UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

CARRERA DE LA MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

TEMA:

“HONEYPOT COMO HERRAMIENTA DE PREVENCIÓN Y DETECCIÓN DE CIBERATAQUES EN LAS REDES DE DATOS DE LA COOPERATIVA DE AHORRO Y CREDITO 23 DE JULIO”

Trabajo previo a la obtención del título en la Magíster en Computación Mención Seguridad Informática**.**

Línea de investigación: Desarrollo, aplicación de software y cyber security

AUTOR:

ROSERO BALSECA CÉSAR ALFONSO

DIRECTOR:

PUSDÁ CHULDE MARCO REMIGIO

IBARRA – ECUADOR 2025

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:

<table>
<tr><th colspan="4">DATOS DE CONTACTO</th></tr>
<tr><td>CÉDULA DE IDENTIDAD:</td><td colspan="3">1713974812</td></tr>
<tr><td>APELLIDOS Y NOMBRES:</td><td colspan="3">Rosero Balseca César Alfonso</td></tr>
<tr><td>DIRECCIÓN:</td><td colspan="3">Conjunto Residencial San Francisco perimetral izquierda y calle s casa 551, Sangolquí, Pichincha, Ecuador</td></tr>
<tr><td>EMAIL:</td><td colspan="3">alfonsin19@hotmail.com</td></tr>
<tr><td>TELÉFONO FIJO:</td><td></td><td>TELÉFONO MÓVIL:</td><td>0999795350</td></tr>
</table>

DATOS DE LA OBRA	
TÍTULO:	HONEYPOT COMO HERRAMIENTA DE PREVENCIÓN Y DETECCIÓN DE CIBERATAQUES EN LAS REDES DE DATOS DE LA COOPERATIVA DE AHORRO Y CREDITO 23 DE JULIO.
AUTOR (ES):	ROSERO BALSECA CÉSAR ALFONSO
FECHA:	27/11/2025
PROGRAMA:	☐ **PREGRADO** ☒ **POSGRADO**
TITULO POR EL QUEOPTA:	Magíster en Computación con mención en seguridad informática
ASESOR /DIRECTOR:	PUSDÁ CHULDE MARCO REMIGIO / GARCÍA SANTILLAN IVÁN DANILO

2. CONSTANCIAS

El autor Rosero Balseca César Alfonso, manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lotanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asumela responsabilidad sobre el contenido de esta y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 27 días del mes de noviembre del 2025

EL AUTOR:

CESAR ALFONSO ROSERO BALSECA

Firmado digitalmente por CESAR ALFONSO ROSERO BALSECA
Fecha: 2025.11.27 13:16:28 -05'00'

Firma: .....

Nombre: César Alfonso Rosero Balseca

APROBACIÓN DEL TUTOR

Yo Ph.D. PUSDÁ CHULDE MARCO REMIGIO, en calidad de director de la tesis titulada: “HONEYPOT COMO HERRAMIENTA DE PREVENCIÓN Y DETECCIÓN DE CIBERATAQUES EN LAS REDES DE DATOS DE LA COOPERATIVA DE AHORRO Y CREDITO 23 DE JULIO.” de auditoría del Ing. Rosero Balseca César Alfonso, para optar por el grado de Magister en Computación con Mención en Seguridad Informática, doy fe de que dicho trabajo reúne los requisitos y méritos suficientes para ser sometidos a presentación privada y evaluación por parte del jurado examinador que se designe.

En la ciudad de Ibarra, a los 27 días del mes de noviembre del 2025

Lo certifico

MARCO REMIGIO PUSDA CHULDE

Firmado digitalmente por MARCO REMIGIO PUSDA CHULDE
Fecha: 2025.11.27 14:44:48 -05'00'

Ing. PUSDÁ CHULDE MARCO REMIGIO,

PhD. DIRECTOR DE TESIS

DEDICATORIA

A mi esposa, por ser mi compañera incansable, brindándome su amor, apoyo y comprensión en cada paso de este viaje. A mis hijas, que llenan mi vida de sentido y me recuerdan cada día la importancia de esforzarme y seguir adelante. Ustedes son mi mayor inspiración y motivo de orgullo.

La presente tesis va dedicada a mi Madre, ya que su apoyo ha sido incondicional en mi vida y más aún en el desarrollo de este trabajo. Doy las gracias por estar a mi lado en cada momento, por ser parte de mis alegrías y más aún por ser mi motor.

Y por supuesto, también a mi padre, que desde el cielo sigue guiando mis pasos. Aunque ya no esté físicamente, su legado y enseñanzas continúan siendo la guía y la fortaleza en mi vida.

Este proyecto es para todos ustedes, quienes con su amor y apoyo me han ayudado a alcanzar cada una de mis metas.

César Alfonso Rosero Balseca

AGRADECIMIENTOS

A mi esposa e hijas, por su amor y apoyo incondicional, que han sido mi mayor motivación. A mi madre, por su sabiduría y constante acompañamiento, y a mi padre, que desde el cielo sigue siendo una guía en mi vida.

Un enorme agradecimiento a la Cooperativa de Ahorro y Crédito "23 de Julio", ya que me abrieron las puertas para desarrollar la tesis en esta prestigiosa institución. A su vez agradezco a los trabajadores que fueron un pilar para este proyecto que fue la pieza clave para alcanzar el objetivo.

César Alfonso Rosero Balseca

ÍNDICE GENERAL

ÍNDICE DE TABLAS

INDICE DE FIGURAS

INDICE DE GRÁFICOS

RESUMEN

La Cooperativa de Ahorro y Crédito 23 de Julio enfrenta riesgos en ciberseguridad el motivo se centra en la vulnerabilidad de su red interna en los cuales se involucran los accesos no autorizados o inclusive ataques de denegación. Son incidentes que complican la seguridad de la información y a su vez la operatividad generando de esta manera un riesgo significante a la información financiera de cada uno de los socios.

El objetivo vital de la tesis se centra en poder mejorar la seguridad de la red interna de la Cooperativa a través de la identificación de las amenazas anticipadas logrando no comprometer los sistemas críticos de la empresa. La metodología que se centró en un enfoque mixto, en el cual se realizó un análisis de las amenazas de la empresa de esta manera permitió evaluar las posibles soluciones de un Honeypot y que su aplicación sea validad para que así sea efectiva en el entorno.

En cuanto a los resultados permitieron determinar que el Honeypot fue capaz de detectar las amenazas para que de esta forma se proporcione información valiosa, es así como permitió mejorar la capacidad de la empresa ante las respuestas de la amenaza.

En general, la implementación del honeypot fue exitosa, pues mejoró la seguridad de la red interna de la cooperativa y redujo los incidentes de seguridad. Como recomendación a la presente investigación, se indicó continuar el uso del honeypot y actualizar periódicamente las medidas de seguridad.

En conclusión, la implementación del Honeypot fue exitosa, mejorando la seguridad de la red interna y reduciendo los incidentes de seguridad. Se recomienda continuar su uso y actualizar periódicamente las medidas de seguridad para mantenerse a la vanguardia ante posibles amenazas.

Palabras Clave: Ciberseguridad, ciberataques, Honeypot, vulnerabilidad, seguridad

ABSTRACT

The 23 de Julio Savings and Credit Cooperative faces cybersecurity risks due to the vulnerability of its internal network, which involves unauthorized access and even denial-of-service attacks. These incidents compromise information security and, in turn, operational efficiency, thus posing a significant risk to the financial information of each of the members.

The main objective of the thesis is to improve the security of the Cooperative's internal network by identifying anticipated threats and ensuring that the company's critical systems are not compromised. The methodology focused on a mixed approach, in which an analysis of the company's threats was carried out, thus allowing the possible solutions of a Honeypot to be evaluated and its application to be validated so that it is effective in the environment.

The results showed that the honeypot was able to detect threats, thus providing valuable information and improving the company's ability to respond to threats.

Overall, the implementation of the honeypot was successful, as it improved the security of the cooperative's internal network and reduced security incidents. As a recommendation to this research, it was suggested to continue using the honeypot and to periodically update security measures.

In conclusion, the implementation of the Honeypot was successful, enhancing the security of the internal network and reducing security incidents. It is recommended to continue its use and periodically update security measures to stay ahead of potential threats.

Keywords: Keywords: Cybersecurity, cyberattacks, Honeypot, vulnerability, security.

GLOSARIO DE TÉRMINOS

Término	**Definición**
Ciberataques	Intentos maliciosos de comprometer sistemas informáticos para robar, alterar o destruir información.
Confidencialidad	Principio que remarca que los datos estén solamente accesibles (al alcance) a aquellos usuarios y sistemas que estén autorizados.
Ciclo por instrucción (CPI)	Medida para evaluar la eficiencia del procesamiento de un sistema y que se calcula a través del número de ciclos de CPU necesarios para completar una instrucción.
Firewall (Cortafuegos)	Es una herramienta que se usa para la seguridad, su característica principal es centrarse en el control de tráfico de red, de esa manera bloquea los accesos pero a su vez

	dependerá de las configuraciones.
HIDS (Sistema de Detección de Intrusos en el Host)	Es un sistema que busca monitorear la actividad en un dispositivo para identificar las posibles intrusiones o amenazas que son anomalías.
Honeypot	Es un sistema de seguridad que fue diseñado para generar simulaciones de vulnerabilidad cuyo fin es la de atraer ataques para determinar las tácticas que usan.
HoneyNet	Red de Honeypots interconectados diseñada para parecer una red real, atrayendo a los atacantes para estudiar sus métodos de ataque.
Integridad	Principio que remarca que los datos no pueden ser modificados o alterados de manera no autorizada.

IPS (Sistema de Prevención de Intrusos)	Herramienta utilizada en el ámbito de la seguridad, que además de detectar, también previene los ataques mediante la intervención activa en la red.
Reducción de incidentes de seguridad	Se lo denomina como un proceso que busca minimizar los riesgos y los problemas de seguridad por medio de medidas preventivas.
Seguridad de la Información	Es el conjunto de técnicas, procedimientos, políticas, métodos y herramientas los cuales se encargan de proteger la confidencialidad, integridad y disponibilidad de los datos.
Vulnerabilidad	Se lo determina como una falla o debilidad de un sistema informático, ya sea en sus procedimientos de seguridad o de diseño que pueden ser explotados violando la política de seguridad.

INTRODUCCIÓN

La tecnología actual resulta beneficiosa para la sociedad, pero también puede representar una brecha para la generación de nuevas amenazas en el campo de la seguridad informática. Por ello, las organizaciones tienen la necesidad de implementar nuevas estrategias y medidas de seguridad tanto a nivel físico como virtual, con el fin de proteger los equipos y sistemas conectados a las redes de internet. Existen varias herramientas de seguridad, y una de las soluciones más efectivas es la configuración de un Honeypot. Esta herramienta permite simular un sistema vulnerable y controlado dentro de una red de datos, con el propósito de atraer a ciberdelincuentes y recopilar información sobre los métodos que utilizan para acceder a los recursos o servicios de la red.

La información que se aloja en el sistema informático es generada por personal experto en el área de redes, pero al mismo tiempo existen atacantes que utilizan esta información de forma mal intencionada, ya que un usuario pude acceder a las redes mediante el Internet o de forma local, los atacantes pueden utilizar diversos paquetes de software que les permite infiltrarse en las redes y robar información de gran importancia dentro de nuestra organización.

En el Capítulo I: el problema, se ha realizado un análisis de la situación actual de la Cooperativa de Ahorro y Crédito 23 de Julio, identificando vulnerabilidades en su infraestructura de red interna que la exponen a diversos ciberataques. Estas amenazas comprometen la confidencialidad, integridad y disponibilidad de la información, poniendo en riesgo la seguridad informática de la institución. En el presente capítulo se permite la definición y justificación del problema de investigación, la determinación de los objetivos generales y específicos, así como la formulación de las hipótesis que se validarán a lo largo del proyecto a elaborar, para finalmente diseñar e implementar una solución, en base a la integración de un Honeypot que fortalezca la seguridad de la red y disminuya los posibles ataques.

En el Capítulo II, marco referencial, se revisan los conceptos teóricos que son necesarios para poder entender la seguridad informática, las amenazas más comunes y el rol a desempeñar por los sistemas de detección de intrusos como son los Honeypots, así como la retroalimentación de investigaciones pasadas y las disposiciones legales aplicables en relación con la seguridad de la información en Ecuador. Este capítulo proporciona la base conceptual y normativa que sustenta el desarrollo del proyecto, explicando la importancia de las tecnologías avanzadas en la protección contra ciberataques.

En el tercer capítulo, el marco metodológico, se encuentran los métodos y enfoques que se emplean para la investigación de la problemática, los cuales combinan métodos de tipo cualitativo y cuantitativos. Es el capítulo en donde se expone el proceso de recolección de la información, el análisis que se realiza de los datos y la forma en cómo se diseña la implementación del Honeypot en la cooperativa. Narra también, como se determinaron y evaluaron las herramientas tecnológicas con las que se trabajó, las formas en las cuales se realizó el monitoreo y la validación de los resultados obtenidos.

Por último, el IV capítulo, resultados y discusión, describe los hallazgos que se identifica una vez que se ha realizado la implementación del Honeypot. En este capítulo se habla de los intentos de intrusión que se logran detectar, del análisis de patrones de ataque y la reducción de incidentes de seguridad que se logra al implementar este tipo de herramientas en la cooperativa. También se mencionan la mejora de la seguridad de la red interna de la cooperativa, las limitaciones y los problemas que se identifican, terminando el capítulo con los resultados, asimismo, con las conclusiones y recomendaciones a fin de mejorar la estrategia de seguridad de la cooperativa en el futuro.

CAPÍTULO I

EL PROBLEMA

El fácil acceso a las redes de información ha impulsado también la evolución de las técnicas de ataque y los escenarios típicos de amenazas en sistemas que operan bajo Internet, que abarcan las vulnerabilidades, los ataques cibernéticos y los riesgos derivados de la exposición de datos, comprometiendo la seguridad y continuidad del servicio. Los delitos informáticos más comunes que podrían presentarse son el acceso no autorizado a sistemas críticos de la entidad, ataques de denegación de servicio (DDoS), ataques a servidores a partir de conexiones externas, entre otros. En la Cooperativa de Ahorro y Crédito 23 de Julio, por ejemplo, la seguridad informática de los sistemas de las agencias fue violentada intencionalmente con equipos del mismo departamento, sin que se advirtiera que el autor del delito informático era la portátil de un funcionario. Con el propósito de mitigar este problema, se sugiere poner en práctica un Honeypot como tecnología de mitigación y detección de ciberataques en las redes de datos de la Cooperativa que garanticen la seguridad de la información en su red interna.

1.1.Problema de investigación

La disponibilidad inmediata de redes de información, ha impulsado el desarrollo de nuevas técnicas de ataque, aumentando así las amenazas para los sistemas que funcionan en línea. En la Cooperativa de Ahorro y Crédito 23 de Julio, ciertas vulnerabilidades han sido expuestas como ser el acceso no autorizado a sistemas sensibles, el ataque de denegación de servicio DDoS y el compromiso de servidores desde enlaces externos. Un caso significativo fue el compromiso deliberado de la seguridad informática en algunas de las agencias, donde una portátil propiedad de un funcionario, sin el conocimiento del mismo, fue usada como medio para cometer un delito informático. Esta situación pone de manifiesto la inmediata necesidad

de blindar la seguridad y establecer estrategias que contrarresten de manera efectiva los riesgos detectados.

1.2.Interrogantes de la investigación

¿Cómo se puede implementar un Honeypot en las redes de datos de la Cooperativa de Ahorro y Crédito 23 de Julio para prevenir y detectar ciberataques, asegurando la protección de la información en su red interna?

1.3.Delimitación

- **Área académica:** Departamento de Seguridad de la Información.
- **Línea de investigación:** Ciberseguridad.
- **Sublínea de investigación:** Seguridad Informática.
- **Delimitación temporal:** La investigación se llevará a cabo en un periodo de seis meses, contados a partir de la fecha de aprobación por parte del Consejo Directivo.
- **Delimitación espacial:** La investigación se realizará en un plazo de seis meses, comenzando desde la fecha de aprobación por parte del Consejo Directivo.

1.4.Objetivos

2. Objetivo general

Implementar un Honeypot como herramienta de prevención y detección de ciberataques en las redes de datos de la Cooperativa de Ahorro y Crédito 23 de Julio que garanticen la seguridad de la información en su red interna.

3. Objetivos específicos

- Analizar el estado actual de la seguridad en la red interna de la cooperativa, identificando posibles vulnerabilidades mediante pruebas sin la presencia del Honeypot.

- Diseñar e implementar un entorno de Honeypot que permita la detección de ataques en tiempo actual.
- Comparar los resultados de monitoreo, al inicio y posteriormente de la implementación del Honeypot, de esta manera se evaluará la efectividad para detectar y mitigar las amenazas.
- Elaborar un manual de políticas en seguridad de la información para la cooperativa de manera que se corrija las vulnerabilidades e inconsistencias por medio de los resultados después de la implementación del Honeypot

3.1.Hipótesis de trabajo

La implementación de un Honeypot para la prevención y detección de ciberataques garantizará la seguridad de la información en la red interna de la Cooperativa de Ahorro y Crédito 23 de Julio.

3.2.Categorización de variables

- **Variable Independiente:** Implementación de un Honeypot para la prevención y detección de ciberataques.
- **Variable Dependiente:** Seguridad de la información en la red interna de la Cooperativa de Ahorro y Crédito 23 de Julio.

3.3.Justificación

La Seguridad de la Información tiene como objetivo principal la protección de la información y de los sistemas de información contra el acceso, uso, divulgación, interrupción o destrucción no autorizada. Actualmente, la Cooperativa de Ahorro y Crédito 23 de Julio se ha propuesto identificar las vulnerabilidades presentes en sus redes de datos y sistemas informáticos. Si bien se han implementado medidas de seguridad a nivel administrativo, es

necesario abordar las inseguridades a un nivel más técnico y general, acorde a las necesidades de la cooperativa.

El uso de un honeypot como herramienta de seguridad de la información, consiste en el diseño de una honeynet que pueda ser comprometida (con vulnerabilidades) por intrusos. Este método permite analizar las técnicas y estrategias utilizadas por los atacantes para acceder y vulnerar la red, y así implementar soluciones efectivas para contrarrestar los problemas de seguridad informática dentro de la cooperativa.

La propuesta denominada “Honeypot como metodología de prevención y detección de ciberataques en las redes de datos de la Cooperativa de Ahorro y Crédito 23 de Julio " es viable en un principio, hoy que contiene una propuesta que se desarrolla en el marco de una investigación en el área de las redes de la cooperativa. El tema es relevante, ya que posibilitará un mejor control de la seguridad informática de la entidad, brindando recomendaciones de cómo evitar delitos informáticos posibles y resguardar la seguridad dentro de la misma entidad.

La aplicación de esta resulta muy útil, ya que permite conocer y neutralizar amenazas posibles, al mismo tiempo que permite proteger a socios, clientes, trabajadores y en definitiva, a todas las personas que ingresan, de manera directa o indirecta, en interacción con las redes de datos de la cooperativa.

CAPÍTULO II

MARCO REFERENCIAL

4.1.Antecedentes

Hoy en día, la comunicación entre ordenadores o equipos informáticos es de vital importancia en el ámbito global, especialmente en el campo de la seguridad informática. El volumen de redes conectadas entre sí a nivel mundial ha superado cualquier expectativa inicial. Las empresas, que manejan grandes cantidades de información a través de sus canales informáticos, destinan recursos humanos y económicos para proteger su seguridad, dado que esta es uno de los activos más importantes dentro de las organizaciones. Es por esto que surgen continuamente nuevas tecnologías diseñadas para contrarrestar las amenazas cibernéticas (Jacintogr, 2020).

En Zambrano et al. (2021), se evaluó la implementación de un honeypot para mejorar la disponibilidad de la red en el Cuerpo de Bomberos de Portoviejo (CBP). Esta herramienta permitió analizar vulnerabilidades, monitorear la red y aplicar técnicas de hacking ético; pero el resultado final fue solo un 42.86% de disponibilidad de la red. Este porcentaje muestra que aunque un honeypot es útil para detectar amenazas y mejorar la seguridad, la infraestructura de red aún necesita optimización.

Jumbo y García (2024), en su estudio titulado " Implementación de un sistema de detección de intrusiones proporcionando Honeypots específicamente para el seudo - procesamiento de pagos y la creación de transacciones falsas, dedicados a la realización de transacciones en línea", simularon procesos de pagos e intercepciones, poniendo especial énfasis en los procesos de pago del sector financiero.

En este caso, se han estructurado como antecedentes los estudios de Jacintogr (2020), Zambrano et al. (2021) y Jumbo y García (2024). Ahora hay una secuencia lógica de los antecedentes que cubren tanto el contexto general de la seguridad informática como investigaciones previas específicas, proporcionando más profundidad al tema.

4.2.Marco Teórico

5. La seguridad informática

Entiéndase por ciberseguridad un conjunto de técnicas y métodos que se centran en proteger la información ante diferentes tipos de amenazas; ya sea por un acceso no autorizado a la información; por distribuciones de usuarios inadecuadas; por pérdida de registros de información, etc. Es así que podemos lograr que la información esté siempre disponible, íntegra y confiable (Corone & Quirumbay, 2022).

En el ámbito de la seguridad informática se definen tres pilares que constituyen la base para garantizar la protección de la información. Estos son:

- La confidencialidad, que delimita el acceso a un determinado tipo de información
- La integridad del mismo tipo de información, es decir, no es modificable
- La disponibilidad que siempre debe dictar la condición de estar disponible y accesible para las personas autorizadas para hacerlo.

Estos principios, que se fundamentan en los estándares internos, como ISO27001, son básicos para construir las correspondientes estrategias que se basan en la protección de la seguridad de los diferentes sistemas informáticos dentro de cualquier tipo de organización. (Guaña, 2023).

- **Disponibilidad:** la información tiene que estar siempre a disposición de los usuarios y accesible en todo momento. Esto conlleva a proteger redes y equipos

informáticos de amenazas, fallos, ataques informados o interrupciones inesperadas, implementar estrategias como copias de seguridad, redundancia, ataques de denegación de servicio (DDoS), etc. (Guaña, 2023).

- **Confidencialidad:** el principio está orientado a limitar el acceso a la información, garantizando que únicamente las personas o sistemas autorizados puedan llegar a conocerla y consultarla. La confidencialidad se establece empleando sistemas de protección referentes a la autenticación de usuarios en función de perfiles, el cifrado de datos y diferentes m é todos de acceso, que impidan la exposición de datos sensibles a amenazas potenciales (Guaña, 2023).
- **Integridad:** la integridad se refiere a la veracidad y exactitud de la información o la que esta almacena, es decir, que los datos no se pueden cambiar o modificar sin tener los permisos correspondientes. Para abordar la integridad se utilizan técnicas y métodos sobre todo el uso de firmas digitales, funciones hash y otras técnicas que determinan que ha habido un cambio o actualización no autorizadas de la información (Guaña, 2023).

La seguridad perimetral y el uso de firewalls, el sistema de prevención de intrusos (IP) y el sistema de detección de intrusos (ID) que han estado a la vanguardia de las organizaciones (Llanos, 2024). Sin embargo, las estrategias de defensa para buscar poder determinar su desarrollo. Sistemas como los Honeypots se han convertido en las armas más mosaicos para definir las amenazas avanzadas (Navarro, 2015).

6. Técnicas para la seguridad informática

En el campo de la seguridad informática, existen diversos sistemas diseñados para proteger la información, las redes y los recursos tecnológicos, los cuales cumplen funciones clave para garantizar la integridad, confidencialidad y disponibilidad de los

datos. Estos sistemas trabajan en conjunto para prevenir accesos no autorizados, detectar amenazas y asegurar la continuidad operativa de los servicios.

- **Detección de intrusos:** Se caracterizan por presentar estrategias y métodos tecnológicos orientados a analizar los patrones de comportamiento de los sistemas informáticos o a examinar sucesos de manera susceptible, basándose en información previamente entrenada, lo que les permite ser considerados como terminales de control (Gómez et al., 2023).
- **Análisis de vulnerabilidades:** la finalidad de estos sistemas es buscar vulnerabilidades previamente acreditadas, y pueden ser utilizados tanto por usuarios autorizados como por aquellos que intentan ingresar maliciosamente al sistema (Salazar & Campoverde, 2022).
- **Conexión de red:** caracterizan por analizar o examinar las conexiones que intentan infiltrarse en la red o en un equipo en particular. El método implementado lleva a cabo acciones en función de métricas y características tales como la configuración la y el grado de la conexión, los derechos de los usuarios, el acceso a servicios, etc. Estas acciones pueden incluir desde bloquear la conexión hasta generar alertas para el administrador de la red. Dentro de esta categoría se encuentran los cortafuegos o firewalls y los servicios de red conocidos como wrappers (IONOS, 2020).
- **Protección a la integridad de información:** existen sistemas que se caracterizan por mantener la información sin modificaciones negativas. Algunas aplicaciones utilizan algoritmos como Message Digest (MD5), mientras que otros sistemas emplean varios algoritmos en programas de cifrado como Good Privacy (PGP), Pretty Good Privacy, Tripwire y DozeCrypt, los cuales garantizan la integridad de los datos (TecnoBits, 2023).

