Construcción de un CSIRT con Herramientas de Software Libre para el Área de Tecnología de una IES

Diego Fernando Reina Arévalo, Zharet Bautista Montes
d.reinaa@uniandes.edu.co, zd.bautista@uniandes.edu.co
Maestría en Seguridad de la Información
Universidad de los Andes, Bogotá, Colombia

***Resumen*—Las instituciones de educación superior enfrentan un incremento de amenazas de ciberseguridad que demandan capacidades eficientes de respuesta ante incidentes. En este contexto, este proyecto sugiere el diseño e implementación de un equipo de respuesta a incidentes de seguridad informática (CSIRT) para el Área de Tecnología de una IES. La propuesta se fundamenta en los marcos NIST SP 800-61, ISO/IEC 27035 y FIRST, e integra aspectos organizacionales, técnicos y operativos que definen roles, servicios, flujos de información y procesos estandarizados para la gestión de incidentes. Como parte del enfoque metodológico, se desarrolla un Mínimo Producto Viable (MVP) basado en las herramientas de software libre (Wazuh y MISP), implementado en un entorno de contenedores y validado mediante simulaciones de web defacement y Ransomware, lo que permitió verificar su comportamiento frente a escenarios reales de compromiso. Se establecen indicadores clave de desempeño (MTTD, MTTR y tasa de eficiencia) para medir la mejora frente a la línea base institucional. Los resultados muestran el potencial del modelo para reducir tiempos de detección y respuesta, fortalecer las capacidades técnicas del área de tecnología y sentar bases para un CSIRT institucional sostenible. Finalmente se elabora un plan de mejora continua y recomendaciones para su despliegue en producción.**

Palabras Claves - CSIRT, Respuesta a incidentes, Wazuh, MISP, Indicadores de compromiso, NIST SP 800-61, ISO/IEC 27035, FIRST

I. Introducción

Un equipo de respuesta a incidentes de seguridad informática (CSIRT) constituye el mecanismo institucional encargado de prevenir, detectar, analizar y coordinar la respuesta ante eventos que afectan los activos digitales. Su implementación permite centralizar procedimientos, reducir los tiempos de reacción, estandarizar la comunicación entre áreas técnicas, fortalecer la resiliencia tecnológica y alinear la institución con marcos de referencia ampliamente reconocidos para dar cumplimiento normativo. Sin embargo, la conformación de un CSIRT no es únicamente un desafío técnico, sino también organizacional, pues implica estructurar roles, servicios, flujos de información, herramientas y métricas de desempeño que garanticen una operación eficaz y sostenible [1-7].

II. Definición del Problema

Las instituciones de educación superior enfrentan crecientes amenazas en materia de ciberseguridad debido al manejo intensivo de datos personales, financieros, académicos e investigativos, y cuando estas amenazas consiguen ocasionar incidentes, la capacidad de respuesta es vital para reconocerlos, resolverlos y prevenir su repetición. En consecuencia, la Institución de Educación Superior (IES) en estudio precisa de un equipo estructurado y formalizado de respuesta ante incidentes de seguridad informática (CSIRT) que articule de manera sistemática la detección, análisis, respuesta y comunicación de incidentes, y aunque ya existen lineamientos, herramientas y procedimientos básicos, estos no constituyen aún un marco integral que garantice tiempos de respuesta óptimos, estandarización de procesos y coordinación entre dependencias. Esta situación expone a la universidad a riesgos de afectación de la confidencialidad, integridad y disponibilidad de la información, además de potenciales incumplimientos normativos.

III. Propuesta de Solución

A. Objetivo General

Diseñar un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) para una IES, que permita fortalecer la capacidad institucional para prevenir, detectar, gestionar y recuperar incidentes de seguridad de la información, garantizando la continuidad académica y administrativa.

B. Objetivos Espectficos

- Analizar el marco normativo, estándares y buenas prácticas internacionales (NIST SP 800-61, ISO/IEC 27035 y FIRST) y compararlos con las políticas y procedimientos actuales de la IES sobre incidentes de seguridad.
- Identificar brechas y necesidades institucionales en la gestión de incidentes de seguridad informática, a partir de entrevistas, revisión documental y análisis de riesgos.
- Diseñar la estructura organizacional y operativa del CSIRT, definiendo roles, responsabilidades, procesos, servicios y herramientas que deben ser implementados en el contexto universitario.
- Proponer un modelo de procesos estandarizados para la gestión del ciclo de vida de incidentes (detección, análisis, contención, erradicación, recuperación y lecciones aprendidas).

