Sistema de Alerta Temprana en Seguridad Informática mediante Honeypots Virtualizados en Redes Empresariales

Early Warning System for IT Security Using Virtualized Honeypots in Corporate Networks

Autor: Oscar Javier Abuawad Lorite

Universidad para el Desarrollo y la Innovación (UDI), Bolivia

Cómo citar este artículo:

American Psychological Association, 7.ª edición (APA 7):

Abuawad Lorite, O.J. (2025). Sistema de alerta temprana en seguridad informática mediante honeypots virtualizados en redes empresariales. *Boletín Científico Fronteras Tecnológicas*, *1*(1), 172-197.

Institute of Electrical and Electronics Engineers (IEEE):

O.J. Abuawad Lorite, "Sistema de alerta temprana en seguridad informática mediante honeypots virtualizados en redes empresariales", *Boletín Científico Fronteras Tecnológicas*, vol. 1, no. 1, 172-197, 2025. [En línea].

RESUMEN

El estudio aborda la problemática de la detección tardía de incidentes de seguridad informática en la infraestructura de red de Lavaseco Universal LTDA., donde el tiempo de respuesta superaba las 12 horas. Con el propósito de reducir este lapso, se diseñó e implementó una solución de alerta temprana basada en honeypots virtualizados, bajo un enfoque preexperimental antes-después. La investigación se desarrolló entre agosto de 2022 y marzo de 2024, abarcando diagnóstico, diseño, implementación y validación. Para la evaluación se registraron 17 incidentes en distintas sucursales, contrastados mediante la prueba t de Welch. Los resultados evidencian una reducción significativa del tiempo medio de detección, pasando de más de 12 horas a un promedio de 4,4 horas. Además, la solución permitió recopilar información relevante sobre tácticas y técnicas de los atacantes, fortaleciendo la capacidad de respuesta y la gestión de la seguridad informática. Entre las principales fortalezas de la propuesta destacan su carácter modular, escalable y de bajo costo al estar basada en tecnologías open source, lo que la hace viable para pequeñas y medianas empresas. Si bien se identificaron limitaciones relacionadas con la ausencia de grupo control y la dependencia de un único responsable de TI, los hallazgos demuestran la efectividad de los honeypots virtualizados como herramienta de detección temprana. Se recomienda su implementación en otras organizaciones y la creación de equipos multidisciplinarios que aseguren la sostenibilidad de la estrategia.

Palabras clave: seguridad informática, honeypots virtualizados, detección temprana de incidentes, ciberseguridad, pequeñas y medianas empresas (PYMES).

ABSTRACT

This study addresses the problem of delayed detection of cybersecurity incidents in the network infrastructure of Lavaseco Universal LTDA., where response times exceeded 12 hours. To reduce this gap, an early-warning solution based on virtualized Honeypots was designed and implemented using a pre-experimental before-after approach. The research was conducted between August 2022 and March 2024, covering diagnosis, design, implementation, and validation. Seventeen incidents recorded across different branches were analyzed using Welch's t-test. Results show a significant reduction in mean detection time, from over 12 hours to an average of 4.4 hours. The solution also enabled the collection of valuable information on attackers' tactics and techniques, strengthening incident response and security management. Key strengths include its modular, scalable, and low-cost nature, as it relies on open source technologies, making it suitable for small and medium-sized enterprises. Although limitations were identified—such as the absence of a control group and reliance on a single IT administrator—the findings demonstrate the effectiveness of virtualized Honeypots as an early detection tool. Broader adoption in other organizations and the establishment of multidisciplinary teams are recommended to ensure sustainability of the strategy.

Keywords: information security, virtualized honeypots, early incident detection, cybersecurity, small and medium-sized enterprises (SMEs).

INTRODUCCIÓN

La presente investigación aborda la necesidad de reducir el tiempo de detección de incidentes de seguridad informática en la infraestructura de red de Lavaseco Universal LTDA. El estudio se desarrolló entre agosto de 2022 y marzo de 2024, abarcando las etapas de diagnóstico, implementación de un sistema honeypot y evaluación de su efectividad.

El diagnóstico inicial permitió identificar múltiples factores que contribuyen a los incidentes de seguridad, entre ellos: evaluaciones de seguridad insuficientes, ausencia de políticas claras para el manejo de datos, falta de clasificación de la información según su nivel de confidencialidad, medidas inadecuadas de protección, tiempos de detección prolongados (superiores a 12 horas), deficiencias en la documentación y control de incidentes, así como carencias en la capacitación del personal y los controles de acceso.

Estos hallazgos evidencian una situación existente en organizaciones que no disponen de estrategias preventivas consolidadas, ni de mecanismos de respuesta eficientes frente a incidentes de seguridad. Esta carencia incrementa la exposición a riesgos cibernéticos y limita la capacidad institucional para contener sus efectos. En este contexto, la investigación se desarrolla en un entorno donde los incidentes de seguridad representan una amenaza creciente para la estabilidad operativa, la continuidad de los servicios y la confianza empresarial.

La problemática identificada en el diagnóstico guarda correspondencia con las tendencias observadas a nivel internacional, donde las brechas de seguridad continúan generando impactos económicos y operativos significativos. De acuerdo con el *Cost of a Data Breach Report de IBM*, en el 2024 el costo promedio global de una violación de datos alcanzó los 4,88 millones de dólares, lo que representó un incremento del 10 % respecto al año anterior (IBM Security, 2024). El uso de

inteligencia artificial y automatización en los centros de operaciones de seguridad ha demostrado reducir significativamente los tiempos de detección y contención de brechas, disminuyendo así los costos asociados (IBM Security, 2024).