7. Protección a la privacidad de la información:

Su funcionamiento se basa en técnicas criptográficas para resguardar y asegurar los datos con los permisos adecuados, asegurando que solo sean accesibles por usuarios autorizados. La criptografía se aplica principalmente en la comunicación entre dos identidades, y entre las herramientas utilizadas se incluyen Pretty Good Privacy (PGP) y los certificados digitales (TecnoBits, 2023).

8. Sistema de Detección de Intrusos (IDS)

Un sistema de detección de intrusos (IDS) es un conjunto de programas que se encargan de identificar intrusos o posibles ataques dentro de una red informática mediante el monitoreo del tráfico de la red y los dispositivos conectados (Gómez et al., 2023).

Existen dos categorías principales para configurar mecanismos de detección de intrusos:

- **Sistemas de Detección de Intrusiones en la Red (NIDS):** es un conjunto de estrategias que se encargan de identificar y examinar el tráfico la red a fin de garantizar la seguridad, estos sistemas buscan dentro de la red patrones sospechosos o actividades anómalas que pueden ser intrusos (Perdigón & Orellana, 2021).
- **Sistemas de Detección de Intrusiones en el Host (HIDS):** estos sistemas se caracterizan por brindar seguridad a los equipos específicos, analizan actividades específicas en los dispositivos o sistemas operativos, como cambios en archivos críticos, actividad de usuarios o procesos, para detectar posibles compromisos (Perdigón & Orellana, 2021).

9. Funcionamiento de un IDS

El funcionamiento fundamental de un IDS o Sistema de Detección de Intrusiones, en una primera fase, se dedica a identificar patrones de ataques comunes, para lo cual hace uso de firmas predeterminadas. Para una actividad de este tipo el IDS ejecuta las dos siguientes funcionalidades generales: 1) Inspección de paquetes que, según el modelo, se encarga de observar los paquetes que circulan por una trama de red para detectar la existencia de datos sospechosos o anómalos y, 2) Reconocimiento de patrones de ataques, que tiene la función de identificar los patrones concretos que pueden asociarse a amenazas predeterminadas en un entorno monitorizado (Guinea, 2021). Estas funcionalidades son complementadas con un motor avanzado, que está orientado a procesar y analizar patrones complejos de forma rápida y eficaz. Aunque un Honeypot persigue algunos de los mismos objetivos que un IDS, no podemos considerarlo como el mismo tipo de herramienta.

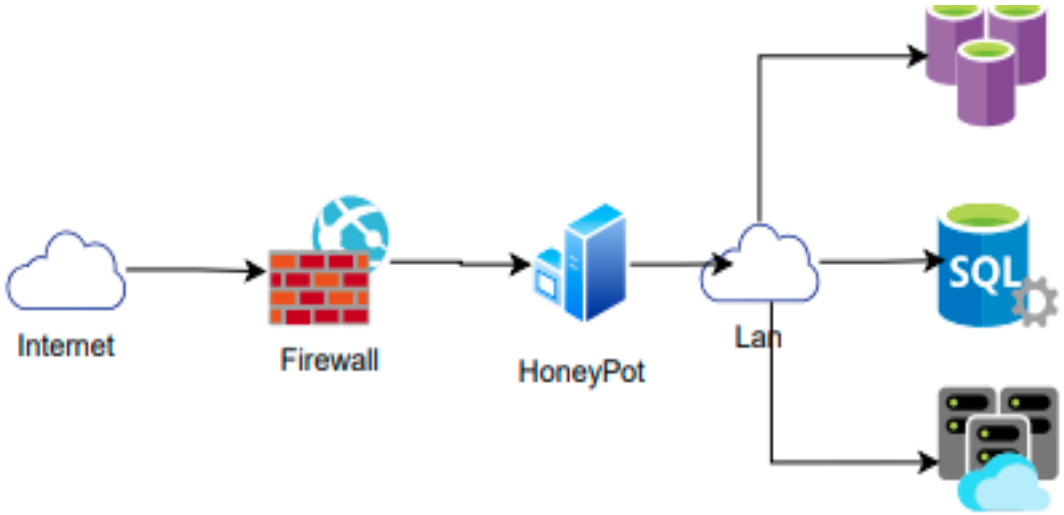
10. Sistema de seguridad basada en Honeypot

Se define como Honeypot a una solución de seguridad que intenta simular vulnerabilidades atractivas para aquellos atacantes que puedan haberlas detectado, con el objetivo de obtener toda la información posible sobre técnicas y comportamientos de ataque, sin poner en riesgo los sistemas que soportan la actividad productiva. El sistema Honeypot se emplea, por tanto, en la investigación en seguridad o en la defensa activa de redes informáticas en general (Vallejos, 2021).

En la Figura 1, se representa un diagrama Honeypot, donde se observar su funcionamiento dentro de una infraestructura de seguridad informática para la detección de intrusos y la respuesta inmediata a estos.

Figura 1

Diagrama Honeypot General



Fuente. Elaboración propia.

La Figura 2 describe los diferentes tipos de honeypot, clasificados en cuanto a su nivel de interacción:

- Honeypot de baja interacción: simulan sistemas y servicios limitados y ofrecen poca interacción con los atacantes. Son utilizados fundamentalmente en la detección de ataques automatizados.
- Honeypots de alta interacción: simulan un entorno completo, como un sistema operativo real, lo que permite a los atacantes interactuar con el sistema en mayor profundidad. Estos Honeypots permiten estudiar de manera detallada las técnicas empleadas por los intrusos (Cibersafety, 2024).

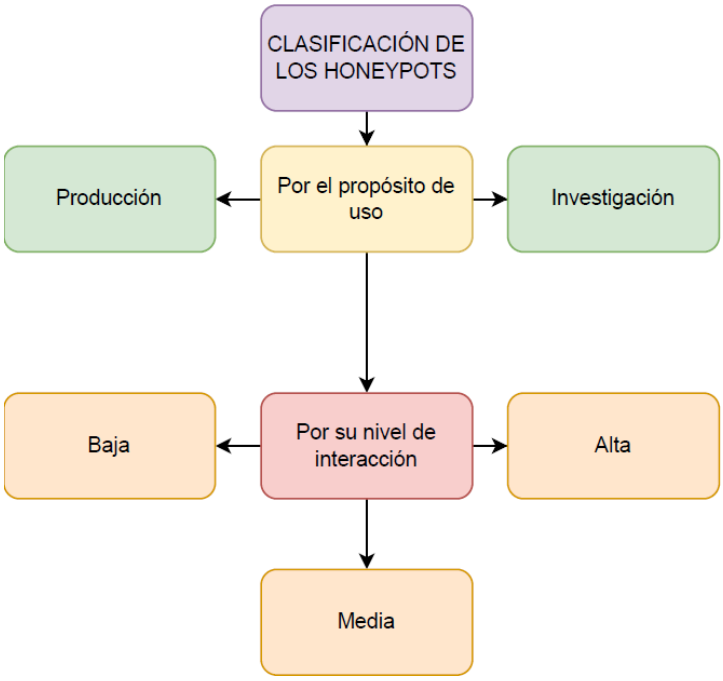
También pueden clasificarse atendiendo a su uso (Veselin, 2024):

- Honeypots de producción: se implementan en entornos reales para detectar y mitigar ataques reales en curso.

- Honeypots de investigación: se usan en entornos controlados para estudiar técnicas de ataque y descubrir nuevas vulnerabilidades.

Figura 2

Clasificación de los Honeypots



Fuente. Elaboración propia.

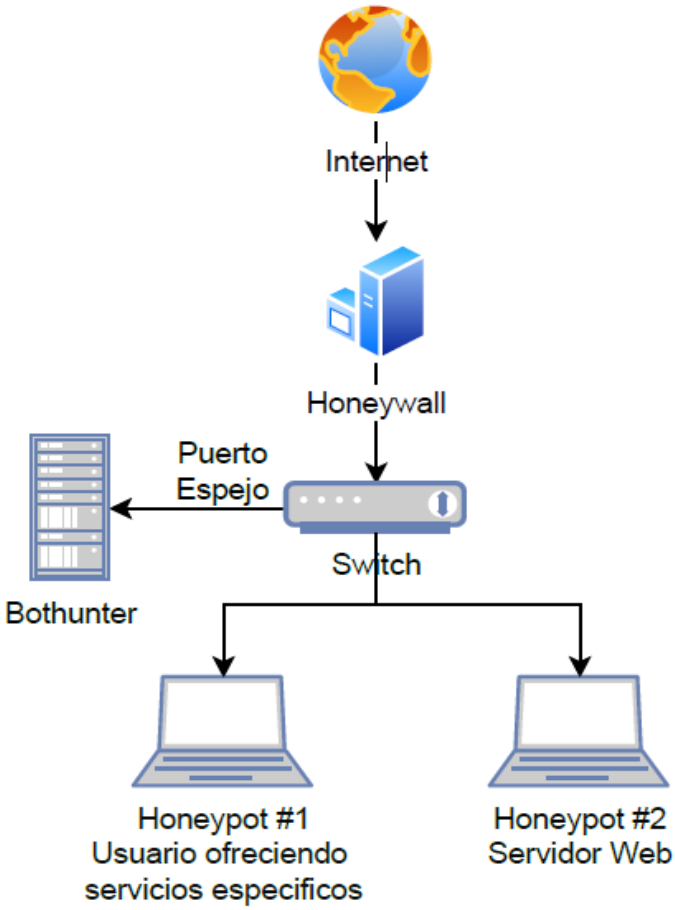
Cuando se conectan diversos Honeypot que se encuentran interconectados se forma el denominado Honeynet, es una red que se encuentra diseñada para atraer a los atacantes con la finalidad de que los atacantes interactúen con la red logrando recolectar la información sobre los métodos que usan para ingresar. La diferencia entre el Honeypot y el Honeynet, es que la una es una red individual mientras que el Honeynet es un conjunto de varios Honeypots, de manera que se simule una red compleja.

En la Figura 3, puede observarse una Honeynet que incluye varios elementos importantes como el Internet , que es la fuente de todos los posibles ataques que interactuará con la Honeynet ; el Honeywall , relacionado con el firewall que filtrará el tráfico entre la Honeynet y el Internet ; la red , que incluye un switch que permite conectar a los Honeypots y

el tráfico que se intercambiará entre estos ; un Bothunter, que es una herramienta de tráfico de detección de tráfico malicioso ; el Honeypot #1 , que simulará un usuario o incluso un sistema con servicios vulnerables y ofreciendo unos servicios o una serie de aplicaciones ; el Honeypot #2, que es el servidor web, que simula un servidor real, como puede ser una aplicación o un sitio web.

Figura 3

Redes Honeynet



Fuente. Elaboración propia.

11. Beneficios del Honeypot

La implementación de un Honeypot puede ofrecer diversos beneficios a las organizaciones, entre los cuales destacan:

- **Detección oportuna de amenazas:** los mecanismos adoptados por los Honeypots es que en sus primeras etapas pueden identificar las amenazas y ataques, lo que permite que no se vean comprometidos los sistemas reales. Debido que la funcionalidad de los honeypots es atraer a los atacantes cualquier alerta que se registre es posibilidad de intrusión. La detección oportuna o temprana de ataques es fundamental para contratacar y resguardar los sistemas frente a los incidentes de seguridad.
- **Disminución de falsos positivos:** los Honeypots tienen una particularidad en comparación con sistemas tradicionales de detección de intrusos (IDS) ya que disminuyen la cantidad de alertas falsas. Debido a que los Honeypots no manejan el tráfico legítimo entonces cualquier actividad en la red puede considerarse sospechosa, entonces el honeypot hace que lo identifique estos sucesos y facilite la identificación precisa de amenazas hacen que los equipos de seguridad realicen las notificaciones adecuadas (Pérez, 2024).
- **Examinar el comportamiento de atacantes:** los Honeypots utilizan algoritmos de análisis que permiten estudiar de manera detallada las tácticas, técnicas y procedimientos que utilizan los ciberdelincuentes. Este análisis ayuda a determinar de mejor manera las amenazas emergentes y seguidamente se diseñan estrategias de defensa contrarreste los ataques. La información obtenida puede ser empleada para entrenar sistemas de detección y de esta manera mejorar la seguridad de infraestructuras que son críticas (Pérez, 2024).
- **Obtención de amenazas internas:** en una red corporativa los Honeypots pueden ser utilizados para identificar accesos no autorizados, lo que resulta muy útil para detectar a usuarios no autorizados para ingresar a los sistemas y tienen la intención maliciosa de dañarlos, además puede detectar fallas en las configuraciones que podría ser perjudicial para la institución (Pérez, 2024).

- **Eficiencia en la respuesta ante incidentes:** la información recopilada de Honeypot se puede utilizar para mejorar los protocolos de reacción en los eventos que ahora están cambiando, actualmente varios métodos de ataque y causando muchos daños y, por lo tanto, las organizaciones pueden desarrollar medidas de reflexión más efectivas y fortalecer de manera proactiva sus sistemas de seguridad (Pérez, 2024).

12. Retos y limitaciones del Honeypot

La implementación de un honeypot es de beneficio para instituciones, pero también presenta ciertos desafíos y limitaciones:

- **Riesgo que la amenaza se apodere del honeypot:** el Honeypot debe configurarse correctamente con todas las características que benefician la función del sistema informático correcto, de lo contrario, existe el riesgo de cibernético confiscado y la utiliza como punto de soporte para viajar a la red de la organización, y Ciberni puede usar ataques mal configurados en sistemas internos (Scott, 2023).
- **Los ataques detecten a la honeypot:** las amenazas con experiencia pueden detectar la presencia de honeypot, es por ello que en la configuración del sistema no debe existir inconsistencias, también debe enfocarse a los tiempos de respuesta inusuales o características que no corresponden a un entorno real (Scott, 2023).
- **Mantenimiento y actualización:** Un Honeypot debe ser efectivo y contar con una supervisión constante. Para ello, es fundamental disponer de personal capacitado que analice la información obtenida. Además, el sistema debe actualizarse regularmente para evitar que se convierta en un punto vulnerable dentro de la red (Scott, 2023). Una gestión deficiente puede ser un factor clave para que el Honeypot sea comprometido y utilizado como un puente para atacar otros sistemas informáticos. Por ello, es crucial implementar controles adecuados y monitorear su funcionamiento de manera continua.

13. Herramientas de seguridad perimetral

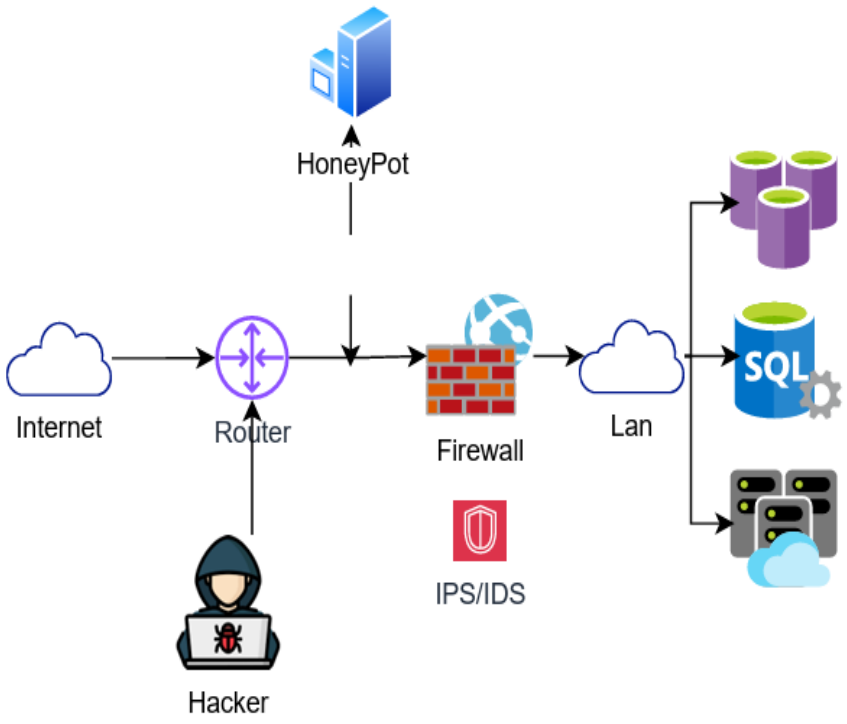
No existe un estándar para la implementación de Honeypot, la mayoría de las configuraciones se lo que se hace por buenas prácticas y como una herramienta de seguridad perimetral para completar las que se dispone actualmente como el firewall, antivirus, entre otros.

Los sistemas Honeypots o “sistemas trampa”, son equipos que pretenden estar desprotegidos, los cuales actúan como señuelos para monitorear, identificar y detectar posibles ataques (Spitzner L. , 2020).

La finalidad primordial de un Honeypot es llamar la atención de los ciberdelincuentes, posteriormente son desviados de la red LAN, además permite monitorear sus actividades y analizar los ataques que estos realicen, para mantener protegido los sistemas reales, como se describe en la Figura 4.

Figura 4

Implantación básica del Honeypot



Fuente. Elaboración propia.

Los Honeypots tienen algunas ventajas que se describen a continuación:

- Almacena gran cantidad de información valiosa al registrar solo actividad ilegitima.
- Establece una cantidad menor de alarmas falsas debido a que no utilizan tráfico legitimado.
- Desecha de firmas de posibles ataques a diferencia de los IDS.
- Identifica ataques nuevos lo que permite exponer las vulnerabilidades del sistema.
- Actúa a tiempo implementa medidas necesarias para posibles nuevos de ataques.

Por otro lado, los Honeypot tiene algunas desventajas las cuales se detallan a continuación:

- Los hackers pueden adueñarse de los Honeypots para actuar en contra de otros sistemas.
- Puede monitorear solamente interacciones realizadas de forma directa con el sistema trampa.
- Existe la posibilidad de ser detectado por los atacantes en caso de estar mal configurado.

Existen diferentes tipos de sistemas Honeypots, de acuerdo a los objetivos y a los niveles de interacción con los atacantes, es por ello que en la Tabla 1 se detalla los Honeypots de acuerdo a su interacción.

Tabla 1

Tipos de Honeypot según su interacción.

Baja	**Media**	**Alta**
Simulan una parte del sistema, recolectan información básica como escaneo de puertos. Bajo consumo de recursos, casi sin afectación al sistema.	Añade más interacción con el atacante, simulando un sistema más completo. Consumo moderado de CPU y memoria.	Simula un sistema real, permite más interacción con el atacante. Consumo de ciclos de CPU del 95% en 3 minutos debido a las operaciones intensivas.

Fuente. Elaboración propia.

En la Tabla 2 se describen los Honeypots de acuerdo a los objetivos, de esta manera poder identificar la configuración adecuada para implantar dentro de la cooperativa tomando en cuenta el tamaño y necesidades de la organización.

Tabla 2

Tipos de Honeypot según sus objetivos.

Tipo	Objetivo	Descripción
Producción	Proteger una red o reducir los daños durante un ataque.	Recolectar Información sobre los atacantes, conocer sus métodos de intrusión, herramientas utilizadas, etc.
Investigación	Estos Honeypots están diseñados para detectar y mitigar los ataques a sistemas reales, desorientando al atacante y evitando que afecten a la infraestructura crítica.	Este tipo de Honeypot se utiliza para entender las tácticas de los atacantes, lo que permite mejorar las defensas y estrategias de seguridad.

Fuente. Elaboración propia.

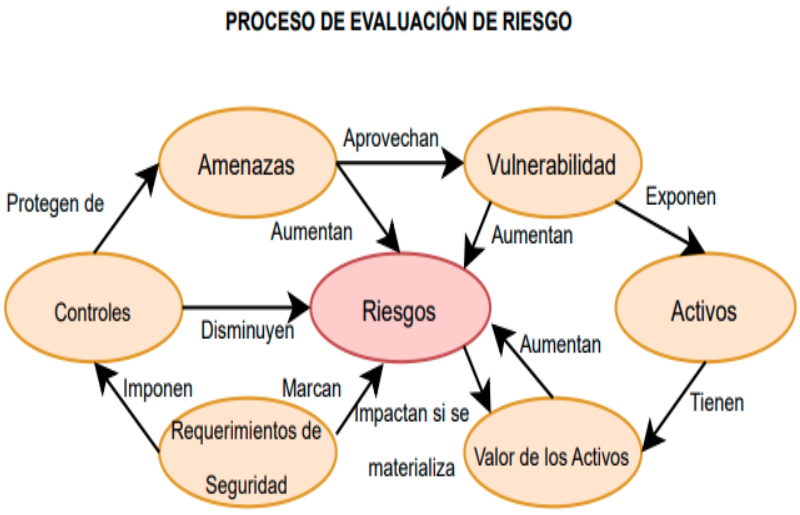
Debe mencionarse que la introducción de sistemas de trampa de alta interacción se considera una serie de honeypot y, por lo tanto, percibe toda la información del delito cibernético para monitorear y percibir toda la información sobre los intentos de atacar, mejorando así la seguridad en función de las amenazas y vulnerabilidades de la red (Rentería et al., 2021).

14. Honeypots de alta interacción

El uso de Honeypots varía en función del nivel de interacción, abarcando desde sistemas de baja interacción, utilizados principalmente en entornos de producción para tareas de protección, prevención, detección y respuesta ante ataques, hasta sistemas de alta interacción, que facilitan la recolección detallada de información sobre las actividades de los atacantes (Llanos, 2024). Los Honeypots de alta interacción permiten detectar tendencias, poner en marcha sistemas de alarmas tempranas, predecir los ataques e investigar de manera

exhaustiva, a lo que hay que añadir un aumento del riesgo potencial y una gran profundidad de conocimiento para su manejo. Las Honeynets son especialmente útiles para la investigación y el análisis de amenazas avanzadas, aunque su puesta en marcha presupone un incremento de riesgo y unas incertidumbres que há sido necesario valorar mediante el uso de evaluaciones de riesgo estructuradas (Llanos, 2024). Hablamos, como hemos dicho, de evaluaciones que sirven para identificar y analizar las vulnerabilidades de los sistemas de información o en las redes de datos, que permiten priorizar las medidas para mitigarlas y optimizar la ejecución de las estrategias de seguridad (Llanos, 2024). En este sentido, los Honeypots y las Honeynets se asientan como herramientas imprescindibles para la ciberseguridad, todo ello siempre que se tomen en serio y se planifiquen su implementación de forma adecuada (Rentería et al., 2021). En la Figura 5 se observa cómo los honeypots se integran de una manera planificada dentro de la evaluación de riesgos, permitiendo que el objetivo principal sea el de identificar la forma de comportarse de los atacantes conservando los activos reales de la organización. La implementación de este sistema ayuda a reforzar los controles, a disminuir vulnerabilidades existentes de tal manera de proporcionar una respuesta inmediatamente a las amenazas.

Figura 5
Proceso de evaluación de riesgo de Honeypot.



Fuente: Elaborado por el autor

15. Uso de Honeypots en cooperativas

En el contexto de instituciones financieras como las cooperativas, los Honeypots han demostrado ser herramientas valiosas para la detección y análisis de ataques dirigidos (Veselin, 2024). Al tratarse de organizaciones que manejan información altamente sensible, como datos financieros de sus socios, la implementación de medidas avanzadas de seguridad informática es crítica.

La información que se maneja en las instituciones financieras es muy crítica, sobre todo las transacciones en línea por parte de los usuarios, en la actualidad se cuenta con información de clientes que utilizan sus aplicaciones en línea para generará alguna transacción es por ello que siempre las instrucciones deben estar a la vanguardia e implementar sistemas de seguridad que respalde la integridad de los datos que e maneja. (Jumbo & García, 2024).

Debido a esto, el uso del honeypot en la cooperativa es una estrategia eficaz para mitigar amenazas internas y externas, como el acceso no autorizado a datos sensibles o los ataques de denegación de servicio (Dos). El uso de estas herramientas ha permitido identificar intentos de intrusión desde el exterior, y también riesgos asociados a dispositivos internos comprometidos (Zambrano et al., 2021).

15.1. Marco legal

La implementación de un honeypot en la Cooperativa de Ahorro y Crédito “23 de Julio” para la detección y prevención de incidentes de seguridad, debe estar sustentada por las normativas legales que rigen la seguridad de la información y la protección de datos personales, en Ecuador. Este marco legal es decisivo a la hora de garantizar que las medidas adoptadas para proteger la información y los sistemas, no comprometan el ejercicio de los derechos fundamentales como son la privacidad, ni violen las regulaciones nacionales e internacionales.

16. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (LCE) como la norma fundamental en dicha materia del Ecuador, se encuentra vigente desde el 2002, y regulando así los aspectos del manejo de la información presentada en soporte electrónico y garantizando, la validez de las transacciones realizadas a través de medios electrónicos. En donde existen varios puntos que afectan la ejecución de las medidas de seguridad para las redes de datos de las organizaciones (Congreso Nacional, 2002).

