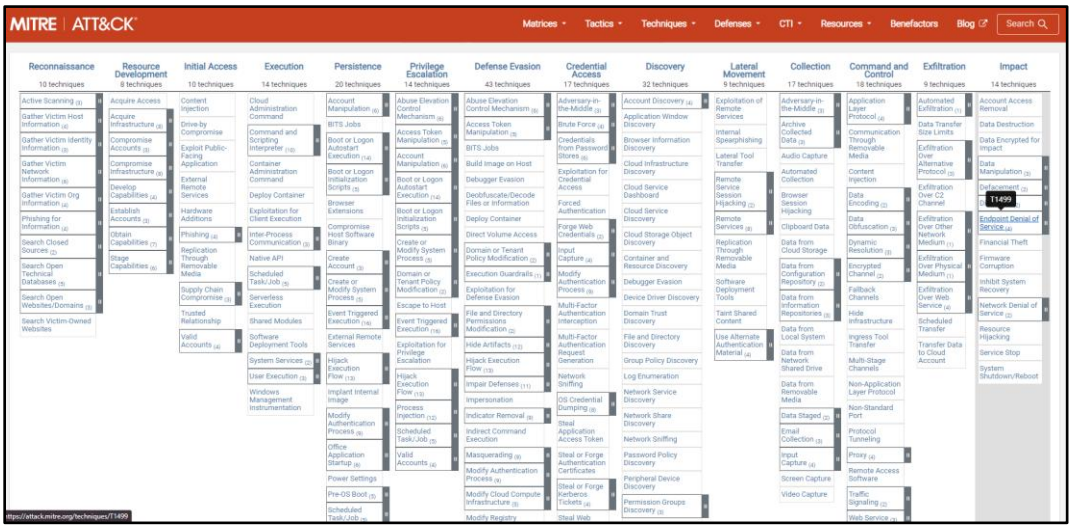


ILUSTRACIÓN 10. IMAGEN DEL MARCO ATT&CK DE MITRE [43].

2.6.5. Mitre CAR.

La definición oficial de CAR es: "El Repositorio de Análisis Cibernético de MITRE (CAR) es una base de conocimiento de análisis basada en el modelo de adversario MITRE ATT&CK®. CAR define un modelo de datos que se aprovecha en sus representaciones de pseudocódigo, pero también incluye implementaciones dirigidas directamente a herramientas específicas (por ejemplo, Splunk, EQL) en sus análisis. Con respecto a la cobertura, CAR se enfoca en proporcionar un conjunto de análisis validados y bien explicados, en particular, en su teoría operativa y fundamento [44]".

2.6.6. Mitre Engage.

Engage es un *framework* para operaciones de enfrentamiento con el adversario que permite a los responsables de ciberseguridad de una organización enfrentarse a sus adversarios y alcanzar sus objetivos de seguridad informática [45].

2.6.7. Mitre Defend.

MITRE DEFEND es un *framework* centrado en las contramedidas y las defensas cibernéticas. Es una extensión del marco ATT&CK, pero mientras ATT&CK documenta las tácticas, técnicas y procedimientos (TTPs) que los atacantes utilizan para comprometer sistemas, DEFEND se centra en las acciones que los defensores pueden tomar para protegerse de estas amenazas [46].

MITRE DEFEND ayuda a las organizaciones a estructurar, planificar y ejecutar defensas más efectivas al documentar contramedidas específicas aplicables en cada etapa de un ataque. Se utiliza como una guía para mejorar la detección, prevención, respuesta y recuperación frente a ciberataques, alineando las defensas con las técnicas de ataque ya conocidas (ver ilustración 11). Es un complemento ideal para aplicar una defensa estratégica, aun cuando se cuenta con un equipo de trabajo reducido.

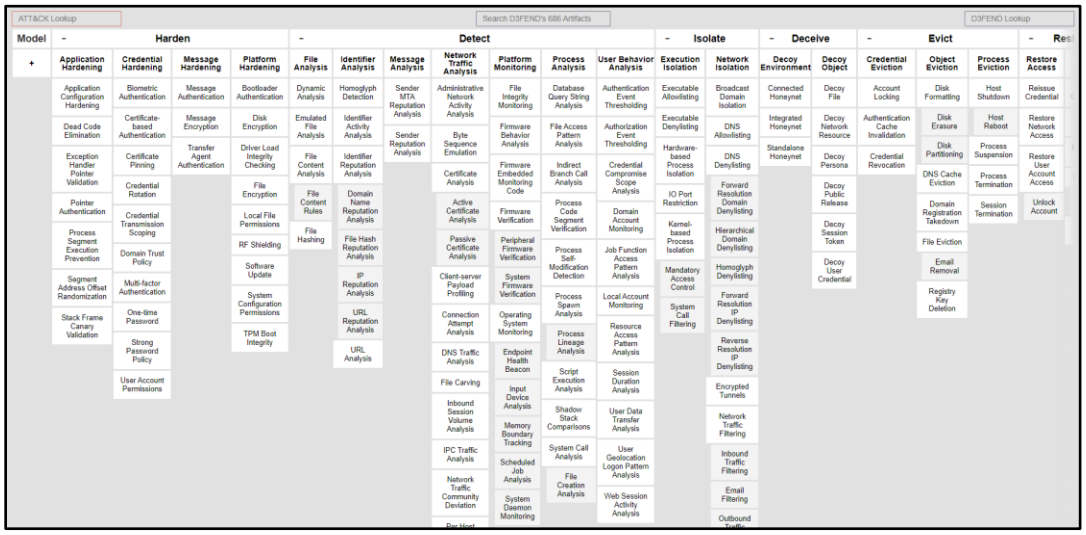


ILUSTRACIÓN 11. MATRIZ DEFEND DE MITRE [46]

2.6.8. Mitre AEP.

MITRE AEP (*Adversary Emulation Plans*) es otra excelente herramienta desarrollada por MITRE. ***AEP*** es una parte de las iniciativas de MITRE para mejorar las defensas cibernéticas, y está relacionada con la matriz ATT&CK [47]. El objetivo principal de los planes de emulación de adversarios (***AEP***) es ayudar a las organizaciones a evaluar sus defensas frente a ataques cibernéticos realistas basados en las tácticas y técnicas observadas en actores de amenaza conocidos. Los ***AEP*** proporcionan guías detalladas y secuencias de pasos que simulan el comportamiento de estos atacantes en entornos de prueba o de simulación controlados. Esto permite a los equipos de ciberseguridad mejorar sus capacidades de detección, respuesta y mitigación. Algunas características clave de MITRE AEP incluyen:

1. Simulación de ataques reales: Los planes se basan en datos de inteligencia sobre amenazas reales y están diseñados para replicar el comportamiento de los adversarios más avanzados.

2. Evaluación de la postura de seguridad: Mediante la emulación de ataques, las organizaciones pueden identificar puntos débiles en sus defensas y fortalecer sus controles de seguridad.
3. Entrenamiento y preparación: AEP puede utilizarse para entrenar a los equipos de respuesta ante incidentes y de seguridad en la detección y la reacción ante ataques sofisticados.
4. Personalización: Aunque los AEP se basan en amenazas conocidas, pueden adaptarse a las necesidades específicas de una organización para probar ciertos vectores de ataque o tecnologías concretas.

MITRE AEP es una herramienta clave para mejorar la ciberseguridad proactiva, enfocada en la emulación de actores maliciosos para identificar vulnerabilidades antes de que ocurran ataques.

2.6.9. Amenaza persistente avanzada ***APT***.

APT es el acrónimo de *Advanced Persistent Threat*. Se conceptualiza como un equipo/grupo (*grupo de amenazas*) o incluso un país (*grupo de estados-nación*) que realiza ataques planeados, constantes y a largo plazo contra organizaciones o países. La palabra "avanzado", no se refiere necesariamente a que estén utilizando tecnología de punta o herramientas totalmente desconocidas, es decir, un *exploit*[5] de día cero, que utilizan comúnmente. Como veremos un poco más adelante, las técnicas que utilizan estos grupos de APT son bastante comunes y pueden detectarse con las implementaciones adecuadas (ver la Ilustración 12).

[5] Un exploit es un programa, secuencia de comandos o fragmento de datos que se aprovecha de una vulnerabilidad o error para provocar un comportamiento no deseado en un dispositivo electrónico, hardware o software [96].

ILUSTRACIÓN 12. APT DE UN ADVERSARIO EN CONCEPTO (PROPIA -CREADA CON IA).

2.6.10. Cadena de ataque cibernético ***(Cyber Kill Chain)***.

El concepto de "cadena de ataque" tiene su origen en el ámbito militar y describe las etapas de un ataque: identificar el objetivo, decidir, atacarlo y, finalmente, destruirlo [48]. Lockheed Martin adaptó este concepto en 2011 al crear el marco "Cyber Kill Chain®" ***CKC***, aplicándolo a la ciberseguridad. Este marco detalla las fases que los atacantes deben seguir para llevar a cabo un ataque exitoso. Entender cómo funciona el ***CKC*** permite a las organizaciones protegerse de amenazas como el ransomware, las violaciones de seguridad y los ataques avanzados. También ayuda a los analistas y expertos en seguridad a identificar intrusiones y las intenciones de los atacantes, mejorando así la defensa y el análisis de la seguridad de los sistemas.

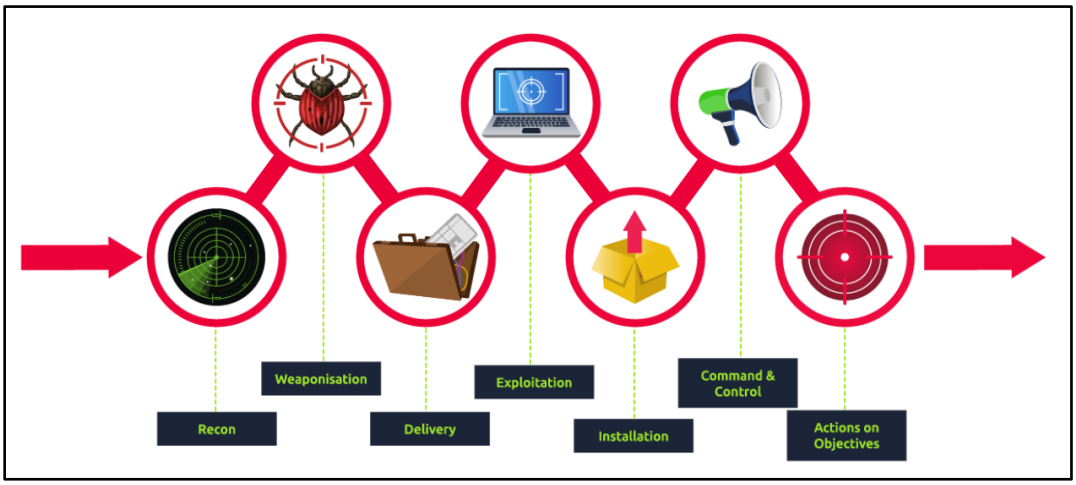


ILUSTRACIÓN 13. FASES DE LA CIBER KILL CHAIN [49].

En la Ilustración 13 se muestran siete fases de la ***CKC*** las cuales son:

- Reconocimiento
- Preparación de armas (**weaponization**)
- Entrega
- Explotación
- Instalación
- Comando y control
- Acciones sobre objetivos

Reconocimiento

Es la primera fase de un ataque cibernético, en la que los atacantes recopilan información sobre su objetivo como parte de su planificación. Esta fase incluye el uso de ***OSINT*** (Inteligencia de Fuentes Abiertas)[50], que consiste en obtener datos públicamente disponibles sobre una empresa o sus empleados, como correos electrónicos, números de teléfono y el tamaño de la empresa. Un atacante, mejor conocido como "**Adversario**", que ha estado planeando un ataque sofisticado, comienza esta fase utilizando herramientas de recolección de direcciones de correo electrónico para llevar a cabo ataques de phishing, como "theHarvester", "Hunter.io" y "***OSINT*** Framework". Además, los atacantes exploran redes sociales como LinkedIn, Facebook y Twitter para obtener información valiosa que facilite sus ataques [49].

Preparación de armas (**weaponization**)

Dentro de un ataque cibernético, en el que el "**Adversario**" se encarga de crear una "arma de destrucción". En lugar de interactuar directamente con la víctima, prefiere construir un "***weapon***", que combina ***malware*** y ***exploits*** en una carga útil (***payload)*** entregable. Los atacantes suelen automatizar la creación del *malware* o comprarlo en la Red Obscura (***DarkWeb)***. Los actores más sofisticados o patrocinados por naciones (**APT**) desarrollan *malware* personalizado para evadir la detección. En este caso, el "Adversario" opta por comprar un *payload* prescrito en la *DarkWeb* para centrarse en otras fases del ataque [49].

Entrega

La fase de entrega de un ataque cibernético es donde un "adversario", elige cómo transmitir un *payload* o *malware*. Se presentan varios métodos:

1. Ataque de ingeniería social: el atacante envía un correo electrónico malicioso dirigido a una persona específica o a varias personas dentro de una empresa, suplantando a alguien de confianza. Por ejemplo, podría enviar una "factura" falsa a una empleada haciéndose pasar por un colega.
2. Distribución de memorias USB infectadas: el atacante deja memorias USB maliciosas en lugares públicos o las envía a empresas, haciéndose pasar por un cliente que envía un regalo.
3. Ataque de abrevadero (**waterhole poisoning**): el atacante compromete un sitio web que sus víctimas frecuentan y las redirige a un sitio malicioso que instala *malware* al visitarlo.

Estos métodos buscan engañar a las víctimas para que instalen involuntariamente software malicioso [49].

Explotación

En esta fase, el "Adversario" utiliza técnicas de ingeniería social para obtener acceso a un sistema. Envía correos maliciosos: uno con un enlace a una página de inicio de sesión falsa, por ejemplo, de Office 365, y otro con un archivo adjunto que ejecuta ***ransomware***. Tras lograr que las víctimas caigan en la trampa, el atacante puede desplazarse lateralmente a través de la red y explotar vulnerabilidades para escalar privilegios y acceder a datos

confidenciales. También regularmente se apoya en el uso de "exploits de día cero", que son vulnerabilidades desconocidas en software o hardware difíciles de detectar inicialmente [49].

Instalación

La instalación de persistencia es un método que permite a un adversario eludir las medidas de seguridad y mantener acceso oculto a un sistema. Una vez que el atacante obtenga acceso, instalará una puerta trasera persistente para asegurar que pueda volver a entrar en el sistema en caso de que se pierda la conexión, se detecte su acceso o se complete la reparación del sistema. Existen varias técnicas que emplean los adversarios para mantener la persistencia en un sistema comprometido [49]. Estas incluyen:

1. Instalación de un shell web: Un script malicioso en lenguajes web como PHP o JSP que permite al atacante mantener acceso remoto al sistema, y que es difícil de detectar debido a su formato.
2. Instalación de puertas traseras: Uso de herramientas como Meterpreter (parte de Metasploit) para instalar software malicioso que permite acceso remoto y ejecución de comandos en la máquina de la víctima.
3. Modificación de servicios de Windows: Creación o modificación de servicios del sistema para ejecutar scripts maliciosos de forma regular, utilizando herramientas como `sc.exe` y `Reg`. Los atacantes pueden enmascarar sus acciones con nombres de servicio legítimos.
4. Agregar claves en el registro o en la carpeta de inicio: Esto asegura que la carga maliciosa se ejecute automáticamente cada vez que el usuario inicie sesión, utilizando ubicaciones específicas para la persistencia a nivel de usuario o del sistema completo, según MITRE ATT&CK.

Comando y Control (***C&C***)

Esta fase describe cómo los atacantes utilizan un canal de ***C&C*** para controlar de forma remota una máquina comprometida mediante *malware*, un proceso conocido como "*C2 Beaconing*". El host infectado se comunica continuamente con el servidor ***C&C*** para que el atacante tome el control completo del sistema. Anteriormente, los atacantes usaban IRC como canal ***C&C***, pero ahora prefieren protocolos más comunes, como HTTP/HTTPS (puertos 80 y 443) y DNS Tunneling, ya que estos se mezclan fácilmente con el tráfico legítimo, ayudando a evadir la detección por firewalls y soluciones de seguridad modernas [49].

Acciones sobre objetivos

Esta última fase describe las acciones que un adversario puede realizar una vez completadas las seis fases de su ataque [49]. Estas acciones incluyen:

1. Exfiltración de datos confidenciales.
2. Eliminación de copias de seguridad y copias instantáneas.
3. Sobrescribir o corromper datos para causar daños adicionales.
4. Cifrado de datos.

2.6.11. Seguridad de la Cadena de Suministro

En el análisis inteligente de amenazas, es vital reconocer que los riesgos no solo provienen de actores externos directos, sino también de la cadena de suministro tecnológica. Esta disciplina se encarga de gestionar las amenazas derivadas de proveedores de software, hardware y servicios administrados por terceros que utiliza la **UACJ** en su operación diaria [51].

Los ataques a la cadena de suministro ocurren cuando un adversario compromete a un proveedor legítimo para insertar código malicioso en actualizaciones de software o de hardware distribuidas. El **SOC-UACJ** debe implementar funciones de supervisión para validar la integridad de los activos adquiridos y monitorear el comportamiento de las herramientas externas integradas, evitando que una vulnerabilidad en un tercero se convierta en una puerta trasera hacia los datos sensibles de la comunidad universitaria.

2.7. Monitoreo de tráfico de red.

Un sistema de monitoreo de tráfico de red es una herramienta que permite supervisar y analizar el tráfico de una red de computadoras en tiempo real, con el objetivo de detectar y solucionar problemas de rendimiento, seguridad y disponibilidad [52]. Este sistema recopila datos sobre el tráfico de la red, como el volumen de datos, la velocidad de transferencia, el origen y el destino de los paquetes de datos, los protocolos utilizados, y los presenta de forma clara y organizada para su análisis por parte de los administradores de red (ver ilustración 14). Además, algunos sistemas de monitoreo de tráfico de red ofrecen funciones de alerta y notificación ante la detección de anomalías o problemas críticos en la red.

ILUSTRACIÓN 14. MONITOREO DE TRÁFICO DE RED (TOMADA DE INTERNET[6])

2.7.1. Sistema de monitoreo de tráfico de red.

El alcance de un sistema de monitoreo de tráfico de red puede variar según los objetivos y necesidades específicos de la organización que lo implementa. Para este caso de uso específico, el alcance del sistema de monitoreo de tráfico de red para la **DGTI** en la **UACJ** puede incluir:

- Supervisión del rendimiento: el sistema podría monitorear el uso de la red, la carga de tráfico, la latencia y otros indicadores de rendimiento para identificar cuellos de botella y optimizar el uso de los recursos de la red.
- Generación de alertas de seguridad: el sistema podría analizar el tráfico de la red para detectar actividades sospechosas, como intentos de intrusión, ataques de denegación de servicio (***DoS***), malware, spam y phishing.
- Análisis de tráfico: el sistema podría proporcionar informes detallados sobre el tráfico de la red, incluyendo los protocolos utilizados, los usuarios y dispositivos conectados, las aplicaciones y servicios utilizados, así como los patrones de tráfico.

En general, un sistema de monitoreo de tráfico de red es una herramienta valiosa para cualquier organización que desee garantizar la disponibilidad, la seguridad y el rendimiento de su red de computadoras. En la Subdirección de Operación y Redes de la **UACJ** ya se cuenta con una herramienta de código abierto para el monitoreo del tráfico de red.

[6] https://www.whatsupgold.com/es/blog/7-claves-de-considerar-antes-de-comprar-un-software-de-monitoreo-de-redes

2.7.2. Honeypot.

En el ámbito de la seguridad informática, un ***Honeypot*** (tarro de miel) cibernético funciona de manera muy similar a un señuelo, creando una trampa para los piratas informáticos malintencionados (ver Ilustración 15). Se trata de un sistema informático que se expone voluntariamente a riesgos de ciberataques, como si fuera un objetivo simulado. Al fingir ser vulnerable ante los piratas informáticos, aprovecha sus intentos de intrusión para obtener información sobre los ciberdelincuentes y su modus operandi y/o desviar su atención de actividades alternativas [53].

ILUSTRACIÓN 15. HONEYPOT (IMAGEN TOMADA DE INTERNET[7])

En [54] el autor describe la definición de ***Honeypot*** como: "un recurso de red destinado a ser atacado o comprometido". De esta forma, un ***Honeypot*** será examinado, atacado y, probablemente, comprometido por cualquier atacante. Los ***Honeypot*** no tienen, en ningún caso, la finalidad de resolver o corregir fallos de seguridad en nuestra red. Son los encargados de proporcionarnos información valiosa sobre los posibles atacantes en potencia a nuestra red antes de que comprometan sistemas reales."

En el capítulo cuarto de su libro, el autor muestra el inicio del uso de ***Honeypot*** como herramienta de inteligencia de amenazas en los años 90. Resalta la importancia de entender que los ***Honeypot*** no sirven para resolver los fallos de seguridad en los sistemas de información, sino para entender las nuevas técnicas que utilizan los atacantes.

[7] https://medium.com/@ecojumper30/creating-a-honeypot-f2b4cc33385a.

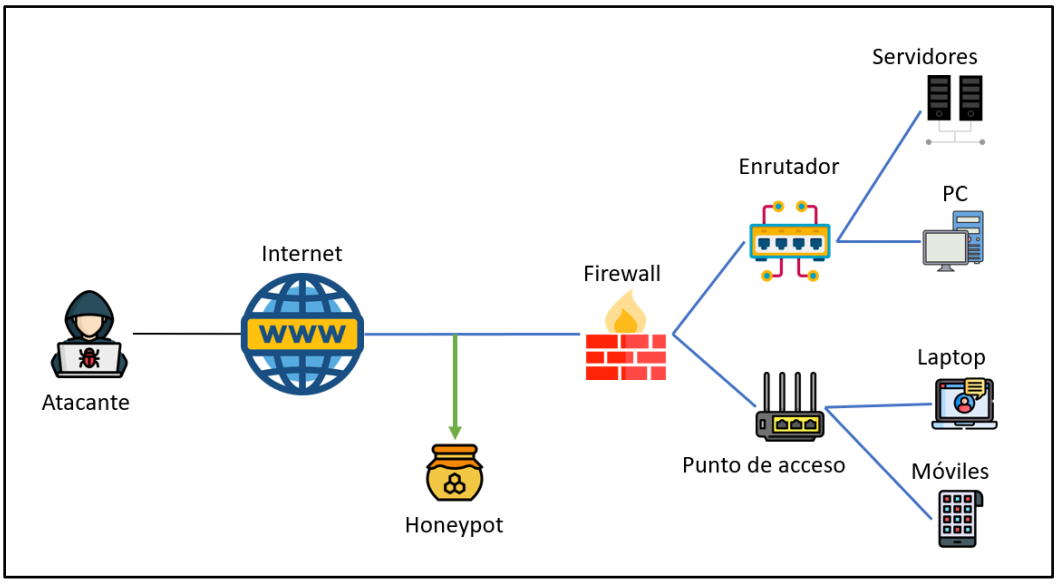


ILUSTRACIÓN 16. DISPOSICIÓN DE UN HONEYPOT SEGURO (PROPIA).

En la Ilustración 16 se puede visualizar la disposición de un ***Honeypot*** en una red de manera segura, también conocida como "Frente al cortafuegos". También existen las opciones de disposición "Detrás del cortafuegos" y "Zona desmilitarizada". Adicionalmente, se pueden combinar las disposiciones de varios ***Honeypot*** en distintos sitios de una red institucional. Por otra parte, existen las llamadas ***Honeynets,*** que son grupos de dispositivos dispuestos en una red local destinados a recopilar información sobre potenciales atacantes.

2.8. Centro de Operaciones de Ciberseguridad.

Un ***SOC*** es un centro de operaciones encargado de monitorear, analizar y responder ante las amenazas de seguridad en una organización. Según [55], un ***SOC*** se define como "un equipo de profesionales de seguridad de la información que utiliza tecnologías, procesos y políticas para proteger los sistemas y datos de una organización contra amenazas internas y externas"[56], [57]. Los miembros del equipo del ***SOC*** trabajan para detectar posibles amenazas de seguridad, investigarlas y responder oportunamente y de manera efectiva. Esto se logra mediante el uso de herramientas de monitoreo y análisis de seguridad, así como mediante el desarrollo de políticas y procedimientos eficaces [58].

El término ***SOC*** se popularizó en la década de 1990 con el aumento de la conciencia sobre la ciberseguridad y la necesidad de sistemas centralizados para monitorear y responder a las

amenazas de seguridad. Aunque no hay una fecha exacta ni un evento específico que marque la primera vez que se utilizó el término "Security Operation Center", su uso se remonta a esa época, cuando las organizaciones comenzaron a consolidar sus recursos de seguridad en un centro para supervisar, detectar, analizar y responder a las amenazas de seguridad de manera más eficaz.

Los ***SOC*** son cada vez más importantes [57], a medida que las organizaciones se vuelven más dependientes de la tecnología y las amenazas a la seguridad aumentan. También pueden ayudar a garantizar que una organización mantenga una postura de seguridad sólida y responda rápidamente a las amenazas de seguridad. Además, son esenciales para cumplir con los requisitos regulatorios de seguridad de la información y mantener la confianza de los clientes y socios comerciales.

Existen varias herramientas que se utilizan en un ***SOC*** como se aprecia en la Ilustración 17, pero aquí se mencionarán algunas de las principales:

- ***SIEM*** (Security Information and Event Management) [59]: Esta herramienta se utiliza para la gestión de eventos e información de seguridad en tiempo real. Permite la recolección, correlación y análisis de datos de diversas fuentes para detectar y responder a incidentes de seguridad.
- ***IDS***/***IPS*** (Intrusion Detection System/Intrusion Prevention System)[60]: Estas herramientas se utilizan para la detección y prevención de intrusiones en la red. Un ***IDS*** detecta las intrusiones y un ***IPS*** previene y bloquea los ataques.
- **Firewalls** [3]: Los firewalls se utilizan para proteger la red frente a amenazas externas. Permiten o bloquean el tráfico de red según reglas predefinidas.
- **Herramientas de análisis forense** [4]: Se utilizan para analizar sistemas comprometidos y determinar la causa de un incidente de seguridad. Ayudan a los equipos de respuesta a identificar y mitigar la amenaza.

ILUSTRACIÓN 17. COMPONENTES DE UN *SOC* (PROPIO).

2.8.1. Arquitectura de un SOC.

Generalmente, al planear un proyecto de software o de desarrollo tecnológico, se diseña una arquitectura; en este caso, se revisaron varias de ellas, como en el ejemplo de la Ilustración 18. Antes de poner en marcha un ***SOC,*** es importante considerar los elementos fundamentales para el diseño de la arquitectura a desarrollar, como son:

- **Monitoreo y detección**: Un ***SOC*** debe contar con herramientas y sistemas de monitoreo y detección de amenazas. Esto implica el uso de sensores de seguridad, firewalls, sistemas de prevención de intrusiones (***IPS***), sistemas de detección de intrusiones (***IDS***), sistemas de gestión de registros (***SIEM***), entre otros. Estas herramientas recopilan y analizan datos de seguridad en tiempo real para identificar patrones y anomalías que puedan indicar actividades maliciosas.
- **Análisis de seguridad**: Un equipo de analistas de seguridad es esencial en un ***SOC***. Estos profesionales son responsables de examinar y analizar las alertas e incidentes de seguridad detectados por las herramientas de monitoreo. Utilizan técnicas y metodologías avanzadas para investigar incidentes, determinar la naturaleza y el impacto de las amenazas, y tomar medidas adecuadas para mitigar los riesgos.

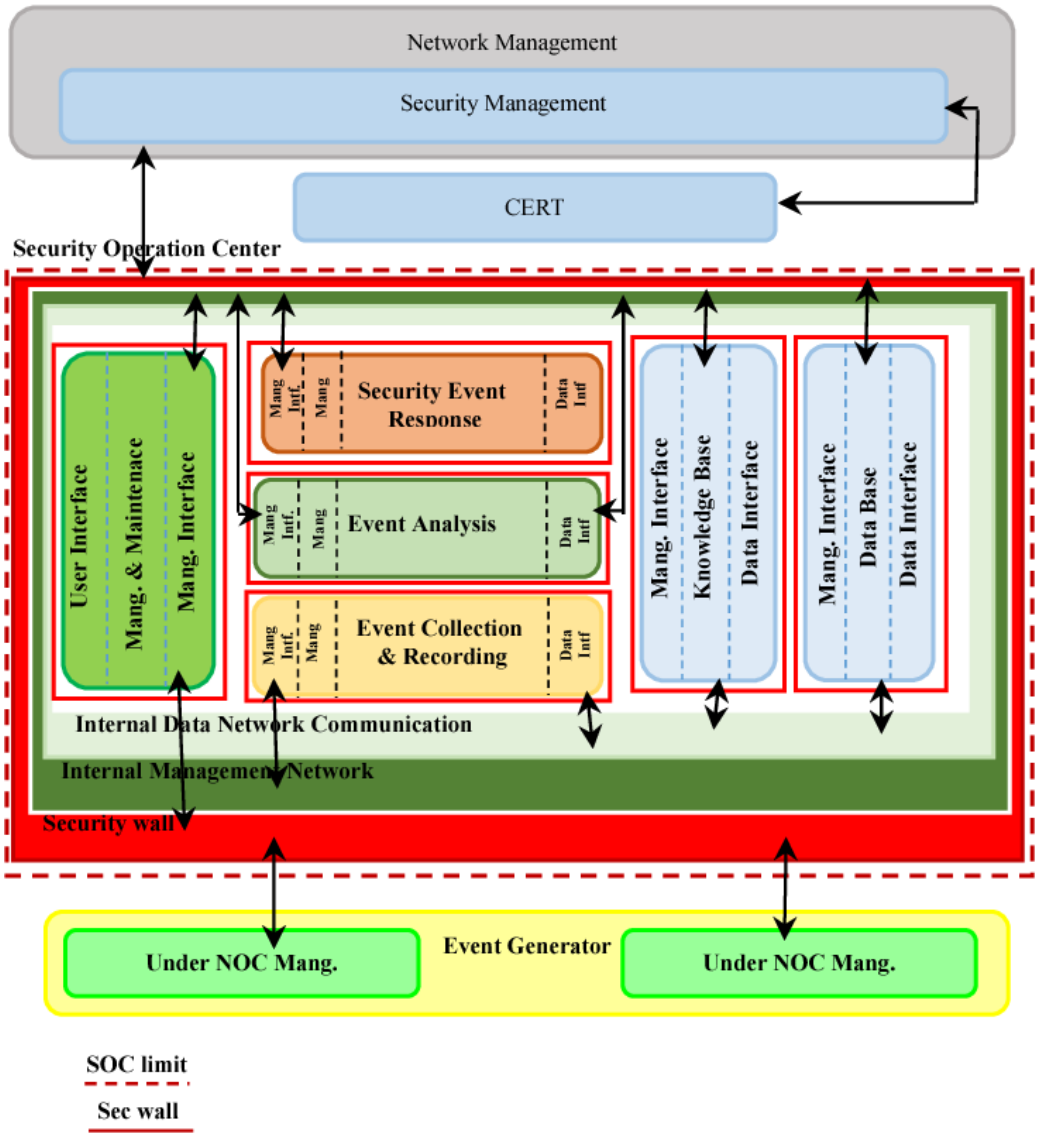


ILUSTRACIÓN 18. REFERENCIA DE ARQUITECTURA DE UN SOC [61].

- **Respuesta a incidentes**: Un ***SOC*** debe contar con procedimientos y políticas establecidos para responder de manera eficiente a incidentes de seguridad. Esto incluye la capacidad de realizar acciones correctivas, como bloquear direcciones **IP** sospechosas, deshabilitar cuentas de usuario comprometidas o realizar análisis forenses en sistemas afectados. Además, es importante contar con protocolos de comunicación claros y establecidos tanto con otros equipos de la organización como con socios externos.
- **Gestión de la información de seguridad**: La gestión de la información de seguridad implica el almacenamiento seguro y el análisis de los datos recopilados mediante las

herramientas de monitorización. Esto puede incluir la implementación de bases de datos de registros de seguridad, sistemas de almacenamiento en la nube o infraestructuras de *big data* para la correlación y el análisis a gran escala de eventos de seguridad.

- **Infraestructura de red segura**: Es fundamental contar con una red segura para un ***SOC***. Esto implica segmentar y aislar adecuadamente los sistemas críticos de seguridad, así como implementar firewalls, la encriptación, la autenticación y otras medidas de protección para prevenir y mitigar posibles ataques.
- **Capacidades de visualización**: Un ***SOC*** debe proporcionar herramientas de visualización que permitan a los analistas y al personal de seguridad comprender rápidamente la situación y la evolución de las amenazas. Estas herramientas pueden incluir paneles de control en tiempo real, mapas de calor, gráficos y otras representaciones visuales de los datos de seguridad.

Dentro de la arquitectura moderna de un ***SOC***, se integra la capacidad de Orquestación, Automatización y Respuesta de Seguridad (***SOAR***). El ***SOAR*** es un conjunto de tecnologías que permiten a la organización recopilar datos de seguridad y alertas de diferentes fuentes (como Wazuh o Elastic Stack) y automatizar las respuestas ante incidentes mediante flujos de trabajo predefinidos denominados playbooks.