- Integrar herramientas y procesos que ya se han implementado para aprovechar los recursos y conocimientos disponibles, así como agilizar la implementación del CSIRT.

- Definir indicadores de desempeño y métricas de efectividad que permitan evaluar el impacto del CSIRT en la reducción de riesgos y en la mejora continua de la seguridad institucional.

IV. Marco Teórico

La creación y operación de un Computer Security Incident Response Team (CSIRT) requiere sustentarse en marcos normativos y guías internacionales que definan buenas prácticas para la gestión de incidentes y la coordinación de la respuesta. Entre los estándares más utilizados se encuentran el NIST SP 800-61r2, la ISO/IEC 27035, y las recomendaciones del FIRST (Forum of Incident Response and Security Teams). Estos marcos proporcionan lineamientos complementarios que permiten estructurar un proceso de gestión de incidentes consistente, repetible y alineado con las necesidades operativas de las organizaciones.

A. NIST SP 800-61r2: Computer Security Incident Handling Guide

El estándar del NIST ofrece un marco operativo centrado en cuatro fases principales: Preparación, Detección y Análisis, Contención–Erradicación–Recuperación, y Actividades Post-Incidente. Su enfoque se distingue por su carácter práctico y orientado a la implementación de procedimientos, métricas y capacidades técnicas específicas [8].

Ventajas

- Proporciona lineamientos detallados y operativos fáciles de adaptar.
- Incluye recomendaciones sobre herramientas, tipos de incidentes y guías para mejorar la detección.
- Adecuado para entornos que necesitan procesos claros y estructurados.

Desventajas

- No está pensado como un estándar certificable.
- Su enfoque es mayormente técnico, por lo que puede requerir complementar normas de gobernanza más generales.

B. ISO/IEC 27035: Gestión de Incidentes de Seguridad de la Información

La ISO 27035 se divide en varias partes que abordan desde los principios y conceptos fundamentales hasta la implementación del proceso completo. Presenta un marco más amplio para asegurar la continuidad de negocio, la gestión del riesgo y la integración con el Sistema de Gestión de Seguridad de la Información (SGSI) [9].

Ventajas

- Enfoque integral, alineado con la ISO/IEC 27001 y con modelos de madurez de seguridad.
- Facilita la estandarización, la documentación y la auditoría.
- Recomendado para organizaciones que requieren cumplimiento normativo formal.

Desventajas

- Menos detallada en aspectos técnicos específicos.
- Su implementación completa puede ser más exigente en términos de documentación y control.

C. FIRST: Best Practices y CSIRT Framework

FIRST es una organización global que reúne a equipos de respuesta a incidentes y define buenas prácticas ampliamente adoptadas. Sus lineamientos se centran en capacidades clave, roles funcionales, intercambio de información (incluyendo IoCs), comunicación coordinada y cooperación internacional [10].

Ventajas

- Promueve estándares para la colaboración, elemento crítico en la respuesta a incidentes.
- Define roles, niveles de madurez y capacidades que debe poseer un CSIRT.
- Apoya el uso de plataformas de intercambio como MISP.

Desventajas

- No es un estándar formal o certificable.
- Sus recomendaciones requieren complementarse con marcos operativos como NIST o ISO.

D. Integración de los Estándares para la Construcción del CSIRT

La complementariedad entre estos marcos permite construir un CSIRT robusto:

- NIST proporciona la estructura operativa y el flujo técnico del ciclo de incidentes, contribuye a delimitar las fases de los procedimientos de gestión de incidentes como Web Defacement y Ransomware.
- ISO/IEC 27035 garantiza coherencia con la gobernanza, el SGSI y el cumplimiento normativo, define los requisitos por verificar en el CSIRT construido.
- FIRST aporta prácticas de cooperación, coordinación, madurez y estandarización del intercambio de inteligencia de amenazas, fundamentales para integrar herramientas, y ayuda a definir los servicios que se formalizan y va a ofrecer el CSIRT.

A partir de esta integración, se establece un CSIRT que combina procesos formales, capacidades técnicas de monitoreo y análisis, y mecanismos de intercambio de información, logrando un modelo funcional, escalable y alineado con los estándares internacionales reconocidos.

V. Diseño e Implementación

En esta sección se detallan los requerimientos que deben cumplir las herramientas seleccionadas para el modelo, se

analizan y comparan las alternativas disponibles y se expone como cada una aporta a la solución del problema identificado. Asimismo, se describe la arquitectura propuesta para el Mínimo Producto Viable (MVP), el cual reproduce a un nivel esencial el funcionamiento esperado de un CSIRT en operación.