- Autenticación de la información: la Ley de Comercio Electrónico establece que la autenticación es un proceso fundamental para identificar a los usuarios de sistemas electrónicos que tienen acceso a la información y los datos de estas organizaciones, lo que se relaciona con la función de los Honeypots para llevar el control de las conexiones no autorizadas e identificar los intrusos.
- Confidencialidad y seguridad de la información de datos electrónicos: las organizaciones tienen el deber de proteger la información y los mensajes de datos de alteraciones, accesos no autorizados o interceptaciones, que hace necesaria la implementación de estos Honeypots que ayudan a salvaguardar estas líneas de actuación.

17. Ley Orgánica de Protección de Datos Personales (LOPDP)

La Ley Orgánica de Protección de Datos Personales (LOPDP), que se aprobó en Ecuador en 2021, establece el marco normativo que regula el tratamiento de los datos de carácter personal. Su objetivo es preservar los derechos fundamentales de la privacidad y la adecuada gestión de la información sensible. En el caso de la aplicación de un Honeypot, comenzando por la interacción con los posibles datos personales en el ámbito de una red

corporativa, este debe ajustarse a los principios que la ley determina (Asamblea Nacional de Ecuador, 2021).

- Principio de legalidad y transparencia: toda actividad referida a la recolección, almacenamiento y tratamiento de los datos personales debe ser legítima, informada y transparente para los titulares de la información (Asamblea Nacional de Ecuador, 2021).
- Principio de proporcionalidad y minimización de datos: Las medidas de seguridad que se establecen, como por ejemplo el Honeypot, deben ser proporcionales al riesgo que buscan contrarrestar y asegurarse de que no se vulnere la privacidad de las personas a las que se refiere en mayor medida de la estrictamente necesaria (Asamblea Nacional de Ecuador, 2021).
- Derechos de los titulares de datos: El derecho a la protección de la privacidad de los titulares de los datos es infranqueable; por ello, el uso de los Honeypots debe asegurar que no se recogen y almacenan datos personales innecesarios, haciendo todo esto con el debido consentimiento.

18. Normas Internacionales de Seguridad de la Información

A nivel internacional, la norma International Organization for Standardization ISO/IEC 27001 (2013) es uno de los estándares más reconocidos para la gestión de la seguridad de la información. Esta norma establece un marco de buenas prácticas y controles que deben adoptarse para proteger los activos de información, entre los cuales destacan:

- **Evaluación de riesgos:** la norma establece la necesidad de realizar un análisis de riesgos continuo para identificar y mitigar amenazas. El Honeypot, como herramienta de detección, se alinea perfectamente con este requisito al actuar como una medida

preventiva y de control para detectar posibles brechas de seguridad (International Organization for Standardization ISO/IEC 27001, 2013).

- **Protección contra ciberataques:** dentro de los controles establecidos por la norma ISO, 2023, se incluyen estrategias para la defensa activa de redes frente a ataques cibernéticos, lo que respalda el uso de Honeypots como una solución adecuada y certificada para proteger los sistemas de información de las organizaciones (International Organization for Standardization ISO/IEC 27001, 2013).

En la Figura 6 se representa una política de seguridad basada en el estándar ISO/IEC 27001, la cual se caracteriza por establecer políticas, procedimientos y directrices para proteger los activos de información, de igual manera estable el nivel de riesgos que existe y las medidas de seguridad aplicar en caso de que existan incidentes con la información (Logo ESG Innova Group, 2023).

Figura 6

Normas ISO 27001, estructura de un Sistema de Gestión de Seguridad de la Información (SGSI).

Fuente: (International Organization for Standardization, 2023).

19. Ley de Instituciones del Sistema Financiero

La Ley General de Instituciones del Sistema Financiero también es relevante para la Cooperativa de Ahorro y Crédito 23 de Julio, dado que regula las obligaciones de las instituciones financieras en términos de seguridad y protección de los datos de sus clientes y socios. Esta ley establece la responsabilidad de las instituciones financieras de garantizar la integridad y confidencialidad de los datos financieros, bajo sanciones severas en caso de incumplimiento (Asamblea Nacional del Ecuador, 2014).

Algunas cuestiones importantes relacionadas con la implementación de medidas de seguridad incluyen:

- **Responsabilidad fiduciaria:** las cooperativas financieras tienen la obligación de tomar las medidas necesarias para proteger los datos financieros y personales de sus socios, y esto además incluye la implementación de tecnologías avanzadas como los honeypot.

- **Seguridad operativa y cibernética:** la ley establece que las instituciones financieras deben incorporar sistemas que aseguren el correcto funcionamiento de las operaciones y protejan contra amenazas cibernéticas. Los honeypot permiten monitorear, detectar y mitigar estos ataques antes de que afecten los sistemas productivos reales de la cooperativa.

20. Normativas de la Superintendencia de Economía Popular y Solidaria (SEPS)

La Superintendencia de Economía Popular y Solidaria (SEPS) es el ente controlador y regulador de las cooperativas y demás entidades del sector financiero popular y solidario de Ecuador. En ese sentido, la SEPS emite una normativa que tiene como objetivo, entre otras cosas, incrementar la seguridad de la información, la gestión de los riesgos tecnológicos y la protección de datos en las entidades sobre las cuales ejerce control, como es el caso de la

Cooperativa de Ahorro y Crédito 23 de Julio (Superintendencia de Economía Popular y Solidaria, 2019).

Las normas emanadas de la SEPS prescriben que las cooperativas deben implementar mecanismos de seguridad apropiados para asegurar la infraestructura tecnológica y los datos de carácter personal sensibles para los socios y clientes, de tal manera que entre los puntos que provocan la implementación de un Honeypot como sistema de detección y prevención de los ciberataques están los siguientes:

a) Resolución sobre la Gestión de Riesgos Tecnológicos

La SEPS, en sus directrices para la gestión de riesgos tecnológicos, exige a las cooperativas adoptar políticas y procedimientos que aseguren la continuidad del negocio y la protección de los sistemas de información, esto incluye:

- La entidad debe contar con un sistema de identificación de vulnerabilidades y amenazas, incluyendo la detección de posibles accesos no autorizados, que podrían comprometer la integridad de la red. La implementación de un Honeypot se alinea con estas directrices al actuar como un sistema de alerta temprana ante posibles ciberataques.

- Los lineamientos de la SEPS exigen que se implementen controles de seguridad para proteger las redes internas y los sistemas operativos de las cooperativas. Un Honeypot es una herramienta eficaz en la detección de ataques dirigidos a vulnerar dicha infraestructura.

b) Control Interno y Seguridad de la Información

La normativa de la SEPS enfatiza la importancia de contar con un sistema de control interno robusto que garantice la confidencialidad, integridad y disponibilidad de la información. En este sentido, se menciona que las cooperativas deben implementar diversos

controles tecnológicos debido a que permiten identificar, prevenir e inclusive mitigar las amenazas cibernéticas que afectan a la operación.

Las cooperativas se encuentran obligadas a definir y manejar un plan de seguridad las cuales deben mantener diversas medidas técnicas logrando proteger a los sistemas y datos de los socios. Un Honeypot puede ser implementado como una solución para detectar las intrusiones y analizar los ataques, de esta manera se establecerá una mejora continua en la seguridad interna.

La SEPS también establecen que las entidades deben aplicar mecanismos de monitoreo sobre los accesos y actividades en sus sistemas. Un honeypot ayuda a cumplir con esta normativa, pues permite capturar datos sobre intentos de intrusión y comportamientos sospechosos en la red (Superintendencia de Economía Popular y Solidaria, 2019).

c) Gestión de Incidentes de Seguridad

Una parte fundamental de las normativas de la SEPS está relacionada con la gestión de incidentes de seguridad de la información. Esta normativa exige que las cooperativas busquen implementar diversos procedimientos para detectar, notificar y dar respuesta ante los incidentes de seguridad los cuales comprometen a los activos de la información.

La implantación de un Honeypot, tiene como finalidad detectar los ataques de manera temprana, logrando brindar una respuesta eficaz y rápida ante una amenaza. Es primordial ya que reduce el impacto ante un ataque antes de que el mismo afecte a los sistemas de la cooperativa.

La SEPS indican que se debe llevar un registro detallado de los incidentes de seguridad, con el propósito de analizar patrones y tomar acciones correctivas. Los honeypot brindan información de interés sobre los ataques, permitiendo a la entidad tomar medidas proactivas para reforzar la seguridad.

d) Auditoría y Cumplimiento Regulatorio

La SEPS también regula la auditoría interna y externa de las cooperativas, con especial énfasis en la evaluación de los sistemas de seguridad y el cumplimiento de las normativas de protección de datos. Las auditorías deben verificar que las cooperativas cuentan con las herramientas necesarias para la detección y prevención de riesgos tecnológicos.

Un honeypot proporciona evidencia sobre la eficacia de las políticas de seguridad implementadas en la cooperativa. Además, los registros generados por esta herramienta pueden ser utilizados en auditorías para demostrar el cumplimiento de las normativas de la SEPS y las mejores prácticas de seguridad.

La cooperativa debe generar informes periódicos sobre la gestión de riesgos tecnológicos, detallando los incidentes y las medidas adoptadas para mitigar las amenazas. La información recopilada a través del honeypot puede ser clave en la preparación de estos informes, ofreciendo un análisis profundo de los intentos de ataque y las respuestas implementadas.

CAPÍTULO III

MARCO METODOLÓGICO

21.1. Descripción del grupo de estudio

1. Población y muestra

La población estuvo compuesta por: funcionarios del equipo técnico de la Cooperativa y los funcionarios del Departamento de Tecnología de la Cooperativa; la infraestructura de redes de la Cooperativa, que incluye el hardware, software y todos los elementos activos de conectividad; la infraestructura de aplicaciones y servicios de la Cooperativa, que incluye todos los sistemas y softwares que garantizan el funcionamiento de la Cooperativa. La muestra estuvo compuesta por subconjuntos de la población, como se detalla en la **Tabla 3**.

Tabla 3

Muestra de la población

Subconjuntos	**Cantidad**
Funcionarios del Departamento de Seguridad de la Información	4
Funcionarios del Departamento de Tecnología	7
Enrutador	4
Conmutador de datos	4
Módem/enrutador ADSL	2
LAN Virtual	2
Firewall	1
Servidor de nombres de dominio (DNS)	1
Servidor de Base de Datos	2
Servidor de clientes ligeros	2
Servidor web	3

Subconjuntos	Cantidad
Servidor de correo	1
Servidor de transferencia de archivos (FTP)	2
Aplicaciones que utiliza la Cooperativa en su trabajo cotidiano	5
Total	**36**

Fuente. Elaboración propia.

21.2. Modalidad de la investigación

Tipo de investigación: Aplicada – experimental – estudio de casos.

Técnicas: implementación de honeypots – simulación de ataques mediante Ethical hacking.

La cooperativa por normativa genera anualmente pruebas de ethical hacking a toda la infraestructura esto incluye los siguientes puntos:

Análisis de vulnerabilidades y pruebas de penetración en modalidad de caja gris, donde se combinan conocimientos internos y externos del sistema para simular ataques reales. Esta metodología permite identificar posibles puntos débiles, entender qué tan comprometida podría estar la seguridad y evaluar el impacto que tendría un ataque en la organización, todo esto con el objetivo de proteger mejor la información y fortalecer los sistemas antes de que ocurra una amenaza real.

Evaluación del compromiso potencial de activos por parte de un atacante remoto, las pruebas se enfocan en determinar si un atacante, con acceso remoto y permisos limitados, podría comprometer activos críticos, esto permitiría identificar riesgos reales que amenacen la seguridad de la cooperativa y tomar medidas preventivas antes de que ocurra un incidente.

Determinación del impacto potencial ante la explotación de vulnerabilidades, en esta etapa se analiza qué tan grave podría ser el daño si un atacante malicioso llegara a aprovechar una debilidad del sistema. Se considera, por ejemplo, la posibilidad de que acceda sin

autorización a información sensible, lo que podría afectar directamente a la organización, sus operaciones y la confianza de sus usuarios.

La primera vez que se gestionó este proceso, en 2024, la empresa Acsys detectó la presencia del honeypot y como resultado, solicitaron su desactivación temporal mientras llevaban a cabo sus actividades de *ethical hacking*, con el fin de no interferir con su trabajo.

Instrumentos: instrucciones automatizadas de ataque, metasploit, nmpa, hydra o lo que utilizó para atacar.

Métricas a considerar: número de ataques detectados, tiempos de detección, tasa de falsos positivos/negativos, tipologías de ataques (DDos, fuerza bruta, escaneo).

21.3. Análisis y diagnóstico de la infraestructura de red

La primera etapa consistió en realizar un análisis de la infraestructura tecnológica de la Cooperativa, enfocándose en las redes de datos y sistemas críticos. Se realizaron auditorías de seguridad, revisando las herramientas de detección de intrusos utilizadas y las políticas existentes para identificar posibles vulnerabilidades. Durante esta fase, se recopilaron datos, como registros de seguridad y patrones de comportamiento en la red, para comprender el estado actual de la ciberseguridad en la cooperativa

22. Herramientas de Detección de Intrusos en la Cooperativa 23 De Julio

Dentro de las cooperativas de ahorro y crédito se alojan cantidades excesivamente grandes de datos que son vulnerables y que posiblemente se encuentran expuestas a algún riesgo o amenaza cibernética. Estas instituciones para proteger todos estos datos y garantizar su buen funcionamiento se utilizan (IDS) sofisticados, los cuales permiten observar y analizar toda la red para detectar ciertas actividades sospechosas o maliciosas e intrusos sobre todo en las transacciones en línea (Jumbo & García, 2024).

Los sistemas de detección de intrusos dentro de las instituciones financieras desempeñan un papel importante en la seguridad, ya que permiten de manera eficiente detectar y mitigar los ataques maliciosos antes de que comprometan información crítica sobre todo cuando se realizan transacciones en línea, la configuración de HIDS, NIDS y herramientas de análisis avanzado ayudaran a crear una protección sólida contra amenazas emergentes en el sector financiero (Jumbo & García, 2024).

Las cooperativas de ahorro y crédito operan con datos sensibles que están relacionados con sus operaciones, clientes y estrategias de mercadeo. Para proteger esta información es primordial establecer estrategias de seguridad basado en las distintas herramientas y de esta manera garantizar la confianza de los clientes enfocado al cumplimiento de regulaciones de seguridad (Díaz, 2024).

La mayoría de las instituciones financieras utilizan estos sistemas de detección de intrusos con la finalidad de:

- Determinar intentos de fraude o accesos no autorizados.
- Resguardar los datos sensibles de clientes y las transacciones.
- Dar cumplimiento a los estándares de seguridad como PCI, DSS e ISO 27001.
- Disminuir el impacto y consecuencias de los ataques cibernéticos, mediante la ejecución de forma automática de un sistema de seguridad.

La Cooperativa 23 de Julio, ha implementado sistemas de seguridad que permiten supervisar el correcto funcionamiento de la red informática, mediante las cuales es posible examinar las transacciones fraudulentas y patrones inusuales que están queriendo acceder a las redes informáticas dentro de la institución (Cooperativa 23 de Julio, 2023).

La Cooperativa actualmente no cuenta con un sistema robusto de detención de intrusos en las redes informáticas, sin embargo, cuenta con algunas herramientas tecnológicas que trabajan por separado para proteger las redes y los equipos informáticos, estas herramientas son:

- Security Operation Center (SOC)
- Equipo de respuesta a incidentes de seguridad de la Información (CSIRT)
- Network Operation Center (NOC)
- Monitoreo de redes mediante Tenable Nessus
- Monitoreo de redes sociales y control Anti phishing (Protección de Marca)
- Monitoreo de correos no deseados (AntiSpam)
- Antivirus (Trellix, Endpoint, Servers y ATM monitoreados) (Cooperativa 23 de Julio, 2023).

23. Security Operation Center (SOC)

El Centro Operaciones de Seguridad (*Security Operations Center* - SOC) es una solución clave para mejorar la detección, respuesta y prevención de amenazas cibernéticas mediante la integración y coordinación de herramientas de seguridad (IBM, 2024).

La Cooperativa 23 de Julio, uno de los principales problemas es la vulnerabilidad en las transacciones financieras, lo que puede dar lugar a fraudes, accesos no autorizados, etcétera. Para mitigar este riesgo, se han implementado sistemas de monitoreo en tiempo real, con los cuales se logran identificar patrones sospechosos y generar alertas de seguridad. Un segundo hallazgo consiste en la protección de la red perimetral, ya que los ataques externos pueden afectar la infraestructura. Para ello, se ha introducido un Sistema de Detección y Prevención de Intrusos (IDS/IPS), que identifica y bloquea accesos no autorizados.

El SOC, respaldado por estándares internacionales, permite centralizar y fortalecer la seguridad digital de la cooperativa, garantizando una respuesta eficiente ante amenazas cibernéticas (Cooperativa 23 de Julio, 2023).

24. Equipo de respuesta a incidentes de seguridad de la Información (CSIRT)

Este equipo da respuesta a las incidencias de la seguridad informática, el cual está formado por personal técnico especializado que analiza las situaciones y da respuesta inmediata a las amenazas dentro del sistema informático. Un CSIRT por sus siglas en inglés Computer Security Incident Response Team puede estar configurado como un ad hoc, cuya finalidad es la implantación de medidas de prevención y reacción inmediata ante incidentes (Sullivan, 2024).

Dentro de la Cooperativa 23 de Julio, esta implementado diversas medidas de seguridad, dentro de las cuales se especifica la concienciación y educación sobre ciberseguridad. Mediante estas medidas se ha logrado identificar advertencias sobre ataques de phishing en las redes sociales, y se ha procedido a dictar procedimientos o consejos para que los usuarios mantengan siempre protegida la información personal (Cooperativa 23 de Julio, 2023).

25. Network Operation Center (NOC)

Un centro de operaciones de red por sus siglas en inglés *Network Operation Center* (NOC) es un lugar que está centralizado para supervisar y gestionar por 24 horas y 7 días a la semana el funcionamiento de los sistemas informáticos redes informáticas, es el encargado de proporcionar la primera alerta ante las interrupciones y daños en la red (IMB, 2024).

Dentro de la cooperativa, los servicios NOC operan de manera eficiente y segura, lo que implica que podría tener algún tipo de estructura para monitorear y mantener su infraestructura tecnológica, ay que cuenta la gestión de múltiples agencias y cajeros automáticos, requiere un

monitoreo de 24/7 para garantizar siempre su disponibilidad ya que se administra múltiples agencias y cajeros automáticos en todo el país, lo cual requiere un monitoreo constante de los sistemas para garantizar su disponibilidad, estos centros ayudan también a identificar los problemas de rendimiento o daños en los servicios de red de la institución (Cooperativa 23 de Julio, 2023).

26. Monitoreo de redes mediante Tenable Nessus

Dentro de la Cooperativa se utiliza Nessus, que es una herramienta que permite detectar vulnerabilidades en los diferentes servidores de red y equipos informáticos conectados a través de escaneos continuo y automatizados, y tiene las siguientes características: 1) detecta todos los equipos y dispositivos conectados a la red identificando posibles accesos no autorizados, 2) escanea vulnerabilidades identificando fallos en las configuraciones de hardware y software, 3) analiza las posibles amenazas clasificando los riesgos según el nivel crítico y actúa mitigando las amenazas graves, 4) Genera informes, proporcionando reportes detallados de las vulnerabilidades encontradas y las recomendaciones para corregirlas institución (Cooperativa 23 de Julio, 2023).

27. Monitoreo de redes sociales y control Anti phishing (Protección de Marca)

La Cooperativa de Ahorro y Crédito 23 de Julio tiene implementada algunas estrategias para monitorear sus redes sociales y combatir el phishing, con el objetivo de proteger la información y la información de sus socios. El monitoreo se lo realiza mediante las plataformas YouTube, Facebook e Instagram para lo cual comparte información importante de sus servicios, promociones y de la misma manera consejos permanentes sobre la seguridad financiera esto ha permitido: 1) identificar y responder inmediatamente a comentarios, consultas o preguntas de sus socios, 2) detectar y eliminar amenazas de publicaciones que

pueden producir fraude a los clientes, 3) concientizar a los socios mediante buenas prácticas de seguridad para no caer en estafas. A continuación, se muestra la figura 7.

Figura 7

Información sobre ataques Phishing

Fuente. Departamento de Seguridad de la Información.

Además, para el control Anti-Phishing, la Cooperativa ha desarrollado las siguientes medidas de prevención: 1) capacitación en concienciación, para lo cual publican información para que no caigan en estafas y que utilicen siempre la información oficial y se sigan los procedimientos establecidos por la cooperativa, 2) educación en seguridad de información, que ofrecen recomendaciones sobre buenas prácticas sobre el uso de la información personal, 3) implantación de políticas de seguridad que estable responsabilidades y procedimientos adecuados para el tratamiento y acceso a la información, creando una cultura de concienciación entre la cooperativa y sus socios (Cooperativa de Ahorro y Crédito 23 de Julio, 2024).

Todas estas estrategias muestran el compromiso de la Cooperativa 23 de Julio con los socios y la seguridad de sus datos, utilizando de manera eficiente las redes sociales como herramientas para poder informar y proteger la información contra amenazas cibernéticas.

28. Antivirus (Trellix, Endpoint, Servers y ATM monitoreados)

Dentro de la Cooperativa de Ahorro y Crédito 23 de Julio se ha instalado soluciones de seguridad de Trellix, la cual consiste en conjunto de estrategias para evitar el robo de información Trellix Data Loss Prevention (DLP) y antivirus, de tal manera de proporcionar protección activa contra malware, ransomware y ataques avanzados al sistema informático y de tener a salvo la información de sus clientes. Trellix a más de ofrecer seguridad ofrece respuesta inmediata para la detección y respuesta a las amenazas ya que cuenta con un sistema de inteligencia artificial, de esta manera la Cooperativa busca prevenir la perdida de datos, la confidencialidad de la información y asegurar que los datos estén siempre disponibles para las personas autorizadas.

29. Políticas de seguridad

Las instituciones financieras almacenan gran cantidad de información confidencial y sensible, lo que se constituye en un blanco fácil para los ciberatacantes. Es por ello que cada institución implementa políticas de seguridad eficaces enmarcadas en las normativas internaciones y utilizan herramientas especializadas para monitorear los sistemas de red para identificar riesgos de riesgos y vulnerabilidades que atenten en contra de la información confidencial de los clientes (Jumbo & García, 2024).

Las instituciones se enmarcan es estándares internacionales y nacionales para la protección de la información dentro de los sistemas informáticos:

- **ISO/IEC 27001**: Este estándar internacional, abarca los requisitos para la gestión de seguridad de la información dentro de una institución, la cual incluye la identificación de riesgos y la adopción de medidas de seguridad (ISO, 2013).
- **NIST SP 800-53**: Este es un estándar que determina todos los controles de seguridad permite identificar y ablandar las vulnerabilidades en las instituciones financieras (National Institute of Standards and Technology, 2020).
- **PCI DSS:** Consiste en un **e**stándar que es primordial para instituciones que procesan pagos electrónicos, para lo cual se basa en la detección y prevención de vulnerabilidades en redes informáticas y aplicaciones tecnológicas (Arundhati, 2024).

La Cooperativa 29 de Julio debe resguardar sus activos más valiosos: su ingente caudal de datos y su infraestructura digital, garantizándolos en términos de integridad, confidencialidad y disponibilidad. Para ello, la cooperativa hace uso de sólidas políticas de seguridad orientadas con estándares internacionales y emplea herramientas específicas para detectar mitigarlas las vulnerabilidades. En este sentido, la Cooperativa 29 de Julio, periódicamente hace auditorías, audita la seguridad, manipula las actualizaciones de seguridad y analiza el comportamiento de sus sistemas, garantizando de esta forma la seguridad de los activos informáticos frente a las amenazas cibernéticas que puedan comprometer su infraestructura tecnológica y financiera.

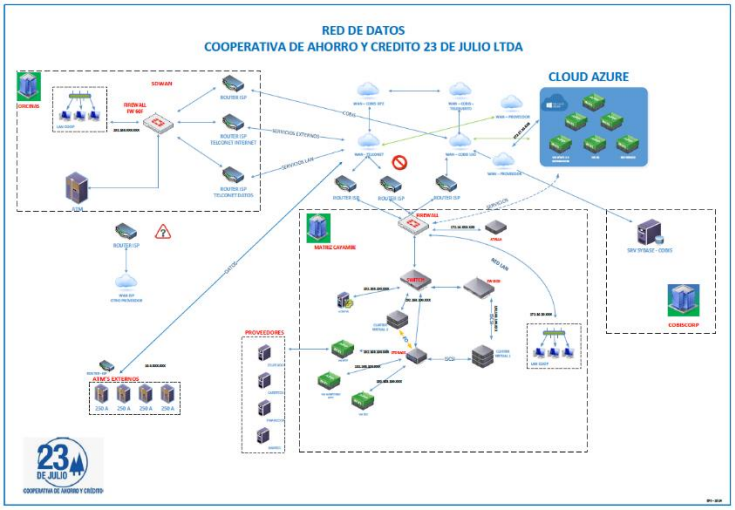
30. Área de estudio e infraestructura de la Red.