A diferencia del **SIEM**, que se enfoca en la correlación de eventos, el **SOAR** orquesta la comunicación entre distintas herramientas de seguridad para ejecutar acciones correctivas rápidas —como bloquear una dirección IP sospechosa en el firewall de Sophos— sin necesidad de intervención manual inmediata. Esta integración es crucial para reducir el tiempo medio de respuesta (MTTR) y combatir la fatiga de alertas en el reducido equipo técnico de la **UACJ**.

2.8.2. Roles del personal de un ***SOC***.

El personal que trabaja en un ***SOC*** desempeña distintos roles para garantizar la protección efectiva de los activos de información y de la infraestructura de la organización. A continuación, se describen algunos de los roles comunes en un ***SOC***:

- **Analista de seguridad:** Los analistas de seguridad son responsables de monitorear los sistemas de seguridad de la organización para detectar posibles amenazas o actividades sospechosas. Analizan los registros y los eventos

generados por los dispositivos de seguridad para identificar incidentes de seguridad y determinar su gravedad. También pueden participar en investigaciones forenses y en el desarrollo de estrategias de mitigación.

- **Analista de incidentes de seguridad:** Los analistas de incidentes de seguridad se encargan de investigar y responder a los incidentes que ocurren en la organización. Evalúan la naturaleza del incidente, determinan su alcance y aplican las contramedidas adecuadas para contenerlo y minimizar su impacto. También documentan los incidentes y elaboran informes posteriores para el análisis y la mejora continua.
- **Ingeniero de seguridad:** Los ingenieros de seguridad son responsables de diseñar, implementar y mantener las soluciones de seguridad del ***SOC***. Esto incluye la configuración y administración de firewalls, sistemas de detección de intrusiones, sistemas de prevención de intrusiones, sistemas de gestión de registros, y otras herramientas y tecnologías relacionadas. También pueden participar en la evaluación de riesgos y en el desarrollo de políticas y procedimientos de seguridad.
- **Gerente de operaciones de seguridad:** supervisa el SOC en su ***conjunto***. Coordina las actividades del equipo, establece políticas y procedimientos, asigna recursos y garantiza la eficiencia y eficacia de las operaciones de seguridad. También puede interactuar con otros departamentos y niveles de la organización para proporcionar informes y recomendaciones sobre la postura de seguridad.
- **Analista de inteligencia de amenazas:** Los analistas de inteligencia de amenazas se encargan de monitorear el panorama de amenazas cibernéticas para obtener información sobre las tácticas, técnicas y procedimientos empleados por los atacantes. Recopilan datos de diversas fuentes, analizan la información y proporcionan alertas tempranas sobre nuevas amenazas. Esto ayuda a la organización a anticiparse a los ataques e implementar medidas de detección y respuesta de incidentes.

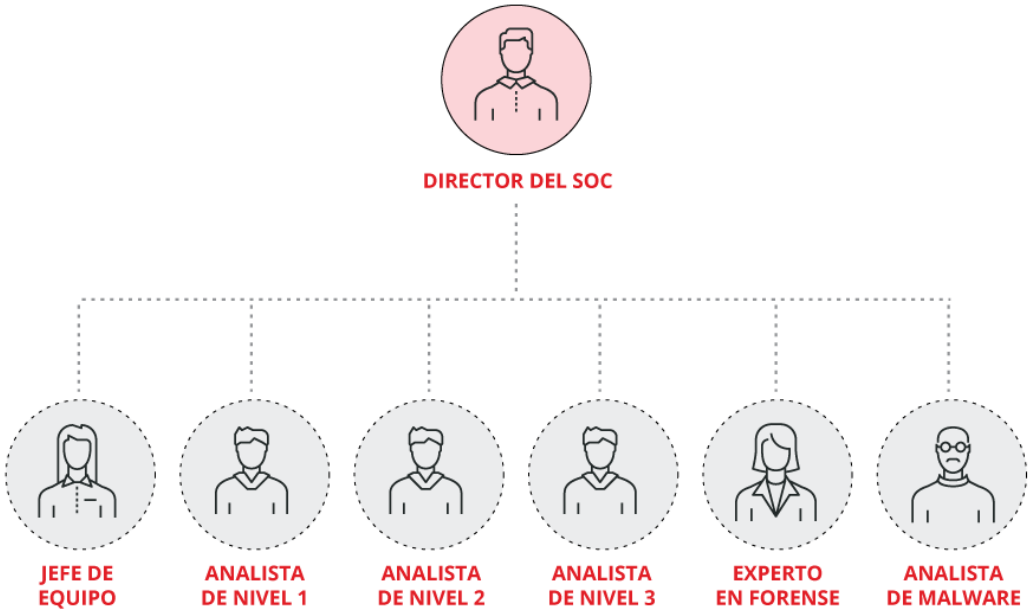


ILUSTRACIÓN 19. EJEMPLO DEL PERSONAL REQUERIDO EN UN SOC[8].

Según el **INCIBE,** en la Ilustración 19 se muestra un ejemplo del personal requerido en un ***SOC*** con la siguiente descripción:

- **Director**: intermediario entre la ***SOC*** y la empresa que sufre un incidente. Será el encargado de reportar la información y la inteligencia generadas por los distintos equipos que puedan coexistir en el centro. El director se encargará de comunicar los avances y de mantener reuniones con la empresa víctima del incidente para mediar en las posibles necesidades que esta pueda tener.
- **Jefe de equipo**: persona que gestionará el equipo o los equipos multidisciplinares en el centro. Es posible que, dadas las dimensiones o la especialización de los equipos, haya un jefe por equipo.
- **Analistas de nivel 1**: la función de los analistas a este nivel será el triaje y la monitorización de incidencias.
- **Analistas de nivel 2**: en este segundo nivel, los analistas realizarán investigaciones básicas, presentarán posibles soluciones para resolver las incidencias y

[8] https://www.incibe.es/incibe-cert/blog/respondiendo-incidentes-industriales-soc-ot.

proporcionarán recomendaciones para realizar cambios en los sistemas, con el fin de contener posibles propagaciones en caso deinfección por *malware*.

- **Analistas de nivel 3**: a este nivel trabajarán los perfiles más especializados, entre ellos especialistas forenses o ingenieros de detección. Su objetivo será realizar tareas muy concretas, como la reversión de *malware*, investigaciones forenses avanzadas y el modelado de amenazas, entre otras.

Estos son solo algunos de los roles comunes en un Centro de Operaciones de Seguridad. Dependiendo del tamaño y de las necesidades específicas de la organización, pueden existir otros roles, como especialistas en respuesta a incidentes, administradores de sistemas de seguridad, analistas de vulnerabilidades y administradores de redes. En general, el personal de un ***SOC*** trabaja en estrecha colaboración para garantizar la seguridad de la organización y responder de manera efectiva a las amenazas cibernéticas.

2.9. Arquitectura de Confianza Cero (Zero Trust)

La Arquitectura de Confianza Cero (**ZTA**, por sus siglas en inglés) representa un cambio de paradigma en la seguridad de las redes, alejándose del modelo tradicional de "perímetro defendido". Bajo el axioma fundamental de "nunca confiar, siempre verificar", la **ZTA** asume que las amenazas pueden originarse tanto fuera como dentro de los límites de la red institucional de la **UACJ**.

Este modelo complementa la arquitectura del **SOC-UACJ** al exigir que cada solicitud de acceso sea autenticada, autorizada y validada de forma continua antes de conceder el acceso. En un entorno de cómputo en la nube, la **ZTA** utiliza el monitoreo del ***SOC*** para aplicar políticas dinámicas basadas en el contexto del usuario y el estado del dispositivo, minimizando así el alcance de la exposición ante un posible compromiso de credenciales. Esta información es tomada de [20].

2.10. Continuidad del Negocio (BCP) y Recuperación ante Desastres (DRP)

La resiliencia operativa de un SOC se define como su capacidad para mantener sus funciones críticas de detección y respuesta ante fallos en su infraestructura o desastres naturales. El Plan de Continuidad del Negocio (***BCP***) se enfoca en mantener la operatividad de la universidad durante una crisis, mientras que el Plan de Recuperación ante Desastres (***DRP***) detalla los procedimientos técnicos para restaurar los sistemas de **TI** y la consola del ***SOC*** tras un evento disruptivo.

Para el **SOC-UACJ**, la resiliencia se garantiza mediante la redundancia de los servicios en la nube y la alta disponibilidad de sus componentes centrales, como el servidor Dell R650. Un ***SOC*** resiliente debe contar con respaldos fuera de sitio de los registros de eventos (***logs***) y una infraestructura capaz de conmutar por error (***failover***) para asegurar que la visibilidad sobre la RedUACJ nunca se pierda, cumpliendo así con los pilares de integridad y disponibilidad de la tríada ***CID***. Con una visión hacia el cumplimiento normativo se desarrolló un ***DRP*** siguiendo [62]

3. Desarrollo del proyecto.

3.1. Metodología.

Existen diferentes técnicas de desarrollo y modelado, así como metodologías, para realizar investigación y desarrollo de prototipos tecnológicos orientados a sistemas de ***IT*** (en inglés, Information Technology). Cuando se desarrolla software, se utiliza principalmente un modelo de prototipado o de desarrollo evolutivo para ofrecer al usuario una visión previa de cómo será el programa o el sistema. El modelo de prototipo es evolutivo porque se desarrolla hasta convertirse en el producto final. Para un ***SOC,*** se requiere considerar diferentes metodologías: no solo el software, sino también la interacción con sistemas de información y con elementos físicos. Tomando en cuenta todo ello, se seguirá la siguiente metodología:

- **Investigar:** Realizar una investigación sobre las metodologías de desarrollo de prototipos existentes, tanto en el ámbito general como en el específico del software. Investigar las nuevas tecnologías relacionadas con la seguridad informática y la ciberseguridad para diseñar un sistema que, de manera integral, sirva como base de desarrollo del ***SOC***.
- **Definir los requisitos:** Identificar y documentar los requisitos clave para el desarrollo del prototipo en el contexto específico de ***SOC***. Considerar factores como las capacidades técnicas, los recursos disponibles y las restricciones del proyecto.
- **Diseñar el proceso:** Crear un marco de trabajo para el proceso de desarrollo del prototipo. Definir los pasos específicos, las actividades y las tareas a realizar en cada etapa del proceso.
- **Selección de herramientas y tecnologías:** Identificar las herramientas y tecnologías adecuadas que respalden la metodología de desarrollo del prototipo. Estas pueden incluir entornos de desarrollo integrados (***IDE***), lenguajes de programación, marcos de referencia y bibliotecas específicas, entre otros.
- **Desarrollar un modelo de ciclo de vida:** definirlo para el desarrollo del prototipo a lo largo de las iteraciones necesarias de la metodología. Esto puede incluir etapas como la definición de requisitos, el diseño del prototipo, la implementación, la prueba y la retroalimentación. La importancia de realizar iteraciones radica en que, durante el desarrollo del prototipo, se podrán hacer ajustes al sistema de puntos no considerados o no contemplados en iteraciones anteriores.

- **Establecer métricas de evaluación:** Definir métricas claras y objetivas para medir la efectividad del prototipo. Estas métricas estarán relacionadas con el rendimiento, la usabilidad, la satisfacción del usuario u otros aspectos relevantes. Para la etapa de evaluación se utilizarán las bases de la metodología propuesta por los autores del documento [63].
- **Realizar pruebas y refinamientos:** llevar a cabo pruebas exhaustivas del prototipo y recopilar comentarios y sugerencias de los usuarios y otras partes interesadas (director, codirector, lectores, revisores y personal de ***IT***). Utilizar esta retroalimentación para mejorar continuamente el prototipo y ajustar la metodología según sea necesario.
- **Documentar y difundir:** Documentar todos los aspectos clave de la metodología de desarrollo del prototipo, incluidos los pasos, las pautas, las herramientas y las mejores prácticas. Compartir esta documentación con el cuerpo de evaluación, con profesionales y otras personas involucradas en el proceso de desarrollo del prototipo.
- **Iterar y mejorar:** Mantener un enfoque iterativo en la metodología de desarrollo del prototipo. Realizar revisiones periódicas y de mejora continua, según los resultados y comentarios obtenidos durante el proceso de desarrollo.

3.2. Investigación.

Para establecer una base sólida para el diseño e implementación del Centro de Operaciones de Seguridad (**SOC**) de la Universidad Autónoma de Ciudad Juárez, se realizó una investigación detallada sobre metodologías de desarrollo de prototipos y tecnologías emergentes en el ámbito de la seguridad informática y la ciberseguridad.

En primer lugar, se revisaron diversas metodologías para el desarrollo de prototipos en entornos de tecnologías de la información. Entre las metodologías analizadas destacan:

- **Modelo de Prototipo Evolutivo**: permite una aproximación iterativa al desarrollo, en la que el sistema mejora progresivamente a partir de la retroalimentación del usuario. Este modelo fue seleccionado como base para el desarrollo del **SOC-UACJ,** ya que facilita la adaptación continua a los requerimientos institucionales y permite una validación temprana de funcionalidades clave [64].

- **Desarrollo incremental**: modelo centrado en la entrega de versiones funcionales parciales que se integran de forma sucesiva. Se tomó como referencia complementaria en las fases críticas del desarrollo del sistema [65].

- **Metodologías ágiles (Scrum y Kanban)**: aunque no fueron adoptadas formalmente, sus principios de iteración rápida y revisión continua influyeron en la organización del proyecto y en la definición de entregables parciales [66].

Posteriormente, se exploró el panorama tecnológico actual en ciberseguridad, con énfasis en soluciones de código abierto para la detección, el análisis y la respuesta a incidentes de seguridad. Como parte de esta revisión, se identificaron y evaluaron las siguientes herramientas:

- **Wazuh**: plataforma de código abierto para la gestión de eventos e información de seguridad (SIEM), la detección de intrusos, el análisis de vulnerabilidades y la respuesta activa. Se eligió la tecnología central del SOC-UACJ por su integralidad, bajo costo, capacidad de personalización y soporte comunitario [67].

- **Elastic Stack (ELK)**: conjunto de herramientas para la recopilación, el almacenamiento y la visualización de logs. Se consideró por su potencial de integración con Wazuh [34].

- **MITRE ATT&CK Framework**: base de conocimiento para la clasificación de tácticas y técnicas adversarias. Se empleó como referencia para definir escenarios de ataque y evaluar la cobertura del SOC [43].

- **OpenVAS, Zeek y Suricata**: herramientas adicionales analizadas para funciones complementarias, como el escaneo de vulnerabilidades y el monitoreo de red [68].

Además, se revisaron publicaciones científicas recientes, tesis universitarias previas, normativas internacionales como NIST SP 800-53 e ISO/IEC 27001, y estudios de caso sobre implementaciones reales de SOC en entornos universitarios [6], [69]. Esta base documental permitió contextualizar el proyecto en las mejores prácticas de la industria y asegurar su alineación con los estándares vigentes.

Como resultado de esta investigación, se establecieron los fundamentos teóricos y tecnológicos para construir un prototipo funcional del **SOC-UACJ**, capaz de evolucionar hacia una solución integral acorde con las necesidades de la institución.

3.3. Ingeniería de requisitos

La ingeniería de requisitos es un proceso fundamental en el desarrollo de proyectos de ciberseguridad, como la implementación de un ***SOC*** en una universidad. Un enfoque general de cómo aplicar la ingeniería de requisitos a este proyecto está de acuerdo con los siguientes pasos:

1. **Identificación de las partes interesadas**: Se identificaron todas las partes interesadas y usuarios que se verán beneficiados por el ***SOC***, los cuales son:

- Beneficiarios: la comunidad universitaria en general, incluidos los alumnos, el personal docente, administrativo y operativo.
- Interesados: Rectoría, Abogado General, Contraloría General, Dirección General de Tecnologías de Información y Dirección de Servicios Administrativos.

2. **Análisis de la situación actual**: Se realizó una encuesta al personal de la **DGTI**, que es quien, directa o indirectamente, se ha responsabilizado de la seguridad informática en la UACJ. También se realizó una estimación de riesgos utilizando la metodología NIST 800-30.

3. **Definición de objetivos y alcance**: Los objetivos, el alcance y las limitaciones se han definido en el punto 1.4.2 de este documento.

4. **Requerimientos funcionales**: Las funciones que debe llevar a cabo el **SOC**, como la monitorización en tiempo real, el análisis de amenazas, la gestión de incidentes y la generación de informes, son esenciales para la operación de un **SOC**. Para efectos del presente proyecto, se realizará la recopilación y el análisis en tiempo real de los ***logs***.

5. **Requerimientos no funcionales**: Los requerimientos no funcionales, como la disponibilidad, la escalabilidad, el rendimiento, la seguridad y el cumplimiento de normativas como la ISO 27001. El manejo de registros de eventos (logs) implica el

tratamiento de datos que pueden vincularse a individuos específicos (direcciones IP de origen, nombres de usuario, patrones de navegación). Por ello, se establece como requerimiento no funcional la implementación de la Privacidad por Diseño, [70]. Esto se traduce en acciones técnicas dentro del ***SOC***, tales como:

- **Minimización de datos:** Recopilar únicamente los campos necesarios para la detección de amenazas.
- **Cifrado y control de acceso:** Asegurar que los logs almacenados en el ***SIEM*** sean accesibles únicamente al personal autorizado del ***SOC*** mediante una autenticación robusta.
- **Anonimización de visualizaciones:** Configurar los dashboards del ***SIEM*** para ocultar datos sensibles en los reportes de nivel gerencial y garantizar la confidencialidad de la comunidad universitaria.

6. **Casos de uso**: El principal caso de uso será la detección de amenazas en los registros de eventos, que brindarán información para realizar acciones como la detección de un ataque, la respuesta a un incidente y la generación de informes de seguridad.

7. **Requerimientos de seguridad**: Los requerimientos de seguridad específicos, como el cifrado de datos, la autenticación de usuarios, la gestión de identidades y accesos, y la protección contra intrusiones en el sistema.

8. **Integración con sistemas existentes**: Se analizará cómo integrar el **SOC** con los sistemas de **TI** de la universidad, como firewalls, sistemas de detección de intrusiones y herramientas de gestión de activos en operación.

9. **Validación y verificación de requisitos**: Para validar el procedimiento, los requisitos deben ser claros, coherentes y verificables. Se realizarán revisiones y pruebas para confirmar el cumplimiento a lo largo de la vida del proyecto.

10. **Gestión de cambios**: Se establecerá un proceso para gestionar los cambios de requisitos a lo largo del proyecto. Los cambios deben evaluarse y documentarse adecuadamente.

11. **Documentación**: Se deberá mantener la documentación completa y actualizada de todos los requisitos, cambios y decisiones tomadas durante el proceso de desarrollo del proyecto.

12. **Comunicación**: Se comunicará regularmente el estado de los requisitos a las partes interesadas y se asegurará de que estén informadas sobre el progreso del proyecto.

La ingeniería de requisitos es esencial para garantizar que el Centro de Operaciones de Seguridad cumpla con las necesidades de la **UACJ** y proporcione una defensa efectiva frente a las amenazas cibernéticas. A lo largo del proyecto, es importante mantener una colaboración estrecha con las partes interesadas y adaptar los requisitos según sea necesario para abordar las amenazas y tecnologías cambiantes en el campo de la ciberseguridad.

3.3.1. Análisis de riesgos.

El análisis de riesgos en el ámbito de la ciberseguridad es un procedimiento sistemático concebido para detectar, evaluar y gestionar los riesgos relacionados con la seguridad de la información y los sistemas informáticos de una organización. Este procedimiento resulta esencial para comprender las amenazas a las que una entidad está expuesta y establecer las medidas más eficaces para mitigarlas.

Según el Instituto Nacional de Estándares y Tecnología (NIST) es un proceso fundamental para identificar, evaluar y priorizar los riesgos asociados con la seguridad de la información en una organización. El NIST proporciona un marco y directrices detallados para realizar este análisis, especialmente mediante la publicación NIST SP 800-30, "Guide for Conducting Risk Assessments". Los puntos clave del análisis de riesgos según el NIST:

1. Identificación de Activos

Descripción: Identificar los activos críticos de la organización, como datos, sistemas de información e infraestructura.

Objetivo: Determinar qué activos deben protegerse y cuál es su valor para la organización.

2. Identificación de Amenazas

Descripción: Identificar las posibles amenazas que podrían explotar vulnerabilidades en los activos. Las amenazas pueden ser internas o externas y abarcan desde ataques cibernéticos hasta desastres naturales.

Ejemplos: Hackers, *malware*, fallas de hardware, empleados descontentos.

3. Identificación de Vulnerabilidades

Descripción: Identificar las debilidades o fallas en los sistemas de seguridad que podrían ser explotadas por amenazas.

Métodos: Revisiones de seguridad, pruebas de penetración, análisis de código.

4. Evaluación de Impacto

Descripción: Evaluar las posibles consecuencias o impactos que tendría la explotación de una vulnerabilidad sobre los activos.

Categorías de Impacto: Confidencialidad, integridad y disponibilidad de los datos.

5. Evaluación de la Probabilidad

Descripción: Estimar la probabilidad de que una amenaza explote una vulnerabilidad específica. Esto se puede hacer de manera cualitativa o cuantitativa.

Factores: Historial de incidentes, sofisticación de las amenazas, exposición del activo.

6. Determinación del Riesgo

Descripción: Combinar la información sobre el impacto y la probabilidad para determinar el nivel de riesgo. El riesgo puede clasificarse en alto, medio o bajo.

Objetivo: Priorizar los riesgos para gestionarlos eficazmente.

7. Desarrollo de Estrategias de Mitigación

Descripción: Identificar y proponer medidas para reducir o mitigar los riesgos identificados.

Opciones de Mitigación: Implementación de controles de seguridad, transferencia del riesgo (por ejemplo, seguros), aceptación del riesgo o evitar el riesgo (por ejemplo, eliminando la actividad que genera el riesgo).

8. Monitoreo y Revisión Continua

Descripción: El análisis de riesgos es un proceso continuo. Se debe monitorear y revisar regularmente para adaptarse a cambios en el entorno, a nuevas amenazas o a cambios en los activos.

Herramientas: Auditorías regulares, sistemas de detección de intrusos, actualizaciones de políticas de seguridad.

El NIST enfatiza que un análisis de riesgos bien realizado es esencial para una gestión eficaz de la seguridad de la información. Permite a las organizaciones tomar decisiones informadas sobre la implementación de controles de seguridad y la asignación de recursos para proteger sus activos más críticos [6]. Además, ayuda a cumplir con las regulaciones y los estándares de seguridad.

El marco de NIST es altamente flexible y puede adaptarse a organizaciones de distintos tamaños y sectores, proporcionando una metodología estructurada para abordar de manera proactiva los desafíos de ciberseguridad. Para este proyecto se realizó un análisis de riesgos inicial; posteriormente, se efectuaron iteraciones para conocer el dominio, los activos, los actores y los propietarios responsables de los activos de la universidad.

Integración de Riesgos de Terceros y Cadena de Suministro

Para complementar la metodología NIST SP 800-30 utilizada para identificar riesgos en activos internos, la matriz de riesgos del **SOC-UACJ** debe incorporar la dimensión de la Cadena de Suministro de Ciberseguridad (***SCRM***). Dado que la universidad depende de proveedores de software, de servicios en la nube y de mantenimiento de hardware, cualquier vulnerabilidad en dichos terceros constituye un vector de ataque indirecto contra la RedUACJ.

Como se define en [51], se deben priorizar riesgos como la "dependencia tecnológica de terceros no auditados" y el "compromiso de las credenciales de soporte externo". Este enfoque permite que el **SOC** no solo monitoree su infraestructura, sino que también establezca alertas tempranas ante brechas de seguridad reportadas en los ecosistemas de sus socios tecnológicos.

3.4. Operación de SOC.

El diseño de un proceso operativo en un ***SOC*** es esencial para garantizar la eficacia y la eficiencia en la detección, la respuesta y la mitigación de amenazas cibernéticas. En la Ilustración 20 se muestra un esquema de los procesos que generalmente se llevan a cabo en un ***SOC***. Mismo esquema que sirve de base para visualizar la naturaleza de dichos procesos.

ILUSTRACIÓN 20. PROCESOS DENTRO DEL SOC (TOMADA DE INTERNET[9]).

A continuación, se describen los elementos clave de un proceso de operación en él:

1. Monitoreo Continuo:

- Implementación de herramientas de monitoreo de seguridad para supervisar de forma continua la red y los sistemas, en busca de actividades sospechosas.
- Configuración de alertas y umbrales para identificar anomalías y posibles amenazas.

[9] https://blog.elhacker.net/2021/03/que-es-como-funciona-centro-de-operaciones-de-seguridad-soc.html

2. Detección de Amenazas:

- Utilización de sistemas de detección de intrusiones (IDS), de prevención de intrusiones (IPS) y otras soluciones de seguridad para identificar posibles amenazas.
- Implementación de análisis de comportamiento para detectar patrones inusuales en el tráfico de red y en las actividades de los usuarios.

3. Registro y Recopilación de Datos:

- Establecimiento de registros de seguridad (logs) para capturar eventos relevantes.
- Agregación y correlación de datos de múltiples fuentes para obtener una visión completa de la seguridad de la red.

4. Análisis de Alertas:

- Asignación de alertas a analistas de seguridad para su investigación y evaluación de la gravedad de la amenaza.
- Uso de herramientas de análisis forense para comprender el alcance y la naturaleza de los alertas.

5. Respuesta a Incidentes:

- Desarrollo de planes de respuesta a incidentes para abordar distintos escenarios.
- Coordinación de acciones para contener, erradicar y recuperarse de un incidente de seguridad.

6. Comunicación y Colaboración:

- Establecimiento de canales de comunicación efectivos para coordinar respuestas con otros equipos de seguridad y partes interesadas.
- Colaboración con equipos internos y externos para compartir información sobre amenazas y vulnerabilidades.

7. Mejora Continua:

- Revisión regular de los incidentes y de la efectividad de los procedimientos de respuesta (lecciones aprendidas).

- Actualización constante de políticas y procedimientos en función de las lecciones aprendidas y la evolución de las amenazas.
- Hablara de

8. Capacitación y Desarrollo:

- Proporcionar capacitación continua a los analistas de seguridad para mantenerse actualizados sobre las amenazas y técnicas más recientes.
- Desarrollar planes de desarrollo profesional para mejorar las habilidades y conocimientos del equipo.

9. Gestión de Identidades y Accesos:

- Implementación de políticas de gestión de identidades y de acceso para garantizar que solo los usuarios autorizados accedan a los recursos críticos.
- Monitoreo de las actividades de los usuarios para detectar comportamientos anómalos.

10. Auditoría y Cumplimiento:

- Realización de auditorías periódicas para evaluar el cumplimiento de las políticas de seguridad.
- Mantenimiento de registros de auditoría para demostrar la conformidad y facilitar investigaciones futuras.

El diseño de un proceso de operación en el ***SOC*** debe adaptarse a la naturaleza y la complejidad específicas de la infraestructura de la UACJ y evolucionar continuamente para hacer frente a las amenazas cambiantes. A sabiendas de que dicha infraestructura es tremendamente heterogénea y de gran escala en cuanto a la cantidad de dispositivos de ***IT,*** propiedad de la UACJ y de la Comunidad Universitaria, que se encuentran dentro de la RedUACJ.

3.5. Software central para el SOC - UACJ.

Wazuh se destaca como la opción preferible para un centro de operaciones de ciberseguridad frente a otras soluciones de pago, gracias a su enfoque integral, flexibilidad y eficacia en la detección y respuesta a amenazas. En primer lugar, Wazuh ofrece una suite completa de funcionalidades que incluye la detección de intrusiones, la gestión de logs y el análisis de vulnerabilidades, todo ello integrado en una única plataforma. Esto elimina la necesidad de invertir en múltiples herramientas y simplifica la administración del entorno de seguridad (ver el Anexo 10).

Además de su amplio conjunto de características, el código abierto de Wazuh proporciona a las organizaciones un nivel significativo de flexibilidad y control. Las empresas pueden adaptar y personalizar la plataforma según sus necesidades específicas, lo que permite una implementación más ajustada a sus requisitos y estructuras internas. A diferencia de las soluciones de pago que a menudo imponen restricciones y costos adicionales por funcionalidades personalizadas, Wazuh permite a las organizaciones diseñar un sistema de seguridad cibernética a medida.

La capacidad de correlación de eventos en tiempo real y la respuesta automática a amenazas son aspectos cruciales de la ciberseguridad moderna, y Wazuh brilla en estas áreas. Con su capacidad para analizar patrones de comportamiento y correlacionar eventos de seguridad, Wazuh mejora significativamente la capacidad de respuesta ante incidentes. La automatización de respuestas a amenazas comunes agiliza la gestión de incidentes, reduce el tiempo de respuesta y minimiza el impacto de posibles ataques.

En términos de costo, la opción de código abierto de Wazuh implica que las organizaciones no incurren en gastos de licencia significativos, lo que la convierte en una alternativa económicamente atractiva frente a las soluciones propietarias. La comunidad activa de usuarios y desarrolladores de Wazuh también ofrece un valioso recurso de soporte, lo que contribuye a la resolución rápida de problemas y a la mejora continua de la plataforma. En pocas palabras, la preferencia por Wazuh en un centro de operaciones de ciberseguridad se basa en su enfoque integral, su flexibilidad, su eficacia en la detección y la respuesta, así como en su modelo de código abierto, que brinda a las organizaciones una solución personalizable y rentable.

Evolución hacia un modelo Zero Trust mediante el monitoreo de identidades.

La arquitectura central basada en **Wazuh** proporciona los cimientos necesarios para avanzar hacia un modelo de Confianza Cero (Zero Trust Architecture - **ZTA**) [71]. Mientras que las defensas tradicionales confían en el tráfico interno, un enfoque **ZTA** asume que la red está comprometida y requiere verificación continua.

El **SOC-UACJ** utiliza el agente **Wazuh** para monitorear los inicios de sesión y la telemetría de los puntos finales en tiempo real. Al integrar estos logs con el motor de correlación de **ELK**, el sistema puede identificar comportamientos anómalos de los usuarios (**UEBA**) que indiquen un uso no autorizado de identidades. Esta visibilidad es el componente esencial del "monitoreo continuo" para validar la postura de seguridad de cada dispositivo y usuario antes de conceder acceso a los activos críticos de la universidad.

3.5.1. Wazuh.

Wazuh es una solución de software gratuita, de código abierto y lista para empresas que requieren diagnóstico de amenazas, análisis de integridad, respuesta a incidentes y cumplimiento de acuerdos y políticas de seguridad. Wazuh se utiliza para recopilar, agrupar, indexar y monitorear datos de seguridad, lo que ayuda a las organizaciones a detectar intrusiones, amenazas y anomalías de comportamiento en sus sistemas de información. Como sistema de detección de intrusiones basado en host (***HIDS***, por sus siglas en inglés), esta herramienta permite monitorear registros, verificar la integridad de archivos, analizar políticas, detectar rootkits y responder activamente mediante métodos basados en firmas y anomalías.

A medida que las amenazas cibernéticas actuales se vuelven más sofisticadas, se requieren análisis en tiempo real y monitoreo de seguridad para detectarlas y remediarlas rápidamente. Por lo tanto, su agente proporciona las capacidades de análisis y respuesta necesarias, mientras que su componente de servidor aporta inteligencia de seguridad y realiza análisis de datos. Se diferencia de OSSEC en su capacidad de integrarse con ELK, su conjunto de reglas renovado y su capacidad de utilizar APIs restful. Wazuh también puede emplearse para analizar archivos en contenedores Docker, centrándose en los volúmenes persistentes y los montajes de enlace. Wazuh ayuda a detectar procesos de exploits ocultos que son más complejos que un simple patrón de firma y que pueden usarse para eludir los sistemas antivirus tradicionales. Además, el agente Wazuh proporciona capacidades de respuesta

activa que pueden utilizarse para bloquear un ataque de red, detener un proceso malicioso o poner en cuarentena un archivo infectado con *malware*.

3.5.2. Wazuh EDR.

Wazuh implementa la detección y respuesta de puntos finales (EDR por sus siglas en inglés), Estas son una serie de herramientas y aplicaciones que monitorean los dispositivos conectados al servidor Wazuh en busca de una actividad que podría indicar una amenaza o violación de seguridad. Estas herramientas y aplicaciones tienen características que incluyen:

- Auditar un dispositivo para detectar vulnerabilidades comunes.
- Monitorear proactivamente un dispositivo para detectar actividades sospechosas, como inicios de sesión no autorizados, ataques de fuerza bruta o escaladas de privilegios.
- Visualizar datos y eventos complejos en gráficos claros y modernos.
- Registrar el comportamiento operativo normal de un dispositivo para ayudar a detectar anomalías.

Establecida en el año 2015, Wazuh representa una solución integral, de código abierto y fácilmente disponible para la detección y respuesta de puntos finales (EDR). Su aplicabilidad se extiende a entornos de diversos tamaños. Básicamente, se designa un dispositivo distinto, conocido como administrador, para ejecutar Wazuh. Dentro de este marco, Wazuh opera según un modelo de administración y agente, en el que el administrador asume la responsabilidad de gestionar los agentes instalados en los dispositivos que requieren supervisión.

3.5.3. Agente Wazuh.

Los dispositivos que registran los eventos y procesos de un sistema se denominan agentes. Los agentes monitorean los procesos y eventos que tienen lugar en el dispositivo, como la autenticación y la gestión de usuarios. Los agentes descargarán estos registros a un recopilador designado para su procesamiento, como Wazuh.