A. Requerimientos Funcionales

- Monitorear continuamente el estado de los activos de interés.
- Identificar y alertar oportuna y detalladamente incidentes de seguridad.
- Categorizar y priorizar los incidentes detectados para asignarles el tratamiento respectivo y recursos razonables.
- Ejecutar y registrar las respuestas aplicadas para cada incidente.
- Comunicar los incidentes y acciones de respuesta a la comunidad universitaria de la IES.
- Documentar el contexto de cada incidente y el proceso manejado para él, con el fin de mejorar continuamente el sistema.

B. Requerimientos No Funcionales

- Disponibilidad mínima: canales de reporte, servicios esenciales y documentación accesibles al menos un 99.9 % del tiempo.
- Eficiencia: dependiendo del tipo y gravedad del incidente, se debe responder en un tiempo razonable que posibilite una recuperación pronta y satisfactoria.
- Escalabilidad: la estructura implementada debe poder adaptarse a la entidad conforme ésta vaya creciendo o cambiando en el futuro.
- Usabilidad: procesos y herramientas que los roles interesados puedan entender y utilizar apropiadamente; en particular, para el reporte de incidentes, formularios e interfaces comprensibles para usuarios no técnicos.
- Trazabilidad: mediante registros de auditoría y documentación de procesos.

C. Requerimientos Técnicos

- Herramientas de software libre, que no representen costos en licencias de uso, según los servicios que aún falten por implementar.

D. Análisis de herramientas

Una vez se analizaron las herramientas existentes en el área de tecnología de la IES e identificar las funciones que realiza cada una, se determinó que precisa herramientas con las funciones de: 1) monitoreo de integridad de archivos (más conocido como FIM), 2) evaluación de la configuración de seguridad (también como SCA) del dispositivo, no limitado por el sistema operativo, 3) inteligencia de amenazas, principalmente correlación de indicadores de compromiso (IoC) y asociación de técnicas, tácticas y procedimientos (TTP) y 4) elaboración de estadísticas y reportes utilizables para análisis post-mortem. Asimismo, como criterios de selección se definen los siguientes:

- Usabilidad: permiten de manera práctica configurar, administrar y revisar el funcionamiento de la herramienta. Por ejemplo: incluye una interfaz gráfica en lugar de depender enteramente de comandos.
- Comunidad y Soporte: dispone de extensa documentación y existen numerosos recursos para consultar sus características y preparación adecuadas, corrección de errores e implementaciones adicionales (como scripts para integración).
- Portabilidad: se pueden implementar en distintos tipos de dispositivos y sistemas operativos, no dependen de aplicaciones externas para su funcionamiento.
- Escalabilidad: sus requerimientos de hardware y software se pueden satisfacer sin demasiado esfuerzo o recursos, corregir errores en ellos toma un tiempo razonable.
- Integración: ofrecen opciones para transferir información y activar funciones de otras herramientas ya presentes y necesarias para continuar el proceso de gestión de incidentes.

Con esto mente, y confirmando que las herramientas consultadas sean de software libre, se realizan los siguientes hallazgos: las funciones 1) y 2) se encuentran OSSEC, Wazuh y OpenEDR [11-13], donde:

- Pese a ser el predecesor de Wazuh, OSSEC presenta limitaciones en su interfaz gráfica y sus opciones de FIM.
- Por su parte, Wazuh y OpenEDR cuentan con un dashboard moderno y capacidades de FIM completas. También permiten integración con otras herramientas mediante recursos mínimos (scripts y llaves API).
- Ahora bien, OpenEDR tiene requerimientos más elevados a nivel de dispositivo final (endpoint) y, al igual que OSSEC, su comunidad de soporte es bastante limitada.
- Mientras tanto, Wazuh dispone de una comunidad activa y documentación actualizada, y sus requerimientos se concentran más a nivel de servidor en lugar de los endpoint, lo que le permite ser más escalable.

En cuanto a las funciones 3) y 4), se estudian MISP y OpenCTI [14, 15] con los siguientes resultados:

- Ambas cuentan con una interfaz gráfica intuitiva, análisis

detallado de IoC, una comunidad de soporte fuerte y capacidades de integración con otras herramientas.
- No obstante, OpenCTI muestra opciones limitadas para TTP y altos requerimientos de infraestructura que limitan su despliegue; en comparación, MISP es más escalable e incluye clusters de información (galaxias) que asocian numerosas características de amenazas e incidentes, proporcionando un análisis más completo.