El área de investigación seleccionada para el trabajo ha sido la Cooperativa de Ahorro y Crédito 23 de Julio, una entidad financiera en el Ecuador que cuenta con una red interna de sucursales que se encuentran interconectadas a través de sistemas informáticos importantes. La infraestructura tecnológica de la cooperativa abarca servidores físicos y en la nube Azure,

almacenamiento de datos, estaciones de trabajo y dispositivos de red, que permiten el acceso remoto y conexiones externas como se expone en la Figura 8.

Figura 8

Infraestructura Cooperativa 23 de Julio Ltda.



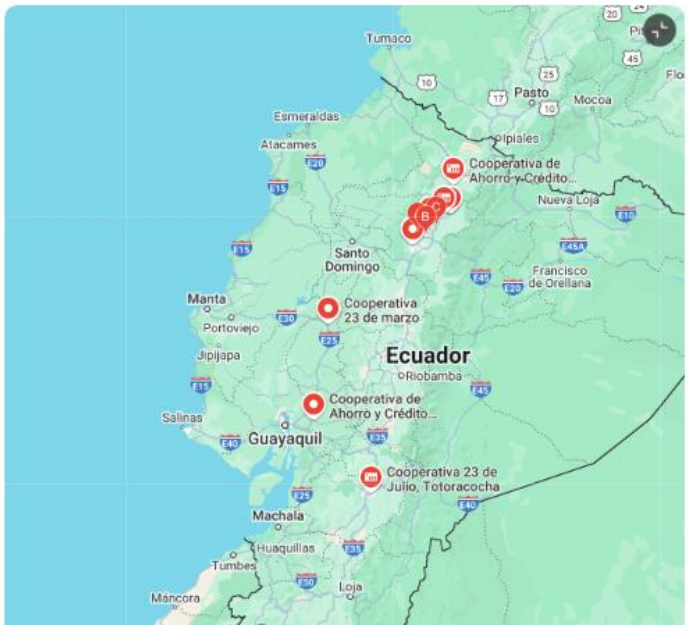
Fuente. Departamento de Tecnología de la Información de Cooperativa 23 de Julio, 2024.

La Figura 9 describe la ubicación física de la Cooperativa 23 de Julio a nivel nacional, cuya matriz se encuentra en Cayambe, Pichincha, Ecuador y cuenta con algunas sucursales en todo el país.

El estudio se centra en la seguridad de la red interna de la cooperativa, donde se identificaron vulnerabilidades, como la falta de mecanismos de detección de intrusos y el riesgo de accesos no autorizados desde dispositivos comprometidos. La implementación de un honeypot en la infraestructura de la cooperativa, persigue el objetivo de detectar y prevenir ciberataques, proporcionando un entorno controlado para analizar las técnicas, estrategias, métodos y herramientas utilizadas por los atacantes y fortalecer la seguridad de la cooperativa.

Figura 9

Ubicación Cooperativa 23 de Julio.



Fuente. Google Maps, 2024.

30.1. Análisis el estado de la seguridad en la red interna

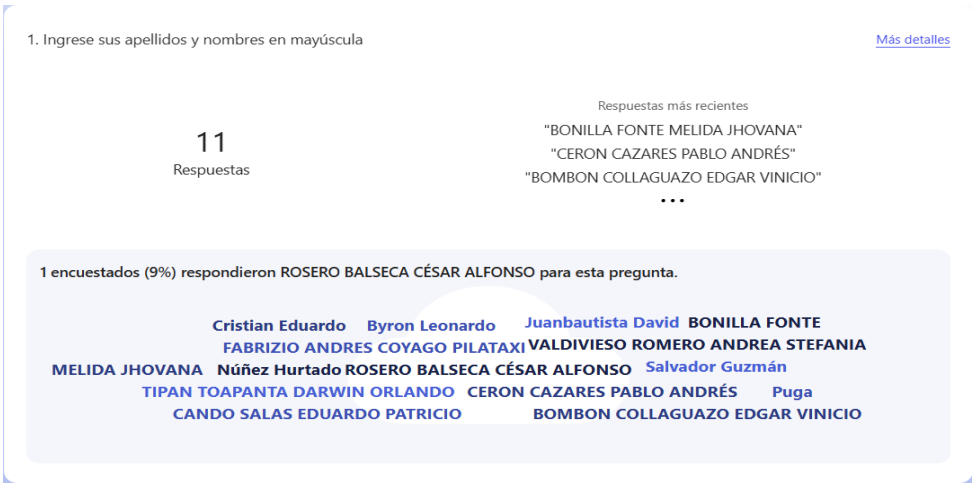
31. Análisis de las técnicas de recolección de datos.

Se llevaron a cabo, encuestas a las once personas que son responsables del área de ciberseguridad, así como al personal técnico de la Cooperativa. Los datos cualitativos que se obtuvieron de las encuestas al personal de la Cooperativa, los registros de actividad y los reportes de las vulnerabilidades de la infraestructura informática, que se habían detectado antes de la implantación del Honeypot, fueron clasificados y organizados en vistas de los patrones y las áreas críticas de la infraestructura de la seguridad informática. Seguido de esto, se dio paso al tratamiento de los datos cuantitativos, como el número de intentos de acceso no autorizado, la frecuencia de los ataques detectados y el tiempo de respuesta a incidentes. Cabe destacar que esta información descansa en un informe de carácter confidencial aportado por un proveedor

que estuvo a cargo del Ethical Hacking en la Cooperativa 23 de Julio, tal y como puede apreciarse en la Figura 10.

Figura 10

Cuestionario para el Departamento de Tecnología y Seguridad de la Información de la Cooperativa 23 de Julio.



2. **¿Cuál es su cargo dentro del área de tecnología o seguridad de la información?** Más detalles

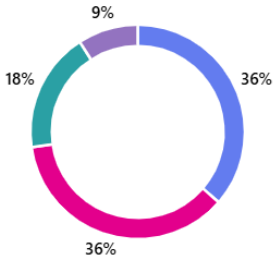
11
Respuestas

Respuestas más recientes
"Analista de Desarrollo de Software"
"Analista de soporte"
"AUXILIAR ADMINISTRATIVO"
...

7 encuestados (64%) respondieron Analista de para esta pregunta.

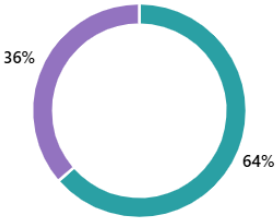
3. **¿Cuánto tiempo ha trabajando en la rama de tecnología en la cooperativa?** Más detalles

Menos de 1 año	4
1-3 años	4
3-5 años	2
Más de 5 años	1



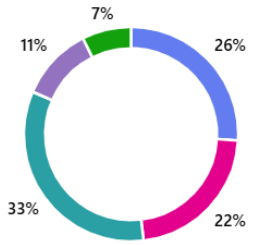
4. **¿Qué tan frecuentemente ha observado incidentes de seguridad (accesos no autorizados, ataques DDoS, etc.) en la red de la cooperativa?** Más detalles

Frecuentemente	0
Ocasionalmente	0
Raramente	7
Nunca	4



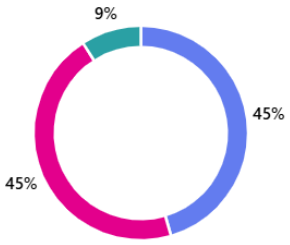
5. **En su opinión, ¿cuáles son las principales vulnerabilidades de la red interna de la cooperativa? (Puede seleccionar más de una opción)** Más detalles

Puertos abiertos no controlados	7
Contraseñas débiles	6
Software desactualizado	9
Falta de monitoreo constante	3
Otras	2



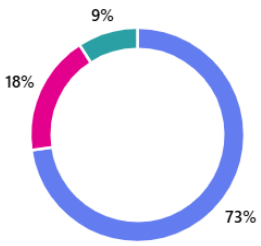
6. **¿Cree que el equipo actual de seguridad está preparado para enfrentar ciberataques avanzados?** Más detalles

Sí, totalmente preparado	5
Parcialmente preparado	5
No lo suficiente	1
No está preparado	0



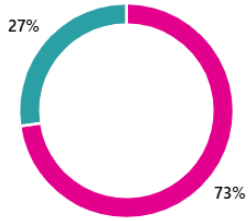
7. **¿Está familiarizado con el concepto y funcionamiento de los Honeypots?** Más detalles

Sí	8
No	2
Algo	1



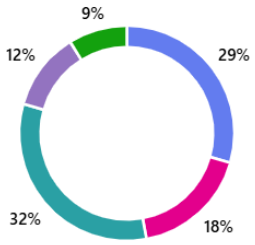
8. **¿La cooperativa ha implementado anteriormente herramientas como Honeypots para la detección de ciberataques?** Más detalles

Sí	0
No	8
No estoy seguro	3



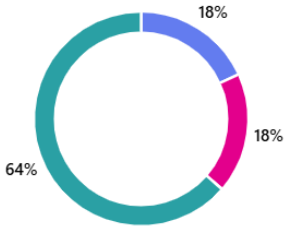
9. **¿Qué otras herramientas de seguridad se utilizan actualmente en la cooperativa para prevenir y detectar ciberataques?** Más detalles

Firewalls	10
Sistemas de detección y prevención de intrusos (IDS/IPS)	6
Soluciones de antivirus/antimalware	11
Monitoreo de logs	4
Otras	3



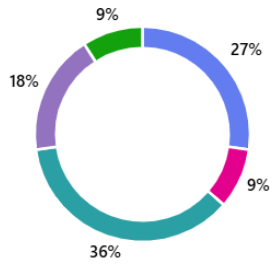
10. **¿Considera que las herramientas de seguridad actuales son suficientes para proteger la red de la cooperativa contra ciberataques?** Más detalles

Sí	2
No	2
En parte	7



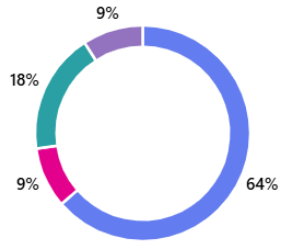
11. **En su opinión, ¿qué beneficios podría traer la implementación de un Honeypot en la red interna de la cooperativa?** Más detalles

Detección temprana de ciberataques	3
Identificación de vulnerabilidades	1
Mejora en la seguridad general de la red	4
Generación de datos para análisis de amenazas	2
Otras	1



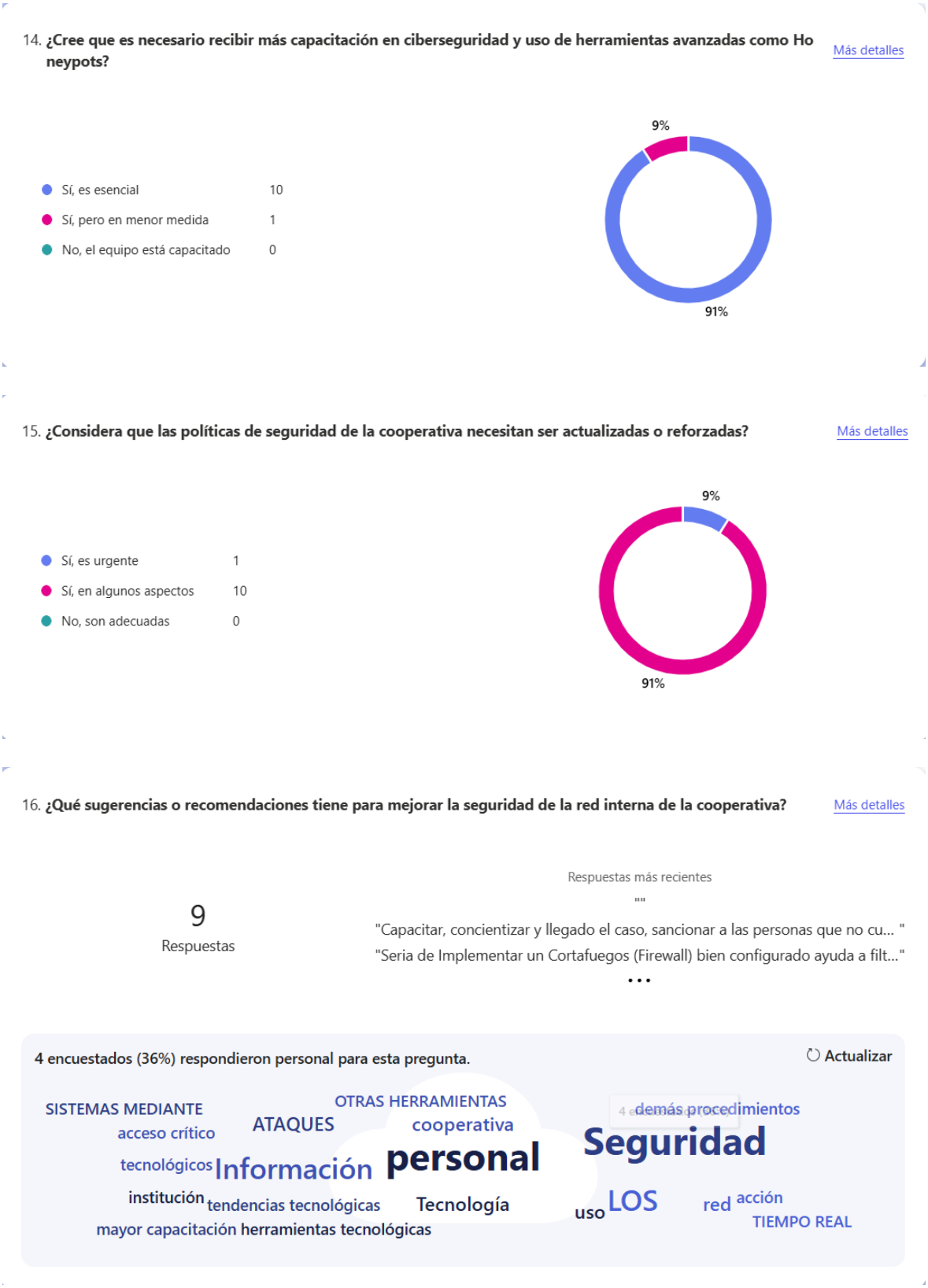
12. **¿Qué retos cree que se enfrentarían al implementar un Honeypot en la cooperativa?** Más detalles

Mantenimiento y monitoreo constante	7
Riesgo de exposición del sistema	1
Falta de personal capacitado	2
Dificultad de integración con otras herramientas	1
Otras	0



13. **¿Estaría dispuesto a capacitarse y participar activamente en el monitoreo y análisis de datos generados por el Honeypot?** Más detalles

Sí	10
No	0
No estoy seguro	1



Fuente. Departamento de Seguridad de la Información.

32. Análisis de las herramientas de detección de intrusos.

Las herramientas actualmente instaladas en la Cooperativa permiten monitorear la red informática de forma parcial, por un lado, se utiliza Nessus para la detección de vulnerabilidades. Con respecto, el antivirus Trellix brinda protección frente a ataques conocidos y amenazas emergentes; sin embargo, estas soluciones operan de forma independiente, lo que limita la efectividad general del sistema de seguridad frente a ciberataques. Por esta razón, se identifica la necesidad de implementar un sistema integrado, como un honeypot de alta interacción, que permita la detección temprana y el análisis detallado de ataques dirigidos. Esta propuesta se detalla en la Tabla 6.

Tabla 4

Comparación de las Herramientas de Detección de Intrusos

Característica	**Trellix**	**Nessus**	**Honeypot**
Propósito	Protección activa contra malware, ransomware y ataques avanzados.	Detección de vulnerabilidades en sistemas y redes.	Busca atraer y registrar los ataques para que se analicen las técnicas que usan los atacantes. Simulando diversos sistemas vulnerables atrayendo a los hackers.
Funcionamiento	Utiliza IA, machine learning y análisis de comportamiento para	Escanea la infraestructura en busca de fallos de seguridad y	

	detectar y bloquear amenazas.	configuraciones incorrectas.	
Interacción con atacantes	Bloqueo de amenazas antes de comprometer a la red.	No interactúa con los hackers lo único que hace es emitir las vulnerabilidades.	Existe una interacción con los atacantes en un sistema falso logrando analizar los métodos, herramientas y estrategias de los hackers.
Método de detección	Monitoreo en tiempo actual de los dispositivos sospechosos.	Análisis pasivo a través de escaneos periódicos.	Análisis activo de ataques dirigidos al honeypot.
Uso principal	Protección de endpoints, servidores y datos.	Identifica y corrige las vulnerabilidades antes de ser explotadas.	Obtención de inteligencia de amenazas y detección temprana de ataques.
Ejemplo de aplicación	Seguridad de estaciones de trabajo, servidores y	Evaluación de seguridad en infraestructura	Implementación en una zona desmilitarizada

	dispositivos en una cooperativa financiera.	bancaria para mitigar riesgos.	(DMZ) para detectar ataques a la red de la cooperativa.
Estrategia de seguridad	Defensa activa contra ataques conocidos y emergentes.	Prevención de vulnerabilidades explotables.	Detección temprana y análisis de ataques dirigidos.

Fuente. Elaboración propia

Por lo cual se concluye, que la implementación de un Honeypot es la solución más efectiva porque se encarga de detectar ataques desconocidos, los atrae y proporciona inteligencia sobre amenazas, complementando las defensas del Antivirus Trellix y Nessus.

33. Análisis de las políticas de seguridad

La Cooperativa cuenta con varias políticas y recomendaciones de seguridad, sin embargo, es necesario que sean actualizadas y abarque las responsabilidades y las acciones a ejecutarse cuando se produzcan los ciberataques dentro de los equipos informáticos.

Como se pudo evidenciar dentro del Departamento de Tecnología de la Cooperativa 23 de Julio, existen políticas de acuerdo a las herramientas y procedimientos actuales que están implementados, sin embargo, con el Honeypot es necesaria la actualización de las siguientes políticas, Seguridad de la red. Seguridad de los servicios de red. Segregación de redes y Filtrado web. Ver Anexo 2 “Manual de Políticas de Seguridad de la Información de la Cooperativa 23 de Julio, a noviembre del 2024”.

34. Adaptación de políticas de seguridad

Uno de los resultados más importantes fue la capacidad de la cooperativa para ajustar sus manuales, políticas, instructivos y procedimientos de seguridad en base a los hallazgos del Honeypot. Durante la prueba, se observó que la red presentaba un alto consumo de ciclos en

operaciones de almacenamiento en memoria (95% en 3 minutos), lo que indica que existe procesos críticos expuestos a posibles ataques. La identificación de los puntos que son vulnerables, en los cuales entran los puertos abiertos y las contraseñas de fácil acceso, esto llevo a que se adopte nuevas prácticas como la segmentación de la red, actualizar las credenciales de acceso y actualización de los firewalls. Determinando que el Honeypot sirve para guiar la evolución de las estrategias.

35. Política de Privacidad, Protección y Tratamiento de Datos Personales

En la tabla 4 se describe la Política de Privacidad, Protección y Tratamiento de Datos Personales de la Cooperativa 23 de Julio año 2023.

Tabla 5

Política de Privacidad, Protección y Tratamiento de Datos Personales

POLÍTICA DE PRIVACIDAD, PROTECCIÓN Y TRATAMIENTO DATOS PERSONALES	
Propósito:	Garantizar el derecho a estar informado sobre cómo Cooperativa 23 de Julio trata los datos personales en las bases de datos.
:	Se aplica a todos los datos recolectados por la Cooperativa de Ahorro y Crédito 23 de Julio Ltda., y que son proporcionados por los socios, clientes, directivos, empleados, proveedores y público en general.
Objetivos:	• Garantizar el derecho a la privacidad y protección de los datos personales. • Promover la seguridad, confidencialidad, disponibilidad e integridad en el tratamiento de los datos personales. • Impulsar el conocimiento de las normas sobre la protección y tratamiento de los datos personales.

	• Fomentar la confianza de los socios, clientes, usuarios y público en general que acceden a los productos y servicios financieros que ofrece la Cooperativa.

Fuente. Información obtenida de https://coop23dejulio.fin.ec/privacidad-cookies

36. Política de Privacidad

Asimismo, en la Tabla 5, se describe la Política de Privacidad de la Cooperativa 23 de Julio año 2023.

Tabla 6

Política de Privacidad

POLÍTICA DE PRIVACIDAD	
Propósito:	Valorar y proteger la privacidad de los datos personales de los socios.
Alcance:	Se aplica a todos los datos recolectados por la Cooperativa de Ahorro y Crédito 23 de Julio Ltda., y que son proporcionados por los socios, clientes, directivos, empleados, proveedores y público en general.
Objetivos:	• Recopilar, utilizar, compartir y proteger la información personal de los socios de la cooperativa. • Utilizar la información personal de los socios de la cooperativa para evaluar la situación financiera y la solvencia. • Analizar la información personal de los socios de la cooperativa para mantenerlos en contacto con ellos y brindarles información sobre los productos y servicios.

Fuente. Información obtenida de https://coop23dejulio.fin.ec/docs/landings/politicas-privacidad.pdf.

37. Política de Seguridad de la Información

Las políticas descritas en el "Manual de Políticas de Seguridad de la Información de la Cooperativa" (ver Anexo 1) establecen los procedimientos que deben seguirse para el tratamiento de la información y la gestión ante posibles ataques. Las políticas se encuentran alineadas a las herramientas tecnológicas disponibles en la Cooperativa. La actualización del año 2024 (página 56 del manual), demuestra las nuevas políticas que se incorporaron las cuales están basadas en reforzar la protección de los datos, mejorando la gestión de accesos y estableciendo diversos protocolos frente a incidentes de ciberseguridad. Lo que represento un avance ante la versión antigua.

El anexo correspondiente contiene el detalle completo de dichas políticas, incluyendo los cambios incorporados, lo que permite visualizar el antes y el después de la actualización mencionada.

38. Consejos de Seguridad

Como medida complementaria, la Cooperativa comparte con sus socios y público en general recomendaciones de seguridad, con el fin de evitar ser víctima de atacantes al utilizar cualquier sistema informático (*Cooperativa de Ahorro y Crédito 23 de Julio, 2023*).

Entre las recomendaciones más importantes, están las siguientes:

- Uso seguro de la tarjeta de débito.
- • Acceso seguro al sistema virtual.
- • Uso seguro de cajeros automáticos.
- • Seguridad física en las oficinas.
- • Seguridad en la app Mi23.

- • Seguridad en las transferencias electrónicas.
- • Protección contra ingeniería social.
- • Seguridad en transferencias financieras

Para el diseño del honeypot, se siguieron las buenas prácticas y se tomaron en cuenta los estándares internacionales de seguridad, los cuales deben pasar por varias fases estructuradas, alineadas con normativas como NIST SP 800-83, ISO/IEC 27001 y CIS Controls. Esto permitió definir seis fases, que comienzan con la planificación y culminan en la implementación y evaluación del honeypot en la Cooperativa de Ahorro y Crédito 23 de Julio.

A continuación, se detallan los pasos seguidos en cada una de las fases del proyecto:

. 1. Planificación: Se definió el objetivo del honeypot (¿qué tipo de amenazas se decidieron detectar o estudiar?), el alcance (red interna, externa, servicios simulados) y los recursos disponibles. También se evaluaron riesgos legales y operacionales.

2. Diseño del entorno: Se decidió el tipo de honeypot (en este caso, de alto nivel de interacción), el software a utilizar, la arquitectura de red, y los mecanismos de aislamiento y monitoreo para evitar que el sistema sea un punto de entrada.

3. Implementación técnica: Se configuró el honeypot en un entorno controlado de la cooperativa, que incluyó la instalación de servicios falsos, configuraciones engañosas, sensores de red, y herramientas de registro y alerta.

4. Validación y pruebas: Se realizaron pruebas para asegurar que el honeypot se comportara como se esperaba, no revelara que es un señuelo o estratagema, y lograra atraer actividad maliciosa por parte de atacantes. Se verificó además que los registros fueran útiles y claros.

5. Despliegue y monitoreo: El honeypot se puso en producción, es decir, operativo de forma real, y comenzó su funcionamiento normal. Fue fundamental implementar sistemas de alerta, análisis de tráfico y eventos, y garantizar la seguridad del entorno real.

6. Evaluación y mejora continua: Se analizaron los datos recolectados a través de los registros del honeypot, como los tipos de ataques, ataques utilizados, patrones de comportamiento, etc. Esto permitió ajustar el honeypot y mejorar las defensas de la infraestructura tecnológica y de red de la cooperativa.

38.1. Diseño e implementación del honeypot

Una vez diagnosticada la infraestructura de seguridad de la cooperativa y analizadas las herramientas de detección de intrusos y las políticas de seguridad existentes, se pasa a la fase de desarrollo del honeypot, que consiste en el diseño e implementación de un sistema honeypot adaptado a las necesidades concretas de la Cooperativa de Ahorro y Crédito 23 de Julio con la idea de fortalecer las capacidades de detección y análisis de ciberataques. Vamos a detallaros los pasos y las consideraciones que formaron parte del desarrollo.

