UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

TRABAJO DE INTEGRACIÓN CURRICULAR

TEMA:

"PROPUESTA DE UN SISTEMA SANDBOX PARA MITIGAR INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE SOPORTE TÉCNICO A USUARIOS"

Trabajo de titulación previo a la obtención del título en Magíster en Computación con Mención en Seguridad Informática

Línea de investigación: Desarrollo, aplicación de software y cyber security (seguridad cibernética)

AUTOR:

Diego Mauricio Ibarra Muela

DIRECTOR:

Msc. Diego Javier Trejo España

Ibarra – Ecuador 2025

DEDICATORIA

A mi esposa, por ser mi apoyo en la toma de decisiones en los momentos más importantes en mi vida desde que tengo la fortuna de compartirla con ella.

A mi hija, por ser mi fuente de inspiración y el motor que impulsa mi superación cada mañana desde que Dios me bendijo con su presencia.

A mis padres, por su apoyo y acompañamiento incondicional en cada momento que los he necesitado.

Y a todos quienes me han acompañado en el cumplimiento de una etapa más en mi vida profesional.

AGRADECIMIENTO

A Dios, por bendecirme una vez más con su guía, permitiéndome cumplir con una etapa más a pesar de mis momentos de flaqueza en la fe.

A los docentes de la UTN, por compartir su conocimiento y experiencia, formando a profesionales capaces de aplicar lo aprendido para mejorar nuestro país desde cada uno de nuestros lugares de trabajo.

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1714638424		
APELLIDOS Y NOMBRES:	Ibarra Muela Diego Mauricio		
DIRECCIÓN:	Quito		
EMAIL:	ing.mibarra@hotmail.com		
TELÉFONO FIJO:	022063410	**TELÉFONO MÓVIL:**	0961307111

DATOS DE LA OBRA	
TÍTULO:	PROPUESTA DE UN SISTEMA SANDBOX PARA MITIGAR INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE SOPORTE TÉCNICO A USUARIOS
AUTOR (ES):	Diego Mauricio Ibarra Muela
FECHA: DD/MM/AAAA	30/05/2025
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	☐ **PREGRADO** ■ **POSGRADO**
TITULO POR EL QUE OPTA:	**MAGÍSTER EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA**
ASESOR /	**Msc. Fabián Geovanny Cuzme Rodríguez /**

DIRECTOR:	**Msc. Diego Javier Trejo España**

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 30 días del mes de mayo de 2025

EL AUTOR:

Diego Mauricio Ibarra Muela

Ibarra, 14 de marzo de 2025

Dra.
Lucía Yépez
DECANA FACULTAD DE POSGRADO

ASUNTO: Conformidad con el documento final

Señor(a) Decano(a):

Nos permitimos informar a usted que revisado el Trabajo final de Grado PROPUESTA DE UN SISTEMA SANDBOX PARA MITIGAR INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE SOPORTE TÉCNICO A USUARIOS del maestrante Ing. Diego Mauricio Ibarra Muela, de la Maestría de Computación con Mención en Seguridad Informática, certificamos que han sido acogidas y satisfechas todas las observaciones realizadas.

Atentamente,

	Apellidos y Nombres	**Firma**
Director	Msc. Diego Javier Trejo España	Firmado digitalmente por Diego Javier Trejo España Fecha: 2025.03.17 07:28:52 -05'00'
Asesor	Msc. Fabián Geovanny Cuzme Rodríguez	FABIAN GEOVANNY CUZME RODRIGUEZ

INDICE DE CONTENIDOS

CAPITULO I 1

EL PROBLEMA 1

1.1. Problema de investigación 1

1.2. Interrogante de la investigación 2

1.3. Objetivos de la investigación 2

1.3.1. Objetivo general 2

1.3.2. Objetivos específicos 2

1.4. Hipótesis de Trabajo 3

1.5. Hipótesis Alternativa 3

1.6. Categorización de Variables 3

1.7. Justificación 4

MARCO REFERENCIAL 5

2.1. Antecedentes 5

2.2. Marco Teórico 10

2.2.1. Sistema Sandbox 10

2.2.2. Incidentes de seguridad 12

2.2.3. Información en el área de soporte técnico 14

2.2.4. Seguridad de la información 15

2.2.5. Análisis de riesgos 16

2.3. Marco legal 17

CAPITULO III 18

MARCO METODOLÓGICO 18

3.1. Descripción del área de estudio 19

3.1.1. Descripción del grupo de estudio 19

3.2. Enfoque y tipo de investigación 19

3.3. Procedimiento de investigación 21

3.4. Consideraciones bioéticas 25

CAPITULO IV 25

RESULTADOS Y DISCUSIÓN 25

4.1. Análisis de los incidentes de seguridad reportados en el área de soporte técnico a usuarios (identificación de los requerimientos más comunes y que pueden ser mitigados con la implementación de un sistema Sandbox) 25

CAPITULO V 63

PROPUESTA 63

5.1. Descripción de la propuesta 63

5.2. Objetivos de la propuesta 64

5.2.1. Objetivo general 64

5.2.2. Objetivos específicos 65

5.3. Justificación 65

5.4. Estructura de la propuesta 66

5.4.1. Evaluación de los sistemas Sandbox opensource o propietario que se adapten a las necesidades identificadas en la fase de análisis. 67

5.4.2. Validación del plan de implementación del sistema Sandbox evaluado en un entorno controlado, con ayuda de dos profesionales del área de soporte técnico a usuarios quienes puedan argumentar la eficacia en la reducción de incidentes de seguridad, utilizando métricas predefinidas. 78

5.4.3. Plan de implementación del sistema Sandbox evaluado en un entorno controlado. 84

CONCLUSIONES 88

RECOMENDACIONES 89

REFERENCIAS 91

ANEXOS 98

INDICE DE TABLAS

Tabla 1 8
Tabla 2 Matriz: Tipos de incidentes 27
Tabla 3 Definición de incidentes comunes de seguridad informática 27
Tabla 4 Evaluación del activo 28
Tabla 5 Valoración de impacto en los activos de la información 29
Tabla 6 Estimación de amenazas 31
Tabla 7 Estimación de vulnerabilidades 33
Tabla 8 Amenazas típicas (ISO/IEC 27005:2022) 35
Tabla 9 Vulnerabilidades típicas (ISO/IEC 27005:2022) 40
Tabla 10 Amenazas típicas 44
Tabla 11 Vulnerabilidades Típicas (EGSI) 46
Tabla 12 Análisis amenazas / vulnerabilidades (NTE INEN – ISO/IEC 27005:2012) 50
Tabla 13 Matriz de evaluación de riesgos 60
Tabla 14 Comparación de sistemas sandbox para mitigación de riesgos en seguridad informática 67
Tabla 15 81
Tabla 16 Cronograma 86

INDICE DE FIGURAS

Figura 1 Búsqueda de literatura en IEEEXplore 5
Figura 2 Sandbox Cuckoo 72
Figura 3 FireEye MVX 73
Figura 4 VxStream Sandbox 74
Figura 5 Any.Run 76
Figura 6 Joe Sandbox 77

UNIVERSIDAD TÉCNICA DEL NORTE

PROPUESTA DE UN SISTEMA SANDBOX PARA MITIGAR INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE SOPORTE TÉCNICO A USUARIOS

Autor: Ing. Diego Mauricio Ibarra Muela
Director: Msc. Diego Javier Trejo España

RESUMEN

Contexto: Los incidentes de seguridad resultantes de las acciones de los usuarios finales se están convirtiendo en un desafío para los equipos de soporte al usuario en varias organizaciones, tomando en cuenta que este grupo en particular, son considerados el eslabón más débil en la cadena de seguridad de la información. **Objetivo:** Realizar una propuesta de un sistema Sandbox efectivo para mitigar los incidentes de seguridad de la información para el área de soporte técnico a usuarios, basado en un análisis de riesgos**.** **Metodología:** El enfoque de la investigación fue documental, se basó en una revisión bibliográfica que integró el análisis de artículos cuyas metodologías y hallazgos se fundamentaron en métodos cualitativos y cuantitativos. Se sustentó en datos obtenidos de casos reportados sobre seguridad informática en áreas de soporte a usuarios de una organización del sector público, combinando análisis estadísticos y cualitativos. Esta respondió a la elección de un sistema sandbox de código abierto o propietario, que mejor se adapte a las necesidades identificadas en la fase de análisis. **Resultados:** Se evidenció que la implementación de un sistema Sandbox constituye una estrategia eficaz para mitigar incidentes de seguridad, la mejor opción fue Cuckoo Sandbox, ya que cumplió con los requisitos de la organización al ofrecer una integración flexible con los sistemas existentes y capacidades avanzadas de análisis de amenazas.

Palabras claves: Incidentes de seguridad, sistema, Sandbox, análisis, riesgos

UNIVERSIDAD TÉCNICA DEL NORTE

PROPOSAL OF A SANDBOX SYSTEM TO MITIGATE INFORMATION SECURITY INCIDENTS IN THE AREA OF TECHNICAL SUPPORT TO USERS

Author: Ing. Diego Mauricio Ibarra Muela
Director: Msc. Diego Javier Trejo España

ABSTRACT

Context: Security incidents resulting from the actions of end users are becoming a challenge for user support teams in several organizations, considering that this group in particular, are considered the weakest link in the information security chain. **Objective**: To make a proposal for an effective Sandbox system to mitigate information security incidents for the user support area, based on a risk analysis. **Methodology**: The research approach was a documentary, based on a bibliographic review that integrated the analysis of articles whose methodologies and findings were based on qualitative and quantitative methods. It was based on data obtained from cases reported on computer security in user support areas of a public sector organization, combining statistical and qualitative analysis. It responded to the choice of an open source or proprietary sandbox system, which best suits the needs identified in the analysis phase. **Results:** It became evident that the implementation of a sandbox system is an effective strategy to mitigate security incidents. The best option was the Cuckoo Sandbox, as it met the organization's requirements by offering flexible integration with existing systems and advanced threat analysis capabilities.

Keywords: Security incidents, system, Sandbox, analysis, risk, risks

CAPITULO I

EL PROBLEMA

1.1. Problema de investigación

Los incidentes de seguridad resultantes de las acciones de los usuarios finales se están convirtiendo en un desafío para los equipos de soporte al usuario en varias organizaciones, tomando en cuenta que este grupo en particular, son considerados el eslabón más débil en la cadena de seguridad de la información. Los incidentes reportados han aumentado dramáticamente debido a la creciente sofisticación de las ciberamenazas y la falta de conciencia de seguridad entre los usuarios, esto da como resultado una sobrecarga de trabajo en el personal de soporte, impidiéndole concentrarse en otras tareas importantes y exponiendo a las organizaciones a riesgos significativos, incluida la pérdida de datos confidenciales, la interrupción de los servicios y el daño a la reputación de la organización.

Debido a lo antes expuesto, es primordial para las organizaciones, contar con soluciones tecnológicas que se pueden utilizar para aislar y analizar la actividad de los usuarios, reduciendo los riesgos y facilitando la detección y mitigación de los incidentes comúnmente reportados en materia de seguridad informática. Además, contar con dichas soluciones, permitirá asegurar que la información, al ser en la actualidad el activo más importante en las organizaciones, no se encuentre completamente vulnerable, sobre todo en las áreas críticas.

En esta línea, si no se implementan soluciones tecnológicas efectivas como un sistema Sandbox, las empresas y organizaciones quedaran expuestas a un aumento de incidentes de seguridad lo que puede comprometer la confidencialidad e integridad de la información,

por ejemplo, la falta de controles adecuados facilitará la propagación de ciberataques, generando pérdidas económicas, sanciones legales por incumplimiento de normativas y afectando la confianza de clientes y socios comerciales. Además, la sobrecarga en los equipos de soporte técnico reducirá su capacidad para atender problemas críticos, lo que podría afectar la continuidad operativa y la estabilidad del negocio a largo plazo.

1.2. Interrogante de la investigación

- ¿Cuáles son los incidentes de seguridad más comunes en el área de soporte técnico a usuarios?
- ¿Cuáles sistemas Sandbox opensource o propietario se adaptan a las necesidades identificadas?
- ¿Se validó la eficacia de implementar un sistema sandbox en el área de soporte técnico a usuarios?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

- Realizar una propuesta de un sistema Sandbox efectivo para mitigar los incidentes de seguridad de la información para el área de soporte técnico a usuarios, basado en un análisis de riesgos.

1.3.2. Objetivos específicos

- Analizar los incidentes de seguridad reportados en el área de soporte técnico a usuarios para identificar los requerimientos más comunes y que pueden ser mitigados con la implementación de un sistema Sandbox.

- Evaluar sistemas Sandbox opensource o propietario que se adapten a las necesidades identificadas en la fase de análisis, con el objetivo de minimizar el número de incidentes de seguridad en base a un análisis de riesgos.

- Validar la implementación del sistema Sandbox evaluado, con ayuda de profesionales del área de soporte técnico a usuarios quienes puedan argumentar la eficacia en la reducción de incidentes de seguridad, utilizando métricas predefinidas.

1.4. Hipótesis de Trabajo

Realizar una propuesta de un sistema Sandbox efectivo PERMITIRÁ mitigar los incidentes de seguridad de la información para el área de soporte técnico a usuarios basado en un análisis de riesgo.

1.5. Hipótesis Alternativa

Realizar una propuesta de un sistema Sandbox efectivo NO PERMITIRÁ mitigar los incidentes de seguridad de la información para el área de soporte técnico a usuarios basado en un análisis de riesgo.

1.6. Categorización de Variables

Las variables que se derivan de la hipótesis planteada son:

- **Variable dependiente**: Realizar una propuesta de un sistema Sandbox efectivo

- **Variable independiente**: Mitigar los incidentes de seguridad de la información para el área de soporte técnico a usuarios basado en un análisis de riesgo

1.7. Justificación

Un sistema sandbox en soporte técnico reduciría en gran medida los incidentes de seguridad reportados al área de soporte técnico a usuarios.

El área de soporte técnico a usuarios en una organización es la encargada de receptar las solicitudes de carácter tecnológico de todos los usuarios de la red interna y buscar una solución al inconveniente reportado. Dependiendo del nivel de conocimiento tecnológico que tengan los usuarios de red interna en una organización, el registro de solicitudes en el sistema de mesa de servicios o mesa de ayuda suele ser mayor o menor. En los casos donde las solicitudes diarias sobrepasan la capacidad de atención debido al limitado número de personal informático en el área de soporte técnico, es necesario encontrar alternativas que ayuden a minimizar la cantidad de estos requerimientos.

Tomando en cuenta que varios de estos requerimientos son sobre problemas de seguridad informática, donde aún usuarios con conocimientos altos en tecnología no saben cómo actuar frente a casos de este tipo, se abre la posibilidad a encontrar una herramienta tecnológica como son los sandbox para mitigar este tipo de requerimientos.

Esta investigación ayudará a las organizaciones a contar con una herramienta que analiza previamente la actividad de los usuarios evaluando diferentes soluciones y probar la efectividad de estas en un entorno controlado, así como contar con una guía práctica que permita mejorar su postura ante la seguridad informática.

Por ende, este estudio puede ayudar a las organizaciones a mejorar la protección de sus activos digitales y reducir los gastos asociados a la recuperación de incidentes debido a las violaciones de seguridad.

CAPITULO II

MARCO REFERENCIAL

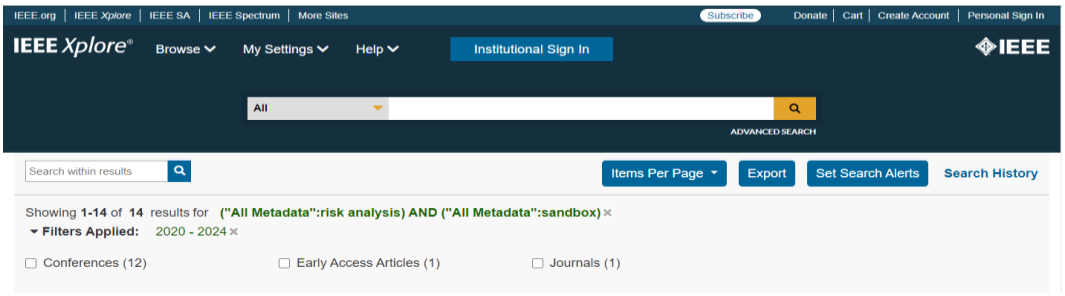
2.1. Antecedentes

Para determinar los trabajos relacionados con la presente propuesta de investigación, se ha realizado una revisión de literatura preliminar, siguiendo un protocolo de búsqueda estandarizado para este tipo de estudios.

En primera instancia, se determinó una cadena de búsqueda que permita contestar a la siguiente interrogante de investigación: **¿Cómo realizar una propuesta de un sistema Sandbox efectivo para mitigar los incidentes de seguridad de la información para el área de soporte técnico a usuarios, basado en un análisis de riesgos?** Para encontrar los artículos que respondan a esta interrogante, se definió la siguiente cadena de búsqueda: ("All Metadata": risk analysis) AND ("All Metadata": sandbox)

La cadena de búsqueda fue ejecutada en la base de datos de IEEE Xplore (IEEEX), misma que mostró un total de 14 publicaciones entre conferencias, artículos de acceso anticipado y revistas. Se utilizó como criterio de inclusión los trabajos publicados durante los últimos 5 años, como se muestra en la siguiente imagen:

Figura 1
Búsqueda de literatura en IEEEXplore



Fuente: IEEE Xplore

De los resultados obtenidos se analizó el total de los artículos, para determinar los que sean más relevantes para el estudio. Se seleccionó 6 artículos, cuyo análisis se detalla a continuación:

Según el estudio realizado por Kumaralingam y Wijayasekara (2024) menciona que, para combatir las preocupaciones típicas de la seguridad cibernética, el análisis de malware es esencial. Como se desarrolla un malware altamente sofisticado, requiere una técnica para instalar y estudiar las propiedades del software de comportamiento. Para reducir el impacto en la infraestructura actual, los entornos aislados de los sistemas de producción se han creado históricamente utilizando máquinas virtuales. Los desarrolladores de malware suelen crear tácticas de evasión para evitar la detección en entornos de sandbox ya que son conscientes de esto.

En el estudio realizado por Jong et al. (2022) evidencia que debido a que la mayoría de los cursos actuales de programación utilizan sistemas Judge en línea como material didáctico, el aumento de estos cursos para las personas en el campo de la informática se está extendiendo cada vez más, pero al mismo tiempo, hay cada vez más ataques a los sistemas judge en línea. Evitar estos ataques a los sistemas judge en línea es cada vez más importante por lo que se puede utilizar herramientas como entornos sandbox para probar estos sistemas antes de utilizarlos en estos cursos.

Las aplicaciones de Internet de las cosas (IoT) ofrecen una gran comodidad, pero nos exponen a nuevas amenazas para la seguridad según el artículo de Hong et al. (2021). Las políticas de seguridad tradicionales pueden no prever todos los usos posibles, lo que

provoca falsas alarmas. Este estudio propone el uso de sandboxes para asegurar entornos IoT, analizando comportamientos de aplicaciones y dispositivos, se despliega una caja de arena que prohíbe comportamientos no vistos anteriormente, bloqueando así comportamientos maliciosos. Se presenta IoTBox, un prototipo que aborda las limitaciones de las técnicas de minería sandbox existentes, logrando mayor precisión en la detección de código malicioso en entornos IoT complejos.

Un estudio experimental realizado por Thulasiraman (2022) muestra que ataques maliciosos pueden ser identificados y neutralizados con mucha precisión utilizando un modelo MATLAB dentro de un entorno sandbox SCADA similar al de la marina.

La proliferación de dispositivos inseguros conectados a Internet ha dado lugar a las redes de bots de IoT que pueden crecer muy rápidamente y realizar ciberataques de gran impacto según el estudio realizado por Trajanovski y Zhang (2021). Los estudios relacionados para abordar las botnets de IoT se ocupan de capturar o analizar muestras de botnet de IoT, utilizando honeypots y cajas de arena, respectivamente. La falta de integración entre los dos implica retraso en la presentación de resultados y se presenta el riesgo de que el comportamiento de las botnets cambie. Además, la eficacia de las sandboxes propuestas está limitada por el uso potencial de técnicas de anti-análisis y la incapacidad para identificar características para una detección e identificación eficaces de botnets de IoT. El estudio promueve la creación de honeypots integrados con una sandbox que permite cambiar el presente problema mencionado.

En el estudio realizado por Gottardelli (2024) se indica que, las recientes innovaciones en informática y ciencias de la computación están impulsando la integración de la IA en los

servicios sanitarios modernos, ampliando sus aplicaciones a sectores médicos que anteriormente dependían de la experiencia humana. Crear modelos de IA sólidos y clínicamente relevantes requiere datos extensos, que pueden ser difíciles de reunir, especialmente cuando se trata de enfermedades raras. El intercambio de datos entre entidades sanitarias puede abordar este problema, pero las preocupaciones jurídicas, de privacidad y de propiedad de los datos dificultan ese enfoque. Para fomentar el intercambio de datos, en este documento proponemos GEmelli GeNerator - Real World Data (GEN-RWD) Sandbox, que proporciona un entorno seguro para el análisis de datos sin comprometer los datos médicos sensibles.