E. Herramientas propuestas y características

Para este proyecto, se eligieron dos herramientas principales de estudio: Wazuh [16, 17], que actúa como HIDS al vigilar la integridad de los datos y los cambios de configuración en el dispositivo analizado, así como activar acciones de respuesta, con lo que soporta las operaciones de detección, contención, erradicación y recuperación; y MISP [18, 19], que ofrece una plataforma para inteligencia de amenazas integral, lo que contribuye al análisis de incidentes, la comunicación de eventos y las lecciones aprendidas.

- Detección de incidentes: Wazuh permite identificar eventos de seguridad en tiempo real mediante reglas configuradas previamente y registrar alertas que contienen información detallada del suceso.
- Registro del incidente: Wazuh puede enviar la información del incidente hacia MSIP, donde se crea el evento de seguridad con sus indicadores, de acuerdo a las etiquetas definidas. Además, MISP genera automaticamente tickets en GLPI y/o envia notificaciones por correo, demostrando la funcionalidad de coordinación integral de todos los componentes del sistema.
- Analisis del incidente: MISP realiza la correlacion de todos los IoC generados y los eventos con información del contexto, incluyendo tácticas, técnicas y procedimientos (TTP) asociados; así, la plataforma no solo registra eventos, si no que añade datos relevantes que ayudan a identificar las características del evento y su impacto.
- Contencion automatica: Ante incidentes especificos, el agente de Wazuh ejecuta scripts de respuesta preliminarmente configurados. Estas acciones constituyen la fase inicial de contención y demuestran la capacidad del sistema para reaccionar de manera automatica ante intervenciones.
- Recuperación integrada: Wazuh puede activar procesos de recuperación mediante su integración con Veeam. Esto hace posible iniciar restauraciones de copias de seguridad cuando así lo determinan las reglas de respuesta.
- Lecciones aprendidas: MISP permite visualizar estadísticas y generar reportes de los eventos registrados. Estos eventos facilitan la documentación de hallazgos, la identificación de patrones y la retroalimentación para mejorar las reglas de detección y respuesta.

F. Modelo de despliegue del MVP

Se investigó la forma de construir un laboratorio donde se visualizara el funcionamiento de ambas herramientas y la simulación de los dos incidentes en estudio para obtener métricas de desempeño y evaluar resultados de manera práctica, y que al mismo tiempo permita satisfacer los requerimientos técnicos de estas herramientas.

El uso de contenedores para el desarrollo del MVP ofrece ventajas en los siguientes ámbitos: permite aislar cada componente del sistema, garantizar entornos reproducibles y facilitar la portabilidad entre distintas plataformas, contribuye a un despliegue ágil y eficiente reduciendo el consumo de recursos, mientras que su modularidad simplifica la integración, configuración previa, actualización y sustitución de herramientas como Wazuh y MISP [21]. Estas características resultan especialmente valiosas en un proyecto experimental, al permitir pruebas controladas, escalabilidad progresiva y una validación precisa del modelo propuesto para el CSIRT. Se optó entonces por implementar el sistema con base en contenedores, organizados de la siguiente forma:

- El primero alberga los componentes del Servidor de Wazuh: el Dashboard, que corresponde a la interfaz gráfica que agiliza su configuración y operación; el Indexer, que administra la información de logs y realiza análisis sobre ellos; y el Manager, que gestiona la comunicación con los agentes y ejecuta las acciones de respuesta.
- El segundo alberga MISP y todas las aplicaciones que necesita para su funcionamiento (Base de Datos, Servidor Web, SMTP, etc.)
- El tercero incluye un servidor web, un volumen de archivos y directorios y un Agente de Wazuh para monitoreo: su propósito es desempeñar el rol del equipo víctima, donde se replicarán los incidentes de Web Defacement y Ransomware.
- El último cuenta con Kali Linux, un sistema operativo de pruebas de penetración, para que actúe como atacante hacia el equipo víctima.

Los contenedores están conectados por una red interna con previas configuraciones personalizadas y cada uno tiene una dirección IP identificable; así mismo, desde el host se puede acceder a las interfaces gráficas de las 2 herramientas principales (Wazuh y MISP) por medio de puertos específicos. La configuración de los contenedores y la comunicación entre ellos se muestra en el siguiente esquema.