39. Diseño del Honeypot

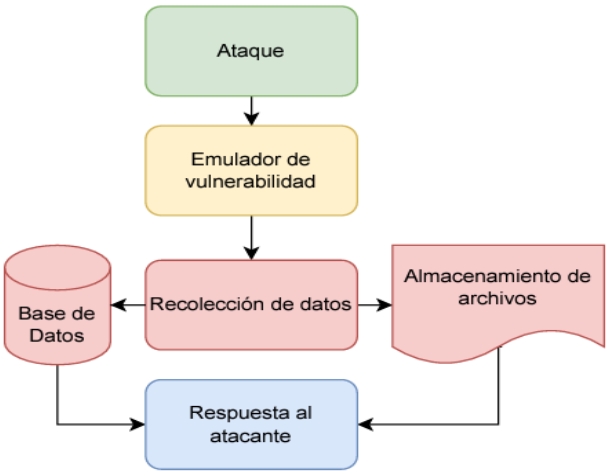
Con base en el diagnóstico analizado, se procedió al diseño del Honeypot, adaptado específicamente a las necesidades y características de la Cooperativa. Se seleccionó un Honeypot de tipo alta interacción para simular un entorno real que pudiera atraer a los atacantes, permitiendo una observación detallada de sus tácticas y técnicas, se definieron los parámetros de configuración y las métricas a utilizar para el monitoreo del sistema, alineadas con los objetivos de detección y prevención de ciberataques.

Cuando un atacante accede a la red, en primera instancia se va a encontrar con el sistema Honeypot, el cual está configurado para atraer los ataques, desviando así la atención hacia él. La eficiente configuración de este es de mucha utilidad para detectar y registrar los

datos de los ataques que recibe, aunque no tiene la capacidad de detenerlos. En la Figura 11 se ilustra el ciclo de funcionamiento del Honeypot.

Figura 11

Funcionamiento de un Honeypot.



Fuente. Elaboración propia.

40. Consideraciones biotécnicas

El desarrollo de un Honeypot para la Cooperativa de Ahorro y Crédito 23 de Julio exige poner en práctica una serie de consideraciones biotécnicas que son fundamentales para lograr la efectividad y seguridad del sistema. En primer lugar, el Honeypot debe ser configurado de manera que no comprometa la infraestructura crítica de la cooperativa, manteniéndose separado de los sistemas productivos y protegido por seguridad adicional (firewalls, IDS/IPS).

El Honeypot debe cumplir además la normativa de protección de los datos, como por ejemplo la Ley Orgánica de Protección de Datos Personales, ya que, de otro modo, se pueden producir extracciones de datos críticos sin consentimiento. El equipo técnico, además, tendrá que poner el sistema bajo monitorización, realizar el mantenimiento del sistema y analizar los datos recolectados, actuando en caso de emergencias si corresponde.

Por otro lado, es necesario que el Honeypot sea implantado según principios éticos y legales, con motivo de que no interfiera con el proceso habitual de la cooperativa y no afecte a los derechos privacidad de los clientes. Finalmente, el rendimiento del Honeypot deberá ser evaluado mediante pruebas de manera cíclica, ya que contrariamente, el Honeypot se convierte en un sistema conocido, el riesgo del cual no se ha tratado de mitigar y, finalmente, es necesario modificar la configuración del Honeypot según se registren nuevas amenazas y usar la información obtenida para las políticas de seguridad interna.

La implementación del honeypot en la Cooperativa de Ahorro y Crédito “23 de Julio” dio resultados significativos en cuanto a la detección y prevención de ciberataques. A continuación, se explican los principales resultados obtenidos luego del despliegue y monitoreo de la herramienta en la red interna de la cooperativa.

En la Tabla 8 se muestra algunos resultados obtenidos en cuanto a la aplicación de un Honeypot como medida de seguridad ante ataques dentro de la institución financiera.

Tabla 7

Aplicación de un Honeypot como medida de seguridad dentro de la institución financiera

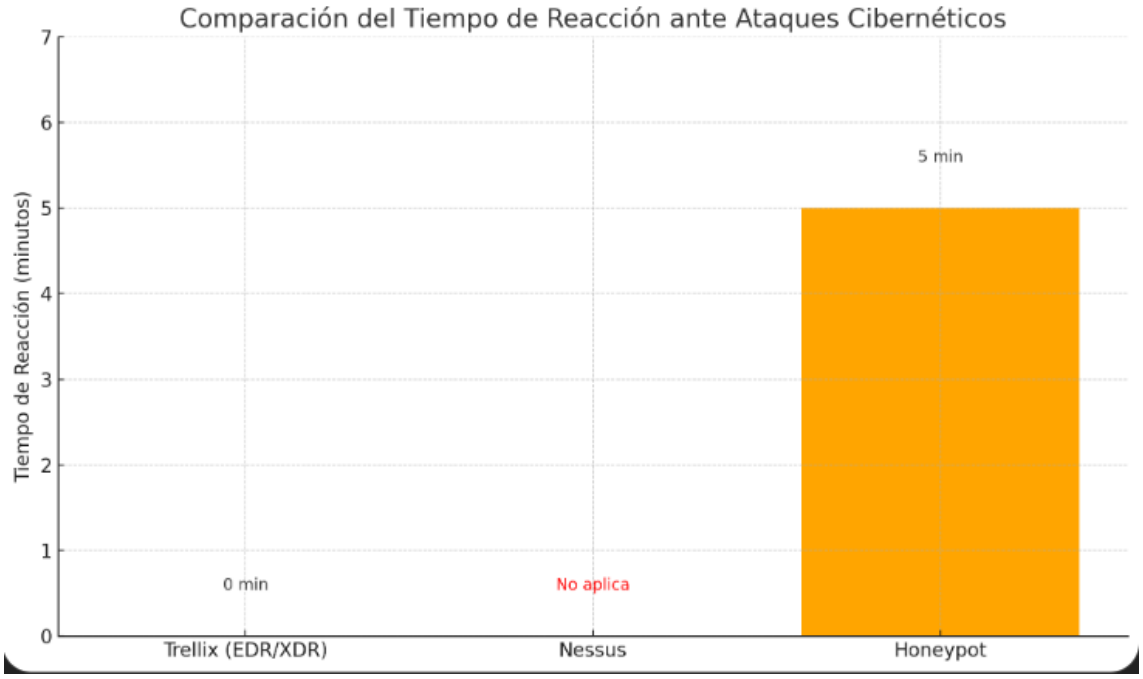
Fase de Tiempo	Comportamiento Observado	Interpretación Posible
Primeros 5 minutos	No se registraron ataques.	- Período de reconocimiento inicial por parte del atacante. - Latencia en la propagación de ataques automatizados. - La honeypot aún no era visible para bots o sistemas de escaneo.

Pico a los 10 minutos	66 ataques detectados.	- Escaneos automatizados identificaron la honeypot como objetivo viable. - Demuestra la rápida efectividad de la honeypot para atraer actividad maliciosa tras su despliegue.
Entre 10-15 minutos	Incremento moderado (66 → 74.5 ataques).	- Posible enfriamiento de actividad automatizada. - La mayoría de intentos se concentraron en el pico inicial. - El atacante pudo identificar la honeypot como señuelo y reducir su actividad.

Fuente. Elaboración propia

Gráfico 1

Comparación del tiempo de reacción ante ataques cibernéticos



Interpretación del Gráfico

- Trellix (EDR/XDR): Reacciona en 0 minutos, es decir, en tiempo real gracias a sus capacidades de inteligencia artificial y machine learning.
- Nessus: No reacciona directamente ante ataques, ya que su función es preventiva (solo identifica vulnerabilidades). Por eso aparece marcado como "No aplica".
- Honeypot: Comienza a detectar actividad maliciosa a partir de los 5 minutos, según lo que muestra el gráfico anterior de ataques detectados en el tiempo.

Tabla 8

Cuadro comparativo de seguridad mediante Honeypot

Herramienta	Tipo de Reacción	Tiempo de Reacción Estimado	Detalles

Trellix (EDR/XDR)	Reacción inmediata en tiempo real	**~0 minutos**	Uso de IA/machine learning para bloqueo instantáneo de amenazas como malware y ransomware.
Nessus (Escaneo de Vulnerabilidades)	Reacción preventiva, no detecta ataques en tiempo real	**No aplica a detección activa**	Su foco está en escanear vulnerabilidades antes de ser explotadas, sin capacidad de respuesta activa ante ataques.
Honeypot (Simulación de sistemas vulnerables)	Reacción pasiva ante interacción con el atacante	**~5 minutos** (según gráfico)	Detección basada en la interacción del atacante. El gráfico 1, demuestra que la detección comienza alrededor de los 5 minutos.

Fuente. Elaboración propia

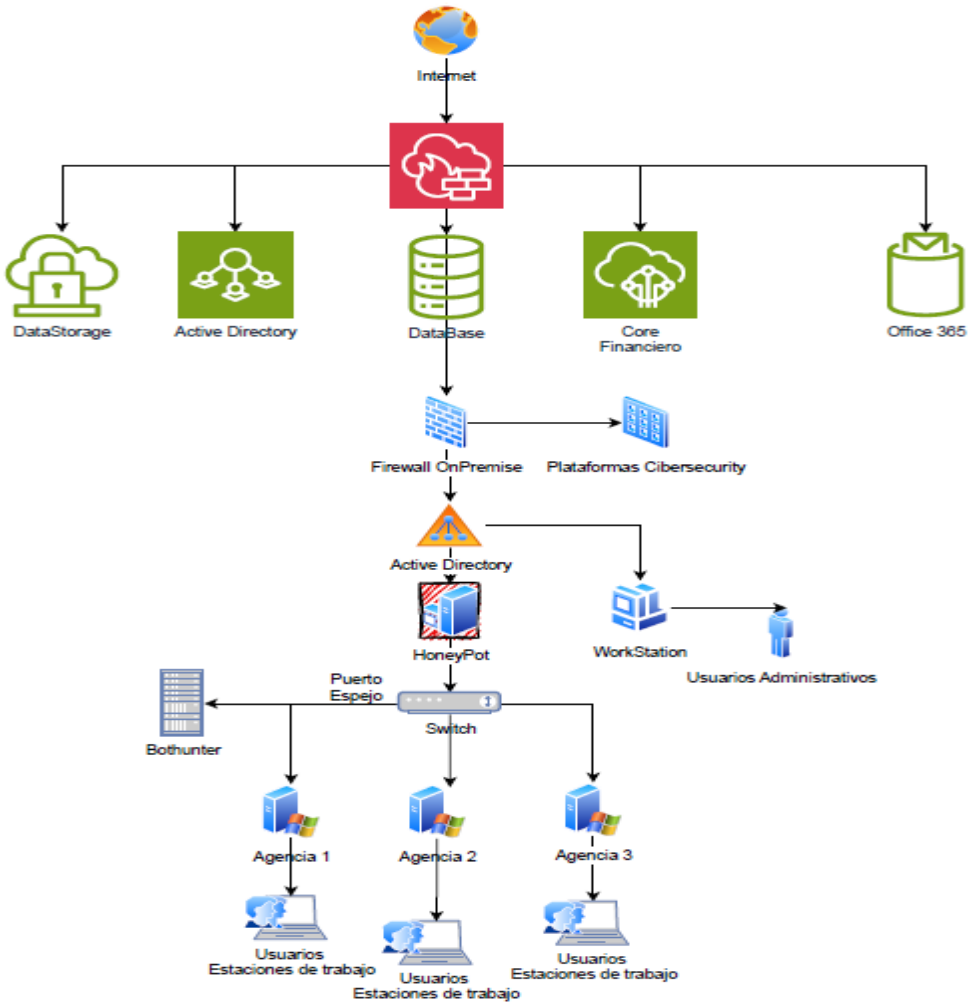
41. Implementación del Honeypot

La implementación se llevó a cabo en un entorno controlado dentro de la red interna de la Cooperativa, asegurando que no afectara las operaciones diarias ni comprometiera los datos sensibles de la entidad. Se instaló el Honeypot en un equipo específico, configurado para registrar y analizar cualquier intento de intrusión o actividad sospechosa. Durante esta fase, se activaron las medidas de seguridad correspondientes dentro de la entidad para aislar el Honeypot del resto de la infraestructura crítica, garantizando que los atacantes no pudieran

acceder a los sistemas productivos. En la Figura 12 se describe la estructura de la red de la Cooperativa 23 de Julio, detallando todos sus competentes y mecanismos utilizados para la seguridad de la red.

Figura 12

Estructura de red de la Cooperativa 23 de Julio.



Fuente. Departamento de Seguridad de la Información de Cooperativa 23 de Julio, 2024.

42. Monitoreo y recopilación de datos

Una vez identificado la institución financiera Cooperativa 23 de Julio, se procedió a identificar al equipo técnico, se consiguió los accesos autorizados para monitorear el sistema de seguridad implementado en las redes y equipos informáticos dentro de la institución

mediante software de monitoreo SON7NOC, lo cual permitió verificar el estado de la red, seguidamente se procedió analizar un sistema de seguridad basado en los Honeypot, como se muestra Figura 13.

Figura 13

Plataforma de monitoreo SON7NOC Cooperativa 23 de Julio

Fuente. Departamento de Seguridad de la Información de Cooperativa 23 de Julio, 2024.

Una vez implementado el Honeypot, comenzó el proceso de monitoreo en tiempo real. El sistema fue supervisado de forma continua, registrando todas las interacciones que los atacantes intentaran realizar. Se recopilaron datos sobre el número de ataques detectados, las tácticas empleadas por los intrusos y el origen de los intentos de acceso no autorizado. Esta fase fue fundamental para generar información valiosa que permitiera mejorar la seguridad de la Cooperativa. En la Figura 14 se representa el esquema de la recopilación datos de la Honeypot T-Pot.

Figura 14

Recopilación de datos de la Honeypot T-Pot.

Figura. Pantalla de la Honeypot implementada en el Departamento de Seguridad de la Información – T-Pot.

43. Detección de ataques e intrusiones

Durante el tiempo de monitoreo, el honeypot pudo detectar diversos intentos de acceso no autorizados a la red interna de la cooperativa. Dichos intentos se identificaron que provenían tanto de fuentes internas como externas, evidenciando el alcance y la naturaleza de las amenazas a las que se enfrenta la cooperativa. Los ataques detectados incluyeron:

- Accesos no autorizados a sistemas críticos de la cooperativa.
- Ataques automatizados, fundamentalmente dirigidos a vulnerar servicios comunes como HTTP, FTP y bases de datos.
- Ataques de denegación de servicio (DDoS), provenientes de direcciones IP externas, cuyo objetivo era interrumpir la disponibilidad de los sistemas.

44. Análisis de resultados y optimización

45. Supervisión de la red.

Una vez recopilados los datos, se realizó un análisis de los registros de actividad y los logs de seguridad existentes en los sistemas de la cooperativa, lo que permitió encontrar patrones de comportamiento sospechosos y eventos repetidos y reiterados relacionados con posibles intentos de ciberataques. Estos registros fueron clave para establecer una línea base para medir la efectividad del honeypot una vez implementado, se emplearon herramientas de auditoría de seguridad, que realizaron escaneos de la red en busca de vulnerabilidades no detectadas previamente. Estas herramientas permitieron validar la existencia de debilidades estructurales y confirmar la necesidad de implementar una solución como el honeypot en la cooperativa.

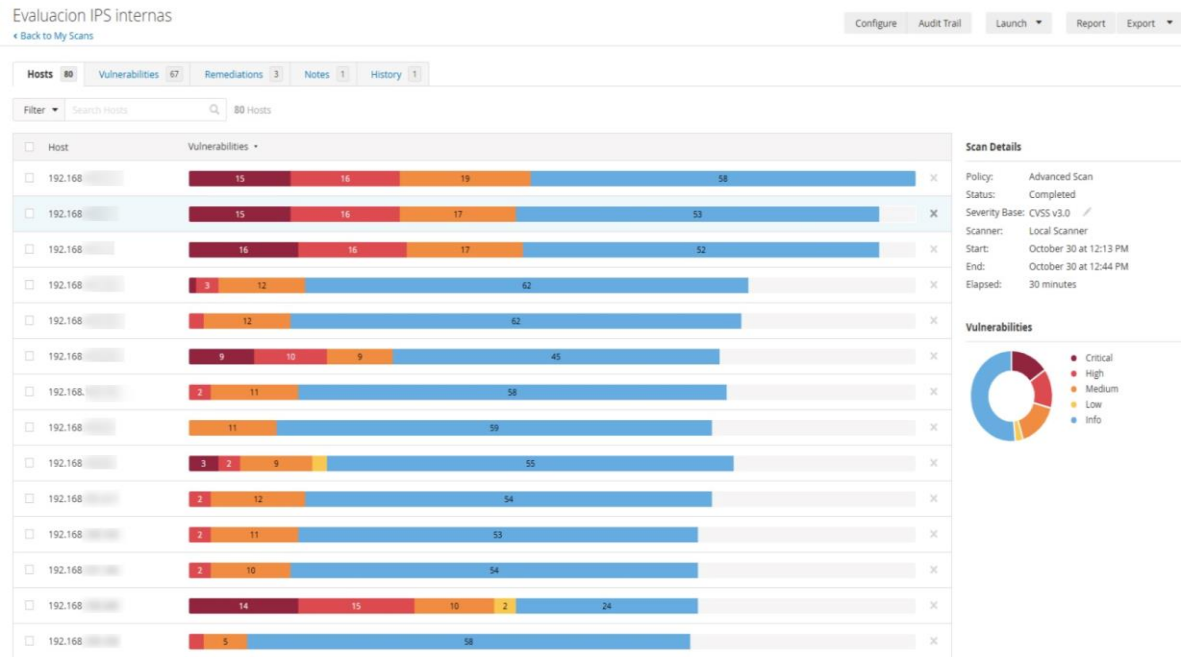
La Figura 15, muestra la evaluación de lP internas dentro de la Cooperativa 23, de julio, la cual fue realizada en un lapso de 30 minutos, encontrando un nivel de vulnerabilidades en cada equipo.

La Figura 16 presenta la evaluación de los Endpoint de la Cooperativa 23 de Julio, la cual fue realizada en un lapso de 24 minutos, encontrando un nivel mínimo de vulnerabilidades.

De igual manera, la Figura 17 presenta la evaluación de las IP Públicas de la Cooperativa 23 de julio, y claramente se pude observar que al salir al internet cuenta con más vulnerabilidades, esta evaluación se realizó por 22 minutos.

Figura 15

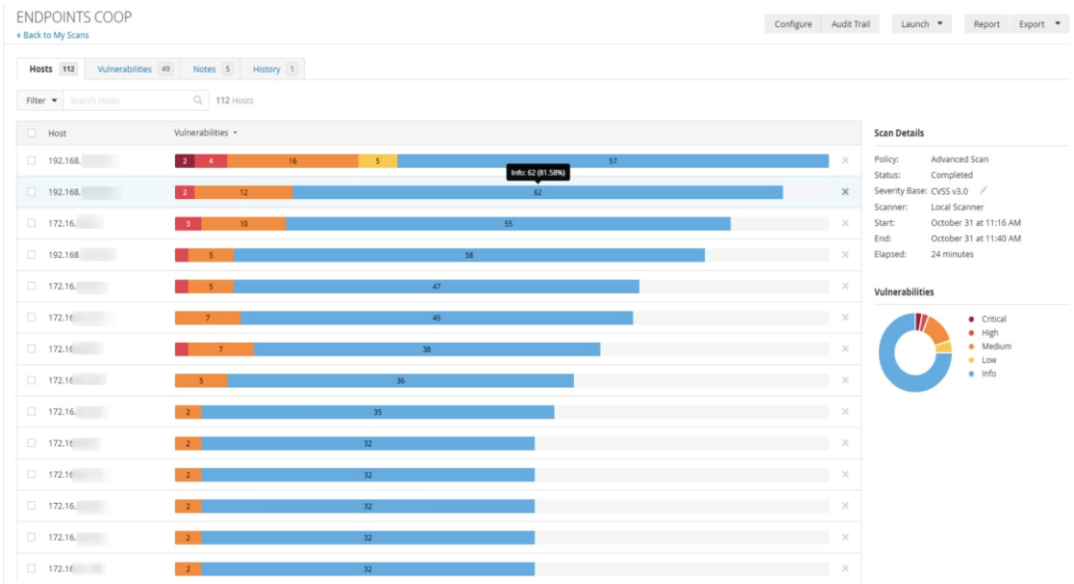
Evaluación de IP Internas red Cooperativa 23 de Julio.



Fuente: Departamento de Seguridad de la Información.

Figura 16

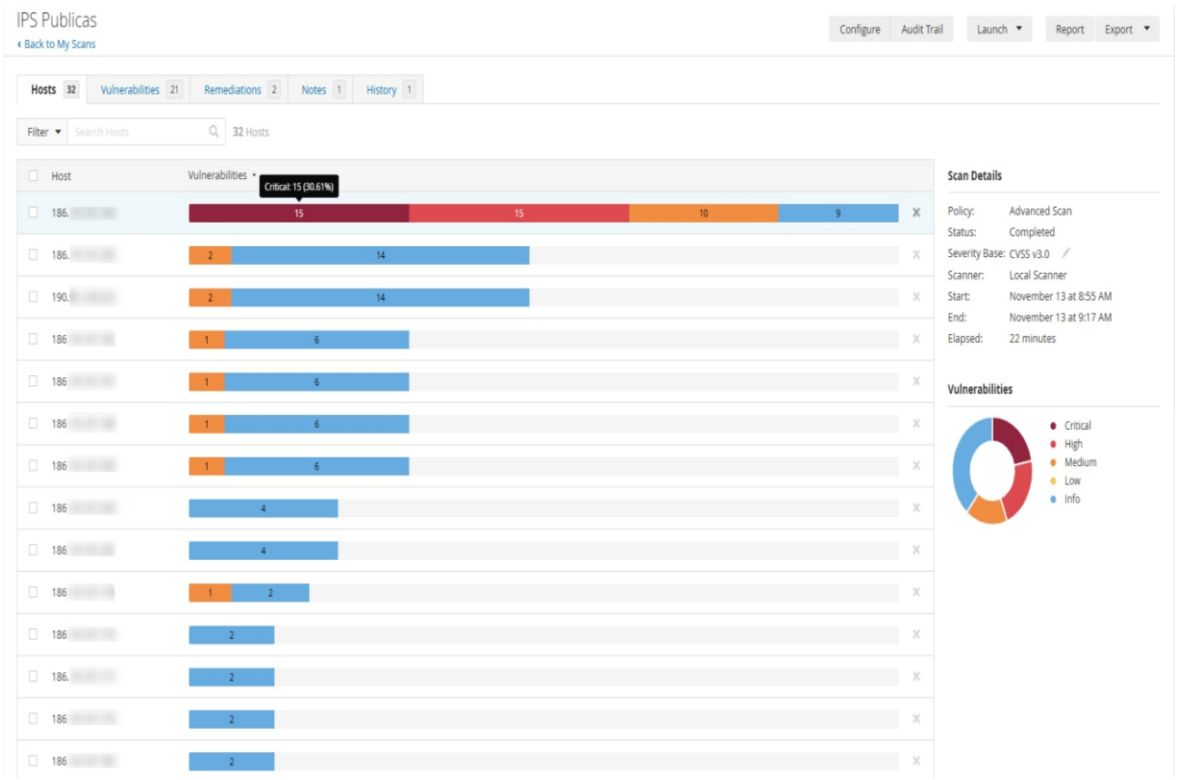
Evaluación de Endpoints Cooperativa 23 de Julio.



Fuente: Departamento de Seguridad de la Información.

Figura 17

Evaluación de IP Publicas red Cooperativa 23 de Julio.



Fuente. Departamento de Seguridad de la Información.

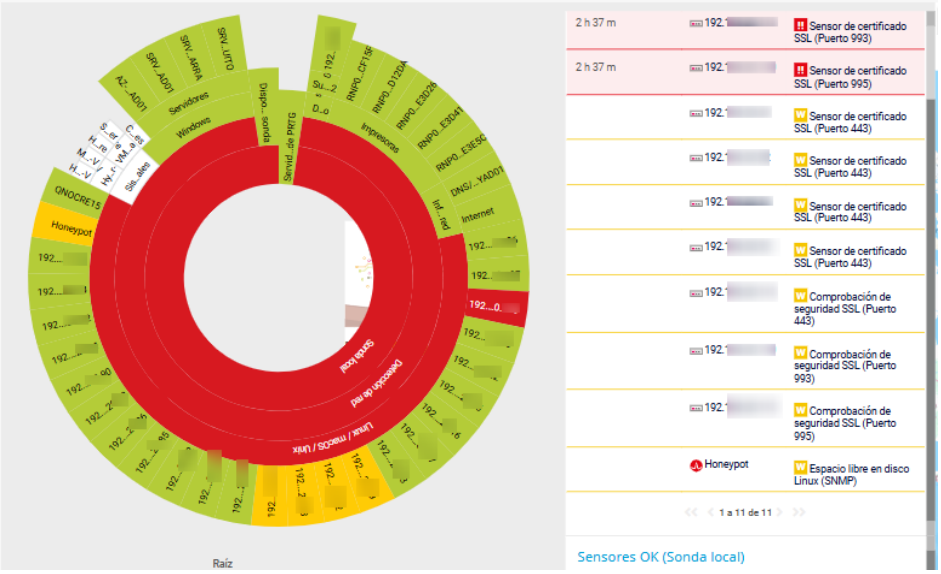
46. Interacciones de la red.