A partir de este panorama, resulta necesario revisar las investigaciones previas que sustentan las estrategias de detección temprana de incidentes. En la literatura especializada, los honeypots han sido considerados como herramientas eficaces que permiten observar comportamientos de atacantes y recopilar información útil para fortalecer la seguridad perimetral. Chapoñan (2021) destaca que los honeypots de baja interacción permiten obtener información sobre los intrusos con un riesgo reducido. Por su parte, Acosta (2022) resalta su utilidad en el reforzamiento de la seguridad perimetral de las PYMES, al constituir una medida preventiva frente a ciberataques.

Los aportes de estudios anteriores, entre ellos los aquí referidos, respaldan el enfoque adoptado en la presente investigación, orientada al diseño e implementación de una solución de alerta temprana basada en honeypots virtualizados. La elección de este enfoque se fundamenta en su capacidad para integrar técnicas de monitoreo proactivo con herramientas de análisis que permiten reducir los tiempos de detección y respuesta ante incidentes.

La relevancia del estudio radica en el contexto actual de la computación y las telecomunicaciones, donde la creciente dependencia de la información digital exige mecanismos avanzados de protección. La aplicación de tecnologías de código abierto y soluciones escalables contribuyen a mejorar la seguridad de las redes empresariales, y promover una cultura de ciberseguridad accesible y sostenible.

Desde una perspectiva práctica, esta investigación busca fortalecer la protección de los activos de información, garantizar la continuidad del negocio y mantener la confianza de los clientes y socios. Además, tiene un impacto social al poner a disposición de otras organizaciones y la comunidad de software libre una solución escalable y modular que puede adaptarse a diversos entornos tecnológicos. Desde el punto de vista económico, ofrece una alternativa de bajo costo basada en tecnologías open source, lo que facilita su adopción por parte de distintas entidades. En el ámbito académico, el trabajo contribuye a la comprensión de amenazas cibernéticas y al desarrollo de estrategias efectivas para su mitigación.

La solución propuesta pretende ser accesible, adaptable y aplicable a las necesidades de distintas organizaciones, lo que facilita su implementación en diversos contextos tecnológicos. La investigación profundiza en la comprensión de las amenazas cibernéticas, contribuye al desarrollo de mejores prácticas en seguridad informática, y fortalece la gestión preventiva y resiliencia digital de las instituciones.

Se busca que la solución propuesta permita:

- Disminuir el tiempo de detección de incidentes de seguridad.
- Mejorar los niveles de seguridad.
- Proteger los activos de información.
- Garantizar la continuidad del negocio.
- Mantener la confianza de los clientes y socios.

El objetivo principal de la investigación fue reducir el tiempo de detección de incidentes de seguridad informática en la infraestructura de red de Lavaseco Universal LTDA., mediante el diseño e implementación de una solución de alerta temprana basada en honeypots virtualizados.

En este sentido, la incorporación de honeypots virtualizados brinda un medio técnico eficaz para registrar y analizar actividades maliciosas en entornos reales, favoreciendo la mejora continua de los mecanismos de vigilancia y la consolidación de una gestión de seguridad más proactiva dentro de la organización.

METODOLOGÍA

La investigación adoptó un diseño preexperimental de un solo grupo, seleccionado por su adecuación a las condiciones operativas de Lavaseco Universal LTDA., donde la interrupción de los procesos normales o la conformación de un grupo control no resultaban factibles. Según Hernández-Sampieri (2014), este tipo de diseño es apropiado cuando no es posible ejercer un control total sobre las variables del entorno, pero se requiere obtener una primera aproximación empírica a la relación causa-efecto entre las variables de estudio. En este caso, el diseño preexperimental permitió evaluar de manera práctica el impacto de la implementación de honeypots virtualizados sobre el tiempo de detección de incidentes de seguridad informática, en condiciones reales de operación.

El estudio comprendió un análisis inicial del estado de la seguridad informática en la infraestructura de red de la empresa y la posterior implementación de una solución de alerta temprana basada en honeypots virtualizados, concebida bajo un enfoque de sistemas. Con un alcance explicativo, se aplicó una prueba de hipótesis orientada a establecer la relación causa-efecto entre la implementación de los honeypots y la reducción del tiempo de detección de incidentes de seguridad.

La población de estudio estuvo conformada por el personal del área de Tecnologías de la Información (TI) y la gerencia de Lavaseco Universal LTDA., quienes intervienen directamente

en la gestión y toma de decisiones sobre la seguridad informática de la empresa. Dado el tamaño reducido de la organización, la muestra coincidió plenamente con la población, la cual estuvo integrada por un miembro del área de TI y dos representantes de la gerencia.

En la fase de validación de la solución de seguridad informática, las unidades de análisis estuvieron constituidas por los incidentes de seguridad registrados en la infraestructura de red de Lavaseco Universal LTDA. Se recopilaron 17 incidentes ocurridos en diferentes sucursales, antes y después de la implementación de la solución propuesta. Estos datos permitieron comparar los tiempos de detección de eventos y evaluar el impacto de los honeypots virtualizados en la mejora de la seguridad informática de la organización.