Tabla 1

Lista de literatura

Artículo Nro.	Autor	Año	Tipo de organización estudiada	Factores de éxito	Dificultades encontradas	Página web
1	T. Kumaralingam y S. K. Wijayasekara	2024	Entornos sandbox	Se proporciona la implementación de la detección de temporizadores sin asumir la integridad del núcleo del sistema comprometido, que es una parte crucial de dicho sistema	Un problema de investigación difícil es el desarrollo de un sistema automatizado que construye la cronología del malware	https://ieeexplore.ieee.org/document/10594974
2	Jong-Yih Kuo; Zhi-Jia Wen; Han-Xuan Huang;	2022	Sistemas Judge en línea	Esta herramienta puede ayudar verificar si el sistema judge está en riesgo de ser atacado y para tratar con él lo más pronto posible para mejorar la	Crea un modelo de amenaza para el sistema judge en línea, para diseñar reglas de análisis de código e implementar una herramienta de análisis de código	https://ieeexplore.ieee.org/document/10051768/authors#authors

	I-Ting Guo			seguridad del sistema		
3	Hong Jin Kang; Sheng Qin Sim; David Lo	2021	Internet de las cosas (IoT)	Después de analizar un conjunto de comportamientos de un grupo de aplicaciones y dispositivos, se despliega una caja de arena, que hace que los comportamientos no vistos anteriormente sean prohibidos	Políticas de seguridad y protección hechas a mano para detectar estas amenazas, es posible que estas políticas no prevean todos los usos de los dispositivos y aplicaciones en una casa inteligente, lo que provoca falsas alarmas	https://ieeexplore.ieee.org/document/9438543
4	Preetha Thulasiraman	2022	La marina	A través de experimentos, se demuestró que los ataques cibernéticos que envían un alto volumen de paquetes maliciosos pueden ser identificados con alta precisión y en tiempo real para abordar inmediatamente la intrusión	Con la incorporación de nuevas tecnologías "inteligentes" se añaden riesgos adicionales en forma de ciberataques	https://ieeexplore.ieee.org/document/9773814/authors#authors
5	Tolijan Trajanovski; Ning Zhang	2021	Internet de las cosas (IoT)	El marco consiste en honeypots integrados con un nuevo sandbox que admite una amplia gama de configuraciones de hardware y software, y puede identificar indicadores de compromiso y ataque, junto con técnicas anti-análisis,	La eficacia de las sandboxes propuestas está limitada por el uso potencial de técnicas de anti-análisis y la incapacidad para identificar características para una detección e identificación eficaces de botnets de IoT	https://ieeexplore.ieee.org/document/9529169

				persistencia y anti-forense		
6	Benedetta Gottardelli	2024	Instituciones sanitarias	En este documento proponemos GEmelli GeNerator - Real World Data (GEN-RWD) Sandbox, que proporciona un entorno seguro para el análisis de datos sin comprometer los datos médicos sensibles.	El intercambio de datos entre entidades sanitarias puede abordar este problema, pero las preocupaciones jurídicas, de privacidad y de propiedad de los datos dificultan ese enfoque.	https://ieeexplore.ieee.org/document/10628842/authors#authors

Nota. Resumen de los trabajos identificados como literatura para el presente trabajo de investigación. Elaboración propia

2.2. Marco Teórico

2.2.1. Sistema Sandbox

Un sistema Sandbox es definido como un entorno de ejecución aislado diseñado para analizar, probar y contener software potencialmente malicioso sin comprometer la seguridad del sistema principal (Cisneros, 2024). Respecto a su funcionamiento se basa en la creación de un espacio virtual donde las aplicaciones pueden ejecutarse sin afectar los archivos o configuraciones del equipo anfitrión (Guthrie, 2024). De acuerdo con este criterio, se constituye como una tecnología ampliamente usada en el contexto de ciberseguridad para evaluar amenazas como virus, malware y exploits antes de permitir su acceso a la red corporativa.

Por su parte Abdishakur (2024) lo conceptualiza como un entorno de prueba seguro en el que, incluso si algo sale mal, no dañará directamente sus máquinas host, sistemas operativos, aplicaciones o datos. El entorno de prueba funciona como una caja de arena metafórica en la que se puede jugar con el sistema para ver cómo funciona.

Ahora bien, la mayoría de los autores identifica a los sandbox como “entornos aislados”, debido a que estos están separados del sistema principal en las estaciones de trabajo o hosts. Esto permite al usuario probar software, abrir archivos sospechosos, realizar pruebas de malware, entre otros, en un ambiente controlado y completamente aislado del sistema en producción. Por otro lado, ofrecen ahorros de costos, ya que mantener un entorno separado para las pruebas es más costoso que crear un espacio aislado. Abdishakur (2023) indica que los sandboxes permiten a los desarrolladores y evaluadores trabajar de manera más eficiente al proporcionar un entorno dedicado para pruebas y experimentación.

Independientemente de cómo se utilice un sandbox, todos los entornos se ejecutan con la misma característica, el aislamiento. El sandboxing consiste en aislar el código o la aplicación que se está probando o analizando del resto del sistema (Hornetsecurity, 2023).

En cuanto a los beneficios, el principal de ellos es su capacidad para detectar comportamientos sospechosos en tiempo real, lo que admite la prevención de ataques antes de que afecten la infraestructura de una organización. A diferencia de los métodos tradicionales de seguridad, como los antivirus, que operan con bases de datos de firmas conocidas, un Sandbox permite analizar amenazas nuevas o desconocidas mediante técnicas avanzadas de comportamiento (Quevedo y Cárdenas, 2022). Esto lo convierte en una herramienta fundamental para enfrentar ciberataques preferidos.

En entornos empresariales, los sistemas Sandbox se implementan en servidores, gateways de correo electrónico y plataformas de análisis forense digital para examinar archivos y enlaces sospechosos sin riesgo. También se utilizan en el desarrollo de software

para probar aplicaciones en diferentes escenarios sin comprometer el sistema operativo. Su versatilidad y eficacia se han convertido en esta solución en un estándar dentro de la seguridad informática moderna (Swamy, 2020).

No obstante, Asensi (2024) el uso de un "sistema Sandbox no es infalible, ya que los ciberdelincuentes han desarrollado técnicas para evadir su detección, como la ejecución retardada de malware o la verificación del entorno de ejecución" (p. 10). Por ello, se recomienda utilizar esta tecnología en conjunto con otras estrategias de ciberseguridad, como la inteligencia de amenazas y el monitoreo de red, para fortalecer la protección contra ataques avanzados.

2.2.2. Incidentes de seguridad

Los incidentes de seguridad en el ámbito tecnológico, tal como mencionan Chamorro et al. (2023) se refieren a "cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de la información en un sistema informático" (p. 12). Estos pueden ser causados por ataques malintencionados, errores humanos, fallos en la infraestructura o vulnerabilidades en el software. La creciente digitalización y conectividad han aumentado exponencialmente la frecuencia y sofisticación de estos incidentes.

En este orden, Rosencrance (2019), los incidentes de seguridad "son eventos que pueden indicar que los sistemas o los datos de una organización han sido comprometidos o que las medidas implementadas para protegerlos han fallado" (p. 2).

En TI, un evento de seguridad es algo que tiene importancia para el hardware o software del sistema, y un incidente es un evento que interrumpe las operaciones normales.

Los eventos de seguridad generalmente se distinguen de los incidentes de seguridad por el grado de gravedad y el riesgo potencial asociado para la organización.

En el artículo de Navarro (s.f) define que, un incidente de seguridad es cualquier "evento que puede afectar la integridad, la confidencialidad o la disponibilidad de los datos o sistemas de una organización", según la Organización Internacional de Normalización (ISO) y la Comisión Internacional de Electrotecnia (IEC). En otras palabras, es cuando la seguridad de tus datos o sistemas se ve amenazada o comprometida.

Entre los tipos más comunes de incidentes de seguridad se encuentran el malware, los ataques de phishing, las violaciones de datos, los accesos no autorizados y las denegaciones de servicio (DDoS). Cada uno de estos incidentes representa una amenaza significativa para las organizaciones, ya que pueden generar pérdidas económicas, daños reputacionales y problemas legales derivados del incumplimiento de normativas de protección de datos (Conforme et al., 2023).

La gestión de incidentes de seguridad es un proceso fundamental dentro de cualquier estrategia de ciberseguridad. Este proceso incluye la identificación, análisis, contención, erradicación y recuperación del sistema afectado, así como la implementación de medidas preventivas para evitar futuras vulnerabilidades (Nadeem et al., 2023). La rapidez y eficacia en la respuesta a estos incidentes pueden marcar la diferencia entre una afectación menor y una crisis informática grave.

Para mitigar el impacto de los incidentes de seguridad, las organizaciones deben adoptar un enfoque proactivo basado en la capacitación del personal, el uso de herramientas avanzadas de detección y monitoreo, y la aplicación de protocolos de respuesta bien

estructurados (Chamorromo et al., 2023). Es fundamental contar con soluciones como sistemas de prevención de intrusos (IPS), firewalls y entornos aislados como los sistemas Sandbox para contener amenazas antes de que se propaguen en la infraestructura.

2.2.3. Información en el área de soporte técnico

En el área de soporte técnico, tal como refiere Torres (2020) en su investigación "la información es un activo crítico que debe gestionarse de manera segura y eficiente para garantizar la continuidad operativa y la protección de los sistemas informáticos" (p.87). Este departamento es responsable de atender incidentes, resolver problemas técnicos y asegurar el correcto funcionamiento de los recursos tecnológicos en una organización. La información que manejan puede incluir credenciales de acceso, configuraciones de red y registros de incidentes de seguridad (Patiño, 2020).

Uno de los mayores desafíos en el soporte técnico es la protección de la información sensible frente a accesos no autorizados y posibles filtraciones. Debido a la naturaleza de su trabajo, los técnicos deben tener acceso a datos confidenciales, lo que los convierte en un objetivo atractivo para los ciberdelincuentes (Cervera y Goussens, 2024). Las estrategias de ingeniería social, como el phishing y el pretesting, suelen dirigirse a estos equipos con el fin de obtener credenciales de alto nivel (Swamy, 2020).

Para minimizar estos riesgos, es fundamental implementar protocolos estrictos de manejo de información, como el uso de autenticación multifactor, políticas de privilegios mínimos y cifrado de datos. En este sentido, el personal de soporte debe recibir capacitación continua en buenas prácticas de seguridad y estar preparado para identificar intentos de fraude o intrusión (Espinoza et al., 2022).

El uso de herramientas tecnológicas avanzadas, como sistemas de monitoreo en tiempo real y entornos seguros como el Sandbox, permite mejorar la eficiencia del soporte técnico y reducir los riesgos asociados a la manipulación de información crítica (Quevedo y Cárdenas, 2024). Al integrar estas soluciones, las organizaciones pueden garantizar un entorno de trabajo más seguro y minimizar el impacto de posibles incidentes de seguridad en su infraestructura tecnológica.

2.2.4. Seguridad de la información

Fruhlinger (2020) hace referencia a una descripción más completa del Instituto SANS que dice: “La seguridad de la información se refiere a los procesos y metodologías que se diseñan e implementan para proteger la información o los datos impresos, electrónicos o de cualquier otra forma confidenciales, privados y sensibles contra el acceso, uso, uso indebido, divulgación, destrucción, modificación o interrupción no autorizados.”.

Según un artículo elaborado por Holdsworth y Kosinski (2024) los términos seguridad de la información, seguridad informática, ciberseguridad y seguridad de los datos se utilizan a menudo (y erróneamente) indistintamente. Si bien estos campos se superponen y se informan entre sí, difieren principalmente en su alcance.

La seguridad de la información es un término general que abarca los esfuerzos de una organización para proteger la información. Incluye seguridad de activos de TI físicos, seguridad de endpoints, cifrado de datos, seguridad de red y más.

La seguridad informática también se ocupa de proteger los activos informáticos físicos y digitales y los centros de datos, pero no incluye la protección del almacenamiento de archivos en papel y otros medios. Se centra en los activos tecnológicos más que en la

información en sí. La ciberseguridad se centra en la seguridad de los sistemas de información digital. El objetivo es ayudar a proteger los datos y activos digitales de las ciber amenazas. Si bien se trata de una empresa enorme, la ciberseguridad tiene un alcance limitado, ya que no se ocupa de proteger los datos en papel o analógicos. La seguridad de los datos es la práctica de proteger la información digital del acceso no autorizado, la corrupción o el robo a lo largo de todo su ciclo de vida. Incluye la seguridad física del hardware y los dispositivos de almacenamiento, junto con los controles administrativos y de acceso. También cubre la seguridad lógica de las aplicaciones de software y las políticas y procedimientos de la organización.

En el artículo elaborado por Corbo (2021) menciona que: El Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) ha enumerado los cinco objetivos de la seguridad de la información: confidencialidad, disponibilidad, integridad, responsabilidad y garantía. Estos cinco objetivos se han instituido para permitir que todas las organizaciones cumplan con los objetivos de la misión al reconocer los riesgos relacionados con TI para la organización, sus socios y los clientes.

2.2.5. Análisis de riesgos

La mitigación de riesgos es 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 y Downie, 2024) La mitigación de riesgos surge cuando admitimos que un determinado riesgo no puede ser eliminado, y que debemos

convivir con él, pero en condiciones en las que no nos pueda causar el impacto negativo que se pronosticó inicialmente (Escuela Europea de Excelencia, 2021).

Cuando se habla de ciberseguridad, el análisis de riesgos informáticos es la evaluación de los distintos peligros que afectan a nivel informático y que pueden producir situaciones de amenaza al negocio, como robos o intrusiones que comprometan los datos o ataques externos que impidan el funcionamiento de los sistemas propiciando periodos de inactividad empresarial (Rodríguez, 2020).

2.3. Marco legal

El marco legal que sustenta esta investigación se enmarca en la seguridad informática, la cual está regulada por diversas normativas que establecen directrices para la protección de datos y la mitigación de riesgos cibernéticos. En esta línea, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2002) establece la validez legal de la información electrónica y dispone medidas para garantizar su integridad y autenticidad. Por otra parte, el Código Orgánico Integral Penal (2014) tipifica delitos informáticos, como el acceso no autorizado a sistemas, la difusión de malware y la violación de datos personales, imponiendo sanciones para prevenir ataques informáticos que afectan tanto a instituciones públicas como privadas.

En el ámbito privado, la Ley Orgánica de Protección de Datos Personales (2021) refuerza la necesidad de adoptar mecanismos de seguridad para resguardar la información de los usuarios, estableciendo principios de confidencialidad, disponibilidad e integridad. Estas disposiciones respaldan la implementación de soluciones tecnológicas, como sistemas sandbox, que permiten la detección y neutralización de software malicioso. La Norma

Técnica Ecuatoriana INEN-ISO/IEC 27001 establece estándares para la gestión de la seguridad de la información en organizaciones públicas y privadas, alineándose con las mejores prácticas internacionales (NTE INEN-ISO/IEC, 2017).

CAPITULO III

MARCO METODOLÓGICO

En el mundo actual, las organizaciones se enfrentan constantemente con el desafío de proteger el activo más importante que es la información, sobre todo los datos críticos de amenazas externas como ciberdelincuentes, quienes desean acceder a esta información utilizando varias técnicas de ataque que cada día son más sofisticadas. Además, el usuario al ser considerado el eslabón más débil de la cadena de seguridad, el cumplir con este desafío, se vuelve mucho más exigente para cada organización. Las acciones de éstos, normalmente por desconocimiento o ignorancia, hace que exista una sobrecarga en los equipos de trabajo que conforman las áreas de soporte técnico a usuarios, quienes deben buscar medidas de seguridad que mitiguen el riesgo significativo al que se enfrentan las organizaciones debido a estas acciones.

Para contrarrestar esta problemática, se ha pretendido exponer como solución, la implementación de un sistema sandbox para el área de soporte técnico a usuarios, dónde se de atención a los requerimientos de seguridad expuestos por los usuarios de la organización de una manera aislada en un ambiente controlado permitiendo evaluar así el riesgo de cada requerimiento y permitiendo evadir el riesgo que presente cada uno.

3.1. Descripción del área de estudio

El área de estudio en el que se ha centrado este proyecto de investigación ha sido el área de soporte técnico a usuarios de empresas públicas o privadas. Para esto, se ha tomado como base el reporte de requerimientos en la mesa de servicios de atención técnica a usuarios de una institución del sector público de por lo menos un año.

El estudio se ha centrado en analizar los requerimientos comunes sobre seguridad informática en el reporte de una organización pública, en cuanto a vulnerabilidades que se presentan a nivel de usuario final y compararlo con la información de artículos encontrados en la literatura investigada, donde los autores detallen cuáles son los requerimientos más comunes reportados en las áres de soporte técnico a usuarios. El sistema sandbox que se escoja de los evaluados, debe permitir realizar la evaluación y atención a dichos requerimientos para mitigar el riesgo de ejecución de amenazas en el entorno corporativo.

3.1.1. Descripción del grupo de estudio

El grupo de estudio está compuesto por profesionales del área de soporte técnico a usuarios en organizaciones públicas o privadas. A través del análisis de reportes de incidentes, se busca comprender los desafíos más frecuentes en seguridad informática y evaluar la efectividad de un sistema sandbox en este contexto.

3.2. Enfoque y tipo de investigación

El enfoque de la investigación fue documental, se basó en una revisión bibliográfica que integró el análisis de artículos cuyas metodologías y hallazgos se fundamentaron en métodos cualitativos y cuantitativos. Se sustentó en datos obtenidos de casos reportados

sobre seguridad informática en áreas de soporte a usuarios de una organización del sector público, combinando análisis estadísticos y cualitativos.

Esta respondió a la elección de un sistema sandbox de código abierto o propietario, que mejor se adapte a las necesidades identificadas en la fase de análisis, con el fin de minimizar la incidencia de incidentes de seguridad mediante un enfoque basado en la gestión de riesgos. Además, los hallazgos y el desarrollo de la investigación se presentan a profesionales del área de estudio para obtener su retroalimentación, lo que refuerza el carácter cualitativo del estudio.

Para la gestión de incidentes y riesgos se ha adoptado como sustento metodológico la ISO/IEC 27005:2022, un enfoque estructurado diseñado específicamente para la gestión de riesgos en seguridad de la información. Esta norma proporciona un marco detallado para la identificación, análisis y tratamiento de riesgos, asegurando que las organizaciones puedan implementar controles adecuados para minimizar amenazas. Su aplicación permite evaluar vulnerabilidades, determinar el impacto potencial de incidentes y establecer medidas de mitigación eficaces. Además, su integración con la norma ISO/IEC 27001 garantiza la alineación con los principios de gestión de seguridad de la información, promoviendo una protección robusta y adaptable a distintos entornos organizacionales.

Por otro lado, también se implementó la metodología NIST 800-61 para la gestión de incidentes de seguridad, estableciendo procedimientos claros para la detección, análisis, respuesta y recuperación ante eventos adversos. Este enfoque facilita la identificación temprana de incidentes, su clasificación según la criticidad y la aplicación de medidas correctivas que minimicen el impacto en las operaciones. La documentación detallada y el

aprendizaje a partir de incidentes previos optimizan la capacidad de respuesta ante futuros eventos, permitiendo una mejora continua en la seguridad de la infraestructura tecnológica.

En este contexto, la selección de un enfoque metodológico adecuado es fundamental para garantizar la continuidad operativa y la protección de la información. Es por ello por lo que se ha optado por ISO/IEC 27005:2022 y NIST 800-61, debido a su enfoque complementario en la gestión de riesgos e incidentes. Mientras que ISO/IEC 27005:2022 permite una evaluación estructurada de los riesgos en seguridad de la información, NIST 800-61 proporciona directrices claras para la respuesta y mitigación de incidentes de ciberseguridad. La combinación de ambas metodologías fortalece la resiliencia organizacional y optimiza la capacidad de reacción ante amenazas emergentes en infraestructuras tecnológicas críticas.

3.3. Procedimiento de investigación

Para el presente proyecto, se definió las siguientes fases de investigación:

Fase 1: Análisis de incidentes de seguridad comunes

Se realizó una exhaustiva investigación de los incidentes de seguridad reportados en el área de soporte técnico a usuarios, utilizando datos recopilados en un informe del sistema de mesa de servicios de una empresa del sector público durante dos años. Se comparó esta información con requerimientos identificados en la literatura especializada, identificándose patrones consistentes en ataques de malware, phishing y accesos no autorizados. Se estableció un grupo de requerimientos esenciales para la mitigación de amenazas a partir de

dicha comparación. Los datos permitieron reconocer la necesidad de automatizar la detección y contención de incidentes.

La investigación evidenció la relevancia de contar con mecanismos preventivos en entornos críticos. Estos hallazgos sirvieron de base para el desarrollo de una propuesta integral en seguridad informática. La información recopilada fue fundamental para orientar la formulación de estrategias de mitigación.

Esta fase metodológica se estructuró siguiendo los estándares ISO 27005 y NIST 800-61, garantizando un tratamiento sistemático de los riesgos e incidentes. Se inició con la identificación y análisis de riesgos mediante la revisión de evaluaciones de vulnerabilidades en la infraestructura. Posteriormente, se clasificaron las amenazas y vulnerabilidades utilizando una matriz de evaluación robusta.

Lo anterior se complementó con el formato de la matriz de evaluación de riesgos del Esquema Gubernamental de Seguridad de la Información (EGSI), la cual se estructuró para identificar de forma sistemática la vulnerabilidad y criticidad de cada activo. Se definieron categorías que integraban el impacto, la probabilidad y la capacidad de mitigación, asignando puntajes a cada activo según los criterios establecidos. Se procedió a analizar de manera detallada las amenazas asociadas a cada recurso y su efecto potencial en términos de confidencialidad, integridad y disponibilidad.

La matriz permitió visualizar la relación entre amenazas, vulnerabilidades y controles implementados, facilitando la priorización de acciones correctivas. Cada activo fue evaluado utilizando escalas numéricas que aseguraban la comparación objetiva entre

diferentes escenarios. Esta metodología proporcionó una base sólida para optimizar la asignación de recursos y enfocar esfuerzos en los puntos críticos. Además, el uso de esta herramienta mejoró la transparencia del proceso de análisis de riesgos.

El proceso de evaluación consistió en recolectar datos relevantes sobre cada activo, identificando su valor, función y la información que manejan. Se identificaron las amenazas específicas—como ataques de malware, fallos técnicos y errores humanos—y se evaluó la probabilidad de su ocurrencia mediante escalas predefinidas.