Una vez implementado el honeypot, se comenzó la fase de monitoreo, durante la cual se recopilaron datos sobre las interacciones con posibles atacantes. Se registró la cantidad de intentos de accesos no autorizados, las tácticas y estrategias empleadas por los atacantes o intrusos y la frecuencia de dichas intrusiones o ataques. Estos datos permitieron medir el rendimiento y la efectividad del honeypot y su capacidad para detectar y prevenir ciberataques.

En la Figura 18 se pude apreciar el monitoreo realizado con la herramienta T-Pot, donde se reportan alertas, servicios en riesgo y certificados SSL que está dentro de la red de la Cooperativa 23 de Julio.

Figura 18

Implementación Honeypot en la red Cooperativa 23 de Julio

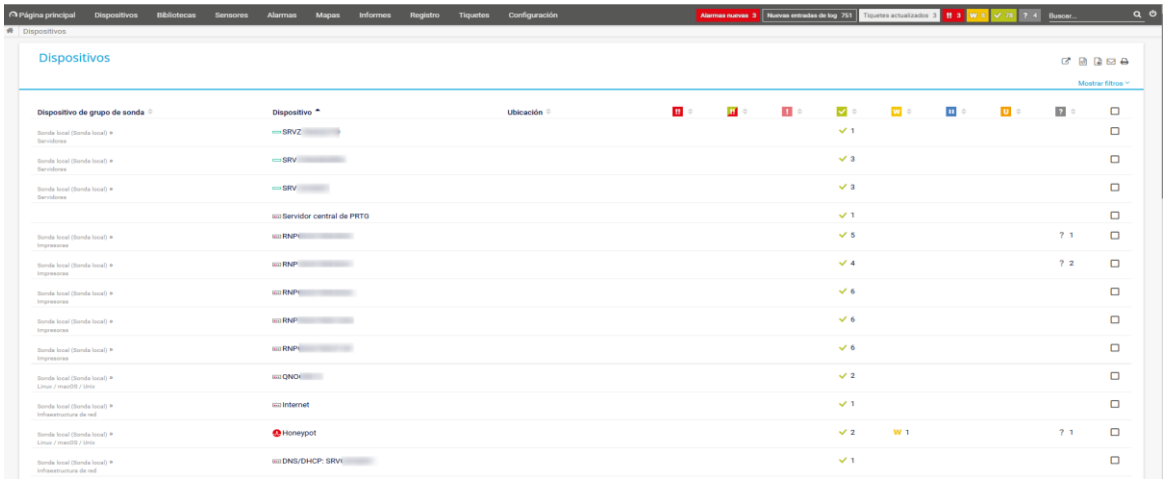


Fuente: Departamento de Seguridad de la Información

La Figura 19 muestra los dispositivos configurados en una red Honeypot de la Cooperativa 23 de Julio, donde se pude apreciar todas las características para el buen funcionamiento de la red.

Figura 19

Implementación Honeypot en la red Cooperativa 23 de Julio

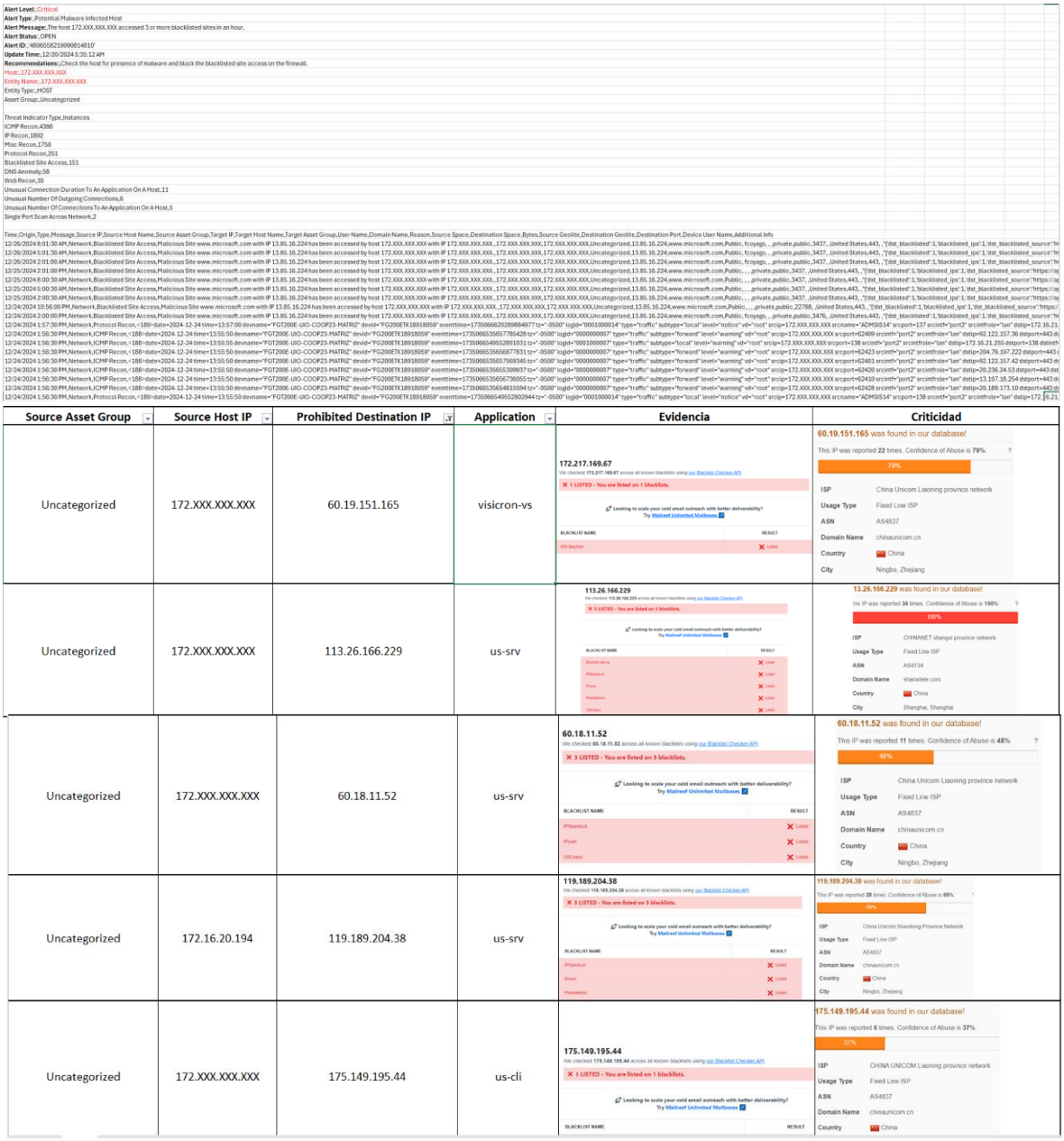


Fuente. Departamento de Seguridad de la Información

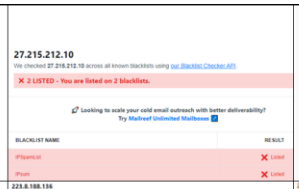
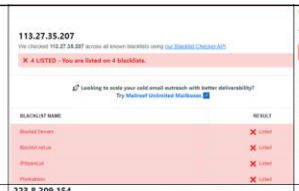
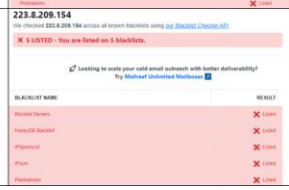
Con la información recopilada se procedió a realizar un análisis y comparación con los indicadores de rendimiento previamente establecidos, tales como el número de ataques detectados, la eficacia de las alertas generadas, y el tiempo de respuesta ante incidentes. Esto permitió evaluar de manera objetiva si la implementación del Honeypot contribuyó a mejorar la seguridad de la red interna de la Cooperativa, tal como se muestra en la Figura 20.

Figura 20

Alertas Generadas por la Honeypot



Source Asset Group	Source Host IP	Prohibited Destination IP	Application	Evidencia	Criticidad
Uncategorized	172.XXX.XXX.XXX	60.19.151.165	visicron-vs	172.217.169.67	60.19.151.165 was found in our database!
Uncategorized	172.XXX.XXX.XXX	113.26.166.229	us-srv	113.26.166.229	113.26.166.229 was found in our database!
Uncategorized	172.XXX.XXX.XXX	60.18.11.52	us-srv	60.18.11.52	60.18.11.52 was found in our database!
Uncategorized	172.16.20.194	119.189.204.38	us-srv	119.189.204.38	119.189.204.38 was found in our database!
Uncategorized	172.XXX.XXX.XXX	175.149.195.44	us-cli	175.149.195.44	175.149.195.44 was found in our database!

Uncategorized	172.16.20.194	27.215.212.10	us-cli		
Uncategorized	172.16.20.194	223.8.188.136	uncategorized		
Uncategorized	172.16.20.194	113.27.35.207	terabase		
Uncategorized	172.16.20.194	223.8.209.154	terabase		
Uncategorized	172.16.20.194	67.231.248.74	SSDP		
Uncategorized	172.XXX.XXX.XXX	113.26.231.71	SIP		

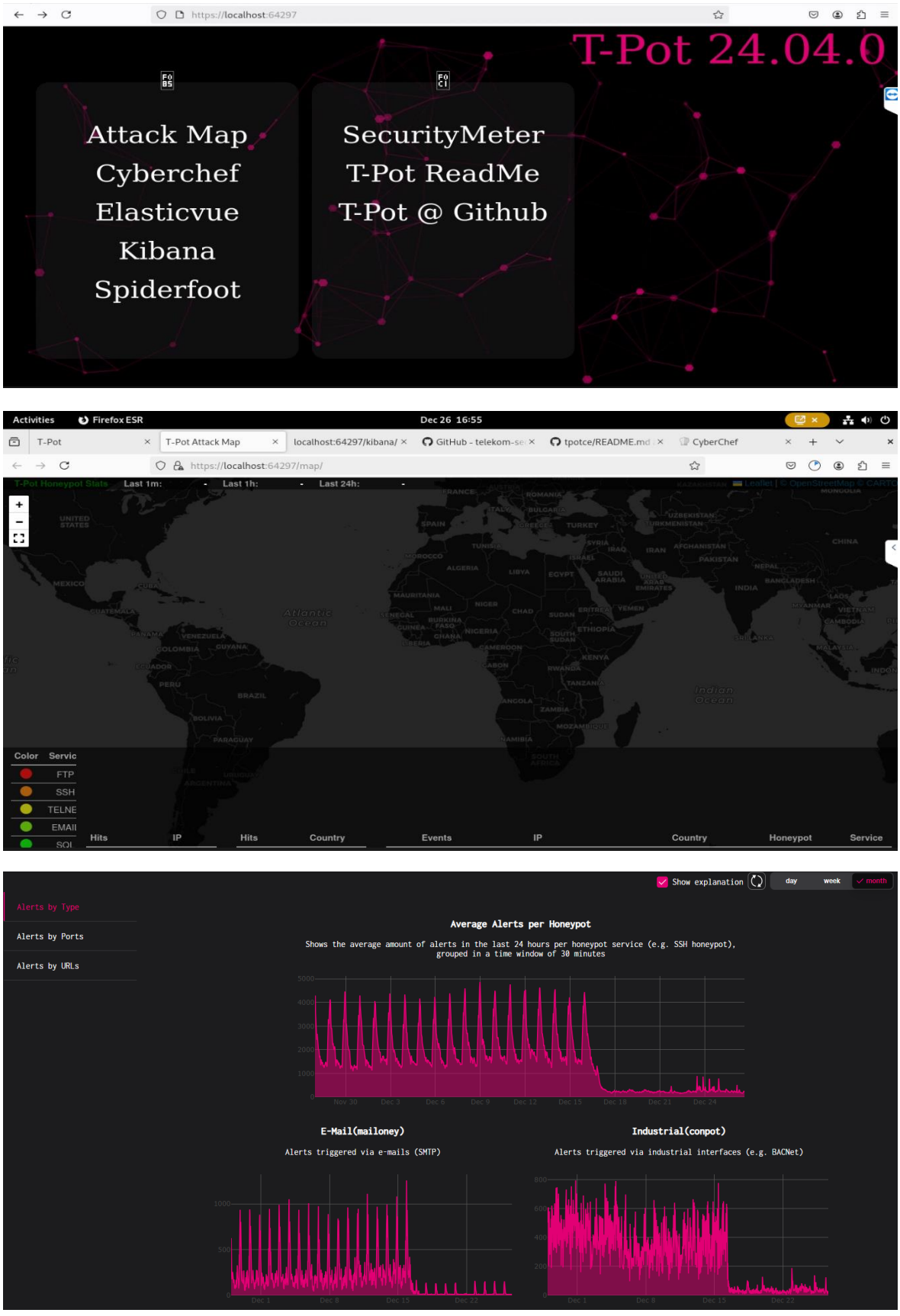
Fuente. Generada desde la T-Pot del Departamento de Seguridad de la Información de la Cooperativa 23 de Julio.

47. Procesamiento y análisis de datos.

En la etapa de supervisión, se llevó a cabo el análisis de los logs que generó el Honeypot para poder determinar las tácticas utilizadas por el atacante, el cual, para ello, considerable la información obtenida, con el fin de poder calcular valores clave, como la proporción de ataques detectados, la eficiencia del sistema, el porcentaje de alertas generadas y el esfuerzo por atenuar la reducción de los riesgos de seguridad en la red interna, tal como se expone en la Figura 21.

Figura 21

Honeypot implementada en la Cooperativa 23 de Julio



Fuente. Departamento de Seguridad de la Información, 2024.

El análisis de los datos también permitió evaluar el comportamiento de los atacantes dentro del entorno controlado del Honeypot, lo que proporcionó una visión de las técnicas y vectores de ataque utilizados. Esta información fue esencial para mejorar las defensas de la Cooperativa y ajustar las políticas de seguridad de manera proactiva.

Se realizó un análisis comparativo de los resultados antes y después de la implementación del Honeypot. Se utilizaron gráficos y tablas para representar visualmente los datos obtenidos y facilitar la interpretación de los resultados por parte de los responsables de seguridad de la entidad. De esta manera, se logró mitigar el impacto del Honeypot en la prevención y detección de ciberataques, lo que permitió tomar decisiones informadas sobre la continuidad y mejora de la estrategia de seguridad implementada, como se muestra en la Figura 22.

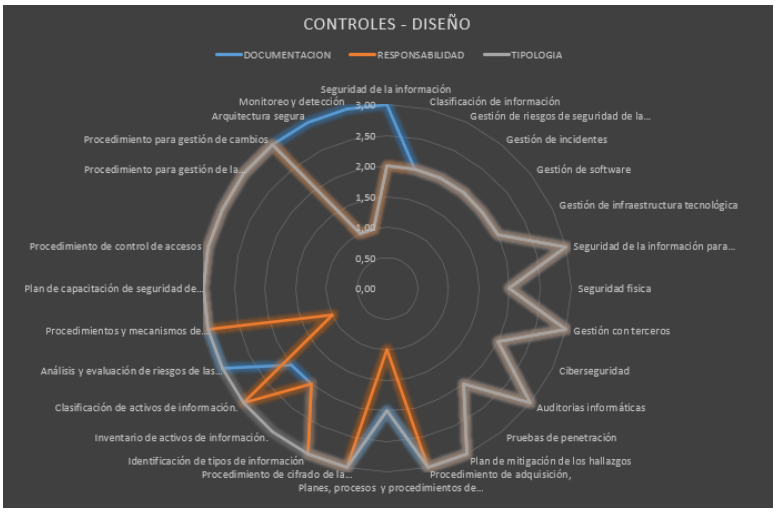
La Figura 23 representa a los controles y la ejecución de las políticas de la información de la Cooperativa 23 de Julio en el periodo de julio a junio del 2024.

La Figura 24 representa los controles y la ejecución de las políticas de la información de la Cooperativa 23 de Julio en el periodo de Julio a diciembre del 2024.

La Figura 25 representa los controles y la ejecución de las políticas de la información de la Cooperativa 23 de Julio en el periodo de Julio a diciembre del 2024.

Figura 22

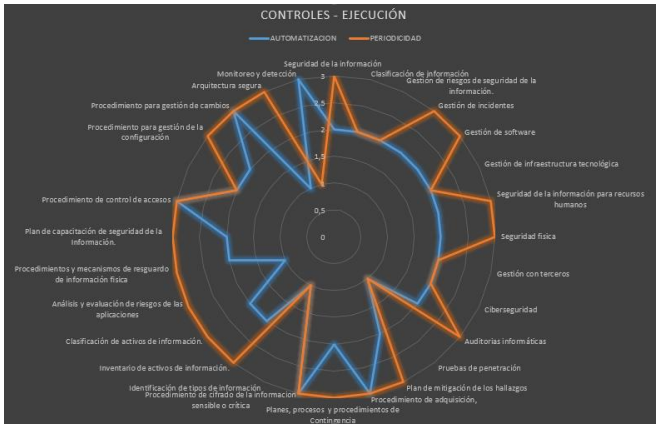
Controles-Diseño de las Políticas de Seguridad de la Información de la Cooperativa 23 de Julio a Junio del 2024



Fuente. Departamento de Seguridad de la Información

Figura 23

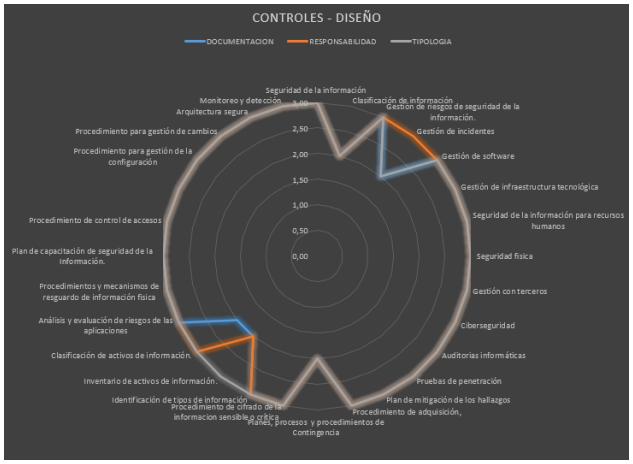
Controles-Ejecución de las Políticas de Seguridad de la Información de la Cooperativa 23 de Julio, a Junio del 2024.



Fuente. Departamento de Seguridad de la Información.

Figura 24

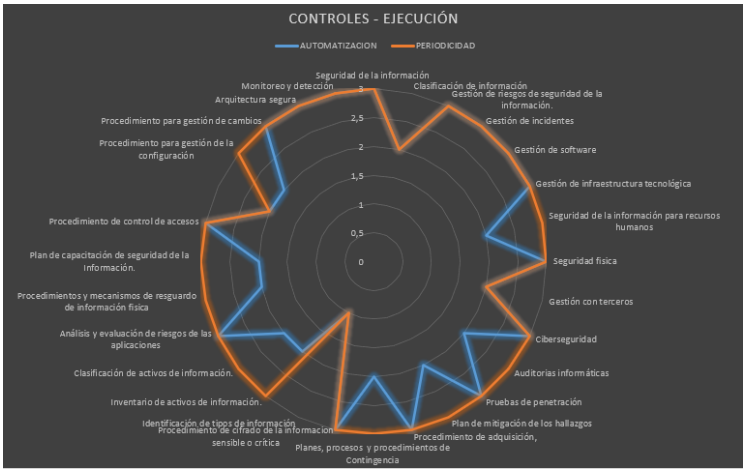
Controles-Diseño de las Políticas de Seguridad de la Información de la Cooperativa 23 de Julio, a diciembre del 2024.



Fuente: Departamento de Seguridad de la Información.

Figura 25

Controles-Diseño de las Políticas de Seguridad de la Información de la Cooperativa 23 de Julio, a diciembre del 2024.



Fuente: Departamento de Seguridad de la Información.

48. Análisis de patrones de ataque

El análisis de los registros obtenidos por el Honeypot reveló patrones recurrentes en los intentos de intrusión. La mayoría de los ataques siguieron tácticas comunes como la explotación de vulnerabilidades en puertos abiertos, intentos de fuerza bruta en contraseñas y uso de herramientas automatizadas de escaneo. Estos hallazgos permitieron identificar puntos críticos en la infraestructura, lo que ayudó a reforzar las políticas de seguridad y mejorar la protección de los sistemas internos de la entidad.

49. Resultados de investigación.

Para analizar los resultados obtenidos durante el monitoreo, se elaboraron una serie de representaciones visuales que permiten observar de forma clara el comportamiento del sistema, así como identificar patrones o variaciones relevantes en los datos recopilados. A continuación, se presentan las figuras correspondientes, donde se detallan los aspectos más relevantes del análisis realizado:

La Figura 26 muestra el comportamiento de un Honeypot en relación al antivirus Trellix actualmente instalado en la Cooperativa 23 de Julio. En primera instancia, no se encontraron ataques por lo cual el Honeypot no realizó ninguna acción y no hubo cambio. En la figura, el Honeypot detectó el primer ataque en los primeros cinco minutos que inmediatamente fue anulado. Seguidamente, se detectó más amenazas observando que el rendimiento y plan de acción efectuado por el Honeypot permitió mantener la red estable y fuera de peligro. Además, se puede apreciar que en la Coordenadas X se representan los ciclos por minutos, mientras que en las coordenadas Y, se representan la cantidad en porcentajes, de esto se puede deducir que:

- **En ciclos inferiores a 5 ciclos por minutos:**

El Honeypot en comparación el antivirus de la red mostro un 66% en su rendimiento.

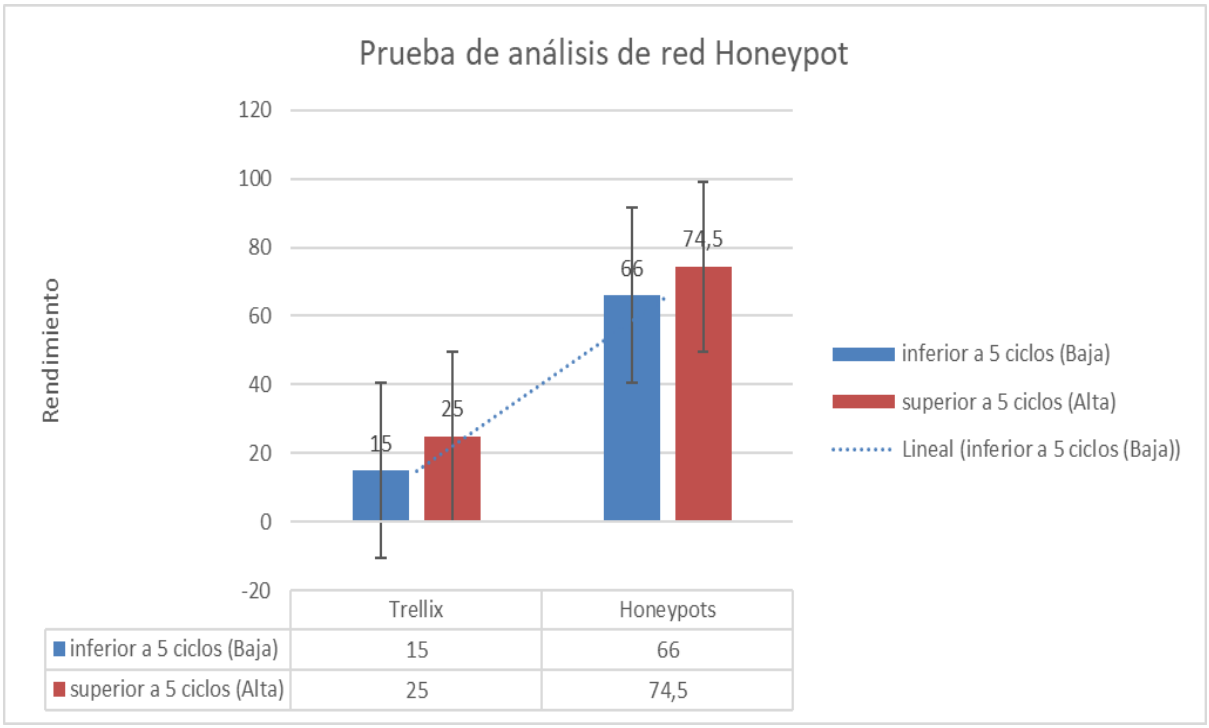
- **En ciclos superiores a 10 por minutos:**

  El Honeypot presenta un rendimiento del 74.50% en comparación con el antivirus de la red.

El análisis realizado en la red Honeypot demuestra que presenta un rendimiento óptimo en comparación al antivirus Trellix.

