Universidad CENFOTEC

Escuela de Ciberseguridad

Profesor: M.Sc. Miguel Pérez Montero

Modelo de recuperación autónomo para entornos virtuales ante incidentes de seguridad.

PIA-01 Proyecto de investigación aplicada

Elaborado por: David Solano Mora

Tutor: MSeg. Mario Andrés Zamora Madriz

Agosto de 2025

Contenido

Documento de aprobación v
Declaratoria vi
Dedicatoria vii
Resumen viii
1. Capítulo 1. Introducción 1
1.1. Generalidades 1
1.2. Antecedentes 1
1.3. Definición y descripción del problema 2
1.4. Justificación 3
1.5. Viabilidad 3
1.5.1. Punto de vista Técnico 4
1.5.2. Punto de vista Operativo 4
1.5.3. Punto de vista Económico 4
1.6. Objetivos 5
1.6.1. Objetivo General 5
1.6.2. Objetivos específicos 5
1.7. Alcance y Limitaciones 6
1.7.1. Alcances 6
1.7.2. Limitaciones 7
1.8. Marco de Referencia Organizacional y Socioeconómico (sobre pymes) 7
1.8.1. Historia 7
1.8.2. Tipo de Negocio y Mercado Meta 8
1.9. Estado de la cuestión 9
1.9.1. Planificación de la revisión 9
1.9.2. Estado de la cuestión 25
2. Capítulo 2. Marco Conceptual 26
2.1. Conceptos 27
2.1.1. PYMEs (Pequeñas y Medianas Empresas) 28
2.1.2. Gestión de incidentes de ciberseguridad 28
2.2. Funcionamiento de las tecnologías clave 32
2.2.1. Wazuh (Detección y Orquestación de la respuesta) 33

2.2.2. Scripting en Python (automatización de la respuesta) 34
2.2.3. VirtualBox (recuperación por snapshot) 35
2.2.4. Trazabilidad 36
3. Capítulo 3. Marco Metodológico 37
3.1. Tipo de investigación 37
3.2. Alcance Investigativo 37
3.3. Enfoque 38
3.3.2. Encuadre Epistemológico 39
3.3.3. Encuadre axiológico 39
3.4. Diseño 40
3.5. Población y muestreo 40
3.6. Instrumento de recolección de datos 41
3.7. Técnicas de análisis de información 42
4. Capítulo 4. Análisis de diagnostico 44
4.1. Descripción del entorno experimental y aplicación de la matriz de evaluación 44
4.2. Descripción de las métricas registradas 45
4.3. Análisis descriptivo de los resultados 47
4.4. Interpretación del desempeño del modelo en términos de MTTR 49
4.5. Discusión de hallazgos y estabilidad del flujo de recuperación 51
4.6. Conclusiones del diagnóstico 52
5. Capítulo 5. Propuesta de solución 53
5.1. Comprensión del negocio 53
5.2. Comprensión de los datos 56
5.3. Preparación de datos 60
5.4. Modelado 64
5.5. Evaluación 67
5.6. Conclusiones parciales del capítulo 70
6. Capítulo 6. Conclusiones 71
7. Capítulo 7. Bibliografía 73

Índice de Tablas

TABLA 1. COSTOS DE LA INVESTIGACIÓN. 5
TABLA 2. PALABRAS CLAVE. 10
TABLA 3. MUESTRA DE RESULTADOS DE BÚSQUEDA 18
TABLA 4. FORMULARIO PARA LA EXTRACCIÓN DE INFORMACIÓN 21
TABLA 5. EXTRACCIÓN DE INFORMACIÓN DEL ARTÍCULO DEVELOPMENT OR THE SYSTEM FOR AUTOMATED INCIDENT MANAGEMENT BASED ON OPEN-SOURCE SOFTWARE 21
TABLA 6. EXTRACCIÓN DE INFORMACIÓN DEL ARTÍCULO COST-EFFECTIVE RESILIENCE: A COMPREHENSIVE SURVEY AND TUTORIAL ON ASSESSING OPEN-SOURCE CYBERSECURITY TOOLS FOR MULTI-TIERED DEFENSE 22
TABLA 7. EXTRACCIÓN DE INFORMACIÓN DEL ARTÍCULO TESTING SOAR TOOLS IN USE 23
TABLA 8. EXTRACCIÓN DE INFORMACIÓN DEL ARTÍCULO MODELING WAZUH RULES WITH WEIGHTED TIMED AUTOMATA 23
TABLA 9. EXTRACCIÓN DE INFORMACIÓN DEL ARTÍCULO SEVERITY-BASED TRIAGE OF CYBERSECURITY INCIDENTS USING KILL CHAIN ATTACK GRAPHS 24
TABLA 10. EXTRACCIÓN DE INFORMACIÓN DEL ARTÍCULO WAZUH SIEM FOR CYBER SECURITY AND THREAT MITIGATION IN APPAREL INDUSTRIES 25
TABLA 11. ANÁLISIS DE RESULTADOS 25
TABLA 12. FLUJO GENERAL 33
TABLA 13.TRAZABILIDAD 36
TABLA 14. RELACIÓN ENTRE PROBLEMÁTICA DE LAS PYMES Y OBJETIVOS DEL MODELO. 56
TABLA 15. FASES DEL FLUJO DE RECUPERACIÓN Y EVIDENCIAS GENERADAS POR EL MODELO. 64
TABLA 16. RESUMEN DE INDICADORES DE DESEMPEÑO DEL MODELO DE RECUPERACIÓN AUTÓNOMA. 70

Índice de Ilustraciones

ILUSTRACIÓN 1. VALIDACIÓN DE CALIDAD DE IEEE 18
ILUSTRACIÓN 2FUENTE: SCIMAGO 18
ILUSTRACIÓN 3. VALIDACIÓN DE CALIDAD DE PROCEDIA COMPUTER SCIENCE 19
ILUSTRACIÓN 4. VALIDACIÓN DE CALIDAD INTERNATIONAL JOURNAL OF MECHANICAL AND MATERIALS ENGINEERING 19
ILUSTRACIÓN 5. VALIDACIÓN DE CALIDAD COMPUTERS AND SECURITY 19
ILUSTRACIÓN 6. VALIDACIÓN DE CALIDAD DE JOURNAL OF INFORMATION SECURITY AND APPLICATIONS 20
ILUSTRACIÓN 7. NUBE DE PALABRAS 26
ILUSTRACIÓN 8. DIAGRAMA SOBRE LAS FASES DEL MODELO 27
ILUSTRACIÓN 9. EJEMPLO DE REGLA 34
ILUSTRACIÓN 10. PSEUDOCÓDIGO DE LA LÓGICA DE DECISIÓN 35
ILUSTRACIÓN 11. ONTOLOGÍA DEL MODELO DE RECUPERACIÓN AUTÓNOMA 38
ILUSTRACIÓN 12. MATRIZ DE EVALUACIÓN - RECUPERACIÓN AUTÓNOMA 42
ILUSTRACIÓN 13. DIAGRAMA DE FLUJO DE TÉCNICAS DE ANÁLISIS DE INFORMACIÓN 43
ILUSTRACIÓN 14. .TIEMPO PROMEDIO DE LAS DIFERENTES MÉTRICAS EVALUADAS. 47
ILUSTRACIÓN 15. PORCENTAJE DEL TIEMPO TOTAL DEL FLUJO QUE CORRESPONDE A CADA FASE. 49
ILUSTRACIÓN 16. ESTABILIDAD DEL MTTR Y LA VARIACIÓN MARGINAL ENTRE EJECUCIONES (TIME_TO_RESTORE, WORKFLOW_TOTAL). 50
ILUSTRACIÓN 17. ARQUITECTURA GENERAL DEL MODELO DE RECUPERACIÓN AUTÓNOMA. 58
ILUSTRACIÓN 18. DIAGRAMA DE FLUJO DEL PROCESO DE RECUPERACIÓN AUTÓNOMA. 66

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: Maestría Profesional en Ciberseguridad, requisito para optar por el título de grado de **Maestría,** para el estudiante: David Solano Mora.

Digitally signed by MIGUEL PEREZ MONTERO (FIRMA)
Date: 2026.03.03 07:58:51 -06'00'

M.Sc. Mario Zamora Madriz
Tutor

M.Sc. Miguel Pérez Montero
Lector 1

REBECA ESQUIVEL FLORES (FIRMA)
Firmado digitalmente por REBECA ESQUIVEL FLORES (FIRMA)
Fecha: 2026.03.03 14:42:43 -06'00'

M.Sc. Rebeca Esquivel Flores
Lector 2

San José, Costa Rica, 02 de marzo de 2026

Declaratoria

Yo, David Solano Mora, autor del trabajo titulado “Modelo de recuperación autónomo para entornos virtuales ante incidentes de seguridad”, presentado como requisito para optar por el grado de Maestría en Ciberseguridad en la Universidad Cenfotec, autorizo a la Universidad Cenfotec a poner a disposición de la comunidad académica este documento en su biblioteca y en los repositorios institucionales que considere pertinentes, con el fin de que pueda ser consultado, reproducido o utilizado con propósitos exclusivamente académicos, educativos o de investigación.

Esta autorización no implica la cesión de los derechos de autor sobre el contenido del trabajo. Los derechos intelectuales derivados de esta investigación continúan siendo propiedad del autor, por lo que cualquier uso distinto al estrictamente académico deberá contar con la autorización previa y expresa del autor.

Asimismo, se permite la reproducción parcial del documento siempre que se realice con fines académicos y se cite adecuadamente la fuente correspondiente.

Dedicatoria

Dedico este trabajo, en primer lugar, a Dios, por darme la fortaleza, la sabiduría y la oportunidad de culminar esta importante etapa de formación académica.

A mi esposa, por su amor, paciencia y apoyo constante durante todo este proceso. Su comprensión y motivación fueron fundamentales para seguir adelante en los momentos de mayor exigencia.

A mis hijos, quienes con su alegría, amor y energía han sido siempre una fuente de inspiración para esforzarme cada día y procurar ser un mejor ejemplo para ellos.

A mis padres y hermanos, por su apoyo, sus palabras de aliento y por motivarme siempre con su ejemplo de esfuerzo, trabajo y perseverancia.

Asimismo, expreso mi sincero agradecimiento a todas aquellas personas que, de una u otra forma, brindaron su apoyo durante el desarrollo de este trabajo. Ya fuera mediante una palabra de aliento, un consejo oportuno o su acompañamiento a lo largo de este proceso, su contribución fue valiosa para poder culminar satisfactoriamente esta etapa académica.

Resumen

Hoy en día, las pequeñas y medianas empresas (PYMEs) son especialmente vulnerables a los ciberataques debido a sus limitaciones de presupuesto y personal especializado. Este trabajo final de graduación propone un modelo de recuperación autónomo ante incidentes de seguridad que prioriza la restauración de los sistemas después de un ciberataque y la continuidad operativa utilizando herramientas de código abierto. Esta arquitectura integra Wazuh para la detección de amenazas y respuesta activa (active response), scripting en Python para la orquestación de la respuesta y VirtualBox (VBoxManage) para la recuperación en entornos virtualizados. Se establecen criterios de activación, trazabilidad y un instrumento de medición aplicado en un laboratorio controlado, mediante el cual se evalúan métricas de desempeño como el tiempo medio de recuperación (MTTR) y la distribución de tiempos por fase del flujo automatizado.

El aporte principal de este trabajo es un “mini-SOAR” de bajo costo, replicable y alineado con el contexto de las PYMEs que buscan reducir sus tiempos de recuperación y mejorar la ciber resiliencia sin depender de licencias propietarias.

Como limitación, la validación del modelo se realiza en un entorno de laboratorio con un conjunto acotado de escenarios de ataque y una topología específica, por lo que se recomienda en trabajos futuros ampliar el número de casos de prueba y entornos evaluados para reforzar la evidencia empírica sobre su eficacia y viabilidad de adopción.

Palabras clave: Ciber resiliencia, respuesta a incidentes, Wazuh, SOAR, VirtualBox, Python, snapshots, PYMEs, recuperación autónoma.

1. Capítulo 1. Introducción

1.1. Generalidades

Con la intención de brindar un apoyo a uno de los problemas más comunes hoy en día como son los ciberataques, se desarrolla este proyecto para crear un modelo de respuesta autónoma, para entornos virtuales, en caso de ataques comunes, como por ejemplo: (ransomware, fuerza bruta SSH, etc). Para esto se piensa utilizar herramientas de Open Source, las cuales, predispuestas en la configuración correcta, formarán un modelo que puede ser capaz de realizar acciones en caso de un ataque cibernético.

1.2. Antecedentes

Hoy en día, los ciberataques han evolucionado a tal punto que han dejado mucho daño a su paso, esto se puede traducir en pérdidas de dinero millonarias, pérdida de confianza en las empresas y problemas legales por la exposición de datos sensibles de clientes o usuarios. Esto, a nivel empresarial, es catastrófico, aún y cuando las empresas cuenten con recursos suficientes para mitigarlo.

Para las Pequeñas y Medianas Empresas (PYMES), la situación es un poco más crítica ya que no cuentan con el recurso económico ni el hardware necesario para una óptima mitigación de amenazas. Sin embargo, los datos que resguardan son igual de importantes que los de una gran empresa.

Es un hecho que los ciberdelincuentes no descansan en la búsqueda de vulnerabilidades y este ha sido uno de los mayores retos de las PYMES, que a menudo son el blanco de atacantes que las buscan por sus sistemas de seguridad cibernética poco robustos.

A nivel mundial, más del 90% de los negocios pertenecen a la categoría de PYMES, siendo uno de los sectores más expuestos a ciberataques. Según datos de la Encuesta Global de Seguridad de la Información 2023, los ciberataques aumentaron en un 60% en Centroamérica, donde Costa Rica es uno de los países más perjudicados con 1.6 millones de intentos de ciberataques contra las PYMES y 742 mil intentos de phishing. (Mellas, 2024).

Según el artículo de Mellas (Mellas, 2024), Yoser González, asociado de Consortium Legal Costa Rica, explica que “Entre las PYMES suele predominar el clásico pensamiento de que los ciberataques sólo les suceden a las grandes empresas, pero no es así. Y esa flexibilidad puede habilitar un tráfico masivo y descontrolado de datos personales. Hoy día en Costa Rica emprender conlleva costos importantes: para iniciar operaciones, se requieren varios permisos, licencias y registros. Por lo tanto, en la escala de prioridades de un emprendedor, la inversión en materia de ciberseguridad no suele encabezar la lista”.

“Es relevante destacar que las empresas más pequeñas a menudo enfrentan dificultades para adquirir la infraestructura necesaria y contar con personal capacitado para enfrentar la ciberdelincuencia. Según la encuesta Transformación Digital para PYMES realizada por Microsoft en Costa Rica, el 35% de las pequeñas y medianas empresas costarricenses han experimentado problemas de ciberseguridad. Además, estas empresas, al sufrir un ciberataque, tienen un riesgo significativamente mayor de desaparecer, según la Alianza Nacional de Ciberseguridad de los Estados Unidos, que informa que más del 60% de las PYMES no logran recuperarse después de un ataque.” (Casas, 2024)

1.3. Definición y descripción del problema

¿Qué tan vulnerables son las Pequeñas y Medianas empresas (PYMES) a los ciberataques y de qué forma es posible mitigar este riesgo que corren día a día?

En el mundo, diariamente se registran miles de ciberataques, de los cuales gran cantidad van dirigidos a las PYMES. Esto se debe, mayormente, a que las empresas pequeñas y medianas no tienen los recursos necesarios para implementar medidas que les ayuden a proteger sus sistemas de información, quedando así expuestos muchos datos sensibles.

Como consecuencia de esta limitación de recursos, las PYMES han llegado a ser el sector del mercado más vulnerable a ciberataques, dejando como resultado una corta vida comercial de muchos emprendimientos.

A pesar de que algunas PYMES recurren a medidas de seguridad de terceros, los altos costos pueden afectar la continuidad operativa de la empresa, ya que se dirigen recursos económicos a la seguridad de su información imposibilitando la continuidad del negocio.

Por lo anterior, es importante crear una solución que sea accesible para empresas con recursos limitados, que sea compatible con su infraestructura informática y que realmente brinde una solución a los problemas de ciberseguridad que hoy en día les atañen.

1.4. Justificación

Este proyecto busca ofrecer una solución realista, avanzada y accesible ante incidentes de seguridad informática, dirigida especialmente a empresas que cuentan con recursos limitados, evaluando y respondiendo en tiempo real a ataques dirigidos a infraestructuras virtuales. Por medio de herramientas de código abierto se estructura un modelo de respuesta autónoma, capaz de monitorear constantemente los procesos del sistema e iniciar una respuesta automática en situaciones de actividad inusual.

La utilización de herramientas Open Source permite que este proyecto tenga el potencial de ser adoptado por organizaciones pequeñas que requieran fortalecer sus sistemas de seguridad.

Con la implementación de este modelo se pretende brindar apoyo a organizaciones que destinan gran cantidad de sus recursos a las actividades propias del negocio, dificultando así la inversión en sistemas para protección de los datos.

1.5. Viabilidad

La viabilidad de este proyecto es importante para asegurar que la investigación se puede llevar a cabo exitosamente. A continuación, se presentan los diferentes aspectos de la viabilidad del proyecto desde los puntos de vista técnico, operativo y económico.

1.5.1. Punto de vista Técnico

De manera técnica, este proyecto es viable ya que se requieren conocimientos básicos en programación, detección de vulnerabilidades, estrategias de recuperación ante eventuales ciberataques y técnicas de creación de entornos virtuales. Como Ingeniero en Sistemas y futuro Máster en Ciberseguridad, el investigador ha adquirido diferentes conocimientos que le servirán como herramientas para la creación e implementación de este modelo.

Así mismo, se cuenta con el software necesario, como herramientas SIEM (Security Information and Event Management), software para virtualización, literatura académica y documentación técnica sobre el tema tratado. Estos recursos permiten diseñar e implementar un modelo en entornos de prueba sin comprometer sistemas reales ni la privacidad de las empresas.

1.5.2. Punto de vista Operativo

Para este proyecto se planea realizar una investigación sobre herramientas de código abierto que sean funcionales en la detección de actividad inusual en entornos virtuales y que brinden datos de eventos útiles para la activación de respuestas automáticas a dichos incidentes. Una vez identificadas las herramientas que más se ajustan a la propuesta, se realiza una guía para la creación de un modelo que analice información y responda de manera autónoma a incidentes de seguridad en dichos entornos. Se planea que, por medio de un servidor virtual, se monitoreen dispositivos finales evaluando así actividad que comprometa la confidencialidad, integridad o disponibilidad de los datos, así como la continuidad del negocio.

1.5.3. Punto de vista Económico

Desde el punto de vista económico, el proyecto es viable. El principal costo asociado son las horas de consultoría del investigador. Este costo se detalla en la Tabla 1. El investigador asume el “costo teórico” del proyecto, el cual ha sido planificado y considerado manejable dentro del presupuesto disponible.

Investigador	Horas semanales	Total semanas (4 meses)	Total horas (4 meses)	Costo por hora	Costo teórico total
David Solano Mora	21	16	336	$10,86	$ 3.648,96

Tabla 1. Costos de la investigación.

Es importante mencionar que el proyecto propone una solución utilizando software de código abierto, el cual no tiene costos económicos.

1.6. Objetivos

Para la selección de los objetivos, tanto el objetivo general como los objetivos específicos se utiliza la taxonomía de Bloom 1956, ya que proporciona una estructura jerárquica clara que organiza y define objetivos de manera consistente y ordenada, facilitando la comprensión y evaluación del trabajo. Además, su uso estándar asegura que los objetivos sean comprendidos uniformemente por evaluadores y lectores.

1.6.1. Objetivo General

Proponer un modelo de recuperación autónomo para entornos virtuales ante incidentes de seguridad por medio de la utilización de software de código abierto, con el fin de brindar una solución viable para organizaciones con recursos limitados.