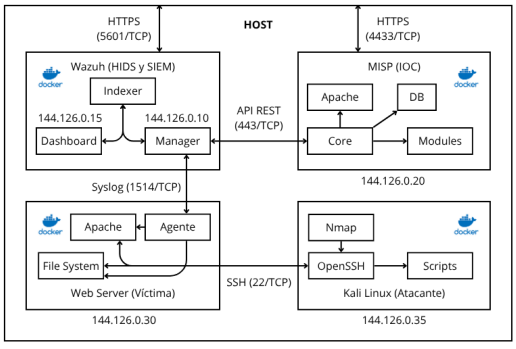

Figura 1. Arquitectura del MVP implementado

VI. Evaluación y Análisis de Resultados

A. Diseño de pruebas para evaluación

Para simular los incidentes, primero se instala en la máquina atacante los paquetes de OpenSSH y Python para ejecución remota de scripts, y luego se dejan dos scripts que ejecutarán versiones simplificadas de Web Defacement y Ransomware. En cada iteración, el contenedor Kali cambiará de IP y ambos scripts recibirán una ruta objetivo diferente como parámetro, para proporcionar variabilidad a las pruebas.

El script de Web Defacement tendrá las siguientes acciones:

- Establecer una conexión SSH con la víctima
- Cambiar los permisos de la ruta /var/www/html del servidor web
- Alterar los archivos del servidor web (/var/www/html)

El script de Ransomware tendrá las siguientes acciones:

- Establecer una conexión SSH con la víctima
- Crear archivo con extensión .enc en la ruta /home/tester/target
- "Cifrar" (cambiar el contenido) los archivos en el volumen de archivos (/home/tester/target)

Después, en el servidor de Wazuh se establecerán reglas de detección personalizadas para los sucesos descritos previamente, cada una asociada a un script de respuesta activa (Active Response) dentro de la víctima y que, una vez recibida la respectiva alerta, el Agente de Wazuh va a ejecutar para una de las siguientes acciones:

- Bloquear conexión desde una IP específica por un tiempo
  - IoC: dirección IP
- Revertir el cambio de permisos sobre una ruta
  - IoC: ruta afectada y permisos configurados
- Eliminar archivo con una extensión particular
  - IoC: nombre del archivo y ruta afectada
- Restaurar archivos de una ruta indicada
  - IoC: ruta afectada

Adicionalmente, dentro del servidor de Wazuh se creará también un script para que, ante la detección de cualquiera de estos sucesos, se contacte con la API de MISP y se cree un evento al que, dependiendo del tipo de incidente y del indicador de compromiso enviados, se le añadirá para caracterización:

- Una etiqueta del protocolo TLP para indicar el nivel de visibilidad que debe tener el evento (va de White → público a Red → altamente confidencial).
- Una etiqueta del Unified Kill Chain para señalar la fase del incidente al que pertenece la alerta (Delivery, Exploitation, Persistente, etc.)
- Un cluster del marco MITRE ATTACK para identificar la amenaza y adjuntar información de indicios, medidas de mitigación e incidentes asociados.

Finalmente, se crean dos flujos de trabajo en MISP para que, cuando se genere un evento con una etiqueta de TLP Red, el primero envíe una notificación de correo a una dirección de prueba dedicada, y el segundo ejecute un script para enviar una solicitud a la API de GLPI y generar un ticket, aunque este último no se activa en la fase de pruebas. En la siguiente imagen se resume el diseño de pruebas planificado para el modelo.

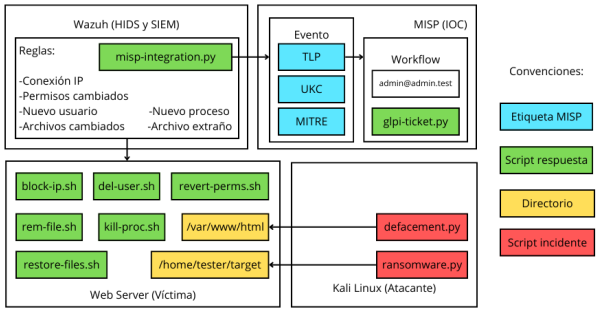

Figura 2. Diseño de pruebas en el MVP

B. Indicadores de desempeño

Para medir el desempeño del MVP construido, se establecen los siguientes indicadores:

- MTTD: Tiempo desde que ocurre el incidente hasta que es detectado
- MTTR: Tiempo desde que detecta hasta que se resuelve el incidente
- Tasa de eficiencia: # incidentes que atravesaron exitosamente todo el proceso de gestión de incidentes / # de incidentes que fueron detectados.

En cada intento se prueba con una IP distinta, 3 repeticiones para cada simulación de incidente, y se registra el tiempo más alto en cada fase. Durante cada intento se miden cuatro tiempos diferentes:

- Alerta en Wazuh: desde que termina el simulacro de incidente hasta que es detectado en Wazuh, esto incluye no sólo el registro en logs, sino también el tiempo que toma en aparecer en la interfaz gráfica.
- Evento en MISP: desde que se registra la alerta en Wazuh hasta que se genera un evento en MISP con todas las respectivas etiquetas.
- Active Response: desde que se registra la alerta en Wazuh hasta que se termina de ejecutar el script de respuesta activa en el agente, incluido el registro en el log.
- Email desde MISP: Desde que se crea el evento en MISP hasta que se recibe el correo, esto incluye todas las verificaciones dentro de MISP.