Durante el proceso de investigación, se desarrollaron etapas secuenciales, diseñadas para asegurar la coherencia del proceso y la replicabilidad de los resultados. Estas etapas comprenden el diagnóstico, la propuesta de solución, la validación, el análisis e interpretación de resultados y la formulación de conclusiones y recomendaciones.

1. Diagnóstico

En la primera etapa de la investigación se llevó a cabo un análisis integral del estado de la seguridad informática en la infraestructura de red de Lavaseco Universal LTDA., con el propósito de identificar vulnerabilidades en los mecanismos de protección y gestión de incidentes. A partir de los datos obtenidos, se identificaron los problemas críticos que limitaban la detección oportuna y la respuesta efectiva ante incidentes de seguridad. Posteriormente, se analizaron las relaciones de influencia y dependencia entre los factores detectados mediante la Matriz de Vester, técnica que posibilitó determinar el nivel de impacto de cada variable y priorizar las áreas de intervención para orientar de manera estratégica el diseño de la solución de alerta temprana.

2. Propuesta de solución

Se diseñó una solución de alerta temprana basada en honeypots virtualizados, desarrollada bajo un enfoque de sistemas que considera la interrelación entre los componentes técnicos, organizacionales y operativos de la seguridad informática. La solución se estructuró en cuatro fases metodológicas:

(a) Análisis de la situación. En esta fase se examinó de manera integral el estado de la seguridad informática en la infraestructura de red de Lavaseco Universal LTDA., identificando vulnerabilidades, debilidades en los mecanismos de detección y deficiencias en la gestión de incidentes. Se recopilaron y analizaron datos provenientes de diagnósticos técnicos, lo que permitió determinar los factores de riesgo más relevantes y definir las necesidades específicas de protección. Este análisis proporcionó la base para orientar el diseño de la solución de alerta temprana de acuerdo con las condiciones reales de la organización.

(b) Diseño del modelo de solución. Durante esta fase se elaboró el modelo conceptual y técnico del sistema de alerta temprana, estableciendo la arquitectura general, los componentes funcionales y las interacciones entre los honeypots virtualizados y los demás elementos de la red. Se definieron los parámetros de configuración, los protocolos de comunicación y los mecanismos de registro y alerta. El diseño siguió un enfoque de sistemas, asegurando la coherencia entre los aspectos tecnológicos, organizacionales y operativos de la seguridad informática.

(c) Implementación del sistema. En esta fase se materializó la propuesta mediante la instalación, configuración y puesta en funcionamiento de los honeypots virtualizados en el entorno real de la empresa. Se desarrollaron versiones adaptadas a las necesidades del sistema —una de escritorio y otra en modo consola— y se integraron a la infraestructura de red para iniciar la captura

de intentos de intrusión y tráfico sospechoso. La implementación incluyó pruebas controladas de funcionamiento para verificar la estabilidad, compatibilidad y desempeño de la solución dentro del entorno corporativo.

(d) Comprobación funcional. Esta fase tuvo como propósito validar la efectividad del sistema implementado en la detección temprana de incidentes de seguridad. Se realizaron análisis comparativos de los tiempos de detección antes y después de la implementación, con el fin de determinar el impacto real de la solución en la mejora de la capacidad de respuesta. Los resultados obtenidos demostraron una disminución significativa en los tiempos de detección, confirmando la eficacia del modelo propuesto y su aplicabilidad en entornos empresariales.

3. Validación

La validación de la solución se llevó a cabo dentro de la infraestructura de red de Lavaseco Universal LTDA., donde se implementó el sistema de seguridad informática basado en honeypots virtualizados. Con el fin de evaluar su efectividad, se desarrolló un proceso preexperimental que resultó adecuado para analizar cambios en un entorno real con una población pequeña y controlada. Este tipo de diseño permitió examinar la relación causa-efecto entre la implementación del honeypot y la reducción del tiempo de detección de incidentes de seguridad informática.

Para verificar esta relación, se aplicó la prueba estadística t de Welch para muestras independientes, lo que permitió comparar los tiempos de detección antes y después de la implementación del sistema. La prueba se ejecutó con un nivel de significancia de 0,05 y consideró un total de 17 incidentes registrados en ambas condiciones. Los resultados obtenidos evidenciaron una disminución significativa en los tiempos de detección tras la introducción del honeypot, lo que confirmó la relación causa-efecto planteada y permitió validar la hipótesis de investigación.

4. Análisis e interpretación de resultados

En esta etapa se realizó un análisis detallado de los datos recolectados durante el proceso de validación, con el propósito de identificar tendencias, patrones y variaciones relevantes en los tiempos de detección de incidentes antes y después de la implementación del honeypot. Este análisis permitió comprender el comportamiento del sistema en condiciones reales y evaluar la consistencia de los registros obtenidos. Se verificó la presencia de mejoras cuantificables en la detección temprana de intrusiones, lo cual proporcionó evidencia preliminar sobre la efectividad de la solución propuesta.

Posteriormente, se interpretaron los resultados obtenidos, contrastando los valores estadísticos con los objetivos planteados en la investigación. La interpretación incluyó la valoración de la magnitud de la reducción del tiempo de detección, la significancia estadística observada y su relación con el diseño preexperimental empleado. Este proceso permitió determinar con claridad el grado de efectividad del sistema de alerta temprana basado en honeypots virtualizados y evidenciar su aporte al fortalecimiento de la seguridad informática en la infraestructura de red de la empresa. La interpretación crítica de los datos facilitó la identificación de oportunidades de mejora y potenciales líneas de investigación futura.