1.6.2. Objetivos específicos

- Identificar los conceptos fundamentales relacionados con incidentes de seguridad en entornos virtualizados y las principales herramientas de código abierto para gestionarlos mediante una revisión teórica y documental de fuentes especializadas y casos reales documentados, para establecer una base conceptual sólida que sirva de sustento para el diseño del modelo de recuperación autónomo.
- Explicar el funcionamiento de herramientas como Wazuh, VirtualBox y otras tecnologías clave en la detección, respuesta y recuperación de incidentes a través del estudio técnico y práctico de sus componentes, configuración y documentación oficial para comprender su aplicabilidad dentro del sistema propuesto y garantizar un uso eficiente de sus capacidades.

- Desarrollar un entorno de laboratorio que simule incidentes de seguridad y permita aplicar mecanismos automatizados de recuperación configurando máquinas virtuales y utilizando software de código abierto para orquestar pruebas controladas para demostrar la viabilidad técnica de un sistema de respuesta y recuperación autónomo en un entorno virtualizado.
- Analizar la efectividad del sistema de recuperación autónomo implementado frente a distintos tipos de incidentes de seguridad a través de la ejecución de pruebas prácticas, recolección de métricas y comparación de resultados para evaluar el desempeño del sistema y validar su capacidad de respuesta y autonomía en escenarios críticos.

1.7. Alcance y Limitaciones

En este proyecto de investigación se propone crear un modelo de recuperación autónomo para entornos virtuales, ante incidentes de seguridad, por medio de la utilización de software de código abierto, con el fin de brindar una solución viable para organizaciones con recursos limitados. A través de una serie de entregables y restricciones se busca delimitar claramente el alcance del estudio y reconocer las limitaciones inherentes al mismo.

1.7.1. Alcances

En este proyecto se contempla el diseño y la implementación de un modelo funcional de recuperación autónoma, ante incidentes de seguridad, en entornos virtualizados, utilizando herramientas como Wazuh, scripting en Python y VirtualBox como entorno de pruebas. Se desarrolla un laboratorio virtual replicable que permita simular incidentes y ejecutar procesos automáticos de detección, respuesta y restauración de servicios críticos, lo cual puede ser documentado y adaptado en escenarios reales o académicos. Además, se plantea la posibilidad de integrar, en fases futuras, un componente de inteligencia artificial para detectar anomalías en procesos y comportamientos de usuarios, Esto puede ayudar a incrementar la capacidad proactiva del sistema. Esta solución está pensada para ser versátil y aplicable en infraestructuras virtuales, orientada a organizaciones con diferentes niveles de capacidad tecnológica.

1.7.2. Limitaciones

Este proyecto presenta algunas limitaciones. Su validación se realiza en un entorno controlado, por lo que su comportamiento en ambientes de producción de gran escala podría requerir adaptaciones. La automatización está enfocada en servicios específicos definidos dentro del laboratorio, sin cubrir toda la diversidad de aplicaciones posibles. La detección de amenazas depende de reglas predefinidas y no de sistemas inteligentes en tiempo real, ya que la integración de técnicas de Machine Learning se proyecta como un desarrollo posterior. Asimismo, no se abordan consideraciones legales o regulatorias asociadas a la automatización de respuestas, y la solución podría requerir personal capacitado para su implementación.

1.8. Marco de Referencia Organizacional y Socioeconómico (sobre pymes)

En este apartado se proporciona una visión general del proyecto de investigación y el contexto en el que se desarrolla. Esto permite una mejor comprensión de las PYMES y de los desafíos de ciberseguridad a los que se enfrentan día a día y el impacto que estos desafíos conllevan.

1.8.1. Historia

“Las pequeñas y medianas empresas (PYME) surgieron como una respuesta natural a las necesidades económicas y sociales de las comunidades locales a lo largo de la historia. Las PYMEs tienen su antecedente más representativo en la Europa posterior a la Segunda Guerra Mundial, cuando las empresas de ese Continente tuvieron que recuperarse de los estragos económicos de una manera rápida.” (UIIM, 2024).

Según la UIIM, las PYMEs son reconocidas por su papel crucial en las economías modernas debido a que son grandes generadoras de empleo, especialmente a nivel local. Muchas innovaciones importantes provienen de PYMEs y además contribuyen a la diversificación de la economía, reduciendo la dependencia de grandes corporaciones y fomentando la competencia.

“Las PYMEs han evolucionado desde pequeñas unidades de producción y comercio en economías preindustriales hasta convertirse en un pilar esencial de las

economías modernas, apoyadas por políticas gubernamentales, avances tecnológicos y un entorno de negocios globalizado.” (UIIM, 2024)

Según Brenes (Brenes, 2021), el impulso institucional a las PYMES en Costa Rica inició en la década de 1950 cuando el Estado comenzó a estimular su creación y a impulsar la economía nacional con la creación de la Ley 2.426 Protección y Desarrollo Industrial de 1959. Esta Ley estableció medidas como promoción bancaria, protección arancelaria y asesoría técnica para apoyar a estas empresas.

Según CAF (CAF, 2023), “la mayor parte del tejido empresarial del país está compuesto por micro, pequeñas y medianas empresas. En los últimos 5 años estas unidades han representado 97.4 % del total de empresas. El segmento PYME enfrenta diferentes situaciones que dificultan el adecuado desarrollo, por ejemplo, no todas pueden acceder a herramientas tecnológicas para comunicarse con sus clientes”. De igual manera, para muchas pequeñas y medianas empresas, es muy difícil acceder a herramientas de ciberseguridad, lo cual ha venido siendo el motivo del incremento en ataques a este sector.

“Según datos de la Encuesta Global de Seguridad de la Información 2023, los ciberataques aumentaron en 60 % en Centroamérica, y Costa Rica es uno de los países más perjudicados: 1.6 millones de intentos de ciberataque contra las pymes y 742 mil intentos de phishing.” (Mellas, 2024)

1.8.2. Tipo de Negocio y Mercado Meta

Hoy en día, las PYMEs abarcan gran cantidad de tipos de negocios, según la Revista Summa (Revista Summa, 2023), la empresa de contabilidad y facturación Alegra.com realizó un análisis con respecto a los sectores más elegidos por los costarricenses a la hora de emprender y determinó que la categoría de Comercio Minorista es la predilecta. También se destaca que otros sectores son el de Servicios y Consultoría, Agricultura, Ganadería, Silvicultura y Pesca.

1.9. Estado de la cuestión

Hoy en día, uno de los mayores esfuerzos a nivel internacional es la lucha contra la cibercriminalidad. Existen muchas herramientas para combatir los ataques cibernéticos, así como especialistas en ciberseguridad. Se desea compilar documentos técnicos y de información sobre herramientas de monitoreo y detección de amenazas e incidentes, ejecución de tareas automáticas y restauración de entornos virtuales que sean relevantes para el desarrollo de esta investigación y se procede a su identificación, selección y análisis.

1.9.1. Planificación de la revisión

En esta sección se formula una pregunta clara y bien definida del tema de la investigación. Se realiza la búsqueda de documentación existente del tema con la intención de conocer los avances investigativos en el tema, así como identificar posibles áreas de mejora o dónde se pueda ampliar la investigación y verificar que no se estén duplicando estudios realizados anteriormente.

1.9.1.1. Formulación de la pregunta

La formulación de la pregunta resulta en la delimitación de búsqueda de información e investigación. La intención de esta es reafirmar la contribución de este trabajo al campo de investigación y las relaciones entre ideas, teoría y aplicación práctica.

1.9.1.1.1. Foco de la pregunta

Para esta investigación, se requiere centralizar la búsqueda de documentos técnicos que especifiquen el uso de herramientas de código abierto y que sean funcionales para la implementación de un modelo de respuesta autónoma para entornos virtuales ante incidentes de seguridad.

1.9.1.1.2. Amplitud y calidad de la pregunta

En esta sección se establece la pregunta de investigación que se desea responder de forma clara y concisa, basado en un problema a resolver. Se listan los términos clave relevantes para la búsqueda de información y para proporcionar contexto al proceso de revisión de literatura, se consideran los siguientes componentes.

a. Problema

La necesidad de invertir en actividades vitales para la continuidad del negocio ha hecho que las Pequeñas y Medianas Empresas recorten recursos destinados a la seguridad de la información haciendo que este gran sector comercial se vuelva cada vez más y más vulnerable a ataques que buscan robar su información y la información de sus clientes, afectando así la confianza y la reputación de estas empresas.

b. Pregunta

Con la anterior definición del problema, se formula la siguiente pregunta de investigación:

¿Qué trabajos de investigación se han realizado anteriormente en el área de defensa y recuperación en entornos virtuales ante ataques cibernéticos?

c. Palabras clave y sinónimos

En la Tabla 2 se presentan las palabras clave en español e inglés utilizadas en la búsqueda de documentación para la revisión literaria.

Palabra en español	Palabra en ingles
Incidentes de ciberseguridad	Cybersecurity incidents
PYME	SME
Centro de Operaciones de Seguridad	Security Operation Center
Recuperación autónoma	Autonomous recovery
Restauración de sistemas	System restoration
Respuesta ante incidentes	Incident response
Sistemas autorrecuperables	Self-healing systems
Herramientas de código abierto	Open Source Tools

Tabla 2. Palabras clave.

d. Intervención

Se analizan los resultados sobre cómo se implementan e intervienen las herramientas de código abierto en la lucha contra la ciberdelincuencia y la

recuperación de sistemas virtualizados. Se extraen los artículos y documentos más relevantes para la investigación.

e. Control

No existe una base de conocimiento previa en el tema de la investigación más allá de los conceptos básicos. Se inicia con una búsqueda de cero a partir de las palabras clave definidas.

f. Efectos

Se espera recopilar suficiente documentación para comprender como funcionan los sistemas autónomos de recuperación ante incidentes de seguridad y la correcta implementación de estos utilizando herramientas de código abierto.

g. Medición de resultados

Para la documentación encontrada se realiza una revisión de la calidad de esta en sitios web destinados a tal fin.

h. Población

El estudio se centra en herramientas de código abierto y herramientas de automatización que permitan la implementación de un modelo funcional de recuperación ante ataques a la seguridad de los datos.

i. Aplicación

Esta investigación pretende beneficiar a las Pequeñas y Medianas Empresas que por sus bajos recursos no tengan la posibilidad de invertir en sistemas de protección proporcionando un modelo que automatice la respuesta a incidentes.

j. Diseño experimental

Los artículos son seleccionados con base en su relevancia para esta investigación, asegurando que contengan información relevante para el tema que se quiere desarrollar.

1.9.1.1.3. Selección de fuentes

Se especifican en esta sección las fuentes para la identificación de estudios primarios que se utilizan para la investigación.

1.9.1.1.3.1. Definición del criterio de selección de fuentes

Para la selección de fuentes se han tomado en cuenta diferentes aspectos como el respaldo teórico con que cuenta la fuente. También se toman en cuenta fuentes que tengan relevancia para la investigación y se observan índices y métricas publicadas por la página web Scimago Journal and Country Rank.

1.9.1.1.3.2. Idioma de la documentación

Las fuentes seleccionadas para la revisión de literatura están en inglés y español, para incrementar el rango de posibles resultados priorizando aquellas que proporcionen información de alta calidad sobre sistemas de respuesta automática ante incidentes, herramientas de código abierto y técnicas de implementación.

1.9.1.1.3.3. Identificación de las fuentes

Es este apartado se describe la selección de fuentes que respaldan la investigación, se describen los métodos de búsqueda y se brinda la lista de las fuentes.

a. Método de selección de fuentes

La principal fuente de búsqueda de documentos se realiza con Google Académico y bases de datos científicas reconocidas, además de páginas web de proveedores de herramientas de código abierto. Se da prioridad a documentos de acceso público o para estudiantes.

b. Cadena de búsqueda

Para la cadena de búsqueda se utilizaron diferentes criterios de búsqueda combinando términos relacionados con la recuperación autónoma de sistemas virtualizados, detección de ataques y PYMEs en diferentes bases de datos como Google Académico, IEEE Explore y ScienceDirect. Los criterios de búsqueda fueron:

- **("Document Title":Automated) AND ("All Metadata":Open Source)** y **("Document Title":Resilience) AND ("All Metadata":Open Source)** para la base de datos IEEE Explore.
- **(intitle:"Wazuh" + "Cyber Security")** y **(intitle:soar tools)** para Google Académico
- **Wazuh** y **Wazuh + "Autonomous"** para ScienceDirect

c. Lista de fuentes

A continuación, se listan las fuentes consideradas para alimentar la investigación:

1. Gestión de eventos e información de seguridad (SIEM): análisis, tendencias y uso en infraestructuras críticas.
2. Desarrollo del sistema de gestión automatizada de incidencias basado en software libre.
3. Wazuh SIEM for Cyber Security and Threat Mitigation in Apparel Industries
4. Automatic incident response solutions: a review of proposed solutions' input and output
5. Automation in the cybersecurity incident Handling process.
6. Incident Response and Recovery
7. Cost-Effective Resilience: A Comprehensive Survey and Tutorial on Assessing Open-Source Cybersecurity Tools for Multi-Tiered Defense.
8. Testing SOAR tools in use
9. Modeling Wazuh rules with Weighted Timed Automata
10. Severity-based triage of cybersecurity incidents using kill chain attack graphs

d. Selección de fuentes

Las siguientes fuentes son las que cumplen con el método de selección y el criterio de selección expuestos anteriormente:

1. Cost-Effective Resilience: A Comprehensive Survey and Tutorial on Assessing Open-Source Cybersecurity Tools for Multi-Tiered Defense.

2. Development of the System for Automated Incident Management Based on Open-Source Software.
3. Wazuh SIEM for Cyber Security and Threat Mitigation in Apparel Industries.
4. Testing SOAR tools in use
5. Modeling Wazuh rules with Weighted Timed Automata
6. Severity-based triage of cybersecurity incidents using kill chain attack graphs

1.9.1.1.3.4. Revisión de referencias

No se cuenta con un experto en sistemas de recuperación autónoma en entornos virtualizados que pueda revisar las referencias seleccionadas. Sin embargo, los artículos utilizados en la investigación son evaluados con base en métricas académicas y criterios de calidad establecidos previamente.

1.9.1.1.4. Selección de estudios

En esta sección se describen los criterios para la inclusión y la exclusión de las investigaciones recuperadas y se define cuáles de ellos forman parte del análisis final.

1.9.1.1.4.1. Definición del criterio de inclusión y exclusión de estudios

Las investigaciones que fueron seleccionadas responden a la pregunta de investigación: *¿Qué trabajos de investigación se han realizado anteriormente en área de defensa y recuperación en entornos virtuales ante ataques cibernéticos?*

Por otro lado, un estudio se incluye en esta investigación si cumple con uno o varios de los siguientes criterios:

a. Contiene información sobre sistemas de respuesta a incidentes, SIEM (Security Information and Event Management) y SOAR (Security Orchestration, Automation, and Response) con fechas entre 2021 y 2025.

b. Muestre resultados sombre detección de amenazas y tiempos de respuesta ante incidentes de seguridad.
c. Evalúen diferentes formas de orquestar sistemas de detección e incluyan el uso de herramientas Open Source así como la viabilidad de uso de estas.
d. Identifique brechas y desafíos en la seguridad de la información y el impacto que tienen en sectores comerciales como las PYMEs.

1.9.1.1.4.2. Definición de tipos de estudios

Para la presente investigación, se consideran diferentes enfoques metodológicos, dentro de los cuales se incluyen:

Estudios cuantitativos: Se realizan pruebas de rendimiento de diferentes herramientas bajo un tráfico controlado, se miden tasas de detección y se evalúa el uso de CPU y escalabilidad. (Hadi, 2024). Además (Islam & Rafique, 2024) realizan una implementación práctica con métricas de eficacia al desplegar Wazuh virtualizados y generando informes automatizados de vulnerabilidades.

Estudios cualitativos: Se realiza una revisión teórica de modelos de ciberseguridad por parte de (Hadi, 2024) por medio de un análisis de características propias de herramientas de código abierto. Además (Gibadullin & Nikonorov, 2021) realizan una descripción de arquitectura y procesos ejecutando un análisis comparativo cualitativo de soluciones SOAR destacando integraciones, escalabilidad y limitaciones.

Estudios mixtos: (Islam & Rafique, 2024) Definen métricas de vulnerabilidades y rendimiento de Wazuh y brindan una descripción de la usabilidad del Dashboard y como se adapta a diferentes normativas. Por otra parte (Gibadullin & Nikonorov, 2021) evalúan tiempos de respuesta y explican la arquitectura y el impacto en la gestión.

1.9.1.1.4.3. Procedimiento para la selección de estudios

Para el proceso de búsqueda se realizó el proceso que se describe a continuación:

a. Se utiliza la opción de búsqueda general o avanzada disponible en fuentes como Google Académico, IEEE Explore y las demás fuentes disponibles. Se introducen diferentes cadenas de búsqueda y se agregan filtros para reducir los resultados.
b. Según los resultados, se seleccionan aquellas investigaciones en las que su título coincidan con los objetivos de la investigación.
c. Se evalúa la fuente del articulo para validar su veracidad.
d. Se realiza la lectura y evaluación del Abstract y en caso de que este sea congruente con los criterios de selección, se procede a con la sección de conclusiones.
e. Se aplican criterios de exclusión y se seleccionan los resultados considerados relevantes para la investigación.

1.9.1.2. Ejecución de la revisión

En esta sección se muestra el procedimiento llevado a cabo para la selección de las diferentes fuentes

1.9.1.2.1. Selección de la ejecución

1. Selección de estudios iniciales: Se aplican cadenas de búsqueda como "Document Title":Automated) AND ("All Metadata":Open Source) en páginas como IEEE Explore, Google Académico y ACM Digital Library. Se aplican filtro de búsqueda para que se muestren investigaciones de los últimos 5 años, la Tabla 3 muestra los resultados.