Cabe recordar que estos valores reflejan las capacidades estrictamente técnicas del potencial CSIRT, no involucran las actividades administrativas o humanas, por lo que se esperan valores reducidos del orden de segundos o minutos, y pueden variar en función de la infraestructura donde se aplique y la carga de información que se maneje. Para el caso de las

pruebas, el MTTD corresponderá al mayor valor entre la Alerta en Wazuh y el Evento en MISP, que ocurren de forma simultánea, mientras que MTTR equivale al tiempo de Active Response.

Por su parte, la línea base, que define la posición actual de la DSIT, se fija en los siguientes indicadores disponibles: tiempo de primer contacto (similar al MTTD) de 12-24 horas, tiempo de respuesta de incidente (similar al MTTR) de 4 a 5 días. Cabe recordar que estos valores corresponden a reportes de incidentes externos e involucran capacidades administrativas además de las técnicas. Teniendo eso en cuenta, los valores objetivo que se esperan lograr para el proyecto en una fase consolidada son: tiempo de primer contacto de máximo 8 horas, tiempo de respuesta de incidente de 2-3 días y una tasa de eficiencia igual o mayor al 90 %.

C. Valores estimados a partir de las pruebas

En la siguiente tabla se puede ver el resumen de los tiempos registrados en las pruebas.

Fase	T1	T2	T3	T4	T5	Media
Alerta en Wazuh	6	12	10	9	8	9
Evento en MISP	3	1	1	2	2	1.8
Active Response	3	5	4	3	1	3.2
Notificación por email	18	17	18	16	16	17
Tiempo Total	30	35	33	30	27	31

Tabla I
TIEMPOS DE RESPUESTA A INCIDENTES POR FASES

Como se puede ver, el MTTD resultante se estima en aproximadamente 8-12 segundos de duración, mientras que el MTTR se calcula como 3-5 segundos de duración, por lo que el proceso completo de respuesta a incidentes se ejecuta en aproximadamente 12-15 segundos en el MVP (llega a 30 segundos si se incluye la notificación por email, aunque esto sólo ocurre para algunos eventos específicos).

Se puede ver que la alerta en Wazuh es la segunda fase que toma más tiempo, principalmente en lo que respecta a la actualización de la interfaz (el principal que se utiliza para detectar los incidentes), aunque a nivel de logs el tiempo de detección y registro de la alerta es de sólo 1-3 segundos. En cuanto a la notificación por email desde MISP, se estima como la fase más extensa debido a que requiere de la intervención de un servidor SMTP y, por tanto, depende de la latencia del sistema en que se implemente.

Finalmente, sin tomar en cuenta la fase de notificación desde MISP, el proceso de respuesta a incidentes completó todas las fases para 26 de 30 pruebas independientes, lo que propone una tasa de eficiencia inicial del 86 %.

D. Resultados logrados en el proyecto

- Se elaboró, con ayuda de los marcos normativos, un diagnóstico sobre las capacidades actuales del área de tecnología y las capacidades futuras que se necesitan implementar para avanzar en la construcción de un CSIRT completamente funcional.
- Se analizaron y evaluaron distintas herramientas para determinar cuáles podían cubrir las capacidades futuras previstas y, al mismo tiempo, ajustarse a los requerimientos establecidos y a los criterios definidos para su selección.
- Se construyó un entorno de laboratorio donde se instalaron, configuraron y consolidaron en funcionamiento las herramientas en estudio (Wazuh y MISP), y se estableció un diseño para las pruebas con este entorno y unos artefactos para verificar su ejecución.
- Luego de la ejecución de pruebas, se estimó para el MVP un MTTD de 8-12 segundos, un MTTR de 3-5 segundos y una Tasa de Eficiencia del 86 %. Con un tiempo notablemente reducido, estos valores sugieren la agilización de las partes más críticas de la respuesta a incidentes (detección, análisis, contención, erradicación y recuperación).