Para completar la configuración de Wazuh, es necesario instalar agentes en los dispositivos para registrar los eventos. Wazuh puede guiarlo a través del proceso de implementación del agente siempre que complete algunos requisitos previos como:

- Sistema operativo.
- La dirección del servidor Wazuh a la que el agente debe enviar los registros (puede ser una dirección DNS o una dirección IP).
- ¿En qué grupo estará el agente? Puede clasificar a los agentes en grupos dentro de Wazuh si lo desea.

3.5.4. Eventos de seguridad y evaluación de vulnerabilidades de Wazuh.

El módulo de evaluación de vulnerabilidades de Wazuh es una poderosa herramienta que puede utilizarse para escanear periódicamente el sistema operativo de un agente en busca de aplicaciones instaladas y sus respectivas versiones. Una vez recopilada esta información, se envía de vuelta al servidor de Wazuh y se compara con una base de datos de CVE para identificar posibles vulnerabilidades.

3.5.5. Auditoría de políticas de Wazuh.

Wazuh es capaz de auditar y monitorear la configuración de un agente y registrar de forma proactiva eventos. Cuando se instala el agente Wazuh, se realiza una auditoría que proporciona una métrica que utiliza múltiples marcos y legislaciones, como NIST, MITRE y GDPR.

3.5.6. Monitoreo de inicios de sesión con Wazuh.

El monitor de eventos de seguridad de Wazuh puede registrar activamente intentos de autenticación tanto exitosos como fallidos. Por ejemplo: La regla con identificación 5710 detecta intentos de conexión que no tuvieron éxito al protocolo SSH.

3.5.7. Recopilación de registros de Windows con Wazuh.

Todo tipo de acciones y eventos se capturan y registran en el sistema operativo de Windows. Esto incluye intentos de autenticación, conexiones de red, archivos a los que se accedió y el comportamiento de las aplicaciones y los servicios. Esta información se almacena en el registro de eventos de Windows mediante una herramienta llamada Sysmon. Se puede utilizar el agente de Wazuh para agregar estos eventos registrados por Sysmon y procesarlos en el administrador de Wazuh. Necesitaremos configurar tanto el agente de Wazuh como la aplicación Sysmon. Sysmon utiliza reglas en formato XML para activarse y operar.

3.6. Desarrollo del modelo de ciclo de vida del SOC-UACJ.

Como parte de la metodología seleccionada para el desarrollo del prototipo del SOC - UACJ, se definió un modelo de ciclo de vida estructurado que permite integrar progresivamente los distintos componentes del sistema y validar su funcionamiento y adecuación en cada iteración. Este enfoque facilita la adaptación continua a los requerimientos institucionales y garantiza una evolución controlada del prototipo hasta alcanzar un nivel óptimo de madurez.

El modelo de ciclo de vida adoptado se fundamenta en la integración del enfoque de prototipo evolutivo con principios del modelo incremental, y se articula en las siguientes etapas:

1. **Definición de requisitos**: Se identificaron los requisitos funcionales y no funcionales del sistema mediante sesiones con el personal de la Dirección General de Tecnologías de Información (**DGTI**), la revisión de estándares de ciberseguridad y el análisis de riesgos basado en NIST SP 800-30 [6].

2. **Diseño del prototipo**: Se definió la arquitectura técnica del **SOC**, incluyendo la selección de herramientas de código abierto como Wazuh, y la estructura de recopilación y análisis de logs. Este diseño contempló la escalabilidad del sistema, su integración con activos críticos de la RedUACJ y su alineación con marcos como MITRE ATT&CK e ISO/IEC 27001 [43] [55] [67].

3. **Implementación**: Se realizó la instalación y configuración de los agentes Wazuh en equipos seleccionados, y se habilitaron funciones básicas de recopilación de eventos, detección de anomalías y generación de alertas. Esta fase incluyó la documentación de procedimientos y el aseguramiento de la trazabilidad de los datos recolectados [34].

4. **Pruebas y validación**: Se realizaron pruebas de funcionamiento para verificar la conectividad, la correcta recepción de los logs, la integridad de los datos y la detección efectiva de patrones sospechosos. Se evaluó la capacidad de respuesta ante eventos simulados y se midió el rendimiento del sistema [68].

5. **Retroalimentación y mejora**: Los resultados de las pruebas y la opinión del personal técnico permitieron introducir mejoras en la configuración de las reglas de

correlación, refinar las políticas de retención de logs y optimizar los dashboards de visualización. Estas mejoras se incorporaron en una nueva iteración del prototipo.

La implementación de este ciclo de vida iterativo ha permitido abordar el desarrollo del SOC-UACJ de forma controlada, asegurando su alineación con los objetivos institucionales de seguridad y facilitando su consolidación como una solución adaptable y robusta, (ver Ilustración 21).

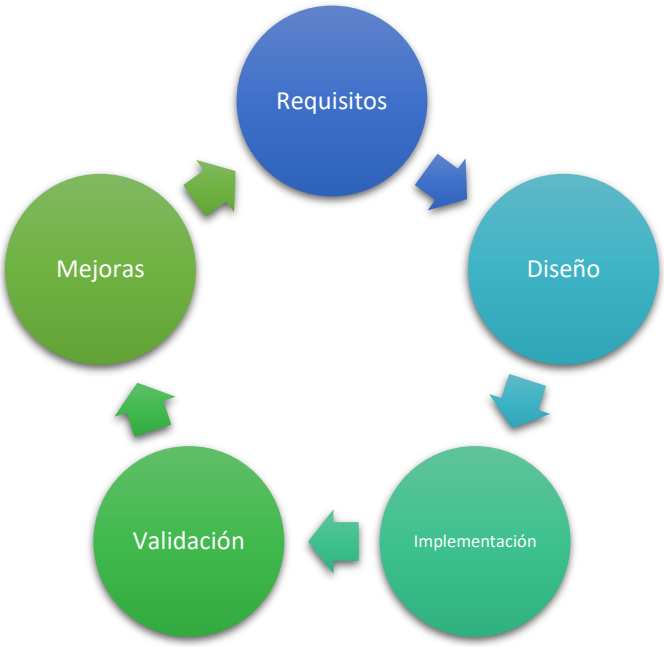


ILUSTRACIÓN 21. CICLO DE VIDA DEL SOC - UACJ.

3.7. Establecimiento de métricas para evaluar el prototipo del SOC-UACJ.

La evaluación del prototipo del SOC-UACJ requiere métricas claras, cuantificables y alineadas con los objetivos del proyecto y con las buenas prácticas de ciberseguridad. Estas métricas permitirán evaluar la eficacia de las funcionalidades implementadas, identificar áreas de mejora y justificar la evolución del prototipo hacia niveles más altos de madurez tecnológica.

Para ello, se utilizaron como base las recomendaciones de la "Guía metodológica para la evaluación de prototipos innovadores" publicada por la Red de Acacia [72], así como los lineamientos internacionales sobre gestión de incidentes y monitoreo continuo del NIST SP 800-137 [6]. Se definieron las siguientes categorías de métricas:

a) Métricas de rendimiento del sistema

- Tiempo medio de detección (MTTD): tiempo promedio desde la ocurrencia ***de*** un evento o anomalía hasta que el SOC lo detecta.
- Tiempo medio de respuesta (MTTR): tiempo que tarda el sistema en registrar, analizar y generar una alerta ante un evento crítico.
- Tasa de eventos procesados por segundo: capacidad del sistema de Wazuh para recibir y almacenar logs sin generar cuellos de botella.

b) Métricas de efectividad de detección

- Tasa de verdaderos positivos (TPR): porcentaje de incidentes reales correctamente identificadas por el ***SOC***.
- Tasa de falsos positivos (FPR): porcentaje de alertas generadas por eventos que no representaban una amenaza.
- Cobertura de activos: proporción de los sistemas críticos de la RedUACJ integrados efectivamente en la plataforma de monitoreo.

c) Métricas de usabilidad y operación

- Tiempo de capacitación del personal: número de horas necesarias para que un operador pueda interpretar los dashboards de Wazuh.
- Satisfacción del usuario: evaluada mediante encuestas aplicadas a los responsables de seguridad informática de la DGTI.
- Errores de configuración: número de fallos detectados en reglas, filtros o scripts durante la operación del prototipo.

d) Métricas de cumplimiento normativo

- Nivel de alineación con los controles del NIST SP 800-53: porcentaje de controles cubiertos por la arquitectura del ***SOC***.

- Cobertura de tácticas MITRE ATT&CK: número de tácticas/técnicas monitoreadas vs. el total documentado en ATT&CK.

Estas métricas permiten realizar una evaluación integral, tanto técnica como operativa, y sientan las bases para una medición futura de la madurez tecnológica mediante el modelo NMT (Nivel de Madurez Tecnológica), que podrá incorporarse en las siguientes fases del proyecto.

3.8. Ejecución de pruebas y refinamiento del prototipo del SOC-UACJ.

Con el objetivo de validar el funcionamiento del prototipo del SOC-UACJ, se realizaron pruebas exhaustivas centradas en la detección de eventos, el comportamiento del sistema ante cargas y la operación por parte del personal asignado a la Dirección General de Tecnologías de Información (DGTI), específicamente a la Jefatura de Función de Administración de Servidores y Servicios de Nube, así como a la Jefatura de Función de Infraestructura y Administración de Redes. Estas pruebas estuvieron alineadas con las métricas previamente establecidas y con las mejores prácticas para las pruebas de sistemas de seguridad [73].

Las pruebas se dividieron en tres fases:

a) Pruebas funcionales

Se simuló la generación de eventos en dispositivos terminales y servidores, observando si el sistema era capaz de:

- Recibir los logs mediante agentes de Wazuh instalados.
- Correlacionar eventos e identificar patrones sospechosos.
- Generar alertas adecuadas y clasificadas.
- Visualizar la información en tiempo real mediante dashboards personalizados.

b) Pruebas de carga y estabilidad

Se introdujeron flujos masivos de datos desde varios activos conectados para evaluar:

- Tolerancia del sistema frente a picos de carga.

- Consumo de recursos (CPU, RAM, red).
- Comportamiento del stack ELK durante consultas complejas.

c) Pruebas de usabilidad y experiencia operativa

Se capacitaron dos perfiles internos en el uso de la consola de Wazuh. Posteriormente se evaluó:

- Tiempo de respuesta ante eventos críticos.
- Facilidad para interpretar las visualizaciones.
- Identificación de errores o dificultades durante la operación.

Retroalimentación y ajustes

Se llevaron a cabo reuniones con el Director de tesis, Lector y personal técnico de la DGTI, quienes proporcionaron observaciones puntuales sobre:

- La necesidad de ajustar los umbrales de alerta.
- La reorganización de los paneles para mejorar la comprensión visual.
- Inclusión de más activos institucionales en la prueba piloto.

Con base en estos comentarios, se realizaron mejoras inmediatas al prototipo, destacando la optimización de las reglas de detección, la actualización de scripts de integración y ampliación de los dashboards. Este enfoque iterativo de validación y retroalimentación permitió afinar progresivamente el sistema y acercarlo a los requerimientos institucionales finales [72] [6].

3.9. Documentación y difusión del desarrollo del SOC-UACJ

La documentación adecuada de cada fase del desarrollo del SOC-UACJ constituye un elemento estratégico para garantizar la transparencia, la trazabilidad, la reproducibilidad y la mejora continua del prototipo. Esta práctica es esencial tanto para la validación del proyecto ante el comité de evaluación como para su escalamiento y su implementación institucional.

Durante el desarrollo del prototipo, se estableció una política de documentación sistemática que incluyó los siguientes componentes:

a) Documentación técnica

- Requerimientos funcionales y no funcionales: definidos a partir del análisis de riesgos y de sesiones con el personal de la DGTI, alineados con NIST SP 800-30 [1].
- Arquitectura del sistema: diagramas lógicos y físicos de la infraestructura del **SOC**, especificación de roles, de activos protegidos y de flujos de información.
- Configuración de herramientas: guías detalladas para la instalación, integración y operación de Wazuh, Elastic Stack, y herramientas complementarias como Suricata [74].
- Procedimientos operativos: descripción de actividades clave, como el análisis de logs, la generación de alertas, la clasificación de incidentes y la elaboración de reportes.

b) Documentación metodológica

- Modelo de ciclo de vida aplicado: pasos seguidos en cada iteración del prototipo, con retroalimentación registrada y decisiones de ajuste.
- Métricas y resultados: registros de pruebas, indicadores clave de desempeño (MTTD, MTTR, TPR, etc.) y observaciones del equipo técnico [6].

c) Buenas prácticas y lecciones aprendidas

- Recomendaciones operativas: configuraciones mínimas necesarias, errores frecuentes y soluciones.
- Políticas de seguridad adoptadas: alineadas con la ISO/IEC 27001 y los controles de NIST SP 800-53 [75].
- Limitaciones y sugerencias de mejora futura: incluyendo aspectos de escalabilidad, interoperabilidad e integración con plataformas **SOAR**.

Toda esta documentación ha de ser validada cuando el proyecto concluya y se logre un punto de madurez de **SOC–UACJ** que convenza a las autoridades correspondientes y será compartida con los siguientes actores:

I. Comité tutorial y lectores del proyecto.
II. Dirección General de Tecnologías de Información (DGTI).
III. Coordinación del Programa Educativo de Posgrado (PEP).
IV. Comunidad técnica interna de la UACJ interesada en ciberseguridad.

El repositorio documental (formato digital) contiene archivos organizados por iteración, incluye material visual (diagramas, capturas de pantalla), registros de configuraciones, plantillas de reportes y el resumen ejecutivo del prototipo. Esta práctica permite preservar el conocimiento generado y facilitar la transferencia tecnológica en futuras fases del SOC-UACJ o en su réplica en otras instituciones.

Es importante comentar que hasta el momento se ha participado en diferentes ocasiones y con diferentes motivos con instancias de colaboración entre Instituciones de Educación Superior (IES), como son:

- La Asociación Nacional de Universidades (ANUIES), con la que se participa en la Campaña de Concientización de Ciberseguridad (ver Anexo 2). Donde la UACJ recibió en dos ocasiones el reconocimiento Sello C3!Cyber [76].
- La Corporación Universitaria para el Desarrollo de Internet (CUDI), participado en las diferentes jornadas de Ciberseguridad y encuentros de CISOs, donde también se ha compartido información del presente proyecto y ha llamado la atención de otras instituciones [77].
- El Consejo Europeo para la Investigación Nuclear (CERN), con el que se ha firmado un acuerdo de intercambio de inteligencia sobre amenazas cibernéticas a través de sus especialistas en ciberseguridad y de su instancia MISP [78].

Esto es un claro ejemplo de que la comunicación y la colaboración son primordiales para mantenerse a la vanguardia frente a las amenazas cibernéticas.

3.10. Iteración y mejora continua del prototipo del SOC-UACJ

Uno de los principios rectores en el desarrollo del SOC-UACJ ha sido la mejora continua, entendida como un proceso iterativo, fundamentado en la revisión sistemática de resultados, el análisis de la retroalimentación y los ajustes sucesivos a la solución implementada. Esta

estrategia se alinea con el enfoque evolutivo del prototipo y con las prácticas recomendadas en ingeniería de software ágil y seguridad informática [64][79].

El desarrollo del SOC se estructuró en ciclos iterativos, cada uno compuesto por las fases de implementación, prueba, evaluación y retroalimentación. Los hallazgos de cada ciclo se documentaron mediante bitácoras de configuración, informes de pruebas y reuniones con el equipo técnico. A partir de estos insumos se formularon propuestas de mejora que dieron origen a nuevas versiones del sistema, incrementando así su madurez y funcionalidad.

Algunas mejoras clave implementadas como resultado de este enfoque fueron:

- Reajuste de las reglas de detección en Wazuh para reducir la tasa de falsos positivos.
- Inclusión de más activos críticos en el monitoreo del sistema.
- Refinamiento de dashboards de visualización para facilitar su uso operativo.
- Reestructuración de las políticas de retención y cifrado de los logs conforme a la NIST SP 800-92 [6].

Esta dinámica iterativa permitió resolver problemas emergentes e incorporar nuevas funcionalidades, sin interrumpir la operatividad del prototipo. Asimismo, promovió la apropiación tecnológica del personal responsable del ***SOC***, al involucrarlo en el análisis de resultados y la toma de decisiones técnicas.

El proceso de mejora continua se mantendrá activo tras la etapa de prototipo, como parte de la estrategia institucional para fortalecer el SOC-UACJ. Se prevé establecer revisiones semestrales, auditorías técnicas y ejercicios de *Red Teaming* como fuentes formales de retroalimentación. Es importante resaltar que se monitorea la madurez del SOC-UACJ conforme a la gráfica del Anexo 1.

En el Anexo 15, se muestra el procedimiento para la instalación de Wazuh siguiendo con el procedimiento sencillo de instalación asistida que se describe en la documentación de Wazuh (https://documentation.wazuh.com/current/quickstart.html).

4. Activos informáticos

Los activos informáticos abarcan una amplia gama de entidades digitales almacenadas en computadoras o en la nube, y el término "activo digital" se refiere a cualquier dato binario con derechos de uso [80]. Estos activos pueden incluir software, hardware y datos, como máquinas equipadas con sensores, conectadas a computadoras locales y remotas, con fines de monitoreo y mantenimiento [81].

En el ámbito de la informática, los activos también pueden extenderse a aplicaciones complejas como CAD e ingeniería de software, donde se utilizan modelos de transacciones extendidas, como ASSET, para satisfacer diversas necesidades de transacción, como las de larga duración y de cooperación [82]. Además, los servicios de gestión de activos de software desempeñan un papel crucial en la obtención, actualización y presentación de informes de dichos activos, lo que subraya la importancia de gestionar eficazmente los activos digitales.

4.1. Activos seleccionados

Durante el proceso de análisis de riesgos, realizado en la etapa de ingeniería de requisitos, se obtuvo del personal de la Jefatura de Seguridad Informática de la RedUACJ un listado de los activos críticos protegidos. Después de los análisis subsecuentes, el listado se incrementó a sesenta activos críticos, de los cuales se identificaron los siguientes grupos:

- Almacenamiento (Dell Compellent)
- Hiperconvergencia (VxRail)
- Almacenamiento (NAS)
- Servidores (Portal institucional, Servidores escolares, etc)
- Controladores de Dominio (Alumnos, Administrativos, Docentes y de Servicio)
- Servidores DNS
- Servidores DHCP
- Servidores DHCP para Red inalámbrica
- Bases de datos
- Campus Virtual (nube publica)
- Servicios de Pago
- Servicios telefónicos

- Equipos de redes (routers y switches)

Es importante aclarar que, para no afectar la confidencialidad, disponibilidad e integridad de la información de la UACJ, no todos los activos seleccionados se agregaron a la plataforma de Wazuh al instalar el agente.

Para efectuar la prueba de concepto del sistema Wazuh como EDR, se instaló el agente en equipos secundarios para los cuales se obtuvo la autorización del usuario propietario y del administrador del activo. Los agentes instalados son los que figuran en la Ilustración 22.

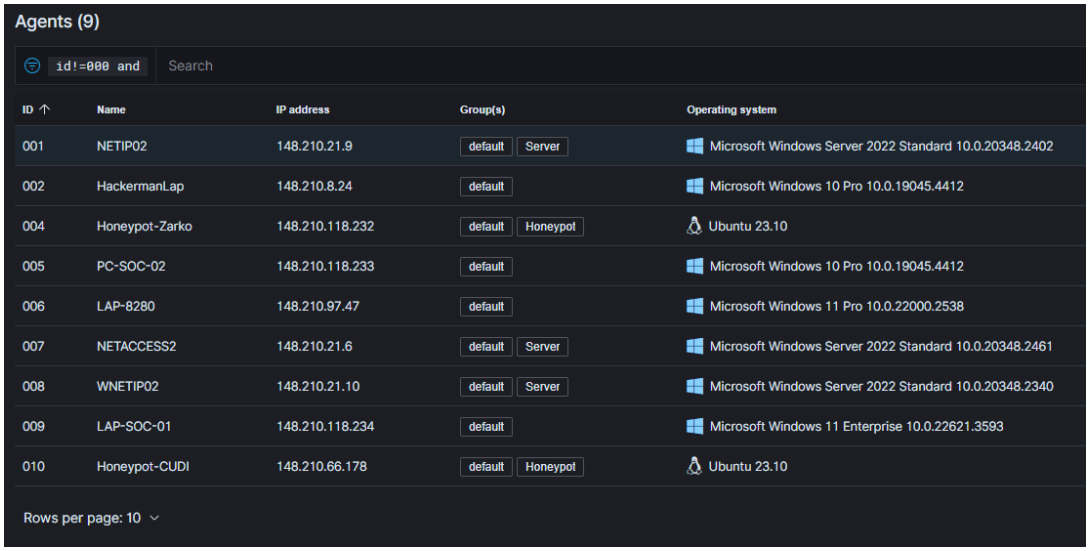


ILUSTRACIÓN 22. LISTADO DE AGENTES INSTALADOS EN LA POC.

Todos los activos informáticos seleccionados se encuentran dentro de un Acuerdo de Nivel de Servicio (ANS), que constituye la parte medular del cumplimiento normativo del SOC – UACJ.

5. Instauración del SOC - UACJ.

5.1. Los beneficios de un *SOC*

Aunque una organización puede intentar protegerse sin un ***SOC***, en la práctica resulta difícil y la expone a mayores riesgos. Un ***SOC*** con IA ofrece beneficios clave, como el monitoreo continuo, la visibilidad mejorada, la reducción de costos operativos y una respuesta más ágil a incidentes.

5.1.1. Monitoreo continuo

Los ciberataques no tienen horario. Mientras la UACJ puede operar en horarios convencionales, los atacantes aprovechan los momentos fuera del horario laboral o los fines de semana y días feriados para lanzar sus ataques. Por ello, es crucial que la UACJ cuente con monitoreo 24/7, de modo que el equipo de seguridad esté disponible en todo momento para prevenir incidentes.

5.1.2. Visibilidad mejorada

Con la proliferación del trabajo remoto, el uso de dispositivos personales y la adopción de tecnologías como la nube y el IoT, las redes corporativas se han vuelto más complejas. Mantener una visibilidad completa de estas redes es esencial para la seguridad. Un ***SOC*** impulsado por IA ofrece visibilidad total y ayuda a identificar y neutralizar posibles vectores de ataque en toda la infraestructura.

5.1.3. Reducción de costos operativos

Proteger una red empresarial requiere diversas herramientas y licencias, lo que puede resultar costoso. Sin embargo, un ***SOC*** centralizado reduce estos costos al eliminar redundancias y silos. Además, la IA permite optimizar la respuesta a amenazas, reduciendo el tiempo de inactividad y evitando incidentes costosos, como ataques de ransomware o filtraciones de datos.

5.1.4. Mejor respuesta a incidentes

La colaboración eficaz entre los equipos es clave para responder con rapidez a ciberataques. Un ***SOC*** basado en IA centraliza los recursos y mejora la coordinación entre los miembros

de los equipos de seguridad, lo que facilita la identificación rápida de amenazas y su eliminación antes de que causen daño.

5.1.5. Protegiendo la RedUACJ con el SOC-UACJ

Implementar un ***SOC*** eficaz requiere herramientas avanzadas y métodos bien definidos. Por ello, se han desarrollado nuevas políticas que, en su momento y de la forma apropiada, se presentarán a los directivos de la UACJ en la cadena de mando, por lo que una solución basada en inteligencia artificial podrá mejorar la precisión y la eficiencia en la detección y respuesta a incidentes. Con una plataforma basada en la nube, ofrecerá una implementación sencilla y un retorno de la inversión elevado, ayudando a la universidad a protegerse con una precisión del 99.0%.

5.2. Funciones objetivo del SOC – UACJ

Las funciones principales de un SOC-UACJ son esenciales para proteger los sistemas de información de una organización. A continuación, se detallan algunas de las funciones principales señaladas como funciones objetivo cuando se consolide el proyecto:

1. **Monitoreo y Detección de Incidentes:** Supervisión continua de la red, los sistemas y las aplicaciones para identificar posibles amenazas o actividades sospechosas.
2. **Gestión de Incidentes:** Respuesta inmediata a incidentes de seguridad, incluyendo la contención, la erradicación y la recuperación de los sistemas afectados.
3. **Análisis de Vulnerabilidades:** Evaluación regular de los sistemas para identificar y mitigar vulnerabilidades antes de que puedan ser explotadas.
4. **Análisis de Amenazas:** Investigación y evaluación de amenazas emergentes para adaptar las estrategias de seguridad de la organización.
5. **Gestión de Logs y Auditoría:** Recolección y análisis de *logs* para identificar patrones anómalos y realizar auditorías de seguridad.
6. **Respuesta a Incidentes de Seguridad:** Proceso formal para gestionar incidentes de seguridad, que incluye la notificación a las partes interesadas y la realización de investigaciones posincidente.
7. **Inteligencia de Amenazas:** Recopilación y análisis de información sobre amenazas cibernéticas para anticiparse a posibles ataques.

8. **Desarrollo de Métodos de Seguridad:** Creación y actualización de métodos empleados por el ***SOC*** para garantizar una postura de seguridad sólida.
9. **Pruebas de Penetración y *Red Teaming*:** Simulación de ataques para evaluar la efectividad de las defensas de la organización.
10. **Educación y Concienciación en Seguridad:** Capacitación regular para los empleados sobre las mejores prácticas de ciberseguridad y sobre cómo identificar posibles amenazas.
11. **Evaluación de Riesgos:** Identificación y análisis de riesgos asociados a las infraestructuras y servicios tecnológicos de la organización.
12. **Gestión de la Configuración:** Monitoreo y auditoría de las configuraciones de los sistemas para asegurarse de que cumplan con las políticas de seguridad establecidas.
13. **Supervisión de la Cadena de Suministro:** Evaluación y control de la seguridad de los proveedores y terceros para prevenir riesgos asociados a la cadena de suministro.
14. **Resiliencia y Recuperación ante Desastres:** Planificación y pruebas de recuperación para asegurar la continuidad de las operaciones críticas ante un ataque cibernético.
15. **Seguridad en la Nube:** Monitoreo y aseguramiento de infraestructuras y servicios en la nube, garantizando el cumplimiento de normativas y buenas prácticas de seguridad.
16. **Análisis Forense Digital:** Realización de análisis forenses en caso de un incidente de seguridad, con el objetivo de recopilar y analizar evidencia para comprender el alcance del ataque y su origen.
17. **Cumplimiento y Conformidad Normativa:** Asegurar que las operaciones y procedimientos de ciberseguridad cumplan con las regulaciones y normativas aplicables, como ISO 27001:2022, NIST 800, GDPR, HIPAA, etc.
18. **Simulación de Ataques (Purple Teaming):** Integración de equipos de *Red Team* y *Blue Team* para simular ataques avanzados y mejorar la capacidad de detección y respuesta del ***SOC***.
19. **Supervisión de la Dark Web:** Monitoreo de actividades en la Dark Web para identificar posibles amenazas o filtraciones de datos relacionadas con la organización.
20. **Gestión de la Seguridad de los Endpoints:** Monitoreo y protección de los dispositivos finales (laptops, smartphones, etc.) contra amenazas cibernéticas.

21. **Insider Threat Management:** Identificación y mitigación de amenazas internas, como empleados malintencionados o negligentes que puedan comprometer la seguridad de la organización.
22. **Evaluación de la Eficacia de los Controles de Seguridad:** Revisión y prueba periódica de los controles de seguridad existentes para asegurarse de que sigan siendo eficaces frente a las amenazas actuales.
23. **Planificación de la Capacidad y Escalabilidad del SOC:** Asegurar que el ***SOC*** pueda escalar sus operaciones para manejar aumentos de la demanda, ya sea debido a un crecimiento de la organización o a una escalada de las amenazas.
24. **Gestión de la Seguridad de Aplicaciones:** Monitoreo y protección de las aplicaciones utilizadas por la organización para asegurar que no actúen como vectores de ataque.
25. **Evaluación de Proveedores de Seguridad:** Revisión y evaluación de servicios y herramientas de terceros que ofrecen soluciones de seguridad para garantizar su efectividad y alineación con las necesidades de la organización.
26. **Investigación y Desarrollo en Ciberseguridad:** Innovación y desarrollo de nuevas técnicas, herramientas y estrategias de seguridad para mantenerse a la vanguardia ante las amenazas emergentes.

Resiliencia y Plan de Respuesta de Recuperación ante Desastres del SOC.

Para garantizar la continuidad operativa del **SOC-UACJ**, no basta con proteger la red universitaria; el propio centro debe contar con una arquitectura resiliente que permita la recuperación inmediata de sus capacidades de monitoreo [83]. Se establece el siguiente Plan de Respuesta Específico para el **SOC**:

- **Alta Disponibilidad y Failover:** La instancia principal de **Wazuh** y el clúster de Elastic Stack operarán con un esquema de replicación en la nube para evitar puntos de falla únicos.
- **Respaldo de Evidencia y Logs:** Se mantendrá una política de retención y cifrado de registros conforme al estándar NIST SP 800-92 [84], asegurando que los registros de eventos críticos se almacenen en un repositorio fuera de línea (off-site) para análisis forense postincidente.
- **Procedimiento de Recuperación (DRP):** Ante una caída de la infraestructura central, se activará una instancia de contingencia con los indicadores de compromiso

(IoC) más recientes descargados de **MISP**, lo que permitirá reanudar el monitoreo básico en menos de 2 horas (RTO < 120 min).

Automatización mediante Playbooks para Incidentes Comunes.

La orquestación de seguridad es vital para reducir el tiempo medio de respuesta (**MTTR**). Se definen los primeros ***Playbooks*** automatizados para los vectores de ataque con mayor incidencia en la RedUACJ:

A**.** Playbook de Respuesta ante Phishing (Crítico para UACJ):

1. **Detección:** Alerta generada por el agente **Wazuh** tras identificar un enlace malicioso en un correo de Office 365.
2. **Enriquecimiento:** Consulta automática de la URL sospechosa en VirusTotal y URLScan.io.
3. **Contención:** Bloqueo inmediato de la IP de origen en el Firewall Perimetral y rotación de credenciales de usuario afectada en Active Directory (recuperación de cuenta).
4. **Erradicación:** Eliminación masiva del correo malicioso de todos los buzones institucionales mediante reglas de transporte.

Para visualizar de manera más completa, en el Anexo 17 se presenta un Playbook para la respuesta ante Phishing, que es uno de los ataques más comunes.

B. Playbook de Ataque de Fuerza Bruta (SSH/RDP):

1. **Detección:** La regla ID 5710 de Wazuh detecta múltiples intentos fallidos de conexión SSH.
2. **Acción:** Ejecución de una Respuesta Activa (Active Response) para bloquear la IP atacante en el firewall local del host, mediante *iptables* o *netsh,* durante 24 horas.

5.3. Funciones de soporte del SOC – UACJ

Funciones secundarias dentro del ***SOC*** que complementan las funciones principales mencionadas anteriormente:

1. **Gestión de la Documentación**: Mantenimiento y actualización de toda la documentación relacionada con los procedimientos, incidentes y políticas de seguridad.

2. **Supervisión de la Infraestructura de Seguridad**: Monitoreo del estado y rendimiento de las herramientas y tecnologías de seguridad, como firewalls, sistemas de detección de intrusiones (IDS), y sistemas de prevención de intrusiones (IPS).

3. **Soporte Técnico y Mantenimiento**: Provisión de soporte técnico para las herramientas de ciberseguridad y aseguramiento de que todos los sistemas estén actualizados y funcionen correctamente.

4. **Análisis de Tendencias**: Recolección y análisis de datos históricos para identificar patrones y tendencias en los incidentes de seguridad, lo que puede ayudar a anticipar y prevenir futuros ataques.

5. **Gestión de la Capacidad del SOC**: Monitoreo y ajuste de la capacidad del ***SOC*** para manejar el volumen de eventos de seguridad y asegurar una respuesta eficiente.

6. **Integración de Nuevas Tecnologías**: Evaluación e integración de nuevas tecnologías y herramientas de seguridad en las operaciones del ***SOC*** para mejorar la capacidad de detección y respuesta.

7. **Gestión de Relaciones con Terceros**: Coordinación con proveedores de servicios de seguridad, consultores externos y otras partes interesadas para garantizar un enfoque integral de ciberseguridad.

8. **Soporte en Auditorías de Seguridad**: Asistencia en auditorías internas y externas, proporcionando datos y evidencia de cumplimiento y eficiencia de las medidas de seguridad.

9. **Simulación y Prueba de Procedimientos**: Realización de simulaciones y pruebas regulares de los procedimientos de respuesta a incidentes para asegurar que el equipo esté preparado ante un ataque real.

10. **Evaluación del Impacto Empresarial**: Análisis del impacto potencial de las amenazas de seguridad en las operaciones comerciales y priorización de las respuestas según la criticidad del negocio.

11. **Gestión de Proyectos de Seguridad**: Planificación y ejecución de proyectos específicos dentro del ***SOC***, como la implementación de una nueva herramienta de monitoreo o la mejora de un proceso de respuesta a incidentes.

12. **Supervisión del Cumplimiento de Políticas de Seguridad**: Asegurarse de que los empleados y otras partes interesadas cumplan con las políticas de seguridad establecidas, incluyendo la revisión y el ajuste de dichas políticas según sea necesario.