#	Titulo	Autor(es)	Año	URL
1	Security Information and Event Management (SIEM): Analysis, Trends, and Use in Critical Infrastructures	Gustavo Gonzalez Granadillo	2021	https://www.mdpi.com/1424-8220/21/14/4759

2	Development of the System for Automated Incident Management Based on Open-Source Software	R. F. Gibadullin	2021	https://ieeexplore.ieee.org/abstract/document/9537385/authors#authors
3	Wazuh SIEM for Cyber Security and Threat Mitigation in Apparel Industries	Md Rafiqul Islam and Raisa Rafique	2024	https://deerhillpublishing.com/index.php/ijemm/article/view/279
4	Automatic incident response solutions: a review of proposed solutions' input and output	Henrik Karlzen, Teodor Sommestad	2023	https://dl.acm.org/doi/abs/10.1145/3600160.3605066
5	Automation in the Cybersecurity Incident Handling Process	Davide Ioan Manco	2022	https://webthesis.biblio.polito.it/24503/
6	Incident Response and Recovery	Jason Edwards	2024	https://ieeexplore.ieee.org/document/10494638
7	Cost-Effective Resilience: A Comprehensive Survey and Tutorial on Assessing Open-Source Cybersecurity Tools for Multi-Tiered Defense	Hassan Jalil Hadi, Naveed Ahmad, Kamran Aziz, Yue Cao, Mohammed Ali Alshara"	2024	https://ieeexplore.ieee.org/abstract/document/10772461/authors#authors
8	Testing SOAR tools in use	Robert A. Bridges, Ashley E. Rice, Sean Oesch, JeffreyA. Nichols, Cory Watson, Kevin Spakes, Savannah Norem, Mike H	2023	https://www.sciencedirect.com/science/article/abs/pii/S0167404823001116

		uettel, Brian Jewell, Brian Weber, Connor Gannon, Olivia Bizovi, Samuel C. Hollifield, Samantha Erwin		
9	Modeling Wazuh rules with Weighted Timed Automata	Anass Haydar, Mathias Ramparison	2024	https://www.sciencedirect.com/science/article/pii/S1877050924033209
10	Severity-based triage of cybersecurity incidents using kill chain attack graphs	Lukáš Sadlek, Muhammad Mudassar Yamin, Pavel Čeleda, Basel Katt	2025	https://www.sciencedirect.com/science/article/abs/pii/S2214212624002588

Tabla 3. Muestra de resultados de búsqueda

2. Evaluación de la calidad de los resultados: En esta sección se muestra la fiabilidad de las fuentes de donde se toman las investigaciones que sustentan este proyecto:

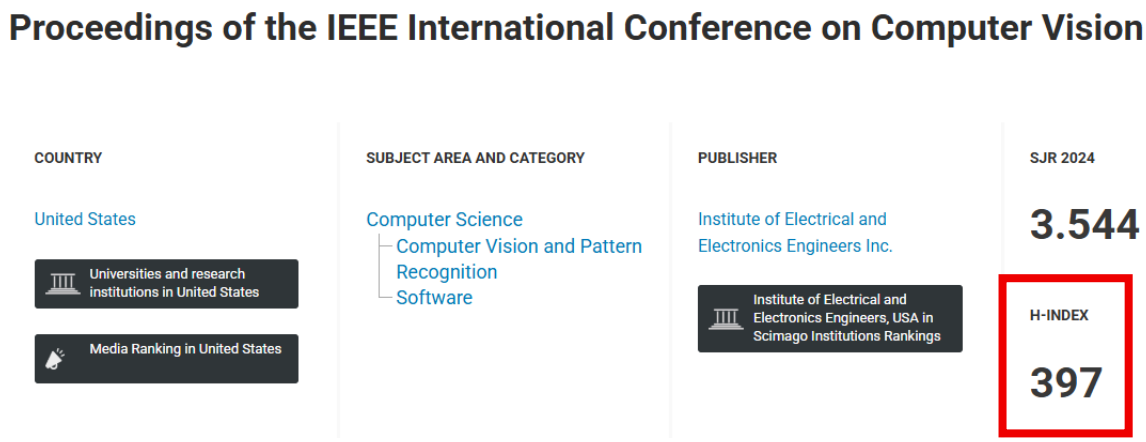

Ilustración 1. Validación de calidad de IEEE

Ilustración 2Fuente: Scimago

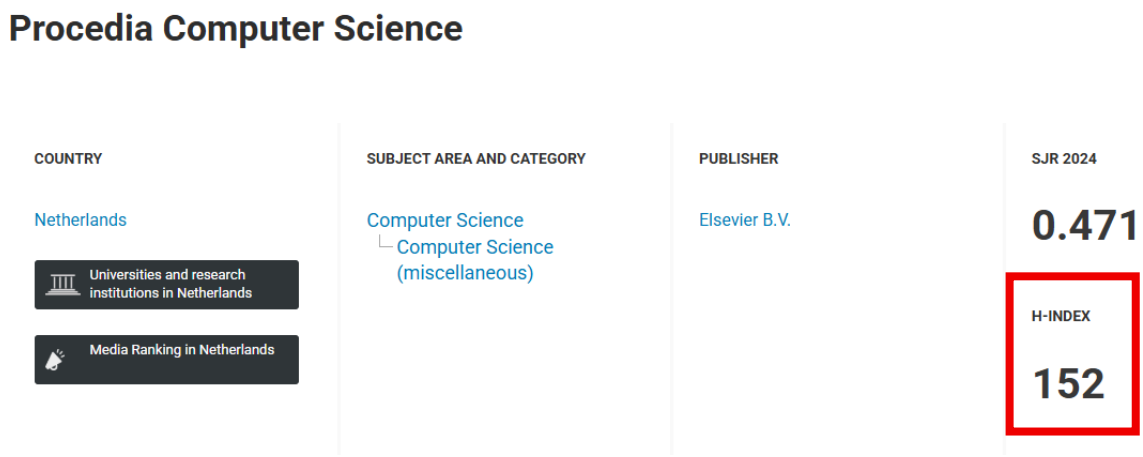

Ilustración 3. Validación de calidad de Procedia Computer Science

Fuente Scimago

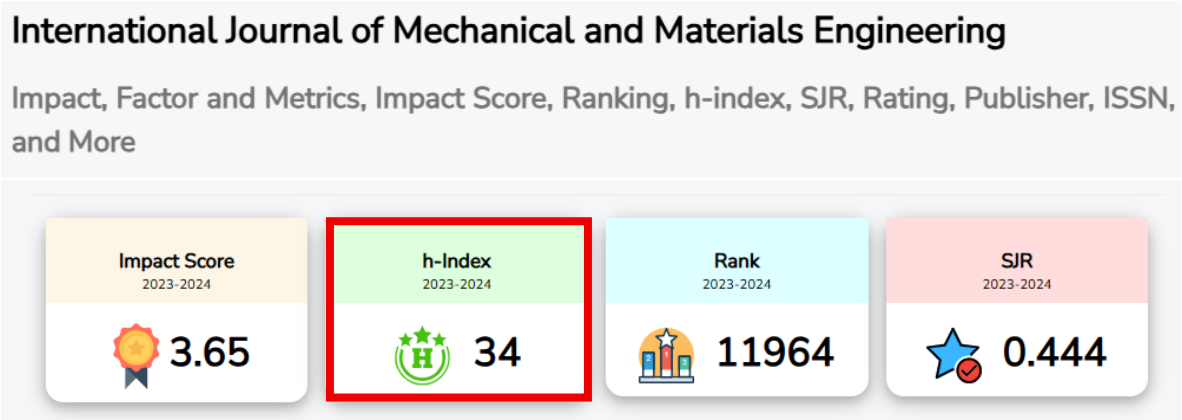

Ilustración 4. Validación de calidad International Journal of Mechanical and Materials Engineering

Fuente: Resurchify

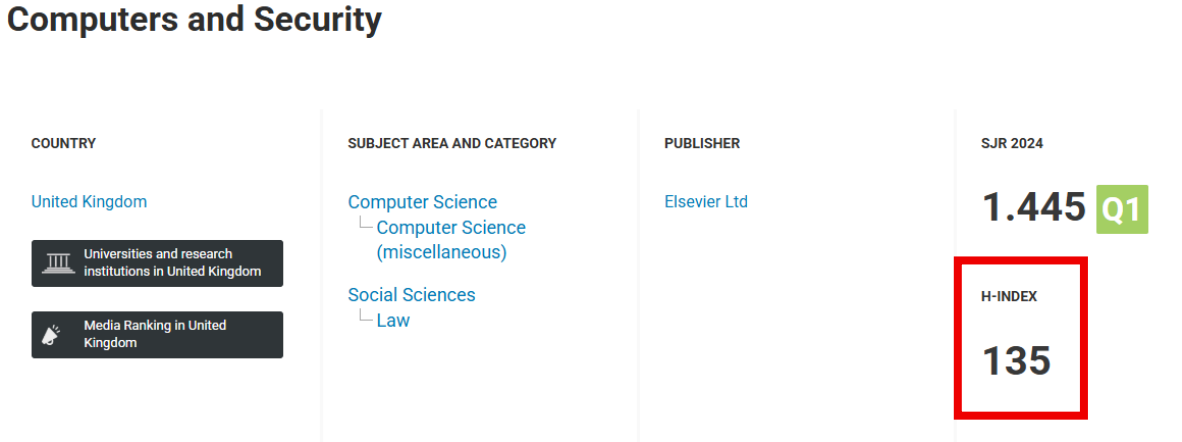

Ilustración 5. Validación de calidad Computers and Security

Fuente: Scimago

Ilustración 6. Validación de calidad de Journal of Information Security and Applications

Fuente: Scimago

La selección de estudios primarios se realiza tras llevar a cabo una revisión de los Abstract y contenido incluido en cada artículo. Para la revisión de estos artículos, los mismos fueron ordenados con base en la relevancia de los artículos.

1.9.1.2.2. Extracción de la información

Para la extracción de la información que es relevante para la investigación, se consideran los siguientes elementos:

- Resiliencia automatizada en sistemas virtualizados
- Evaluación de herramientas SIEMs y métodos de implementación
- Detección y respuesta autónoma ante incidentes de seguridad cibernética.
- Estudios de diferentes herramientas de código abierto para protección de sistemas
- Evaluación de tiempos máximos aceptables de respuesta ante ciberataques.

1.9.1.2.2.1. Formularios de extracción de datos

Se muestra en la Tabla 4, el formulario utilizado para extraer la información de la literatura seleccionada.

Repositorio	
Titulo	
Fuente	
Autores	
Referencia	
Resumen	
Aspectos a destacar	

Tabla 4. Formulario para la extracción de información

1.9.1.2.2.2. Ejecución de la extracción

Repositorio	IEEE Explore
Titulo	Development of the System for Automated Incident Management Based on Open-Source Software
Autores	R. F. Gibadullin
Referencia	Gibadullin, R., & Nikonorov, V. (2021). Development of the System for Automated Incident Management Based on Open-Source Software. *International Russian Automation Conference (RusAutoCon)*, (págs. 521-525). Sochi, Russian.
Resumen	La investigación muestra el desarrollo de un sistema automatizado de gestión de incidentes de seguridad basado en software libre aplicando diferentes tecnologías. Se enfoca reducir el tiempo de respuesta ante incidentes de seguridad y automatizar procesos minimizando la intervención humana.
Aspectos a destacar	• Desarrollo de una solución SOAR de código abierto • Utilización de scripting para la automatización

Tabla 5. Extracción de información del artículo Development or the System for Automated Incident Management Based on Open-Source Software

Repositorio	IEEE Explore
Titulo	Cost-Effective Resilience: A Comprehensive Survey and Tutorial on Assessing Open-Source Cybersecurity Tools for Multi-Tiered Defense
Autores	"Hassan Jalil Hadi, Naveed Ahmad, Kamran Aziz, Yue Cao, Mohammed Ali Alshara"
Referencia	Hadi, H. J. (2024). Cost-Effective Resilience: A Comprehensive Survey and Tutorial on Assessing Open-Source Cybersecurity Tools for Multi-Tiered Defense. *IEEE Explore*, 24.
Resumen	Se trata de una encuesta y un tutorial sobre herramientas de código abierto con el propósito de ayudar a las organizaciones de recursos limitados a construir una resiliencia cibernética de manera que sea rentable para ellos.
Aspectos a destacar	• Categorización de herramientas por nivel de defensa y función (prevención, detección, respuesta, recuperación y post-mortem). • Destaca herramientas como Pfsense, Wazuh, TheHive, Clonezilla y Autopsy

Tabla 6. Extracción de información del artículo Cost-Effective Resilience: A Comprehensive Survey and Tutorial on Assessing Open-Source Cybersecurity Tools for Multi-Tiered Defense

Repositorio	Science Direct
Titulo	Testing SOAR tools in use
Autores	Robert A. Bridges, Ashley E. Rice, Sean Oesch, Jeffrey A. Nichols, Cory Watson, Kevin Spakes, Savannah Norem, Mike Huettel, Brian Jewell,

	Brian Weber, Connor Gannon, Olivia Bizovi, Samuel C. Hollifield, Samantha Erwin
Referencia	Robert A. Bridges, A. E. (2023). Testing SOAR tools in use. *Computers & Security*.
Resumen	Describe el proceso de evaluación de diferentes herramientas SOAR y analiza que tan aplicables son y que tal el rendimiento de dichas herramientas en el contexto de la ciberseguridad.
Aspectos a destacar	• Se implementan y se prueban diferentes herramientas SOAR en escenarios reales.

Tabla 7. Extracción de información del artículo Testing SOAR tools in use

Repositorio	Science Direct
Titulo	Modeling Wazuh rules with Weighted Timed Automata
Autores	Anass Haydar, Mathias Ramparison
Referencia	Haydar, A., & Ramparison, M. (2024). Modeling Wazuh rules with Weighted Timed Automata. *Procedia Computer Science*, 75-82.
Resumen	La investigación propone un marco para modelar las reglas de detección de amenazas, propiamente del sistema Wazuh. Se escriben reglas de Wazuh en XML que son importantes para la detección de eventos inusuales o violación de políticas de la herramienta
Aspectos a destacar	• Se presentan formas de modelar reglas simples y compuestas • Se realizan distintos análisis en la funcionalidad de la herramienta

Tabla 8. Extracción de información del artículo Modeling Wazuh rules with Weighted Timed Automata

Repositorio	Science Direct
Titulo	Severity-based triage of cybersecurity incidents using kill chain attack graphs
Autores	Lukáš Sadlek, Muhammad Mudassar Yamin, Pavel Čeleda, Basel Katt
Referencia	Sadlek, L., Yamin, M. M., Čeleda, P., & Katt, B. (2025). Severity-based triage of cybersecurity incidents using kill chain attack graphs. *Journal of Information Security and Applications*.
Resumen	La investigación manifiesta la necesidad de clasificar los tipos de alerta en herramientas SOAR según su severidad y para esto se genera un gráfico de ataque tipo “kill chain” a partir de los datos de la red y de los hosts. Se generan secuencias de alertas detectadas y les asigna niveles de severidad basándose en las fases avanzadas del “kill chain”
Aspectos a destacar	Aborda problemas como la “fatiga de alertas” y la alta carga de trabajo para los SOCs Utiliza detección de ataques multi-capa.

Tabla 9. Extracción de información del artículo Severity-based triage of cybersecurity incidents using kill chain attack graphs

Repositorio	International Journal of Engineering Materials and Manufacture
Titulo	Wazuh SIEM for Cyber Security and Threat Mitigation in Apparel Industries
Autores	Md Rafiqul Islam and Raisa Rafique
Referencia	Islam, M. R., & Rafique, R. (2024). Wazuh SIEM for Cyber Security and Threat Mitigation in Apparel Industries.

	International Journal of Engineering Materials and Manufacture (IJEMM), 136-144.
Resumen	En este proyecto, se muestra una investigación sobre la implementación de Wazuh como forma de fortalecer la ciberseguridad en las industrias de recursos limitados ya que son estas las industrias más vulnerables a ataques cibernéticos. En la investigación se muestra como Wazuh permite detectar, analizar y responder a incidentes de seguridad
Aspectos a destacar	• Se utiliza Wazuh como herramienta central

Tabla 10. Extracción de información del artículo Wazuh SIEM for Cyber Security and Threat Mitigation in Apparel Industries

1.9.2. Estado de la cuestión

Como parte del proceso de selección de resultados, como se muestra en la tabla 12, se analizaron 10 estudios, de los mismos 6 fueron identificados como relevantes, basados en su contenido, número de referencias, año de publicación y calidad.

Fuente	Estudios	Relevantes
IEEE Explore	3	2
Science Direct	3	3
Sensors Journal	1	0
Politécnico di Torino	1	0
International Journal of Engineering Materials and Manufacture	1	1
Association for Computing Machinery, Nueva York, NY, EE.UU.	1	0
Total	10	6

Tabla 11. Análisis de resultados

2. Capítulo 2. Marco Conceptual

Se crea la siguiente nube de palabras con la intención de extraer los términos más relevantes que se mencionan en las diferentes investigaciones incluidas en el estado de la cuestión. Estos son conceptos clave extraídos de los resúmenes de dichas investigaciones.

Con el objetivo de proporcionar un mejor contexto sobre el tema, los conceptos se presentan en un orden jerárquico, desde lo más general hasta lo más específico (Ver Figura 7). Esta organización facilita la comprensión de los elementos esenciales relacionados con la recuperación autónoma ante incidentes de seguridad y la orquestación de un sistema resiliente.

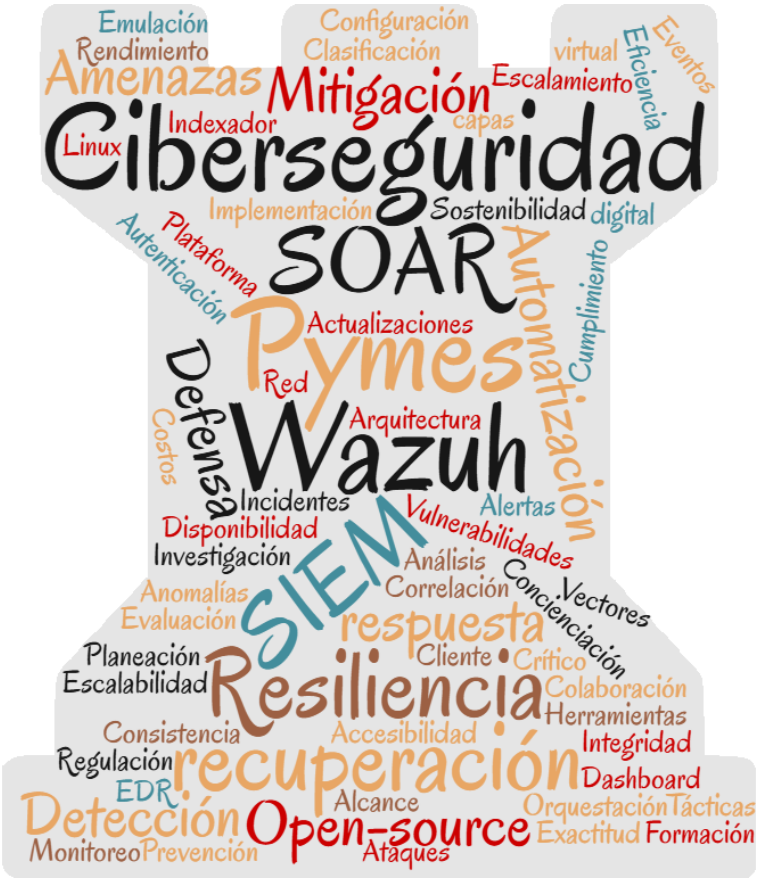

Ilustración 7. Nube de palabras

Fuente: Elaboración propia utilizando el sitio https://classic.wordclouds.com/

2.1. Conceptos

Considerando las diferentes fases del modelo que se quiere implementar, las diferentes herramientas y los conceptos a utilizar, es necesario describir una serie de aspectos y características que forman parte de esta implementación y que conforman la estructura de dicho modelo.

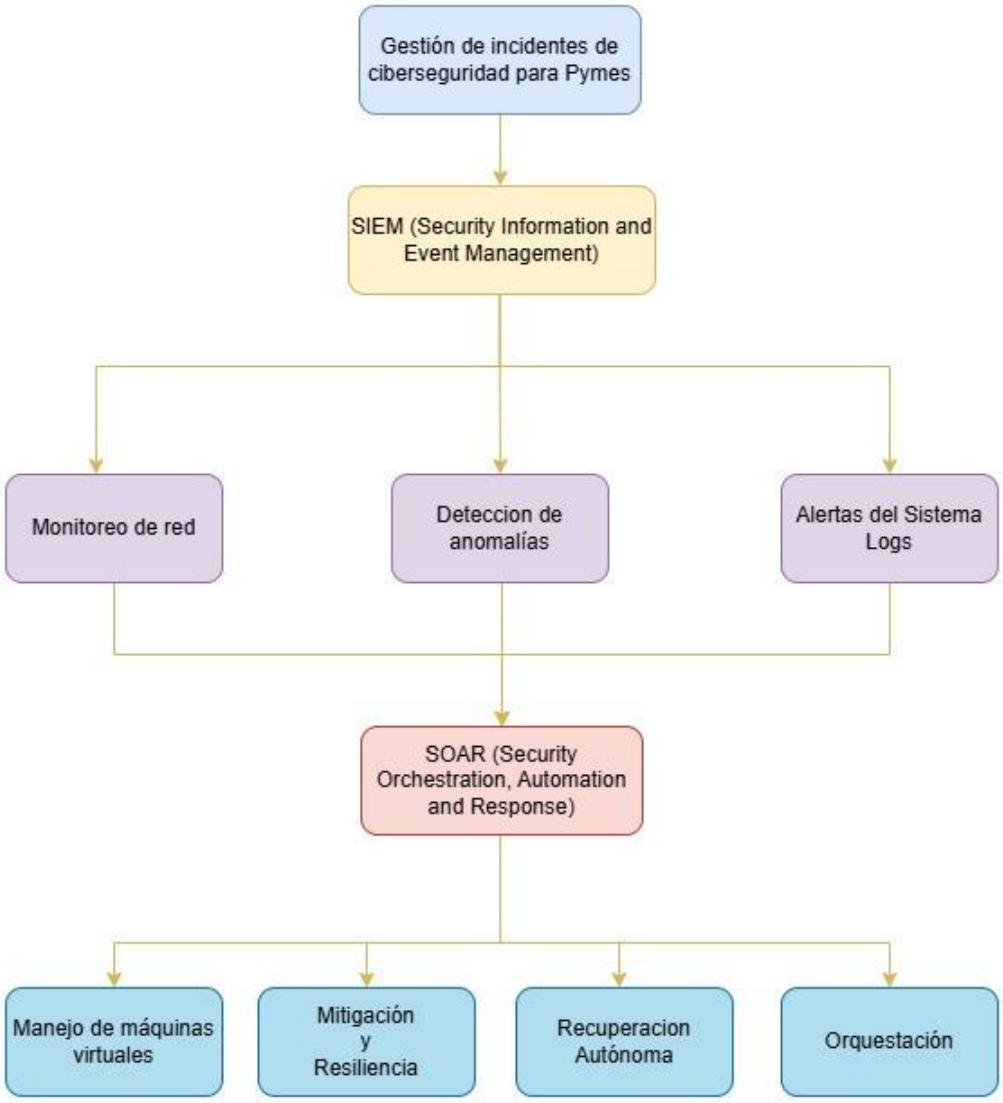

Ilustración 8. Diagrama sobre las fases del modelo

Fuente: Elaboración propia

2.1.1. PYMEs (Pequeñas y Medianas Empresas)

(Asamblea Legislativa, 2002) La Asamblea Legislativa indica que "Las pymes, se entiende por pequeñas y medianas empresas (pymes) toda unidad productiva de carácter permanente que disponga de los recursos humanos los maneje y opere, bajo las figuras de persona física o de persona jurídica, en actividades industriales, comerciales, de servicios o agropecuarias que desarrollen actividades de agricultura orgánica." (Asamblea Legislativa, 2002).