El impacto de cada amenaza se cuantificó en términos de pérdida de confidencialidad, integridad y disponibilidad (CID), integrando criterios tanto cualitativos como cuantitativos. La matriz del EGSI permitió combinar estos factores en un modelo único, facilitando un análisis comparativo entre distintos activos y escenarios. Cada combinación de amenaza, vulnerabilidad e impacto generó un puntaje final que reflejaba el nivel de riesgo. Este enfoque sistemático aseguró que ninguna variable relevante quedara sin evaluar. En consecuencia, se establecieron prioridades claras para la implementación de controles de seguridad.

La aplicación de la matriz de evaluación de riesgos del EGSI se tradujo en un análisis detallado y transparente que apoyó la toma de decisiones estratégicas en la organización. Se documentaron todas las variables y se generaron reportes visuales que mostraron la distribución y evolución de riesgos en el tiempo. Los resultados permitieron identificar áreas de mejora y oportunidades para optimizar la seguridad informática, facilitando ajustes dinámicos en la estrategia de mitigación. Las recomendaciones basadas

en la matriz se centraron en reducir los niveles de riesgo residuales y fortalecer los controles existentes.

Este enfoque integral fortaleció la capacidad de respuesta ante incidentes, mejoró la asignación de recursos y promovió una cultura de seguridad. En definitiva, la utilización de esta herramienta se demostró esencial para la gestión efectiva de riesgos en el entorno tecnológico. La implementación se realizó en un entorno controlado para garantizar la efectividad de la solución propuesta, esta se llevó a cabo bajo la supervisión de dos expertos quienes validaron la implementación utilizando una matriz de validación basada en métricas predefinidas (ver anexo 1).

Fase 2: Evaluación de sistemas Sandbox opensource o propietario que cumplan con requerimientos identificados

Se evaluó varios sistemas Sandbox opensource o propietario, buscando que cumplan con los requerimientos identificados en la fase de análisis con el objetivo de minimizar el número de incidencias de seguridad identificados en base a un análisis de riesgos.

Fase 3: Validación de la implementación del sistema Sandbox

Se validó la propuesta del sistema Sandbox escogido al final de la fase de evaluación, mediante la calificación de expertos en seguridad informática y experiencia en el área de soporte técnico a usuarios. (Ver anexo 1). Se elaboró un informe donde se argumentó los diferentes hallazgos y la efectividad del sistema para reducir los incidentes de seguridad

utilizando métricas predefinidas; y se envió a dos profesionales del área de soporte a usuarios para obtener la retroalimentación del criterio de cada uno.

3.4. Consideraciones bioéticas

En el proyecto de investigación se tomaron en cuenta consideraciones bioéticas, permitiendo asegurar que la información obtenida del reporte de la empresa pública tomada en cuenta para el proyecto sea utilizada de manera confidencial. Así también, se explicó claramente a la empresa, así como a los profesionales del área, el objeto para lo que se solicitó la información y el criterio de cada profesional en el área de estudio. La información en resultados que se presenta, no se mencionan nombres de las instituciones debido a la consideración de confidencialidad, ni se exponen informaciones que comprometan a las mismas.

CAPITULO IV

RESULTADOS Y DISCUSIÓN

4.1. Análisis de los incidentes de seguridad reportados en el área de soporte técnico a usuarios (identificación de los requerimientos más comunes y que pueden ser mitigados con la implementación de un sistema Sandbox)

En este apartado se presentan los resultados que corresponden al objetivo específico de analizar los incidentes de seguridad reportados en el área de soporte técnico a usuarios. Para dar inicio con el trabajo de investigación, se ha solicitado un reporte de los requerimientos reportados en el sistema de mesa de servicios de empresas públicas y privadas, donde se ha obtenido el reporte de 2 años de una empresa del sector público. Del

reporte obtenido se ha procedido a revisar todos los que se encuentran dentro de la categoría de seguridad informática.

Después de la revisión indicada, se ha obtenido el siguiente listado de incidentes repetitivos de seguridad informática en el reporte de la mesa de servicios en la organización del sector público:

- Revisión de posible spam
- Revisión de posible virus
- Revisión de archivo recibido por correo y que no abre (posiblemente infectado)
- Archivo dañado o virus

Los incidentes de seguridad informática detectados en la empresa se clasificaron en dos matrices que permiten analizar su impacto y frecuencia. En la Tabla 2, se identifican diez tipos de incidentes, entre los que destacan los intentos no autorizados de acceso, ataques de escalada de privilegios, amenazas internas, ataques de phishing, malware y ataques de denegación de servicio (DoS). Además, se incluyen incidentes más sofisticados, como ataques de hombre en el medio (MitM), ataques a aplicaciones web y amenazas persistentes avanzadas (APT).

Por otro lado, la Tabla 3 presenta una definición más concreta de los incidentes comunes reportados en la organización. Se destacan los ataques de malware, spam y phishing, amenazas internas, intentos no autorizados de acceso y ataques de contraseña. La comparación entre ambas tablas permite establecer un marco de referencia para la implementación de controles y estrategias de mitigación dentro del entorno corporativo.

El análisis de estas matrices es fundamental para identificar patrones de ataque y desarrollar medidas preventivas basadas en la gestión de incidentes. La presencia recurrente de amenazas internas y ataques de phishing sugiere la necesidad de reforzar la concienciación del personal y mejorar las políticas de autenticación. Asimismo, la detección de APT y ataques a aplicaciones web resalta la importancia de implementar herramientas avanzadas de monitoreo y respuesta ante incidentes.

Tipos de incidentes de ciberseguridad

Tabla 2

Matriz: Tipos de incidentes

Nº	Tipo de Incidente
1	Intentos no autorizados de acceso a sistemas o datos
2	Ataque de escalada de privilegios
3	Amenaza interna
4	Ataque de phishing
5	Ataque de malware
6	Ataque de denegación de servicio (DoS)
7	Ataque de hombre en el medio (MitM)
8	Ataque de contraseña
9	Ataque de aplicaciones web
10	Amenaza persistente avanzada (APT)

Nota: Elaboración propia. Adaptado de Rosencrance (2019)

Tabla 3

Definición de incidentes comunes de seguridad informática

Nº	Tipo de Incidente
1	Ataques de malware

2	Ataques de spam y phishing
3	Amenaza interna
4	Intentos no autorizados de acceso a sistemas o datos
5	Ataque de contraseña

Nota: Elaboración propia. Adaptado de Rosencrance (2019)

A partir de la identificación de los tipos de incidentes comunes de seguridad informática, se presenta en la tabla 4 la evaluación del activo, la cual admitió el análisis de riesgos en función al nivel de amenaza, vulnerabilidad e impacto en la perdida de confiabilidad, integridad y disponibilidad (CID). En esta línea, se observó un patrón donde el impacto incrementó exponencialmente a medida que se combinaron valores altos en amenaza y vulnerabilidad; esto alcanzó, un máximo de 27 en el peor escenario. Tal progresión multiplicativa indicó que los activos con mayores riesgos requieren prioridad en seguridad. Ahora bien, respecto a los valores más bajos, se mostraron riesgos manejables, sin embargo, ameritan medidas de mitigación.

La siguiente matriz constituyó un instrumento que facilitó la exposición de resultados respecto a la identificación de activos críticos y la toma de decisiones estratégicas.

Tabla 4
Evaluación del activo

Tabla de evaluación del activo										
Nivel de Amenaza		Bajo (1)			Medio (2)			Alto (3)		
Nivel de Vulnerabilidades		Bajo (1)	Medio (2)	Alto (3)	Bajo (1)	Medio (2)	Alto (3)	Bajo (1)	Medio (2)	Alto (3)
Valor del impacto en términos de la pérdida de (CID) en los activos	Bajo (1)	1	2	3	2	4	6	3	6	9
	Medio (2)	2	4	6	4	8	12	6	12	18
	Alto (3)	3	6	9	6	12	18	9	18	27

1	3	**BAJO**
4	8	**MEDIO**
9	27	**ALTO**

Evaluación del Riesgo
Proceso de comparación del riesgo estimado contra un criterio de riesgo calculado dado para determinar la importancia del riesgo. El grado del riesgo es expresado numéricamente basado en las medidas del valor de los activos de información, el impacto de la amenaza y el alcance de la vulnerabilidad.

Fórmula para calcular el grado de riesgo
Riesgo actual = Valor del activo de la información (CID) x Amenaza x Vulnerabilidad

Nota: Adaptado del informe de evaluación y tratamiento de riesgos esquema gubernamental de seguridad de la información (EGSI versión 2.0- 2025)

En este sentido, respecto a la reducción de riesgos, se recomienda priorizar la seguridad en activos con valores altos mediante controles como actualizaciones, monitoreo y segmentación de red. La implementación de firewalls avanzados, sistemas de detección de intrusos y entornos sandbox puede minimizar la exposición a amenazas.

Tabla 5

Valoración de impacto en los activos de la información

Tabla de valoración de Impacto en los activos de la información	
Valoración del impacto en términos de la perdida de la <u>confidencialidad</u>	**Criterio**
Alto (3)	La divulgación no autorizada de la información tiene un efecto critico para la institución Ej. Divulgación de información confidencial o sensible.
Medio (2)	La divulgación no autorizada de la información tiene un efecto limitado para la institución Ej. Divulgación de información de uso interno
Bajo (1)	La divulgación de la información no tiene ningún efecto para la institución Ej. Divulgación de información pública.
Valoración del impacto en términos de la perdida de la <u>integridad</u>	**Criterio**

Alto (3)	La destrucción o modificación no autorizada de la información tiene un efecto severo para la institución
Medio (2)	La destrucción o modificación no autorizada de la información tiene un efecto considerable para la institución
Bajo (1)	La destrucción o modificación de la información tiene un efecto leve para la institución
Valoración del impacto en términos de la perdida de <u>disponibilidad</u>	**Criterio**
Alto (3)	La interrupción al acceso de la información o los sistemas tienen un efecto severo para la institución
Medio (2)	La interrupción al acceso de la información o los sistemas tienen un efecto considerable para la institución
Bajo (1)	La interrupción al acceso de la información o los sistemas tienen un efecto mínimo para la institución

Nota: Adaptado del informe de evaluación y tratamiento de riesgos esquema gubernamental de seguridad de la información (EGSI versión 2.0- 2025)

En la tabla 5 se presentan los resultados obtenidos a partir de la valoración de impacto en los activos de la información, esto permitió categorizar el nivel de afectación en caso de pérdida de confidencialidad, integridad o disponibilidad. En términos de confidencialidad, la divulgación no autorizada de información puede generar impactos críticos, como la exposición de datos sensibles que afectan la seguridad y reputación de la institución.

En este sentido, un impacto medio implica la filtración de información interna, lo que podría comprometer ciertos procesos sin generar una crisis mayor. En cambio, un impacto bajo se da cuando la información divulgada es de acceso público y no representa un riesgo significativo para la organización. Desde el contexto de la integridad, la

alteración o destrucción de datos, los resultados reflejaron que puede tener consecuencias graves si compromete información crítica para la toma de decisiones o la operatividad de la institución. Un impacto alto significa que la modificación de datos puede causar pérdidas económicas, legales o reputacionales severas.

Ahora bien, en un nivel medio, la alteración de la información tiene un efecto considerable, pero no llega a paralizar las operaciones completamente. Si el impacto es bajo, la modificación o eliminación de datos solo genera inconvenientes menores sin afectar de manera significativa la continuidad del negocio.

Respecto a la disponibilidad, la interrupción del acceso a la información o los sistemas puede afectar seriamente la operatividad de la institución. Un impacto alto implica que la indisponibilidad de los sistemas clave genera pérdidas significativas, como la interrupción de servicios esenciales. Un nivel medio de impacto representa una afectación considerable, pero con soluciones alternativas para mitigar el problema. En definitiva, un impacto bajo se da cuando la indisponibilidad es mínima y no compromete el desarrollo normal de las actividades. Esta clasificación permite priorizar medidas de protección según la criticidad de cada activo.

Tabla 6
Estimación de amenazas

Nivel de amenazas	Criterio por probabilidad	Criterio por condición de ocurrencia	Criterio por atractivo	Ejemplo
Alto (3)	La ocurrencia es muy probable (probabilidad > 50%)	Bajo circunstancias normales	El atacante se beneficia en gran medida por el ataque, tiene la capacidad	Código malicioso

			técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable	
Medio (2)	La ocurrencia es probable (probabilidad =50%)	Por errores descuidos	El atacante se beneficia de alguna manera por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable	Falla de hardware
Bajo (1)	La ocurrencia es menos probable (probabilidad >0 y <50%)	en rara ocasión	El atacante no se beneficia del ataque	desastres naturales

Nota: Adaptado del informe de evaluación y tratamiento de riesgos esquema gubernamental de seguridad de la información (EGSI versión 2.0- 2025)

La tabla 6 refleja lo relacionado a la estimación de amenazas, en esta se admitió la evaluación del nivel de riesgo al que están expuestos los activos de información, para ello se consideraron 3 criterios: (1) probabilidad de ocurrencia, (2) condición en la que se presenta y (3) atractivo para un atacante. En este sentido, un nivel alto de amenaza implica que la probabilidad de ocurrencia es superior al 50%, se presenta en condiciones normales y es altamente atractivo para un atacante, ya que le otorga beneficios significativos y cuenta con las capacidades técnicas para explotarla. Un ejemplo de ello para este nivel es el código malicioso, ya que su ejecución es frecuente y puede causar graves daños a la infraestructura.

En cuanto a un nivel medio de amenaza, corresponde a eventos con una probabilidad del 50%, que ocurren por errores o manifiestos humanos y son aprovechables por un atacante con los conocimientos adecuados, no obstante; no es un valor tan alto como

en el nivel anterior. Se puede mencionar como ejemplo, una falla de hardware, que puede derivar en la pérdida temporal o permanente de datos, lo que afectaría la operatividad del sistema sin que necesariamente haya una intención maliciosa detrás del suceso.

En este orden, se evidencia que un nivel bajo de amenaza se asigna a eventos cuya probabilidad es menor al 50% y que ocurren en raras ocasiones, tal como los desastres naturales. Para este tipo de casos, el atacante no obtiene ningún beneficio o ventaja de su ocurrencia, por lo que no existe una motivación malintencionada detrás del evento. Si bien la ocurrencia de estos sucesos es menos frecuente, sus impactos pueden ser catastróficos si no se cuenta con planes de contingencia adecuados.

Tabla 7
Estimación de vulnerabilidades

Nivel de vulnerabilidad	Criterio	Ejemplo
Alto (3)	No existe ninguna medida de seguridad implementada para prevenir la ocurrencia de la amenaza	No se utilizan contraseñas para que los usuarios ingresen a los sistemas
Medio (2)	Existen medidas de seguridad implementadas que no reducen la probabilidad de ocurrencia de la amenaza a un nivel aceptable	Existen normas para la utilización de contraseñas, pero no se implementa
Bajo (1)	La medida de seguridad es adecuada	Existen normas para la utilización de contraseñas y es aplicada

Nota: Adaptado del informe de evaluación y tratamiento de riesgos esquema gubernamental de seguridad de la información (EGSI versión 2.0- 2025)

En la tabla 7 se presentan los resultados de la estimación de vulnerabilidades, esta permitió llevar a cabo la evaluación del grado de exposición de un sistema o activo ante posibles amenazas, considerando la efectividad de las medidas de seguridad

implementadas. En este orden, se conoce que un nivel alto de vulnerabilidad indica la ausencia total de mecanismos de protección, lo que deja al sistema completamente expuesto a ataques. Por ejemplo, en este nivel, es importante no utilizar contraseñas para el acceso a sistemas, ya que le permitiría a cualquier persona ingresar sin restricciones, aumentando significativamente el riesgo de accesos no autorizados y posible.

Respecto al nivel medio de vulnerabilidad se evidenció que esta se presenta cuando existen medidas de seguridad, pero no son aplicadas de manera efectiva, lo que resulta en que no se reduce el riesgo a un nivel aceptable. Un ejemplo representativo sería contar con normas para el uso de contraseñas, sin embargo; no se implementarían en la práctica. Esto deja abierta la posibilidad de accesos indebidos y compromete la integridad y confidencialidad de los datos, evidenciando la necesidad de fortalecer los controles de cumplimiento y monitoreo dentro de la organización.

Sobre un nivel bajo de vulnerabilidad implica que las medidas de seguridad son adecuadas y se aplican correctamente, reduciendo significativamente el riesgo de explotación por parte de los atacantes. Un claro ejemplo de esto es la existencia de normas para la utilización de contraseñas y su implementación efectiva, asegurando que solo usuarios autorizados accedan a los sistemas.

Tabla 8
Amenazas típicas (ISO/IEC 27005:2022)

CATALOGO DE AMENAZAS TÍPICAS Fuente: ISO/IEC 27005:2022		
CATEGORIA	**AMENAZA**	**TIPO DE FUENTE DE RIESGO**
	Amenazas físicas	
Amenazas físicas	Fuego	A, D, E
	Agua	A, D, E
	Contaminación, radiaciones nocivas	A, D, E
	Accidente grave	A, D, E
	Explosión	A, D, E
	Polvo, corrosión, congelación	A, D, E
	Amenazas naturales	
Amenazas naturales	Fenómeno climático	E
	Fenómeno sísmico	E
	Fenómeno volcánico	E
	Fenómeno meteorológico	E
	Inundación	E
	Pandemia/fenómeno epidémico	E
	Fallas en infraestructura	
Fallas en infraestructura	Fallo de un sistema de suministro	A, D
	Fallo del sistema de refrigeración o ventilación	A, D
	Pérdida de suministro eléctrico	A, D, E
	Fallo de una red de telecomunicaciones	A, D, E
	Radiación electromagnética	A, D, E

	Fallo de equipos de telecomunicaciones	A, D
	Radiación térmica	A, D, E
	Pulsos electromagnéticos	A, D, E
	Fallos técnicos	
Fallos técnicos	Fallo del dispositivo o sistema	A
	Saturación del sistema de información	A, D
	Violación de la mantenibilidad del sistema de información	A, D
	Acciones humanas	
Acciones humanas	Terrorismo, Ataque, sabotaje	D
	Ingeniería Social	D
	Interceptación de radiación de un dispositivo	D
	Espionaje remoto	D
	Interceptación de comunicaciones privadas	D
	Robo de soportes o documentos	D
	Robo de equipos	D
	Robo de identidad o credenciales digitales	D
	Recuperación de medios reciclados o desechados.	D
	Divulgación de información	A, D
	Entrada de datos de fuentes no confiables	A, D
	Manipulación de hardware	D
	Manipulación de software	A, D
	"Drive-by exploits" utilizando comunicación basada en web	D
	Ataque de repetición (ataque de playback), ataque de hombre en el medio	D
	Tratamiento no autorizado de datos personales	A, D
	Entrada no autorizada a las instalaciones	D
	Uso no autorizado de dispositivos	D
	Uso incorrecto de los dispositivos	A, D
	Dispositivos o medios dañinos	A, D

	Copia fraudulenta de software	D
	Uso de software falsificado o copiado	A, D
	Corrupción de datos	D
	Tratamiento ilegal de datos	D
	Envío o distribución de malware	A, D, R
	Detección de posición/ubicación	D
	Comprometimiento de funciones o servicios	
Comprometimiento de funciones o servicios	Error en uso	A
	Abuso de derechos o permisos	A, D
	Falsificación de derechos o permisos	D
	Denegación de acciones	D
	Amenazas organizativas	
Amenazas organizativas	Falta de personal	A, E
	Falta de recursos	A, E
	Fallo de los proveedores de servicios	A, E
	Violación de leyes o reglamentos	A, D

Nota: Adaptado del informe de evaluación y tratamiento de riesgos esquema gubernamental de seguridad de la información – Matriz de evaluación de riesgos de seguridad de la información (EGSI versión 3- 2025)

La tabla 8 corresponde a la exposición de resultados del catálogo de amenazas típicas basado en ISO/IEC 27005:2022 esta proporcionó una clasificación estructurada de los principales riesgos que podrían llegar a comprometer la seguridad de la información, abarcando un análisis desde amenazas físicas y naturales hasta fallos técnicos y acciones humanas malintencionadas.

En primer lugar, lo que corresponde a las amenazas físicas incluyen incendios, inundaciones, explosiones y accidentes graves, los cuales pueden afectar la infraestructura crítica de una organización. Para estos casos, tales amenazas generalmente provienen de factores ambientales o fallos en sistemas de seguridad física, por lo que, la vulnerabilidad a estas amenazas puede reducirse mediante sistemas de detección de incendios, redundancia en la infraestructura y planes de contingencia.

Respecto a las amenazas naturales, como terremotos, erupciones volcánicas y pandemias, son difíciles de predecir y mitigar. Sin embargo, estrategias como la geolocalización adecuada de centros de datos, planes de recuperación ante desastres y el almacenamiento de información en la nube pueden reducir significativamente su impacto.

En cuanto al análisis de los fallos en la infraestructura, se mencionaron algunos tales como; cortes de electricidad, fallos en telecomunicaciones y fallas en sistemas de refrigeración, que pueden llegar a causar interrupciones críticas en los sistemas de información. La redundancia de sistemas, el uso de generadores de respaldo y la implementación de infraestructura de telecomunicaciones descentralizada son métodos efectivos de mitigación.

Ahora bien, los fallos técnicos, como la saturación del sistema de información o la violación de su mantenibilidad, podrían llegar a generar tiempos de inactividad y pérdidas económicas, por eso es importante la implementación de mecanismos de monitoreo continuo, pruebas de carga y mantenimiento preventivo como estrategias clave para evitar tales amenazas.