5. Conclusiones y recomendaciones

Con base en los resultados alcanzados, se elaboraron las conclusiones de la investigación, sintetizando los aportes principales del sistema de alerta temprana y su impacto en la reducción del tiempo de detección de incidentes de seguridad informática. Estas conclusiones destacan la efectividad del honeypot virtualizado como mecanismo de monitoreo y evidencian su capacidad para generar información temprana y útil sobre intentos de intrusión. Se formularon

recomendaciones orientadas a futuras investigaciones y la implementación de soluciones similares en otras organizaciones.

La articulación de cada fase garantizó una transición ordenada entre el diagnóstico inicial y la interpretación final de los resultados, asegurando la consistencia interna del estudio y la validez de los hallazgos obtenidos. Este proceso metodológico secuencial permitió que cada etapa generara información necesaria para la siguiente, manteniendo la coherencia del procedimiento y evitando discontinuidades en el análisis. Esta estructura permitió evaluar de manera integrada el comportamiento del sistema y sustentar la solidez de las conclusiones obtenidas.

Para complementar la descripción metodológica, se presentan las principales herramientas tecnológicas empleadas en el desarrollo y validación del sistema de alerta temprana basado en honeypots virtualizados. En la siguiente tabla se sintetizan las herramientas tecnológicas utilizadas, con el principal propósito de ofrecer una visión clara y organizada de los recursos fundamentales que hicieron posible la implementación y evaluación del sistema propuesto.

Tabla 1

Herramientas tecnológicas utilizadas en la investigación

Linux Mint 21.2	Sistema operativo anfitrión donde se montó el entorno experimental y se gestionaron las máquinas virtuales.
Oracle VirtualBox 7.0	Hipervisor utilizado para crear la VM del honeypot y el entorno controlado de pruebas.
Windows XP SP3 (VM)	Sistema invitado donde se desplegó la versión de escritorio del honeypot para simular un activo vulnerable.
Archivo JSON del honeypot	Archivo que permitió definir interfaz, filtros, destino de logs (Syslog/PostgreSQL) y los once servicios vulnerables habilitados.
Kali Linux 2023.1	Plataforma utilizada para ejecutar las campañas de ataque controladas.
Nmap	Herramienta de código abierto que permitió realizar escaneos de puertos y detección de servicios durante la validación.

Metasploit Framework	Proyecto de código abierto empleado para explotar vulnerabilidades y evaluar la capacidad del honeypot para registrar ataques reales.
Microsoft Excel	Herramienta que se utilizó para procesar datos recolectados, ejecutar cálculos estadísticos y la prueba t de Welch.
Matriz de Vester	Herramienta de análisis usada en el diagnóstico para identificar influencias y dependencias entre problemas de seguridad.
Mendeley	Gestor bibliográfico utilizado para gestionar las referencias bibliográficas aplicadas en el estudio.
Python	Lenguaje de programación con el que se creó la versión de consola y la gestión de servicios vulnerables.
Amazon Web Services	Plataforma utilizada para almacenar copias de seguridad y respaldos importantes en el proceso de investigación.

Nota. La tabla presenta las principales herramientas empleadas en el desarrollo, ejecución y análisis del sistema de alerta temprana. Fuente: Elaboración propia.

En la Tabla 2 se muestran los parámetros esenciales del entorno experimental utilizado en la investigación para desplegar el honeypot y ejecutar las campañas de validación. En este sentido, se describen las características del hardware, la configuración de las máquinas virtuales, los servicios vulnerables habilitados, las herramientas de ataque empleadas y las variables medidas durante el proceso. Todo ello permite comprender las condiciones técnicas bajo las cuales se evaluó el desempeño del sistema.

Tabla 2

Parámetros del entorno experimental utilizado en la investigación

Parámetro	Descripción
Host físico	Linux Mint 21.2, 16 GB RAM, 1 TB SSD.
Hipervisor	Oracle VirtualBox 7.0.
VM del Honeypot	Windows XP SP3, 1 vCPU, 1 GB RAM, adaptador puente.
Configuración de red	Modo puente; servicios vulnerables habilitados para captura de ataques.
Servicios expuestos	HTTP, FTP, Telnet, SMTP, DNS, POP3, Echo, Finger, Daytime, TFTP y puertos mapeados.
Archivo de configuración	JSON con interfaz, filtros y destino de logs (Syslog/PostgreSQL).
Origen de ataques	Kali Linux 2023.1 con herramientas Nmap, Metasploit y accesos FTP señuelo.

Iteraciones de prueba	10 repeticiones por campaña; 17 observaciones pre y post implementación.
Variable medida	Tiempo de detección (ms) e identificación de huellas de ataque.
Método estadístico	Prueba t de Welch ($\alpha = 0,05$).

Nota. En la tabla se exponen los principales parámetros que conforman el entorno experimental de la investigación. Fuente: Elaboración propia.

La metodología aplicada permitió estructurar un proceso coherente para el diseño, implementación y validación del sistema de alerta temprana basado en honeypots virtualizados. La combinación del diagnóstico inicial, el desarrollo de la solución, su comprobación funcional y el análisis estadístico ofreció un enfoque integral para evaluar su efectividad en condiciones reales de operación. De este modo, la metodología empleada contribuyó al logro de los objetivos propuestos y sentó las bases para futuras mejoras del sistema en contextos empresariales similares.