Además, en la Ley N° 8262 se detalla que aparte de la definición general, se establecen criterios más específicos como el número de empleados, los activos y las ventas. Estos criterios se establecen mediante reglamento por el Consejo Asesor Mixto de la PYME.

2.1.2. Gestión de incidentes de ciberseguridad

Según el U.S. Department of Commerce, "la gestión de riesgos es el conjunto de estrategias, políticas y procesos que están hechos para identificar, evaluar y controlar los riesgos asociados a amenazas de seguridad en los sistemas e integran la preparación la detección, la respuesta y la recuperación frente a incidentes en las operaciones de una organización." (Nelson, Rekhi, Souppaya, & Scarfone, 2025)

Para la Unidad de riesgos y Seguridad de la Universidad de Costa Rica, "La gestión de incidentes de seguridad tiene como objetivo minimizar el impacto de forma rápida ante cualquier amenaza que vulnere la seguridad de la organización" (Unidad de riesgos y Seguridad, 2022)

2.1.3. SIEM (Security Information and Event Manager)

(Microsoft, 2025) a continuación "Un componente esencial de la ciberseguridad es una solución de gestión de eventos e información de seguridad (SIEM). Estos tipos de soluciones recopilan, agregan y analizan grandes volúmenes de datos de aplicaciones, dispositivos, servidores y usuarios en toda la organización en tiempo real. Al consolidar esta vasta cantidad de datos en una única plataforma unificada, las soluciones SIEM proporcionan una visión integral de la postura de seguridad de una organización, empoderando los centros de operaciones de seguridad (SOC)

para detectar, investigar y responder a incidentes de seguridad de manera rápida y efectiva. Las soluciones SIEM ayudan a las organizaciones de todos los tamaños a:

- Obtener visibilidad sobre su posición de seguridad al centralizar y analizar datos de orígenes dispares.
- Detectar e identificar posibles brechas de seguridad y amenazas en tiempo real, lo que minimiza el riesgo de los ciberataques.
- Investigar y clasificar los incidentes de seguridad de manera eficiente, lo que permite reducir el tiempo y los recursos necesarios para la resolución.
- Cumplir los estándares y marcos de seguridad específicos de la industria y las regulaciones.”

"El SIEM permite la recopilación, normalización y análisis de eventos de seguridad, brindando una vista centralizada de las amenazas potenciales." (Islam & Rafique, 2024)

2.1.4. Monitoreo de red

Según IBM el monitoreo de una red es utilizar distintos programas para verificar el estado y la confiabilidad continua de una red informática y así detectar señales de alarma como actividad inusual y optimizar flujos de datos. (IBM, s.f.)

2.1.5. Detección de anomalías

Para IBM “La detección de anomalías, o detección de valores atípicos, es la identificación de observaciones, eventos o puntos de datos que se desvían de lo habitual, estándar o esperado, lo que los hace inconsistentes con el resto de un conjunto de datos.” (IBM, s.f.)

Por otra parte, CrowdStrike define la detección de anomalías como “el proceso de analizar un conjunto de datos e identificar incidencias únicas o patrones que se desvían significativamente de la actividad de referencia” (Cross, 2024)

2.1.6. Logs (Archivos de registro)

Según TechTarget un archivo de registro es una documentación que se genera de manera automática y con marca de tiempo de eventos relevantes dentro de un sistema informático. Estos logs registran eventos como errores, ejecución de procesos o mensajes, junto con estampas de tiempo lo que permite analizar el comportamiento de un sistema especifico y detectar anomalías incidentes de seguridad. (Awati & Wigmore, 2024)

2.1.7. SOAR (Security Orchestration, Automation and Response)

“Un SOAR hace referencia a un conjunto de servicios y herramientas que automatizan la prevención y respuesta contra los ciberataques. Para lograr esta automatización, se unifican las integraciones, se define cómo deben ejecutarse las tareas y se desarrolla un plan de respuesta a incidentes adaptado a las necesidades de tu organización.” (Microsoft, 2025)

Esto significa que se unen diferentes herramientas, que orquestadas de la manera correcta pueden automatizar la detección y la pronta respuesta a incidentes de seguridad, minimizando la intervención humana, logrando reducir el Objetivo de Tiempo de Recuperación (RTO por sus siglas en inglés) de las empresas y mejorar su respuesta ante desastres en el contexto de ciberseguridad.

2.1.8. Mitigación

La mitigación es, según IBM “La estrategia de planificación y desarrollo de opciones para reducir las amenazas a los objetivos del proyecto a las que suele enfrentarse una empresa u organización.” (Finn & Downie, 2024)

También, este mismo autor se refieren a la mitigación como “La culminación de las técnicas y estrategias utilizadas para minimizar los niveles de riesgo y reducirlos a niveles tolerables. Al tomar medidas para negar amenazas y desastres, una organización estará en una posición sólida para eliminar y limitar los contratiempos.” (Finn & Downie, 2024)

Por otra parte, la NIST define Mitigación como “Una decisión, acción o práctica destinada a reducir el nivel de riesgo asociado con uno o más eventos de amenaza, escenarios de amenaza o vulnerabilidades”. También aclara que puede referirse a la disminución temporal del impacto de una vulnerabilidad o de la probabilidad de su explotación. (National Institute of Standards and Technology, s.f.)

2.1.9. Resiliencia

En el contexto de la ciberseguridad, la resiliencia es hoy en día uno de los aspectos más importantes, ya que es la manera en que se asegura la continuidad del negocio. Según IBM (IBM, 2022), “La resiliencia cibernética es la capacidad de una organización para prevenir, resistir y recuperarse de incidentes de ciberseguridad. Es la capacidad de continuar brindando los resultados esperados a pesar de experimentar eventos cibernéticos desafiantes, como ataques cibernéticos, desastres naturales o recesiones económicas. Un nivel medido de competencia y resiliencia en materia de seguridad de la información afecta a la forma en que una organización puede continuar con las operaciones empresariales con poco o ningún tiempo de inactividad.”

2.1.10. Recuperación Autónoma

Cuando hablamos de ciberseguridad, es correcto referirse a la recuperación autónoma como la capacidad que tienen los sistemas para restaurarse de manera automática a un estado que es funcional después de una interrupción, esto sin la intervención humana y utilizando mecanismos de “auto-reparación”.

Para SentinelOne “El objetivo de la fase de recuperación es devolver el componente afectado a su estado operativo normal. Esto implica restaurar las copias de seguridad de las últimas instantáneas seguras conocidas, verificar la integridad del componente y restaurar el software, los servicios y las cuentas deshabilitados. Es posible que algunos datos, como los datos que se escribieron después de que el componente se viera comprometido, se pierdan después de la recuperación, pero puede recuperar esos datos y moverlos al componente limpio. Si ha implementado la redundancia de datos, esto podría ayudar a recuperar datos. Una vez que el

sistema se haya trasladado de nuevo al entorno de producción, supervise para detectar cualquier signo de infección.” (SentinelOne, 2025)

2.1.11. Orquestación

Hoy día, utilizar diversas herramientas en un sólo sistema, entrelazadas de la manera correcta permite la creación de un modelo funcional de mucho valor para un fin en específico. Se habla de orquestación a este tipo de sistemas que en conjunto realizan una tarea de valor. Según Bunce (Bunce, 2022) la orquestación es “la capacidad de utilizar la tecnología para organizar múltiples elementos de una empresa, como sus personas, sistemas, datos y bots. Da a los equipos de TI visibilidad de los diferentes sistemas utilizados para llevar a cabo tareas de automatización y cómo están conectados, y les permite supervisar estos sistemas en una única plataforma para optimizar las operaciones.”

Por otro lado, a la hora de hablar de ciberseguridad, Imán (Imán, 2019) se refiere a la orquestación como “el acto de integrar tecnologías dispares y conectar herramientas de seguridad, tanto específicas de seguridad como no específicas de seguridad, con el fin de hacerlas capaces de trabajar juntas y mejorar la respuesta a incidentes.”

2.2. Funcionamiento de las tecnologías clave

Es este apartado se explica la forma en como operan e interactúan las tecnologías a utilizar en el modelo para lograr detectar, responder y restaurar de forma autónoma. A continuación se presenta el flujo general del modelo.

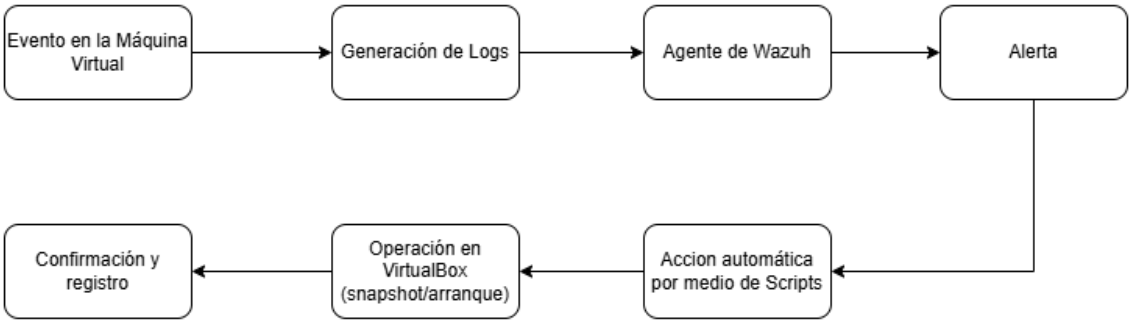

Tabla 12. Flujo general

2.2.1. Wazuh (Detección y Orquestación de la respuesta)

Arquitectura práctica

- Cada máquina virtual ejecuta un agente de Wazuh que recolecta eventos por medio de archivos de logs.
- El servidor de Wazuh centraliza estos eventos y los correlaciona con reglas para generar alertas con diferentes niveles de severidad.
- Dependiendo del nivel de alerta, se dispara una acción ya preconfigurada (active responses) que delegan en un script.

Configuración

Para la correcta funcionalidad del modelo, deben configurarse los siguientes elementos:

a) Fuentes de logs en cada Máquina Virtual, algunas ubicaciones de estos los son /var/log/auth.log, /var/log/syslog
b) Reglas que son las encargadas de describir las condiciones de interés como por ejemplo múltiples fallos de autenticación o modificaciones masivas de archivos. (Wazuh, Rules Sintax, s.f.)
c) Active responses asociadas a reglas o grupos de reglas. Estas involucran un Script de Python encargado de la respuesta autónoma cuando la alerta supera el umbral. (Wazuh, Active Response, s.f.)

La Ilustración 9 muestra un ejemplo de una regla de Wazuh donde si un agente de Wazuh reporta N cantidad de eventos de modificación de archivos críticos en X cantidad de segundos, se eleva el nivel y se dispara la alerta

```
<rule id="100200" level="10">
  <if_matched_sid>554</if_matched_sid>        <!-- Regla base: modificación de archivos -->
  <frequency>50</frequency>                  <!-- 50 eventos -->
  <timeframe>60</timeframe>                  <!-- en 60 segundos -->
  <description>Posible cifrado masivo de archivos (ransomware)</description>
  <group>malware, ransomware, recovery</group>
</rule>

```

Ilustración 9. Ejemplo de Regla

Disparo de la acción

En Wazuh, las active responses se asocian a reglas o grupos y ejecutan un comando con el payload de la alerta. Ese payload será consumido por el script Python.

2.2.2. Scripting en Python (automatización de la respuesta)

Rol del script

Recibe el evento que proporciona Wazuh por medio del Active Response

Decide la acción a tomar según la regla que se dispara y los metadatos como el host afectado y la criticidad.

Ejecuta las operaciones utilizando VBoxManage (herramienta de administración incluida en VirtualBox)

Registra el resultado en logs para ver la trazabilidad de la operación.

La Ilustración 10 muestra cual sería la lógica de decisión del script utilizando pseudocódigo

```
if alerta.level >= 10 and 'ransomware' in alerta.groups:
    vm = mapear_vm(alerta.agent.name)      # 'Debian12_TFG'
    snap = obtener_snapshot_por_defecto(vm) # 'snapshot-inicial'
    ejecutar_restauracion(vm, snap)         # vía VBoxManage
    verificar_estado(vm)                    # VM arrancada y estable
    loggear_resultado(vm, snap, OK/ERROR)
else:
    registrar("No cumple criterios de recuperación automática")

```

Ilustración 10. Pseudocódigo de la lógica de decisión

2.2.3. VirtualBox (recuperación por snapshot)

Según Oracle “Con las instantáneas, puede guardar un estado particular de una máquina para su uso posterior. En cualquier momento posterior, puede volver a eso , aunque haya cambiado considerablemente la máquina virtual desde entonces. Por lo tanto, una instantánea de una máquina virtual es similar a una máquina en estado Guardado, pero puede haber muchos de ellos, y estos salvados se conservan los estados.” (Oracle, Snapshots, s.f.)

VirtualBox proporciona el punto de recuperación mediante snapshots predefinidos como por ejemplo un snapshot inicial antes de iniciar las pruebas.

“VBoxManage es la interfaz de línea de comandos de Oracle VM VirtualBox. Con él, puedes controlar completamente Oracle VM VirtualBox desde la línea de comandos de tu sistema operativo anfitrión. VBoxManage admite todas las funciones a las que la interfaz gráfica de usuario te da acceso, pero también ofrece muchas más. Expone todas las capacidades del motor de virtualización, incluso aquellas que no están disponibles desde la GUI.” (Oracle, VBoxManage, s.f.)

Por medio del VBoxManage permite apagar, restaurar e iniciar la máquina virtual sin la necesidad de intervención humana.

Flujo de acciones de VirtualBox

a) Aísla o apaga la máquina virtual afectada si es que aún se encuentra encendida para evitar daños adicionales.
b) Restaura el ultimo snapshot seguro.
c) Reinicia la máquina virtual afectada con el snapshot seguro cargado para continuar con los servicios.

Para la ejecución de estas operaciones, VirtualBox necesita que previamente exista un snapshot válido y documentado donde se conozca exactamente los nombres del snapshot y de la máquina virtual.

2.2.4. Trazabilidad

Componente	Función	Entrada	Salida	Evidencia
Wazuh (agent/ manager)	Detecta patrón y genera alerta con nivel	Logs del host	Alerta con rule.id, level, agent.name, groups	Regla 100200 (ejemplo), grupo recovery
Active Response	Invoca la automatización	Alerta (JSON)	Ejecución de script con payload	Configuración de AR asociada al grupo/regla
Python (Script)	Decide y orquesta la recuperación	Payload de alerta	Comandos VBoxManage ejecutados; log de resultado	Script y bitácora de ejecución
VirtualBox	Aplica recuperación	Comandos del script	VM restaurada y arrancada	Snapshot “snapshot-inicial”, estados de VM
Verificación	Confirma estabilidad	VM en marcha	OK/ERROR + tiempos	Registro de verificación (ping/puertos)

Tabla 13.Trazabilidad

3. Capítulo 3. Marco Metodológico

3.1. Tipo de investigación

En concordancia con el objetivo general de esta investigación “Proponer un modelo de recuperación autónomo para entornos virtuales ante incidentes de seguridad”, Este estudio se enmarca en el tipo de investigación aplicada.

Este estudio no busca producir conocimiento nuevo sino utilizar conocimiento y herramientas ya existentes para crear una nueva herramienta que funcione como modelo de recuperación autónoma ante incidentes de seguridad y así atender una necesidad particular.

3.2. Alcance Investigativo

Dado el contexto de la presente investigación se consideran los siguientes tipos de investigación.

Exploratorio

La profesora Ana Isabel Mora Vargas en la revista Educación de la Universidad de Costa Rica, define la investigación exploratoria como la investigación que “tiene por objeto esencial familiarizar al investigador con un tema que no ha abordado antes, novedoso o escasamente estudiado.” (Mora Vargas, 2024). Esto es congruente con esta investigación ya que, si bien, hasta la fecha se han realizado diversos estudios acerca de herramientas de detección y recuperación, existen pocos estudios del tema o que combinen el uso de estos programas de código abierto para la implementación de un SOAR de bajo costo.

Descriptivo

Según el concepto de investigación descriptiva de la profesora Mora Vargas, el cual dice que” Los estudios descriptivos son útiles para analizar cómo es y cómo se manifiesta un fenómeno y sus componentes.”, podemos definir esta investigación como descriptiva ya que se pretende medir el rendimiento del modelo así como el tiempo de recuperación del sistema posterior a un incidente de seguridad.

3.3. Enfoque

Para esta investigación, se propone un enfoque alternativo siguiendo el modelo propuesto por M. Phil. Luis Carlos Naranjo Zeledón (Naranjo Zeledón, 2020) desde una perspectiva integral que cumpla con los objetivos planteados.

A continuación se abordan los encuadres ontológico, epistemológico y axiológico, los cuales son pilares de este enfoque.

3.3.1. Encuadre Ontológico

Para el encuadre ontológico se presenta el siguiente mapa conceptual. Este descompone el objeto de estudio que en este caso es el modelo de recuperación autónomo, para poder entender con claridad los conceptos involucrados en la detección, respuesta y restauración ante incidentes de seguridad en entornos virtualizados.