Si ahora nos remitimos a los niveles de madurez del marco SIM3, podemos afirmar, por un lado, que el nivel del área de tecnología al inicio estaba en el nivel 2 (Definido), pues ya contaba con políticas, procedimientos, clasificación de incidentes, inventario de activos y capacitación inicial en respuesta a incidentes; por otro lado, se estima que, luego de finalizar el MVP, el área de tecnología se podría ubicar en el nivel 3 (Implementado/Operacional), donde ya puede establecer métricas de MTTD y MTTR, llevar a cabo ejercicios table-top o simulaciones de respuesta a incidentes y generar informes post-mortem, todo de forma consistente; finalmente, al avanzar a la fase consolidada, se espera que llegue por lo menos a un nivel 4 (Integrado/Gestionado), donde ya ejecuta respuesta automatizadas, se integra con otras áreas de gestión de riesgos, coopera con otros CSIRT y produce una mejora continua de las políticas, lo que se denomina un CSIRT institucionalizado.

VII. CONCLUSIONES

- El estudio permitió determinar que, aunque la IES cuenta con lineamientos generales sobre seguridad de la información, estos no alcanzan el cumplimiento normativo de estándares internacionales como NIST SP 800-61, ISO/IEC 27035 y directrices de FIRST, ni un nivel de madurez satisfactorio según SIM3. La revisión documental y el análisis de riesgos reflejaron brechas en capacidades técnicas, procesos, roles y mecanismos de respuesta, lo que confirma la necesidad institucional de establecer un CSIRT.

- Además, la interacción de herramientas ya presentes en la universidad permite optimizar recursos, mejorar la automatización y acelerar la implementación del CSIRT sin sustituir la infraestructura establecida. Finalmente, la definición de indicadores de desempeño y métricas de

efectividad sienta las bases para evaluar el impacto del equipo y promover la mejora continua de la postura de ciberseguridad institucional.

- Con respecto a la construcción del MVP, para la selección de herramientas se revisaron no sólo sus requerimientos técnicos, sino sobre todo las capacidades adicionales que podrían ofrecer al sistema actual y, aunque en esta fase se presentaron desafíos para consolidar el funcionamiento y la ejecución de pruebas en el modelo, eventualmente permitió comprender mejor la configuración y operación de estas herramientas, información que luego servirá para agilizar su implementación en la IES.

- En conjunto, los resultados demuestran que la creación del CSIRT es una necesidad fundamental para fortalecer la resiliencia operativa, reducir riesgos y consolidar la seguridad de la información en la IES en estudio. El resultado final de este proyecto establece un punto de referencia a partir del cual el área de tecnología de la IES puede avanzar en la efectiva implementación y funcionamiento del CSIRT.

VIII. Trabajo Futuro

Con base en el progreso alcanzado hasta la fecha, se definen las siguientes tareas pendientes para completar la implementación, validación y despliegue del proyecto.

- Realizar un proceso de revisión sobre la gestión del propio proyecto para identificar qué ámbitos se deben solventar antes de pasar al despliegue en producción.
- Preparar un plan de implementación que priorice unas tareas específicas de forma que el Piloto ya empiece a apoyar la gestión de incidentes en la misma área de tecnología de la IES.
- Definir en el mismo plan las tareas que se desarrollaran posteriormente para avanzar hacia la fase consolidada del CSIRT.
- Adelantar los procedimientos de gestión para la instalación y configuración de sus componentes técnicos (herramientas y recursos) del CSIRT en producción.
- Establecer un tiempo para la verificación de operación del CSIRT en producción y la capacitación del personal que va a administrarlo.
- Examinar su utilidad y desempeño en un espacio de tiempo que permita comparar el beneficio actual obtenido con el estimado en el planteamiento.
- Realizar mantenimiento periódico para asegurar su funcionamiento y eficiencia, registrar su desempeño a lo largo de la gestión de diversos casos de incidentes.

Referencias

[1] Banco Santander y SEGIB, Ün 60 % de las universidades iberoamericanas sufrió ciberincidentes o ciberataques en el último año,Çomunicación Universidades, Banco Santander, Madrid, España, 18-Jun-2025. [En línea]. Disponible en: https://www.santander.com/es/sala-de-comunicacion/notas-de-prensa/2025/06/un-60-de-las-universidades-iberoamericanas-sufrio-ciberincidentes-o-ciberataques-en-el-ultimo-ano

[2] J. Carvallo, Ïnnovando en el sector de la ciberseguridad,"Tendencias emergentes en ciberseguridad: retos actuales y futuros en entornos TIC, 03-Jul-2024. [En línea]. Disponible en: https://multimedia.cedia.edu.ec/wp-content/docs/VTIC_ciberseguridad.pdf

[3] I. U. Colmayor, "Modelo de Seguridad y Privacidad de la Información,"2025. [En línea]. Disponible en: https://www.colmayor.edu.co/wp-content/uploads/2025/07/Modelo-de-Seguridad-y-Privacidad-de-la-Informacio %CC %81n.pdf