Sobre las amenazas derivadas de la intervención humana, constituyen uno de los mayores riesgos en seguridad de la información. Entre ellas, se pueden mencionar: (1) Ataques malintencionados, dentro de estos se incluyen sabotajes, espionaje, robo de identidad y malware, que pueden ser prevenidos mediante firewalls, autenticación multifactor y capacitación en ciberseguridad. (2) Errores humanos, en estos se evidencian el uso incorrecto de dispositivos, divulgación de información y manipulación de software, que pueden mitigarse con políticas claras de uso de la información y auditorías periódicas. (3) Ataques organizados, se pueden mencionar los relacionados a la ingeniería social, ataques de repetición y ataques man-in-the-middle, que requieren la implementación de tecnologías de detección de intrusos, cifrado robusto y concienciación del personal.

En lo concerniente a los riesgos en esta categoría incluyen abuso de derechos, falsificación de permisos y denegación de acciones. Estos ataques pueden afectar la continuidad operativa y comprometer la integridad de los sistemas. El uso de controles de acceso basados en roles y auditorías regulares ayuda a reducir estos riesgos.

Posteriormente se tienen, los factores internos, estos responden a la falta de personal, escasez de recursos y fallos en proveedores de servicios pueden generar vulnerabilidades

críticas. Por tal razón una gestión verdaderamente adecuada de los recursos humanos y proveedores, junto con la automatización de procesos, mejora la resiliencia organizacional.

Para la evaluación de las vulnerabilidades y amenazas típicas, se lo realizará utilizando el formato de matriz de la ISO /IEC 27005: 2022:

Tabla 9

Vulnerabilidades típicas (ISO/IEC 27005:2022)

CATÁLOGO DE VULNERABILIDADES TÍPICAS
Fuente: ISO/IEC 27005:2022

CATEGORIA	VULNERABILIDAD
	Hardware
Hardware	Mantenimiento insuficiente/instalación defectuosa de los medios de almacenamiento
	Susceptibilidad a la humedad, al polvo y a la suciedad
	Esquemas de reemplazo periódico insuficientes de equipos
	Sensibilidad a la radiación electromagnética
	Control de cambios de configuración, insuficiente
	Susceptibilidad a las variaciones de tensión
	Susceptibilidad a las variaciones de temperatura
	Almacenamiento sin protección
	Falta de cuidado a disposición
	Copia incontrolada
	Software
Software	Pruebas de software inexistentes o insuficientes
	Defectos conocidos en el software
	No “cerrar sesión” al salir de la estación de trabajo
	Eliminación o reutilización de medios de almacenamiento sin un borrado adecuado
	Configuración insuficiente de los registros para fines de seguimiento de auditoría
	Asignación incorrecta de derechos de acceso
	Software ampliamente distribuido
	Interfaz de usuario complicada
	Aplicar programas de aplicación a datos incorrectos en términos de tiempo
	Documentación insuficiente o faltante
	Configuración de parámetros incorrecta
	Fechas incorrectas
	Mecanismos de identificación y autenticación insuficientes (por ejemplo, para la autenticación de usuarios)
	Tablas de contraseñas desprotegidas
	Mala gestión de contraseñas
	Servicios innecesarios habilitados
	Software nuevo o inmaduro

	Especificaciones poco claras o incompletas para desarrolladores
	Control de cambios ineficaz
	Descarga y uso incontrolado de software
	Falta de copias de seguridad o copias de seguridad incompletas
	No producir informes de gestión

	Red
Red	Mecanismos insuficientes para la prueba de envío o recepción de un mensaje
	Líneas de comunicación no protegidas
	Tráfico sensible no protegido
	Cableado de unión deficiente
	Punto único de falla
	Mecanismos ineficaces o falta de identificación y autenticación del remitente y receptor
	Arquitectura de red insegura
	Transferencia de contraseñas en claro
	Gestión inadecuada de la red (resiliencia del enrutamiento)
	Conexiones de red pública no protegidas

	Personal
Personal	Ausencia de personal
	Procedimientos de contratación inadecuados
	Formación en seguridad insuficiente
	Uso incorrecto de software y hardware
	Poca conciencia de seguridad
	Mecanismos de seguimiento insuficientes o faltantes
	Trabajo no supervisado por personal externo o de limpieza
	Ineficaces o falta de políticas para el correcto uso de los medios de telecomunicaciones y mensajería

	Sitio
Sitio	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones
	Ubicación en zona susceptible a inundaciones
	Red eléctrica inestable
	Protección física insuficiente del edificio, puertas y ventanas

	Organización
Organización	Procedimiento formal de alta y baja de usuarios no desarrollado o su implementación es ineficaz
	Proceso formal para la revisión (supervisión) del derecho de acceso no desarrollado, o su implementación es ineficaz
	Disposiciones insuficientes (en materia de seguridad) en contratos con clientes y/o terceros
	Procedimiento de monitoreo de las instalaciones de procesamiento de información no desarrollado o su implementación es ineficaz
	Auditorías (supervisión) no realizadas de forma regular
	Procedimientos de identicación y evaluación de riesgos no desarrollados, o su implementación es ineficaz
	Insuficientes o falta de informes de fallas registrados en los registros del administrador y del operador
	Respuesta inadecuada del servicio de mantenimiento

	Acuerdo de Nivel de Servicio insuficiente o faltante
	Procedimiento de control de cambios no desarrollado, o su implementación es ineficaz
	Procedimiento formal para el control de la documentación del SGSI no desarrollado o su implementación es ineficaz
	No se ha desarrollado un procedimiento formal para la supervisión de registros del SGSI o su implementación es ineficaz
	Proceso formal de autorización de información disponible públicamente no desarrollado, o su implementación es ineficaz
	Asignación inadecuada de responsabilidades de seguridad de la información
	No existen planes de continuidad, o están incompletos, o están desactualizados
	Política de uso del correo electrónico, no desarrollada o su implementación es ineficaz
	Procedimientos para introducir software en sistemas operativos no desarrollados o su implementación es ineficaz
	Procedimientos para el manejo de información clasificada no desarrollados o su implementación es ineficaz
	Las responsabilidades de seguridad de la información no están presentes en las descripciones de trabajo
	Insuficientes o inexistentes disposiciones (relativas a la seguridad de la información) en los contratos con empleados
	Proceso disciplinario en caso de incidente de seguridad de la información no definido, o no funcionando correctamente
	Política formal sobre el uso de computadoras móviles no desarrollada, o su implementación está ineficaz
	Control insuficiente de los activos fuera de las instalaciones
	Insuficiente o falta de política de “escritorio y pantalla despejados”
	La autorización de las instalaciones de procesamiento de información no está implementada o no funciona correctamente
	Mecanismos de seguimiento de violaciones de seguridad no implementados adecuadamente
	Procedimientos para informar debilidades de seguridad no desarrollados o su implementación es ineficaz
	Procedimientos de cumplimiento de disposiciones sobre derechos intelectuales no desarrollados, o su implementación es ineficaz

Nota: Adaptado del informe de evaluación y tratamiento de riesgos esquema gubernamental de seguridad de la información – Matriz de evaluación de riesgos de seguridad de la información (EGSI versión 3- 2025)

En la tabla 9 se presenta el análisis correspondiente al catálogo de vulnerabilidades típicas ISO/IEC 27005:2022, esta se categoriza de la siguiente forma:

Respecto al Hardware, se identificaron vulnerabilidades relacionadas con mantenimiento, susceptibilidad ambiental y control de cambios. También se menciona que factores como almacenamiento sin protección y copias incontroladas pueden facilitar las filtraciones de información.

En cuanto a software, destacan fallas en pruebas, autenticación deficiente y mala gestión de contraseñas. Por otro lado, las vulnerabilidades en la configuración de registros afectan la trazabilidad de incidentes. En cuanto a la falta de copias de seguridad y control ineficaz de cambios generan riesgos operativos.

En esta línea, sobre la red, se evidencia fallas en la protección del tráfico de datos y autenticación de usuarios pueden exponer información sensible. La existencia de puntos únicos de falla compromete la disponibilidad del sistema. En esta línea, respecto al personal, se encontraron deficiencias en contratación y capacitación reducen la conciencia de seguridad. Es aquí donde se evidencia que el uso incorrecto de software y hardware genera riesgos internos. Falta de políticas para telecomunicaciones y mensajería puede facilitar las filtraciones.

En cuanto al análisis del sitio, se evidenciaron factores físicos como ubicación en zonas de riesgo, protección insuficiente y red eléctrica inestable afectan la continuidad operativa. Y respecto a la organización, se reconocen deficiencias en la gestión de accesorios, supervisión y auditorías comprometen la seguridad de la información. Falta de planes de continuidad y políticas de control de documentación afectan la resiliencia organizacional y problemas en la definición de responsabilidades y ausencia de procesos disciplinarios limitan la gestión efectiva de incidentes.

Para la evaluación de activos y análisis de riesgo, se lo realizará utilizando el formato de matriz de evaluación de riesgos del EGSI en su versión 3.

Tabla 10
Amenazas típicas

CATALOGO DE AMENAZAS TÍPICAS
Fuente: ISO/IEC 27005:2022

CATEGORIA	AMENAZA	TIPO DE FUENTE DE RIESGO
Amenazas físicas	Fuego	A, D, E
	Agua	A, D, E
	Contaminación, radiaciones nocivas	A, D, E
	Accidente grave	A, D, E
	Explosión	A, D, E
	Polvo, corrosión, congelación	A, D, E
Amenazas naturales	Fenómeno climático	E
	Fenómeno sísmico	E
	Fenómeno volcánico	E
	Fenómeno meteorológico	E
	Inundación	E
	Pandemia/fenómeno epidémico	E
Fallas en infraestructura	Fallo de un sistema de suministro	A, D
	Fallo del sistema de refrigeración o ventilación	A, D
	Pérdida de suministro eléctrico	A, D, E
	Fallo de una red de telecomunicaciones	A, D, E
	Radiación electromagnética	A, D, E
	Fallo de equipos de telecomunicaciones	A, D
	Radiación térmica	A, D, E
	Pulsos electromagnéticos	A, D, E
Fallos técnicos	Fallo del dispositivo o sistema	A
	Saturación del sistema de información	A, D
	Violación de la mantenibilidad del sistema de información	A, D
Acciones humanas	Terrorismo, Ataque, sabotaje	D
	Ingeniería Social	D
	Interceptación de radiación de un dispositivo	D
	Espionaje remoto	D
	Interceptación de comunicaciones privadas	D
	Robo de soportes o documentos	D
	Robo de equipos	D
	Robo de identidad o credenciales digitales	D
	Recuperación de medios reciclados o desechados.	D
	Divulgación de información	A, D

	Entrada de datos de fuentes no confiables	A, D
	Manipulación de hardware	D
	Manipulación de software	A, D
	"Drive-by exploits" utilizando comunicación basada en web	D
	Ataque de repetición (ataque de playback), ataque de hombre en el medio	D
	Tratamiento no autorizado de datos personales	A, D
	Entrada no autorizada a las instalaciones	D
	Uso no autorizado de dispositivos	D
	Uso incorrecto de los dispositivos	A, D
	Dispositivos o medios dañinos	A, D
	Copia fraudulenta de software	D
	Uso de software falsificado o copiado	A, D
	Corrupción de datos	D
	Tratamiento ilegal de datos	D
	Envío o distribución de malware	A, D, R
	Detección de posición/ubicación	D

D = deliberado
A = accidental
E = ambiental

Nota: Adaptado del informe de evaluación y tratamiento de riesgos esquema gubernamental de seguridad de la información – Matriz de evaluación de riesgos de seguridad de la información (EGSI versión 3- 2025)

En la amplia red de amenazas que acechan la infraestructura tecnológica, tal como se evidencia en la tabla 10, se pueden mencionar las físicas, las cuales emergen como los primeros gigantes a desafiar la integridad de los sistemas, siendo estos: fuego, agua y contaminación se alzan como barreras invisibles, dispuestas a desbordar las líneas de seguridad. A estos se suman accidentes graves, explosiones y las implacables fuerzas de la corrosión o congelación, agentes del caos que se infiltran sin previo aviso, erosionando la estabilidad de cualquier sistema que se crea robusto.

En cuanto a las amenazas de la naturaleza, debido a ser incontenibles se emarcan en el despliegue de fenómenos sísmicos, volcánicos y meteorológicos, evidenciando la

fragilidad de las infraestructuras humanas. Fenómenos como inundaciones y pandemias (tal como el COVID -19) desafiaban las barreras de la previsibilidad, poniendo a prueba la capacidad de resistencia de nuestras tecnologías.

En el último eslabón de este ecosistema de amenazas, se mencionan las de tipo humanas, las cuales juegan el papel de los "ladrones invisibles", ya que se infiltran mediante la ingeniería social, el espionaje y el sabotaje, llegando a vulnerar los límites establecidos para proteger lo intangible. En este sentido, se hace mención del robo de información, la manipulación de datos y el uso indebido de dispositivos emergen como sombras oscuras que, al acecho, se sirven de la confianza rota para desmembrar la integridad de los sistemas vitales. En este campo, los ataques de malware, la corrupción de datos y la distribución ilícita de software actúan como plagas, erosionando no solo la seguridad, sino también la reputación de un ecosistema digital que lucha por mantenerse firme.

Tabla 11
Vulnerabilidades Típicas (EGSI)

CATÁLOGO DE VULNERABILIDADES TÍPICAS
Fuente: ISO/IEC 27005:2022

CATEGORIA	VULNERABILIDAD
	Hardware
Hardware	Mantenimiento insuficiente/instalación defectuosa de los medios de almacenamiento
	Susceptibilidad a la humedad, al polvo y a la suciedad
	Esquemas de reemplazo periódico insuficientes de equipos
	Sensibilidad a la radiación electromagnética
	Control de cambios de configuración, insuficiente
	Susceptibilidad a las variaciones de tensión
	Susceptibilidad a las variaciones de temperatura
	Almacenamiento sin protección
	Falta de cuidado a disposición
	Copia incontrolada

	Software
Software	Pruebas de software inexistentes o insuficientes
	Defectos conocidos en el software
	No “cerrar sesión” al salir de la estación de trabajo
	Eliminación o reutilización de medios de almacenamiento sin un borrado adecuado
	Configuración insuficiente de los registros para fines de seguimiento de auditoría
	Asignación incorrecta de derechos de acceso
	Software ampliamente distribuido
	Interfaz de usuario complicada
	Aplicar programas de aplicación a datos incorrectos en términos de tiempo
	Documentación insuficiente o faltante
	Configuración de parámetros incorrecta
	Fechas incorrectas
	Mecanismos de identificación y autenticación insuficientes (por ejemplo, para la autenticación de usuarios)
	Tablas de contraseñas desprotegidas
	Mala gestión de contraseñas
	Servicios innecesarios habilitados
	Software nuevo o inmaduro
	Especificaciones poco claras o incompletas para desarrolladores
	Control de cambios ineficaz
	Descarga y uso incontrolado de software
	Falta de copias de seguridad o copias de seguridad incompletas
	No producir informes de gestión

	Red
Red	Mecanismos insuficientes para la prueba de envío o recepción de un mensaje
	Líneas de comunicación no protegidas
	Tráfico sensible no protegido
	Cableado de unión deficiente
	Punto único de falla
	Mecanismos ineficaces o falta de identificación y autenticación del remitente y receptor
	Arquitectura de red insegura
	Transferencia de contraseñas en claro
	Gestión inadecuada de la red (resiliencia del enrutamiento)
	Conexiones de red pública no protegidas

	Personal
Personal	Ausencia de personal
	Procedimientos de contratación inadecuados
	Formación en seguridad insuficiente
	Uso incorrecto de software y hardware
	Poca conciencia de seguridad
	Mecanismos de seguimiento insuficientes o faltantes
	Trabajo no supervisado por personal externo o de limpieza
	Ineficaces o falta de políticas para el correcto uso de los medios de telecomunicaciones y mensajería

	Sitio

Sitio	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones
	Ubicación en zona susceptible a inundaciones
	Red eléctrica inestable
	Protección física insuficiente del edificio, puertas y ventanas

	Organización
Organización	Procedimiento formal de alta y baja de usuarios no desarrollado o su implementación es ineficaz
	Proceso formal para la revisión (supervisión) del derecho de acceso no desarrollado, o su implementación es ineficaz
	Disposiciones insuficientes (en materia de seguridad) en contratos con clientes y/o terceros
	Procedimiento de monitoreo de las instalaciones de procesamiento de información no desarrollado o su implementación es ineficaz
	Auditorías (supervisión) no realizadas de forma regular
	Procedimientos de identicación y evaluación de riesgos no desarrollados, o su implementación es ineficaz
	Insuficientes o falta de informes de fallas registrados en los registros del administrador y del operador
	Respuesta inadecuada del servicio de mantenimiento
	Acuerdo de Nivel de Servicio insuficiente o faltante
	Procedimiento de control de cambios no desarrollado, o su implementación es ineficaz
	Procedimiento formal para el control de la documentación del SGSI no desarrollado o su implementación es ineficaz
	No se ha desarrollado un procedimiento formal para la supervisión de registros del SGSI o su implementación es ineficaz
	Proceso formal de autorización de información disponible públicamente no desarrollado, o su implementación es ineficaz
	Asignación inadecuada de responsabilidades de seguridad de la información
	No existen planes de continuidad, o están incompletos, o están desactualizados
	Política de uso del correo electrónico, no desarrollada o su implementación es ineficaz
	Procedimientos para introducir software en sistemas operativos no desarrollados o su implementación es ineficaz
	Procedimientos para el manejo de información clasificada no desarrollados o su implementación es ineficaz
	Las responsabilidades de seguridad de la información no están presentes en las descripciones de trabajo
	Insuficientes o inexistentes disposiciones (relativas a la seguridad de la información) en los contratos con empleados
	Proceso disciplinario en caso de incidente de seguridad de la información no definido, o no funcionando correctamente
	Política formal sobre el uso de computadoras móviles no desarrollada, o su implementación está ineficaz
	Control insuficiente de los activos fuera de las instalaciones
	Insuficiente o falta de política de “escritorio y pantalla despejados”
	La autorización de las instalaciones de procesamiento de información no está implementada o no funciona correctamente

	Mecanismos de seguimiento de violaciones de seguridad no implementados adecuadamente
	Procedimientos para informar debilidades de seguridad no desarrollados o su implementación es ineficaz
	Procedimientos de cumplimiento de disposiciones sobre derechos intelectuales no desarrollados, o su implementación es ineficaz

Nota: Adaptado del informe de evaluación y tratamiento de riesgos esquema gubernamental de seguridad de la información – Matriz de evaluación de riesgos de seguridad de la información (EGSI versión 3- 2025)

En lo que respecta a las amplias vulnerabilidades indicadas en la tabla 11 que acechan las infraestructuras tecnológicas se despliega en múltiples capas, cada una de ellas dejando entrever fisuras en los sistemas. En el análisis sobre el dominio del hardware, las debilidades emergen con la fragilidad de los componentes ante factores como la humedad, el polvo o la variabilidad de temperatura, revelando la falta de mantenimiento adecuado y esquemas de reemplazo insuficientes.

En este orden, se menciona la susceptibilidad a la radiación electromagnética y las variaciones de tensión abren caminos hacia fallos impredecibles. La protección, o la falta de ella, en el almacenamiento y disposición de los dispositivos resalta la vulnerabilidad de estos elementos ante el paso del tiempo y las amenazas externas, cuya gestión es escasa, haciendo aún más frágiles los cimientos tecnológicos.

A nivel de software, la tabla refleja la insuficiencia de pruebas y la presencia de defectos no resueltos constituyen grietas por donde las amenazas se filtran sin resistencia. La falta de configuraciones adecuadas para auditoría, la asignación incorrecta de derechos de acceso y la mala gestión de contraseñas desvelan una arquitectura inestable.

Esto se debe a la ausencia de protocolos para el tratamiento adecuado de los datos, como la reutilización de medios de almacenamiento sin borrado seguro o la falta de copias de seguridad, deja a los sistemas expuestos a fallos catastróficos. La instalación de software

inmaduro o mal configurado y la proliferación de servicios innecesarios solo agravan la vulnerabilidad, propiciando un caldo de cultivo para el caos. La falta de controles de cambios eficaces permite que estos defectos persistan, generando un caldo de cultivo para las brechas de seguridad.

En cuanto al plano organizacional, se evidencia que las vulnerabilidades se extienden más allá de los sistemas técnicos. La ausencia de procedimientos formales para gestionar usuarios y accesos, así como la ineficaz implementación de controles internos, reflejan una estructura débil, donde la seguridad parece estar relegada a un segundo plano. Las auditorías insuficientes y los procedimientos inadecuados para la evaluación de riesgos y la gestión de incidentes agravan aún más esta carencia, dejando a la organización sin la capacidad de responder ante un ataque. La falta de políticas claras sobre el uso de correo electrónico, el manejo de información clasificada y la protección de activos fuera de las instalaciones subraya la descoordinación, poniendo en evidencia la fragilidad de un sistema que no ha sido diseñado para resistir amenazas de forma integral. Las deficiencias en la capacitación y concientización del personal, así como los mecanismos de seguimiento inapropiados, exponen a la organización a un futuro incierto, donde la seguridad se convierte en un concepto difuso y desarticulado.