13. **Educación Continua del Personal del SOC**: Provisión de oportunidades de formación continua para el personal del ***SOC***, asegurando que se mantenga actualizado sobre las últimas amenazas y tecnologías.

14. **Gestión del Cambio**: Coordinación de cambios en las configuraciones de seguridad y aseguramiento de que no introduzcan nuevos riesgos ni vulnerabilidades.

15. **Comunicación y Reportes a la Alta Dirección**: Preparación y presentación de informes periódicos sobre el estado de la seguridad, los incidentes recientes y las recomendaciones estratégicas.

16. **Supervisión de la Seguridad Física del SOC**: Aseguramiento de que las instalaciones del ***SOC*** estén protegidas contra accesos no autorizados y otras amenazas físicas que podrían comprometer las operaciones.

17. **Control de Calidad de los Procesos del SOC**: Revisión y mejora continua para garantizar su eficiencia y eficacia.

18. **Colaboración con Equipos de IT**: Coordinación con otros equipos de IT para asegurar la alineación de las operaciones de seguridad con las infraestructuras tecnológicas de la organización.

19. **Escalado y Escalamiento de Incidentes**: Determinación de cuándo y cómo escalar incidentes a niveles superiores dentro de la organización o a otros equipos especializados.

20. **Soporte en la Implementación de Herramientas de SIEM**: Ayuda en la implementación y optimización de herramientas de gestión de información y eventos de seguridad para mejorar la capacidad de análisis de seguridad.

Gestión de Riesgos de Proveedores y Cadena de Suministro (S-CCRM).

Dada la heterogeneidad de la infraestructura universitaria y la dependencia de servicios externos, el ***SOC*** integrará una tarea continua de auditoría de terceros:

- **Auditoría de Acceso Externo:** Supervisión de las sesiones de soporte técnico brindadas por proveedores (p.ej., Sophos, Dell) mediante la revisión de los logs de la **VPN Sophos Remote Access**.
- **Colaboración con Compras y DGTI:** Evaluación de la seguridad de cualquier software o hardware nuevo antes de su adquisición, verificando que los dispositivos cuenten con soporte para los protocolos estándar de exportación de registros (**Syslog/SIEM**).
- **Monitoreo de Vulnerabilidades de Terceros:** Uso de **Greenbone** para identificar brechas en sistemas administrados por proveedores con presencia en la **RedUACJ**.

5.4. Organización del equipo de trabajo del SOC–UACJ

Se propone, como equipo de trabajo del ***SOC,*** un esquema que organiza su personal en varios roles y niveles jerárquicos para garantizar la detección, el monitoreo y la respuesta efectiva a incidentes. Este equipo operaría en una etapa inicial, bajo un esquema de 8 x 5 (8 horas laborales, 5 días a la semana). Posteriormente, se propone, en una segunda etapa, cubrir el horario de operación regular de la UACJ, que sería de 15 x 5, y en una tercera etapa, proporcionar una cobertura total en horario de 24 x 7. Con la posibilidad de brindar soporte a instituciones afiliadas a la UACJ.

5.5. Roles del personal

Los roles y responsabilidades del personal de **SOC - UACJ** se definen mediante diversas normativas, estándares y mejores prácticas que buscan establecer estructuras organizacionales y operativas para garantizar una defensa eficaz en ciberseguridad. Algunos de los estándares o de los más relevantes que sirven como base para definir los roles de trabajo son:

- **NIST SP 800-181 (National Initiative for Cybersecurity Education - NICE Framework)** [85]**:** Este marco describe categorías y especialidades laborales en el ámbito de la ciberseguridad, ayudando a definir roles específicos dentro de un ***SOC***, tales como analistas de seguridad, incident responders, y roles de liderazgo. Proporciona un desglose detallado de las tareas, conocimientos, habilidades y capacidades requeridos para estos roles.
- **ISO/IEC 27001:2022, 27035 y 27032 (Sistema de Gestión de Seguridad de la Información)** [75]**:** Aunque esta norma se centra en la gestión de la seguridad de la información, puede servir de base para definir roles clave en un ***SOC*** en cuanto a la implementación y monitoreo de controles de seguridad, auditoría, y gestión de incidentes de seguridad.
- **NIST SP 800-53 (Security and Privacy Controls for Information Systems and Organizations)** [86]**:** Este estándar ofrece controles de seguridad y privacidad que se pueden aplicar a las operaciones del ***SOC***, estableciendo roles necesarios para implementar estos controles, incluyendo personal de monitoreo, respuesta a incidentes, y gestión de riesgos.
- **MITRE ATT&CK Framework** [43]**:** Aunque no es una norma en sí misma, este marco es ampliamente utilizado en los ***SOC*s** para la clasificación de ataques y amenazas. Ayuda a definir roles basados en la capacidad del personal para identificar, responder a y mitigar diversas técnicas de ataque.
- **SANS Institute - Security Operations Center (SOC) Framework** [87]**:** SANS es una organización que provee directrices específicas para la estructura de un ***SOC***. Sus marcos incluyen recomendaciones para el equipo de respuesta a incidentes, los analistas de inteligencia de amenazas y el personal encargado del monitoreo.
- **ISO/IEC 20000 (Gestión de Servicios TI)** [88]**:** Este estándar está orientado a la gestión de servicios **IT**, pero en muchos ***SOC*** se utiliza para definir roles relacionados

con la prestación de servicios de seguridad, tales como soporte técnico, gestión de incidentes y operaciones continuas.

- **ENISA (European Union Agency for Cybersecurity)** [89]**:** Ofrece varias guías y recomendaciones sobre la operación de ***SOC*** en Europa, que incluyen la estructura organizativa y las responsabilidades clave.

5.6. Estructura

La estructura del equipo de trabajo y las especificaciones clave de cada rol dentro del SOC-UACJ son:

I. Analistas de Nivel 1 (N1) - Analistas de Monitorización:

Responsabilidades:

- Monitorear alertas y eventos de seguridad en tiempo real.
- Investigar y escalar incidentes según sea necesario.
- Realizar análisis básicos para identificar la naturaleza de los eventos.
- Aplicar los procedimientos de respuesta inicial a los incidentes.

Habilidades:

- Conocimientos básicos en ciberseguridad, uso de herramientas de **SIEM**, y análisis de logs.
- Conocimientos de redes, sistemas operativos y procesos de autenticación.

II. Analistas de Nivel 2 (N2) - Analistas de Incidentes:

Responsabilidades:

- Analizar los incidentes escalados por el equipo de N1.
- Investigar a fondo las amenazas y confirmar si las alertas son incidentes reales.
- Ejecutar tareas de respuesta más avanzadas, como la contención y la mitigación.
- Identificar patrones de ataque y proponer medidas preventivas.

Habilidades:

- Mayor experiencia en ciberseguridad, conocimiento profundo de redes, *malware*, y análisis forense.
- Conocimiento de sistemas operativos y herramientas de análisis forense.

III. Analistas de Nivel 3 (N3) - Especialistas en Respuesta y Mitigación:

Responsabilidades:

- Responder a incidentes críticos y complejos.
- Realizar análisis forense en sistemas comprometidos.
- Desarrollar planes de contención, erradicación y recuperación.
- Proporcionar retroalimentación para mejorar las reglas de detección y las herramientas del ***SOC***.

Habilidades:

- Especialización técnica avanzada en ciberseguridad, análisis forense, y amenazas avanzadas persistentes (APT).

IV. Personal de Threat Intelligence (Inteligencia de Amenazas):

Responsabilidades:

- Recolectar, analizar y difundir información sobre amenazas emergentes.
- Desarrollar informes y alertas para el equipo de **SOC** basados en la inteligencia de amenazas.
- Colaborar con el equipo de respuesta para anticipar ataques.

Habilidades:

- Expertise en análisis de amenazas, dark web y correlación de datos procedentes de diversas fuentes.

V. Equipo de Ingeniería de Seguridad:

Responsabilidades:

- Configurar, gestionar y mantener las herramientas del **SOC** (**SIEM**, **IDS/IPS**, ***firewalls***, etc.).
- Desarrollar y ajustar las reglas de detección para mejorar la precisión.
- Implementar automatización para mejorar la eficiencia de la detección y respuesta.

Habilidades:

- Conocimientos técnicos avanzados en infraestructura de seguridad y en herramientas de **SIEM**.

VI. Gerentes de **SOC** / Coordinadores de Incidentes:

Responsabilidades:

- Supervisar el funcionamiento del **SOC** y coordinar la respuesta a incidentes de alto impacto.
- Comunicarse con los equipos de **IT**, los directores de seguridad (CISO) y otras áreas de la organización.
- Asegurar que el equipo de trabajo cumpla con las políticas y los procedimientos.
- Mejorar la postura de seguridad mediante la revisión de incidentes y la implementación de mejoras.

Habilidades:

- Capacidad de liderazgo, gestión de crisis, y conocimiento profundo en ciberseguridad y gestión de incidentes.

VII. CISO (Chief Information Security Officer) / Director de Seguridad de la Información:

Responsabilidades:

- Supervisar todas las operaciones de ciberseguridad, incluido el **SOC**.
- Desarrollar y alinear la estrategia de ciberseguridad con los objetivos de la organización.
- Reportar a la alta dirección sobre el estado de la seguridad y coordinar las respuestas a incidentes críticos.

Habilidades:

- Experiencia en gestión de seguridad, estrategia corporativa y cumplimiento normativo.

5.7. Organigrama

Para visualizar la estructura, los roles y las relaciones del equipo de trabajo, se presenta el organigrama en la Ilustración 23.

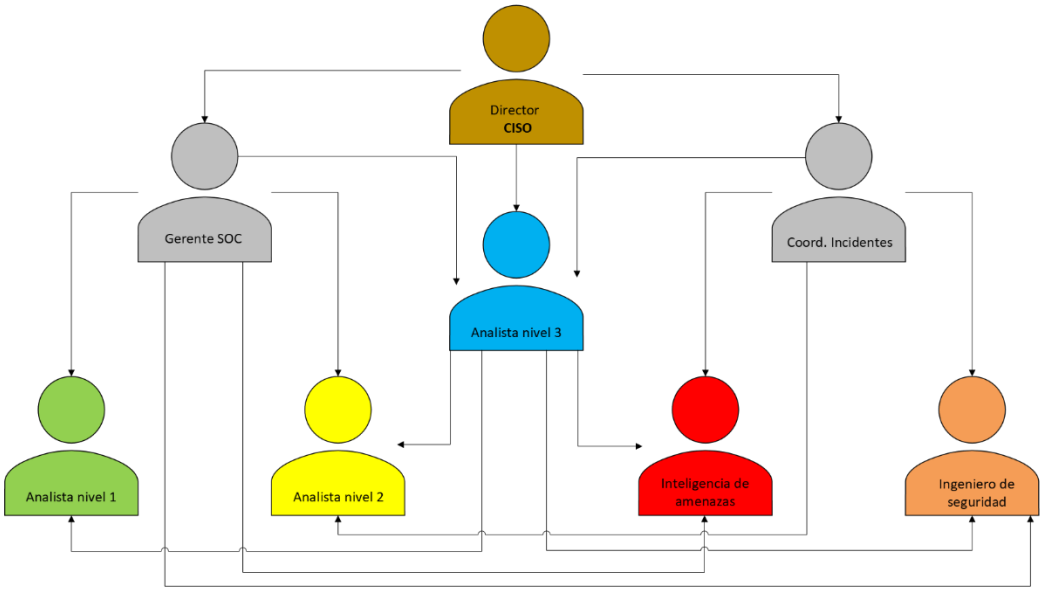


ILUSTRACIÓN 23. ORGANIGRAMA DEL SOC - UACJ (PROPIO).

5.8. Catálogo de Reportes de Cumplimiento

La operación del SOC-UACJ genera una gran cantidad de datos que deben procesarse y presentarse de manera estructurada para satisfacer las necesidades de transparencia, auditoría y cumplimiento legal. El siguiente catálogo establece los documentos oficiales que el centro debe emitir para garantizar que la Dirección General de Tecnologías de la Información (DGTI) cumpla con sus obligaciones institucionales y legales.

5.8.1. Reporte de Notificación de Brechas de Seguridad (LGPDPPSO)

Este es el reporte de mayor criticidad legal. De acuerdo con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, cualquier vulneración a la seguridad que afecte la integridad, disponibilidad o confidencialidad de datos personales debe ser documentada y notificada.

- **Finalidad:** Cumplir con los artículos correspondientes de la ley y facilitar la comunicación con el Abogado General y la Contraloría.
- **Contenido:** Descripción del incidente, categorías de datos personales afectados, acciones de mitigación inmediatas y recomendaciones para los titulares de datos.

5.8.2. Reporte Mensual de Cumplimiento Operativo y Postura de Seguridad

Este reporte ofrece una visión ejecutiva del desempeño del ***SOC***, alineada con los controles de monitoreo continuo del marco **NIST SP 800-53**.

- **Finalidad:** Informar a la alta dirección sobre la eficacia de los controles de seguridad y la evolución del riesgo institucional.
- **Contenido:** Métricas clave (MTTD, MTTR, % de falsos positivos y verdaderos positivos), resumen de alertas críticas detectadas por Wazuh, nivel de cobertura de activos y estado de la higiene de parches en la RedUACJ.

5.8.3. Reporte Técnico de Hallazgos y Acciones Correctivas

Derivado de la identificación de vulnerabilidades mediante herramientas como Greenbone y de la detección de anomalías en Elastic Stack, este reporte técnico se dirige a los administradores de sistemas y redes.

- **Finalidad:** Documentar debilidades específicas y dar seguimiento a su remediación.
- **Estructura de Hallazgos:** Para asegurar la trazabilidad, cada entrada debe seguir el formato institucional:

    1. **Nº:** identificador único del hallazgo.
    2. **Hallazgo:** Descripción clara de la vulnerabilidad o anomalía.
    3. **Análisis técnico/Evidencia:** Datos extraídos de logs o capturas de tráfico.
    4. **Conclusión:** Evaluación del riesgo asociado.
    5. **Acción correctiva o de mejora:** Pasos específicos para la solución.
    6. **Responsable:** Área técnica encargada de la ejecución.
    7. **Fecha:** Plazo máximo de atención según el SLA.

5.8.4. Reporte de Auditoría de Acceso a Datos Sensibles

Enfocado en el principio de "Privacidad por Diseño", este reporte monitorea los patrones de acceso a las bases de datos escolares y sistemas financieros.

- **Finalidad:** Garantizar que el acceso a la información de la comunidad universitaria se realice conforme a los principios de legalidad y lealtad.

- **Contenido:** Auditoría de inicios de sesión de cuentas administrativas, actividad en los activos, detección de movimientos laterales y validación de accesos externos.

5.8.5. Reporte Trimestral de Inteligencia de Amenazas y Colaboración

Documenta la actividad de intercambio de información con instituciones externas (como el CERN vía MISP).

- **Finalidad:** Evaluar la efectividad de los indicadores de compromiso (IoC) recibidos y fortalecer la defensa proactiva.
- **Contenido:** Resumen de campañas de malware detectadas de forma preventiva y aportaciones de la UACJ a los consorcios de ciberseguridad.

Todos estos reportes, entre otros más, serán propuestos para su alineación con las diferentes normas y marcos de referencia competentes y aplicables en cuanto a ciberseguridad en México; véase Anexo 14.

6. Aplicación del conocimiento multidisciplinario en el diseño y operación del SOC.

6.1. Conocimientos adquiridos.

El diseño y la operación de un ***SOC*** no solo requieren conocimientos técnicos aislados, sino también una integración efectiva de múltiples disciplinas. A lo largo del desarrollo de este trabajo, se aplicaron competencias adquiridas en áreas clave como el cómputo aplicado, la ciberseguridad y el análisis de datos. Este capítulo tiene como objetivo exponer cómo se aprovecharon estos conocimientos para construir una solución robusta, escalable y alineada con las mejores prácticas del sector.

6.2. Aplicación del cómputo.

Durante la implementación del ***SOC***, se emplearon habilidades adquiridas en entornos de cómputo moderno:

- Contenerización y automatización: Se utilizaron herramientas como Docker para la contenerización de algunos servicios y scripts en Python y Power Shell para la automatización de tareas repetitivas. Esto permitió una gestión eficiente de los servicios desplegados [90].
- Gestión de infraestructura con código (IaC): Mediante scripts de shell, se logró reproducir el entorno del SOC de forma controlada, lo que facilitó la escalabilidad y la mantenibilidad [91].
- Sistemas operativos y redes: El conocimiento de Linux y de redes TCP/IP , así como de la administración de infraestructura de redes de Cisco, fue esencial para configurar el monitoreo del tráfico, los servicios Syslog y la recolección de eventos desde dispositivos distribuidos.

6.3. Aplicación de principios de ciberseguridad.

En el diseño del ***SOC*** se integraron las siguientes prácticas y normativas:

- Framework NIST 800-61r2 para la respuesta a incidentes, que establece un ciclo de preparación, detección, contención, erradicación, recuperación y lecciones aprendidas [92].
- Controles técnicos basados en ISO/IEC 27001:2022, tales como la gestión de eventos de seguridad, la protección contra malware, el control de acceso y la auditoría de registros [75].
- Detección basada en comportamiento y en firmas, utilizando herramientas como Suricata, Fail2Ban y Wazuh, alineadas con el marco MITRE ATT&CK [43].
- Políticas y procedimientos institucionales que aseguren el cumplimiento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), la LFPDPPSJ y la NOM-151-SCFI-2016 [19].

7. Resultados

La implementación del prototipo del Centro de Operaciones de Seguridad en la Universidad Autónoma de Ciudad Juárez representa un hito estratégico en la evolución de la ciberseguridad institucional. Los resultados obtenidos reflejan avances sustanciales tanto en el diseño tecnológico como en el fortalecimiento organizacional. Estos logros han sentado las bases para la maduración progresiva del ***SOC***, promoviendo una cultura de seguridad proactiva, colaborativa y alineada a estándares internacionales. A continuación, se detallan los principales resultados alcanzados.

7.1. Diseño de la arquitectura del SOC.

Se estableció una arquitectura técnica robusta y escalable, basada en tecnologías de código abierto, que permite la recolección, correlación, análisis y visualización de eventos de seguridad. Esta arquitectura facilita la integración de activos críticos y habilita las capacidades avanzadas de detección, respuesta y monitoreo continuo, véase Anexo 11.

7.2. Análisis de riesgos.

Con base en la metodología NIST SP 800-30, se realizó un análisis de riesgos institucionales que permitió identificar y categorizar vulnerabilidades, amenazas y activos prioritarios. Esta evaluación orientó la priorización de controles y configuraciones en el ***SOC*** y sirvió de base para establecer políticas técnicas de protección.

7.3. Acuerdo de Nivel de Servicio (SLA).

Se definieron indicadores clave de desempeño (KPIs) y tiempos de respuesta esperados mediante un Acuerdo de Nivel de Servicio para el ***SOC***. Este SLA garantiza compromisos claros de monitoreo, atención y escalamiento de incidentes, lo que formaliza la operación del ***SOC*** en el contexto institucional; véase el Anexo 16.

7.4. Wazuh como plataforma EDR.

Se implementó Wazuh como solución central de detección y respuesta en endpoints (EDR), lo que permite el monitoreo detallado de sistemas operativos, servicios, autenticaciones y cambios en la integridad de archivos. Esta herramienta ha demostrado ser efectiva para identificar de manera temprana amenazas internas y externas. Es deseable que, como parte de las nuevas etapas en la Jefatura de Función de Ciberseguridad, se realicen las configuraciones correspondientes para que Wazuh pase de ser un EDR a un XDR con las capacidades de respuesta necesarias para brindar esa capa extra de seguridad que necesita la UACJ.

7.5. Elastic Stack como sistema SIEM.

La integración con Elastic Stack (Elasticsearch, Logstash y Kibana) ha proporcionado capacidades avanzadas para la recopilación, el almacenamiento y la visualización de logs. Este componente de SIEM permite realizar análisis forenses, detectar patrones anómalos y generar alertas personalizadas que fortalecen la respuesta operativa (ver el Anexo 6).

7.6. Greenbone como herramienta de identificación de vulnerabilidades.

Se incorporó Greenbone (basado en OpenVAS) como motor de escaneo de vulnerabilidades. Su uso ha facilitado la identificación de configuraciones inseguras, servicios expuestos y aplicaciones obsoletas en servidores y dispositivos de red (ver el Anexo 7).

7.7. Instancia de MISP para el intercambio de inteligencia sobre amenazas.

Se desplegó una instancia local de MISP (Malware Information Sharing Platform) como repositorio de indicadores de compromiso (IoCs) y de eventos de inteligencia de amenazas. Esta plataforma permite automatizar la aplicación de reglas de detección, compartir hallazgos con otras instituciones y anticiparse a campañas maliciosas.

7.8. Certificado Premio Internacional Metared TIC 2025.

Se presentó un resumen de este trabajo como propuesta de participación en los Premios Metared TIC, con el cual obtuvo el primer lugar en la categoría de Ciberseguridad. Con lo cual se motivó a más IES a implementar este sistema como parte de su postura de ciberseguridad, ofreciendo también asesorías sobre la implementación rápida y la adaptación de la arquitectura propuesta a su propio ecosistema tecnológico; véase Anexo 12.

7.9. Reconocimiento por campaña de concientización.

Como resultado de las acciones paralelas de concientización impulsadas desde el SOC, la universidad obtuvo el "Reconocimiento C3!Cyber" en dos ocasiones por su campaña institucional de concientización en ciberseguridad. Esta distinción valida el impacto positivo de la sensibilización en la comunidad universitaria y refuerza el componente educativo del proyecto, véase Anexo 13.

7.10. Colaboración con instituciones externas.

El proyecto promovió el acercamiento a otras universidades y organizaciones nacionales e internacionales, con las cuales se han establecido canales de colaboración para el intercambio de inteligencia, de buenas prácticas y de mecanismos conjuntos de defensa cibernética.

7.11. Consolidación de un nuevo equipo de trabajo.

Uno de los logros más significativos fue la conformación de un nuevo equipo de trabajo comprometido con la visión del **SOC**. Este equipo, integrado por personal técnico de diversas áreas, ha mostrado una disposición constante para capacitarse, certificarse y mantenerse actualizado en materia de ciberseguridad, lo que ha fomentado una cultura operativa resiliente y colaborativa.

En conjunto, estos resultados consolidan al SOC-UACJ como un modelo funcional, replicable y en crecimiento, que contribuye a la defensa institucional y promueve el desarrollo de capacidades técnicas internas sostenibles.

8. Conclusiones

Esta sección se incluye como requisito para el presente documento, aunque en esencia se lograron las metas establecidas, no significa que el proyecto en realidad concluyó. Como resultado del aprendizaje, se constató que la ciberseguridad es una rama de la ciencia en constante evolución. Por tal motivo, no se puede dar por hecho que el trabajo de instauración y definición de un ***SOC*** haya alcanzado su punto final.

8.1. Reflexión crítica.

La experiencia adquirida durante el posgrado permitió articular una solución integral de ciberseguridad que consideró tanto los aspectos técnicos como los estratégicos. El enfoque multidisciplinario fue determinante para tomar decisiones basadas en evidencia, adaptar herramientas de código abierto al entorno institucional y diseñar un sistema sostenible.

8.2. Recomendaciones para futuros desarrolladores de SOC.

Tras la implementación y validación del prototipo funcional del **SOC-UACJ**, se identifican áreas estratégicas que permitirán elevar el nivel de madurez tecnológica de la institución. Se proponen las siguientes recomendaciones para los desarrolladores y administradores que continúen con la evolución del centro:

Adopción de la Filosofía DevSecOps para la Seguridad de Aplicaciones.

Si bien el alcance actual del proyecto se centró primordialmente en la infraestructura de red y sistemas operativos, la seguridad institucional depende críticamente de sus portales web y sistemas escolares. Se recomienda implementar prácticas de **DevSecOps** que permitan al ***SOC*** monitorear el ciclo de vida de desarrollo de software interno.

- **Monitoreo de Aplicaciones:** Trascender el análisis de registros de red para incluir la detección de vulnerabilidades en el código y comportamientos anómalos en las aplicaciones institucionales.

- **Seguridad Continua:** Integrar herramientas de análisis estático (**SAST**) y dinámico (**DAST**) que alimenten automáticamente el **SIEM**, permitiendo al ***SOC*** identificar debilidades antes de que las aplicaciones pasen a producción.

Evolución de TheHive hacia una capacidad SOAR completa.

El prototipo actual utiliza **TheHive** como gestor de incidentes durante la fase de despliegue. No obstante, para optimizar los tiempos de respuesta y reducir la carga operativa del personal, es imperativo evolucionar esta instancia hacia una plataforma de **Orquestación, Automatización y Respuesta de Seguridad (SOAR)**.

- **Implementación de Playbooks:** Se sugiere desarrollar flujos de trabajo automatizados que permitan al sistema realizar acciones de contención inmediatas.
- **Respuesta automatizada:** Integrar **TheHive** con **Wazuh** y otros equipos de contención (como los firewalls Sophos XGS) para que, ante la detección de un incidente crítico, el sistema pueda aislar hosts o bloquear direcciones IP maliciosas sin intervención manual inicial.
- Invertir en capacitación continua en herramientas open source y en estándares globales.
- Priorizar la automatización como pilar para la escalabilidad y la reducción de errores.
- Fomentar la integración entre los equipos técnicos y normativos para garantizar el cumplimiento.
- Aplicar principios de la ciencia de datos para enriquecer los procesos de monitoreo y de toma de decisiones.

Además de estas recomendaciones, se considera continuar con la colaboración interinstitucional; como proyecto futuro, se prevé la creación de una fuente de inteligencia de amenazas cibernéticas que considere, en primera instancia, los riesgos integrales como organización y, posteriormente, se integre con la localidad y se afiance a nivel nacional.

8.3. Conclusión.

La implementación del ***SOC*** no habría sido posible sin la integración efectiva del conocimiento adquirido durante la Maestría. Las competencias desarrolladas en cómputo

aplicado, ciberseguridad y análisis de datos proporcionaron las bases para construir una solución moderna, adaptable y alineada con las exigencias actuales del ciberespacio. La colaboración entre las diferentes áreas de la **DGTI** proporcionó un nivel de transparencia y comunicación que facilitó enormemente el desarrollo del presente proyecto.

Aunque el tiempo para el desarrollo de la tesis ha sido mucho mayor de lo previsto, se entiende que ello se debe a la complejidad de analizar la infraestructura tecnológica de la **UACJ**. El avance constante y el crecimiento, la modernización y los cambios organizacionales representaron un reto y, en su momento, una amenaza para la continuidad del proceso de desarrollo del proyecto.

Finalmente, el SOC-UACJ se consolida como una base sólida y evolutiva que permite a la universidad enfrentar los desafíos del ciberespacio con una postura proactiva y resiliente. Al integrar la excelencia técnica con el compromiso ineludible de proteger los datos de la comunidad universitaria, este proyecto asegura que la infraestructura institucional opere en un marco de integridad y confianza absolutos. Con esta implementación, la UACJ no solo fortalece su defensa operativa, sino que también reafirma su posición como referente en seguridad de la información y en transparencia en el ámbito académico nacional.

Referencias bibliográficas

[1] M. De la Vega y Al. Et, *Introducción al cómputo en la nube*. México, 2016. Consultado: el 14 de agosto de 2022. [En línea]. Disponible en: https://iibi.unam.mx/archivistica/InterPARES_8_020617.pdf

[2] C. Kraft, "What Is SaaS and How Can It Help Build Our Profession?", *JOURNALOF GOVERNMENT FINANCIAL MANAGEMENT*, vol. 68, núm. 2, pp. 26–31, 2018, Consultado: el 14 de febrero de 2023. [En línea]. Disponible en: https://www.proquest.com/openview/4e91ed1ce91929c6b258c0b791cc650b/1?cbl=26015&pq-origsite=gscholar&parentSessionId=9FLg7N2CAB5PVRXJWd8bwHGf9gKddPleKxylfEpgHs4%3D

[3] P. Saripalli y B. Walters, "QUIRC: A quantitative impact and risk assessment framework for cloud security", en *Proceedings - 2010 IEEE 3rd International Conference on Cloud Computing, CLOUD 2010*, 2010, pp. 280–288. doi: 10.1109/CLOUD.2010.22.

[4] A. Shameli-Sendi, R. Aghababaei-Barzegar, y M. Cheriet, "Taxonomy of Information Security Risk Assessment (ISRA)", *Computer & Security*, vol. 57, pp. 14–30, mar. 2016, doi: https://doi.org/10.1016/j.cose.2015.11.001.

[5] Devo, "2022 Devo SOC Performance Report ™", 2022. [En línea]. Disponible en: www.wakefieldresearch.com

[6] NIST, "Security and Privacy Controls for Information Systems and Organizations", Gaithersburg, MD, sep. 2020. doi: 10.6028/NIST.SP.800-53r5.

[7] R. Ross, V. Pillitteri, K. Dempsey, M. Riddle, y G. Guissanie, "Protecting controlled unclassified information in nonfederal systems and organizations", Gaithersburg, MD, feb. 2020. doi: 10.6028/NIST.SP.800-171r2.

[8] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, y R. McQuaid, "Developing Cyber-Resilient Systems":, Gaithersburg, MD, dic. 2021. doi: 10.6028/NIST.SP.800-160v2r1.

[9] R. C. Cabrera Jurado y L. C. Agüero Herrera, "Planificación de un SIEM para la red de la UACJ y desarrollo virtual de un IDS", Tesis, Universidad Autónoma de Ciudad Juárez, Juárez, Chihuahua, 2015. Consultado: el 30 de enero de 2023. [En línea]. Disponible en: http://erecursos.uacj.mx/handle/20.500.11961/2915

[10] L. Tao, "A DATA TRIAGE RETRIEVAL SYSTEM FOR CYBER SECURITY OPERATIONS CENTER", 2018.

[11] C. and Y. J. and L. P. Lin Tao and Zhong, "Retrieval of Relevant Historical Data Triage Operations in Security Operation Centers", en *From Database to Cyber Security: Essays Dedicated to Sushil Jajodia on the Occasion of His 70th Birthday*, I. and R. I. Samarati Pierangela and Ray, Ed., Cham: Springer International Publishing, 2018, pp. 227–243. doi: 10.1007/978-3-030-04834-1_12.

[12] M. Vielberth, F. Bohm, I. Fichtinger, y G. Pernul, "Security Operations Center: A Systematic Study and Open Challenges", *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3045514.

[13] E. Agyepong, Y. Cherdantseva, P. Reinecke, y P. Burnap, "Challenges and performance metrics for security operations center analysts: a systematic review", *Journal of Cyber Security Technology*, vol. 4, núm. 3, pp. 125–152, 2020, doi: 10.1080/23742917.2019.1698178.

[14] Kaspersky, "CYBERTHREAT REAL-TIME MAP". Consultado: el 14 de febrero de 2023. [En línea]. Disponible en: https://cybermap.kaspersky.com/

[15] ISOTools Excellence, "Seguridad de la información", https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/.

[16] Normas ISO, "ISO 27001 SEGURIDAD DE LA INFORMACIÓN", https://www.normas-iso.com/iso-27001/.

[17] Cámara De Diputados, *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*. Mexico.