Figura 26

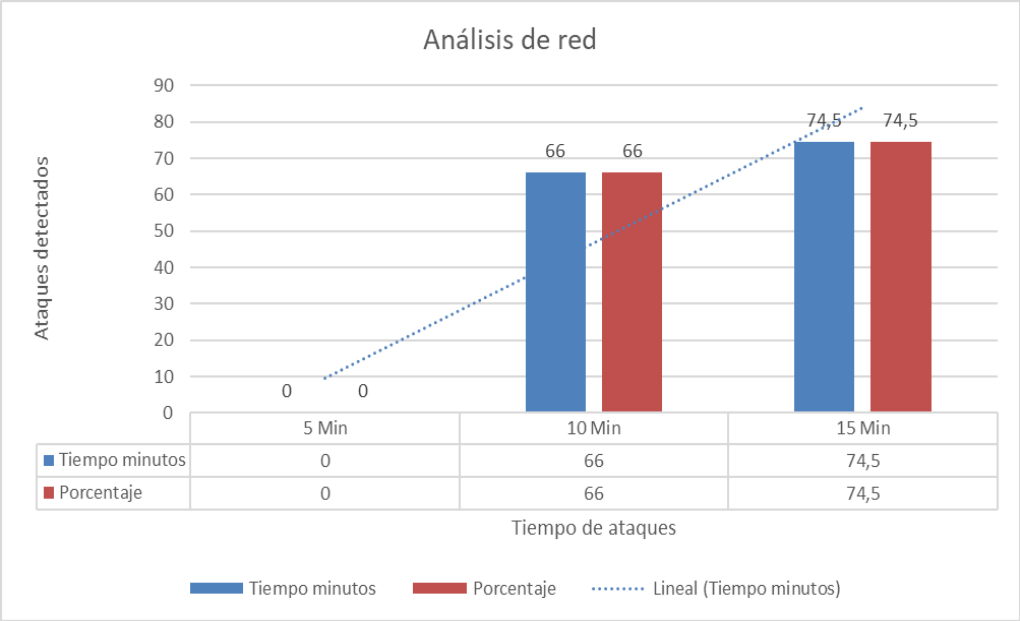
Pruebas de análisis de red Honeypot.



Fuente. Departamento de Seguridad de la Información.

Figura 27

Análisis de red sin Honeypot



Fuente. Departamento de Seguridad de la Información

Tabla 9

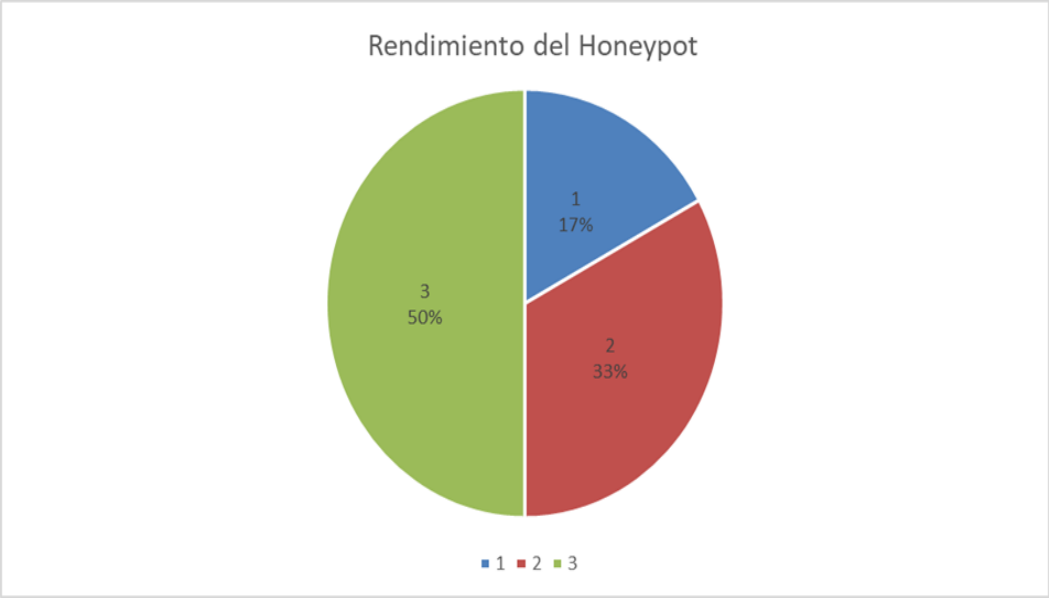
Resultados de rendimiento

Tipo de Instrucción	Porcentajes de uso	Ciclos de tiempo
Operaciones aritméticas lógicas	69%	1 minuto
Carga desde memoria	88%	2 minutos
Almacenamiento en memoria	95%	3 minutos

Fuente. Departamento de Seguridad de la Información.

Figura 28

Rendimiento del Honeypot

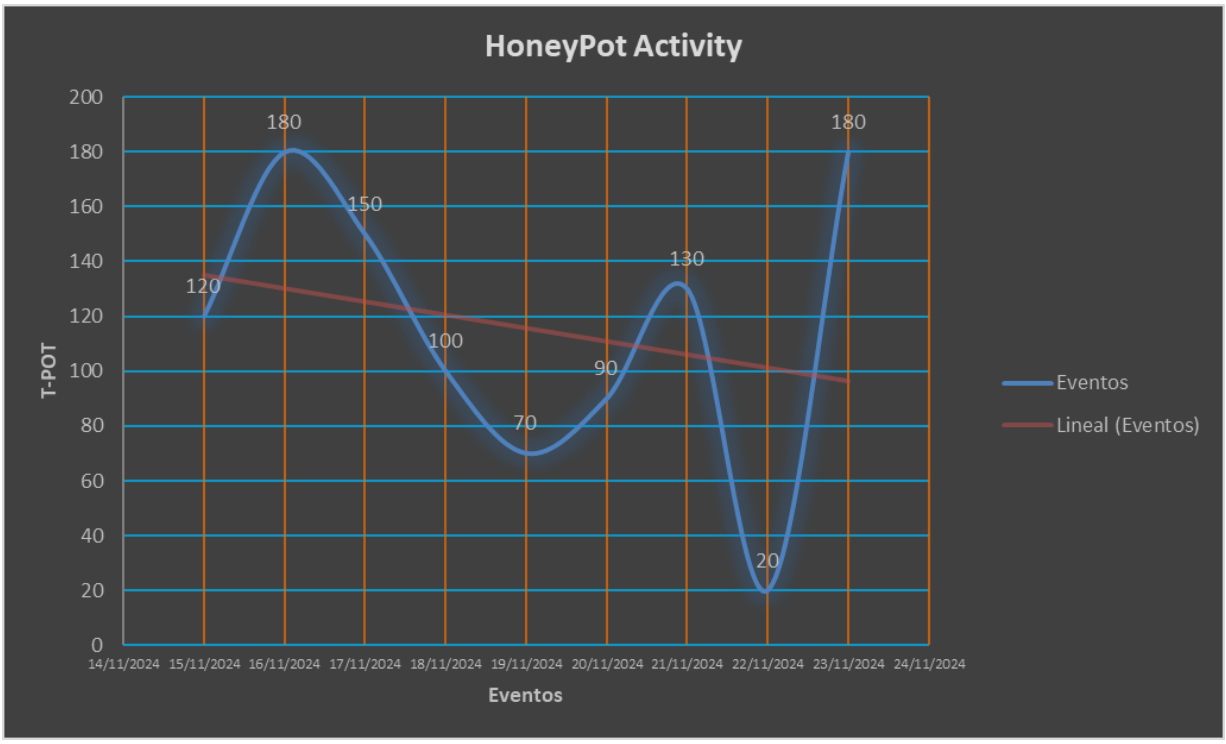


Fuente. Departamento de Seguridad de la Información

Por otro lado, también se pudieron observar los diferentes eventos que afectaron a la red. Para ello se utilizó la interfaz del Honeypot, mediante la cual se pudo constatar que la red sufrió un nivel alto de ataque alcanzado los 150K y por otro lado un nivel mínimo de ataque que alcanzó los 35K, donde K representa la tasa de rendimiento, de lo cual se promedió aproximadamente eventos detectados en un 90K. Para ello el sistema mediante colores permite representar los ataques realizados donde: 1) el color celeste simboliza el rendimiento del Honeypot en relación a ataques simulados, que alcanzó un 17%; 2) El color naranja simboliza segundo ciclo que alcanzó un rendimiento de 33%; 3) el color gris representa un rendimiento 50% de rendimiento, en operaciones de ataques simulados. Además, el Honeypot, identificó los lugares de donde se originaban dichos ataques, como se muestra en la Figura 29.

Figura 29

Estadísticas de actividades de honeypot en cuanto a tiempo.



Fuente. Departamento de Seguridad de la Información

Por otra parte, en la Figura 29, se puede evidenciar de una manera clara, las actividades realizadas por el servidor de Honeypot. Este servidor se encarga de evaluar todas las actividades y/o eventos efectuados de acuerdo al tiempo de iteración. En las coordenadas de las X, se representan la fecha de los eventos, mientras que, en las coordenadas de las Y, se representa el porcentaje en escala de 10 a 10. Simplemente, es un reporte general que lo realiza el Honeypot para mostrar los eventos efectuados.

50. Evaluación final del Honeypot.

El monitoreo se ejecutó para ciclos inferiores a 10 ciclos por minutos y ciclos superiores a 10 ciclos por minutos, a partir de los cuales se evaluó la efectividad del Honeypot y contemplando indicadores claves, como son los ataques detectados, la reducción de riesgos y la eficiencia en la generación de alertas. A partir de las pruebas obtenidas, también se realizó

actualización de la configuración del Honeypot y la mejora de las políticas de seguridad, firewalls, antivirus de la Cooperativa, se realizaron las identificaciones de los ataques relevantes e idóneos en cuanto a la preparación de medidas preventivas adicionales.

Una vez hecho el monitoreo y evaluación, se ejecutó el análisis por medio de gráficos empleados con los datos obtenidos, para ello, también se utilizaron fórmulas para medir el rendimiento de los equipos, con el fin de obtener un resultado óptimo de rendimiento del Honeypot implementado en la Cooperativa.

A continuación, se describen las fases:

Fase Inicial: Monitoreo de red Honeypot sin ataques

- Prueba efectuada con la finalidad de verificar que la red de Honeypot se encontraba funcionando correctamente.
- Se realizaron comparativos de la evaluación del rendimiento.
- No existieron complicaciones dentro de la red.

Fase 2: Monitoreo de red Honeypot con ataques menores a 10 ciclos simulados (Leve):

- Prueba de duración de 8 minutos.
- Se observó que la red Honeypot detecto muchos más atacantes con respecto a Trellix.
- La red Honeypot detecto un 60% de amenazas en comparación a Trellix que detecto un 40% de las amenazas.

Fase 3: Monitoreo de Honeypot con ataques mayores a 10 ciclos simulados (Altos):

- Prueba de duración de 12 minutos.

- De una manera óptima se detectaron a ciber atacantes simulados dentro de la red, de los cuales un 70% de atacantes fueron desviados hacia la red ficticia.
- La red Honeypot demostró un nivel alto de rendimiento al identificar gran cantidad de intrusos.
- Se monitoreo el comportamiento del Honeypot, el funcionamiento de un servidor dedicado que emulaba la función del Honeypot y la operacionalización de un software libre programado para Honeypot Dbt (Direct Base Transfer o transferencia de datos directo).
- Mediante este monitoreo, fue posible registrar la duración del evento y, posteriormente, evaluar su rendimiento utilizando la Ecuación N.º 1, la cual está diseñada específicamente para calcular el nivel de desempeño:

Ecuación No. 1:

$$CPI = \sum \frac{n}{i} = 1(CPli.Fli)$$

Donde:

CPI: Ciclos por instrucción

Fi: Frecuencia de instrucción

Entonces, tomando en cuenta, sus ciclos con relación a porcentajes de productividad y según los recursos utilizados por dicha red conlleva a que todos los ataques fueron simulados en la entrada de Xploits (Virus) al servidor.

El Honeypot detectó todos los ataques que fueron simulados para el estudio de su comportamiento, para posteriormente determinar su rendimiento total.

Cada ciclo, representa 01 minuto de duración, entonces:

- Ciclos inferiores a cinco por minuto, se consideran ataques leves;
- Ciclos superiores los diez por minuto, se consideran ataques fuertes.

Para ello, se consideró que la simulación de los ataques utilice distintos tipos de equipos de cómputo integrados y sincronizados entre sí; los cuales atacaban al servidor de Honeypot cada determinado tiempo, de esta manera se pudo observar su eficiente rendimiento.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

51.1. Comparación de ambos escenarios

52. Reducción de incidentes de seguridad

A partir de la implementación del Honeypot, la cooperativa percibe una disminución importante de los incidentes en seguridad, que dañan los sistemas productivos. Con la detección de los intentos de ataque, fue posible abordar los riesgos sin llegar al impacto en la producción. Las medidas correctivas: la mejora en las políticas de acceso y en la limitación del puerto, por ejemplo, servían para reducir las brechas de seguridad.

53. Impacto en la capacidad de respuesta

El añadir la integración del Honeypot no sólo incrementó la capacidad de detección de ataques, sino también la integración de la capacidad de respuesta ante un incidente. Se disminuyó notablemente el tiempo de respuesta ante ataques de intrusión, facilitando la toma de decisiones rápidas para contrarrestar los ataques detectados por parte del equipo de seguridad. Esto también llevó a una mayor proactividad para gestionar la seguridad, siendo cada vez más aplicadas las medidas de prevención.

54. Efectividad en la detección temprana de los ciberataques

La implementación del Honeypot permitió detectar intentos de ciberataques en etapas tempranas, lo que es fundamental para evitar que las amenazas comprometan los sistemas críticos. Según los resultados reflejados en la Figura 26, la red Honeypot detectó el primer ataque en los primeros cinco minutos y logra anularlo de inmediato. A menudo que se

realizaron más pruebas, se observó un incremento en la detección de amenazas, manteniendo un rendimiento óptimo del 74,5% en ciclos superiores a 10 minutos.

El hecho de que se detectaran patrones recurrentes y ataques automatizados, manifiesta la vulnerabilidad de la red de la cooperativa ante amenazas comunes, y refuerza la necesidad de implementar medidas avanzadas de seguridad, que complementen el uso del honeypot, como sistemas de prevención de intrusos (IPS) y controles de acceso más estrictos.

55. Mejora continua de seguridad

El honeypot proporcionó información valiosa que permitió a la cooperativa mejorar sus defensas, pero los resultados también muestran que la seguridad es un proceso continuo. Como se evidenció en el análisis de los cálculos de MPS, el rendimiento del honeypot varió en función de la carga de trabajo (estrés del sistema), alcanzando una eficiencia de 31.32 MHz/segs. Esto evidencia la importancia de mantener actualizado el honeypot y de complementar su uso con una vigilancia constante de la red, análisis periódicos de vulnerabilidades y la capacitación del personal en seguridad informática de la cooperativa.

56. Implicaciones para la cooperativa

La implementación del Honeypot tuvo un impacto positivo en la cultura de seguridad de la cooperativa, promoviendo una mayor conciencia sobre los riesgos cibernéticos. El equipo técnico y de seguridad ganó experiencia en la gestión de incidentes y en el uso de herramientas avanzadas para la detección y análisis de amenazas. A nivel estratégico, los resultados sugieren que la cooperativa debe continuar invirtiendo en tecnologías de seguridad avanzadas, ya que los ataques detectados alcanzaron picos de hasta 150k Este dato indica que la entidad es un objeto frecuente de ataques, lo que justifica la necesidad de reforzar su infraestructura y

continuar con la capacitación del personal, a fin de mantenerse protegida frente a las amenazas emergentes.

57. Variables de investigación

EL avance tecnológico ha generado varias y sofisticadas amenazas para los diferentes sistemas de información, para lo cual es necesario la adopción de medidas de seguridad de tal manera de salvaguardar y mantener la información integra y confiable, y más aún cuando se almacenan gran cantidad de datos en las instituciones financieras. Hoy en día existen varias herramientas para mitigar riesgos y amenazas informáticas de una manera correcta, pero a pesar de todas estas medidas suelen existir vulnerabilidades. Es por ello que se ha visto la necesidad de la implementación de un sistema Honeypot dentro de la Cooperativa 23 de julio, para lo cual se realizaron diferentes pruebas y se establecieron diferentes fases. Durante las pruebas se pudo determinar los niveles de rendimiento y seguridad en situaciones en tres situaciones: 1) en peligro nulo; 2) eventos inferiores a ciclos de 5 minutos (o leves); y 3) eventos superiores a 10 ciclos por minutos (o fuertes), de la cual se obtuvieron resultados óptimos de estas pruebas de red Honeypot en cuanto a su rendimiento. Una configuración adecuada de la red Honeypot pude simular un sistema Firewall o barrera protectora Honeypot obteniendo resultados muy satisfactorios en comparación con métodos tradicionales independientes como el empleo antivirus. Por otra parte, con la configuración adecuada de los complementos se puede analizar e interpretar el comportamiento del tráfico en la red de datos, de esta manera brindar un mejor control de todo el contenido, negar u obstruir los puertos innecesarios y de esta manera permitir el monitoreo de paquetes de los diferentes paquetes software dentro de sistemas informáticos y red de datos. De esto se puede concluir, que el Honeypot alcanzó un nivel del 95.4% de rendimiento, esto conlleva a que una herramienta para el buen rendimiento y una estrategia para como medida de seguridad para la protección de los datos dentro de la institución

financiera. Finalmente, se recomienda la utilización de estos estemas en las diferentes organizaciones para evitar ser víctimas de ciber ataques, que pueden afectar de una forma negativa el funcionamiento del sistema de cualquier organización.

57.1. Propuesta de nuevo manual

Debido a que el Manual de Políticas es confidencial de la Cooperativa, no se incluye en la presente memoria descriptiva de tesis. No obstante, a continuación, se abordan u conjunto de elementos que caracterizan a dicho Manual.

El nuevo Manual consolida las prácticas de seguridad actualmente vigentes en la Cooperativa 23 de Julio e integra los hallazgos derivados de la implementación de un honeypot y de pruebas técnicas específicas, generando un marco cohesionado que busca reforzar la integridad, la confidencialidad y la disponibilidad de todos los activos de la red. En este texto se delimita el alcance a las redes internas de sucursales y sus conexiones, a los dispositivos finales como estaciones de trabajo, y a los elementos críticos de infraestructura física y virtual. Asimismo, se explicitan los objetivos de estandarizar la gestión de incidentes, formalizar los criterios de acceso remoto y regular el uso de honeypots, con la meta de cerrar brechas de seguridad detectadas y optimizar una respuesta proactiva ante eventos maliciosos.

En la Cooperativa 23 de Julio coexisten un *Security Operations Center* que vigila el flujo de eventos, un equipo CSIRT encargado de responder a incidentes, y un *Network Operations Center* que vela por la continuidad y disponibilidad de la infraestructura. A estos pilares se suman escaneos de vulnerabilidades mediante Tenable Nessus, filtros anti-phishing y anti-spam, y soluciones antivirus centralizadas, como Trellix en endpoints y servidores. Sin embargo, cada una de estas herramientas opera de manera aislada, sin un punto único de integración que permita correlacionar alertas ni priorizar de forma eficiente los riesgos, lo que limita la visibilidad global del entorno.

La revisión de los registros y el análisis de las pruebas revelan debilidades recurrentes que deben abordarse de inmediato. El tiempo medio de detección supera las cuatro horas, existiendo patrones de actividad maliciosa de bajo perfil que escapan a los controles convencionales. La fragmentación de los datos de monitoreo dificulta la generación de un único tablero de mando y provoca que tanto falsos positivos como falsos negativos se disparen, consumiendo recursos valiosos en filtrados manuales. Además, la ausencia de un sistema de prevención de intrusos a nivel de red y la falta de ejercicios de simulación limitan la madurez del CSIRT, que hasta ahora carece de experiencias reales para afinar su capacidad de respuesta.

Al contrastar estas observaciones con los requisitos de la norma ISO/IEC 27001 y los controles CIS, se evidencia que los registros de eventos no están centralizados conforme al control A.12.4, la gestión de incidentes permanece en un enfoque reactivo de la cláusula A.16, el monitoreo disgregado refuta las recomendaciones del Control 12 de CIS, y el acceso sigue careciendo de un sistema de gestión de identidades unificado, contraviniendo la cláusula A.9. Estas brechas sugieren con claridad la necesidad de implementar un SIEM que aglutine logs de SOC, NOC, Nessus y del honeypot, documentar procesos de clasificación y escalado de incidentes con tiempos de respuesta definidos, integrar métricas de eficacia y adoptar una política de control de acceso centralizada.

Para cerrar estas brechas, proponemos políticas renovadas que aborden de forma integral cada área de riesgo. La gestión de incidentes debe orientarse a detectar, clasificar y remediar eventos en menos de una hora, estableciendo roles claros para el CSIRT lead, los analistas del SOC y la dirección de TI, y definiendo fases de escalado, contención de sistemas comprometidos (incluido el propio honeypot), erradicación de vectores de ataque y un informe post-mortem que retroalimente las mejoras continuas. El monitoreo permanente requerirá la integración de un SIEM y paneles en tiempo real donde se contrasten métricas como el tiempo

medio hasta la detección y el de resolución, con umbrales de alerta calibrados para reducir tanto el ruido como los vacíos de vigilancia. El acceso remoto se autorizará exclusivamente mediante VPN con autenticación de múltiples factores, redes segmentadas por zonas de confianza, grabación de sesiones con retención de noventa días y revisiones trimestrales de cuentas para revocar permisos innecesarios. Finalmente, el honeypot de alta interacción, aislado en una red de señuelo sin posibilidad de propagación al entorno real, recopilará logs y muestras de código malicioso cifradas y archivadas durante un año, bajo acceso restringido al equipo forense y al CSIRT, y se someterá a revisiones mensuales y pruebas de evasión.

Para garantizar la adopción de este marco reforzado, se presentará a la dirección un documento ejecutivo que contraste el estado actual con la proyección tras la implantación del honeypot, destacando mejoras cuantificables en tiempos de detección y retorno de inversión en horas-hombre. A continuación, se organizará un taller interactivo con el comité directivo, donde se mostrará en vivo cómo un ataque es capturado por el honeypot y se abrirá un espacio de preguntas para validar recursos y plazos. El plan de despliegue se estructurará en fases: durante los primeros tres meses se implementará el SIEM y se formalizarán las políticas de incidentes, en los tres meses siguientes se desplegará el honeypot y los paneles de monitoreo, y en los seis meses restantes se avanzará hacia la automatización de procesos y la incorporación de análisis de machine learning.

Este manual contempla su propia gobernanza mediante revisiones anuales por auditorías externas de cumplimiento ISO 27001 y CIS, ajustes trimestrales tras cada ejercicio de “table-top” o simulacro de intrusión, y un programa continuo de capacitación para asegurar que el personal mantenga vivo el conocimiento de las nuevas políticas. Como apoyo final, se incluyen anexos con un glosario de términos, una matriz RACI que vincula responsabilidades y actividades, diagramas de la red segmentada y formatos estándar para reportar incidentes,

dotando así a la Cooperativa 23 de Julio de un marco sólido y alineado con las mejores prácticas internacionales que facilita la detección temprana, la respuesta coordinada y la mejora continua en ciberseguridad.

57.2. Discusión

Los resultados obtenidos corroboran la efectividad del Honeypot como una herramienta fundamental para mejorar la seguridad de la red interna de la Cooperativa de Ahorro y Crédito 23 de Julio.

La implantación del honeypot redujo el tiempo de detección de horas o días a minutos, lo que confirma su valor como sistema de alerta temprana. Esta mejora radical en la latencia de detección le permitió al personal de la Cooperativa, pasar de un modo reactivo a uno proactivo, alineándose con los objetivos de los marcos NIST e ISO de “detección rápida” y “respuesta oportuna”.

Se corroboró que hubo una ampliación del espectro de amenazas antes de la implementación del Honeypot, ya que el personal solo veía ataques con firmas conocidas; tras la implementación del honeypot, se detectaron tácticas avanzadas (movimientos laterales, escaneos inéditos) y se generaron artefactos forenses (muestras de malware, direcciones IP nuevas). Esto coincidió con estudios que muestran que los honeypots de alta interacción revelan vectores ocultos que se escapan a los IDS/IPS tradicionales.

Hubo además una reducción de falsos negativos y visibilidad interna. El honeypot actuó como un “imán” para actividad maliciosa de bajo perfil, reduciendo considerablemente los ataques no detectados. Además, atrajo intrusos desde la red interna, por tanto, mejoró la visibilidad sobre amenazas internas (*insiders* o máquinas comprometidas).

Sin dudas, se percibió un impacto en la carga operativa y la auditoría, al aislar el tráfico malicioso fuera de los sistemas de producción, por lo que bajó la carga de eventos que debe procesar el NOC y el SOC. Al mismo tiempo, las evidencias claras (logs, muestras, hashes) mejoraron la calidad de los informes de auditoría y facilitaron el cumplimiento de controles CIS y de ISO/IEC 27001.