RESULTADOS

Los resultados obtenidos se presentan mediante tablas y figuras que ofrecen una visión ordenada de los hallazgos alcanzados a lo largo del estudio. En primer lugar, se exponen los problemas identificados en la infraestructura de red de Lavaseco Universal LTDA., los cuales fueron analizados mediante la matriz de Vester para determinar sus niveles de influencia y dependencia. Este análisis permitió identificar los factores que ejercen mayor impacto sobre la seguridad informática de la organización y establecer prioridades para la intervención. El coeficiente obtenido confirmó la consistencia del diagnóstico realizado, aportando rigor metodológico al proceso de evaluación.

Posteriormente, se describen los resultados relacionados con el diseño, implementación y validación de la solución basada en honeypots virtualizados. La presentación de estos datos evidencia la efectividad de la herramienta en la reducción del tiempo de detección de incidentes

de seguridad, demostrando su aporte directo a la disminución del riesgo tecnológico. Las tablas y figuras asociadas permiten interpretar el desempeño del honeypot, así como el impacto positivo de su incorporación en la infraestructura de red. Estos resultados consolidan la relevancia de la propuesta tecnológica y su contribución al fortalecimiento de la seguridad informática en la organización.

El diagnóstico inicial permitió identificar los principales problemas en la infraestructura de red, los cuales fueron organizados y codificados para su análisis mediante la matriz de Vester. La Tabla 3 presenta los problemas detectados, que incluyen deficiencias en evaluaciones internas de seguridad, ausencia de políticas de manejo de información, sistemas expuestos a vulnerabilidades y limitaciones en los controles de acceso.

Tabla 3

Problemas identificados en la infraestructura de red de Lavaseco Universal LTDA.

Cód.	Problema
P1	Las evaluaciones de seguridad internas son insuficientes.
P2	Falta de una clasificación de la información según su nivel de confidencialidad
P3	Las actuales medidas de protección de datos son insuficientes para asegurar la información frente a amenazas emergentes
P4	Ausencia de políticas explícitas para el manejo, retención y eliminación de datos.
P5	El tiempo de detección de incidentes de seguridad puede llegar a más de 12 h.
P6	No se documentan los incidentes de seguridad.
P7	Falta de control de incidentes y medidas de seguridad adicionales para mitigar amenazas.
P8	Sistemas expuestos a agujeros de seguridad.
P9	No hay indicación de capacitación o concienciación en seguridad informática entre el personal.
P10	Los controles de acceso son limitados.
P11	Los sistemas críticos no están protegidos ni monitoreados activamente.

Nota. La tabla resume los problemas identificados en la infraestructura de red de Lavaseco Universal LTDA. Fuente: Elaboración propia.

Con el objetivo de determinar la relevancia y el impacto de cada problema identificado, se elaboró la matriz de relación influencia-dependencia, cuyos valores se muestran en la Figura 1. Esta matriz permitió identificar los problemas críticos que ejercen mayor influencia sobre la seguridad de la red y aquellos más dependientes de otros factores.

Figura 1

Matriz de relación influencia-dependencia

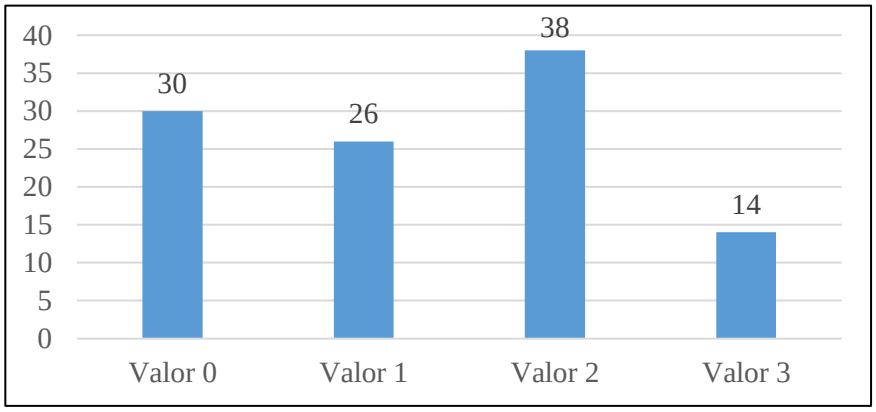
Código	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	Eje X
P1	0	0	0	0	0	3	2	0	0	3	2	10
P2	2	0	2	2	2	2	0	1	1	1	2	15
P3	0	0	0	0	2	0	0	1	2	0	1	6
P4	0	0	0	0	2	0	0	0	0	0	1	3
P5	3	2	2	3	0	2	2	3	3	3	3	26
P6	2	2	1	1	2	0	0	0	0	0	2	10
P7	2	0	3	1	3	2	0	0	1	1	1	14
P8	2	0	2	2	3	0	2	0	1	1	3	16
P9	2	2	2	1	2	2	1	0	0	2	2	16
P10	1	1	1	1	3	0	1	1	0	0	2	11
P11	2	2	1	1	3	1	1	2	2	2	0	17
Eje Y	16	9	14	12	22	12	9	8	10	13	19	

Nota. La figura presenta la matriz de relación influencia-dependencia utilizada para analizar el nivel de impacto entre los problemas identificados en la infraestructura de red de Lavaseco Universal LTDA. Fuente: Elaboración propia.