[18] H. Congreso de la Unión, “LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES”, vol. 1, pp. 1–16, mar. 25d. C., Consultado: el 21 de marzo de 2025. [En línea]. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf
[19] Instituto Nacional de Transparencia (INAI), “Guía para el cumplimiento de la Ley Federal de Protección de Datos Personales”, https://home.inai.org.mx/.
[20] S. Rose, O. Borchert, S. Mitchell, y S. Connelly, “NIST Special Publication 800-207 Zero Trust Architecture”, doi: 10.6028/NIST.SP.800-207.
[21] D. Hernández, “DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN”, vol. 1, núm. 1, 2011, Consultado: el 15 de abril de 2023. [En línea]. Disponible en: https://repository.unilibre.edu.co/bitstream/handle/10901/9097/PROYECTO%20FINAL.pdf?sequence=1
[22] G. Michael, “DESIGN AND IMPLEMENTATION OF A SECURE CAMPUS NETWORK”. [En línea]. Disponible en: http://www.ijpam.eu
[23] G. Singh y Dr. M. Garg, “Data Security In Cloud Computing: A Review”, *INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY*, vol. 17, núm. 2, pp. 7206–7214, jul. 2018, doi: 10.24297/ijct.v17i2.7551.
[24] J. Camargo, “Diseno de un sistema de gestion de seguridad de la informacion SGSI”, p. 119, 2017, Consultado: el 15 de abril de 2023. [En línea]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/11992/75104100.pdf;jsessionid=6030BA8509C9F80DC17A7764620C2BE0?sequence=1
[25] N. Memon, M. S. Vighio, Y. Muhammad, y Z. H. Abro, “Fault Tolerance Framework for Composite Web Services”, *IEEE Access*, vol. 9, pp. 95469–95480, 2021, doi: 10.1109/ACCESS.2021.3094980.
[26] D. V. S. Kaja, Y. Fatima, y A. B. Mailewa, “Data Integrity Attacks in Cloud Computing: A Review of Identifying and Protecting Techniques”, *International Journal of Research Publication and Reviews*, pp. 713–720, feb. 2022, doi: 10.55248/gengpi.2022.3.2.8.
[27] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, y E. Akin, “A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions”, *Electronics (Basel).*, vol. 12, núm. 6, p. 1333, mar. 2023, doi: 10.3390/electronics12061333.
[28] J. Mirkovic y P. Reiher, “A taxonomy of DDoS attack and DDoS defense mechanisms”, abril de 2004. doi: 10.1145/997150.997156.
[29] M. Humpiri, “Revisión sistemática: vulnerabilidades de seguridad cibernética en los activos digitales”, *Ñawparisun - Revista de Investigación Científica*, vol. 2, núm. Vol. 4, Num. 2, pp. 93–100, may 2023, doi: 10.47190/nric.v4i2.250.
[30] M. Díaz, “DATOS INTEGRADOS A LA HERRAMIENTA POWER BI PARA LA EMPRESA TELEFÓNICA TECH MARIA CAMILA DIAZ HOYOS AUTOR UNIVERSIDAD COOPERATIVA DE COLOMBIA FACULTAD INGENIERÍA PROGRAMA INGENIERÍA DE TELECOMUNICACIONES BOGOTÁ 2024”, 2024. Consultado: el 15 de octubre de 2024. [En línea]. Disponible en: https://repository.ucc.edu.co/server/api/core/bitstreams/58a6bc58-562c-4e96-8e3a-5ce7c3091ef4/content
[31] O. Cossio, “VULNERABILIDADES DE CIBERSEGURIDAD EN SISTEMAS DE CONTROL INDUSTRIAL Y ACCESIBILIDAD A TRAVÉS DE REDES PÚBLICAS”, Universidad Nacional del Nordeste , Argentina. Consultado: el 18 de marzo de 2023. [En línea]. Disponible en: https://repositorio.unne.edu.ar/handle/123456789/28453
[32] M. Oiner *et al.*, “Model log management for the audit information, to support decision making in the organizations”, 2012. [En línea]. Disponible en: http://scielo.sld.cu
[33] T. Weiss, “Las 7 herramientas para el manejo de logs (registros) que todo desarrollador Java debe conocer”, https://www.overops.com/blog/las-7-herramientas-para-el-manejo-de-logs-registros-que-todo-desarrollador-java-debe-conocer/.
[34] Elastic, “Elasticsearch”, https://www.elastic.co/es/what-is/elasticsearch.
[35] Elastic, “Logstash”, https://www.elastic.co/es/logstash/.
[36] Elastic, “Kibana”, https://www.elastic.co/es/kibana/.

[37] Fluentd Project, “Fluentd”, https://www.fluentd.org/.
[38] Graylog, “Graylog”, https://www.graylog.org/.
[39] Splunk, “Splunk”, https://www.splunk.com/.
[40] NXLog FZE, “NxLog”. Consultado: el 9 de julio de 2024. [En línea]. Disponible en: https://nxlog.co/
[41] J. Frank, “Your Next Move: Threat Intelligence Analyst”, https://www.comptia.org/blog/your-next-move-threat-intelligence-analyst.
[42] D. P. F. Möller, “Threats and Threat Intelligence”, en *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices*, D. P. F. Möller, Ed., Cham: Springer Nature Switzerland, 2023, pp. 71–129. doi: 10.1007/978-3-031-26845-8_2.
[43] Mitre Corporation, “MITRE ATT&CK”, https://attack.mitre.org/.
[44] Mitre Corporation, “MITRE Cyber Analytics Repository”. Consultado: el 1 de octubre de 2023. [En línea]. Disponible en: https://car.mitre.org/
[45] Mitre Corporation, “Mitre Engage”. Consultado: el 1 de octubre de 2023. [En línea]. Disponible en: https://engage.mitre.org/
[46] Mitre Corporation, “Mitre Defend”. Consultado: el 1 de octubre de 2023. [En línea]. Disponible en: https://d3fend.mitre.org/
[47] Mitre Corporation, “Mitre AEP”. Consultado: el 1 de octubre de 2023. [En línea]. Disponible en: https://attack.mitre.org/resources/adversary-emulation-plans/
[48] Lockheed Martin Corporation., “The Cyber Kill Chain”. Consultado: el 12 de octubre de 2023. [En línea]. Disponible en: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
[49] TryHackMe, “Cyber Kill Chain”. Consultado: el 12 de octubre de 2023. [En línea]. Disponible en: https://tryhackme.com/r/room/cyberkillchainzmt
[50] INCIBE y A. Martínez, “OSINT”. Consultado: el 12 de octubre de 2023. [En línea]. Disponible en: https://www.incibe.es/incibe-cert/blog/osint-la-informacion-es-poder
[51] J. Boyens, A. Smith, N. Bartol, K. Winkler, A. Holbrook, y M. Fallon, “Withdrawn NIST Technical Series Publication Warning Notice Withdrawn Publication Series/Number NIST SP 800-161r1 Title Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations Publication Date(s) Superseding Publication(s) (if applicable) Series/Number NIST SP 800-161r1-upd1 Title Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations Additional Information (if applicable)”, 2022, doi: 10.6028/NIST.SP.800-161r1-upd1.
[52] P. Kaur y N. Misra, “A Methodical Review on Network traffic monitoring and Analysis tools”, 2019. [En línea]. Disponible en: https://www.researchgate.net/publication/337481341
[53] Kaspersky, “https://latam.kaspersky.com/resource-center/threats/what-is-a-honeypot”.
[54] G. Verdejo Alvarez, “CAPITULO 4 Honeypots y Honeynets”. [En línea]. Disponible en: http://tau.uab.es/~gaby
[55] International Organization for Standardization, *Information technology - Security techniques - Information security management systems - Requirements*. Switzerland: https://www.iso.org/standard/27001, 2013.
[56] Trustwave y K. Daniels, “Evolution of the SOC”. Consultado: el 26 de febrero de 2023. [En línea]. Disponible en: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/evolution-of-the-soc-from-the-dark-ages-to-enlightenment-shifting-to-an-agile-threat-informed-cyber-defense-program/
[57] H. B, A. Abdi, Md. I. Hossain, y A. Pujol, *The Role of SOC in Ensuring the Security of IoT Devices: A Review of Current Challenges and Future Directions*. 2023. doi: 10.1109/MECO58584.2023.10155021.
[58] Wikipedia contributors, “Security Operations Center”. Consultado: el 2 de marzo de 2023. [En línea]. Disponible en: https://en.wikipedia.org/wiki/Security_operations_center
[59] S. Maheshwaram, “A Study on Security Information and Event Management (SIEM)”, vol. 5, pp. 705–708, mar. 2018.

[60] H. J. Liao, C. H. Richard Lin, Y. C. Lin, y K. Y. Tung, “Intrusion detection system: A comprehensive review”, enero de 2013. doi: 10.1016/j.jnca.2012.09.004.
[61] T. Tafazzoli y H. G. Garakani, “Security operation center implementation on OpenStack”, en *2016 8th International Symposium on Telecommunications (IST)*, 2016, pp. 766–770. doi: 10.1109/ISTEL.2016.7881927.
[62] M. Swanson, P. Bowen, A. W. Phillips, D. Gallup, y D. Lynes, “Contingency Planning Guide for Federal Information Systems”, doi: 10.6028/NIST.SP.800-34r1.
[63] J. , A. Sarraipa y J. H. A, “Metodología de Evaluación de Prototipo Innovador”, Lisboa, 2019. Consultado: el 20 de marzo de 2023. [En línea]. Disponible en: https://acacia.red/wp-content/uploads/2019/07/Gu%C3%ADa-Metodologi%CC%81a-de-evaluaci%C3%B3n-de-prototipo-innovador.pdf
[64] R. Pressman y B. Maxim, *Software Engineering: A Practitioner’s Approach, 8th Ed*. 2014.
[65] Ian. Sommerville, *Ingeniería del software*, 7ma ed. Madrid: Addison-Wesley, 2005.
[66] K. Schwaber and J. Sutherland., “The Scrum Guide”, https://scrumguides.org/.
[67] Wazuh, “Wazuh Documentation”, https://documentation.wazuh.com/.
[68] Greenbone Networks, “OpenVAS – Open Vulnerability Assessment Scanner”, https://www.greenbone.net/en/product/openvas/.
[69] Julian. N. Ruseel, “NQA-ISO-27001-Guia-de-implantacion”.
[70] A. Cavoukian, “Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices”, 2012, Consultado: el 22 de abril de 2026. [En línea]. Disponible en: www.privacybydesign.ca
[71] S. Rose, O. Borchert, S. Mitchell, y S. Connelly, “NIST Special Publication 800-207 Zero Trust Architecture”, doi: 10.6028/NIST.SP.800-207.
[72] J. Sarraipa y A. Artificie, “Metodología de Evaluación de Prototipo Innovador”, Lisboa, 2019. Consultado: el 10 de mayo de 2024. [En línea]. Disponible en: https://acacia.red/wp-content/uploads/2019/07/Gu%C3%ADa-Metodologi%CC%81a-de-evaluaci%C3%B3n-de-prototipo-innovador.pdf
[73] J. Andress y S. Winterfeld, “The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice: Second Edition”, pp. 1–217, may 2014.
[74] Suricata, “Who we are”, https://suricata.io/our-story/who-we-are/.
[75] ISO, “ISO 27001:2022”. Consultado: el 14 de octubre de 2023. [En línea]. Disponible en: https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27001:ed-3:v1:en
[76] Metared TIC by Universia, “Sello C3!Cyber”, https://www.metared.org/global/sello-c3-cyber.html.
[77] CUDI, “Acerca de CUDI”, https://cudi.edu.mx/acerca-de-cudi/acerca-de-cudi.
[78] CERN, “About CERN”, https://home.cern/about.
[79] Beck. Et. Al. Kent, “Manifesto for Agile Software Development”, https://agilemanifesto.org/.
[80] A. Toygar, C. E. T. Rohm, y J. Zhu, “A New Asset Type: Digital Assets”, *Journal of International Technology and Information Management*, vol. 22, núm. 4, nov. 2013, doi: 10.58729/1941-6679.1024.
[81] J. B. Ehlen, “Arrangement of Computing Assets in a Data Center”, US 20140355185A1, 2014 Consultado: el 23 de febrero de 2024. [En línea]. Disponible en: https://patents.google.com/patent/US20140355185A1/en
[82] Vainberg et al., “Computer monitoring, servicing, and management of remote equipment and assets”, US 20150.066782A1, 2015 Consultado: el 22 de febrero de 2024. [En línea]. Disponible en: https://patents.google.com/patent/US20150066782A1/en
[83] M. Swanson, P. Bowen, A. W. Phillips, D. Gallup, y D. Lynes, “Archived NIST Technical Series Publication Archived Publication Series/Number: Title: Publication Date(s): Withdrawal Date: Superseding Publication(s) NIST Special Publication 800-34 Contingency Planning Guide for Information Technology Systems Contingency Planning Guide for Federal Information Systems”, 2002, doi: 10.6028/NIST.SP.800-34r1.

[84] K. Kent y M. Souppaya, “Special Publication 800-92 Guide to Computer Security Log Management Recommendations of the National Institute of Standards and Technology”.
[85] R. Petersen, D. Santos, M. C. Smith, K. A. Wetzel, y G. Witte, “Workforce Framework for Cybersecurity (NICE Framework)”, Gaithersburg, MD, nov. 2020. doi: 10.6028/NIST.SP.800-181r1.
[86] JOINT TASK FORCE, “Security and Privacy Controls for Information Systems and Organizations”, Gaithersburg, MD, sep. 2020. doi: 10.6028/NIST.SP.800-53r5.
[87] SANS Institute, “Guide_To_Security_Operations”, pp. 1–63, sep. 23d. C..
[88] Manage Engine, “La guía ISO 20000”. Consultado: el 14 de octubre de 2023. [En línea]. Disponible en: https://download.manageengine.com/es/iso20000/images/iso-20000.pdf
[89] ENISA, “ENISA”. Consultado: el 14 de octubre de 2023. [En línea]. Disponible en: https://www.enisa.europa.eu/
[90] Docker, “Dockerdocs”, https://docs.docker.com/get-started/.
[91] Microsoft, “PowerShell”, https://learn.microsoft.com/es-es/training/modules/script-with-powershell/.
[92] A. Nelson, “Incident Response Recommendations and Considerations for Cybersecurity Risk Management”:, 2025. doi: 10.6028/NIST.SP.800-61r3.
[93] Elastic, “Kibana Guide”, https://www.elastic.co/guide/en/kibana/current/index.html.
[94] Scikit-learn, “User Guide”, https://scikit-learn.org/stable/user_guide.html.
[95] OTX Alien Vault, “Open Threat Exchange”, https://otx.alienvault.com/.
[96] Bitdefender, “¿Qué es un Exploit? Prevención de Exploits”. Consultado: el 1 de octubre de 2023. [En línea]. Disponible en: https://www.bitdefender.es/consumer/support/answer/22884/#:~:text=Un%20exploit%20es%20un%20software,usar%20algo%20en%20beneficio%20propio%E2%80%9D.

Anexos

Anexo 1: Nivel de Madurez de Ciberseguridad de la UACJ.

Visualizar el nivel de madurez del SOC-UACJ es fundamental para comprender su capacidad actual de prevención, detección, análisis y respuesta ante incidentes de seguridad. Esta visualización no solo permite identificar fortalezas y debilidades del sistema implementado, sino que también habilita una hoja de ruta para su evolución estratégica hacia un SOC institucional más sólido, automatizado y alineado con marcos internacionales como NIST, ISO/IEC 27001 y MITRE ATT&CK. Evaluar la madurez permite además establecer prioridades de inversión, justificar decisiones ante instancias directivas y garantizar que los esfuerzos en ciberseguridad estén alineados con las necesidades reales de la institución y su entorno de amenazas en constante transformación.

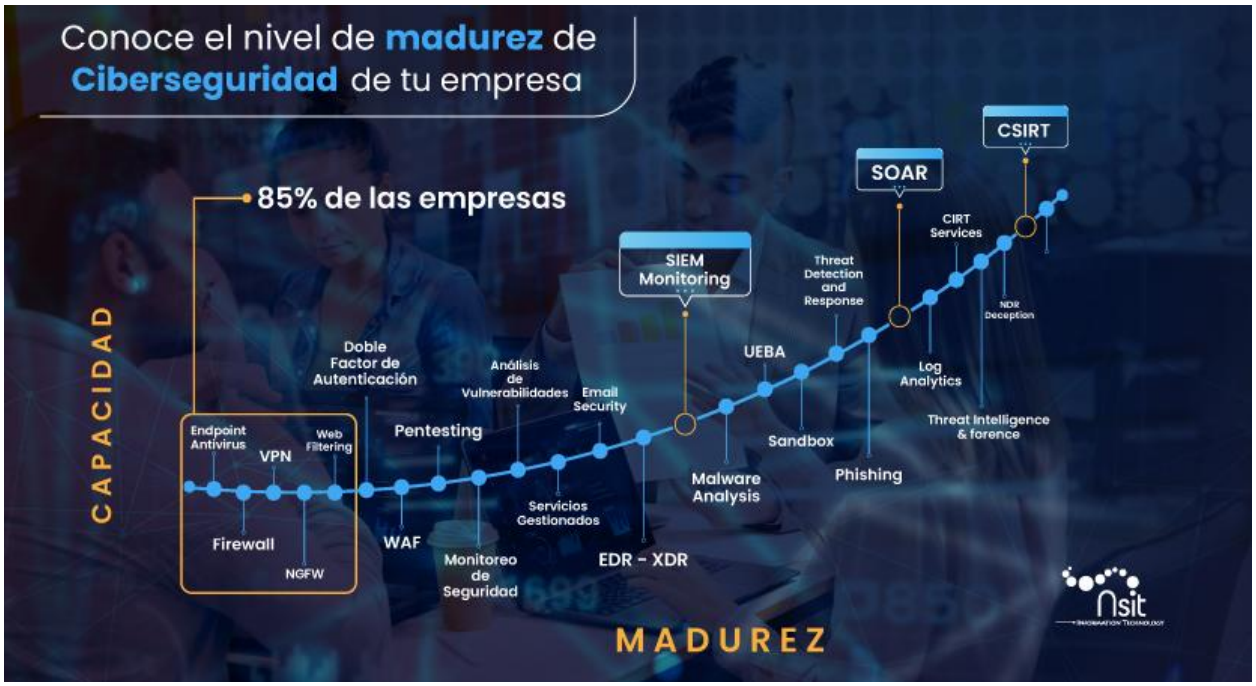


ILUSTRACIÓN 24. GRÁFICA DEL NIVEL DE MADUREZ DE CIBERSEGURIDAD DE LAS EMPRESAS (TOMADA DE INTERNET[10]).

Antivirus:

- Microsoft Defender (Endpoints y Servers)
- Sophos Intercept X (Servers)

Firewall:

- Firewall de Windows (Endpoints y servers)
- Firewall Lan Sophos XG 750 (a sustituirse por EoL)

[10] https://www.nsit.com.co/como-instaurar-una-cultura-de-ciberseguridad-en-mi-empresa-parte-1/

VPN:

- VPN pptp (Servidores)
- Sophos Remote Access para personal de la DGTI (IPsec, SSL VPN, L2TP y PPTP)
- VPN IPSec con pFsense para personal de la DGTI y funcionarios en movilidad internacional.

NGFW:

- Sophos NGF XGS 8500

Web Filtering:

- Sophos NGF XGS 8500 (Basado en políticas)

MFA:

- Con Officce 365 (No forzada)

Pentesting:

- Tenable, Nmap, Metasploit, Burp, Wireshark, Jacktheriper,SQLmap)

Monitoreo de Seguridad:

- SIEM (ELK)
- IDS/IPS (Sophos)
- Tráfico y administración de red (Wireshark y Nagios XI)
- Inteligencia de Amenazas (Sophos, Alien Vault, Polarity, Virus Total y SOC Radar)
- Wazuh
- Libre NMS (monitoreo de infraestructura de red)

Análisis de vulnerabilidades:

- Tenable (Nessus)
- Greenbone (Openvas)
- Wazuh

Servicios Gestionados:

- Sophos (Xtream Protection 8 x 5)

Email Sucurity:

- Con Officce 365.

XDR:

- Wazuh (en proceso)

Malware Analysis:

- Recolección y categorización (Virus Total)
- Análisis Estático (PEStudio)
- Análisis Dinámico (Any.Run)
- Ingeniería inversa (Ghidra)
- Monitoreo (Sysmon y Wireshark)

UEBA (User and Entity Behavior Analytics):

- Actualmente no (pero se pretende configurar Wazuh y ELK para aplicar modelos de IoB)

Sandbox:

- Any.Run
- Sophos Sandbox & Policy Test

Threat Detection and response:

- Wazuh XDR
- Elastic

Phishing:

- Filtrado y Bloqueo (Microsoft Defender de Officce 365)
- Análisis (Virus Total, PhishTank y URLScan.io)
- Concientización (Campaña vigente y próximamente campaña de Phishing)

SOAR:

- GLPI
- TheHIve (en despliegue)

Log Analysis:

- Elastic
- Wazuh
- Análisis manual de los de DNS (en despliegue pDNSSOC Unicorn)

CIRT Services:

- SOC - UACJ
- Colaboración con Universidades.
- Colaboración con Guardia Nacional (retomando).

Threat Intelligence and forense:

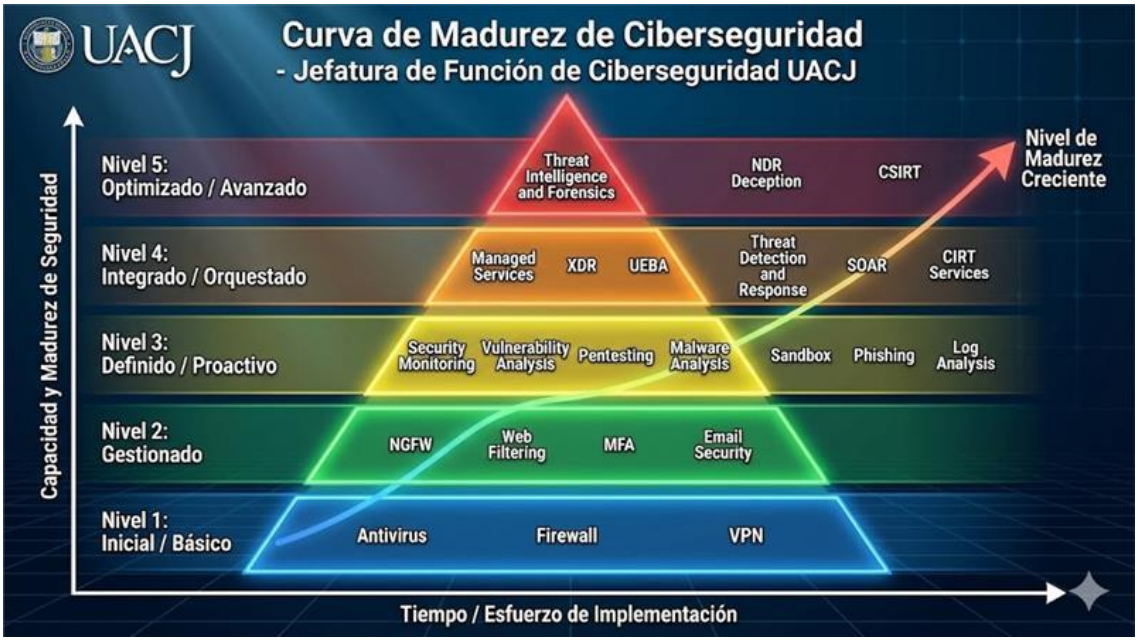
- Forense (CSI Linux)
- CTIS (próximamente, una fuente propia de inteligencia de amenazas).
- MISP con el CERN.

NDR Deception:

- Honeynet (por reubicar)

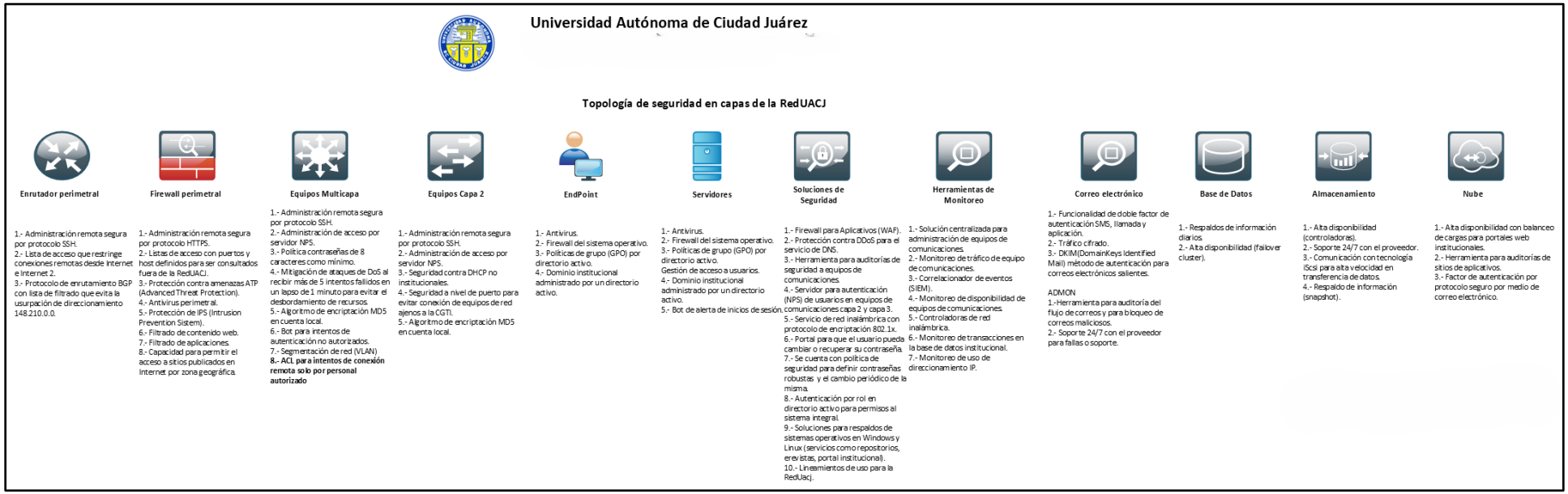
CSIRT:

- CSIRT – CUDI

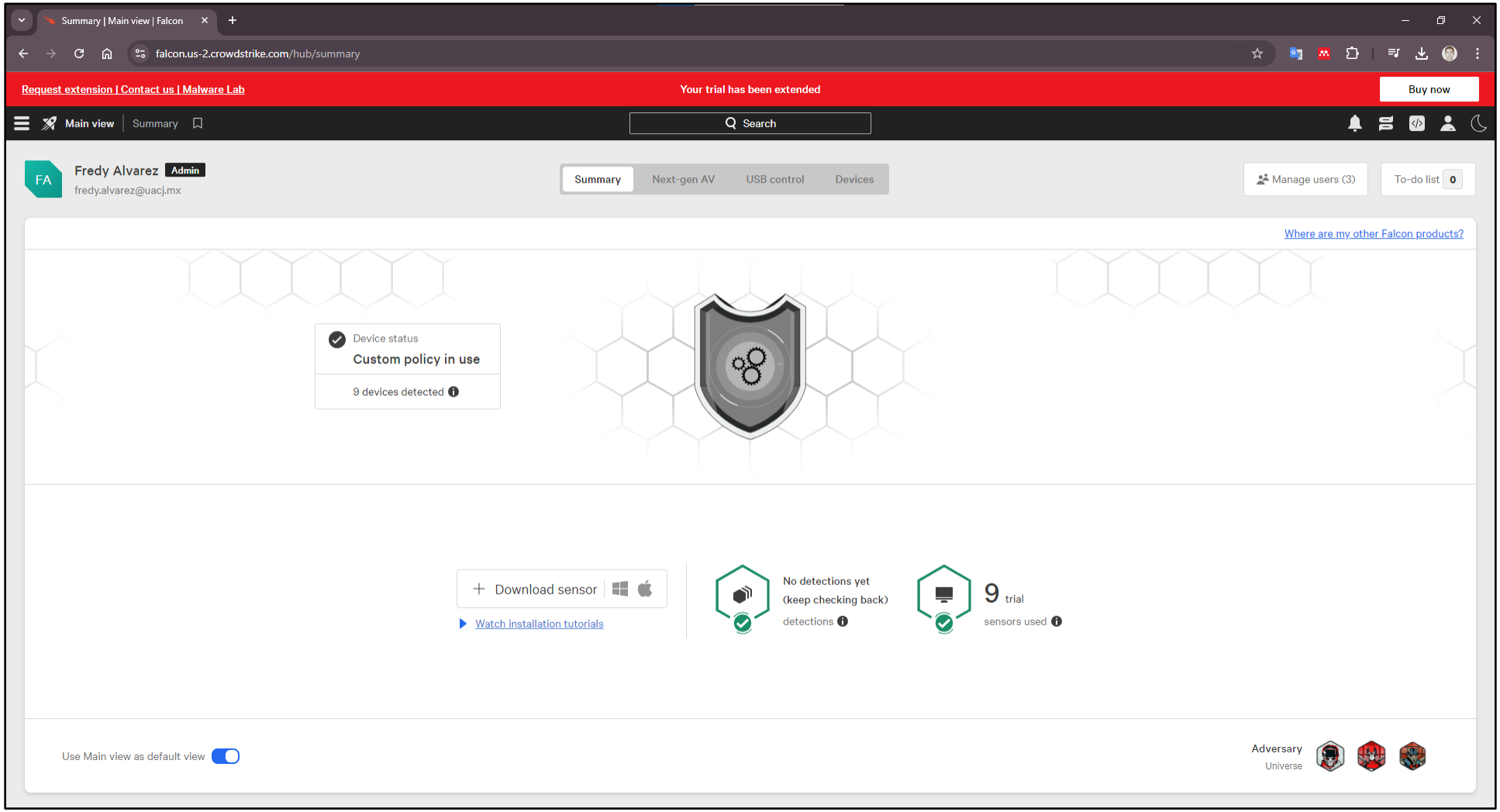


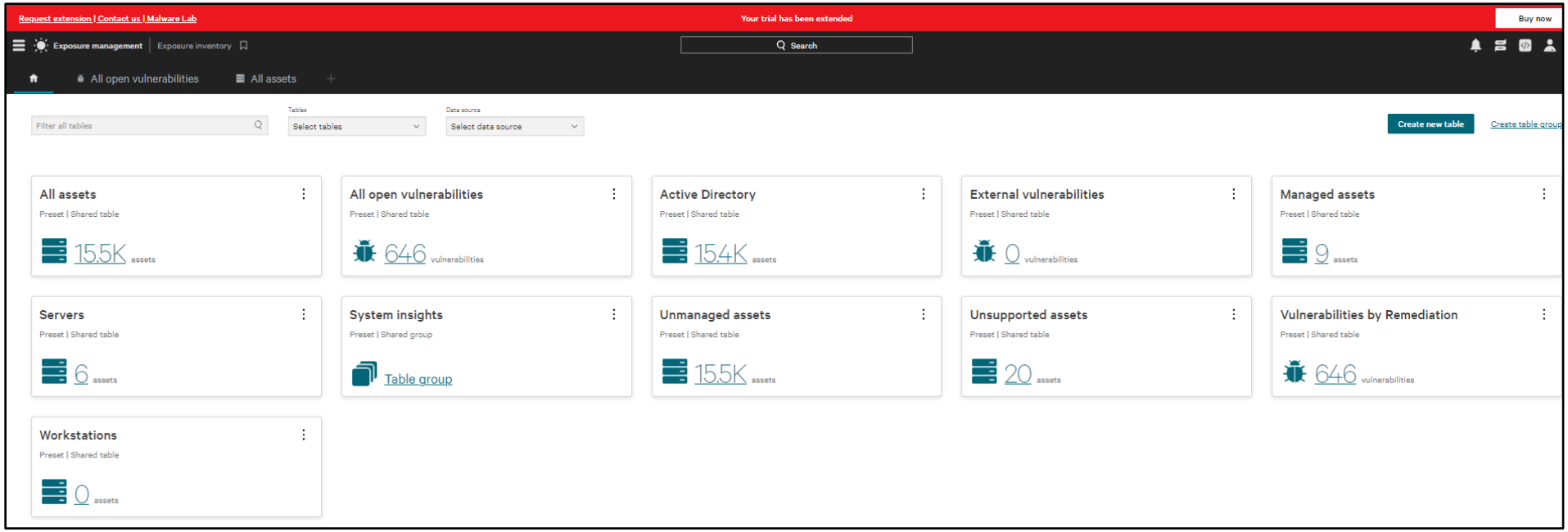
Anexo 2: Ejemplo de mensaje de la campaña de concientización de Ciberseguridad.