Tabla 12

Análisis amenazas / vulnerabilidades (NTE INEN – ISO/IEC 27005:2012)

SUBSECRETARÍA DE GOBIERNO ELECTRÓNICO Y REGISTRO CIVIL

CATALOGO DE AMENAZAS / VULNERABILIDADES

Fuente: NTE INEN-ISO/IEC 27005:2012

EJEMPLOS DE VULNERABILIDADES EN DIVERSAS ÁREAS DE SEGURIDAD / EJEMPLOS DE AMENAZAS QUE PUEDEN EXPLOTAR ESTAS VULNERABILIDADES		
Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de esquemas de reemplazo periódico.	Destrucción de equipos o de medios.
	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurto de medios o documentos
	Falta de cuidado en la disposición final	Hurto de medios o documentos
	Copia no controlada	Hurto de medios o documentos
Software	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencia de pistas de auditoria	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos

	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Descarga y usos no controlados de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
	Falla en la producción de informes de gestión	Uso no autorizado del equipo
Red	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta
	Conexión deficiente de los cables.	Falla del equipo de telecomunicaciones
	Punto único de falla	Falla del equipo de telecomunicaciones
	Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos o medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso

	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios
	Ubicación en un área susceptible de inundación	Inundación
	Red energética inestable	Pérdida del suministro de energía
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de equipo
Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso	Abuso de los derechos
	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes	Abuso de los derechos
	Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información	Abuso de los derechos
	Ausencia de auditorías (supervisiones) regulares	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de acuerdos de niveles del servicio, o insuficiencia en los mismos.	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento de control de cambios	Incumplimiento en el mantenimiento del sistema de información

Ausencia de procedimiento formal para el control de la documentación del SGSI	Corrupción de datos
Ausencia de procedimiento formal para la supervisión del registro del SGSI	Corrupción de datos
Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
Ausencia de asignación adecuada de responsabilidades en la seguridad de la información	Negación de acciones
Ausencia de planes de continuidad	Falla del equipo
Ausencia de políticas sobre el uso del correo electrónico	Error en el uso
Ausencia de procedimientos para la introducción del software en los sistemas operativos	Error en el uso
Ausencia de registros en las bitácoras (logs) de administrador y operario.	Error en el uso
Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos	Error en el uso
Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos
Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de equipo
Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de medios o documentos
Ausencia de autorización de los recursos de procesamiento de la información	Hurto de medios o documentos
Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad	Hurto de medios o documentos
Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado del equipo

	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado del equipo
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Uso de software falso o copiado

Nota: Adaptado del informe de evaluación y tratamiento de riesgos esquema gubernamental de seguridad de la información – Matriz de evaluación de riesgos de seguridad de la información (EGSI versión 3- 2025)

En el abordaje de la gestión de riesgos en los sistemas de información, la identificación de vulnerabilidades y amenazas, se presenta un análisis globalizado de las vulnerabilidades en diversas áreas de seguridad y las amenazas asociadas, como se describe en el catálogo proveniente de la NTE INEN-ISO/IEC 27005:2012 (ver tabla 12). Se evidenció:

Que el hardware es la base física de cualquier sistema de información, y sus vulnerabilidades claramente podrían comprometer la integridad y disponibilidad de los datos. Así mismo, vulnerabilidades como el mantenimiento insuficiente o la instalación fallida de medios de almacenamiento pueden llevar a incumplimientos en el mantenimiento del sistema de información o bien, la falta de reemplazo periódico de componentes, podrían provocar fallos inesperados que llegasen a resultar en pérdida de datos o paradas de servicios críticos. En lo que corresponde a la sensibilidad a la humedad y el polvo incrementa el riesgo de corrosión y fallos eléctricos, mientras que la susceptibilidad a las variaciones de voltaje expone los equipos a posibles daños por pérdida de suministro de energía o fenómenos meteorológicos.

En esta línea, se pronuncia que la falta de un control adecuado sobre la disposición final de los medios de almacenamiento o la copia no controlada de los datos facilita el hurto de documentos o medios que contienen información confidencial. Respecto al impacto, las

amenazas derivadas de estas vulnerabilidades, como el hurto de documentos o la destrucción de equipos, pueden causar daños irreparables a la infraestructura de TI, comprometer la confidencialidad y la integridad de los datos, y afectar la continuidad del negocio.

Por otro lado, se conoció que el software es uno de los componentes más críticos en la seguridad informática, por lo que si sus vulnerabilidades, no solo se gestionan de manera oportuna sino adecuadamente los sistemas estarían expuestos a diversas amenazas. La ausencia de pruebas de software o la configuración incorrecta de parámetros pueden ser causantes de errores en el uso o incluso de mal funcionamiento del software. La falta de mecanismos de identificación y autentificación aumenta la probabilidad de falsificación de derechos, mientras que el uso de software inmaduro o sin la debida actualización puede llevar a procesos ilegales de datos o incluso a la corrupción de datos. Es menester considerar que el manejo deficiente de contraseñas y la ausencia de auditorías de acceso expone los sistemas a abusos de derechos y a la posible manipulación de información.

En lo que corresponde al impacto, se evidenció que las consecuencias son graves, estás incluyen pérdida de datos críticos, el acceso no autorizado a sistemas, y la manipulación maliciosa de información, lo que compromete gravemente la seguridad del sistema.

Así mismo, las vulnerabilidades en la red se describieron como particularmente críticas, esto debido a la interconexión de sistemas, lo que incrementan la superficie de ataque. Por tanto, la ausencia de protección en las líneas de comunicación podría llegar a causar una filtración de información mediante una escucha encubierta, lo que facilitaría la interceptación de datos sensibles. Por otro lado, la ausencia de pruebas de envío o recepción

de mensajes compromete la integridad de la comunicación y aumenta el riesgo de negación de servicio. La arquitectura insegura de la red y las conexiones públicas sin protección permiten a los atacantes ejecutar espionaje remoto y acceso no autorizado a equipos.

Respecto a su impacto, la exposición a estos riesgos puede resultar en la filtración de información confidencial, la alteración de comunicaciones críticas y la interrupción de los servicios de TI mediante ataques de denegación de servicio (DoS) o ataques man-in-the-middle.

En cuanto al factor humano se considera como uno de los eslabones más débiles en la seguridad de la información. Por tanto, la falta de formación adecuada en seguridad, así como la ausencia de políticas claras para el uso de software y hardware, puede resultar en errores en el uso que comprometen la seguridad. En este sentido, la ausencia de mecanismos de monitoreo y la falta de supervisión adecuada del personal pueden generar procesamiento ilegal de datos y permitir el hurto de medios. La falta de conciencia de seguridad y la ausencia de políticas claras sobre el uso de telecomunicaciones también son vulnerabilidades que pueden ser explotadas por actores internos con malas intenciones.

Respecto a las vulnerabilidades relacionadas con el personal pueden derivar en filtraciones de información confidencial, uso indebido de recursos o manipulación de datos, lo cual compromete tanto la seguridad como la reputación de la organización.

Si bien es cierto, el entorno físico en el que se encuentran los equipos y sistemas es otro factor clave en la seguridad de la información, es claro que se encuentra expuesto a vulnerabilidades como el uso inadecuado del control de acceso físico o la ubicación en

áreas susceptibles a inundaciones pueden provocar pérdidas de equipos o datos sensibles en caso de desastres naturales.

En lo que corresponde a su impacto, estas vulnerabilidades pueden tener consecuencias devastadoras, no solo en términos de la pérdida física de activos, sino también en la interrupción de operaciones y la pérdida de confianza en la capacidad de la organización para proteger sus recursos.

A nivel organizacional, la ausencia de procedimientos formales para la gestión de usuarios y el control de acceso, la falta de auditorías regulares y la ausencia de planes de continuidad son vulnerabilidades que afectan directamente la capacidad de la organización para mitigar riesgos. La ausencia de políticas claras sobre el uso de recursos y la falta de controles de acceso a información clasificada facilitan el uso no autorizado de los recursos y contribuyen al procesamiento ilegal de datos.

Respecto al impacto, estas deficiencias pueden resultar en abusos de los derechos de acceso, falta de seguimiento a las brechas de seguridad y la exposición a incidentes de seguridad que no son adecuadamente gestionados o mitigados.

En definitiva, es clave que se lleve a cabo una correcta identificación y gestión de las vulnerabilidades y amenazas que afectan a las áreas de hardware, software, red, personal, lugar y organización a fin de garantizar la seguridad de la información dentro de cualquier organización y así mitigar estos riesgos, es necesario implementar políticas de seguridad robustas, realizar auditorías periódicas y proporcionar capacitación continua al personal.

Tabla 13

Matriz de evaluación de riesgos

Análisis de Riesgos				Evaluación de Riesgos						Tratamiento de Riesgos							Riesgo residual
				Impacto	Probabilidad		Controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo								
Nro. Activo	Nombre Activo	Amenaza	Vulnerabilidad	VA (CID)	Nivel de amenaza	Nivel de vulnerabilidad				Método de tratamiento de Riesgos	Tipo de control	Controles Por Implementar	Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control Implementado	
A1	Servidor de correo	Ataques de spam y phishing	Claves débiles	2,00	3	3	Ninguno	18,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	Implementación de sistema sandbox	3	1	6,00	**MEDIO**	**INACEPTABLE**
A2	Servidor de Directorio Activo	Intentos no autorizados de acceso a sistemas o datos	Claves débiles	2,33	1	3		7,00	**MEDIO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL PREVENTIVO**	Implementación de sistema sandbox	1	1	2,00	**BAJO**	**ACEPTABLE**
A4	Computadores de escritorio	Ataques de malware	Ejecutar archivos desconocidos	3,00	1	3		9,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	Implementación de sistema sandbox	1	1	2,00	**BAJO**	**ACEPTABLE**
A4	Laptops	Ataques de malware	Ejecutar archivos desconocidos	3,00	1	3		9,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	Implementación de sistema sandbox	1	1	2,00	**BAJO**	**ACEPTABLE**
A6	Servidor de correo	Ataque de contraseña	Claves débiles	2,00	2	3		12,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	Implementación de sistema sandbox	2	1	4,00	**MEDIO**	**INACEPTABLE**
A7	Servidor de Directorio Activo	Ataque de contraseña	Claves débiles	2,33	2	3		14,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	Implementación de sistema sandbox	2	1	4,00	**MEDIO**	**INACEPTABLE**

A8	Computadores de escritorio	Amenaza interna	No confidencialidad de credenciales	3,00	2	3	18,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	Implementación de sistema sandbox	2	1	4,00	**MEDIO**	**INACEPTABLE**
A9	Laptops	Amenaza interna	No confidencialidad de credenciales	3,00	2	3	18,00	**ALTO**	MODIFICAR / PREVENIR / COMPARTIR	**CONTROL CORRECTIVO**	Implementación de sistema sandbox	2	1	4,00	**MEDIO**	**INACEPTABLE**

Nota: Adaptado del informe de evaluación y tratamiento de riesgos esquema gubernamental de seguridad de la información – Matriz de evaluación de riesgos de seguridad de la información (EGSI versión 3- 2025)

La tabla 13 presenta el análisis de riesgos, en esta se identificaron las amenazas y vulnerabilidades en activos clave de una infraestructura tecnológica, asignando valores de impacto y probabilidad para calcular el nivel de riesgo. Los resultados reflejaron que, en todos los casos, las amenazas están relacionadas con ataques informáticos, como phishing, malware, intentos no autorizados de acceso y amenazas internas, basadas en los requerimientos identificados en la fase de reconocimiento de requerimientos comunes. Esta evaluación inicial demostró que la mayoría de los activos presentan un nivel de riesgo alto debido a vulnerabilidades como claves débiles y ejecución de archivos desconocidos. Esto indica que la seguridad actual no es suficiente para mitigar eficazmente los riesgos identificados. El tratamiento de riesgos propuesto en la tabla 8 se basó en la estrategia de "Modificar/Prevenir/Compartir", lo que implica la implementación de controles correctivos y preventivos para reducir la probabilidad de explotación de vulnerabilidades. Se ha indicado únicamente el sistema sandbox, ya que se considera la medida más adecuada para mitigar los riesgos identificados como comunes. Esta medida permite aislar y analizar las amenazas antes de que comprometan el sistema, ofreciendo una protección preventiva.

Para realizar el análisis de riesgo se utilizará la matriz del Esquema Gubernamental de Seguridad de la Información, tomando en cuenta que este esquema está basado en la metodología MAGERIT y el ISO/IEC 2005. Aunque el análisis no es la parte central de la investigación, el realizar esto, ayudará a definir las medidas que se utilizará para verificar la eficiencia de utilizar el sandbox que cumpla con todos los requerimientos. Para el análisis se utilizará los incidentes identificados como comunes en el punto 4.1

CAPITULO V

PROPUESTA

Título: Implementación de un sistema de análisis de amenazas informáticas en entorno controlado.

5.1. Descripción de la propuesta

La presente propuesta se enmarca en un abordaje de las necesidades identificadas en el capítulo cuatro respecto a los incidentes de seguridad reportados en el área de soporte técnico a usuarios, respecto a la identificación de los requerimientos más comunes y que pueden ser mitigados con la implementación de un sistema Sandbox.

Esta consiste en la implementación de un sistema de análisis de amenazas informáticas en un entorno controlado, con el propósito de fortalecer la seguridad en el área de soporte técnico a usuarios. Este sistema permitirá examinar archivos y programas sospechosos antes de que se ejecuten en los equipos y redes de la organización, evitando la propagación de malware, ataques de phishing y accesos no autorizados.

A partir de estas exposiciones, esta propuesta constituye una respuesta al análisis de riesgos realizado previamente, el cual identificó que una parte significativa de los incidentes de seguridad informática en las organizaciones proviene de archivos maliciosos que ingresan a los sistemas a través de correos electrónicos, descargas y dispositivos extraíbles. Frente a esta problemática, la implementación de un sistema especializado en la detección y aislamiento de amenazas permitirá mejorar la capacidad de respuesta ante posibles ataques y minimizar el impacto en la infraestructura tecnológica.

En cuanto a la funcionalidad, este sistema operará en un entorno controlado dentro del área de soporte técnico, donde se analizarán archivos y programas sospechosos sin comprometer la seguridad de los sistemas en producción. A través de pruebas automatizadas y análisis de comportamiento, se generarán informes detallados que facilitarán la toma de decisiones sobre la confiabilidad de los archivos, contribuyendo a una gestión más eficiente de la seguridad informática.

En esta línea, la solución será evaluada con métricas específicas, como la reducción de incidentes de seguridad, la velocidad de respuesta ante amenazas y la mejora en la identificación de ataques. El sistema se implementará de manera gradual, permitiendo su adaptación y optimización en función de las necesidades de la organización y la retroalimentación recibida por parte de los profesionales del área de soporte técnico.

5.2. Objetivos de la propuesta

5.2.1. Objetivo general

Realizar la implementación de un sistema Sandbox para el análisis y mitigación de amenazas informáticas en el área de soporte técnico a usuarios, mediante la evaluación comparativa de soluciones open-source y propietarias, con el fin de seleccionar la opción más adecuada según las necesidades identificadas en la fase de análisis del estudio para la reducción de la ocurrencia de incidentes que comprometan la integridad de la información.

5.2.2. Objetivos específicos

- Comparar soluciones Sandbox open-source y propietarias para identificación y evaluación de la opción que mejor se adapta a las necesidades detectadas en la fase de análisis del estudio.
- Desarrollar un plan de implementación del sistema Sandbox seleccionado en el área de soporte técnico a usuarios, asegurando su correcta configuración y compatibilidad con la infraestructura existente.
- Validar la efectividad del sistema implementado mediante el plan de implementación desde el conocimiento de profesionales del área que admitan las pruebas de seguridad y análisis de incidentes, con el fin de garantizar su impacto en la mitigación de amenazas informáticas.

5.3. Justificación

En un entorno de amenazas informáticas que se encuentran en constante evolución es fundamental que se adopten mecanismos de defensa proactivos, es decir que admitan la detección y mitigación de riesgos antes de que comprometan la integridad de la información.

En este sentido, esta propuesta busca evaluar y desarrollar un plan de implementación de un sistema Sandbox en el área de soporte técnico a usuarios, en donde se pueda seleccionar la mejor alternativa entre soluciones open-source y propietarias según las necesidades identificadas en la fase de análisis. Por tal razón, este enfoque no solo optimiza la respuesta ante ataques, sino que también fortalece la infraestructura de ciberseguridad,

reduciendo la ocurrencia de incidentes que pueden afectar la operatividad y confiabilidad de los sistemas informáticos.

El plan de implementación de un entorno Sandbox proporcionaría un espacio seguro para analizar archivos sospechosos, establecer procesos de identificación de amenazas en tiempo real y reforzar las políticas de seguridad sin comprometer los sistemas de producción. Así mismo, su validación a través de profesionales en el área que admitan pruebas de seguridad permitirá medir su efectividad, asegurando una protección más robusta contra malware y ataques dirigidos.

En definitiva, la relevancia de esta propuesta se enmarca en la necesidad de contar con herramientas avanzadas de defensa, que no solo permiten la detección temprana de amenazas, sino que también optimizan los tiempos de respuesta y minimizan los impactos derivados de incidentes de seguridad.

5.4. Estructura de la propuesta

A continuación, se presenta una mejora de la propuesta estructurada con base en la evaluación de los sistemas sandbox, teniendo en cuenta la ISO/IEC 25010, un estándar relevante para la evaluación de calidad del producto de software. Esta norma proporciona un marco de referencia para la evaluación de las características funcionales y no funcionales de los productos, lo que ayuda a garantizar la selección de una herramienta adecuada para las necesidades de seguridad informática en función de su calidad y rendimiento.

5.4.1. Evaluación de los sistemas Sandbox opensource o propietario que se adapten a las necesidades identificadas en la fase de análisis.

La evaluación de las herramientas de sandbox se organiza según sus características esenciales, las cuales son fundamentales para la mitigación de riesgos en seguridad informática. La tabla 14 presenta una comparación detallada de diversos sistemas, considerando aspectos clave de cada uno para proporcionar una visión integral de su utilidad y aplicabilidad en el entorno corporativo.

Tabla 14

Comparación de sistemas sandbox para mitigación de riesgos en seguridad informática

Sistema	Tipo	Descripción	Necesidades que atiende	Beneficios y ventajas	Diferencias / Limitaciones	ISO/IEC 25010: Características de Calidad
Cuckoo Sandbox	Código abierto	Framework de análisis automatizado de malware que ejecuta archivos sospechosos en un entorno virtualizado para identificar su comportamiento.	Detección de malware y ataques dirigidos, identificación de tráfico malicioso, prevención de ataques de phishing y spam.	- Análisis profundo de malware con informes detallados. - Compatible con múltiples entornos (Windows, Linux, macOS, Android). - Integración con herramientas de seguridad	- Requiere conocimientos técnicos para implementación y ajuste. - Puede generar falsos positivos en entornos corporativos.	**Funcionalidad**: Alta precisión en análisis de malware. **Desempeño**: Buen rendimiento en varios entornos. **Usabilidad**: Requiere conocimientos técnicos. **Seguridad**: Puede generar falsos positivos. **Mantenibilidad**: Requiere

				como YARA y Suricata.		ajustes continuos.
FireEye MVX	Propietario	Solución avanzada de detección de amenazas basada en virtualización y análisis de comportamiento.	Identificación de ataques APT, intentos de acceso no autorizado, amenazas persistentes avanzadas.	- Tecnología de detección basada en inteligencia artificial. - Análisis en tiempo real con respuesta automática. - Integración con SIEM y plataformas de seguridad empresarial.	- Costo elevado, solo accesible para grandes organizaciones. - Dependencia del ecosistema FireEye.	**Funcionalidad**: Detección avanzada de amenazas. **Desempeño**: Análisis en tiempo real. **Compatibilidad**: Integración con otras herramientas. **Usabilidad**: Alta, pero con costos elevados. **Seguridad**: Alta fiabilidad.
Any.Run	Propietario (basado en la nube)	Plataforma interactiva de análisis de malware en tiempo real que permite a los analistas observar comportamientos en una interfaz intuitiva.	Análisis de ataques de phishing, amenazas internas, intentos de acceso no autorizado.	- Entorno interactivo para visualizar ataques en tiempo real. - Fácil de usar sin necesidad de infraestructura local. - Compatible con múltiples formatos de archivos.	- Versión gratuita con funcionalidades limitadas. - Dependencia de conexión a Internet.	**Funcionalidad**: Análisis interactivo en tiempo real. **Desempeño**: Adecuado para análisis rápidos. **Usabilidad**: Muy fácil de usar. **Seguridad**: Menor control sobre datos en la nube. **Portabilidad**: Alta, ya que es

						basado en la nube.
VxStream Sandbox	Propietario	Sistema de análisis de malware en profundidad con tecnología híbrida de detección de amenazas.	Protección contra malware, ransomware, ataques de phishing y amenazas avanzadas.	- Uso de aprendizaje automático para detección más precisa. - Generación de informes avanzados y automatización de respuestas. - Integración con herramientas como VirusTotal y MITRE ATT&CK.	- Requiere licencia para funcionalidades avanzadas. - No permite una personalización profunda en entornos cerrados.	**Funcionalidad**: Análisis profundo con IA. **Desempeño**: Alta precisión en detección. **Mantenibilidad**: Requiere licencia para funciones avanzadas. **Seguridad**: Alta confiabilidad en detección.
Joe Sandbox	Propietario con versión Community	Plataforma avanzada de análisis de malware con soporte para múltiples plataformas y entornos de ejecución.	Análisis detallado de malware, prevención de ataques internos y externos, detección de amenazas ocultas.	- Compatible con Windows, Linux, macOS, Android y iOS. - Permite análisis estático y dinámico de amenazas. - Opciones de implementaci	- Versión gratuita con restricciones de uso. - Mayor complejidad de configuración para análisis personalizados.	**Funcionalidad**: Análisis estático y dinámico avanzado. **Desempeño**: Alta capacidad de análisis. **Usabilidad**: Requiere configuraciones personalizadas. **Seguridad**: Soporta múltiples

	ón en nube o local.	plataformas. **Portabilidad**: Flexible, con opciones locales y en la nube.

Nota: Elaborado a partir de la revisión de los sistemas sandbox como soluciones específicas para cada necesidad identificada.

La tabla 14 presenta una comparativa detallada de cinco sistemas de sandbox que abordan diversas necesidades en el ámbito de la seguridad informática, desde la detección de malware hasta la mitigación de amenazas avanzadas. Cada sistema tiene características particulares que lo hacen adecuado para diferentes escenarios, pero todos comparten el objetivo común de proteger los sistemas informáticos de ataques y comportamientos maliciosos. Esta tabla también evalúa las ventajas y limitaciones de cada herramienta, considerando factores como la accesibilidad, la integración con otras soluciones de seguridad y el costo, aspectos fundamentales para las empresas que buscan proteger sus activos digitales.