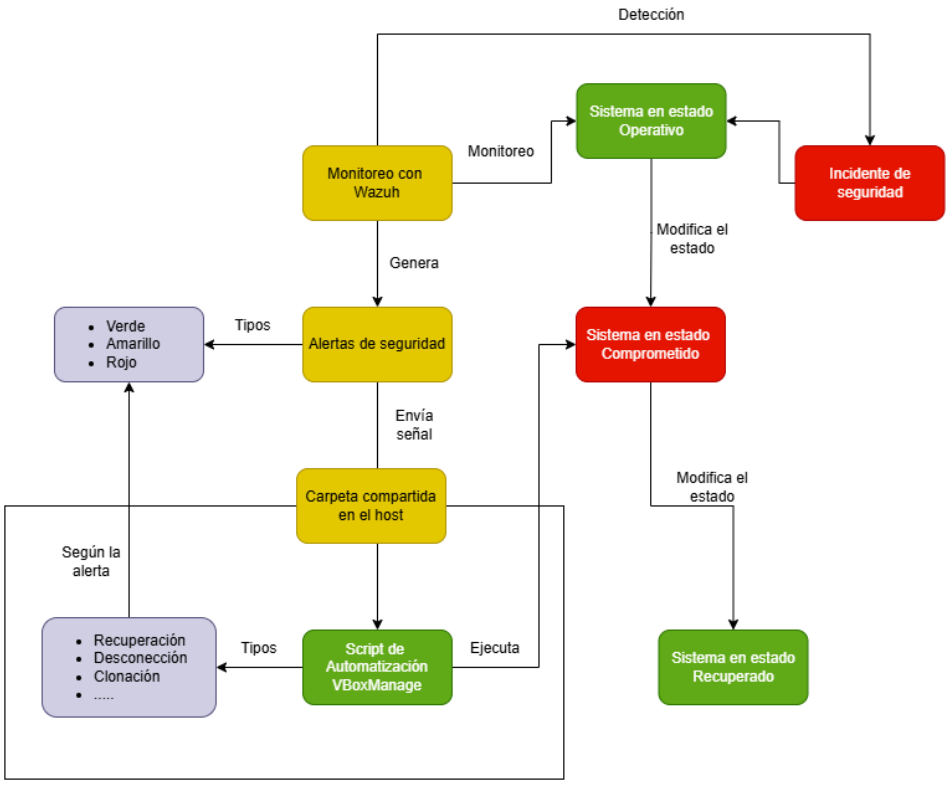

Ilustración 11. Ontología del Modelo de recuperación autónoma

Fuente: Elaboración propia

3.3.2. Encuadre Epistemológico

Esta investigación se aborda de una postura técnico observacional, donde el investigador asume el rol de analista e intérprete del comportamiento del sistema frente a diferentes escenarios de incidentes de seguridad. Se simulan diversas situaciones simuladas para observar cómo interactúan los diferentes componentes del modelo.

Por medio de pruebas, y la medición de tiempos de respuesta, se recopila evidencia que permitan demostrar la efectividad del modelo, así como los factores que influyen en su desempeño. Esto permite recolectar conocimiento técnico-práctico fundamentado en la observación del comportamiento de cada componente.

3.3.3. Encuadre axiológico

Para poner a prueba el modelo de recuperación autónoma, se van a simular distintos tipos de incidentes de seguridad dentro de un entorno virtual preparado para este fin. La idea es ver cómo se comporta el sistema frente a situaciones reales, sin que haya intervención humana directa.

Este proceso se apoya en valores que son clave para este trabajo: la importancia de mantener la seguridad, asegurar la continuidad de los servicios y lograr una respuesta rápida y eficiente ante cualquier amenaza que afecte la infraestructura. Lo que se busca, en el fondo, es que el sistema sea confiable y útil para organizaciones que no tienen muchos recursos.

Durante cada prueba se irá documentando lo que ocurre: cuánto tarda en detectar el problema, qué acciones ejecuta por sí mismo, cuánto tiempo lleva la recuperación, y cuál es el estado final del entorno al finalizar la prueba. Con esa información, se podrá evaluar si el modelo realmente responde como se espera.

También se va a observar si las máquinas virtuales afectadas vuelven a su estado original correctamente, si el sistema queda estable y si puede manejar diferentes

tipos de amenazas sin fallar. Todo esto permitirá tener una idea más clara de qué tan útil y aplicable es esta solución en la práctica.

3.4. Diseño

El diseño de este proyecto está enfocado en la creación, prueba y evaluación de un modelo funcional para recuperación autónoma ante incidente de seguridad. Este diseño va de acuerdo con el enfoque seleccionado y permite el diseño de un artefacto medible, replicable y que resuelve una necesidad real del campo de la ciberseguridad.

Este diseño busca recopilar diferentes variables como el tiempo de detección, respuesta y recuperación ante incidentes simulados, asi como el estado final de las máquinas después de la intervención automática del modelo. Con estas variables, se espera establecer una relación entre el tipo de incidente y la efectividad del modelo en cuanto a autonomía, eficiencia y estabilidad.

Este diseño permite evaluar el modelo desde la etapa de la ocurrencia del incidente hasta la recuperación del sistema, estructurando etapas como la construcción del entorno virtual de pruebas, la integración de herramientas como Wazuh, scripting personalizado y técnicas de virtualización, la ejecución de incidentes controlados y, finalmente, la recolección y análisis de los resultados.

3.5. Población y muestreo

Para esta investigación, la población será conformada por entornos virtuales vulnerables a incidentes de seguridad. Es este caso serán máquinas virtuales que simularán servicios críticos en un contexto organizacional. Estos entornos representan casos comunes donde la disponibilidad y continuidad del sistema pueden verse comprometidas.

La muestra serán diversas máquinas virtuales diseñadas para esta investigación y configuradas de manera que representen diferentes servicios como servidor de archivos, servidor web y servidor de base de datos. Se realizarán pruebas sobre estas máquinas que simulen diferentes tipos de incidentes para así poder evaluar la capacidad del modelo para detectar, responder y recuperar los sistemas antes

mencionados. La selección de estas máquinas y escenarios se realizó de forma intencional, considerando su representatividad y relevancia para el contexto de ciberseguridad.

3.6. Instrumento de recolección de datos

Para la recolección de datos se utilizará una tabla de evaluación técnica, diseñada para la recolección de las métricas que se observan en la ejecución de cada simulación con la intención de cumplir con el objetivo de "*Analizar la efectividad del sistema de recuperación autónomo implementado frente a distintos tipos de incidentes de seguridad a través de la ejecución de pruebas prácticas, recolección de métricas y comparación de resultados para evaluar el desempeño del sistema y validar su capacidad de respuesta y autonomía en escenarios críticos.*". Este instrumento va a permitir documentar la información real del modelo de recuperación autónoma ante diferentes simulaciones de incidentes de seguridad.

La tabla contempla los siguientes campos:

- Id de la simulación
- Tipo de incidente simulado
- Máquina virtual afectada
- Tiempo de detección en segundos
- Tiempo de respuesta en segundos
- Tiempo total de recuperación en segundos
- Acción ejecutada automáticamente
- Estado final de la máquina virtual
- Resultado de la restauración
- Observaciones relevantes

Este instrumento se construyó con base a los objetivos específicos y validado mediante su uso en pruebas piloto.

3.6.1. Matriz de evaluación

Con el fin de recopilar la información necesaria para la evaluación del modelo de recuperación autónoma y comprobar la efectividad de este en entornos virtuales

controlados, se elabora una matriz de evaluación que va a ser fundamental para documentar la ejecución de cada prueba realizada.

Simulación #					
Tipo de Incidente					
VM Afectada					
Tiempo de Detección (s)					
Tiempo de Respuesta (s)					
Tiempo de Recuperación (s)					
Acción Ejecutada					
Estado Final de la VM					
¿Se restauró correctamente?					
Observaciones					

Ilustración 12. Matriz de Evaluación - Recuperación Autónoma

Fuente: Elaboración propia

3.7. Técnicas de análisis de información

En esta sección, se describe el proceso general de análisis de la información recopilada a partir de pruebas controladas ejecutando el modelo de recuperación autónoma para entornos virtuales ante incidentes de seguridad. El análisis se centra en evaluar la capacidad y tiempos de respuesta del modelo como tal.

Para lo anterior se diseñará un diagrama de flujo que muestre el proceso que se siguió para la recolección de datos, a partir de pruebas en entornos controlados. Estos datos se analizarán por medio de técnicas de estadística descriptiva con la intención de identificar patrones de comportamiento del modelo de recuperación autónoma ante distintos tipos de incidentes de seguridad.

Se pretende calcular:

- Tiempo promedio de detección, respuesta y recuperación
- Tasas de éxito en la restauración de máquinas virtuales
- Frecuencia de acciones ejecutadas
- Porcentaje de estabilidad post-recuperación

Estos datos serán organizados en tablas comparativas y representados de manera gráfica, lo que va a facilitar la interpretación visual de los datos.

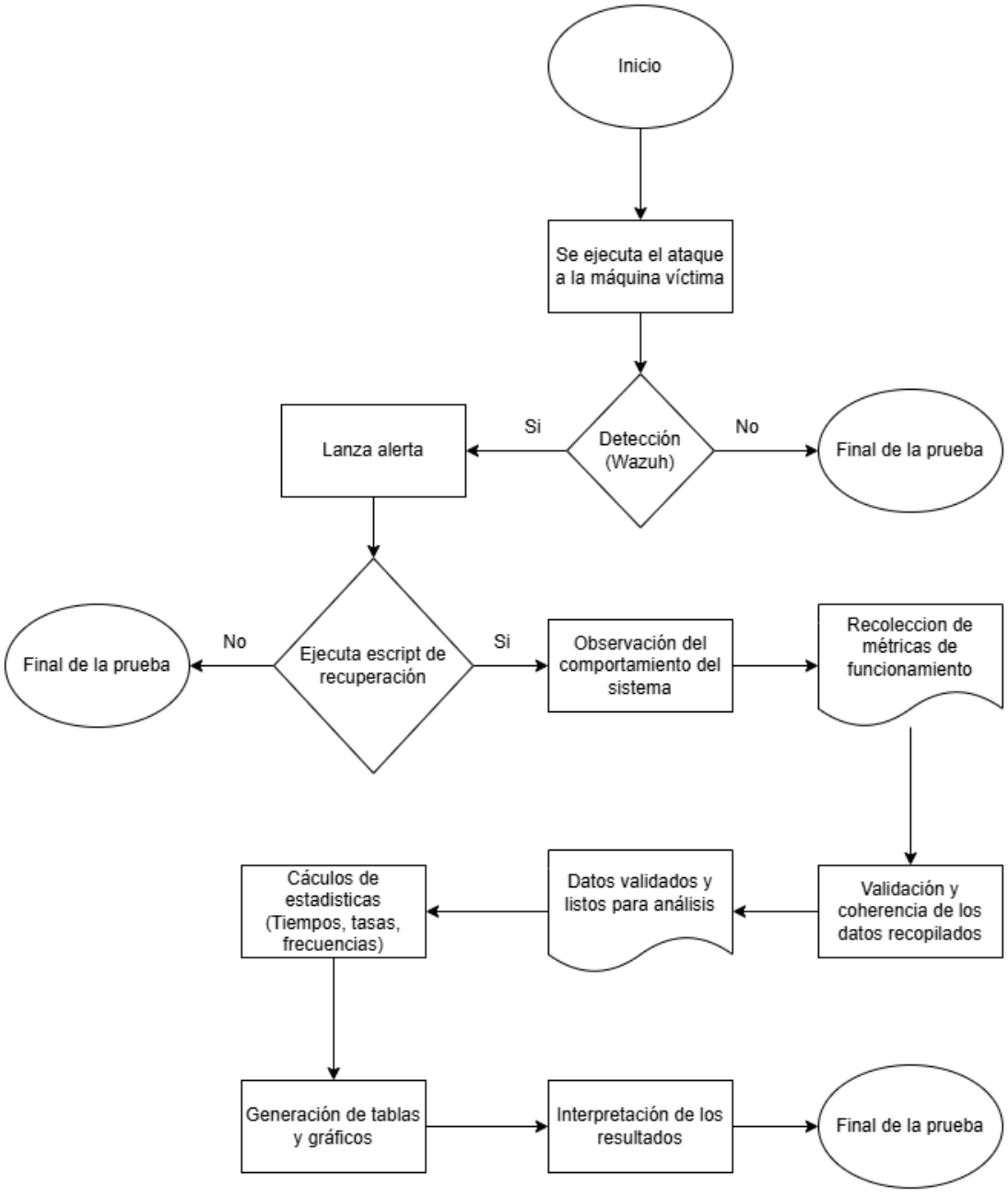

Ilustración 13. Diagrama de flujo de Técnicas de Análisis de Información

Fuente: Elaboración propia

4. Capítulo 4. Análisis de diagnostico

En este capítulo se presenta el análisis del desempeño del modelo de recuperación autónoma desarrollado para entornos virtuales ante incidentes de seguridad. El objetivo es valorar, a partir de ejecuciones controladas en laboratorio, la capacidad del modelo para restaurar una máquina virtual comprometida y completar el flujo de recolección de evidencias en tiempos consistentes y adecuados para el contexto de las pymes.

El análisis se apoya en los lineamientos metodológicos definidos en el marco metodológico del proyecto, en particular en el uso de una matriz de evaluación técnica para la recolección de métricas y en la aplicación de estadística descriptiva para sintetizar los resultados obtenidos a lo largo de múltiples simulaciones.

4.1. Descripción del entorno experimental y aplicación de la matriz de evaluación

El diagnóstico se realiza íntegramente en el laboratorio diseñado para esta investigación, compuesto por una infraestructura virtual basada en Oracle VirtualBox y un conjunto de máquinas que representan servicios críticos dentro de una organización tipo pyme. El rol central lo desempeña el servidor de monitoreo y correlación de eventos, sobre el cual se ejecuta Wazuh en su arquitectura completa (Manager, Indexer y Dashboard). A este se conectan los agentes desplegados en las máquinas virtuales víctimas, encargados de reportar los eventos relevantes del sistema operativo y de activar, cuando corresponde, el mecanismo de respuesta autónoma.

El modelo de recuperación autónoma integra tres elementos principales: Wazuh como plataforma de detección y orquestación de la respuesta, un script desarrollado en Python responsable de la ejecución secuencial de las acciones de recuperación y recolección de evidencias, y VirtualBox, que proporciona las capacidades de snapshot y restauración de las máquinas virtuales. Esta integración fue descrita en detalle en los capítulos previos del presente proyecto y constituye la base sobre la cual se aplica el análisis de diagnóstico.

En concordancia con el instrumento definido en el Capítulo 3, la recolección de datos se lleva a cabo mediante una matriz de evaluación que registra, para cada simulación de incidente, los tiempos parciales de cada fase del flujo de trabajo y los tiempos globales de restauración y finalización del proceso.

Para el análisis aquí presentado se dispone de veinte ejecuciones completas del modelo bajo un mismo escenario de incidente, lo que permite evaluar la estabilidad temporal del sistema y la consistencia de su comportamiento.

Cada ejecución del modelo comprende, de forma general, las siguientes etapas: detección del incidente por parte de Wazuh, activación del módulo de respuesta activa, ejecución del script de automatización, recolección de evidencias (volcado de memoria, generación de hash, compresión de logs y clonación de disco), apagado controlado de la máquina virtual afectada, restauración del snapshot previamente definido como estado limpio, arranque de la máquina restaurada, verificación de disponibilidad mediante guest control y, finalmente, generación del reporte de resultados. Estas fases se reflejan en las métricas recogidas en la tabla de resultados del laboratorio.

4.2. Descripción de las métricas registradas

El instrumento de evaluación contempla, para cada ejecución, diez métricas temporales expresadas en el formato **minutos:segundos,milisegundos**, las cuales corresponden a fases específicas del flujo automatizado. Estas métricas permiten descomponer el comportamiento del modelo y entender la contribución de cada etapa al tiempo total de recuperación.

El indicador time_to_restore_s representa el tiempo global de restauración observado por el sistema, es decir, la duración del proceso desde que se inicia el flujo de recuperación hasta que la máquina virtual se considera nuevamente disponible para la operación. El promedio obtenido en las 20 ejecuciones es de 3:58,107, lo que equivale aproximadamente a cuatro minutos de recuperación por incidente.

El indicador workflow_total_s recoge el tiempo total de ejecución del script de automatización, incluyendo todas las tareas de recolección de evidencias y validaciones finales. El valor promedio registrado es de 4:17,292, lo que muestra que el flujo completo, desde la activación del script hasta la finalización del reporte, se mantiene claramente por debajo de los cinco minutos en todas las ejecuciones.

Las métricas asociadas a las evidencias son las siguientes. El tiempo medio de generación del dump de memoria (memory_dump_s) es de 0:34,066, mientras que el cálculo del hash SHA-256 de la memoria (memory_sha256_s) presenta un promedio de 0:04,366. La recolección y compresión de los logs del sistema invitado (guest_logs_collection_s) requiere en promedio 0:09,044. Estos tiempos indican que la captura y aseguramiento de evidencia volátil y de registros se realiza en menos de un minuto en todos los casos, lo cual resulta adecuado para un proceso que se ejecuta inmediatamente antes de la restauración.

La sección de control del estado de la máquina incluye el indicador shutdown_and_poweroff_s, con un tiempo promedio de 0:30,052, que refleja la duración del apagado controlado de la máquina virtual comprometida. La restauración del snapshot (snapshot_restore_s) presenta un tiempo medio de 0:01,444, evidenciando que el mecanismo de recuperación basado en snapshots es particularmente eficiente en este entorno. A continuación, el tiempo de arranque de la máquina restaurada y confirmación de disponibilidad mediante guestcontrol (vm_boot_and_guestcontrol_ready_s) registra un promedio de 0:19,093.

Por último, dos métricas describen el comportamiento de la clonación de disco, considerada la tarea más intensiva en el flujo de evidencias. El indicador disk_clone_total_s muestra un tiempo promedio de 1:45,026, mientras que el tiempo para el cálculo del hash del clon de disco (disk_clone_hash_total_s) es de 0:52,631. La suma aproximada de ambos tiempos indica que el manejo del disco representa una proporción significativa del esfuerzo total del modelo.

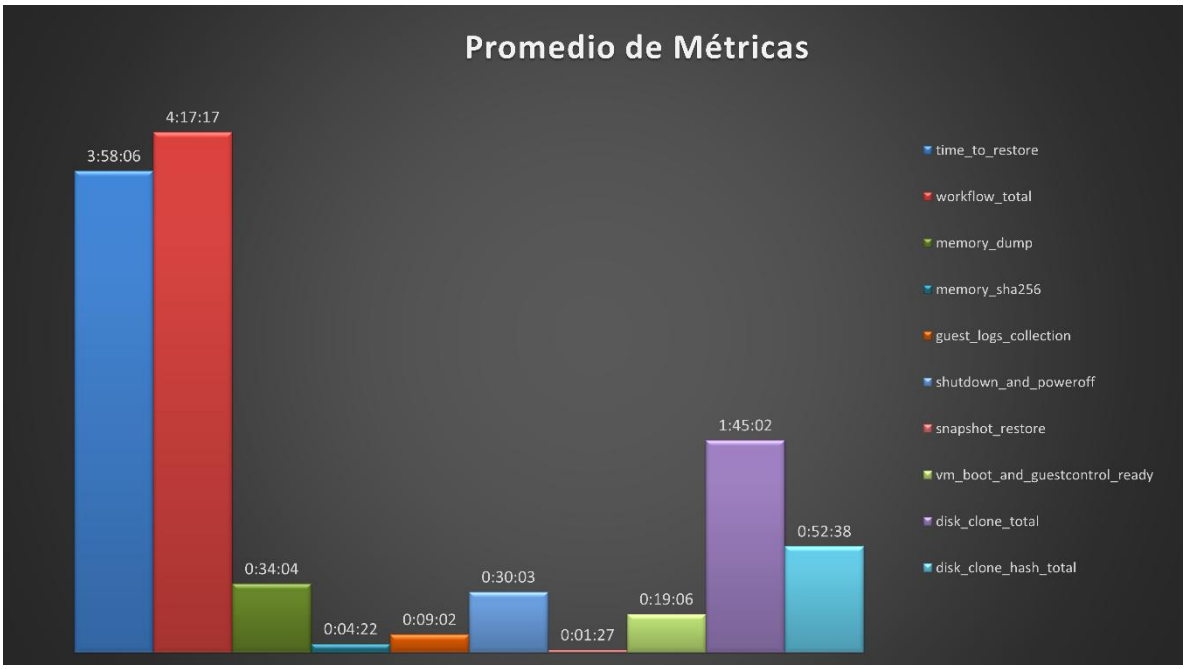

Ilustración 14. .Tiempo promedio de las diferentes métricas evaluadas.

Fuente: Elaboración Propia

4.3. Análisis descriptivo de los resultados

El análisis descriptivo de las veinte ejecuciones evidencia que el modelo de recuperación autónoma se comporta de manera estable y predecible ante el escenario de incidente considerado. El tiempo total de flujo (workflow_total_s) se mantiene consistentemente cercano al promedio de 4:17,292, con variaciones que no superan el orden de decenas de segundos entre la ejecución más rápida y la más lenta. Esta baja dispersión sugiere que el modelo no presenta comportamientos anómalos ni cuellos de botella impredecibles, lo cual es relevante para su uso en entornos operativos de pymes que requieren tiempos de respuesta confiables.