A pesar de todas las mejoras y ventajas tras la implementación del honeypot, también se divisaron algunas limitantes: el honeypot exige personal especializado para evitar que se convierta en vector de ataque; ningún honeypot es omnisciente; por lo que ciertos ataques muy dirigidos o a nivel de aplicación pueden no caer en el señuelo; además de la existencia de falsos positivos, debido al uso en la Cooperativa de bots indiscriminados o escáneres legítimos, que pueden generar ruido, requiriendo filtrado adicional.

Se recomienda, en la misma línea de investigación y desarrollo, automatizar la ingesta de logs del honeypot en un módulo para visualización en tiempo real; implementar *machine learning* para clasificar patrones de ataque inéditos; desplegar honeypots segmentados según tipo de servicio (web, FTP, RDP) y comparar su eficacia; y evaluar el retorno de inversión midiendo el ahorro en horas-hombre de respuesta y mitigación.

Aunque el Honeypot demostró ser efectivo con un 95,4% (Figura 28), su uso presenta algunas limitaciones. Al tratarse de una herramienta pasiva, depende de la atracción de atacantes para generar datos. Como se observa en la Figura 29, algunos eventos registrados no representaron ataques reales, lo que evidencia que la herramienta no es suficiente por si sola para la protección total de la red. Esto significa que, si un atacante no interactúa con el Honeypot, podría no detectarse su actividad en la red. Además, no es capaz de prevenir ataques por sí solo, por lo que debe utilizarse en conjunto con otras medidas de seguridad, como sistemas de prevención y políticas de gestión de vulnerabilidades.

De manera resumida, se pudo establecer la siguiente comparación, antes de la implementación del honeypot y después de la implementación de este:

Métrica	Antes del Honeypot	Después del Honeypot
Tiempo de detección de amenazas	Horas o días (basado en alertas genéricas y revisión manual)	Minutos (detección inmediata de actividad en el honeypot)
Tipos de ataques identificados	Limitados a firmas conocidas (malware, phishing, spam)	Se detectan técnicas nuevas, movimientos laterales y escaneo de red
Reducción de falsos negativos	Alta tasa de omisión en ataques de bajo perfil	Se reducen falsos negativos gracias al señuelo explícito del honeypot
Nivel de visibilidad de amenazas internas	Baja (depende del monitoreo tradicional)	Alta (el honeypot captura comportamientos sospechosos internos)
Inteligencia de amenazas recolectada	Básica (registro de eventos estándar)	Enriquecida (muestras de malware, IPs, vectores, patrones nuevos)
Carga sobre equipos de producción	Alta (eventos dispersos y no priorizados)	Baja (el honeypot aísla eventos sospechosos fuera del entorno real)
Capacidad de respuesta del personal	Reactiva (poca anticipación)	Proactiva (se anticipan escenarios reales de ataque)
Soporte para auditorías de seguridad	Basado en logs convencionales	Evidencias claras y trazables desde el honeypot

Con la implementación del honeypot, no solo mejoró la detección y el análisis de amenazas, sino que también se convirtió en una fuente de entrenamiento para el personal de la Cooperativa y en un elemento clave en los informes de auditoría o cumplimiento normativo.

Hasta este punto, y teniendo en cuenta la hipótesis de trabajo inicial “la implementación de un Honeypot para la prevención y detección de ciberataques garantizará la seguridad de la información en la red interna de la Cooperativa de Ahorro y Crédito 23 de Julio”, se puede afirmar que se cumple, ya que se demostró que además de las medidas tecnológicas que se llevaban a cabo inicialmente en la red y los dispositivos de la cooperativa, estas no eran suficientes, y a partir de la implementación del honeypot, se identificaron nuevos incidentes de seguridad que atentaban gravemente contra la seguridad de la información.

CONCLUSIONES

- La Cooperativa de Ahorro y Crédito 23 de Julio se caracteriza por presentar una eficiente gestión de seguridad de información, ya que utiliza herramientas avanzadas como Trellix y Nessus para el monitoreo de intrusos que permiten la protección de sus redes, datos y sistemas informáticos contra las actuales amenazas cibernéticas. Además, permiten la detección oportuna y respuesta efectiva ante los incidentes de seguridad. Sin embargo, cada vez aparecen nuevas amenazas es por ello que la infraestructura y los requisitos de seguridad específicos cada vez deben ser actualizados de manera oportuna.
- Dentro de la institución financiara existen políticas de seguridad enfocadas en garantizar que la información permanezca disponible, integra y confiable como lo determina el estándar internacional de la ISO 27001 estableciendo todas las métricas de actuación al momento que existen vulnerabilidades dentro de los equipos y redes informáticos. El análisis de estas vulnerabilidades permitió evaluar la efectividad de las políticas de seguridad existentes y realizar ajustes basados en evidencia concreta, fortaleciendo la red ante nuevos ataques de tal manera de mejorar los manuales y procedimientos de seguridad dentro de la institución, es por ello que se actualizo la Política Noviembre 2024, en base a la Seguridad de la red, Seguridad de los servicios de red, Segregación de redes y Filtrado Web.
- La tecnología cambia cada día y aparecen nuevas amenazas que hace que la institución adopte otros sistemas de seguridad para proteger su información, para lo cual se realizó un levantamiento de la información lo que conllevó a diseñar un Honeypot con un nivel alto de interacciones que actúa como una trampa para la detección de ciberataques en las redes de datos de la Cooperativa de Ahorro y Crédito 23 de Julio, de acuerdo a sus objetivos y al número de interacciones, esta

red se caracteriza ser una estrategia efectiva para fortalecer la seguridad de la información dentro de la institución en comparación con las actuales herramientas de detección de intrusos utilizadas. La configuración del Honeypot proporcionó una visión más detallada sobre los intentos de ataque permitiendo mejorar la capacidad de respuesta y de esta manera reducir los incidentes de seguridad en la red interna.

- Se implementó un honeypot y se dio monitoreo y recopilaron los datos. Se detectaron nuevos ataques e intrusiones que anteriormente no se habían detectado. Se analizaron además patrones de ataques.
- Durante las pruebas realizadas al Honeypot implementado se pudo determinar en 94,5% de rendimiento enfocado en detectar, analizar y mitigar intrusos o amenazas dentro de la red Cooperativa de Ahorro y Crédito 23 de Julio. Su implementación permite obtener experiencia sobre ataques en tiempo real sin afectar a buen desempeño de los equipos y de la red principal. Sin embargo, la eficiencia depende de una correcta configuración que permita el constante monitoreo con ajustes periódicos para adaptarse a nuevas tácticas utilizadas por ciberdelincuentes.
- A partir de la implementación del Honeypot, la cooperativa percibió una disminución importante de los incidentes en seguridad, que dañan los sistemas productivos. Con la detección de los intentos de ataque, fue posible abordar los riesgos sin llegar al impacto en la producción.
- La red Honeypot detectó el primer ataque en los primeros cinco minutos y logra anularlo de inmediato. A menudo que se realizaron más pruebas, se observó un incremento en la detección de amenazas, manteniendo un rendimiento óptimo del 74,5% en ciclos superiores a 10 minutos.
- A nivel estratégico, los resultados sugieron que la cooperativa debe continuar invirtiendo en tecnologías de seguridad avanzadas, ya que los ataques detectados

alcanzaron picos de hasta 150k Este dato indica que la entidad es un objeto frecuente de ataques, lo que justifica la necesidad de reforzar su infraestructura y continuar con la capacitación del personal, a fin de mantenerse protegida frente a las amenazas emergentes.

- El nuevo Manual consolida las prácticas de seguridad actualmente vigentes en la Cooperativa 23 de Julio e integra los hallazgos derivados de la implementación de un honeypot y de pruebas técnicas específicas, generando un marco cohesionado que busca reforzar la integridad, la confidencialidad y la disponibilidad de todos los activos de la red.
- El nuevo manual contempla su propia gobernanza mediante revisiones anuales por auditorías externas de cumplimiento ISO 27001 y CIS, ajustes trimestrales tras cada ejercicio de “table-top” o simulacro de intrusión, y un programa continuo de capacitación para asegurar que el personal mantenga vivo el conocimiento de las nuevas políticas.

RECOMENDACIONES

- Es importante mantener actualizado el Honeypot de forma periódica, en vista que las amenazas siempre están buscando nuevas vulnerabilidades en los sistemas, es por ello que se debe configurar el Honeypot de tal manera de reflejar las últimas amenazas, de esta manera actualizar su software y realizar las configuraciones para alcanzar la efectividad ante las nuevas tácticas de los atacantes.
- Actualizar los políticas y procedimientos de seguridad dentro de la institución haciendo partícipes a todos los usuarios, para mejorar el control de accesos, cambiar configuraciones de firewall, cerrar puertos expuestos o actualizar contraseñas tomando en cuenta que los datos obtenidos del Honeypot muestra claramente las debilidades de la red y mediante las soluciones adecuadas la información siempre esté disponible, integra y confiable dentro de la institución financiera.
- El equipo del Departamento de Seguridad de la Cooperativa 23 de Julio debe familiarizarse con el funcionamiento y mantenimiento del Honeypot para aprovecharlo al máximo, para determinar las últimas amenazas y técnicas de ataque, para lo cual debe realizar entrenamientos constantes haciendo uso de herramientas avanzadas en respuesta a incidentes dentro de las redes.
- Mantener planes de contingencia y de recuperación en caso de un ataque exitoso, el cual debe enfocarse en saber cómo reaccionar ante un incidente y establecer los procedimientos claros para restaurar los sistemas y minimizar el impacto, además definir métricas clave para evaluar la efectividad de las medidas de seguridad.

BIBLIOGRAFÍA

Arundhati, G. (2024). *PCI DSS 4.0.1 simplificado: una guía para el cumplimiento de la seguridad de pagos (PCI)*. Obtenido de https://www.scrut.io/post/pci-dss-4-0-1-guide

Asamblea Nacional del Ecuador. (2014). *Ley General de Instituciones del Sistema Financiero (Ley No. 2000-13)*. Obtenido de https://www.asambleanacional.gob.ec

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales.* Quito.

Cibersafety. (14 de septiembre de 2024). *Honeypots: La trampa perfecta para ciberdelincuentes y una valiosa herramienta de defensa cibernética*. Obtenido de https://cibersafety.com/honeypots-trampa-ciberdelincuentes/?utm_source=chatgpt.com

COBIS. (2023). *Caso de éxito: Cooperativa 23 de Julio y COBIS OmniTeller*. Obtenido de https://blog.cobistopaz.com

Congreso Nacional. (2002). *Comercio electrónico, firmas y mensajes de datos.* Quito.

Conti, G., Raymond, D., & Russel, T. (2018). *Penetration Testing for Financial Institutions.* CRC Press.

Cooperativa 23 de Julio. (2023). *Política de Protección de Datos Personales.* Cayambe.

Cooperativa 23 de Julio. (2024). *Medidas de seguridad en plataformas digitales*. Obtenido de https://coop23dejulio.fin.ec

Cooperativa de Ahorro y Crédito 23 de Julio. (2023). *Blog y Noticias que te mantendrán la vida fácil y estarás siempre al día con tu cooperativa.* Obtenido de https://coop23dejulio.fin.ec/blog-seguridad

Cooperativa de Ahorro y Crédito 23 de Julio. (2023). *Política de Privacidad, Proteccción y Tratamiento de Datos Personales*. Obtenido de https://coop23dejulio.fin.ec/privacidad-cookies

Cooperativa de Ahorro y Crédito 23 de Julio. (2024). Obtenido de https://coop23dejulio.fin.ec/blog-seguridad

Corone, I., & Quirumbay, D. (2022). Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web. *Revista Científica y Tecnológica UPSE (RCTU), 9*(2), 97-108.

Díaz, I. (2024). *Gestión de la Protección de datos y Seguridad de la información para Cooperativas de Ahorro y Crédito en Ecuador*. Obtenido de https://www.globalsuitesolutions.com/es/privacidad-y-seguridad-en-cooperativas-de-ahorro-en-ecuador/

Gómez, J., Castaño, N., & Correa, L. (2023). Sistemas de detección y prevención de intrusos: una taxonomía experimental basada en código abierto orientada a la industria 4.0. *Revista unimilitar, 3*(1), 75-86.

Guaña, J. (2023). La importancia de la seguridad informática en la educación digital: retos y soluciones. *Recimundo, 7*(1), 609-616.

Guinea, M. (2021). *Implementación de un Sistema de Detección de Intrusos IDS mediante la inspección de tráfico de la red.* Catalunya: Universidad Catalunya.

IMB. (2024). *¿Qué es un centro de operaciones de red (NOC)?* Obtenido de https://www.ibm.com/mx-es/topics/network-operations-center

International Organization for Standardization ISO/IEC 27001. (2013). *Information security management systems - Requirements*. Obtenido de ISO/IEC 27001:2013: https://www.iso.org/standard/54534.html

IONOS. (2020). *¿Qué es un wrapper en programación?* Obtenido de https://www.ionos.com/es-us/digitalguide/paginas-web/desarrollo-web/que-es-un-wrapper/

ISO. (2013). *ISO/IEC 27001: Information Security Management Systems Requirements.*

Jacintogr. (25 de noviembre de 2020). *La importancia de la calidad de los datos en las empresas*. Obtenido de IT:Blog: https://itblogsogeti.com/2020/11/25/la-importancia-de-la-calidad-de-los-datos-en-las-empresas/

Jumbo, K., & García, M. (2024). *Implementación de un sistema de detección de intrusiones utilizando honeypots especializados en el procesamiento de pagos y generación de transacciones falsas, diseñado específicamente para su aplicación en entornos de transacciones en línea.* ESPE, Latacunga.

Llanos, A. (Enero de 2024). *Minery Report*. Obtenido de https://mineryreport.com/blog/honeypots-estrategia-seguridad-ciberataques/?utm_source=chatgpt.com

Logo ESG Innova Group. (09 de noviembre de 2023). *Blog Especializado En Ciberseguridad*. Obtenido de https://www.pmg-ssi.com/2023/11/estructura-para-un-sistema-de-gestion-de-seguridad-de-la-informacion/

Mapas, G. (2020). *Google Maps*. Obtenido de https://www.google.com/maps/search/cooperativa+de+ahorro+y+credito+23+de+julio/@-0.1898437,-78.511805,22964m/data=!3m1!1e3?entry=ttu&g_ep=EgoyMDI0MTIxMS4wIKXMDSoASAFQAw%3D%3D

Mokube, I., & Adams, M. (2007). Honeypots: Concepts, Approaches, and Challenges. *Proceedings of the 45th Annual Southeast Regional Conference*, 321–326. doi:https://doi.org/10.1145/1233341.1233395

Moreno, M. A. (2018). Desarrollar Un Análisis De Vulnerabilidades En Cooperativa Alianza, Para La Identificación Y Corrección De Las Vulnerabilidades Y Accesos No Autorizados A Los Diferentes Sistemas De Información.

National Institute of Standards and Technology. (2020). *NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations*. Obtenido de https://csrc.nist.gov/publications

Navarro, M. (01 de julio de 2015). *Revista Byte*. Obtenido de https://revistabyte.es/tendencias-tic/evolucion-y-tendencias-de-la-seguridad-perimetral/?utm_source=chatgpt.com

Perdigón, R., & Orellana, A. (2021). Sistemas para la detección de intrusiones en redes de datos de instituciones de salud. *Revista Cubana de Informática Médica, 13*(2).

Pérez, A. (2024). *Honeypot: 5 tipos principales para proteger tus datos*. Obtenido de https://www.obsbusiness.school/blog/honeypot-5-tipos-principales-para-proteger-tus-datos

Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in Computing* . Pearson.

Rentería, H., Ramírez, J., Plata, C., & Cárdenas, J. (2021). Análisis de intrusiones cibernéticas con el uso del Honeypots. Una revisión sistemática. *Brazilian Applied Science Review, 5*(6), 2218-2248. doi:10.34115/basrv5n6-012

Salazar, J., & Campoverde, M. (2022). Dectección de vulnerabilidades informáticas en estaciones de trabajo: Caso de estudio Hospital de Especialidades José Carrasco Arteaga. *Pol del conocimiento, 7*(4), 446-465.

Scott, R. (2023). *¿Qué es un honeypot? ¿Cómo protege contra ciberataques?* Obtenido de https://www.techtarget.com/searchsecurity/definition/honey-pot

Spitzner, L. (2020). *Honeypots: Tracking Hackers, 2nd Edition.* Addison-Wesley.

Sullivan, P. (2024). *Equipo de Respuesta a Emergencias Informáticas (CERT)*. Obtenido de https://www.techtarget.com/whatis/definition/CERT-Computer-Emergency-Readiness-Team

Superintendencia de Economía Popular y Solidaria. (2019). *Normativa sobre la constitución de cooperativas de ahorro y crédito*. Obtenido de https://www.seps.gob.ec

TecnoBits. (2023). Obtenido de ¿Qué es el algoritmo de cifrado MD5?: https://tecnobits.com/que-es-el-algoritmo-de-cifrado-md5/?

Vallejos, D. (2021). Honeypots dinámicos basados en Blockchain. *Investigación, Ciencia y Tecnología en Informática*(8), 65-67. doi:https://ojs.umsa.bo/ojs/index.php/inf_fcpn_pgi/article/view/50

Veselin, P. (2024). *Cómo funcionan los honeypots para atrapar atacantes en redes*. Obtenido de https://veselin.es/como-funcionan-los-honeypots-para-atrapar-atacantes/?utm_source=chatgpt.com

Whitman, M., & Mattord, H. (2018). *Principles of Information Security*. Cengage Learning.

Zambrano, A., Centeno, V., & Cárdenas, L. (2021). *Revista de las Tecnologías de la Informática y las Telecomunicaciones, 5*(2), 1-17. doi:https://doi.org/10.33936/isrtic.v5i2.3708 | ISSN 2550-6730

ANEXOS

Anexo 1: Manual de Políticas de Seguridad de la Información de la Cooperativa 23 de Julio, a Julio del 2024

COOPERATIVA DE AHORRO Y CRÉDITO
"23 DE JULIO" LTDA.

COOPERATIVA FINANCIERA CONTROLADA POR LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

MNL-GSI-03

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

JULIO 2024

TABLA DE CONTENIDO

Anexo 2: Manual de Políticas de Seguridad de la Información de la Cooperativa 23 de Julio, a noviembre del 2024.

COOPERATIVA DE AHORRO Y CRÉDITO
"23 DE JULIO" LTDA.

COOPERATIVA FINANCIERA CONTROLADA POR LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

MNL-GSI-03

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

NOVIEMBRE 2024

TABLA DE CONTENIDO

Anexo 3: Carta de solicitud de autorización de implementación de la Honeypot

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

Acreditada Resolución Nro. 173-SE-33-CACES-2020

MAESTRÍA EN COMPUTACIÓN MENCIÓN SEGURIDAD INFORMÁTICA

Solicitud de Autorización para la Implementación del Proyecto de Tesis: "Honeypot como Herramienta de Prevención y Detección de Ciberataques en las Redes de la Cooperativa de Ahorro y Crédito 23 de Julio"

Quito, 16 de agosto del 2024

Estimada;

Ing. Mónica Nicolalde
Gerente General
Cooperativa de Ahorro y Crédito 23 de Julio Ltda.

Presente. -

Estimada Ingeniera Nicolalde,

Reciba un cordial saludo.

El motivo de la presente es solicitar su autorización para la implementación de mi proyecto de tesis de maestría, requisito previo para la obtención del título de Magíster en Computación con mención en Seguridad Informática por la Universidad Técnica del Norte. El proyecto lleva por título "Honeypot como herramienta de prevención y detección de ciberataques en las redes de datos de la Cooperativa de Ahorro y Crédito 23 de Julio" y tiene como principal objetivo fortalecer la seguridad informática de nuestra institución mediante la implementación de un sistema Honeypot. Esta herramienta permitirá identificar y analizar posibles ciberataques que puedan comprometer nuestras redes.

Para llevar a cabo esta implementación, es necesario adquirir un equipo CPU físico, con un costo estimado de 1.000 dólares. Dicho equipo estará ubicado fuera de la red principal de la cooperativa, pero dentro de nuestro firewall, lo que permitirá monitorear y registrar los diferentes tipos de ataques dirigidos hacia el equipo. Además, los softwares necesarios para la configuración del Honeypot serán

implementados por mi persona, sin incurrir en costos adicionales para la entidad.

El tiempo estimado de implementación será de un mes a partir de la adquisición del equipo.

Los resultados obtenidos a través de este proyecto nos proporcionarán valiosa información sobre las vulnerabilidades presentes, lo que facilitará la creación de políticas de seguridad basadas en los hallazgos registrados.

El objetivo final es contribuir a la mejora continua de la seguridad de nuestras redes y, por ende, a la protección de los datos de nuestros socios y la integridad de nuestros sistemas.

Quedo atento a cualquier consulta o requerimiento adicional y a la espera de su autorización para proceder con la implementación.

Agradezco de antemano su atención y apoyo.

Atentamente,

CESAR ALFONSO ROSERO BALSECA

Firmado digitalmente por CESAR ALFONSO ROSERO BALSECA
Fecha: 2024.08.16 12:45:55 -05'00'

César Alfonso Rosero Balseca
C.I: 1713974812
EURO/2022-14151-1901-1311986

Anexo 4: Encuesta

1.- ¿Cuál es su cargo dentro del área de tecnología o seguridad de la información?

- *Ingeniero de redes*
- *Analista de seguridad*
- *Técnico de soporte*
- *Otro (especifique)*

2.- ¿Cuánto tiempo lleva trabajando en el área de seguridad informática de la cooperativa?

- *Menos de 1 año*
- *1-3 años*
- *3-5 años*
- *Más de 5 años*

Percepción sobre las amenazas y vulnerabilidades

3.- ¿Qué tan frecuentemente ha observado incidentes de seguridad (accesos no autorizados, ataques DDoS, etc.) en la red de la cooperativa?

- *Frecuentemente*
- *Ocasionalmente*
- *Raramente*
- *Nunca*

4.- En su opinión, ¿cuáles son las principales vulnerabilidades de la red interna de la cooperativa?

(Puede seleccionar más de una opción)

- *Puertos abiertos no controlados*
- *Contraseñas débiles*
- *Software desactualizado*
- *Falta de monitoreo constante*
- *Otros (especifique)*

5.- ¿Cree que el equipo actual de seguridad está preparado para enfrentar ciberataques avanzados?

- *Sí, totalmente preparado*
- *Parcialmente preparado*
- *No lo suficiente*
- *No está preparado*

Herramientas y tecnologías de seguridad

6.- ¿Está familiarizado con el concepto y funcionamiento de los Honeypots?

- *Sí*
- *No*

- *Algo*

7.- ¿La cooperativa ha implementado anteriormente herramientas como Honeypots para la detección de ciberataques?

- *Sí*
- *No*
- *No estoy seguro*

8.- ¿Qué otras herramientas de seguridad se utilizan actualmente en la cooperativa para prevenir y detectar ciberataques?

- *Firewalls*
- *Sistemas de detección y prevención de intrusos (IDS/IPS)*
- *Soluciones de antivirus/antimalware*
- *Monitoreo de logs*
- *Otros (especifique)*

9.- ¿Considera que las herramientas de seguridad actuales son suficientes para proteger la red de la cooperativa contra ciberataques?

- *Sí*
- *No*
- *En parte (explique brevemente)*

Implementación y uso de Honeypot

10.- En su opinión, ¿qué beneficios podría traer la implementación de un Honeypot en la red interna de la cooperativa?

- *Detección temprana de ciberataques*
- *Identificación de vulnerabilidades*
- *Mejora en la seguridad general de la red*
- *Generación de datos para análisis de amenazas*
- *Otros (especifique)*

11.- ¿Qué retos cree que se enfrentarían al implementar un Honeypot en la cooperativa?

- *Mantenimiento y monitoreo constante*
- *Riesgo de exposición del sistema*
- *Falta de personal capacitado*
- *Dificultad de integración con otras herramientas*
- *Otros (especifique)*

12.- ¿Estaría dispuesto a capacitarse y participar activamente en el monitoreo y análisis de datos generados por el Honeypot?

- *Sí*
- *No*

- *No estoy seguro*

Capacitación y mejora continua

13.- ¿Cree que es necesario recibir más capacitación en ciberseguridad y uso de herramientas avanzadas como Honeypots?

- *Sí, es esencial*
- *Sí, pero en menor medida*
- *No, el equipo está capacitado*

14.- ¿Considera que las políticas de seguridad de la cooperativa necesitan ser actualizadas o reforzadas?

- *Sí, es urgente*
- *Sí, en algunos aspectos*
- *No, son adecuadas*

15.- ¿Qué sugerencias o recomendaciones tiene para mejorar la seguridad de la red interna de la cooperativa?

(Respuesta abierta)

……

……

……

……..

Gracias por su participación. Sus respuestas serán de gran valor para mejorar la seguridad de la información en la Cooperativa de Ahorro y Crédito 23 de Julio.