Anexo 3: Topología de Seguridad en capas diseñada por la Jefatura de Función de Seguridad Informática de la Red en 2023

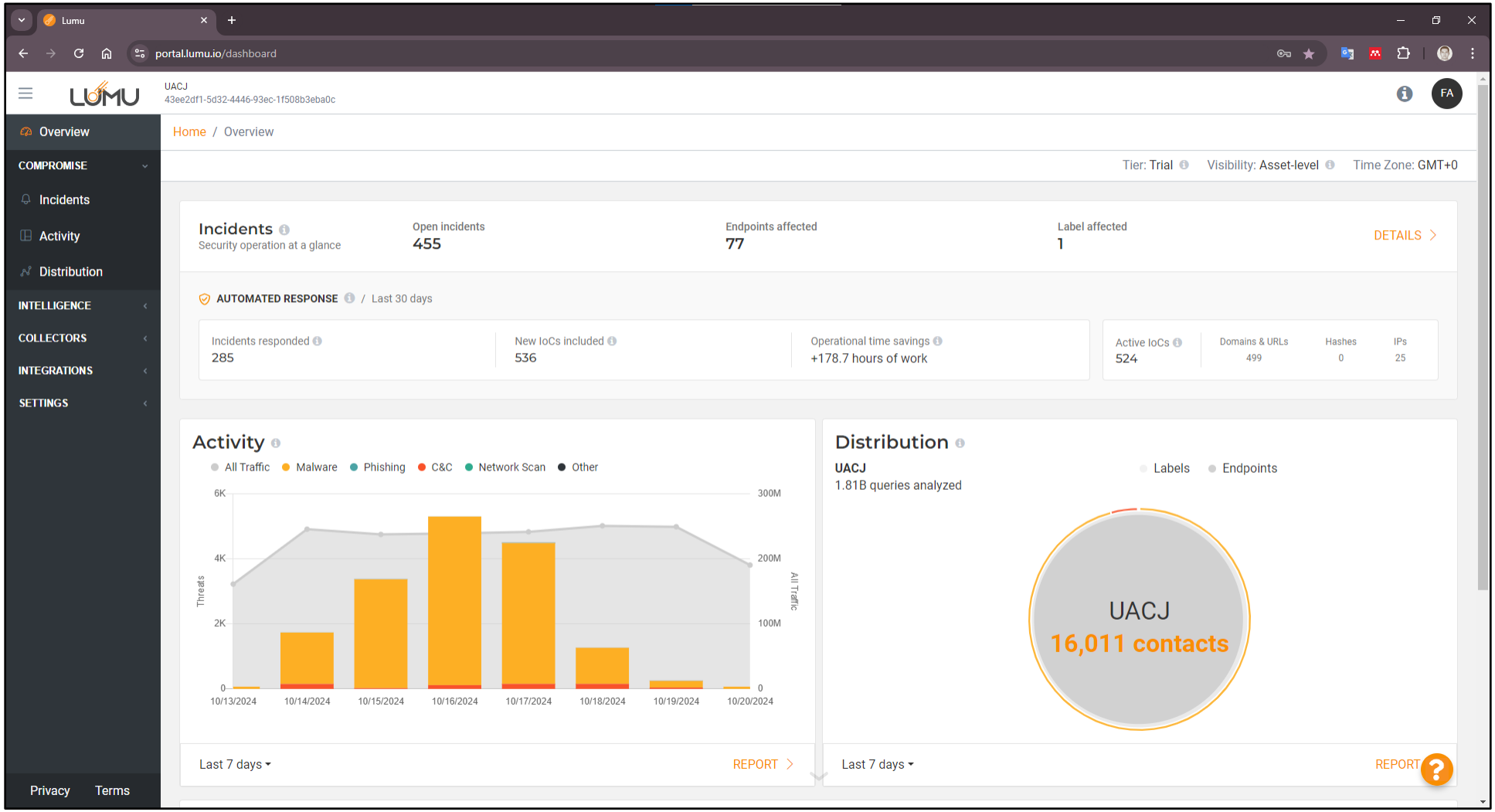


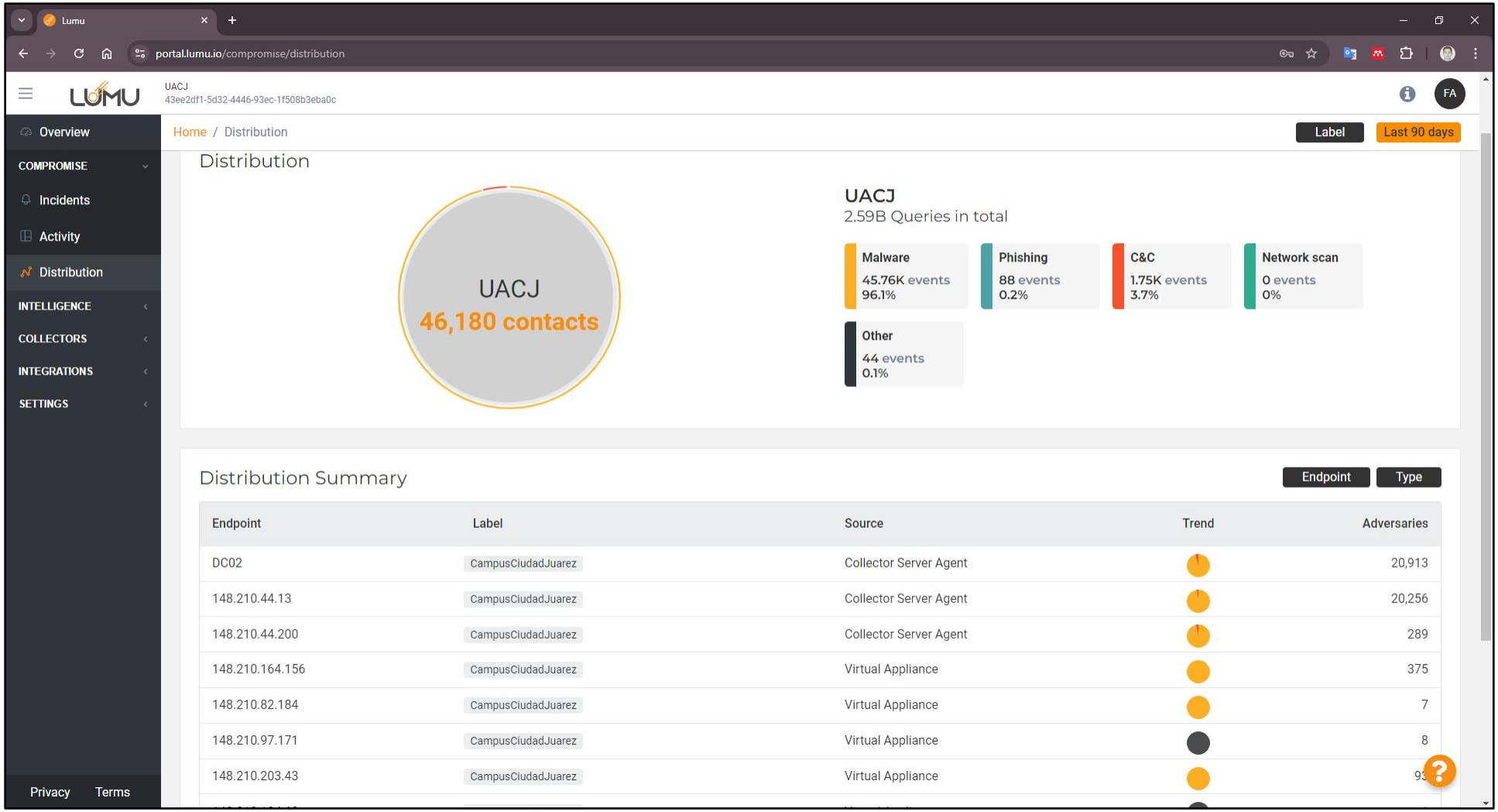
Anexo 4: Vista de la consola del NG – SIEM Falcon de Crowdstrike.



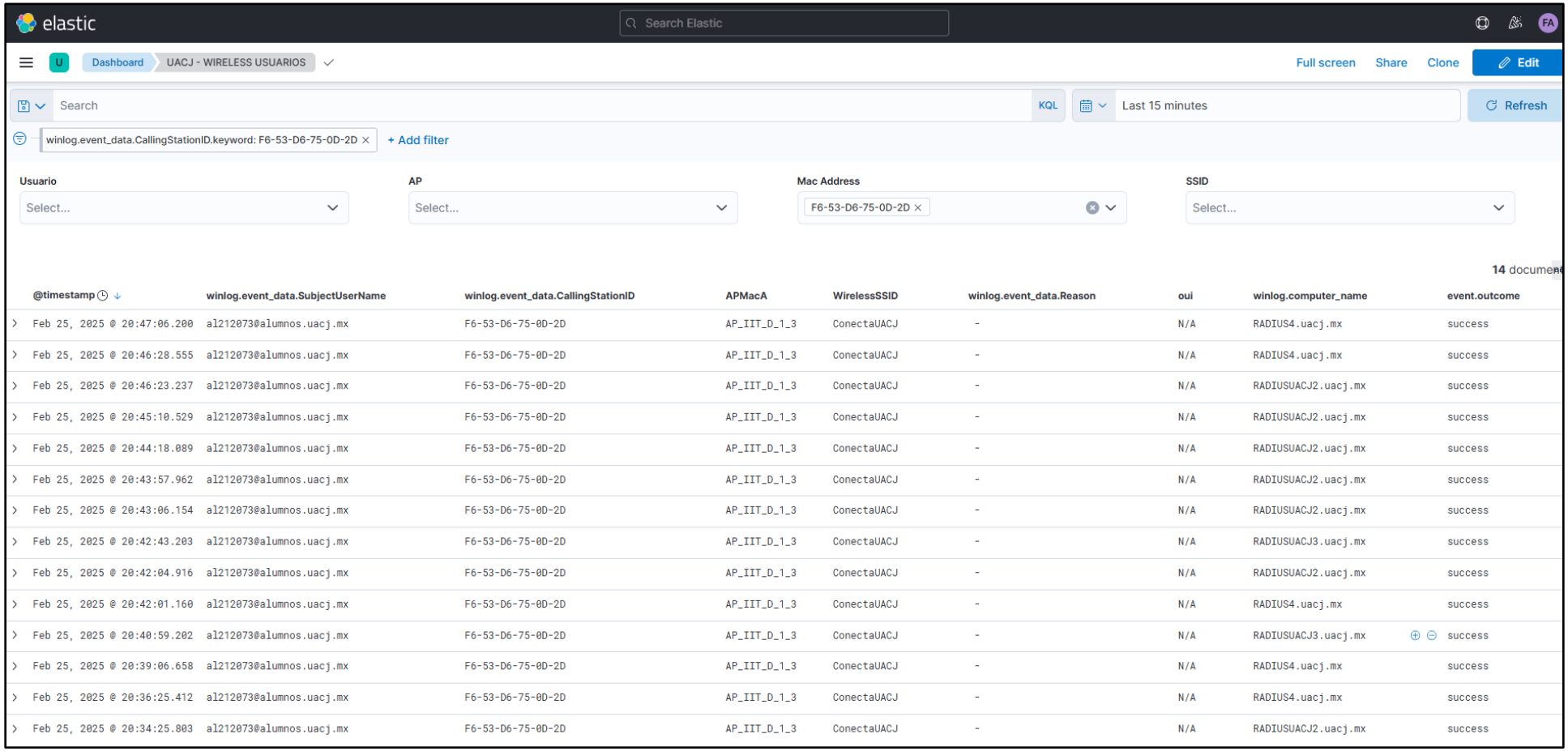

Request extension | Contact us | Malware Lab
Your trial has been extended
Buy now
Exposure management
Exposure inventory
Search
All open vulnerabilities
All assets
Filter all tables
Tables
Select tables
Data source
Select data source
Create new table
Create table group
All assets
Preset | Shared table
15.5K assets
All open vulnerabilities
Preset | Shared table
646 vulnerabilities
Active Directory
Preset | Shared table
15.4K assets
External vulnerabilities
Preset | Shared table
0 vulnerabilities
Managed assets
Preset | Shared table
9 assets
Servers
Preset | Shared table
6 assets
System insights
Preset | Shared group
Table group
Unmanaged assets
Preset | Shared table
15.5K assets
Unsupported assets
Preset | Shared table
20 assets
Vulnerabilities by Remediation
Preset | Shared table
646 vulnerabilities
Workstations
Preset | Shared table
0 assets

Anexo 5: Consola de la solución Lumu.



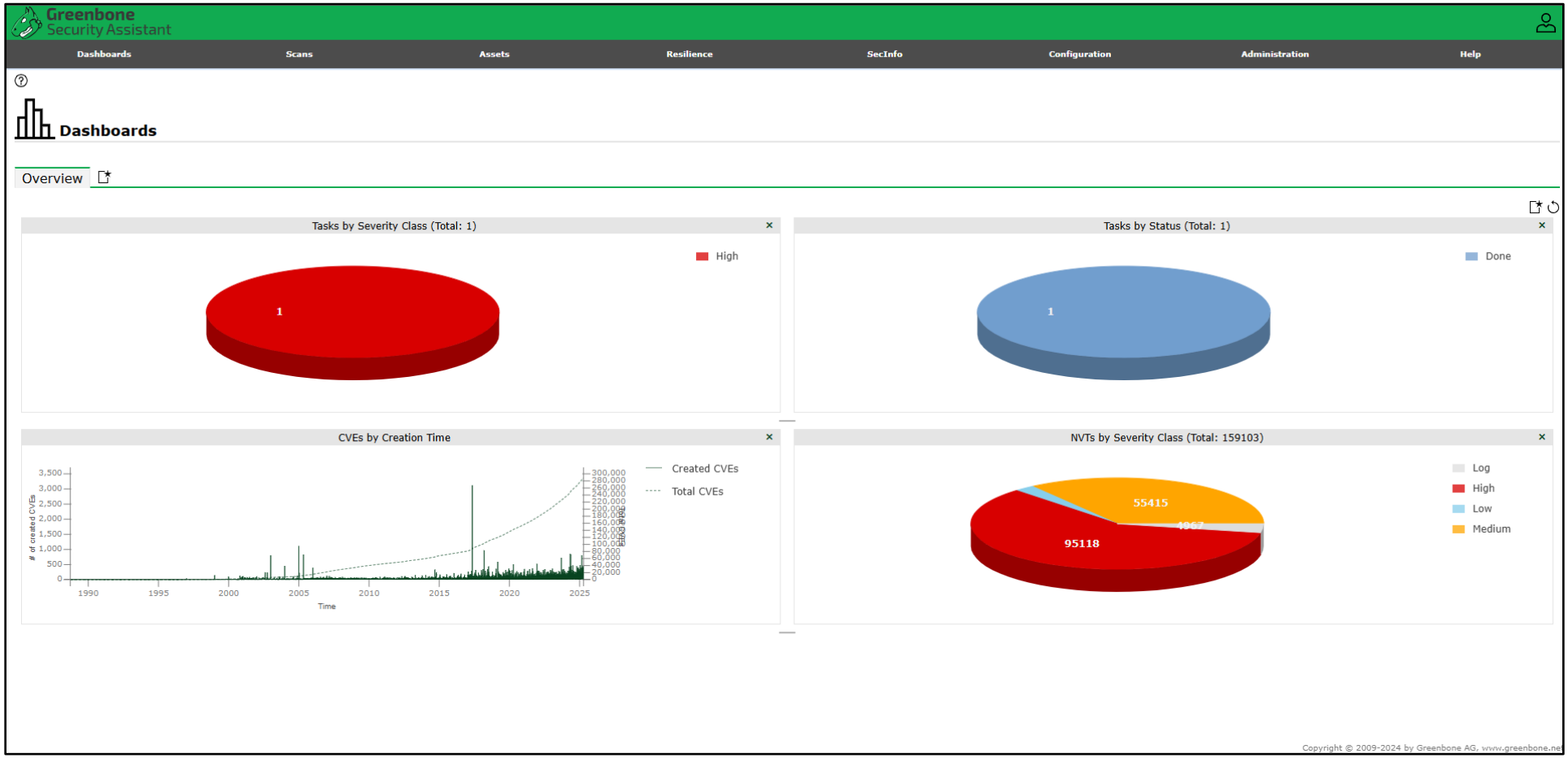

Lumu
portal.lumu.io/compromise/distribution
LUMU
UACJ
43ee2df1-5d32-4446-93ec-1f508b3eba0c
FA
Overview
COMPROMISE
Incidents
Activity
Distribution
INTELLIGENCE
COLLECTORS
INTEGRATIONS
SETTINGS
Privacy
Terms
Home / Distribution
Label
Last 90 days
Distribution
UACJ
46,180 contacts
UACJ
2.59B Queries in total
Malware
45.76K events
96.1%
Phishing
88 events
0.2%
C&C
1.75K events
3.7%
Network scan
0 events
0%
Other
44 events
0.1%
Distribution Summary
Endpoint
Type
Endpoint
Label
Source
Trend
Adversaries
DC02
CampusCiudadJuarez
Collector Server Agent
20,913
148.210.44.13
CampusCiudadJuarez
Collector Server Agent
20,256
148.210.44.200
CampusCiudadJuarez
Collector Server Agent
289
148.210.164.156
CampusCiudadJuarez
Virtual Appliance
375
148.210.82.184
CampusCiudadJuarez
Virtual Appliance
7
148.210.97.171
CampusCiudadJuarez
Virtual Appliance
8
148.210.203.43
CampusCiudadJuarez
Virtual Appliance

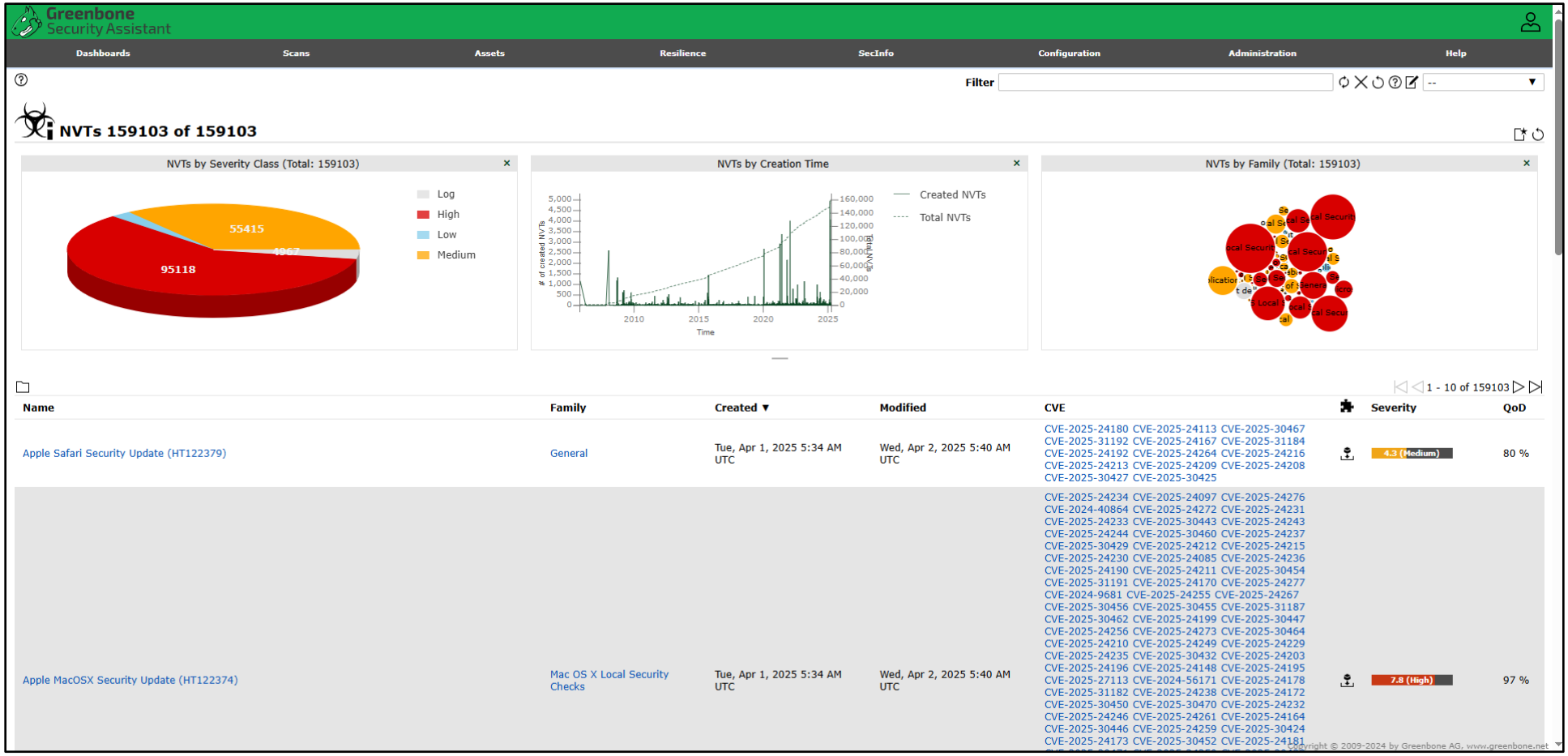
Anexo 6: Interfaz del SIEM Elastick Stack.

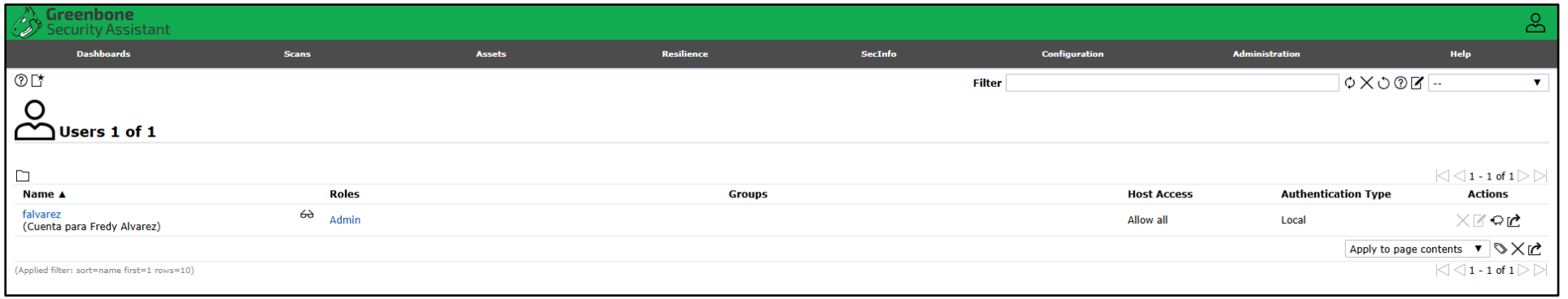


@timestamp	winlog.event_data.SubjectUserName	winlog.event_data.CallingStationID	APMacA	WirelessSSID	winlog.event_data.Reason	oui	winlog.computer_name	event.outcome
Feb 25, 2025 @ 20:47:06.200	al212073@alumnos.uacj.mx	F6-53-D6-75-0D-2D	AP_IIT_D_1_3	ConectaUACJ	-	N/A	RADIUS4.uacj.mx	success
Feb 25, 2025 @ 20:46:28.555	al212073@alumnos.uacj.mx	F6-53-D6-75-0D-2D	AP_IIT_D_1_3	ConectaUACJ	-	N/A	RADIUS4.uacj.mx	success
Feb 25, 2025 @ 20:46:23.237	al212073@alumnos.uacj.mx	F6-53-D6-75-0D-2D	AP_IIT_D_1_3	ConectaUACJ	-	N/A	RADIUSUACJ2.uacj.mx	success
Feb 25, 2025 @ 20:45:10.529	al212073@alumnos.uacj.mx	F6-53-D6-75-0D-2D	AP_IIT_D_1_3	ConectaUACJ	-	N/A	RADIUSUACJ2.uacj.mx	success
Feb 25, 2025 @ 20:44:18.089	al212073@alumnos.uacj.mx	F6-53-D6-75-0D-2D	AP_IIT_D_1_3	ConectaUACJ	-	N/A	RADIUSUACJ2.uacj.mx	success
Feb 25, 2025 @ 20:43:57.962	al212073@alumnos.uacj.mx	F6-53-D6-75-0D-2D	AP_IIT_D_1_3	ConectaUACJ	-	N/A	RADIUSUACJ2.uacj.mx	success
Feb 25, 2025 @ 20:43:06.154	al212073@alumnos.uacj.mx	F6-53-D6-75-0D-2D	AP_IIT_D_1_3	ConectaUACJ	-	N/A	RADIUSUACJ2.uacj.mx	success
Feb 25, 2025 @ 20:42:43.203	al212073@alumnos.uacj.mx	F6-53-D6-75-0D-2D	AP_IIT_D_1_3	ConectaUACJ	-	N/A	RADIUSUACJ3.uacj.mx	success
Feb 25, 2025 @ 20:42:04.916	al212073@alumnos.uacj.mx	F6-53-D6-75-0D-2D	AP_IIT_D_1_3	ConectaUACJ	-	N/A	RADIUSUACJ2.uacj.mx	success
Feb 25, 2025 @ 20:42:01.160	al212073@alumnos.uacj.mx	F6-53-D6-75-0D-2D	AP_IIT_D_1_3	ConectaUACJ	-	N/A	RADIUS4.uacj.mx	success
Feb 25, 2025 @ 20:40:59.202	al212073@alumnos.uacj.mx	F6-53-D6-75-0D-2D	AP_IIT_D_1_3	ConectaUACJ	-	N/A	RADIUSUACJ3.uacj.mx	success
Feb 25, 2025 @ 20:39:06.658	al212073@alumnos.uacj.mx	F6-53-D6-75-0D-2D	AP_IIT_D_1_3	ConectaUACJ	-	N/A	RADIUS4.uacj.mx	success
Feb 25, 2025 @ 20:36:25.412	al212073@alumnos.uacj.mx	F6-53-D6-75-0D-2D	AP_IIT_D_1_3	ConectaUACJ	-	N/A	RADIUS4.uacj.mx	success
Feb 25, 2025 @ 20:34:25.803	al212073@alumnos.uacj.mx	F6-53-D6-75-0D-2D	AP_IIT_D_1_3	ConectaUACJ	-	N/A	RADIUSUACJ2.uacj.mx	success

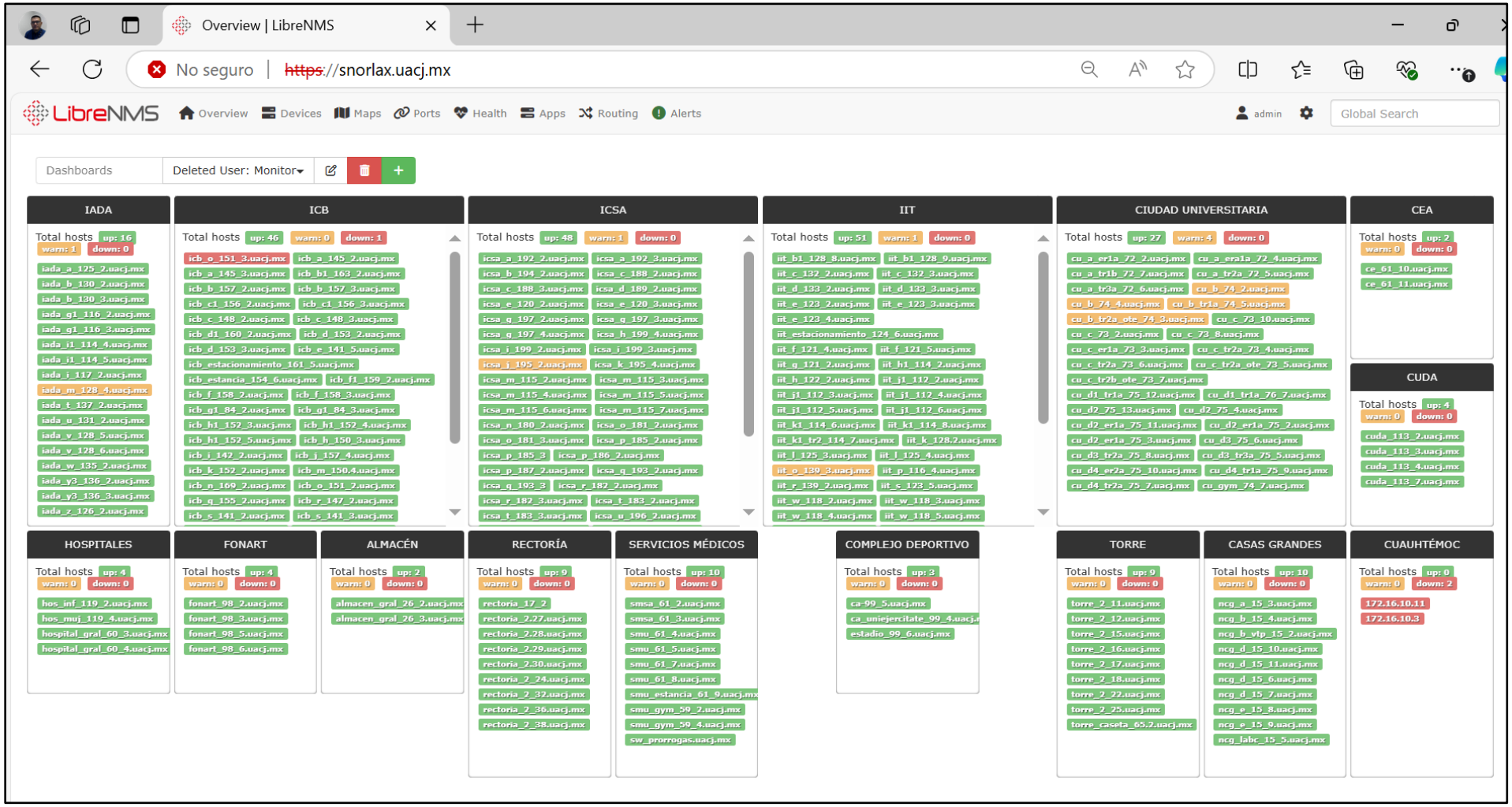
Anexo 7: Interfaz de la herramienta Greenbone.

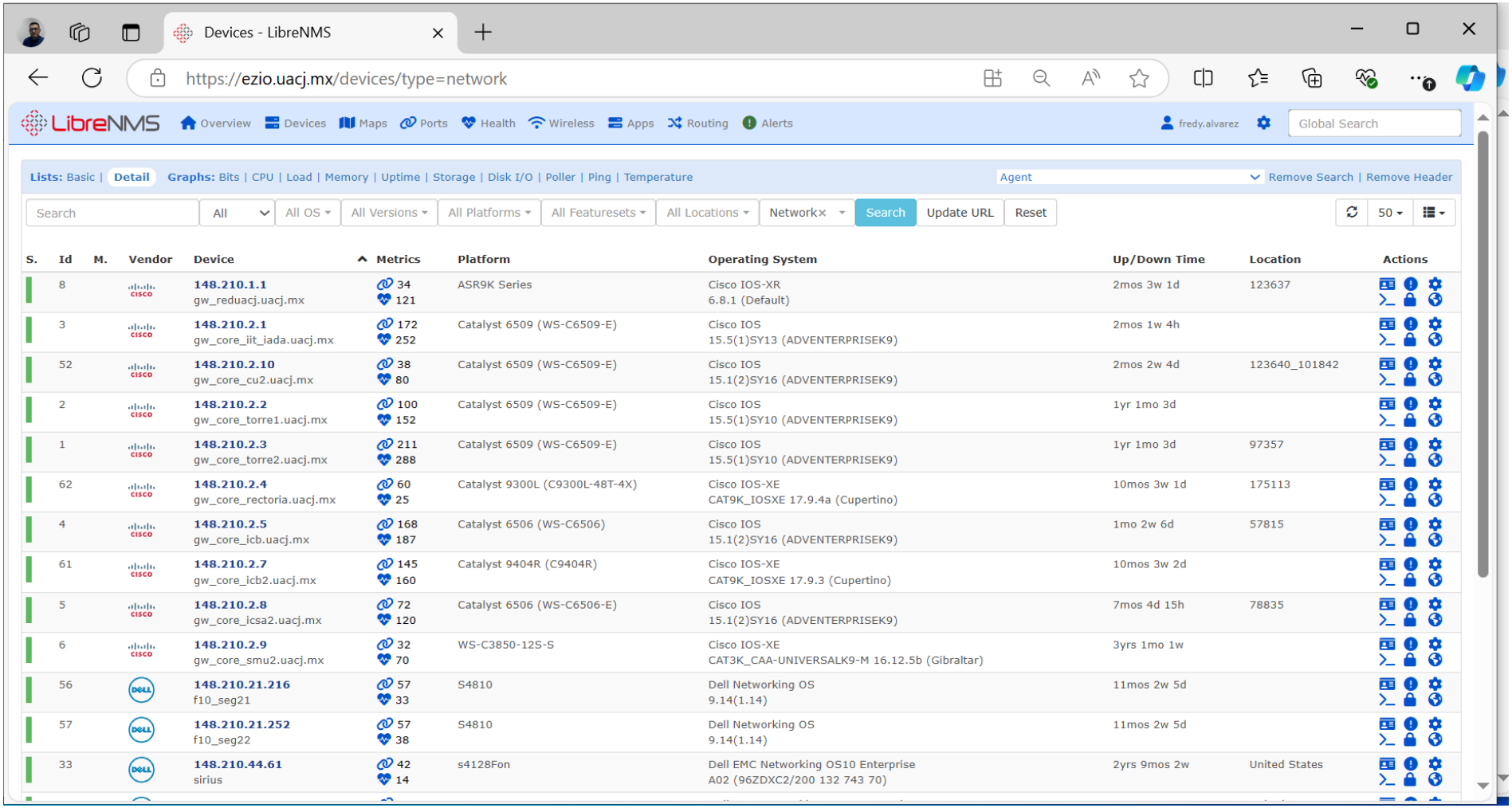


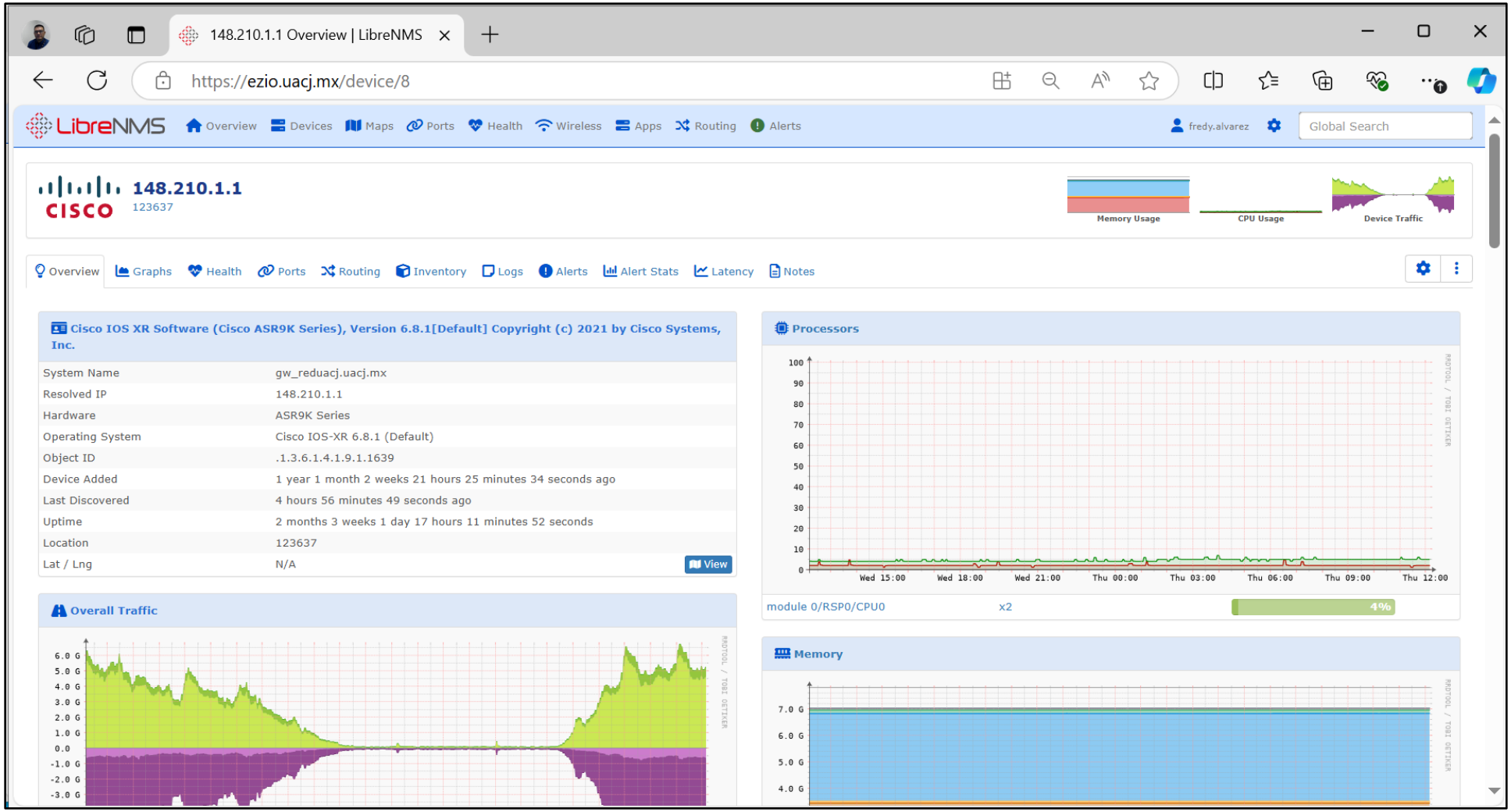

Greenbone
Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Filter
NVTs 159103 of 159103
NVTs by Severity Class (Total: 159103)
Log
High
Low
Medium
55415
4067
95118
NVTs by Creation Time
Created NVTs
Total NVTs
# of created NVTs
Total NVTs
Time
NVTs by Family (Total: 159103)
1 - 10 of 159103
Name
Family
Created
Modified
CVE
Severity
QoD
Apple Safari Security Update (HT122379)
General
Tue, Apr 1, 2025 5:34 AM UTC
Wed, Apr 2, 2025 5:40 AM UTC
CVE-2025-24180 CVE-2025-24113 CVE-2025-30467 CVE-2025-31192 CVE-2025-24167 CVE-2025-31184 CVE-2025-24192 CVE-2025-24264 CVE-2025-24216 CVE-2025-24213 CVE-2025-24209 CVE-2025-24208 CVE-2025-30427 CVE-2025-30425
4.3 (Medium)
80 %
Apple MacOSX Security Update (HT122374)
Mac OS X Local Security Checks
Tue, Apr 1, 2025 5:34 AM UTC
Wed, Apr 2, 2025 5:40 AM UTC
CVE-2025-24234 CVE-2025-24097 CVE-2025-24276 CVE-2024-40864 CVE-2025-24272 CVE-2025-24231 CVE-2025-24233 CVE-2025-30443 CVE-2025-24243 CVE-2025-24244 CVE-2025-30460 CVE-2025-24237 CVE-2025-30429 CVE-2025-24212 CVE-2025-24215 CVE-2025-24230 CVE-2025-24085 CVE-2025-24236 CVE-2025-24190 CVE-2025-24211 CVE-2025-30454 CVE-2025-31191 CVE-2025-24170 CVE-2025-24277 CVE-2024-9681 CVE-2025-24255 CVE-2025-24267 CVE-2025-30456 CVE-2025-30455 CVE-2025-31187 CVE-2025-30462 CVE-2025-24199 CVE-2025-30447 CVE-2025-24256 CVE-2025-24273 CVE-2025-30464 CVE-2025-24210 CVE-2025-24249 CVE-2025-24229 CVE-2025-24235 CVE-2025-30432 CVE-2025-24203 CVE-2025-24196 CVE-2025-24148 CVE-2025-24195 CVE-2025-27113 CVE-2024-56171 CVE-2025-24178 CVE-2025-31182 CVE-2025-24238 CVE-2025-24172 CVE-2025-30450 CVE-2025-30470 CVE-2025-24232 CVE-2025-24246 CVE-2025-24261 CVE-2025-24164 CVE-2025-30446 CVE-2025-24259 CVE-2025-30424 CVE-2025-24173 CVE-2025-30452 CVE-2025-24181
7.8 (High)
97 %
Copyright © 2009-2024 by Greenbone AG, www.greenbone.net


Greenbone
Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Filter
--
Users 1 of 1
1 - 1 of 1
Name ▲
Roles
Groups
Host Access
Authentication Type
Actions
falvarez
(Cuenta para Fredy Alvarez)
Admin
Allow all
Local
Apply to page contents
(Applied filter: sort=name first=1 rows=10)
1 - 1 of 1

Anexo 8: Interfaz de la herramienta Libre NMS.