El indicador time_to_restore_s, con un promedio de 3:58,107, se mantiene sistemáticamente inferior al tiempo total del flujo, lo que indica que la porción del proceso estrictamente necesaria para devolver la máquina a un estado operativo se completa antes de que finalicen las tareas accesorias, como el cálculo de hashes o la redacción del reporte. Este comportamiento es coherente con el objetivo de la solución, que prioriza la continuidad operativa del servicio por encima de la finalización de tareas administrativas o de documentación.

Al descomponer el flujo en sus componentes, se observa que las tareas asociadas a la recolección de evidencias de memoria y registros (dump, hash y compresión de logs) suman en conjunto alrededor de 47 segundos de ejecución. Desde la perspectiva de un incidente en producción, este tiempo resulta razonable, pues añade un sobrecosto mínimo a la restauración a cambio de garantizar evidencia valiosa para cualquier análisis posterior. Además, la coherencia de los promedios sugiere que estas tareas se ven poco afectadas por factores externos como el estado del sistema o las oscilaciones de carga del host de virtualización.

Por otra parte, el apagado controlado, la restauración del snapshot y el arranque posterior de la máquina implican, en conjunto, un tiempo promedio cercano a un minuto, lo que refuerza la viabilidad del enfoque basado en snapshots para procesos de recuperación rápida. El hecho de que la restauración del snapshot presente un promedio de 0:01,444 confirma que la inversión temporal asociada a la creación previa de estos puntos de recuperación se ve ampliamente compensada durante la fase de respuesta a incidentes.

Desde el punto de vista del consumo temporal, la mayor carga recae sobre la clonación de disco y el cálculo de su hash. Si se consideran los promedios mencionados, estas dos tareas concentran aproximadamente el 61% del tiempo total del flujo de ejecución, lo que las convierte en el componente más costoso en términos de tiempo. Sin embargo, se trata de actividades necesarias para garantizar la preservación íntegra del estado del disco comprometido, lo que aporta valor añadido al modelo, ya que no se limita a restaurar el servicio, sino que asegura una copia forense que puede ser posteriormente analizada en un entorno aislado.

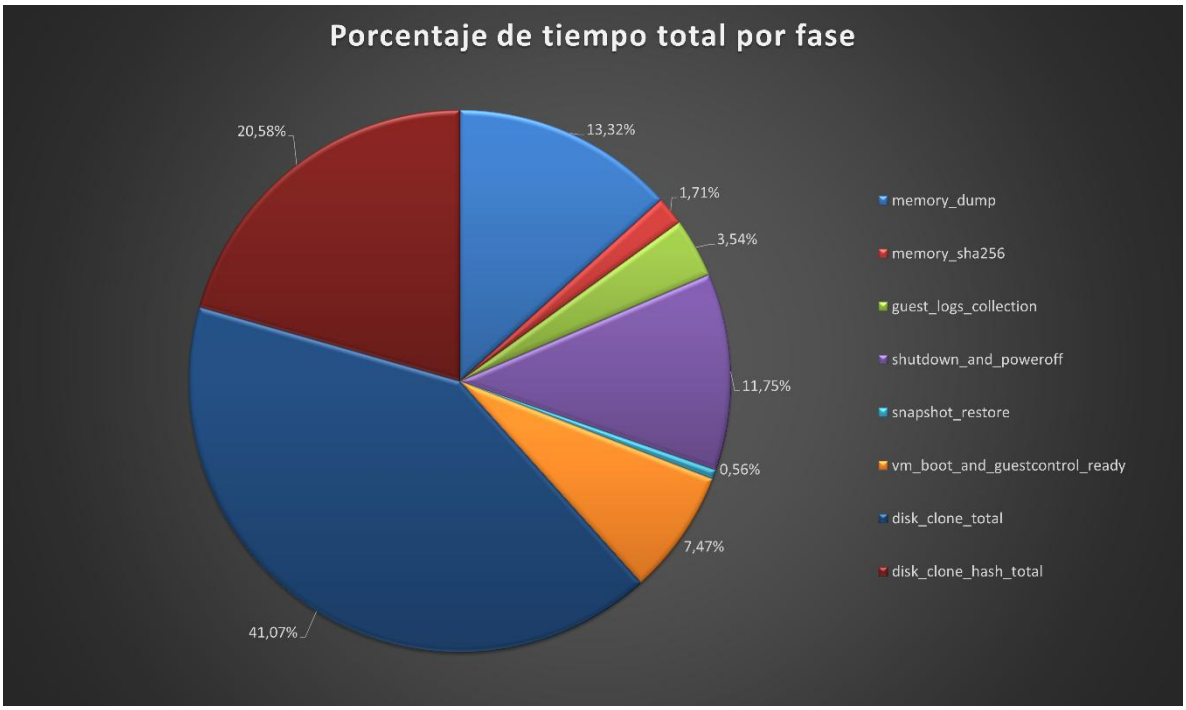

Ilustración 15. Porcentaje del tiempo total del flujo que corresponde a cada fase.

Fuente: Elaboración propia

4.4. Interpretación del desempeño del modelo en términos de MTTR

El indicador más relevante para la valoración del modelo en el contexto de la continuidad operativa de las pymes es el tiempo medio de recuperación (MTTR). Para efectos de este diagnóstico, el MTTR puede aproximarse a partir del indicador time_to_restore_s, dado que este representa el tiempo que transcurre desde la activación del flujo hasta que la máquina virtual se encuentra nuevamente disponible.

El valor promedio de 3:58,107 por ejecución indica que, ante un incidente de seguridad del tipo simulado en el laboratorio, la organización podría recuperar el servicio en un tiempo cercano a los cuatro minutos sin intervención humana directa. Este resultado contrasta con los escenarios tradicionales de recuperación manual, en los cuales la restauración de una máquina virtual, la verificación de su estado y la ejecución de tareas de recolección de evidencia tienden a ser considerablemente más lentas y dependientes de la intervención humana, especialmente en entornos de pymes sin procedimientos formalizados. En ese sentido, el modelo cumple con

el objetivo de reducir de forma significativa los tiempos de recuperación y, por ende, el tiempo de indisponibilidad del servicio.

La estabilidad observada en las veinte ejecuciones refuerza esta interpretación. La variación entre la ejecución más rápida y la más lenta no compromete el orden de magnitud del MTTR, que se mantiene consistentemente inferior al umbral de cinco minutos. Ello sugiere que el modelo es robusto frente a pequeñas fluctuaciones en el entorno de ejecución y que puede considerarse fiable para ser aplicado de forma repetida en contextos similares.

Desde una perspectiva cualitativa, este comportamiento es especialmente relevante para las pymes, ya que ofrece una ventana de recuperación que se encuentra muy por debajo de los tiempos que usualmente se asocian a la intervención manual de personal técnico. El ahorro en tiempo de indisponibilidad se traduce, por tanto, en una mitigación efectiva del impacto operativo y en una mejora tangible del nivel de resiliencia ante incidentes de seguridad.

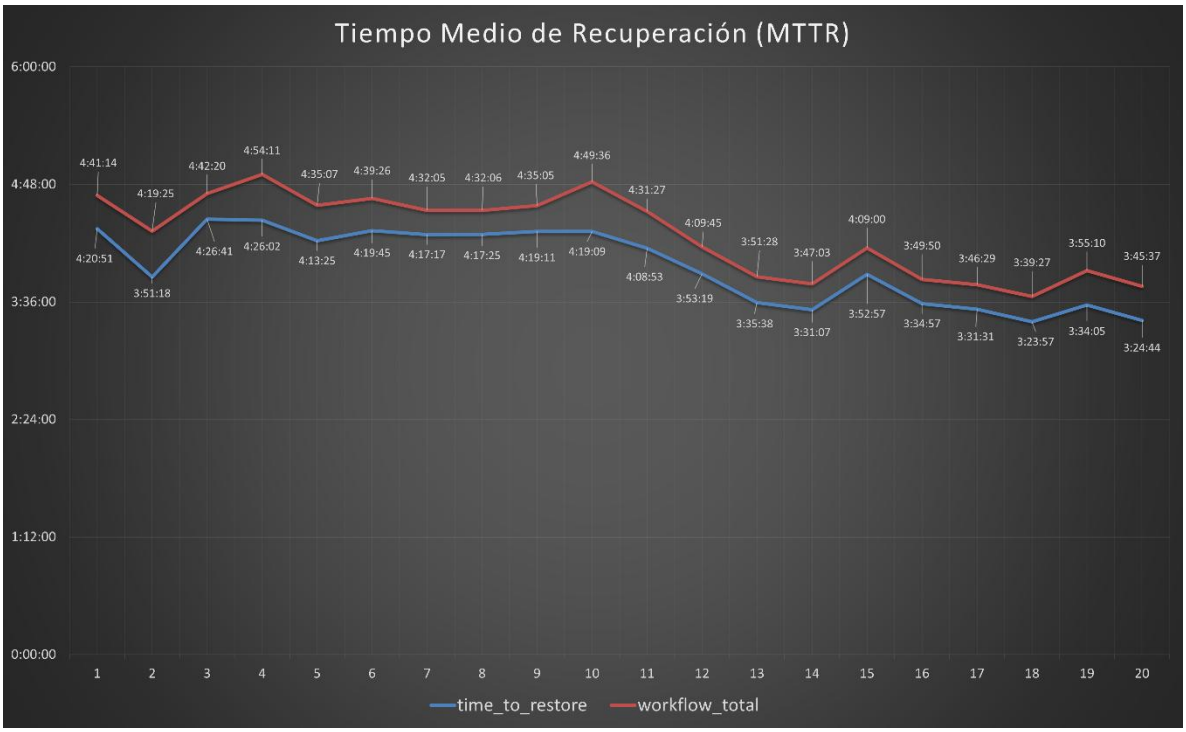

Ilustración 16. Estabilidad del MTTR y la variación marginal entre ejecuciones (time_to_restore, workflow_total).

Fuente: Elaboración propia.

En el gráfico anterior se observa una ligera tendencia decreciente en los valores de time_to_restore y workflow_total conforme avanzan las ejecuciones. Esta tendencia no obedece a cambios en la lógica del modelo, sino a la estabilización del entorno de laboratorio: calentamiento de cachés de disco y memoria, finalización de procesos de fondo del sistema anfitrión y reducción de sobrecarga en las máquinas virtuales. En conjunto, estos factores disminuyen gradualmente la latencia de operaciones de E/S y provocan una reducción suave pero consistente del MTTR observado.

4.5. Discusión de hallazgos y estabilidad del flujo de recuperación

Más allá de la cuantificación de tiempos, el análisis de diagnóstico permite discutir la coherencia interna del flujo de recuperación y su alineación con los objetivos de diseño del modelo. La secuencia de tareas implementada en el script Python refleja un equilibrio entre dos ejes: por un lado, la rapidez en la restauración del servicio, y por otro, la rigurosidad en la preservación de evidencia digital.

El hecho de que la clonación de disco y el cálculo de su hash consuman la mayor parte del tiempo del flujo tiene un impacto directo en el tiempo de recuperación, ya que en la versión actual del modelo estas tareas se ejecutan antes de la restauración del snapshot y forman parte del camino crítico que determina el MTTR. Esta decisión de diseño responde a la necesidad de preservar una imagen fiel del estado comprometido del sistema, garantizando que el clon de disco corresponda al momento del incidente y no a un estado ya restaurado, lo cual carecería de valor desde la perspectiva forense. En consecuencia, el modelo asume explícitamente un compromiso entre rapidez y rigor forense. Prioriza la obtención de una copia íntegra del sistema afectado, aun a costa de incrementar el tiempo medio de recuperación observado. Las posibles mejoras futuras deberían enfocarse en optimizar el rendimiento de la clonación (por ejemplo, mediante ajustes en el subsistema de almacenamiento o en la asignación de recursos de virtualización), y no en desplazar esta tarea a una fase posterior a la restauración, dado que ello supondría perder la evidencia del estado real del sistema comprometido.

Por otra parte, la brevedad de las tareas de captura de memoria y registros, sumadas a su baja variabilidad entre ejecuciones, sugiere que su inclusión en el flujo no compromete la rapidez de la restauración. Esto es especialmente importante, ya que la evidencia de memoria y de logs suele ser crítica para la comprensión de la causa raíz del incidente y, a su vez, es altamente volátil si no se captura de forma oportuna.

El mecanismo de apagado, restauración de snapshot y arranque controlado también demuestra un comportamiento estable, con tiempos reducidos y consistentes. Esta estabilidad permite prever que el modelo podría escalarse a otros escenarios de laboratorio con características similares, siempre que se mantengan condiciones de hardware comparables. La dependencia de snapshots como unidad de recuperación implica, desde luego, la necesidad de una gestión adecuada de estos puntos de restauración, pero los resultados del diagnóstico confirman que, cuando se administran correctamente, proporcionan una ventaja significativa frente a otros mecanismos de recuperación más pesados.

En conjunto, los resultados obtenidos muestran que el modelo de recuperación autónoma, en su estado actual, cumple con los criterios de desempeño definidos en la planificación metodológica: es capaz de restaurar la máquina virtual afectada en tiempos reducidos, de manera repetible y con generación sistemática de evidencias. Ello sienta una base sólida para considerar su aplicación en entornos reales de pymes, siempre que se ajuste la infraestructura y se establezcan procesos complementarios de monitoreo y notificación acordes a la realidad de cada organización.

4.6. Conclusiones del diagnóstico

El análisis de las veinte ejecuciones del modelo de recuperación autónoma permite concluir que la solución propuesta ofrece un desempeño adecuado para las necesidades de continuidad operativa de las pymes. El tiempo medio de recuperación, cercano a los cuatro minutos, y el tiempo total de flujo, inferior a cinco minutos, constituyen indicadores favorables en términos de reducción del impacto de los incidentes de seguridad sobre la disponibilidad de servicios críticos.

La descomposición del flujo en fases específicas evidencia que la mayor carga temporal recae sobre la clonación de disco y el cálculo de su hash, mientras que la captura de evidencias de memoria y registros, así como las operaciones de snapshot y arranque, se ejecutan en tiempos reducidos y con alta estabilidad. Este balance respalda la tesis de que es posible combinar, en un mismo modelo, tiempos de recuperación competitivos con buenas prácticas de preservación de evidencia digital.

Los resultados del diagnóstico confirman, además, que el modelo se comporta de forma consistente a lo largo de múltiples ejecuciones, lo que refuerza su idoneidad como mecanismo de recuperación automatizada en entornos controlados. Aunque los experimentos se realizaron en un laboratorio, las características de la infraestructura utilizada son representativas de lo que una pyme podría implementar con recursos limitados, lo que aporta realismo a las conclusiones obtenidas.

A partir de este análisis, se reconoce que futuras líneas de mejora podrían orientarse a optimizar el tiempo asociado a la clonación de disco, a introducir mecanismos de ejecución diferida para tareas no críticas y a complementar el modelo con canales de notificación automatizada hacia el personal responsable de la seguridad. No obstante, desde la perspectiva estrictamente diagnóstica, los resultados permiten afirmar que el modelo de recuperación autónoma cumple con las expectativas planteadas en los objetivos específicos y se consolida como una alternativa viable para fortalecer la resiliencia cibernética de las pequeñas y medianas empresas.

5. Capítulo 5. Propuesta de solución

5.1. Comprensión del negocio

El presente capítulo describe la propuesta de solución diseñada para atender la problemática identificada en las pequeñas y medianas empresas (pymes) respecto a la limitada capacidad de respuesta y recuperación ante incidentes de seguridad que afectan su infraestructura virtual. En este tipo de organizaciones, los recursos destinados a ciberseguridad son habitualmente insuficientes, y la dependencia de servicios de terceros o de procedimientos manuales aumenta la vulnerabilidad

operativa. De acuerdo con Andrés Casas de la Cámara de Industrias de Costa Rica (Casas, 2024), indica que “la Alianza Nacional de Ciberseguridad de los Estados Unidos, informa que más del 60% de las PYMES no logran recuperarse después de un ataque.”, lo cual expone a estas entidades a pérdidas financieras y operativas significativas ante ataques como ransomware, intrusiones o errores humanos.

El proyecto denominado Modelo de Recuperación Autónoma para Infraestructura Virtual ante Incidentes de Seguridad responde a la necesidad de contar con una solución tecnológica adaptable, económica y de implementación accesible para este tipo de organizaciones. Su propósito fundamental es reducir los tiempos de respuesta ante incidentes, automatizar las tareas de recuperación y garantizar la continuidad del negocio mediante la restauración inmediata de los entornos virtuales comprometidos.

En términos estratégicos, la propuesta se enmarca en la categoría de soluciones de respuesta automatizada ante incidentes de seguridad, combinando herramientas de monitoreo, scripting y virtualización. Sin embargo, a diferencia de las plataformas de orquestación y automatización de seguridad (SOAR) utilizadas por grandes corporaciones, el modelo propuesto emplea únicamente tecnologías de código abierto y de bajo costo, haciendo posible su adopción por pymes sin requerir inversión adicional en licenciamiento ni infraestructura compleja.

La solución está construida sobre tres pilares tecnológicos principales. En primer lugar, Wazuh se utiliza como sistema de monitoreo, detección de intrusiones y correlación de eventos. Este componente permite identificar comportamientos anómalos, correlacionar alertas y ejecutar respuestas automatizadas cuando las condiciones de seguridad lo requieren. En segundo lugar, se emplea un script desarrollado en Python, el cual actúa como motor de automatización encargado de ejecutar las acciones de recuperación, así como de recolectar y preservar evidencias forenses. Finalmente, Oracle VirtualBox, mediante su herramienta de línea de comandos VBoxManage, provee el entorno de virtualización en el que se gestionan los snapshots y se efectúa la restauración de las máquinas virtuales comprometidas.

El modelo propuesto establece un flujo autónomo de detección, decisión y acción, orientado a minimizar el tiempo entre la identificación del incidente y la restauración del servicio. La secuencia lógica se inicia con la detección de un evento de seguridad a través de Wazuh; posteriormente, el sistema evalúa la severidad del incidente y, si el nivel supera el umbral configurado (nivel 15), ejecuta una respuesta activa que lanza el script de recuperación. Dicho script realiza un conjunto de acciones estructuradas: recolección de evidencias, validación de integridad, restauración de snapshot y generación de un reporte de auditoría.

En el contexto de las pymes, esta propuesta ofrece beneficios tangibles. Permite reducir la dependencia de especialistas, disminuye los costos asociados a la recuperación y mejora los indicadores de resiliencia operativa. Además, fortalece la cultura de seguridad mediante la incorporación de mecanismos automáticos de preservación de evidencia digital. El modelo, en consecuencia, constituye una herramienta de valor para las organizaciones que buscan alcanzar un equilibrio entre viabilidad económica y madurez tecnológica en la gestión de la ciberseguridad.

Problemática identificada en las PYMEs	**Consecuencia para la organización**	**Objetivo del modelo de recuperación autónoma**	**Componente principal involucrado**
Ausencia de capacidades de respuesta automatizada ante incidentes de seguridad (dependencia total de intervención manual).	Aumento del tiempo de indisponibilidad de los servicios críticos y prolongación del impacto del incidente.	Reducir el tiempo medio de recuperación (MTTR) mediante la automatización completa del proceso de restauración de las máquinas virtuales afectadas.	Integración Wazuh – Active Response con script en Python y comandos VBoxManage.
Limitaciones presupuestarias que impiden la adopción de soluciones SOAR comerciales o plataformas de ciberseguridad avanzadas.	Imposibilidad de implementar herramientas corporativas de orquestación y respuesta, manteniendo altos niveles de riesgo residual.	Proponer una solución de bajo costo basada en herramientas de código abierto que pueda ser implementada en infraestructuras modestas típicas de PYMEs.	Uso combinado de Wazuh, Python y Oracle VirtualBox en un entorno de laboratorio replicable.
Falta de procedimientos	Dificultad para reconstruir la causa	Automatizar la generación y	Script de Python encargado de

formales para la recolección y preservación de evidencia digital durante un incidente.	raíz, debilidades en la trazabilidad y posibles problemas de validez probatoria.	almacenamiento de evidencias (dump de memoria, clon de disco, logs y hashes) antes de ejecutar la restauración del sistema.	memory dump, clonación de disco, compresión de logs y cálculo de hashes SHA-256.
Carencia de personal especializado dedicado exclusivamente a ciberseguridad y respuesta ante incidentes.	Dependencia de recursos humanos multitarea, tiempos de reacción irregulares y elevada probabilidad de error humano.	Disminuir la dependencia de la intervención humana durante la fase crítica de respuesta y recuperación, delegando tareas repetitivas en el modelo.	Orquestación automática disparada por reglas de Wazuh (nivel de alerta ≥ umbral definido) que ejecutan el flujo de recuperación sin supervisión constante.
Escasa formalización de planes de continuidad de negocio y recuperación ante desastres en entornos virtualizados.	Recuperaciones ad hoc, sin métricas ni garantías de tiempo, lo que compromete la continuidad operativa ante incidentes severos.	Definir y validar un flujo estructurado de recuperación para entornos virtuales que pueda integrarse como parte de un plan de continuidad de negocio para PYMEs.	Modelo de recuperación autónoma documentado, con métricas de desempeño (MTTR, tiempos por fase) obtenidas en el laboratorio.