La matriz de relación influencia-dependencia evidencia una estructura problemática heterogénea dentro de la infraestructura de red de Lavaseco Universal LTDA., donde ciertos factores actúan como elementos detonantes y otros como consecuencias de fallas sistémicas. Esta configuración permite identificar prioridades estratégicas de intervención y orientar la formulación de una solución que atienda los factores más influyentes para producir mejoras de alcance transversal en la seguridad de la red.

Figura 2

Valores asignados para los cálculos en el análisis realizado mediante la matriz de Vester



Nota. La figura ilustra los valores asignados a cada categoría para el cálculo de influencias y dependencias dentro del análisis realizado mediante la matriz de Vester. Fuente: Elaboración propia.

Para realizar los cálculos de influencia y dependencia, se asignaron valores específicos a cada categoría, como se ilustra en la Figura 2. Este procedimiento permitió cuantificar de manera sistemática el nivel de influencia y dependencia de cada problema identificado, facilitando la comparación y priorización de los mismos dentro de la infraestructura de red. Además, la asignación de valores estandarizados asegura que cada factor sea evaluado bajo criterios

uniformes, lo que disminuye la subjetividad del análisis y posibilita identificar de forma objetiva los problemas con mayor impacto en la seguridad de la red, así como aquellos cuya resolución depende de otros elementos críticos.

La consistencia del análisis se verificó mediante el coeficiente obtenido a partir de la matriz de Vester, que resultó en 14,89 % (menor al 30 %), lo cual indica que los resultados son confiables y reflejan de manera precisa la criticidad relativa de los problemas priorizados (Véase: Tabla 4). Este enfoque proporciona una base sólida para la toma de decisiones, asegurando que las intervenciones propuestas se centren en los aspectos más críticos de la seguridad informática de Lavaseco Universal LTDA.

Tabla 4

Coeficiente obtenido a partir de la matriz de Vester

Total, de ponderaciones asignadas	94
No. de ponderaciones con valor asignado 3	14
Coeficiente obtenido (%)	14,89%

Nota. La tabla muestra el coeficiente resultante del análisis de ponderaciones asignadas en la matriz de Vester, utilizado para determinar el nivel de criticidad del problema priorizado. Fuente: Elaboración propia.

La investigación incluyó el desarrollo e implementación de un honeypot virtualizado como solución de alerta temprana frente a incidentes de seguridad. Los aspectos principales del proceso se resumen en la Tabla 6, destacando el diseño de versiones de escritorio y consola, la instalación en la infraestructura de Lavaseco Universal LTDA., y la validación mediante la prueba t de Welch

para analizar la relación entre la implementación del honeypot y la reducción del tiempo de detección de incidentes.

Tabla 5

Aspectos clave del diseño, implementación y validación del honeypot

Aspecto	Descripción
Diseño del honeypot	Se desarrolló un honeypot virtualizado con dos versiones: una de escritorio y otra en modo consola.
Implementación del honeypot	El honeypot se instaló en la infraestructura de red de Lavaseco Universal LTDA., ubicada en Santa Cruz de la Sierra, Bolivia.
Prueba de hipótesis	Se aplicó la prueba t de Welch para muestras independientes con el propósito de analizar la relación causa-efecto entre la implementación del honeypot y la reducción del tiempo de detección. La hipótesis de investigación (H1) plantea un efecto positivo, mientras que la hipótesis nula (H0) sostiene la ausencia de impacto significativo.
Disminución del tiempo de detección	Se registró una reducción notable en el tiempo de detección de incidentes, pasando de más de 12 horas a un promedio de 4,4 horas.

Nota. La tabla sintetiza los elementos principales del proceso de diseño, implementación y validación del honeypot virtualizado aplicado en la investigación. Fuente: Elaboración propia.

Los resultados obtenidos en esta investigación demuestran que la implementación de un sistema de alerta temprana mediante honeypots virtualizados contribuye de manera significativa a resolver el problema de la detección tardía de incidentes de seguridad en la infraestructura de red de Lavaseco Universal LTDA. La solución desarrollada permitió reducir el tiempo de detección de incidentes de más de 12 horas a un promedio de 4,4 horas, lo que facilita una respuesta más rápida frente a las amenazas y minimiza el impacto potencial de los incidentes sobre la operación de la empresa. Este hallazgo evidencia la efectividad del enfoque propuesto y su relevancia para mejorar la protección de los sistemas críticos dentro de la organización.

La información obtenida a través de los honeypots sobre las tácticas y técnicas empleadas por los atacantes proporciona insumos valiosos para mejorar las estrategias de defensa y prevenir futuros incidentes de seguridad. La solución implementada optimiza la gestión de la seguridad de

la información en Lavaseco Universal LTDA., y ofrece un modelo replicable para otras organizaciones que buscan implementar sistemas de alerta temprana en sus redes. Estos resultados demuestran la importancia de integrar herramientas de monitoreo proactivo como los honeypots virtualizados para el desarrollo de soluciones de seguridad informática más efectivas y sostenibles.