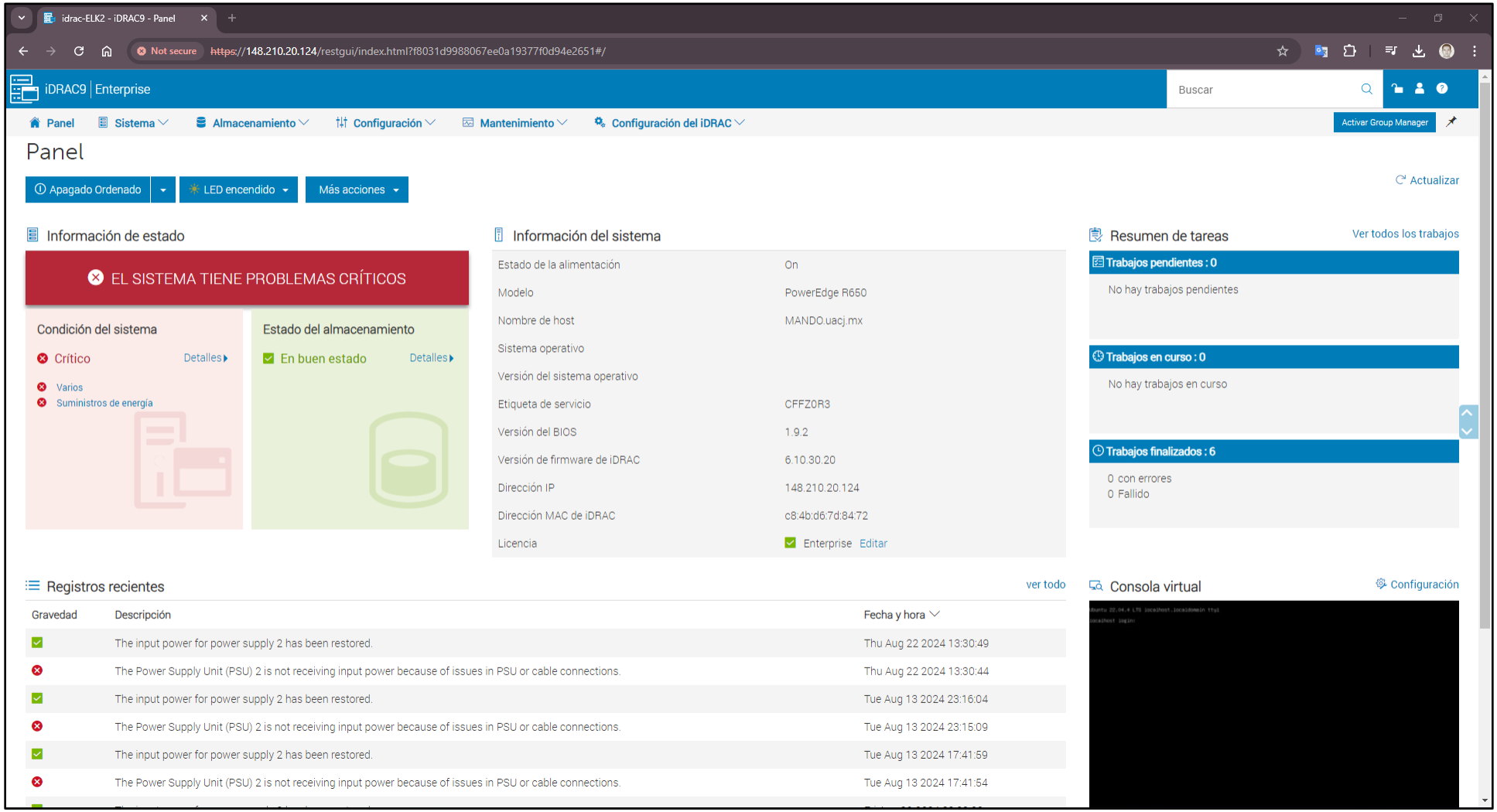



Devices - LibreNMS
https://ezio.uacj.mx/devices/type=network
LibreNMS
Overview
Devices
Maps
Ports
Health
Wireless
Apps
Routing
Alerts
fredy.alvarez
Global Search
Lists: Basic | Detail Graphs: Bits | CPU | Load | Memory | Uptime | Storage | Disk I/O | Poller | Ping | Temperature
Agent
Remove Search | Remove Header
Search
All
All OS
All Versions
All Platforms
All Featuresets
All Locations
Network×
Search
Update URL
Reset
50
S. Id M. Vendor Device Metrics Platform Operating System Up/Down Time Location Actions
8 148.210.1.1 gw_reduacj.uacj.mx 34 121 ASR9K Series Cisco IOS-XR 6.8.1 (Default) 2mos 3w 1d 123637
3 148.210.2.1 gw_core_iit_iada.uacj.mx 172 252 Catalyst 6509 (WS-C6509-E) Cisco IOS 15.5(1)SY13 (ADVENTERPRISEK9) 2mos 1w 4h
52 148.210.2.10 gw_core_cu2.uacj.mx 38 80 Catalyst 6509 (WS-C6509-E) Cisco IOS 15.1(2)SY16 (ADVENTERPRISEK9) 2mos 2w 4d 123640_101842
2 148.210.2.2 gw_core_torre1.uacj.mx 100 152 Catalyst 6509 (WS-C6509-E) Cisco IOS 15.5(1)SY10 (ADVENTERPRISEK9) 1yr 1mo 3d
1 148.210.2.3 gw_core_torre2.uacj.mx 211 288 Catalyst 6509 (WS-C6509-E) Cisco IOS 15.5(1)SY10 (ADVENTERPRISEK9) 1yr 1mo 3d 97357
62 148.210.2.4 gw_core_rectoria.uacj.mx 60 25 Catalyst 9300L (C9300L-48T-4X) Cisco IOS-XE CAT9K_IOSXE 17.9.4a (Cupertino) 10mos 3w 1d 175113
4 148.210.2.5 gw_core_icb.uacj.mx 168 187 Catalyst 6506 (WS-C6506) Cisco IOS 15.1(2)SY16 (ADVENTERPRISEK9) 1mo 2w 6d 57815
61 148.210.2.7 gw_core_icb2.uacj.mx 145 160 Catalyst 9404R (C9404R) Cisco IOS-XE CAT9K_IOSXE 17.9.3 (Cupertino) 10mos 3w 2d
5 148.210.2.8 gw_core_icsa2.uacj.mx 72 120 Catalyst 6506 (WS-C6506-E) Cisco IOS 15.1(2)SY16 (ADVENTERPRISEK9) 7mos 4d 15h 78835
6 148.210.2.9 gw_core_smu2.uacj.mx 32 70 WS-C3850-12S-S Cisco IOS-XE CAT3K_CAA-UNIVERSALK9-M 16.12.5b (Gibraltar) 3yrs 1mo 1w
56 148.210.21.216 f10_seg21 57 33 S4810 Dell Networking OS 9.14(1.14) 11mos 2w 5d
57 148.210.21.252 f10_seg22 57 38 S4810 Dell Networking OS 9.14(1.14) 11mos 2w 5d
33 148.210.44.61 sirius 42 14 s4128Fon Dell EMC Networking OS10 Enterprise A02 (96ZDXC2/200 132 743 70) 2yrs 9mos 2w United States

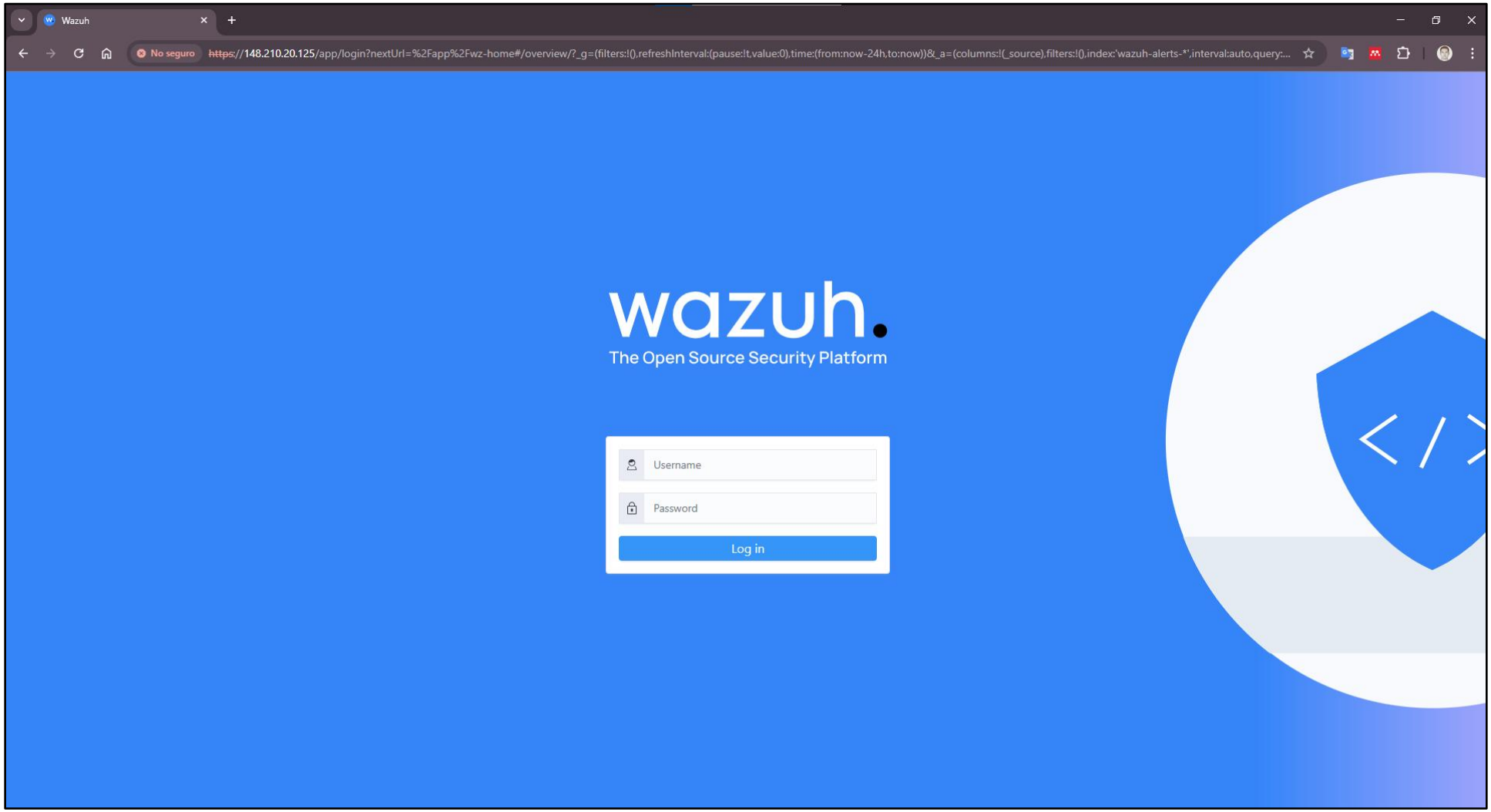

148.210.1.1 Overview | LibreNMS
https://ezio.uacj.mx/device/8
LibreNMS
Overview
Devices
Maps
Ports
Health
Wireless
Apps
Routing
Alerts
fredy.alvarez
Global Search
148.210.1.1
123637
Memory Usage
CPU Usage
Device Traffic
Overview
Graphs
Health
Ports
Routing
Inventory
Logs
Alerts
Alert Stats
Latency
Notes
Cisco IOS XR Software (Cisco ASR9K Series), Version 6.8.1[Default] Copyright (c) 2021 by Cisco Systems, Inc.
System Name gw_reduacj.uacj.mx
Resolved IP 148.210.1.1
Hardware ASR9K Series
Operating System Cisco IOS-XR 6.8.1 (Default)
Object ID .1.3.6.1.4.1.9.1.1639
Device Added 1 year 1 month 2 weeks 21 hours 25 minutes 34 seconds ago
Last Discovered 4 hours 56 minutes 49 seconds ago
Uptime 2 months 3 weeks 1 day 17 hours 11 minutes 52 seconds
Location 123637
Lat / Lng N/A
View
Processors
100
90
80
70
60
50
40
30
20
10
0
Wed 15:00
Wed 18:00
Wed 21:00
Thu 00:00
Thu 03:00
Thu 06:00
Thu 09:00
Thu 12:00
module 0/RSP0/CPU0
x2
4%
Overall Traffic
6.0 G
5.0 G
4.0 G
3.0 G
2.0 G
1.0 G
0.0
-1.0 G
-2.0 G
-3.0 G
Memory
7.0 G
6.0 G
5.0 G
4.0 G

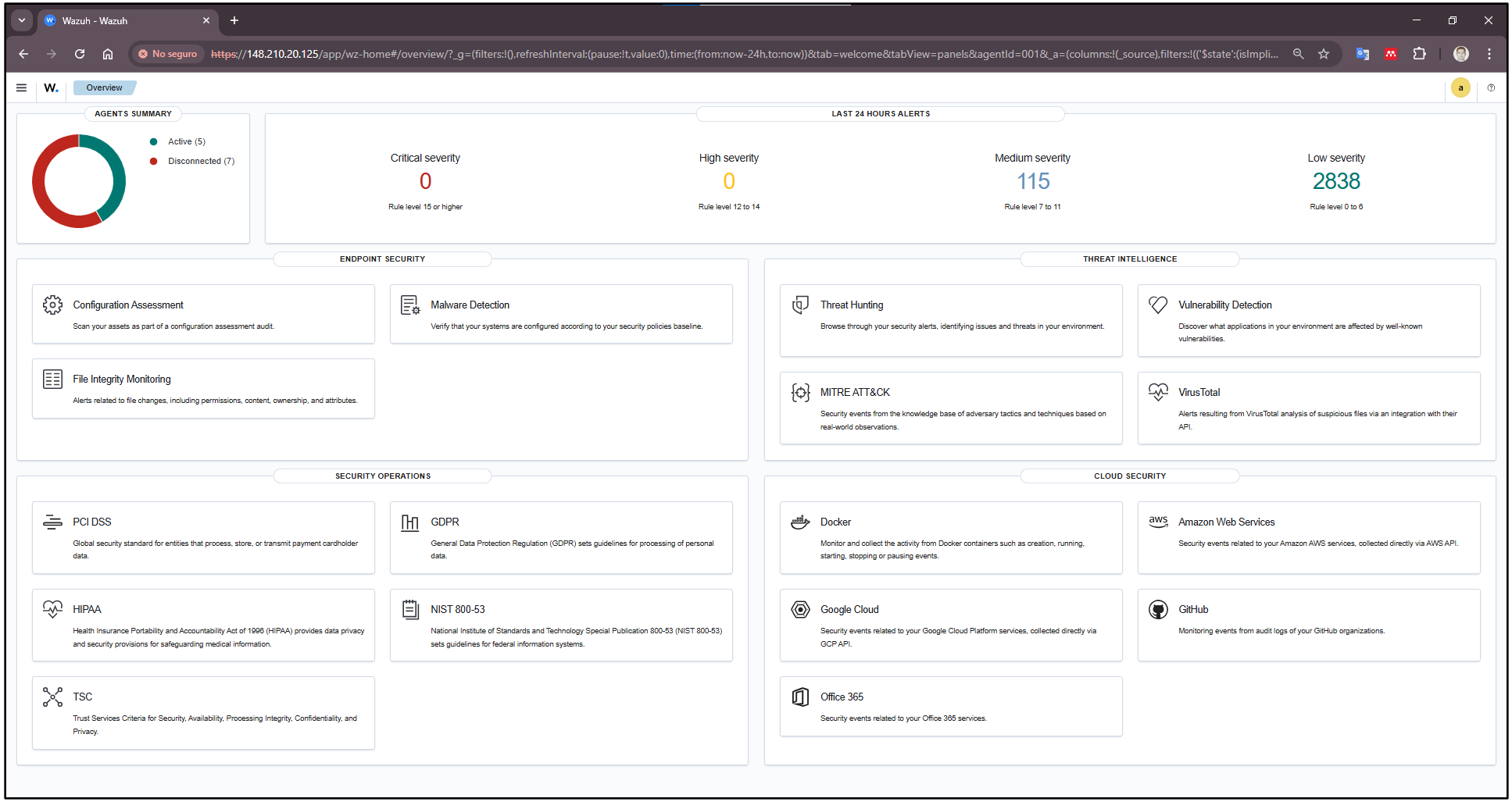

LibreNMS
https://ezio.uacj.mx/graphs/to=1729188600/device=8/type=device_bits/from=1729102200/legend=...
LibreNMS
Overview
Devices
Maps
Ports
Health
Wireless
Apps
Routing
Alerts
fredy.alvarez
Global Search
148.210.1.1 :: Total Traffic
Bits
6 Hours
24 Hours
48 Hours
One Week
Two Weeks
One Month
Two Months
One Year
Two Years
From
2024-10-16 12:10
To
2024-10-17 12:10
Update
Show Legend | Show Previous | Show RRD Command
6.0 G
5.0 G
4.0 G
3.0 G
2.0 G
1.0 G
0.0
-1.0 G
-2.0 G
-3.0 G
-4.0 G
-5.0 G
-6.0 G
13:00
14:00
15:00
16:00
17:00
18:00
19:00
20:00
21:00
22:00
23:00
00:00
01:00
02:00
03:00
04:00
05:00
06:00
07:00
08:00
09:00
10:00
11:00
12:00

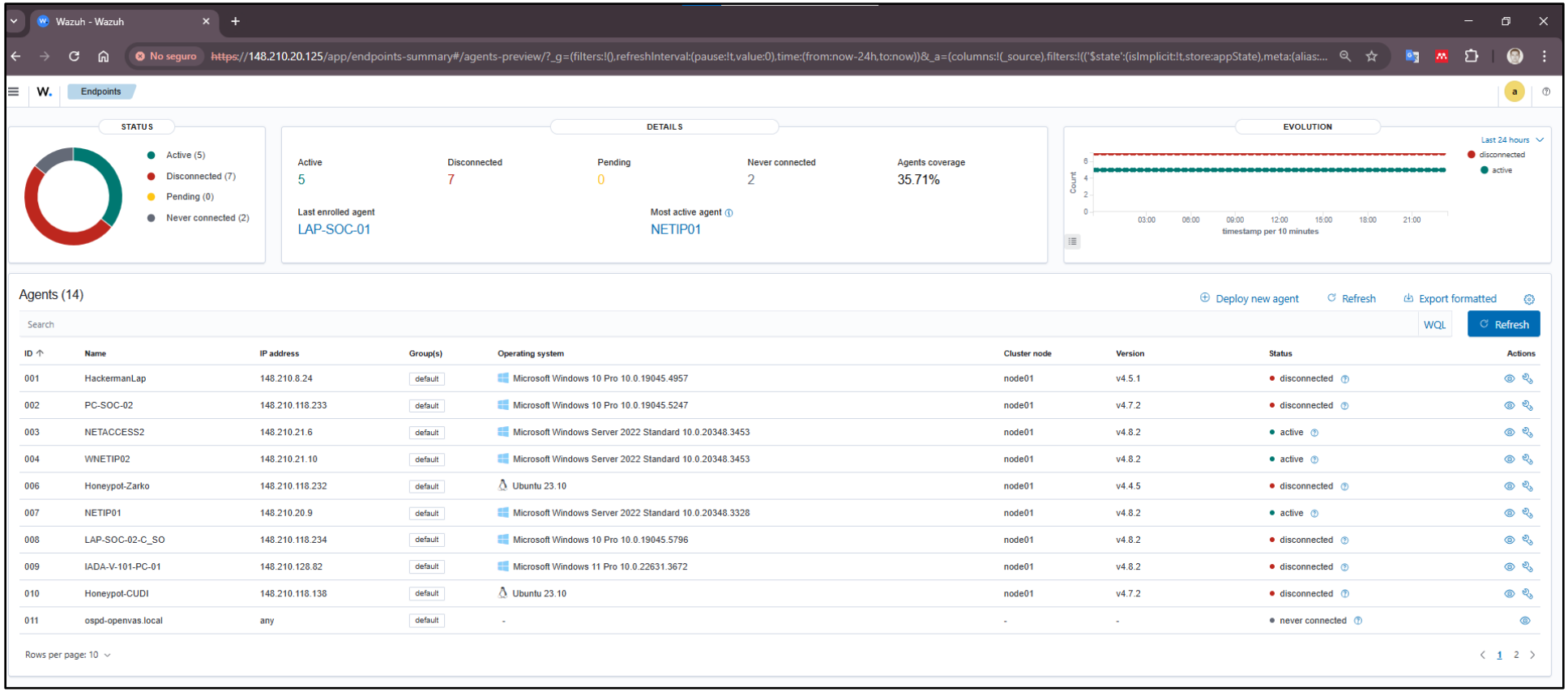
Anexo 9: Interfaz de sistema iDRAC del servidor Dell R650 utilizado para instalar las soluciones.

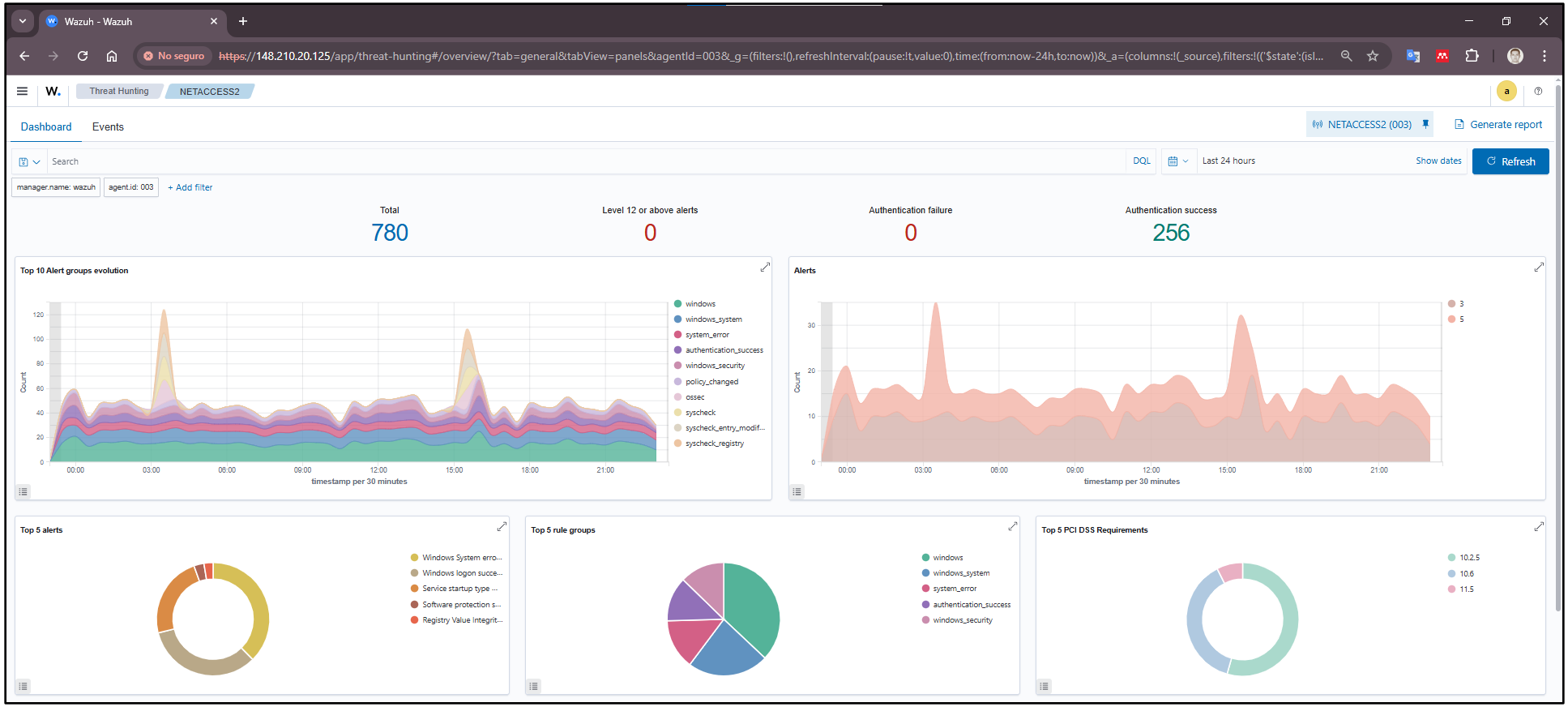


Anexo 10: Wazuh

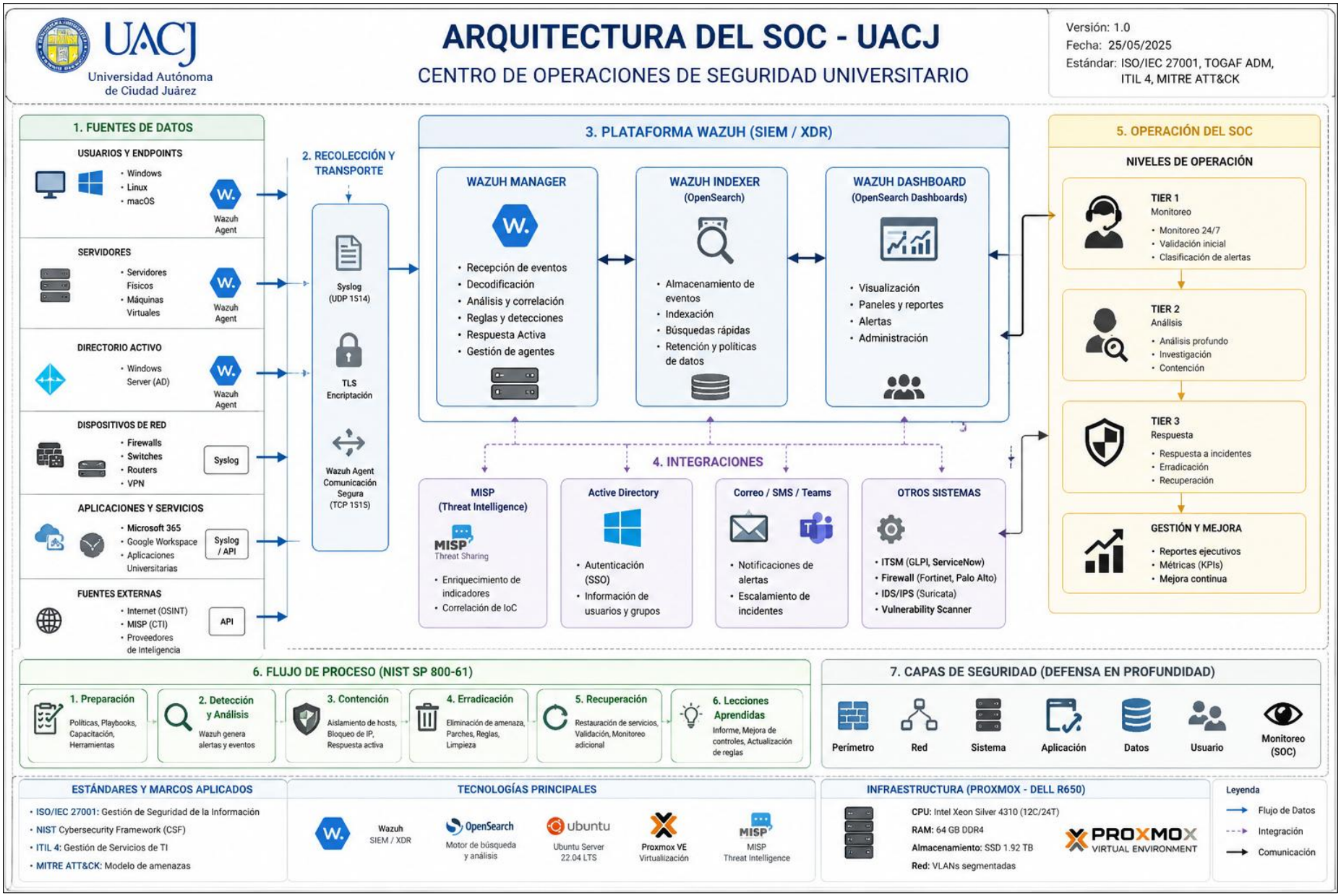



Wazuh - Wazuh
No seguro
https://148.210.20.125/app/wz-home#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&tab=welcome&tabView=panels&agentId=001&_a=(columns:!(_source),filters:!(('$state':(isImpli...
Overview
AGENTS SUMMARY
Active (5)
Disconnected (7)
LAST 24 HOURS ALERTS
Critical severity
0
Rule level 15 or higher
High severity
0
Rule level 12 to 14
Medium severity
115
Rule level 7 to 11
Low severity
2838
Rule level 0 to 6
ENDPOINT SECURITY
Configuration Assessment
Scan your assets as part of a configuration assessment audit.
Malware Detection
Verify that your systems are configured according to your security policies baseline.
File Integrity Monitoring
Alerts related to file changes, including permissions, content, ownership, and attributes.
THREAT INTELLIGENCE
Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.
Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.
MITRE ATT&CK
Security events from the knowledge base of adversary tactics and techniques based on real-world observations.
VirusTotal
Alerts resulting from VirusTotal analysis of suspicious files via an integration with their API.
SECURITY OPERATIONS
PCI DSS
Global security standard for entities that process, store, or transmit payment cardholder data.
GDPR
General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.
HIPAA
Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides data privacy and security provisions for safeguarding medical information.
NIST 800-53
National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.
TSC
Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.
CLOUD SECURITY
Docker
Monitor and collect the activity from Docker containers such as creation, running, starting, stopping or pausing events.
Amazon Web Services
Security events related to your Amazon AWS services, collected directly via AWS API.
Google Cloud
Security events related to your Google Cloud Platform services, collected directly via GCP API.
GitHub
Monitoring events from audit logs of your GitHub organizations.
Office 365
Security events related to your Office 365 services.