Tabla 14. Relación entre problemática de las PYMEs y objetivos del modelo.

Fuente: Elaboración propia.

5.2. Comprensión de los datos

La comprensión de los datos dentro del modelo implica el análisis de las fuentes de información, los flujos de registro y las evidencias generadas durante el proceso de recuperación. A diferencia de proyectos centrados en el análisis de datos convencionales, esta propuesta se orienta a la gestión de eventos de seguridad y a la manipulación de datos forenses derivados de un incidente.

El entorno experimental está conformado por tres máquinas virtuales ejecutadas en Oracle VirtualBox. La primera, denominada wazuh-server, aloja el sistema Wazuh en su arquitectura completa (Manager, Indexer y Dashboard). Este componente constituye el núcleo de detección y correlación, desde el cual se gestionan las reglas de seguridad y se desencadenan las acciones de respuesta activa. La segunda máquina virtual, victima-linux, corresponde a un sistema Debian 12 sobre el cual se simulan incidentes como cifrado de archivos, sobrecarga de procesos o modificaciones no autorizadas en el sistema de archivos. La tercera máquina,

victima-windows, sirve como entorno complementario para futuras pruebas orientadas a evaluar la interoperabilidad del modelo en sistemas híbridos.

La arquitectura del modelo propuesto se organiza en tres capas. En la capa de monitoreo y detección, los agentes de Wazuh desplegados en las máquinas virtuales víctimas reportan eventos al Wazuh Manager, el cual aplica reglas de correlación y activa el módulo de Active Response cuando se detectan incidentes con un nivel de criticidad igual o superior al umbral establecido. En la capa de orquestación y automatización, el módulo de respuesta activa invoca un script desarrollado en Python que ejecuta de forma secuencial las tareas de recolección de evidencias, interacción con la capa de virtualización y generación del reporte del incidente. Finalmente, en la capa de infraestructura virtual y gestión de evidencias, Oracle VirtualBox, mediante VBoxManage, realiza las operaciones de apagado, restauración del snapshot confiable y arranque de la máquina virtual, mientras que el script almacena en un repositorio dedicado los artefactos forenses generados (dump de memoria, clon de disco, logs comprimidos, hashes y reporte en formato Markdown).

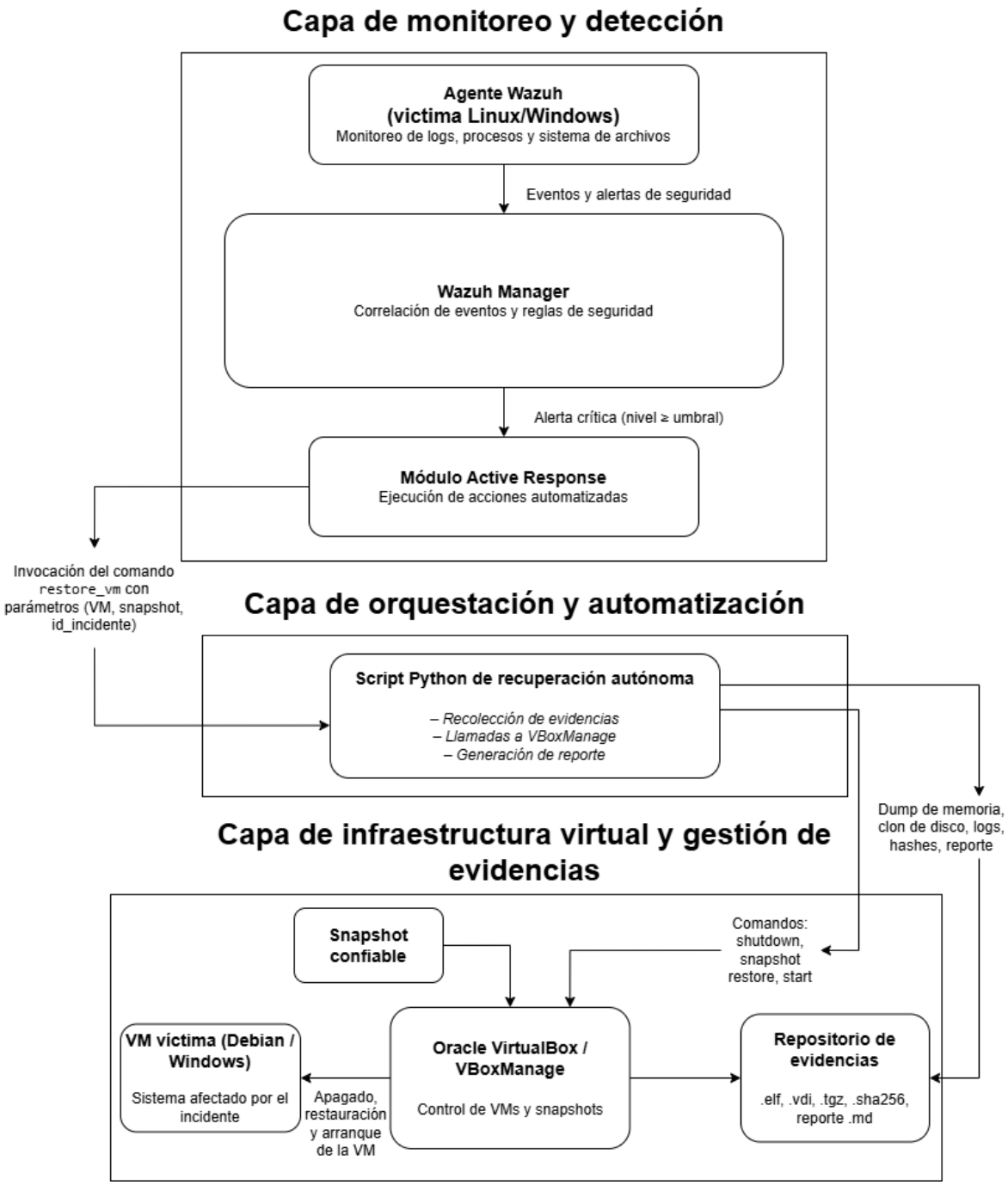

Ilustración 17. Arquitectura general del modelo de recuperación autónoma.

Fuente: Elaboración propia.

Los datos de entrada al sistema se componen de eventos de registro generados por los agentes de Wazuh instalados en cada máquina. Estos agentes recopilan información relacionada con procesos, accesos, integridad de archivos, auditorías de comandos y tráfico de red, que luego son enviados al Wazuh Manager para su

correlación. Cada evento recibe una puntuación de severidad según las reglas definidas, lo que permite priorizar los incidentes y activar respuestas específicas.

Cuando una alerta alcanza el nivel de severidad configurado, Wazuh ejecuta un módulo de Active Response que invoca el script Python encargado de la recuperación. Este script inicia un proceso de recolección de evidencias digitales, cuya finalidad es garantizar la trazabilidad y la posibilidad de análisis posterior. Actualmente, el sistema genera seis tipos de artefactos: un dump de memoria en formato ELF (aproximadamente 4 GB), un archivo hash SHA-256 para validación de integridad, un conjunto de logs del sistema guest comprimidos (11 MB en promedio), un clon del disco virtual de la máquina afectada (alrededor de 10 GB), un reporte Markdown que documenta el proceso completo, y un escaneo post-restauración con ClamScan, cuya implementación se encuentra parcialmente completada.

Cada uno de estos artefactos cumple una función particular dentro del marco forense. El dump de memoria captura el estado volátil del sistema al momento del incidente, permitiendo identificar procesos activos, conexiones abiertas y posibles rastros de malware en ejecución. El hash SHA-256 garantiza la integridad de los archivos recolectados, lo cual es fundamental para mantener la validez probatoria de la evidencia. Los logs del guest documentan la actividad previa al evento y facilitan la reconstrucción de la línea temporal de los hechos. El clon de disco virtual representa una copia completa del entorno afectado, que puede ser analizada en un entorno aislado para determinar la causa raíz del incidente. Finalmente, el reporte Markdown consolida toda la información de la respuesta, mientras que el escaneo ClamScan, una vez finalizado, servirá para confirmar la eliminación de posibles amenazas residuales tras la restauración.

Estos datos, al ser generados de forma automática, permiten que el modelo actúe de manera autónoma y precisa, reduciendo la posibilidad de error humano y garantizando la preservación de evidencia conforme a las mejores prácticas internacionales. Según la documentación de Wazuh (Wazuh, s.f.), el módulo Active Response está diseñado para ejecutar scripts personalizados en función de reglas

predefinidas, lo que convierte a esta herramienta en un elemento ideal para la automatización de la respuesta ante incidentes en entornos de bajo costo.

5.3. Preparación de datos

La fase de preparación comprende todas las actividades necesarias para configurar el entorno de ejecución y establecer las condiciones óptimas que permitan el correcto funcionamiento del modelo. En esta etapa se definen las reglas de detección, las condiciones de ejecución del script, la estructura de almacenamiento de evidencias y las variables de entorno para la gestión de snapshots en VirtualBox.

El primer paso consiste en configurar los agentes de Wazuh instalados en las máquinas virtuales. En el archivo de configuración ossec.conf se definen los directorios y archivos que serán monitoreados, especificando el formato de los logs y los niveles de severidad. En el caso de la máquina victima-linux, se habilita el monitoreo de rutas críticas como por ejemplo /etc, /home, /var/log y /tmp, con el fin de detectar modificaciones inusuales o la creación de archivos cifrados. Esta configuración se complementa con reglas locales personalizadas en el archivo local_rules.xml, en las cuales se establecen condiciones específicas de detección para procesos sospechosos, cambios masivos de extensión o ejecución de comandos no autorizados.

Posteriormente, se define la acción de respuesta activa en la configuración del Wazuh Manager. En esta sección se especifica el comando a ejecutar, los parámetros necesarios y el nivel de alerta requerido. Cuando una alerta cumple las condiciones configuradas, Wazuh invoca el comando de respuesta activa asociado al script de recuperación, el cual recibe como argumentos el nombre de la máquina virtual afectada, el snapshot que debe restaurarse y un identificador único del incidente.

En paralelo, se realiza la preparación del entorno de VirtualBox. Cada máquina virtual dispone de un snapshot confiable, el cual representa un estado limpio y funcional del sistema. Este snapshot es el punto de restauración al que se retorna automáticamente cuando se detecta un incidente crítico. La herramienta de línea de comandos VBoxManage es el componente que permite la ejecución de acciones

como apagado de la máquina (VBoxManage controlvm poweroff), restauración de snapshot (VBoxManage snapshot restore), y reinicio (VBoxManage startvm --type gui). De acuerdo con la documentación de Oracle (Oracle, s.f.), estos comandos pueden integrarse en scripts externos, posibilitando la automatización de procesos de recuperación sin necesidad de intervención manual. El almacenamiento de las evidencias generadas por el script sigue una estructura jerárquica que utiliza el nombre de la máquina afectada como variable de nomenclatura. Por ejemplo, una ejecución del script sobre la máquina victima-linux generará un directorio con el nombre esta máquina, dentro del cual se almacenarán los archivos .elf, .sha256, .tgz, .vdi y .md. Esta práctica permite una trazabilidad ordenada y facilita la consulta posterior durante auditorías o investigaciones forenses.

Fase del flujo de recuperación	**Descripción de la actividad**	**Evidencia generada**	**Tipo de archivo**	**Propósito forense u operativo**
Captura de memoria de la VM víctima	Se ejecuta un volcado completo de la memoria RAM de la máquina virtual afectada antes de cualquier acción de restauración.	Dump de memoria	.elf	Conservar el estado volátil del sistema (procesos, conexiones, claves en memoria) para análisis posterior del incidente.
Cálculo de hash de la memoria	Se calcula el hash criptográfico del archivo de dump de memoria inmediatamente después de su creación.	Hash SHA-256 del dump de memoria	.sha256	Garantizar la integridad del volcado de memoria y permitir la verificación de que no ha sido

				alterado durante el análisis.
Recolección y compresión de logs del sistema invitado	Se recopilan los archivos de registro relevantes dentro de la VM víctima (sistema, aplicaciones, seguridad) y se comprimen en un único paquete.	Paquete de logs del guest	.tgz	Consolidar la trazabilidad de eventos previos al incidente y facilitar la reconstrucción de la línea de tiempo de los hechos.
Clonación del disco de la VM víctima	Se realiza una copia completa del disco virtual asociado a la máquina afectada antes de restaurar el snapshot.	Clon de disco de la VM	.vdi (copia)	Preservar una imagen completa del sistema comprometido para análisis forense detallado sin afectar el entorno de producción.
Cálculo de hash del clon de disco	Se calcula el hash criptográfico del archivo de clon de disco una vez finalizada la clonación.	Hash SHA-256 del clon de disco	.sha256	Asegurar la integridad de la imagen de disco utilizada en el análisis forense y documentar su autenticidad.
	Se detiene la máquina virtual afectada			Evitar daños adicionales en el sistema,

Apagado controlado de la VM víctima	mediante comandos de apagado controlado antes de aplicar el snapshot.	Registro de apagado en logs y reporte	(incluido en .md y logs)	garantizar un cierre limpio y documentar el momento exacto del inicio de la recuperación.
Restauración del snapshot confiable	Se aplica el snapshot previamente definido como estado limpio sobre la VM afectada.	Evento de restauración del snapshot	(registrado en reporte .md y en logs de VirtualBox)	Devolver el sistema a un estado estable previo al incidente, minimizando el tiempo de indisponibilidad.
Arranque y verificación de disponibilidad	Se inicia la máquina restaurada y se verifica su estado mediante comandos de guestcontrol u otros mecanismos de validación.	Confirmación de disponibilidad de la VM	(registrada en reporte .md)	Comprobar que el servicio ha sido efectivamente restablecido y que la instancia restaurada se encuentra operativa.
Generación del reporte consolidado del incidente	Se elabora un informe automatizado que resume todas las tareas ejecutadas, tiempos, rutas y hashes generados.	Reporte de incidente y recuperación	.md	Documentar de forma estructurada el incidente, las acciones de respuesta y los artefactos generados, sirviendo como insumo para auditoría y

				lecciones aprendidas.
Escaneo post-restauración (en desarrollo)	Se ejecuta un análisis antivirus sobre la máquina restaurada para detectar posibles remanentes de malware o archivos sospechosos.	Registro de resultados del escaneo	(referencia en reporte .md, salida de ClamScan)	Complementar la restauración con una verificación adicional de seguridad que confirme la limpieza del entorno recuperado.

Tabla 15. Fases del flujo de recuperación y evidencias generadas por el modelo.

Fuente: Elaboración propia.

Cada archivo recolectado es verificado mediante su hash SHA-256, el cual se registra tanto en el reporte Markdown como en los logs del sistema. Esto asegura que los datos no hayan sido alterados durante el proceso de copia o transferencia. Asimismo, el script emplea control de excepciones para registrar cualquier fallo en la ejecución y mantener la consistencia de las operaciones.

Finalmente, se implementa un reporte automatizado en formato Markdown que detalla el resultado de cada fase. Este documento incluye la lista de tareas ejecutadas, los tiempos de ejecución, el tamaño de las evidencias y los hashes generados. El reporte se convierte en el artefacto final de la respuesta, proporcionando una visión clara y verificable del proceso de recuperación.

5.4. Modelado

El diseño del modelo de recuperación autónoma se basa en la integración coordinada de tres componentes: detección (Wazuh), automatización (Python) y virtualización (VirtualBox). La interacción entre estos elementos forma un flujo de trabajo que garantiza la detección oportuna de incidentes y la recuperación automática de las máquinas virtuales afectadas.

La arquitectura lógica del modelo se estructura en tres fases: detección, decisión y acción. En la fase de detección, los agentes de Wazuh recogen y envían los registros de actividad al Manager, el cual analiza la información en tiempo real y genera alertas cuando identifica patrones de comportamiento anómalos. La correlación de eventos se apoya en reglas personalizadas que incrementan la precisión en la identificación de incidentes relevantes para el entorno pyme.

En la fase de decisión, el Wazuh Manager evalúa la severidad de la alerta y determina si se cumplen las condiciones establecidas para ejecutar una respuesta activa. Si la alerta alcanza un nivel de criticidad igual o superior al umbral predefinido, se activa el módulo Active Response, que ejecuta el comando asociado al script Python. Según Wazuh (Wazuh, s.f.), este módulo puede ser configurado para ejecutar scripts tanto en el agente afectado como en el servidor central, lo cual ofrece flexibilidad y control sobre el punto de ejecución.

La fase de acción corresponde a la ejecución del script Python, que constituye el núcleo operativo del modelo. Este script realiza de manera automática una serie de tareas secuenciales diseñadas para preservar la evidencia, restaurar la máquina virtual y registrar el resultado del proceso. En primer lugar, captura un dump de memoria del sistema afectado, el cual se guarda en formato ELF. Posteriormente, genera un hash SHA-256 de los archivos recolectados, comprime los logs del guest en un archivo .tgz y realiza un clon completo del disco virtual en formato .vdi y genera un hash SHA-256 de dicho clon. Una vez finalizada la recolección de evidencias, el script ejecuta el comando de restauración de snapshot, devolviendo la máquina a su estado seguro previo al incidente. Finalmente, genera un reporte Markdown que resume toda la operación, incluyendo los hashes generados y el estado final de cada tarea.