[4] Insighted Media, Çiberseguridad: universidades aumentan la protección ante la suba de ataques,"29-Jul-2025. [Publicación en línea]. Disponible en: https://insighted.media/post/ciberseguridad-universidades-aumentan-la-proteccion-ante-la-suba-de-ataques

[5] UNAD, Ïnteligencia artificial y ciberseguridad: retos en la educación superior,"Noticias UNAD, 04-Oct-2025. [Publicación en línea]. Disponible en: https://noticias.unad.edu.co/index.php/2025/7791-inteligencia-artificial-y-ciberseguridad-retos-en-la-educacion-superior

[6] UNAD, Resultados del análisis de riesgos de ciberseguridad: universidades frente a las nuevas amenazas digitales,"Noticias UNAD, 15-Oct-2025. [Publicación en línea]. Disponible en: https://noticias.unad.edu.co/index.php/2025/7818-resultados-del-analisis-de-riesgos-de-ciberseguridad-universidades-frente-a-las-nuevas-amenazas-digitales

[7] UNAD-CSIRT, Resolución del Comité Directivo Técnico CSIRT,ÜNAD CSIRT, 2023. [En línea]. Disponible en: https://csirt.unad.edu.co/images/2023/Publicaciones/ResolucionCDTCSIRT.pdf

[8] National Institute of Standards and Technology (NIST), Ïncident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile,"NIST Special Publication 800-61 Revision 3. Gaithersburg, MD, USA: NIST, Abr. 2025. DOI: 10.6028/NIST.SP.800-61r3. [En línea]. Disponible en: https://csrc.nist.gov/pubs/sp/800/61/r3/final

[9] Gesdata Consulting, ÏSO 27035: Gestión de Incidentes de Seguridad de la Información,"Gesdata Consulting, Ago. 2024. [Publicación en línea]. Disponible en: https://gesdataconsulting.es/iso-27035

[10] Forum of Incident Response and Security Teams (FIRST), Çomputer Security Incident Response Team (CSIRT) Services Framework, Version 2.1."Nov. 2019. [En línea]. Disponible en: https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2-1

[11] A. Trunck, .ºSSEC vs Wazuh,"trunc.org, 10-Dic-2017. [Publicación en línea]. Disponible en: https://trunc.org/ossec/ossec-vs-wazuh

[12] OpenEDR, .ºpenEDR - Open Source EDR,.ºpenEDR. [En línea]. Disponible en: https://www.openedr.com/

[13] M. Monteros, J. F. Chuqui, N. Benitez Cacao, y P. Velez Guerrero, Ïmplementar un sistema de gestión y análisis de seguridad con la herramienta Wazuh, en el Instituto Superior Universitario Tecnológico del Azuay,.ªTENAS Revista Científica Técnica Y Tecnológica, vol. 3, no. 1, p. 16, Ago. 2024. DOI: 10.36500/atenas.3.006. [Documento en línea]. Disponible en: https://atenas.tecazuay.edu.ec/index.php/revista/article/view/79

[14] OpenCTI-Platform, .ºpenCTI-Platform/opencti: Cyber Threat Intelligence platform,"GitHub. [Repositorio de código en línea]. Disponible en: https://github.com/OpenCTI-Platform/opencti

[15] Cosive, .ºpenCTI alternative,Çosive Blog, 05-Abr-2022. [Publicación en línea]. Disponible en: https://www.cosive.com/opencti-alternative

[16] Wazuh, Çonfiguration assessment - Use cases,"Wazuh documentation, 18-Sep-2023. [Documento en línea]. Disponible en: https://documentation.wazuh.com/current/getting-started/use-cases/configuration-assessment.html

[17] Wazuh, Üse cases - File integrity monitoring,"Wazuh documentation, 02-May-2023. [Documento en línea]. Disponible en: https://documentation.wazuh.com/current/user-manual/capabilities/file-integrity/use-cases/index.html

[18] MISP Project, "MISP - The Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing,"MISP Project. [En línea]. Disponible en: https://www.misp-project.org/

[19] CGII, "02- Direcciones IP con actividad de malware evento MISP,ÇGII - CSIRT Bolivia. [Documento en línea]. Disponible en: https://www.cgii.gob.bo/bookstack/books/gestion-de-incidentes-publico/page/02-direcciones-ip-con-actividad-de-malware-evento-misp

[20] Gcore, Çontainers vs Virtual Machines: Key Differences and Use Cases,"Gcore Learning. [Publicación en línea]. Disponible en: https://gcore.com/learning/containers-vs-virtual-machines