Mejorar un modelo de gestión de incidentes de seguridad estándar, mediante el uso de una base de conocimiento de ataques a servicios web en ambientes IoT, construida con tecnologías Honeypot, Big data y bases de datos distribuidas sobre Blockchain, que facilite el manejo de eventos de seguridad informática.

Carlos Andrés Pabón Álvarez

Manuel Flórez Lasprilla

Instituto Tecnológico Metropolitano

Facultad de Ingenierías

Medellín, Colombia

2022

Mejorar un modelo de gestión de incidentes de seguridad estándar, mediante el uso de una base de conocimiento de ataques a servicios web en ambientes IoT, construida con tecnologías Honeypot, Big Data y bases de datos distribuidas sobre Blockchain, que facilite el manejo de eventos de seguridad informática.

Carlos Andrés Pabón Álvarez

Manuel Flórez Lasprilla

Tesis o trabajo de investigación presentada(o) como requisito parcial para optar al título de:

Magister en Seguridad Informática

Director:

Magister Gerley Eliumer Restrepo Ortiz

Línea de Investigación:

Manejo de incidentes de seguridad y análisis forense

Instituto Tecnológico Metropolitano

Facultad de Ingenierías

Medellín, Colombia

2022

"La creatividad es la conexión entre las cosas.
Si le preguntas a una persona creativa cómo
logró hacer algo, verás que se siente frustrada.
Eso se debe a que no lo sabe explicar con exactitud,
simplemente vio algo claro y trabajó en ello".

Steve Jobs

Agradecimientos

Nuestro más sincero agradecimiento al director de esta investigación, Magister. Gerley Eliumer Restrepo Ortiz, por su paciencia, acompañamiento, sus valiosos aportes y todo el conocimiento que nos transfirió, al profesor Magister Héctor Fernando Vargas Montoya por mantenernos motivados y por sus valiosos aportes, a nuestras familias, por su apoyo incondicional y paciencia, y finalmente a Dios, por ser nuestro compañero en las largas horas de trabajo y nuestro consuelo y guía en momentos de confusión.

Resumen

El presente proyecto de investigación propone una mejora a un modelo de gestión de incidentes de seguridad mediante el uso de una base de conocimiento de ataques a servicios web en ambientes IoT, construida con tecnologías Honeypot, Big data y bases de datos distribuidas sobre Blockchain, que facilite el manejo de eventos de seguridad informática; dicha mejora busca lograr una gestión proactiva de los incidentes de seguridad de la información, es decir, la gestión de incidentes de seguridad en ambientes no productivos (ambientes señuelo) que permite utilizar la información recolectada de estos incidentes en dichos ambientes, a fin de definir controles que permiten mitigar su materialización en ambientes productivos. Para lograr el cumplimiento del objetivo del proyecto, fue necesario 1) Seleccionar las herramientas tecnológicas que se implementarían en el laboratorio de pruebas, 2) Instalar y configurar las herramientas tecnológicas seleccionadas, 3) Analizar algunos modelos, guías y buenas prácticas de gestión de incidentes de seguridad, 4) Definir las fases y actividades clave que conforman el nuevo modelo proactivo de incidentes de seguridad, y, 5) validar el funcionamiento del nuevo modelo de gestión de incidentes proactivo propuesto. Como resultado se obtuvo un nuevo modelo de gestión de incidentes de seguridad proactivo, es decir, un modelo que permite gestionar los incidentes de seguridad en ambientes no productivos con el fin de generar una base de conocimiento, que permite definir e implementar controles que mitiguen los incidentes en ambientes productivos, facilitando su gestión.

Palabras clave: Base de datos distribuida, Big Data, Blockchain, eventos de seguridad informática, Honeypot, IoT, modelo de gestión de incidentes de seguridad.