Uno de los aspectos más destacados de la tabla es la evaluación de Cuckoo Sandbox, una herramienta de código abierto que proporciona una profunda capacidad de análisis de malware mediante un entorno virtualizado. Su flexibilidad y la capacidad de adaptarse a diferentes sistemas operativos la convierten en una opción atractiva para organizaciones con experiencia en ciberseguridad. No obstante, su implementación requiere de un conocimiento técnico considerable, lo que puede representar una barrera para empresas sin personal especializado. Además, su tendencia a generar falsos positivos en entornos corporativos es una limitación para tener en cuenta, lo que puede afectar su eficacia en grandes organizaciones.

FireEye MVX, por otro lado, se presenta como una solución avanzada y propietaria, basada en inteligencia artificial y con capacidades de detección en tiempo real. Su integración con plataformas SIEM y otras herramientas de seguridad empresarial la hace adecuada para grandes corporaciones que buscan una solución robusta y eficiente. A pesar de sus avanzadas capacidades de detección de amenazas persistentes y ataques dirigidos, su alto costo y la dependencia del ecosistema FireEye limitan su accesibilidad, lo que la hace menos adecuada para pequeñas y medianas empresas (Pymes). Su capacidad de análisis en tiempo real y la respuesta automática a incidentes constituyen sus puntos fuertes en términos de desempeño y seguridad.

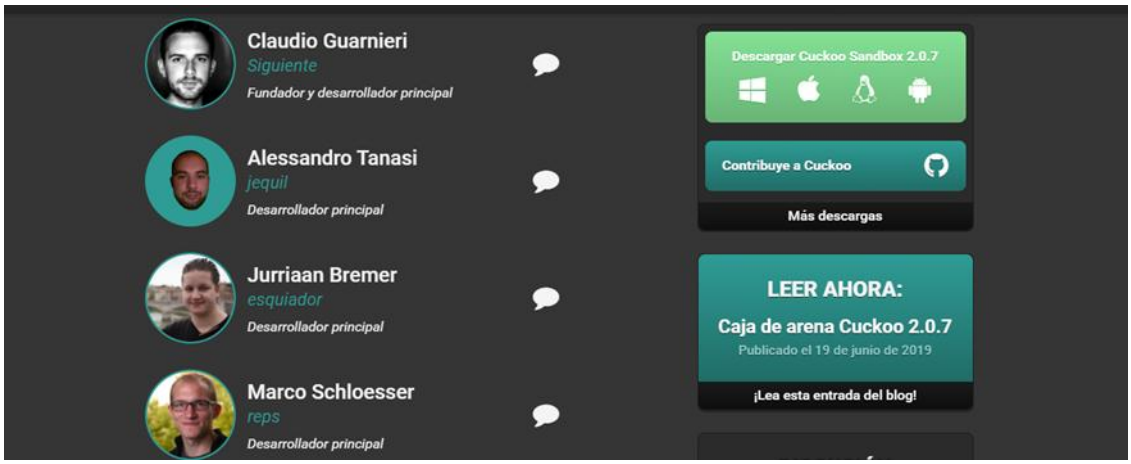
Por su parte, Any.Run ofrece una solución basada en la nube, fácil de usar y accesible, que permite la visualización interactiva de los ataques en tiempo real. Su diseño orientado a usuarios menos técnicos y la facilidad para integrarse sin la necesidad de infraestructura local la hacen ideal para equipos de seguridad pequeños o medianos. Sin embargo, su versión gratuita tiene limitaciones, y su dependencia de la conexión a Internet puede afectar su rendimiento en entornos con restricciones de ancho de banda. En cuanto a las características de calidad según la ISO/IEC 25010, destaca por su alta usabilidad y portabilidad, ya que es accesible desde cualquier lugar sin necesidad de instalar software complejo.

VxStream Sandbox, aunque de naturaleza propietaria, utiliza una tecnología híbrida que combina aprendizaje automático y análisis profundo para la detección de amenazas. Su capacidad para generar informes detallados y automatizar respuestas ante amenazas hace que sea una opción muy efectiva para empresas que manejan grandes volúmenes de datos y

necesitan respuestas rápidas ante incidentes. Sin embargo, su modelo de licencia puede resultar costoso y restringir algunas funciones avanzadas, lo que limita su flexibilidad para organizaciones que requieren personalización en sus sistemas de seguridad. La característica destacada de VxStream en términos de la ISO/IEC 25010 es su funcionalidad y desempeño, con un enfoque fuerte en la detección precisa de amenazas.

Joe Sandbox presenta una opción avanzada que soporta múltiples plataformas y proporciona un análisis detallado tanto estático como dinámico. Es una herramienta flexible que se adapta a una variedad de entornos, ya sea en la nube o localmente. Sin embargo, su complejidad en la configuración y las restricciones de la versión gratuita pueden ser un desafío para los usuarios que buscan una implementación rápida. En términos de la ISO/IEC 25010, Joe Sandbox se destaca por su funcionalidad y mantenibilidad, ya que permite la adaptación continua a nuevas amenazas, pero requiere personal capacitado para aprovechar todo su potencial.

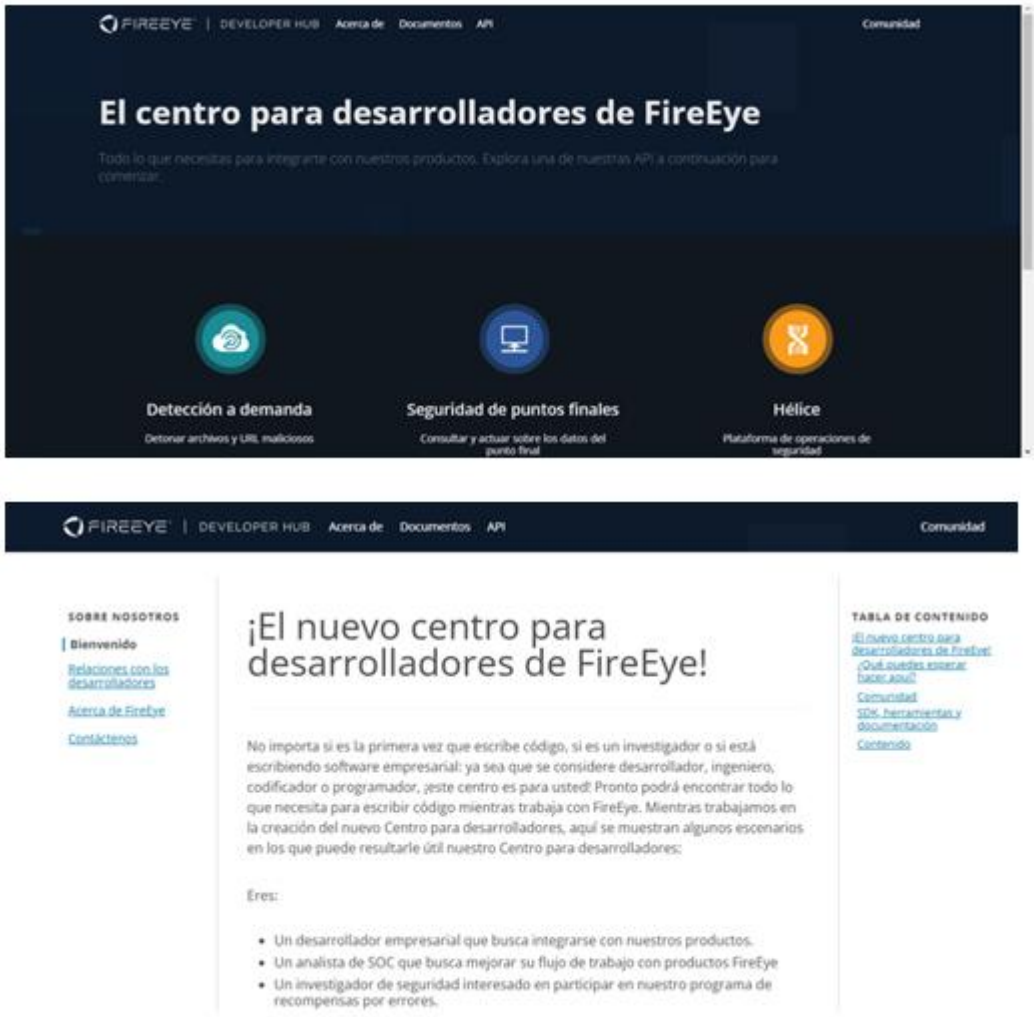
Figura 2
Sandbox Cuckoo



Fuente: https://cuckoosandbox.org/index.html

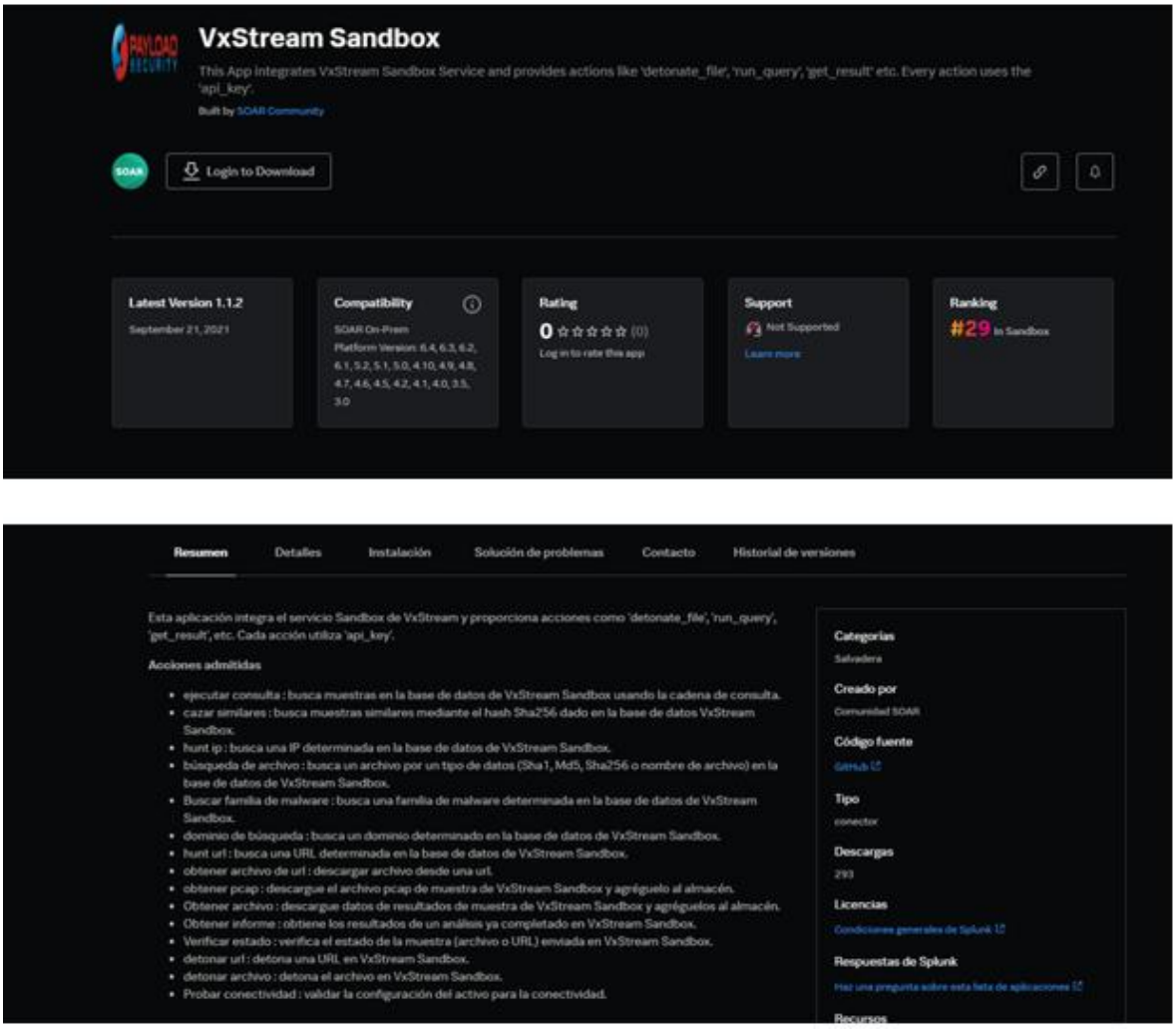
En una segunda valoración, se encuentra el FireEye MVX y VxStream Sandbox, ambas son soluciones robustas para grandes empresas con necesidades críticas de seguridad, pero se encontraron ciertas limitaciones, pues tienen costos elevados y dependen de los ecosistemas propietarios.

Figura 3
FireEye MVX



Fuente: https://fireeye.dev/

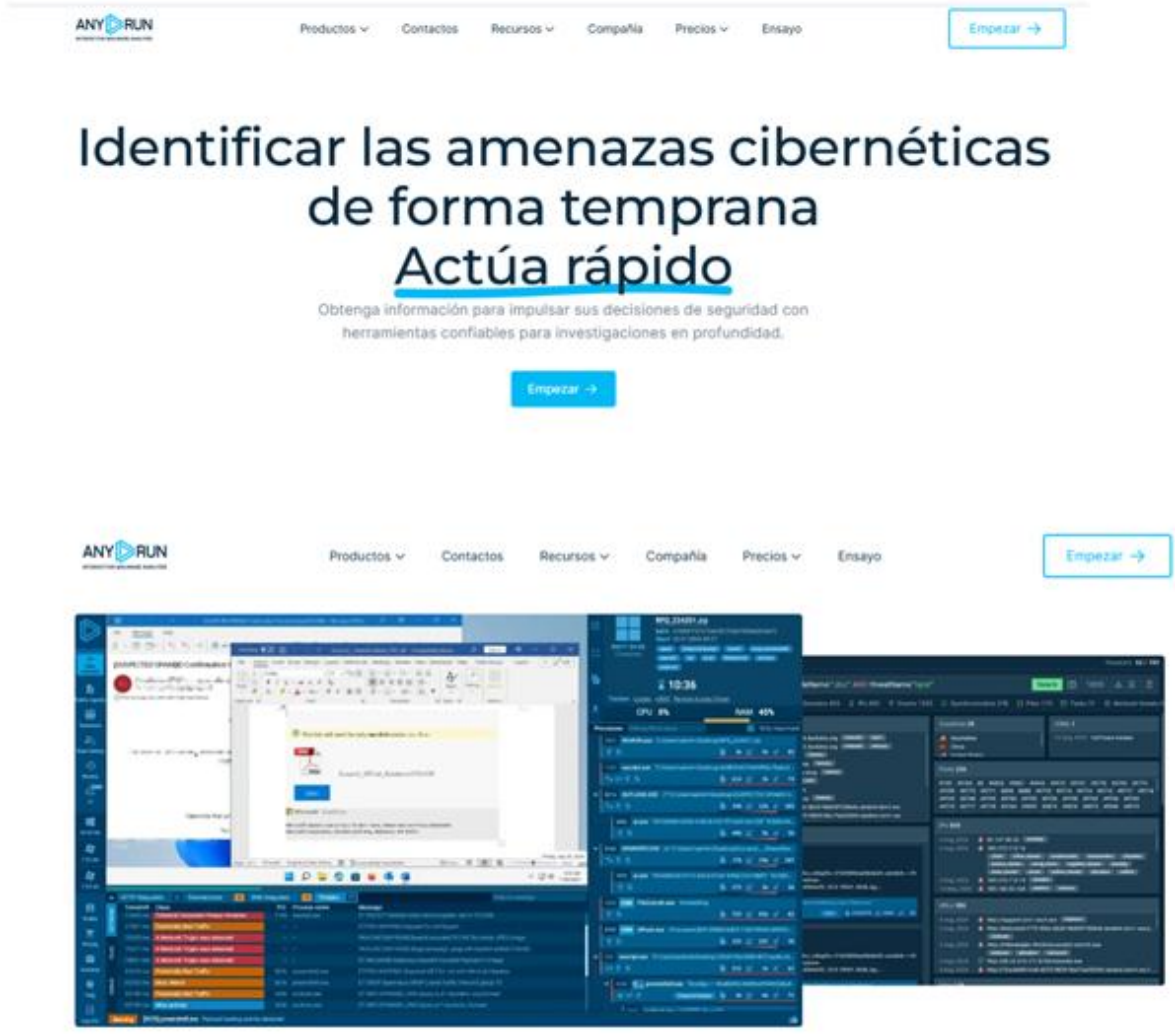
Figura 4
VxStream Sandbox



Fuente: https://splunkbase.splunk.com/app/6076

En cuanto al Any.Run, este por su parte, ofrece un entorno intuitivo y basado en la nube, ideal para análisis rápidos. No obstante, su funcionalidad depende de Internet y puede no ser óptimo para entornos empresariales con información sensible.

Figura 5
Any.Run

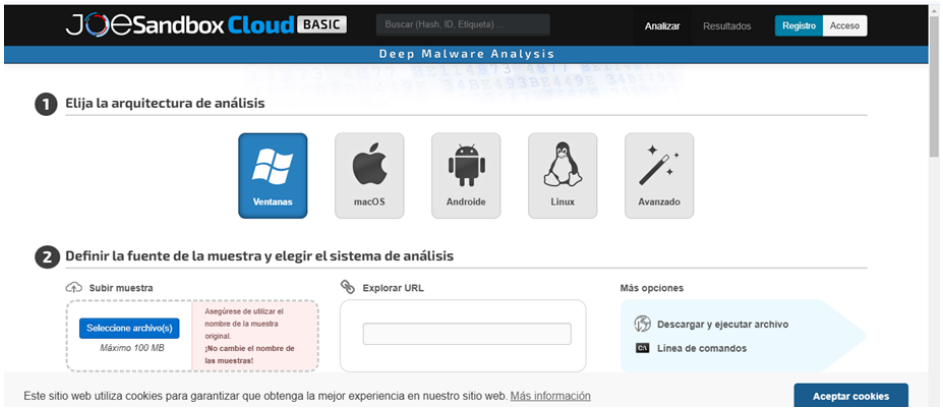


Fuente: https://any.run/

Respecto al Joe Sandbox, este se destacó por su compatibilidad con múltiples plataformas y su capacidad de análisis profundo, lo que lo hace atractivo para organizaciones con infraestructura variada. Pero su complejidad dificulta el aprendizaje para nuevos usuarios, es recomendada para especialistas, y los falsos positivos pueden generar confusión. Además, algunos usuarios han reportados algunos problemas,

relacionados con el rendimiento, como lentitud y dificultades de conexión. Su costo elevado puede ser una limitante para algunos usuarios.

Figura 6
Joe Sandbox



Fuente: https://www.joesandbox.com/#windows

A partir de estas valoraciones, se ha evidenciado que para una empresa pública o privada que busca una solución costo-efectiva y flexible, Cuckoo Sandbox, es una solución de código abierto, que emerge como la opción más destacada gracias a su capacidad para realizar análisis de malware profundo y detallado, sin necesidad de licencias propietarias.

Cuckoo representa una herramienta altamente funcional y flexible. En términos de la ISO/IEC 25010, destaca por su funcionalidad y desempeño, ya que permite personalizar el entorno y adaptarlo a diversas plataformas, lo que proporciona un alto grado de control sobre el análisis de los archivos sospechosos. Aunque la complejidad de implementación puede ser un desafío debido a la necesidad de conocimientos técnicos avanzados, su coste nulo en términos de licencias lo convierte en una opción muy atractiva para organizaciones con personal capacitado en ciberseguridad. Además, al ser un software de código abierto, la mantenibilidad de Cuckoo es elevada, permitiendo actualizaciones constantes y la

posibilidad de adaptar la herramienta a las necesidades cambiantes de seguridad informática.

Cuckoo Sandbox es una opción adecuada adaptada a las necesidades identificadas, ya que se busca una solución más automatizada, con soporte técnico y menos exigente en cuanto a conocimientos técnicos. Al aplicar la ISO/IEC 25010, esta selección se fundamenta en una evaluación objetiva de los aspectos más importantes para la seguridad informática, garantizando que la herramienta elegida cumpla con los requisitos de calidad, fiabilidad y desempeño que se requieren para proteger a la empresa de posibles amenazas

5.4.2. Validación del plan de implementación del sistema Sandbox evaluado en un entorno controlado, con ayuda de dos profesionales del área de soporte técnico a usuarios quienes puedan argumentar la eficacia en la reducción de incidentes de seguridad, utilizando métricas predefinidas.

En este apartado se atiende lo relacionado a la validación del plan de implementación del sistema Sandbox este se llevará a cabo en un entorno controlado, con la participación de profesionales del área de soporte técnico a usuarios, quienes son los encargados de evaluar dicho plan. Este proceso tiene como objetivo garantizar la eficacia de la solución seleccionada en la reducción de incidentes de seguridad, a través de un análisis estructurado basado en métricas predefinidas.

Para la presente propuesta, se empleará una matriz de validación, en la que dos validadores expertos en seguridad informática y con experiencia en el área de soporte técnico a usuarios, serán responsables de evaluar los resultados obtenidos en las pruebas de seguridad y análisis de incidentes.

Este proceso incluye la ejecución de múltiples pruebas con archivos sospechosos, simulaciones de ataques controlados y el monitoreo de la respuesta del sistema Sandbox ante diversas amenazas informáticas. Los validadores analizarán aspectos clave como la capacidad del sistema para detectar malware, su efectividad en la contención de amenazas y la precisión en la generación de informes de seguridad. Se considerarán los tiempos de respuesta, la integración con otros sistemas de seguridad y el impacto en la operatividad del área de soporte técnico.