DISCUSIÓN

Los resultados obtenidos en este estudio permiten realizar una interpretación crítica de la importancia que desempeñan los honeypots virtualizados dentro de una estrategia de seguridad informática aplicada a una organización en crecimiento. El diagnóstico inicial evidenció brechas significativas en la gestión de incidentes y la capacidad de detección temprana, lo que refuerza la necesidad de integrar mecanismos que alerten ante actividades maliciosas y proporcionen información detallada sobre el comportamiento de los atacantes. En este sentido, las evidencias obtenidas en Lavaseco Universal LTDA. coinciden con la definición propuesta por INCIBE (2019), que caracteriza a los honeypots como sistemas diseñados para atraer ataques con el propósito de estudiar tácticas, técnicas y procedimientos (TTP). En la presente investigación se demuestra cómo la virtualización optimiza la eficiencia operativa, reduce la dependencia de infraestructura física y habilita capacidades avanzadas de monitoreo que no han sido exploradas con la misma profundidad en trabajos previos centrados en entornos tradicionales.

Un análisis comparativo con investigaciones anteriores permite contextualizar la relevancia de los hallazgos. Joshi & Sardana (2011) demostraron la eficacia de los honeypots para identificar escaneos, ataques de fuerza bruta y accesos no autorizados en estudios experimentales. Los resultados obtenidos en Lavaseco Universal LTDA. concuerdan con estas observaciones, pero aportan evidencia adicional al provenir de un entorno empresarial real, con variaciones operativas,

tráfico auténtico y múltiples factores internos, lo que incrementa la validez de los datos recopilados.

Spitzner (2003) y Jurado (2016) destacaron las ventajas complementarias entre honeypots de baja y alta interacción; sin embargo, la presente investigación introduce una dimensión adicional al demostrar que la virtualización permite ajustar los niveles de interacción sin comprometer los recursos computacionales, disminuyendo barreras de adopción para organizaciones pequeñas o medianas. Este contrapunteo entre teoría y práctica evidencia que la virtualización reafirma los beneficios identificados en estudios previos, y habilita nuevas posibilidades en términos de escalabilidad, automatización y gestión integrada de incidentes.

Otro aspecto relevante se relaciona con la interacción entre los honeypots y otras herramientas de seguridad. Los resultados del presente estudio evidencian que su integración con sistemas como Metasploit, Nessus o plataformas en la nube genera un ecosistema de seguridad más robusto. Esta integración permite trascender un registro meramente descriptivo de eventos y adoptar un enfoque de inteligencia de amenazas capaz de correlacionar patrones, identificar vulnerabilidades explotadas y sustentar decisiones estratégicas de seguridad. En Lavaseco Universal LTDA., los honeypots se consolidan como un componente articulado en una estrategia de defensa integral, lo cual aporta insumos relevantes para el análisis forense, la priorización de vulnerabilidades y la mitigación de riesgos.

A pesar de los avances logrados, el estudio presenta limitaciones metodológicas que deben ser consideradas. El número reducido de incidentes registrados (17) restringe la posibilidad de establecer patrones con un alto grado de generalización y puede limitar la observación de variantes más sofisticadas de ataque. Por otra parte, la falta de un grupo de control impide comparar la

efectividad de la solución con tecnologías o configuraciones alternativas, lo que reduce el alcance de las conclusiones. El reconocimiento de estas limitaciones permite contextualizar los resultados y orientar investigaciones futuras hacia muestras ampliadas y análisis comparativos más complejos.

Desde la perspectiva académica, los hallazgos del estudio permiten profundizar en la discusión teórica sobre la utilidad de los honeypots en entornos empresariales. Tradicionalmente, la literatura ha enfatizado su función como mecanismo de captura de información; sin embargo, los resultados muestran que su implementación también contribuye a la consolidación de prácticas de seguridad preventiva, al fortalecimiento de competencias en análisis forense y a la generación de datos relevantes para la comprensión de amenazas emergentes.

La documentación sistemática de incidentes constituye un recurso valioso para la formación de profesionales en ciberseguridad, ya que facilita el estudio de patrones de explotación, técnicas de ataque y comportamientos adversarios, elementos esenciales para la generación de conocimiento aplicado. El estudio abre vías para explorar la interoperabilidad de los honeypots con arquitecturas de monitoreo avanzado, ofreciendo un marco conceptual para investigaciones orientadas a la automatización, la inteligencia artificial o la correlación dinámica de eventos.

Desde la perspectiva profesional, los resultados indican que los honeypots virtualizados constituyen una estrategia viable y costo-efectiva para fortalecer la postura de seguridad de organizaciones con recursos limitados. La reducción del tiempo de detección de incidentes, la visibilidad detallada sobre amenazas y la capacidad de integrar información operativa aportan beneficios directos para la gestión de riesgos.

La implementación de esta solución contribuye a la estructuración formal de procesos de respuesta a incidentes, la consolidación de roles más definidos dentro del equipo de TI y al fortalecimiento de una cultura organizacional orientada a la seguridad. Estas capacidades adquieren un valor estratégico en contextos como el de Lavaseco Universal LTDA., donde se proyecta la creación de un Centro de Operaciones de Seguridad (SOC) y la adopción progresiva de modelos de ciberseguridad más maduros.

Esta investigación valida la relevancia de los honeypots virtualizados como herramientas de alerta temprana y análisis de amenazas, y propone un marco integral para su uso en entornos empresariales reales. Los resultados ofrecen implicaciones significativas para el ámbito académico y la práctica profesional, pues permiten demostrar que la combinación de honeypots con mecanismos de gestión de vulnerabilidades y herramientas de análisis contribuyen a mejorar la seguridad informática, minimizar riesgos y fortalecer la resiliencia organizacional. Los hallazgos abren oportunidades para nuevas líneas de investigación orientadas a la automatización, el análisis avanzado de amenazas y la evolución de arquitecturas adaptativas de seguridad.