Wazuh - Wazuh
No seguro
https://148.210.20.125/app/endpoints-summary#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filters:!(('$state':(isImplicit:!t,store:appState),meta:(alias:...
Endpoints
STATUS
Active (5)
Disconnected (7)
Pending (0)
Never connected (2)
DETAILS
Active
5
Disconnected
7
Pending
0
Never connected
2
Agents coverage
35.71%
Last enrolled agent
LAP-SOC-01
Most active agent
NETIP01
EVOLUTION
Last 24 hours
disconnected
active
Count
timestamp per 10 minutes
Agents (14)
Deploy new agent
Refresh
Export formatted
Search
WQL
Refresh
ID
Name
IP address
Group(s)
Operating system
Cluster node
Version
Status
Actions
001 HackermanLap 148.210.8.24 default Microsoft Windows 10 Pro 10.0.19045.4957 node01 v4.5.1 disconnected
002 PC-SOC-02 148.210.118.233 default Microsoft Windows 10 Pro 10.0.19045.5247 node01 v4.7.2 disconnected
003 NETACCESS2 148.210.21.6 default Microsoft Windows Server 2022 Standard 10.0.20348.3453 node01 v4.8.2 active
004 WNETIP02 148.210.21.10 default Microsoft Windows Server 2022 Standard 10.0.20348.3453 node01 v4.8.2 active
006 Honeypot-Zarko 148.210.118.232 default Ubuntu 23.10 node01 v4.4.5 disconnected
007 NETIP01 148.210.20.9 default Microsoft Windows Server 2022 Standard 10.0.20348.3328 node01 v4.8.2 active
008 LAP-SOC-02-C_SO 148.210.118.234 default Microsoft Windows 10 Pro 10.0.19045.5796 node01 v4.8.2 disconnected
009 IADA-V-101-PC-01 148.210.128.82 default Microsoft Windows 11 Pro 10.0.22631.3672 node01 v4.8.2 disconnected
010 Honeypot-CUDI 148.210.118.138 default Ubuntu 23.10 node01 v4.7.2 disconnected
011 ospd-openvas.local any default - - - never connected
Rows per page: 10
1 2


Wazuh - Wazuh
No seguro
https://148.210.20.125/app/threat-hunting#/overview/?tab=general&tabView=panels&agentId=003&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filters:!(('$state':(isl...
Threat Hunting
NETACCESS2
Dashboard
Events
NETACCESS2 (003)
Generate report
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: wazuh
agent.id: 003
+ Add filter
Total
780
Level 12 or above alerts
0
Authentication failure
0
Authentication success
256
Top 10 Alert groups evolution
Count
timestamp per 30 minutes
windows
windows_system
system_error
authentication_success
windows_security
policy_changed
ossec
syscheck
syscheck_entry_modif...
syscheck_registry
Alerts
Count
timestamp per 30 minutes
3
5
Top 5 alerts
Windows System erro...
Windows logon succe...
Service startup type ...
Software protection s...
Registry Value Integrit...
Top 5 rule groups
windows
windows_system
system_error
authentication_success
windows_security
Top 5 PCI DSS Requirements
10.2.5
10.6
11.5

Anexo 11. Arquitectura.



Anexo 12. Certificado Premio Internacional Metared TIC 2025.

meta red
by universia

Certificado

Premio Internacional MetaRed TIC 2025

a

Fredy Fernando Alvarez Sanchez

Ganador de la Categoría Ciberseguridad del Premio Internacional MetaRed TIC 2025, con su proyecto: "Diseño de un Centro de Operaciones de Seguridad (SOC) basado en herramientas de Código Abierto", representando a la Universidad Autónoma de Ciudad Juárez.

18/7/2025

Tomás Jiménez García
Coordinador Global de MetaRed

Premio Internacional
meta red
2025

Anexo 13. Segundo reconocimiento Sello C3!Cyber 2025.

metared
by universia

Otorga el presente certificado en calidad de

Institución con Sello C3!Cyber

a

Universidad Autónoma de Ciudad de Juárez

Acreditando la obtención del Sello C3!Cyber de MetaRed TIC, en reconocimiento a su compromiso con la Cultura, Concienciación y Comunicación en ciberseguridad en las Instituciones de Educación Superior Iberoamericanas, con vigencia hasta 2027.

6/4/2026

Tomás Jiménez García
Coordinador Global de MetaRed

Anexo 14. Reporte de brecha de seguridad.

Conforme a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

Código:	SOC-UACJ-BS-001
Versión:	1.0
Clasificación:	CONFIDENCIAL
Fecha de emisión:	[DD/MM/AAAA]
Elaboró:	SOC – UACJ
Destinatario:	Contraloría / Abogado General UACJ

1. DATOS GENERALES DEL INCIDENTE

1.1 Identificación del Reporte	
Número de folio del incidente:	
Fecha y hora de detección:	
Fecha y hora de notificación interna:	
Fecha y hora de contención (si aplica):	
Clasificación de severidad (Crítica / Alta / Media / Baja):	

1.2 Responsable del Reporte	
Nombre completo del analista SOC:	
Cargo:	
Unidad administrativa:	
Correo electrónico institucional:	
Teléfono de contacto:	

2. DESCRIPCIÓN DE LA BRECHA DE SEGURIDAD

(Artículos 31, 32, 33 y 34 de la LGPDPPSO; Lineamientos del SNT)

2.1 Naturaleza del Incidente	
Tipo de brecha (Confidencialidad / Integridad / Disponibilidad):	
Vector de ataque (phishing, ransomware, acceso no autorizado, error humano, otro):	
Descripción técnica detallada del incidente:	
Información adicional:	

2.2 Sistemas y Activos Afectados	
Sistemas de información comprometidos:	
Bases de datos afectadas:	
Servidores / Equipos involucrados (IP, hostname):	
Redes o segmentos de red afectados:	

3. DATOS PERSONALES COMPROMETIDOS

(Artículo 3, fracciones IX, X y XVII de la LGPDPPSO)

3.1 Titulares Afectados	
Número estimado de titulares afectados:	
Perfil de los titulares (estudiantes, docentes, personal administrativo, proveedores):	
3.2 Categorías de Datos Comprometidos	
Datos de identificación (nombre, CURP, RFC, INE):	
Datos de contacto (correo, teléfono, domicilio):	
Datos académicos (matrícula, calificaciones, historial):	
Datos laborales (nómina, RFC, puesto, antigüedad):	
Datos financieros (cuentas bancarias, CLABE):	
Datos sensibles (salud, biométricos, origen étnico, afiliación sindical):	
Otros (especificar):	
3.3 Nivel de Exposición	
Los datos fueron accedidos:	
Los datos fueron copiados o exfiltrados:	
Los datos fueron alterados:	
Los datos fueron destruidos:	
Los datos fueron publicados en línea:	

4. ANÁLISIS DE IMPACTO Y RIESGO

4.1 Evaluación de Daño Potencial	
Riesgo de daño patrimonial a los titulares:	
Riesgo de discriminación:	
Riesgo de suplantación de identidad:	
Riesgo de daño moral o reputacional:	
Nivel de riesgo global (Crítico / Alto / Medio / Bajo):	

4.2 Impacto Institucional	
Afectación a la operación universitaria:	
Riesgo legal y regulatorio:	
Riesgo reputacional para la UACJ:	
Posible incumplimiento normativo (arts. LGPDPPSO):	

5. ACCIONES DE CONTENCIÓN Y RESPUESTA

(Artículos 31 y 32 de la LGPDPPSO; Art. 82 de los Lineamientos Generales del SNT)

Acción Realizada	Fecha/Hora	Responsable

6. NOTIFICACIONES REALIZADAS

(Artículos 33 y 34 de la LGPDPPSO – plazo máximo de 72 horas para notificar a titulares)

6.1 Notificación a Titulares de Datos Personales	
¿Se notificó a los titulares? (Sí / No / En proceso):	
Fecha de notificación:	
Medio utilizado (correo, aviso web, comunicado):	
Número de titulares notificados:	

6.2 Notificación al INAI / Órgano Garante Estatal	
¿Se notificó al organismo garante? (Sí / No / En proceso):	

Fecha de notificación:	
Número de expediente o acuse:	
6.3 Notificación Interna UACJ	
Rectoría:	
Abogado General:	
Contraloría:	
Dirección General de Tecnologías de Información:	
Comité de Transparencia:	

7. EVIDENCIA TÉCNICA ADJUNTA

No.	Tipo de Evidencia	Descripción	Referencia / Anexo
1			
2			
3			
4			
5			

Tipos sugeridos: Logs de acceso, capturas de pantalla, volcados de memoria, reportes SIEM, análisis forense, IOCs, cadena de custodia digital.

8. PLAN DE REMEDIACIÓN Y MEDIDAS CORRECTIVAS

8.1 Medidas Técnicas Inmediatas	

8.2 Medidas Administrativas y Organizacionales	

8.3 Medidas a Mediano y Largo Plazo	

8.4 Cronograma de Implementación	

9. FUNDAMENTO LEGAL APLICABLE

El presente reporte se emite en cumplimiento de las siguientes disposiciones:

Disposición	Contenido Relevante
Art. 3, fr. IX, X, XVII LGPDPPSO	Definiciones de datos personales, datos sensibles, responsable y vulneraciones de seguridad.
Art. 31 LGPDPPSO	Obligación de establecer y mantener medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales.
Art. 32 LGPDPPSO	Acciones inmediatas ante vulneraciones: análisis de causas, implementación de medidas correctivas y acciones de mitigación.
Art. 33 LGPDPPSO	Obligación de informar sin dilación a los titulares sobre vulneraciones que afecten de forma significativa sus derechos.
Art. 34 LGPDPPSO	Contenido mínimo de la notificación a titulares: naturaleza del incidente, datos comprometidos, acciones correctivas y medios para obtener información.
Art. 82, Lineamientos Grales. SNT	Procedimiento para la gestión de vulneraciones de seguridad de datos personales por sujetos obligados.
Art. 163 LGPDPPSO	Infracciones por incumplimiento de medidas de seguridad y omisión de notificaciones.
Ley General de Transparencia	Obligaciones de transparencia proactiva y protección de información confidencial.

10. LECCIONES APRENDIDAS Y RECOMENDACIONES

10.1 Causas Raíz Identificadas	

10.2 Recomendaciones del SOC	

10.3 Mejoras al Programa de Protección de Datos	

11. FIRMAS Y VALIDACIÓN

Las firmas a continuación validan la veracidad, completitud y entrega formal del presente reporte.

ELABORÓ	
Nombre:	
Cargo:	Analista SOC – UACJ
Firma:	
Fecha:	

REVISÓ	
Nombre:	
Cargo:	Coordinador SOC – UACJ / Jefatura de Ciberseguridad
Firma:	
Fecha:	

RECIBIÓ – CONTRALORÍA	
Nombre:	
Cargo:	
Firma:	
Fecha y hora de recepción:	

RECIBIÓ – ABOGADO GENERAL	
Nombre:	
Cargo:	
Firma:	
Fecha y hora de recepción:	

12. CONTROL DE VERSIONES

Versión	Fecha	Autor	Descripción del Cambio
1.0	[DD/MM/AAAA]	SOC – UACJ	Creación del documento.

AVISO DE CONFIDENCIALIDAD

Anexo 15. Instalación de Wazuh en una única instancia.

```
falvarez@wazuh:~$ curl -sO https://packages.wazuh.com/4.14/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
30/04/2023 02:59:48 INFO: Starting Wazuh installation assistant. Wazuh version: 4.14.5
30/04/2023 02:59:48 INFO: Verbose logging redirected to /var/log/wazuh-install.log
30/04/2023 03:00:04 INFO: Verifying that your system meets the recommended minimum hardware requirements.
30/04/2023 03:00:04 INFO: Wazuh web interface port will be 443.
30/04/2023 03:00:20 INFO: --- Dependencies ----
30/04/2023 03:00:20 INFO: Installing apt-transport-https.
30/04/2023 03:00:28 INFO: Installing debhelper.
30/04/2023 03:01:17 INFO: Wazuh repository added.
30/04/2023 03:01:17 INFO: --- Configuration files ---
30/04/2023 03:01:17 INFO: Generating configuration files.
30/04/2023 03:01:19 INFO: Generating the root certificate.
30/04/2023 03:01:21 INFO: Generating Admin certificates.
30/04/2023 03:01:21 INFO: Generating Wazuh indexer certificates.
30/04/2023 03:01:22 INFO: Generating Filebeat certificates.
30/04/2023 03:01:24 INFO: Generating Wazuh dashboard certificates.
30/04/2023 03:01:25 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and
passwords necessary for installation.
30/04/2023 03:01:25 INFO: --- Wazuh indexer ---
30/04/2023 03:01:25 INFO: Starting Wazuh indexer installation.
30/04/2023 03:06:22 INFO: Wazuh indexer installation finished.
30/04/2023 03:06:22 INFO: Wazuh indexer post-install configuration finished.
30/04/2023 03:06:22 INFO: Starting service wazuh-indexer.
30/04/2023 03:07:10 INFO: wazuh-indexer service started.
30/04/2023 03:07:10 INFO: Initializing Wazuh indexer cluster security settings.
30/04/2023 03:07:21 INFO: Wazuh indexer cluster security configuration initialized.
30/04/2023 03:07:21 INFO: Wazuh indexer cluster initialized.
30/04/2023 03:07:21 INFO: --- Wazuh server ---
30/04/2023 03:07:21 INFO: Starting the Wazuh manager installation.
30/04/2023 03:10:34 INFO: Wazuh manager installation finished.
30/04/2023 03:10:34 INFO: Wazuh manager vulnerability detection configuration finished.
30/04/2023 03:10:34 INFO: Starting service wazuh-manager.
30/04/2023 03:11:06 INFO: wazuh-manager service started.
30/04/2023 03:11:06 INFO: Starting Filebeat installation.
30/04/2023 03:11:22 INFO: Filebeat installation finished.
30/04/2023 03:11:33 INFO: Filebeat post-install configuration finished.
30/04/2023 03:11:33 INFO: Starting service filebeat.
30/04/2023 03:11:37 INFO: filebeat service started.
30/04/2023 03:11:37 INFO: --- Wazuh dashboard ---
30/04/2023 03:11:37 INFO: Starting Wazuh dashboard installation.
30/04/2023 03:16:01 INFO: Wazuh dashboard installation finished.
30/04/2023 03:16:01 INFO: Wazuh dashboard post-install configuration finished.
30/04/2023 03:16:01 INFO: Starting service wazuh-dashboard.
30/04/2023 03:16:04 INFO: wazuh-dashboard service started.
30/04/2023 03:16:08 INFO: Updating the internal users.
30/04/2023 03:16:15 INFO: A backup of the internal users has been saved in the /etc/wazuh-indexer/internalusers-
backup folder.
30/04/2023 03:16:45 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore username and
password.
30/04/2023 03:17:39 INFO: Initializing Wazuh dashboard web application.
30/04/2023 03:17:39 INFO: Wazuh dashboard web application not yet initialized. Waiting...
30/04/2023 03:17:55 INFO: Wazuh dashboard web application not yet initialized. Waiting...
30/04/2023 03:18:11 INFO: Wazuh dashboard web application initialized.
30/04/2023 03:18:11 INFO: --- Summary ---
30/04/2023 03:18:11 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: U9Nyr?XXXXXXau8FtXXXXXt?Elscav
30/04/2023 03:18:11 INFO: Installation finished.
falvarez@wazuh:~$
```

Anexo 16. Matriz de priorización y tiempos de respuesta

MATRIZ DE PRIORIZACIÓN Y TIEMPOS DE RESPUESTA

ACUERDO DE NIVEL DE SERVICIO (SLA)

Centro de Operaciones de Seguridad – UACJ

Dirección General de Tecnologías de la Información (DGTI)

Código:	**SOC-UACJ-SLA-001**
Versión:	1.0
Clasificación:	**USO INTERNO**
Fecha:	[DD/MM/AAAA]
Elaboró:	SOC – UACJ
Aprueba:	DGTI / Rectoría
Marco normativo:	NIST SP 800-61r3, ISO/IEC 27001:2022, LGPDPPSO, MITRE ATT&CK

Alineado con las métricas MTTD, MTTA y MTTR definidas en la Sección 3.7 de la tesis «Diseño e implementación de un SOC basado en cómputo en la nube».

1. OBJETIVO

Establecer los tiempos de detección, reconocimiento y respuesta que el SOC-UACJ se compromete a cumplir ante incidentes de ciberseguridad, clasificados por nivel de severidad. Este Acuerdo de Nivel de Servicio (SLA) formaliza las expectativas de rendimiento entre el SOC y las áreas de la UACJ (Rectoría, Contraloría, Abogado General, DGTI), y se alinea con los marcos NIST SP 800-61r3, ISO/IEC 27001:2022, la LGPDPPSO y las métricas definidas en la Sección 3.7 del proyecto SOC-UACJ.

2. DEFINICIÓN DE MÉTRICAS CLAVE

Métrica	Nombre Completo	Definición Operativa para el SOC-UACJ
MTTD	Mean Time to Detect	Tiempo promedio desde que ocurre un evento de seguridad hasta que el SIEM (Elastic Stack) o Wazuh genera la alerta correspondiente. Incluye la latencia de recolección de logs y la correlación de reglas.
MTTA	Mean Time to Acknowledge	Tiempo promedio desde que la alerta aparece en el dashboard del SOC hasta que un analista N1 la reconoce (cambia estado a «En progreso») e inicia el triaje. Mide la disponibilidad y la carga operativa del equipo.
MTTR	Mean Time to Respond / Remediate	Tiempo promedio desde la detección hasta la contención verificada del incidente (aislamiento del host, bloqueo de IP en Sophos, desactivación de cuenta en AD, eliminación de malware). Comprende el ciclo completo de triaje, escalamiento, investigación y respuesta activa.
MTTC	Mean Time to Contain	Subconjunto del MTTR: tiempo desde la confirmación del incidente hasta la ejecución exitosa de la acción de contención (p. ej., ejecución de Active Response de Wazuh o bloqueo en firewall Sophos XGS).
FPR	False Positive Rate	Proporción de alertas que, tras el triaje del analista N1, resultan no ser amenazas reales. Meta del SOC-UACJ: FPR < 25% en alertas críticas, < 50% en alertas altas. Se monitorea para ajustar reglas de correlación y reducir fatiga de alertas.

3. CLASIFICACIÓN DE SEVERIDAD DE INCIDENTES

La clasificación se basa en los criterios de impacto sobre la tríada CID (Confidencialidad, Integridad, Disponibilidad), el número de activos y titulares afectados, y la obligación de notificación conforme a los artículos 31-34 de la LGPDPPSO.

Severidad	Criterios de Clasificación	Impacto en la UACJ
S1 CRÍTICO	Compromiso masivo de datos personales sensibles Afectación a más de 3 activos críticos simultáneamente Explotación activa con movimiento lateral confirmado Pérdida de control de infraestructura central (AD, DNS, DHCP)	Obligación de notificación al INAI en 72 horas (Art. 33 LGPDPPSO) Riesgo reputacional severo para la UACJ Posible interrupción de operaciones académicas y administrativas Activación del DRP del SOC
S2 ALTO	Compromiso confirmado de credenciales con acceso a datos Malware activo en segmento de red con datos institucionales Vulnerabilidad explotada en servidor expuesto a Internet Afectación a 1-3 activos críticos	Posible brecha de datos personales (evaluación en curso) Impacto operativo en área específica (IIT, ICB, IADA, etc.) Requiere coordinación con DGTI y Jefatura de Ciberseguridad Notificación interna al Coordinador SOC y DGTI
S3 MEDIO	Amenaza detectada y contenida sin propagación Vulnerabilidad crítica sin evidencia de explotación Actividad sospechosa que requiere investigación profunda Violación de políticas sin exposición de datos	Impacto limitado a endpoint(s) individual(es) Sin afectación a datos personales ni servicios críticos Registro para análisis de tendencias y ajuste de reglas Oportunidad de mejora en controles preventivos
S4 BAJO	Actividad anómala sin compromiso confirmado Reconocimiento externo (escaneos, fingerprinting) Evento aislado sin persistencia ni propagación Incumplimiento menor de higiene de seguridad	Sin impacto operativo directo Información útil para inteligencia de amenazas (MISP) Contribuye a la línea base de comportamiento normal Acción correctiva programable (no urgente)
S5 INFO	Eventos de auditoría rutinarios sin anomalía Notificaciones informativas de feeds de TI	Sin impacto. Valor para baseline y cumplimiento Alimenta dashboards de Kibana para reportes gerenciales

	Resultados de escaneos programados de Greenbone Cambios de configuración documentados y autorizados	Evidencia de monitoreo continuo (ISO 27001 A.8.15/A.8.16) Soporte para auditorías de Contraloría

4. MATRIZ DE TIEMPOS DE RESPUESTA (SLA)

Horario base de operación del SOC-UACJ: 8×5 (Fase 1). Los tiempos SLA aplican durante horario operativo. Fuera de horario, los incidentes S1 activan el protocolo de guardia.

Nivel	MTTD (Detección)	MTTA (Reconoc.)	MTTR (Respuesta)	Escalamiento Máximo	Ejemplos Contextualizados UACJ
S1 – CRÍTICO	**≤ 15 min**	**≤ 5 min**	**≤ 1 hora**	Inmediato a CISO, Rectoría, Abogado Gral.	Exfiltración de datos escolares o de nómina Ransomware activo en servidores críticos Compromiso de Active Directory (Domain Admin) Brecha de datos personales sensibles (LGPDPPSO) Caída total del Campus Virtual o Portal Institucional
S2 – ALTO	**≤ 30 min**	**≤ 10 min**	**≤ 4 horas**	N2 + Coordinador SOC + DGTI	Phishing exitoso con credenciales comprometidas Malware activo en segmento de red académica Acceso no autorizado a servidores de bases de datos Ataque de fuerza bruta exitoso (SSH/RDP) Compromiso de cuenta de correo institucional de funcionario
S3 – MEDIO	**≤ 2 horas**	**≤ 30 min**	**≤ 8 horas**	N2 + Notificación a Coordinador SOC	Detección de malware contenido en endpoint aislado Intentos de phishing sin víctimas confirmadas Violación menor de políticas de acceso Vulnerabilidad crítica detectada sin explotación activa

					Tráfico anómalo hacia IP sospechosa (sin exfiltración)
S4 – BAJO	**≤ 4 horas**	**≤ 1 hora**	**≤ 24 horas**	N1 con registro en bitácora	Escaneo de puertos desde IP externa Intentos de login fallidos aislados Dispositivo no autorizado en la red (BYOD sin riesgo) Alerta informativa de Threat Intelligence (IoC bajo) Actualización de firma de antivirus retrasada
S5 – INFORMATIVO	**≤ 8 horas**	**≤ 4 horas**	**≤ 48 horas**	Registro automático, revisión en turno siguiente	Eventos rutinarios de auditoría de Wazuh Cambios de configuración programados Notificaciones informativas de MISP/AlienVault OTX Resultados de escaneo programado de Greenbone Log de mantenimiento preventivo

5. PROTOCOLO DE ESCALAMIENTO POR NIVEL

Severidad	Primer Responsable	Escalamiento Nivel 2	Escalamiento Nivel 3	Notificación Gerencial	Notificación Ejecutiva
S1	N1 (inmediato)	N2 (< 5 min)	N3 (< 15 min)	Coord. SOC + DGTI (< 15 min)	CISO + Rectoría + Abogado Gral. (< 30 min)
S2	N1 (< 10 min)	N2 (< 15 min)	N3 (si req.)	Coord. SOC (< 30 min)	DGTI (< 1 hora)
S3	N1 (< 30 min)	N2 (< 1 hora)	Según análisis	Coord. SOC (reporte diario)	No requerida
S4	N1 (< 1 hora)	Solo si persiste	No aplica	Reporte semanal	No requerida
S5	Automático	No aplica	No aplica	Reporte mensual	No requerida

6. METAS DE RENDIMIENTO TRIMESTRAL

Las siguientes metas representan los objetivos de desempeño que el SOC-UACJ se compromete a alcanzar progresivamente, evaluados en ciclos de 90 días conforme a las mejores prácticas de la industria.

Indicador (KPI)	Meta Fase 1 (8×5)	Meta Fase 2 (15×5)	Meta Fase 3 (24×7)
Cumplimiento SLA de incidentes S1	≥ 85%	≥ 92%	≥ 98%
Cumplimiento SLA de incidentes S2	≥ 80%	≥ 90%	≥ 95%
Tasa de Falsos Positivos (S1-S2)	< 40%	< 30%	< 25%
Cobertura de activos críticos monitoreados	≥ 60%	≥ 80%	≥ 95%
Alertas procesadas por analista/día	≤ 30	≤ 25	≤ 20
Cobertura de tácticas MITRE ATT&CK	≥ 40%	≥ 60%	≥ 80%
Disponibilidad del SIEM (Elastic Stack)	≥ 95%	≥ 98%	≥ 99.5%
Tiempo de capacitación por operador	≤ 40 horas	≤ 30 horas	≤ 20 horas

7. MAPEO DE INCIDENTES CON PLAYBOOKS Y HERRAMIENTAS SOC-UACJ

Tipo de Incidente	Severidad Típica	Herramienta de Detección	Acción de Contención	Playbook Asociado
Ransomware activo	**S1**	Wazuh (FIM + Active Response)	Aislamiento de host + bloqueo en Sophos XGS	**PB-RANSOM-001**
Exfiltración de datos personales	**S1**	ELK (correlación de tráfico anómalo) + Suricata	Bloqueo de IP destino + notificación LGPDPPSO	**PB-EXFIL-001**
Phishing exitoso	**S2**	Wazuh (log de O365) + VirusTotal	Reset de credenciales + purga de correo	**PB-PHISH-001**

Fuerza bruta SSH/RDP	S2	Wazuh (Regla 5710) + Fail2Ban	Bloqueo IP 24h (Active Response / iptables)	**PB-BRUTE-001**
Malware en endpoint aislado	S3	Wazuh EDR + Microsoft Defender	Cuarentena + análisis en Any.Run	**PB-MALW-001**
Vulnerabilidad crítica detectada	S3	Greenbone (OpenVAS) + Wazuh	Parcheo programado + monitoreo reforzado	**PB-VULN-001**
Escaneo de puertos externo	S4	Suricata + LibreNMS	Registro en MISP + monitoreo	**PB-RECON-001**
Alerta informativa de TI	S5	MISP / AlienVault OTX	Actualización de IoCs en Wazuh	Automático

8. CONDICIONES OPERATIVAS Y EXCEPCIONES

Horario de cobertura Fase 1: lunes a viernes, 8:00 a 16:00 hrs (horario UACJ). Los incidentes S1 detectados fuera de horario activan el protocolo de guardia vía llamada al Coordinador SOC.

Los tiempos SLA se pausan durante ventanas de mantenimiento programadas del SIEM, previamente notificadas con 48 horas de anticipación.

La severidad de un incidente puede reclasificarse durante la investigación. Un incidente S3 que revele compromiso de datos personales se eleva automáticamente a S1.

Todo incidente S1 genera obligatoriamente un Reporte de Brecha de Seguridad (formato SOC-UACJ-BS-001) para Contraloría y Abogado General.

Las métricas se revisan trimestralmente en reunión de Coordinador SOC con DGTI, y se presentan semestralmente ante Rectoría.

Los activos no integrados al SIEM (por limitaciones técnicas documentadas en la Sección 1.4.4 de la tesis) quedan excluidos de la cobertura SLA hasta su incorporación.

9. REFERENCIAS NORMATIVAS

Documento / Estándar	Aplicación en el SLA
NIST SP 800-61r3	Guía de manejo de incidentes: ciclo de preparación, detección, contención, erradicación, recuperación y lecciones aprendidas. Base para la definición de MTTD/MTTR.
NIST SP 800-53r5	Controles IR-4 (Incident Handling), IR-5 (Incident Monitoring), IR-6 (Incident Reporting), SI-4 (Information System Monitoring).

ISO/IEC 27001:2022	Controles A.5.24 (Planificación de respuesta a incidentes), A.5.25 (Evaluación y decisión), A.5.26 (Respuesta a incidentes), A.8.15 (Logging), A.8.16 (Monitoreo).
LGPDPPSO (Arts. 31-34)	Obligación de medidas de seguridad, acciones correctivas ante vulneraciones, notificación a titulares en máximo 72 horas, y contenido mínimo de la notificación.
NIST SP 800-92	Guía de gestión de logs: políticas de retención, cifrado y almacenamiento de evidencia para análisis forense post-incidente.
MITRE ATT&CK	Clasificación de tácticas y técnicas adversarias para evaluar cobertura de detección del SOC y priorizar reglas de correlación.
NIST SP 800-137	Monitoreo continuo de seguridad de la información: base para la definición de frecuencias de revisión y dashboards del SOC.

10. APROBACIÓN Y VIGENCIA

Coordinador SOC	Director DGTI	Contraloría	Abogado General
Nombre:	**Nombre:**	**Nombre:**	**Nombre:**
Firma:	Firma:	Firma:	Firma:
Fecha:	**Fecha:**	**Fecha:**	**Fecha:**

Vigencia: Este SLA entra en vigor a partir de su firma y será revisado cada 12 meses

o cuando un cambio significativo en la infraestructura, normativa o nivel de amenaza lo re

Anexo 17. PLAYBOOK SOC vs PHISHING

Caso: Posible phishing/malware en infraestructura externa a la UACJ
Indicadores:
IP: `XXX.XXX.XXX.XXX` (Se declara la IP de destino del portal que suplanta)
Dominio: `urlmaliciosa.com` (Se define el dominio utilizado)
Proveedor: `AWS/Azure/GCC` (Se identifica el proveedor del servicio de hosting)

🎯 Objetivo

Detectar, contener y erradicar amenazas alojadas en servicios cloud compartidos.

🔎 Fase 1: Detección y validación

📥 Fuentes de alerta

SIEM (Wazuh / ELK).
EDR (CrowdStrike).
Proxy / Firewall / DNS logs.
Reporte de usuario.

🧪 Validaciones técnicas

1. Resolución DNS

```
nslookup "urlmaliciosa.com "
```

2. WHOIS / RDAP

Confirmar proveedor (**AWS**, Azure, Google, etc)

3. HTTP inspection o sandbox (Any.Run)

```
curl -I http:// urlmaliciosa.com
```

⚠️ Nunca abrir directo en endpoint productivo.

🔍 Enriquecimiento

VirusTotal
URLScan
Passive DNS
Certificados TLS

⚠️ Fase 2: Clasificación

Criterio	Resultado
Infraestructura	Cloud compartido
Suplantación	Sí (UACJ)
Historial abuso	Sí
Riesgo	**MEDIO-ALTO**

🛑 Fase 3: Contención

🔐 Acciones inmediatas

Tenant de Microsoft

Informar al administrador del Tenant de Microsoft (Ing. Luis Carpio) para que actúe conforme a sus procedimientos.

Obtener indicadores: direcciones IP de origen de los correos, cantidad de correos recibidos, listado de usuarios, etc.

Firewall / Proxy

```
block domain urlmaliciosa.com (Portal malicioso)
block ip XXX.XXX.XXX.XXX (Portal malicioso)
block ip XXX.XXX.XXX.XXX (Mail sender)
```

EDR

Buscar conexiones hacia esa IP/dominio en Firewall y en SIEM

Aislar endpoints sospechosos

🔎 Threat hunting

Buscar en logs:

Ejemplo (SIEM query genérica):

```
WHERE dns_query = " urlmaliciosa.com "
OR destination_ip = " XXX.XXX.XXX.XXX "
```

🧹 Fase 4: Erradicación

Si hubo impacto:

Eliminar payloads

Reset de credenciales comprometidas

Revisión de persistencia:

tareas programadas

servicios

registry

📢 Fase 5: Notificación

Reportar a AWS (abuse)

Reportar AbuseIPDB

Reportar CSIRT- LACNIC (en caso de persistencia)

Notificar usuarios internos

Documentar incidente

🧠 Fase 6: Lecciones aprendidas

Bloqueo de dominios dinámicos

Concientización phishing

Reglas de detección nuevas