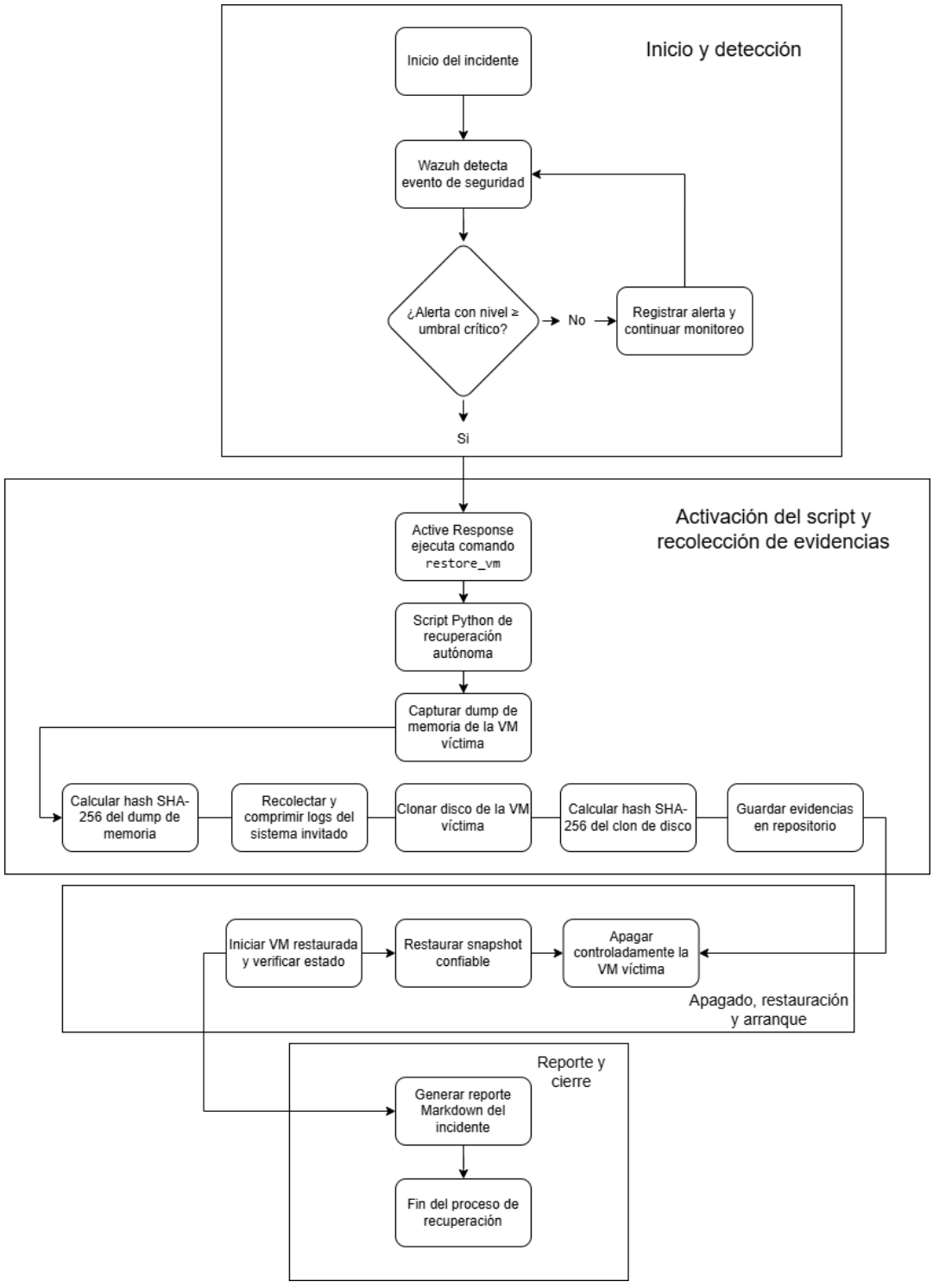

Ilustración 18. Diagrama de flujo del proceso de recuperación autónoma.

Fuente: Elaboración propia.

El diagrama ilustra la secuencia de actividades que conforman el modelo de recuperación autónoma. A partir de la detección de un evento de seguridad por parte de Wazuh y la evaluación de su nivel de criticidad, el módulo de Active Response invoca un script desarrollado en Python que ejecuta la recolección sistemática de evidencias (volcado de memoria, clon de disco, logs y hashes), seguido de las acciones de apagado de la máquina virtual comprometida, restauración del snapshot confiable y arranque de la instancia recuperada. Finalmente, se genera un reporte consolidado del incidente que documenta las tareas realizadas y las rutas de las evidencias almacenadas.

La secuencia del proceso garantiza que el sistema logre un equilibrio entre automatización y trazabilidad. Ninguna acción de restauración se realiza sin antes haber asegurado la captura completa de evidencias, lo que preserva la integridad del análisis forense. Esta metodología cumple con los principios recomendados por (MICITT, 2023) para la preservación y documentación de la evidencia digital.

El modelo, además, incluye un componente de verificación post-restauración mediante la herramienta ClamScan, cuyo objetivo es analizar el sistema restaurado en busca de remanentes de malware o alteraciones persistentes. Aunque esta funcionalidad se encuentra parcialmente implementada, su inclusión en la arquitectura general del modelo refuerza el concepto de restauración segura y controlada.

5.5. Evaluación

La evaluación del modelo propuesto se basa en indicadores de rendimiento y confiabilidad orientados a medir su efectividad en entornos simulados de pyme. Los principales indicadores empleados son el tiempo medio de detección (MTTD), el tiempo medio de recuperación (MTTR), la tasa de automatización exitosa, la integridad de las evidencias y la disponibilidad general del sistema.

Durante las pruebas de laboratorio, se llevaron a cabo simulaciones de incidentes de seguridad en la máquina victima-linux, incluyendo un ataque de tipo ransomware. Para este caso, Wazuh detectó la anomalía en cuestión de segundos y generó una alerta crítica que activó el proceso de respuesta. La ejecución automática del script

permitió que la restauración de la máquina virtual se completara en un tiempo promedio de menos de cinco minutos, dependiendo del tamaño del disco y de la cantidad de datos involucrados en el clon.

En cuanto a la generación de evidencias, el modelo demostró una tasa de éxito del 100% en la producción de los artefactos esperados. Cada ejecución del script generó correctamente el dump de memoria, el archivo hash SHA-256, los logs comprimidos, el clon de disco y el reporte Markdown. Las validaciones posteriores confirmaron la integridad de los archivos mediante verificación de hashes, lo que demuestra la consistencia del proceso de preservación.

El análisis del rendimiento evidenció que la automatización del proceso reduce significativamente el tiempo de respuesta en comparación con la restauración manual. En escenarios tradicionales, la recuperación de un sistema virtual puede requerir tiempos prolongados, dependiendo del operador y del tamaño de la máquina. En contraste, el modelo propuesto logró reducir este tiempo, situando el MTTR dentro de márgenes aceptables para la continuidad del negocio en pymes.

Asimismo, el modelo fue evaluado en términos de resiliencia y estabilidad. Las pruebas prolongadas confirmaron que el sistema mantiene su funcionalidad tras múltiples ejecuciones consecutivas, sin degradación en el rendimiento ni errores en los procesos de restauración. Este comportamiento respalda la viabilidad de la solución en entornos productivos de pequeña escala.

La evaluación del modelo de recuperación autónoma se centra en la medición de indicadores de desempeño directamente vinculados con la continuidad operativa y la preservación de evidencias. En el entorno de laboratorio se ejecutaron veinte pruebas controladas bajo el mismo escenario de incidente, registrando tiempos por fase y tiempos globales del flujo de recuperación. A partir de estas mediciones se calcularon valores promedio y rangos, con el fin de caracterizar el comportamiento del modelo en términos de rapidez, estabilidad y completitud de las tareas críticas.

En la Tabla 16 se sintetizan los principales indicadores obtenidos durante el proceso de evaluación, incluyendo el tiempo medio de recuperación (MTTR), el tiempo total

del flujo de trabajo, la tasa de éxito en la generación de evidencias y el rango observado entre la ejecución más rápida y la más lenta.

Indicador	Descripción	Valor obtenido en laboratorio	Observación
Número de ejecuciones evaluadas	Cantidad de corridas completas del modelo bajo el mismo escenario de incidente.	20 ejecuciones	Permite obtener promedios y observar la estabilidad del comportamiento del modelo.
MTTR aproximado (time_to_restore_s promedio)	Tiempo desde la activación del flujo de recuperación hasta que la máquina virtual se encuentra nuevamente disponible para su uso.	≈ 3:58 min	Representa el tiempo medio de recuperación percibido por el servicio. Se mantiene por debajo de 4 minutos en todas las ejecuciones.
Tiempo total del flujo (workflow_total_s promedio)	Duración completa del flujo de trabajo, incluyendo recolección de evidencias, restauración, arranque y generación del reporte.	≈ 4:17 min	El flujo completo se mantiene por debajo de 5 minutos, lo que resulta adecuado para entornos pyme.
Rango de MTTR (mínimo – máximo)	Diferencia entre la ejecución más rápida y la más lenta en términos de time_to_restore_s.	3:24 min – 4:26 min	La variación se mantiene dentro de un rango cercano a 1 minuto, evidenciando estabilidad y ausencia de valores extremos.
	Diferencia entre la ejecución con menor y		Las oscilaciones responden a variaciones normales del entorno de

Rango de tiempo total del flujo (workflow_total_s)	mayor valor de workflow_total_s.	3:55 min – 4:45 min	virtualización y no alteran el orden de magnitud del tiempo total.
Tasa de ejecuciones exitosas	Porcentaje de ejecuciones en las que el flujo se completó sin errores críticos.	100 % (20/20)	En todas las ejecuciones se alcanzó el final del flujo, con restauración exitosa de la VM y generación del reporte.
Tasa de generación completa de evidencias	Porcentaje de ejecuciones en las que se generaron correctamente dump de memoria, clon de disco, logs y hashes asociados.	100 % (20/20)	En todas las corridas se obtuvieron los artefactos previstos (.elf, .tgz, .vdi, .sha256, .md), lo que garantiza trazabilidad.
Proporción del tiempo dedicada a clonación de disco y hash	Fracción aproximada del tiempo total de flujo consumida por disk_clone_total_s y disk_clone_hash_total_s.	≈ 21 % del tiempo total	La mayor carga temporal recae en la gestión de evidencias de disco, sin comprometer el MTTR de restauración.

Tabla 16. Resumen de indicadores de desempeño del modelo de recuperación autónoma.

Fuente: Elaboración propia.

5.6. Conclusiones parciales del capítulo

El desarrollo del modelo de recuperación autónoma demuestra que es posible implementar un sistema eficaz de detección, respuesta y recuperación automatizada utilizando únicamente herramientas de código abierto. La integración de Wazuh, Python y VirtualBox constituye una solución técnica accesible y escalable, adecuada para las necesidades y limitaciones de las pymes.

El modelo permite reducir los tiempos de inactividad provocados por incidentes de seguridad, garantizando al mismo tiempo la preservación de evidencia digital y la trazabilidad completa del proceso. La autonomía operativa alcanzada mediante la automatización contribuye a fortalecer la resiliencia organizacional y a minimizar la dependencia de personal especializado.

Si bien la propuesta cumple su propósito de restaurar entornos virtuales comprometidos de forma rápida y segura, aún existen áreas de mejora que podrían potenciar su funcionalidad. Entre ellas destacan la finalización del escaneo post-restauración con ClamScan, la integración de sistemas de notificación en tiempo real mediante correo electrónico o mensajería instantánea, y la ampliación del sistema de correlación mediante algoritmos de aprendizaje automático. Estas mejoras permitirían evolucionar el modelo hacia una arquitectura más cercana a un sistema de orquestación de seguridad completo, adaptado al contexto de las pymes.

En síntesis, la propuesta representa un avance significativo en la búsqueda de soluciones de recuperación automatizada asequibles. La experiencia obtenida en su desarrollo evidencia que la combinación de herramientas de código abierto puede ofrecer resultados de alto nivel, contribuyendo a la consolidación de una cultura de resiliencia digital en organizaciones con recursos limitados.

6. Capítulo 6. Conclusiones

La evidencia recolectada para esta investigación confirma que las PYMEs son el sector comercial más vulnerables a ciberataques, esto debido a la gran limitante de recursos económicos y personal técnico, es por esto por lo que frente a la cantidad de soluciones que alertan pero no restauran, se priorizó en la recuperación de los sistemas de una manera autónoma siguiendo un flujo orientado a reducir los RTO al detectar, responder y restaurar sin la necesidad de la intervención humana. Este énfasis en la continuidad operativa del negocio es lo que diferencia a este modelo.

La arquitectura planteada durante el desarrollo de este proyecto, la cual se basa en herramientas de código abierto, es real, de bajo costo y replicable en entornos sencillos, lo que la hace fácil de implementar para las pequeñas y medianas empresas.

Se definen roles y límites para cada componente donde Wazuh es el encargado de detectar la amenaza y ejecuta la respuesta activa, el script de Python decide y orquesta las acciones y VirtualBox, por medio de VBoxManage restaura y pone en servicio los sistemas.

En esta fase del trabajo se construyó un laboratorio controlado en el cual se ejecutaron diferentes escenarios de incidente, permitiendo recolectar métricas de desempeño del modelo. Estas métricas fueron analizadas para obtener valores precisos sobre los tiempos de recuperación y el comportamiento del flujo automatizado, proporcionando una primera aproximación cuantitativa al impacto del modelo en la continuidad del negocio. En trabajos futuros se recomienda ampliar el conjunto de escenarios evaluados y extender las pruebas a otras configuraciones de infraestructura, con el fin de reforzar la evidencia empírica y explorar su comportamiento en contextos más cercanos a entornos productivos reales.

De esta manera, se deja bien fundamentada una propuesta innovadora, viable y alineada con las necesidades de las PYMEs, un modelo de recuperación autónoma que integra detección, orquestación y recuperación automática utilizando herramientas de código abierto. Las pruebas realizadas en entornos controlados respaldan el potencial de este modelo para contribuir a la reducción de los tiempos de recuperación y al fortalecimiento de la ciber resiliencia de las pequeñas y medianas empresas, al tiempo que establecen una base sólida para futuras fases de validación y despliegue en contextos reales.

Con el objetivo de facilitar la replicabilidad del modelo propuesto y promover la investigación académica en el área de la ciber resiliencia en entornos virtualizados, el código correspondiente al script de orquestación utilizado en este trabajo ha sido publicado en un repositorio abierto. Este recurso permite a otros investigadores y profesionales analizar, reproducir y extender el enfoque presentado en esta investigación. El repositorio puede consultarse en: https://zenodo.org/records/18820905

7. Capítulo 7. Bibliografía

Asamblea Legislativa. (27 de mayo de 2002). *Sistema Costarricense de Información Jurídica*. Obtenido de Ley N°8262 Fortalecimiento de las Pequeñas y Medianas Empresas: https://pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=48533

Awati, R., & Wigmore, I. (7 de junio de 2024). *TechTarget*. Obtenido de What is a log file?: https://www.techtarget.com/whatis/definition/log-log-file

Brenes, K. C. (enero de 2021). *ResearchGate*. Obtenido de EL SURGIMIENTO DE LAS PYMES EN COSTA RICA DESDE UNA PERSPECTIVA HISTÓRICO-ECONÓMICA (1950-2018): https://www.researchgate.net/publication/348655167_EL_SURGIMIENTO_DE_LAS_PYMES_EN_COSTA_RICA_DESDE_UNA_PERSPECTIVA_HISTORICO-ECONOMICA_1950-2018

Bunce, C. (12 de mayo de 2022). *Bizagi*. Obtenido de Automatización y orquestación: ¿cuál es la diferencia y cómo benefician ambas a su organización?: https://www.bizagi.com/es/contents/Blog/ES/automatizacion-vs-orquestacion.html#:~:text=La%20palabra%20%22orquestaci%C3%B3n%22%20tiene%20su,plataforma%20para%20optimizar%20las%20operaciones.

CAF. (2023). *Banco de Desarrollo de América Latina y el Caribe*. Obtenido de Serie las PYMES en América Latina y el Caribe: https://scioteca.caf.com/bitstream/handle/123456789/2132/CAF_PYMES_COSTARICA.pdf

Casas, A. (24 de enero de 2024). *Camara de Industrias de Costa Rica*. Obtenido de Ciberseguridad en Empresas Costarricenses: Más allá de la Tecnología: https://cicr.com/noticias_pt/ciberseguridad-en-empresas-costarricenses-mas-alla-de-la-tecnologia/

Cross, K. (9 de setiembre de 2024). *CrowdStrike*. Obtenido de Anomaly Detection in Cybersecurity: https://www.crowdstrike.com/en-us/cybersecurity-101/next-gen-siem/anomaly-detection

Finn, T., & Downie, A. (7 de mayo de 2024). *IBM*. Obtenido de ¿Qué es la mitigación de riesgos?: https://www.ibm.com/mx-es/topics/risk-mitigation

Gibadullin, R., & Nikonorov, V. (2021). Development of the System for Automated Incident Management Based on Open-Source Software. *International Russian Automation Conference (RusAutoCon)*, (págs. 521-525). Sochi, Russian.

Hadi, H. J. (2024). Cost-Effective Resilience: A Comprehensive Survey and Tutorial on Assessing Open-Source Cybersecurity Tools for Multi-Tiered Defense. *IEEE Explore*, 24.

Haydar, A., & Ramparison, M. (2024). Modeling Wazuh rules with Weighted Timed Automata. *Procedia Computer Science*, 75-82.

IBM. (20 de enero de 2022). *IBM*. Obtenido de What is cyber resilience?: https://www.ibm.com/think/topics/cyber-resilience

IBM. (s.f.). *IBM*. Obtenido de ¿Qué es el monitoreo de red?: https://www.ibm.com/mx-es/topics/network-monitoring

IBM. (s.f.). *IBM*. Obtenido de What is anomaly detection?: https://www.ibm.com/think/topics/anomaly-detection

Imán, F. (12 de marzo de 2019). *Infosec*. Obtenido de Security Orchestration, Automation and Response (SOAR): https://www.infosecinstitute.com/resources/incident-response-resources/security-orchestration-automation-and-response-soar

Islam, M. R., & Rafique, R. (2024). Wazuh SIEM for Cyber Security and Threat Mitigation in Apparel Industries. *International Journal of Engineering Materials and Manufacture (IJEMM)*, 136-144.

Mellas, R. (26 de setiembre de 2024). *Lexlatin*. Obtenido de Ciberseguridad: Las pymes en Costa Rica están bajo constantes ataques: https://lexlatin.com/entrevistas/ciberseguridad-pymes-costa-rica-ataques

MICITT. (Octubre de 2023). *Guia de Acción Ante Incidentes de Ransomware.* Obtenido de https://www.micitt.go.cr/sites/default/files/2023-12/Playbook%20Ransomware.pdf

Microsoft. (2025). *Microsoft*. Obtenido de Seguridad de Microsoft ¿Que es un SIEM?: https://www.microsoft.com/es-es/security/business/security-101/what-is-siem

Microsoft. (2025). *Microsoft*. Obtenido de ¿Qué es SOAR?: https://www.microsoft.com/es-es/security/business/security-101/what-is-soar

Mora Vargas, A. I. (2024). Guía para elaborar una propuesta de investigación. *Revista Educación Universidad de Costa Rica*, 92.

Naranjo Zeledón, L. C. (2020). Investigación en Informática: el enfoque alternativo. *Technology Inside by CPIC*.

National Institute of Standards and Technology. (s.f.). *CSRC glossary*. Obtenido de Mitigation: https://csrc.nist.gov/glossary/term/mitigation

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). *NIST Special Publication 800.* Gaithersburg, MD: U.S. Department of Commerce. Obtenido de Incident Response Recommendations .

Oracle. (s.f.). *Snapshots*. Obtenido de Oracle® VM VirtualBoxUser Manual for Release 6.0: https://docs.oracle.com/en/virtualization/virtualbox/6.0/user/snapshots.html

Oracle. (s.f.). *VBoxManage*. Obtenido de Oracle® VM VirtualBoxUser Manual for Release 6.0: https://docs.oracle.com/en/virtualization/virtualbox/6.0/user/vboxmanage-intro.html

Revista Summa. (28 de febrero de 2023). *Revista Summa*. Obtenido de ¿En qué emprenden los costarricenses ? Estos son los sectores más elegidos: https://revistasumma.com/en-que-emprenden-los-costarricenses-estos-son-los-sectores-mas-elegidos

Robert A. Bridges, A. E. (2023). Testing SOAR tools in use. *Computers & Security*.

Sadlek, L., Yamin, M. M., Čeleda, P., & Katt, B. (2025). Severity-based triage of cybersecurity incidents using kill chain attack graphs. *Journal of Information Security and Applications*.

SentinelOne. (14 de abril de 2025). *SentinelOne*. Obtenido de Cyber Security Incident Response: Definition & Best Practices: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-incident-response/

UIIM. (20 de junio de 2024). *¿Quién inventó las PYMEs?* Obtenido de Universidad de Investigación e Innovación de Mexico: https://uiix.edu.mx/quien-invento-las-pymes/

Unidad de riesgos y Seguridad. (20 de setiembre de 2022). *Universidad de Costa Rica*. Obtenido de Gestión de incidentes de seguridad: https://ci.ucr.ac.cr/gestion-incidentes-seguridad

Wazuh. (s.f.). *Active Response*. Obtenido de User Manual: https://documentation.wazuh.com/current/user-manual/capabilities/active-response/index.html

Wazuh. (s.f.). *Rules Sintax*. Obtenido de User Manual: https://documentation.wazuh.com/current/user-manual/ruleset/ruleset-xml-syntax/rules.html