CONCLUSIONES

Los resultados obtenidos evidencian que la incorporación de los honeypots virtualizados constituyen una estrategia efectiva para fortalecer la detección temprana de incidentes en entornos corporativos con recursos limitados. La reducción del tiempo medio de detección, sustentada en mediciones comparativas antes y después de la implementación, confirma que la captura directa de tráfico malicioso permite identificar comportamientos hostiles con mayor rapidez y precisión. Este desempeño se traduce en un incremento sustancial de la capacidad de monitoreo, una mejora

en la visibilidad sobre las actividades no autorizadas y un soporte más sólido para la toma de decisiones operativas en materia de seguridad informática.

El proceso desarrollado permitió demostrar que una arquitectura basada en honeypots virtualizados puede integrarse con éxito en la infraestructura tecnológica de una PYME, sin afectar la operación diaria ni exigir inversiones elevadas. Las mejoras observadas en los tiempos de reacción, la gestión de incidentes y la comprensión del comportamiento de los atacantes reflejan el alcance de la propuesta y aportan evidencia de su utilidad en contextos empresariales que buscan elevar su madurez en ciberseguridad.

En función de los resultados, se proyectan varias líneas de acción que pueden ampliar el impacto de esta iniciativa. Una primera dirección consiste en replicar la solución en organizaciones con distintos niveles de complejidad tecnológica, con el fin de validar su rendimiento en infraestructuras heterogéneas y explorar su integración con controles avanzados de seguridad. Resulta pertinente promover investigaciones orientadas a comparar distintos tipos de honeypots, automatizar la correlación de eventos y evaluar su desempeño frente a amenazas emergentes. Se recomienda fortalecer los programas de capacitación del personal técnico y operativo, ya que la eficacia de estas soluciones depende de la adecuada interpretación de los registros obtenidos y la capacidad institucional para responder de forma oportuna ante incidentes.

AGRADECIMIENTOS

El autor expresa su agradecimiento a Lavaseco Universal LTDA. por facilitar el acceso a su infraestructura tecnológica y brindar las condiciones necesarias para el desarrollo de esta investigación, como el apoyo operativo y la disponibilidad del personal del área de Tecnologías de la Información. Asimismo, se reconoce el respaldo académico recibido durante su formación

como Ingeniero Informático y Magíster en Auditoría y Seguridad Informática en la Universidad Autónoma Gabriel René Moreno (UAGRM), cuyo acompañamiento técnico y orientaciones metodológicas contribuyeron al fortalecimiento de este estudio.

BIBLIOGRAFÍA

Acosta, R. (2022). *Propuesta basada en la seguridad lógica perimetral en las Pymes, como estrategia para la protección contra ciberataques*. [Monografía presentada para optar por el título de Especialista en Seguridad Informática, Universidad Nacional Abierta y a Distancia-UNAD]. Repositorio Institucional UNAD, Bogotá. https://repository.unad.edu.co/handle/10596/49276

Chapoñan, S.D. (2021). *Análisis comparativo de honeypot de baja interacción honeyd y kfsensor implementados virtualmente*. [Tesis de Grado, Universidad Señor de Sipán]. Repositorio Universidad Señor de Sipán (USS). https://repositorio.uss.edu.pe/handle/20.500.12802/9066

Genero, M., Cruz-Lemus, J.A. & Piattini, M.G. (2015). *Métodos de investigación en ingeniería del software*. Bogotá, Colombia: Ediciones de la U. https://dspace.itsjapon.edu.ec/xmlui/handle/123456789/2525

Hernández- Sampieri, R., Fernández-Collado, C. & Baptista-Lucio, P. (2014). *Metodología de la Investigación*. (6a edición). Mc Graw Hill Education. https://apiperiodico.jalisco.gob.mx/api/sites/periodicooficial.jalisco.gob.mx/files/metodologia_de_la_investigacion_-_roberto_hernandez_sampieri.pdf

IBM Security. (30 de julio de 2024). *Cost of a Data Breach Report 2024: Escalating data breach disruption pushes costs to new highs*. Newsroom IBM. https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs

Instituto Nacional de Ciberseguridad (INCIBE). (2019). *Guía de implantación de un honeypot industrial*. https://www.incibe.es/sites/default/files/contenidos/guias/doc/incibe-cert_guia_implantacion_honeypot_industrial.pdf

Joshi, R.C. & Sardana, A. (2011). *Honeypots. A new paradigm to Information Security*. CRC Press. https://www.iacr.org/books/2015_tf_joshi_honeypots.pdf

Jurado, D. (2016). *Análisis y estudio de honeypots complejos: honeynets* [Trabajo de Fin de Grado en Ingeniería Informática, Universidad Autónoma de Madrid, Escuela Politécnica Superior]. Repositorio Institucional UAM. https://repositorio.uam.es/handle/10486/676952

Spitzner, L. (2003). *Honeypots: Tracking Hackers*. Addison Wesley. Pearson Education. https://archive.org/details/honeypotstrackin0000spit/page/n5/mode/2up

Swathi, T., Srikanth, K., & Raghunath, S. (2014). Virtualization in Cloud Computing. *International Journal of Computer Science and Mobile Computing*, 3(5), 540 – 546. https://www.ijcsmc.com/docs/papers/May2014/V3I5201499a.pdf