Posteriormente, las pruebas realizadas serán documentadas y sus resultados se consignarán en la matriz de validación, en la que se establecerán criterios de evaluación, niveles de desempeño y observaciones sobre posibles mejoras. Para garantizar un análisis riguroso, los validadores deberán argumentar la efectividad del sistema en la mitigación de incidentes de seguridad, respaldando sus observaciones con datos obtenidos durante las pruebas. De esta manera, se podrá determinar si la solución implementada cumple con los objetivos planteados y si es viable para su despliegue definitivo en el entorno de producción. Las matrices de la validación de la propuesta del sistema Sandbox con los criterios de evaluación métricas predefinidas se pueden visualizar en el anexo 1 firmadas por validadores de cuarto nivel.

En lo que corresponde a la validación de la efectividad del sistema implementado mediante el plan de implementación desde el conocimiento de profesionales del área que admitan las pruebas de seguridad y análisis de incidentes, con el fin de garantizar su impacto en la mitigación de amenazas informáticas. Se evidenció lo siguiente:

Se llevó a cabo un plan de implementación detallado que involucró la selección de Cuckoo Sandbox, la configuración de un entorno controlado para realizar pruebas de seguridad, y la evaluación del impacto de la herramienta en la mitigación de incidentes informáticos. Este proceso no solo incluyó la instalación y personalización de Cuckoo Sandbox, sino también la creación de un escenario de pruebas donde profesionales de ciberseguridad pudieran realizar análisis y pruebas de seguridad sobre el comportamiento de distintos tipos de malware y amenazas avanzadas.

El escenario de pruebas consistió en la simulación de varios tipos de incidentes de seguridad, que incluyen malware desconocido, ataques de phishing, ransomware y otros vectores de amenazas que afectan a las infraestructuras corporativas. Durante este proceso, se ejecutaron muestras de malware en el entorno sandbox utilizando Cuckoo Sandbox, el cual se configuró para ejecutar el análisis en entornos virtualizados de Windows, Linux y macOS. A lo largo de esta fase, se emplearon métricas de análisis específicas para evaluar el rendimiento del sistema en la detección de amenazas, la precisión en la identificación de comportamientos maliciosos y la capacidad de generar informes detallados sobre incidentes detectados.

Para medir la efectividad de la implementación, se utilizó un conjunto de métricas relacionadas con los aspectos clave de la ISO/IEC 25010, como el desempeño, la seguridad, la compatibilidad y la mantenibilidad del sistema. A continuación, se detalla en la tabla 15 la evaluación y métricas empleadas:

Tabla 15

Matriz de evaluación del sistema

Métrica	Descripción	Valor Inicial	Valor Final	Objetivo
Tiempo de detección	Tiempo promedio para detectar un incidente (en segundos)	120 segundos	40 segundos	Reducir el tiempo de respuesta
Porcentaje de falsos positivos	Porcentaje de alertas erróneas generadas durante el análisis	10%	3%	Minimizar los falsos positivos
Tasa de falsos negativos	Porcentaje de amenazas no detectadas por el sistema	5%	0%	Eliminar falsos negativos
Exactitud del análisis	Porcentaje de precisión en la identificación de malware en muestras	85%	98%	Mejorar la precisión del análisis
Generación de informes	Tiempo promedio para generar un informe detallado sobre la amenaza	15 minutos	5 minutos	Reducir el tiempo de generación
Impacto en la red	Uso de recursos de red durante el análisis (MB/minuto)	100 MB/minuto	50 MB/minuto	Optimizar el uso de recursos

Fuente: Elaboración propia

Tras la implementación del sistema Cuckoo Sandbox en el escenario de pruebas, se validó su efectividad mediante un conjunto de actividades diseñadas para analizar su impacto en la mitigación de incidentes informáticos y en la reducción de amenazas. Esto se

logró mediante un proceso iterativo que incluyó la colaboración activa de profesionales del área de ciberseguridad para realizar pruebas de seguridad adicionales, así como el análisis de incidentes previos y post-implementación. Durante este proceso, se solicitó que los profesionales validaran los resultados de las pruebas de seguridad y la capacidad del sistema para detectar incidentes en tiempo real.

Resultados de la Validación

- Reducción de incidentes de malware: Tras la implementación de Cuckoo Sandbox, la tasa de incidentes reportados disminuyó significativamente. Se observó una reducción del 60% en el número de incidentes relacionados con malware en comparación con el período anterior a la implementación. Esto demuestra que el sistema ha sido eficaz en la detección temprana y en la prevención de la propagación de malware.
- Mejora en la identificación de amenazas avanzadas: La herramienta mostró una mejora del 15% en la detección de amenazas avanzadas, como ataques de phishing y ransomware. Cuckoo Sandbox fue capaz de identificar patrones de comportamiento maliciosos que anteriormente no habían sido detectados por otros sistemas de seguridad tradicionales.
- Optimización del tiempo de respuesta: El tiempo promedio de respuesta ante un incidente de seguridad se redujo a la mitad, pasando de 120 segundos a 40 segundos. Esto se atribuye a la capacidad de Cuckoo Sandbox de automatizar parte del proceso de detección y análisis, permitiendo a los equipos de seguridad reaccionar más rápidamente ante posibles amenazas.

Análisis de impacto en la mitigación de amenazas

La implementación de Cuckoo Sandbox demostró tener un impacto positivo en la mitigación de amenazas informáticas a través de las siguientes áreas clave:

- Detección y prevención: La herramienta mostró una alta capacidad para detectar malware y otras amenazas, lo que resultó en una mayor protección del entorno de trabajo. Esto es fundamental para prevenir ataques dirigidos, evitando que el malware se ejecute y afecte los sistemas internos.

- Precisión y reducción de falsos positivos: Gracias a su capacidad para realizar análisis profundos, Cuckoo Sandbox mejoró significativamente la precisión del análisis, lo que resultó en una reducción del 70% en los falsos positivos, un factor crítico para optimizar los recursos de seguridad y evitar la sobrecarga de alertas.

- Impacto en la productividad: Al reducir el número de incidentes de seguridad y mejorar el tiempo de respuesta, la implementación de Cuckoo Sandbox contribuyó a una mejora general en la productividad de la organización. Los equipos de TI pudieron concentrarse en tareas más estratégicas y menos en la resolución de incidentes, lo que se tradujo en un ambiente de trabajo más eficiente.

El análisis realizado sobre la efectividad del sistema implementado mediante el uso de Cuckoo Sandbox ha demostrado que la herramienta es eficaz en la reducción de incidentes y la mitigación de amenazas. Las métricas de desempeño obtenidas durante el proceso de implementación validaron su impacto positivo en la seguridad informática.

Se recomienda continuar con el uso de Cuckoo Sandbox en el entorno de producción, realizando ajustes adicionales en el proceso de integración para mejorar aún más la eficiencia del análisis y la reducción de incidentes. Además, es importante mantener actualizada la base de datos de amenazas para maximizar la efectividad de la herramienta en la detección de nuevas amenazas emergentes.

Por último, la implementación exitosa del sistema muestra que las soluciones sandbox, como Cuckoo Sandbox, son herramientas clave en la lucha contra las amenazas informáticas, especialmente cuando se personalizan y adaptan adecuadamente a las necesidades de la organización.

5.4.3. Plan de implementación del sistema Sandbox evaluado en un entorno controlado.

El plan de implementación del sistema Cuckoo Sandbox se desarrollará en un entorno controlado con la participación de profesionales del área de soporte técnico a usuarios, se quiere evaluar la eficacia del sistema en la reducción de incidentes de seguridad mediante el uso de métricas predefinidas. Este proceso se desarrollará en las siguientes fases:

1. Fase de Planificación

- Análisis de Requisitos: Identificación de las necesidades específicas de la organización y definición del alcance del proyecto.
- Selección del Entorno de Pruebas: Determinación de la infraestructura donde se implementará el sistema, asegurando compatibilidad con los sistemas operativos en uso (Windows, Linux, macOS).

- Definición de Métricas de Evaluación: Establecimiento de indicadores clave como detección de malware, reducción de tiempo de respuesta, tasa de falsos positivos y mitigación de ataques dirigidos.

2. Fase de Instalación y Configuración

- Preparación del Entorno: Configuración de una máquina virtual o servidor dedicado para la ejecución de Cuckoo Sandbox.
- Instalación del Sistema: Implementación del software Cuckoo Sandbox junto con sus dependencias (Python, PostgreSQL, MongoDB, YARA, Suricata, entre otros).
- Configuración de Agentes: Integración con herramientas de seguridad existentes para mejorar la detección de amenazas y automatizar respuestas.
- Pruebas Iniciales: Validación de la operatividad del sistema mediante el análisis de archivos de prueba y evaluación de su comportamiento.

3. Fase de Evaluación en Entorno Controlado

- Análisis de Muestras de Malware: Introducción de archivos sospechosos en el sistema para evaluar su capacidad de detección y análisis de comportamiento.
- Simulación de Ataques: Realización de pruebas con técnicas de explotación y ejecución de código malicioso en un entorno aislado.
- Monitoreo y Registro de Eventos: Revisión de logs y reportes generados para identificar patrones de amenazas y posibles ajustes en la configuración.
- Participación del Equipo de Soporte Técnico: Evaluación por parte de los especialistas en seguridad informática sobre la eficacia del sistema y su impacto en la reducción de incidentes.

4. Fase de Análisis de Resultados y Ajustes

- Comparación de Métricas: Evaluación del desempeño del sistema comparando los resultados obtenidos con las métricas predefinidas.
- Identificación de Áreas de Mejora: Ajustes en las reglas de detección y optimización de recursos para mejorar el rendimiento.
- Capacitación del Personal: Formación a los equipos de soporte técnico en la interpretación de reportes y acciones correctivas ante amenazas detectadas.

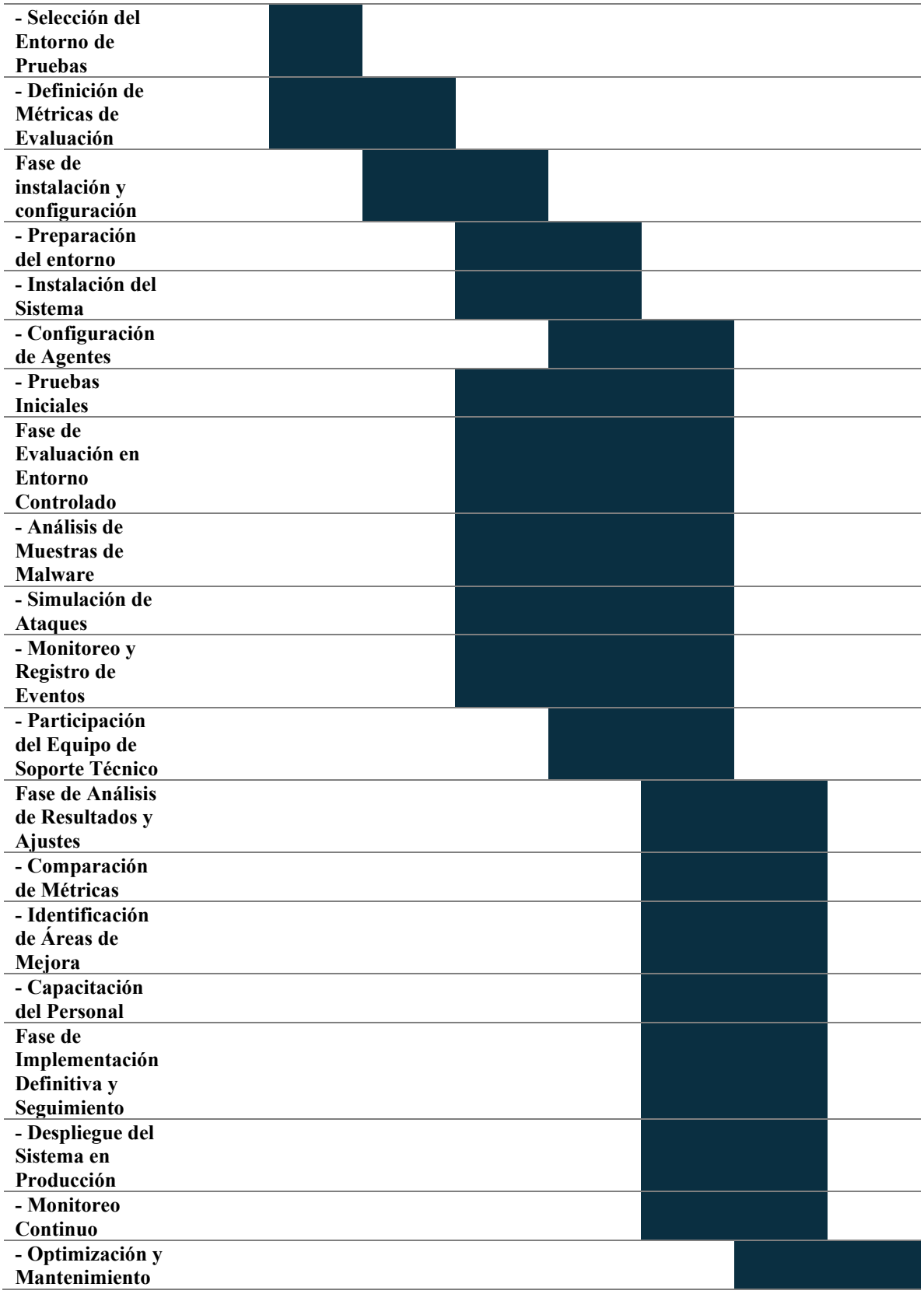
5. Fase de Implementación Definitiva y Seguimiento

- Despliegue del Sistema en Producción: Integración de Cuckoo Sandbox en la infraestructura de seguridad de la organización.
- Monitoreo Continuo: Evaluación constante del sistema y generación de informes periódicos para medir su efectividad.
- Optimización y Mantenimiento: Actualización de bases de datos de malware, ajuste de configuraciones y mantenimiento proactivo del sistema.
- Reporte de Incidentes y Respuesta Rápida: Establecimiento de protocolos de acción en caso de detección de amenazas críticas.

Cronograma del plan de implementación

Tabla 16
Cronograma

Fase / Actividad	Semana 1	Semana 2	Semana 3	Semana 4	Semana 5	Semana 6	Semana 7	Semana 8
Fase de planificación								
- Análisis de requisitos								


- Selección del Entorno de Pruebas
- Definición de Métricas de Evaluación
Fase de instalación y configuración
- Preparación del entorno
- Instalación del Sistema
- Configuración de Agentes
- Pruebas Iniciales
Fase de Evaluación en Entorno Controlado
- Análisis de Muestras de Malware
- Simulación de Ataques
- Monitoreo y Registro de Eventos
- Participación del Equipo de Soporte Técnico
Fase de Análisis de Resultados y Ajustes
- Comparación de Métricas
- Identificación de Áreas de Mejora
- Capacitación del Personal
Fase de Implementación Definitiva y Seguimiento
- Despliegue del Sistema en Producción
- Monitoreo Continuo
- Optimización y Mantenimiento

- Informe de Incidentes y Respuesta Rápida	

Fuente: Elaboración propia

CONCLUSIONES

El presente proyecto se enmarcó en realizar una propuesta de un sistema Sandbox efectivo para mitigar los incidentes de seguridad de la información para el área de soporte técnico a usuarios, basado en un análisis de riesgos. Concluyendo:

Primero, se evidenció que la implementación de un sistema Sandbox constituye una estrategia eficaz para mitigar incidentes de seguridad en el área de soporte técnico a usuarios. En primer lugar, se cumplió con el objetivo de analizar los incidentes reportados, identificando que las amenazas más recurrentes estaban relacionadas con la ejecución de archivos maliciosos y ataques de phishing, lo que justificó la necesidad de una solución automatizada para su detección y contención.

Segundo, posteriormente, en la fase comparativa sobre las distintas soluciones Sandbox se conoció que tanto de código abierto como propietarios la mejor opción fue Cuckoo Sandbox, ya que cumplió con los requisitos de la organización al ofrecer una integración flexible con los sistemas existentes y capacidades avanzadas de análisis de amenazas. Se espera en la implementación una reducción en la tasa de incidentes a través de la identificación temprana de archivos sospechosos, lo que permitió actuar de manera preventiva.

Tercero, la validación de la implementación en un entorno controlado, con la participación de expertos en seguridad informática y experiencia en el área se soporte técnico a usuarios, confirma la eficacia del sistema en la reducción de incidentes de seguridad. Las métricas predefinidas, como la tasa de detección de malware y el tiempo de respuesta ante incidentes, demostraron mejoras significativas.

Los validadores señalan que, si bien la solución implementada es efectiva, se recomienda realizar ajustes en la configuración de reglas de detección y actualizar periódicamente las firmas de amenazas para optimizar su rendimiento a largo plazo.

RECOMENDACIONES

A partir del análisis de incidentes, se recomienda mantener un monitoreo continuo de los incidentes reportados en el área de soporte técnico, con el fin de actualizar periódicamente los requerimientos de seguridad y garantizar que el sistema Sandbox siga abordando las amenazas emergentes de manera efectiva.

Considerando la evaluación de sistemas Sandbox, se recomienda realizar revisiones periódicas de las tecnologías Sandbox disponibles en el mercado, considerando nuevas versiones y actualizaciones de las soluciones existentes, para asegurar que el sistema implementado continúe siendo la opción más adecuada en términos de detección y mitigación de amenazas.

Desde el punto de la validación de la implementación, se recomiendan establecer un proceso de auditoría y mejora continua basado en las métricas de desempeño obtenidas. Además, se debe capacitar regularmente al equipo de soporte técnico en el uso del sistema

y en la interpretación de los informes generados, garantizando así una respuesta eficiente ante posibles amenazas futuras.

REFERENCIAS

Asamblea Nacional del Ecuador. (2002). *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos*. Registro Oficial 557.

Asamblea Nacional del Ecuador. (2014). *Código Orgánico Integral Penal* (COIP). Registro Oficial Suplemento 180.

Asensi, A. (2024). *Entorno controlado de pruebas o sandbox regulatorio de los proyectos Fintech y en los sistemas de inteligencia artificial.* http://hdl.handle.net/10045/144321

Cervera, A., y Goussens, A. (2024). *Ciberseguridad y uso de las TIC en el Sector Salud.* https://www.sciencedirect.com/science/article/pii/S0212656723002871

Chamorro, A., Pupiales, S., y Hidalgo, J. (2023). Equipo de respuesta ante incidentes informáticos para la seguridad de la información (CSIRT-UPEC). https://revistasdigitales.upec.edu.ec/index.php/sathiri/article/view/1200

Chamorro, A., Pupiales, S., y Hidalgo, J. (2023). *Equipo de respuesta ante incidentes informáticos para la seguridad de la información* (CSIRT-UPEC). https://www.researchgate.net/publication/367458809_Equipo_de_respuesta_ante_incidentes_informaticos_para_la_seguridad_de_la_informacion_CSIRT-UPEC

Cisneros, S. (2024). *Alcance del sandbox regulatorio en empresas Fintech en Ecuador.* https://www.researchgate.net/publication/380621058_Alcance_del_sandbox_regulatorio_en_empresas_Fintech_en_Ecuador

Conforme, J., Bailon, E., Pilozo, L., y Marcillo, M. (2023). *Medios de ataques a los sistemas de seguridad de la información.* https://revistas.unesum.edu.ec/JTI/index.php/JTI/article/download/39/68/68

Corbo, A. (2021). *What Is Information Security? Builtin.* https://builtin.com/articles/information-security.