Abstract

This research project proposes an improvement to a security incident management model through the use of a knowledge base of attacks on web services in IoT environments, built with Honeypot technologies, Big data and distributed databases on Blockchain, which facilitate the handling of computer security events; This improvement seeks to achieve a proactive management of information security incidents, that is, the management of security incidents in non-productive environments (decoy environments) that allows the use of the information collected from these incidents in said environments, in order to define controls that allow mitigating its materialization in productive environments. In order to achieve the fulfillment of the project objective, it was necessary to 1) Select the technological tools that would be implemented in the test laboratory, 2) Install and configure the selected technological tools, 3) Analyze some models, guides and good incident management practices 4) Define the key phases and activities that make up the new proactive model for security incidents, and 5) validate the operation of the proposed new proactive incident management model. As a result, a new proactive security incident management model was obtained, that is, a model that allows managing security incidents in non-productive environments in order to generate a knowledge base, which allows defining and implementing controls that mitigate the incidents in productive environments, facilitating their management.

Keywords: Distributed database, Big Data, blockchain, cyber incidents, Honeypot, IoT, security incident management model

Contenido

Lista de figuras

Pag.

Lista de Tablas

Pag.

Glosario de términos

El siguiente Glosario de términos pretende ofrecer una definición corta o breve explicación de los principales conceptos, convenciones y términos que se utilizaron en el desarrollo del presente trabajo de investigación.

B

- **Big data**: Son el conjunto de tecnologías que han sido creadas para recopilar, analizar y gestionar los datos que generan los usuarios de Internet. Su función es recopilar los datos masivos que son generados en "bruto", y procesarlos para identificar patrones u otro tipo de comportamientos que puedan ayudar a sectores concretos.
- **Bitcoin**: Fue la primera moneda digital completamente descentralizada en el mundo.
- **Blockchain**: Es un conjunto de tecnologías que permiten llevar un registro seguro, descentralizado, sincronizado y distribuido de las operaciones digitales, sin necesidad de la intermediación de terceros. Cada uno de los bloques de datos se encuentra protegido y vinculado entre sí, permitiendo la participación de determinados usuarios (cada uno, asociado a un bloque). Así, la transacción no la verifica un tercero, sino la red de nodos (computadores conectados a la red), que también es la que autoriza en consenso cualquier actualización en la Blockchain.
- **Botnet**: Es una red de equipos informáticos que han sido infectados con software malicioso que permite su control remoto, obligándoles a enviar spam, propagar virus o realizar ataques de denegación de servicio distribuido (DDoS) sin el conocimiento o el consentimiento de los propietarios reales de los equipos.

- **Brute Force:** Se traduce como fuerza bruta y hace referencia a un método de resolución de problemas en los campos de la informática, la criptografía y la teoría de juegos. El método de fuerza bruta recibe este nombre porque está basado en probar todas las soluciones posibles o muchas de ellas, siendo conocido también como búsqueda exhaustiva y utilizado, especialmente, cuando no hay otros algoritmos disponibles. Esta técnica es utilizada por hackers para descifrar contraseñas y, de este modo, obtener acceso a datos externos. Para ello se utiliza un software con un algoritmo simple que realiza la sucesión de varias combinaciones de caracteres compuestos por dígitos, espacios y letras hasta una longitud máxima definida.

C

- **Corda**: Es un software de registro distribuido que procesa y registra datos para promover un entorno de red descentralizado. Principalmente Corda está orientada hacia los sectores financieros.
- **Cuórum**: Está diseñado para impedir escenarios de cerebro dividido que pueden producirse cuando hay una partición en la red y los subconjuntos de nodos no se pueden comunicar entre sí.

D

- **Dashboard**: Es una herramienta de gestión de la información que monitoriza, analiza y muestra de manera visual los indicadores clave de desempeño (KPI), métricas y datos fundamentales para hacer un seguimiento del estado de una empresa, un departamento, una campaña o un proceso específico.

- **DHCP**: Protocolo de Configuración Dinámica de Host) es un método para asignar direcciones IP en forma automática a clientes de red.
- **Docker**: Es una plataforma de software de código abierto para crear, implementar y administrar contenedores de aplicaciones virtualizados en un sistema operativo (SO) común, con un ecosistema de herramientas aliadas.