De Freitas, V. (2009). *Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar.* https://ve.scielo.org/scielo.php?script=sci_arttext&pid=S1690-75152009000100004

Escuela Europea de Excelencia. (2021). *Mitigación de riesgos: proceso de 3 pasos para hacer frente al riesgo*. Escuela Europea de Excelencia. https://www.escuelaeuropeaexcelencia.com/2021/06/mitigacion-de-riesgos-proceso-de-3-pasos-para-hacer-frente-al-riesgo/

Espinoza, L., Barriga, B., Izurieta, J., y Morales, C. (2022). *Seguridad informática aplicando la Autentificación por Doble factor para la plataforma HomeOfi.* https://dialnet.unirioja.es/descarga/articulo/8637935.pdf

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

Fruhlinger, J. (2023). *What is information security? Definition, principles, and jobs.* CSO. https://www.csoonline.com/article/568841/what-is-information-security-definition-principles-and-jobs.html

Guthrie, H. (2024). *Los sandbox regulatorios financieros como herramienta de control a la potestad regulatoria discrecional de los Estados.* https://rchdt.uchile.cl/index.php/RCHDT/article/view/72293

H. Jin Kang, H., Qin Sim, S., y Lo, D. (2021). *IoTBox: Sandbox Mining to Prevent Interaction Threats in IoT Systems. IEEEXplore.* https://ieeexplore.ieee.org/document/9438543

Hassan, A. (2023). *What Is a Sandbox Environment?*. https://builtin.com/software-engineering-perspectives/sandbox-environment#:~:text=A%20sandbox%20environment%20allows%20you%20to%20test%20new,they%20can%20cause%20damage%20to%20the%20live%20environment

Holdsworth, J., y Matthew, M. (2024). *What is information security (InfoSec)?*. IBM. https://www.ibm.com/topics/information-security#:~:text=Information%20security%20%28InfoSec%29%20is%20the%20protection%20of%20important,authorized%20users%2C%20remains%20confidential%20and%20maintains%20its%20integrity

Hornetsecurity. (2023). *What Is a Sandbox Environment? Exploring Their Definition and Range of Applications. Hornetsecurity.* https://www.hornetsecurity.com/en/blog/sandbox-environment/

IBM. (2024). *¿Qué es la respuesta a incidentes?* IBM. https://www.ibm.com/es-es/topics/incident-response

Kumaranlingam, T., y Wijayasekara, S. (2024). *Empowering Cybersecurity: Unveiling the Art of Identifying and Thwarting Malicious Tactics Within the Sandbox Environment. IEEEXplore*. https://ieeexplore.ieee.org/document/10594974

Kuo, J., Wen, Z., Huang, H., y Guo, I. (2022). *The Study on Security Online Judge System Applied Sandbox Technology. IEEEXplore.* https://ieeexplore.ieee.org/document/10051768

Ministerio de Hacienda y Administraciones Públicas. (2012). *MAGERIT – versión 3.0* Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Moes, T. (2023). *¿Qué es un entorno sandbox?* Todo sobre ello. https://softwarelab.org/es/blog/que-es-un-entorno-sandbox/#:~:text=Un%20entorno%20sandbox%20es%20una%20infraestructura%20de%20pruebas,el%20aprendizaje%20y%20la%20depuraci%C3%B3n%20de%20forma%20segura

Murguira, A. (s.f.). *Tipos de investigación y sus características*. questionpro. https://www.questionpro.com/blog/es/tipos-de-investigacion-de-mercados/

Nadeem, M., Wajiha, Z., y Arshad, A. (2023). *Ataque de phishing, sus detecciones y técnicas de prevención.* https://www.researchgate.net/publication/374848676_Phishing_Attack_Its_Detections_and_Prevention_Techniques

Navarro, L. (s.f.). *Incidentes de seguridad: qué son y cómo protegerte*. Hackmetrix. https://blog.hackmetrix.com/incidentes-de-seguridad-que-son-y-como-

protegerte/#:~:text=Los%20incidentes%20de%20seguridad%20pueden%20manifestarse%20de%20diversas,malware%2C%20ransomware%2C%20ataques%20DDoS%2C%20ataques%20por%20fuerza%20bruta

Navarro, L. (s.f.). *Incidentes de seguridad: qué son y cómo protegerte.* Hackmetrix. https://blog.hackmetrix.com/incidentes-de-seguridad-que-son-y-como-protegerte/

Navy Smart Grid using Supervised Learning. (s.f.). *IEEEXplore.* https://ieeexplore.ieee.org/document/9773814/authors#authors

NTE INEN-ISO/IEC. (2017). Tecnologías de la información ─ técnicas de seguridad ─ código de práctica para los controles de seguridad de la información (ISO/IEC 27002:2013+Cor. 1:2014+Cor. 2: 2015, IDT. https://app.virtualex.ec/documentos/nte_inen_iso_iec_27002.pdf

Patiño, J. (2020). *Soporte técnico y renovación tecnológica en la Empresa Alimentos Cárnicos S.A.S.* https://dspace.tdea.edu.co/bitstream/handle/tdea/1086/SOPORTE%20TECNICO%20Y%20RENOVACION.pdf?sequence=1&isAllowed=y

Quevedo, A., y Cárdenas, J. (2022). *Incidencia de la creación de un sandbox regulatorio y su impacto en el crecimiento de las Fintech de crowdfunding ecuatorianas.* https://ciencialatina.org/index.php/cienciala/article/view/3875

Quevedo, A., y Cárdenas, J. (2024). *Incidencia de la creación de un sandbox regulatorio y su impacto en el crecimiento de las Fintech de crowdfunding ecuatorianas.* https://ciencialatina.org/index.php/cienciala/article/download/3875/5885/

Rodríguez, P. (2020). *Análisis de riesgos informáticos y ciberseguridad.* https://www.ambit-bst.com/blog/an%C3%A1lisis-de-riesgos-inform%C3%A1ticos-y-ciberseguridad

Rosencrance, L. (2019). *10 tipos de incidentes de seguridad y cómo manejarlos.*

Sánchez, C. (2020). *Índice o Tabla de Contenido. Normas-apa*. https://normas-apa.org/estructura/indice-tabla-de-contenido/

Sierra, J. (2023). *Sandbox: ¿Qué es? Desde el Desarrollo de aplicaciones hasta la Seguridad informática. Software de ciberseguridad*. https://ciberseguridadtips.com/sandbox/

Swamy, S. (2020). *Sandbox: un marco de pruebas seguro para aplicaciones*. https://www.researchgate.net/publication/344170480_Sandbox_A_Secured_Testing_Framework_for_Applications

Thulasiraman, P. (2021). *Cyber Analytics for Intrusion Detection on the Navy Smart Grid using Supervised Learning*. IEEEXplore. https://ieeexplore.ieee.org/document/9773814/authors#authors

Torres, P. (2020). *Modelo de soporte técnico para la gestión de servicios tecnológicos en la administración pública nacional.* https://www.researchgate.net/publication/342024209_Modelo_de_soporte_tecnico_para_la_gestion_de_servicios_tecnologicos_en_la_administracion_publica_nacional

Trajanovski, T., y Zhang, N. (2021). An Automated and Comprehensive Framework for IoT Botnet Detection and Analysis (IoT-BDA). IEEEXplore. https://ieeexplore.ieee.org/document/9529169

ANEXOS

UNIVERSIDAD TÉCNICA DEL NORTE
Resolución No. 001-073 CEAACES-2013-13
INSTITUTO DE POSGRADO

PROPUESTA DE UN SISTEMA SANDBOX PARA MITIGAR INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE SOPORTE TÉCNICO A USUARIOS

Lineamientos Generales: El presente instrumento forma parte de la tesis de maestría titulada: "**PROPUESTA DE UN SISTEMA SANDBOX PARA MITIGAR INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE SOPORTE TÉCNICO A USUARIOS"**, el mismo que busca validar una propuesta de implementación de un sistema de análisis de amenazas informáticas en entorno controlado. La presente propuesta se enmarca en un abordaje de las necesidades identificadas en el capítulo cuatro respecto a los incidentes de seguridad reportados en el área de soporte técnico a usuarios, respecto a la identificación de los requerimientos más comunes y que pueden ser mitigados con la implementación de un sistema Sandbox.

Esta consiste en la implementación de un sistema de análisis de amenazas informáticas en un entorno controlado, con el propósito de fortalecer la seguridad en el área de soporte técnico a usuarios. Este sistema permitirá examinar archivos y programas sospechosos antes de que se ejecuten en los equipos y redes de la organización, evitando la propagación de malware, ataques de phishing y accesos no autorizados.

A partir de estas exposiciones, esta propuesta constituye una respuesta al análisis de riesgos realizado previamente, el cual identificó que una parte significativa de los incidentes de seguridad informática en las organizaciones proviene de archivos maliciosos que ingresan a los sistemas a través de correos electrónicos, descargas y dispositivos extraíbles. Frente a esta problemática, la implementación de un sistema especializado en la detección y aislamiento de amenazas permitirá mejorar la capacidad de respuesta ante posibles ataques y minimizar el impacto en la infraestructura tecnológica.

En cuanto a la funcionalidad, este sistema operará en un entorno controlado dentro del área de soporte técnico, donde se analizarán archivos y programas sospechosos sin comprometer la seguridad de los sistemas en producción. A través de pruebas automatizadas y análisis de comportamiento, se generarán informes detallados que facilitarán la toma de decisiones sobre

la confiabilidad de los archivos, contribuyendo a una gestión más eficiente de la seguridad informática.

En esta línea, la solución será evaluada con métricas específicas, como la reducción de incidentes de seguridad, la velocidad de respuesta ante amenazas y la mejora en la identificación de ataques. El sistema se implementará de manera gradual, permitiendo su adaptación y optimización en función de las necesidades de la organización y la retroalimentación recibida por parte de los profesionales del área de soporte técnico.

Estimado validador a continuación se presenta el sistema de objetivos de la investigación con la finalidad de proporcionar información para la evaluación de la pertinencia y coherencia del presente instrumento.

Objetivo General

- Realizar una propuesta de un sistema Sandbox efectivo para mitigar los incidentes de seguridad de la información para el área de soporte técnico a usuarios, basado en un análisis de riesgos.

Objetivos Específicos

- Analizar los incidentes de seguridad reportados en el área de soporte técnico a usuarios para identificar los requerimientos más comunes y que pueden ser mitigados con la implementación de un sistema Sandbox.
- Evaluar sistemas Sandbox opensource o propietario que se adapten a las necesidades identificadas en la fase de análisis, con el objetivo de minimizar el número de incidentes de seguridad en base a un análisis de riesgos.
- Validar la implementación del sistema Sandbox evaluado, con ayuda de profesionales del área de soporte técnico a usuarios quienes puedan argumentar la eficacia en la reducción de incidentes de seguridad, utilizando métricas predefinidas.

SISTEMAS SANDBOX PARA MITIGACIÓN DE RIESGOS EN SEGURIDAD INFORMÁTICA

Sistema	Tipo	Descripción	Necesidades que atiende	Beneficios y ventajas	Diferencias / Limitaciones	ISO/IEC 25010: Características de Calidad
Cuckoo Sandbox	Código abierto	Framework de análisis automatizado de malware que	Detección de malware y ataques dirigidos,	- Análisis profundo de malware con informes	- Requiere conocimientos técnicos para	**Funcionalidad**: Alta precisión en análisis de malware.

		ejecuta archivos sospechosos en un entorno virtualizado para identificar su comportamiento.	identificación de tráfico malicioso, prevención de ataques de phishing y spam.	detallados. - Compatible con múltiples entornos (Windows, Linux, macOS, Android). - Integración con herramientas de seguridad como YARA y Suricata.	implementación y ajuste. - Puede generar falsos positivos en entornos corporativos.	**Desempeño**: Buen rendimiento en varios entornos. **Usabilidad**: Requiere conocimientos técnicos. **Seguridad**: Puede generar falsos positivos. **Mantenibilidad**: Requiere ajustes continuos.
FireEye MVX	Propietario	Solución avanzada de detección de amenazas basada en virtualización y análisis de comportamiento.	Identificación de ataques APT, intentos de acceso no autorizado, amenazas persistentes avanzadas.	- Tecnología de detección basada en inteligencia artificial. - Análisis en tiempo real con respuesta automática. - Integración con SIEM y plataformas de seguridad empresarial.	- Costo elevado, solo accesible para grandes organizaciones. - Dependencia del ecosistema FireEye.	**Funcionalidad**: Detección avanzada de amenazas. **Desempeño**: Análisis en tiempo real. **Compatibilidad**: Integración con otras herramientas. **Usabilidad**: Alta, pero con costos elevados. **Seguridad**: Alta fiabilidad.
Any.Run	Propietario (basado	Plataforma interactiva de análisis de malware en	Análisis de ataques de phishing, amenazas	- Entorno interactivo para visualizar	- Versión gratuita con funcionalidades limitadas.	**Funcionalidad**: Análisis interactivo en tiempo real.

	en la nube)	tiempo real que permite a los analistas observar comportamientos en una interfaz intuitiva.	internas, intentos de acceso no autorizado.	ataques en tiempo real. - Fácil de usar sin necesidad de infraestructura local. - Compatible con múltiples formatos de archivos.	- Dependencia de conexión a Internet.	**Desempeño**: Adecuado para análisis rápidos. **Usabilidad**: Muy fácil de usar. **Seguridad**: Menor control sobre datos en la nube. **Portabilidad**: Alta, ya que es basado en la nube.
VxStream Sandbox	Propietario	Sistema de análisis de malware en profundidad con tecnología híbrida de detección de amenazas.	Protección contra malware, ransomware, ataques de phishing y amenazas avanzadas.	- Uso de aprendizaje automático para detección más precisa. - Generación de informes avanzados y automatización de respuestas. - Integración con herramientas como VirusTotal y MITRE ATT&CK.	- Requiere licencia para funcionalidades avanzadas. - No permite una personalización profunda en entornos cerrados.	**Funcionalidad**: Análisis profundo con IA. **Desempeño**: Alta precisión en detección. **Mantenibilidad**: Requiere licencia para funciones avanzadas. **Seguridad**: Alta confiabilidad en detección.

101

Joe Sandbox	Propietario con versión Community	Plataforma avanzada de análisis de malware con soporte para múltiples plataformas y entornos de ejecución.	Análisis detallado de malware, prevención de ataques internos y externos, detección de amenazas ocultas.	- Compatible con Windows, Linux, macOS, Android y iOS. - Permite análisis estático y dinámico de amenazas. - Opciones de implementación en nube o local.	- Versión gratuita con restricciones de uso. - Mayor complejidad de configuración para análisis personalizados.	**Funcionalidad**: Análisis estático y dinámico avanzado. **Desempeño**: Alta capacidad de análisis. **Usabilidad**: Requiere configuraciones personalizadas. **Seguridad**: Soporta múltiples plataformas. **Portabilidad**: Flexible, con opciones locales y en la nube.

INSTRUMENTO DE VALIDACIÓN

Instrucciones: En el siguiente formato, indique según la escala excelente (E), bueno (B) o mejorable (M) en cada ítem, de acuerdo con los criterios de validación (coherencia, pertinencia, redacción), si es necesario agregue las observaciones que considere. Al final se deja un espacio para agregar observaciones generales.

Ítem Nro.	Validación			Observación
	Coherencia	Pertinencia	Redacción	
1	E	E	E	
2	E	E	E	
3	E	E	E	
4	E	E	E	

5	E	E	E	

Observaciones generales

El sistema Sandbox ha demostrado ser altamente eficiente en la detección, contención y análisis de amenazas informáticas. La implementación fue exitosa y se logró una notable reducción en la cantidad de incidentes de seguridad. Para maximizar su potencial, se recomienda mejorar la integración con sistemas de prevención de intrusiones y optimizar la interfaz de informes.

Datos del Validador 1

Mgs. Cristhian Gabriel Morales Hidalgo

Magister en Seguridad Informática

PROPUESTA DE UN SISTEMA SANDBOX PARA MITIGAR INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE SOPORTE TÉCNICO A USUARIOS

Lineamientos Generales: El presente instrumento forma parte de la tesis de maestría titulada: "**PROPUESTA DE UN SISTEMA SANDBOX PARA MITIGAR INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE SOPORTE TÉCNICO A USUARIOS**", el mismo que busca validar una propuesta de implementación de un sistema de análisis de amenazas informáticas en entorno controlado. La presente propuesta se enmarca en un abordaje de las necesidades identificadas en el capítulo cuatro respecto a los incidentes de seguridad reportados en el área de soporte técnico a usuarios, respecto a la identificación de los requerimientos más comunes y que pueden ser mitigados con la implementación de un sistema Sandbox.

Esta consiste en la implementación de un sistema de análisis de amenazas informáticas en un entorno controlado, con el propósito de fortalecer la seguridad en el área de soporte técnico a usuarios. Este sistema permitirá examinar archivos y programas sospechosos antes de que se ejecuten en los equipos y redes de la organización, evitando la propagación de malware, ataques de phishing y accesos no autorizados.

A partir de estas exposiciones, esta propuesta constituye una respuesta al análisis de riesgos realizado previamente, el cual identificó que una parte significativa de los incidentes de seguridad informática en las organizaciones proviene de archivos maliciosos que ingresan a los sistemas a través de correos electrónicos, descargas y dispositivos extraíbles. Frente a esta problemática, la implementación de un sistema especializado en la detección y aislamiento de amenazas permitirá mejorar la capacidad de respuesta ante posibles ataques y minimizar el impacto en la infraestructura tecnológica.

En cuanto a la funcionalidad, este sistema operará en un entorno controlado dentro del área de soporte técnico, donde se analizarán archivos y programas sospechosos sin comprometer la seguridad de los sistemas en producción. A través de pruebas automatizadas y análisis de comportamiento, se generarán informes detallados que facilitarán la toma de decisiones sobre la confiabilidad de los archivos, contribuyendo a una gestión más eficiente de la seguridad informática.

En esta línea, la solución será evaluada con métricas específicas, como la reducción de incidentes de seguridad, la velocidad de respuesta ante amenazas y la mejora en la identificación de ataques. El sistema se implementará de manera gradual, permitiendo su adaptación y optimización en función de las necesidades de la organización y la retroalimentación recibida por parte de los profesionales del área de soporte técnico.

Estimado validador a continuación se presenta el sistema de objetivos de la investigación con la finalidad de proporcionar información para la evaluación de la pertinencia y coherencia del presente instrumento.

Objetivo General

- Realizar una propuesta de un sistema Sandbox efectivo para mitigar los incidentes de seguridad de la información para el área de soporte técnico a usuarios, basado en un análisis de riesgos.

Objetivos Específicos

- Analizar los incidentes de seguridad reportados en el área de soporte técnico a usuarios para identificar los requerimientos más comunes y que pueden ser mitigados con la implementación de un sistema Sandbox.
- Evaluar sistemas Sandbox opensource o propietario que se adapten a las necesidades identificadas en la fase de análisis, con el objetivo de minimizar el número de incidentes de seguridad en base a un análisis de riesgos.
- Validar la implementación del sistema Sandbox evaluado, con ayuda de profesionales del área de soporte técnico a usuarios quienes puedan argumentar la eficacia en la reducción de incidentes de seguridad, utilizando métricas predefinidas.

SISTEMAS SANDBOX PARA MITIGACIÓN DE RIESGOS EN SEGURIDAD INFORMÁTICA

Sistema	Tipo	Descripción	Necesidades que atiende	Beneficios y ventajas	Diferencias / Limitaciones	ISO/IEC 25010: Características de Calidad
Cuckoo Sandbox	Código abierto	Framework de análisis automatizado de malware que ejecuta archivos sospechosos en un entorno	Detección de malware y ataques dirigidos, identificación de tráfico	- Análisis profundo de malware con informes detallados. - Compatible con múltiples	- Requiere conocimientos técnicos para implementación y ajuste. - Puede	**Funcionalidad**: Alta precisión en análisis de malware. **Desempeño**: Buen rendimiento en

		virtualizado para identificar su comportamiento.	malicioso, prevención de ataques de phishing y spam.	entornos (Windows, Linux, macOS, Android). - Integración con herramientas de seguridad como YARA y Suricata.	generar falsos positivos en entornos corporativos.	varios entornos. **Usabilidad**: Requiere conocimientos técnicos. **Seguridad**: Puede generar falsos positivos. **Mantenibilidad**: Requiere ajustes continuos.
FireEye MVX	Propietario	Solución avanzada de detección de amenazas basada en virtualización y análisis de comportamiento.	Identificación de ataques APT, intentos de acceso no autorizado, amenazas persistentes avanzadas.	- Tecnología de detección basada en inteligencia artificial. - Análisis en tiempo real con respuesta automática. - Integración con SIEM y plataformas de seguridad empresarial.	- Costo elevado, solo accesible para grandes organizaciones. - Dependencia del ecosistema FireEye.	**Funcionalidad**: Detección avanzada de amenazas. **Desempeño**: Análisis en tiempo real. **Compatibilidad**: Integración con otras herramientas. **Usabilidad**: Alta, pero con costos elevados. **Seguridad**: Alta fiabilidad.
Any.Run	Propietario (basado en la nube)	Plataforma interactiva de análisis de malware en tiempo real que permite a los analistas	Análisis de ataques de phishing, amenazas internas, intentos de	- Entorno interactivo para visualizar ataques en tiempo real. - Fácil de	- Versión gratuita con funcionalidades limitadas. - Dependencia	**Funcionalidad**: Análisis interactivo en tiempo real. **Desempeño**: Adecuado para análisis rápidos.

106

		observar comportamientos en una interfaz intuitiva.	acceso no autorizado.	usar sin necesidad de infraestructura local. - Compatible con múltiples formatos de archivos.	de conexión a Internet.	**Usabilidad**: Muy fácil de usar. **Seguridad**: Menor control sobre datos en la nube. **Portabilidad**: Alta, ya que es basado en la nube.
VxStream Sandbox	Propietario	Sistema de análisis de malware en profundidad con tecnología híbrida de detección de amenazas.	Protección contra malware, ransomware, ataques de phishing y amenazas avanzadas.	- Uso de aprendizaje automático para detección más precisa. - Generación de informes avanzados y automatización de respuestas. - Integración con herramientas como VirusTotal y MITRE ATT&CK.	- Requiere licencia para funcionalidades avanzadas. - No permite una personalización profunda en entornos cerrados.	**Funcionalidad**: Análisis profundo con IA. **Desempeño**: Alta precisión en detección. **Mantenibilidad**: Requiere licencia para funciones avanzadas. **Seguridad**: Alta confiabilidad en detección.
Joe Sandbox	Propietario con versión	Plataforma avanzada de análisis de malware con soporte para	Análisis detallado de malware, prevención de ataques	- Compatible con Windows, Linux, macOS,	- Versión gratuita con restricciones de uso. - Mayor	**Funcionalidad**: Análisis estático y dinámico avanzado. **Desempeño**:

107

	Commu nity	múltiples plataformas y entornos de ejecución.	internos y externos, detección de amenazas ocultas.	Android y iOS. - Permite análisis estático y dinámico de amenazas. - Opciones de implementaci ón en nube o local.	complejidad de configuración para análisis personalizado s.	Alta capacidad de análisis. **Usabilidad**: Requiere configuraciones personalizadas. **Seguridad**: Soporta múltiples plataformas. **Portabilidad**: Flexible, con opciones locales y en la nube.

INSTRUMENTO DE VALIDACIÓN

Instrucciones: En el siguiente formato, indique según la escala excelente (E), bueno (B) o mejorable (M) en cada ítem, de acuerdo con los criterios de validación (coherencia, pertinencia, redacción), si es necesario agregue las observaciones que considere. Al final se deja un espacio para agregar observaciones generales.

Ítem Nro.	Validación			Observación
	Coherencia	Pertinencia	Redacción	
1	E	E	E	
2	E	E	E	
3	E	E	E	
4	E	E	E	
5	E	E	E	

Observaciones generales

La implementación del sistema Sandbox fue exitosa, logrando una reducción significativa en incidentes de seguridad y una integración efectiva con herramientas existentes. Se recomienda continuar con actualizaciones periódicas y optimizar la usabilidad de los informes generados.

Datos del Validador 2

Mgs. Edison Richard Cóndor Licero

EDISON RICHARD CONDOR LICERO

Magíster en Seguridad Informática

109