E

- **ElasticSearch**: Es un motor de búsqueda que se basa en Lucene, el cual nos permite realizar rastreo por una gran cantidad de datos de un texto específico. Está escrito en Java y se basa sobre una licencia Apache.
- **ELK**: Es la sigla para tres proyectos open source: Elasticsearch, Logstash y Kibana. Elasticsearch es un motor de búsqueda y analítica**,** Kibana permite a los usuarios visualizar los datos en cuadros y gráficos con Elasticsearch.
- **Ethereum**: Es una plataforma open source, que sirve para programar contratos inteligentes. La plataforma es descentralizada a diferencia de otras cadenas de bloques. Es programable, lo que significa que los desarrolladores pueden usarlo para crear nuevos tipos de aplicaciones descentralizadas.

F

- **Firmware**: Es un conjunto de instrucciones de un programa informático que se encuentra registrado en una memoria ROM, flash o similar. Estas instrucciones fijan la lógica primaria que ejerce el control de los circuitos de alguna clase de artefacto.

H

- **Hyperledger Fabric**: Es un proyecto de código abierto de Linux Foundation, es la infraestructura modular de Blockchain y el estándar de facto para plataformas Blockchain empresariales. Diseñada como base para desarrollar aplicaciones de nivel empresarial y soluciones sectoriales, la arquitectura modular y abierta utiliza componentes plug-and-play para acomodar una amplia gama de casos de uso.
- **Honeypot**: Este es un sistema trampa o señuelo, dispuesto en una red o sistema informático para ser un objetivo tentador para atacantes.

I

- **ICMP**: Internet Control Message Protocol, es un protocolo que permite administrar información relacionada con errores de los equipos en red.
- **IDS**: Intrusion Detection System o sistema de detección de intrusiones, es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red, es decir, son sistemas que monitorizan el tráfico entrante y lo cotejan con una base de datos actualizada de firmas de ataque conocidas. Ante cualquier actividad sospechosa, emiten una alerta a los administradores del sistema Estos sistemas sólo detectan los accesos sospechosos emitiendo alertas anticipatorias de posibles intrusiones, pero no tratan de mitigar la intrusión.
- **IoT**: Internet of things o internet de las cosas, es un concepto que se refiere a la interconexión digital de objetos cotidianos con internet.

K

- **Kali Linux:** Es una distribución de Linux muy utilizada para llevar a cabo auditorías de seguridad informática y poner a prueba los equipos. Cuenta con una gran cantidad de herramientas instaladas.
- **Kernel**: Núcleo o parte esencial de un sistema operativo. Provee los servicios básicos del resto del sistema.
- **KVM**: Kernel Virtual Machine, es una tecnología de virtualización open source integrada a Linux®. (KVM puede convertir a Linux en un hipervisor que permite que una máquina host ejecute varios entornos virtuales aislados llamados máquinas virtuales.

M

- **Malware**: Es un software que interfiere con el propósito de dañar al usuario del ordenador. El objetivo es robar datos personales, financieros y/o comerciales.
- **Merkle**: Es un árbol de decisión estadístico compuesto por hashes. Se utiliza por motivos de seguridad, verificación y como forma de comprensión de datos.

N

- **Nmap**: Network Mapper, es un software gratuito y de código abierto que funciona principalmente para efectuar rastreo de puertos, descubrimiento de la red y auditorías de seguridad

O

- **Sistema Operativo:** Es el conjunto de programas responsables de la conexión entre los recursos materiales de un ordenador y las aplicaciones informáticas del usuario.

- **Open Source:** Es un código diseñado de manera que sea accesible al público: todos pueden ver, modificar y distribuir el código de la forma que consideren conveniente.

P

- **PFSense**: Es una distribución personalizada de FreeBSD adaptado para su uso como Firewall y Enrutador. Se caracteriza por ser de código abierto, cuenta con una interfaz web para su configuración y administración.
- **Proxmox Virtual Environment, o Proxmox VE:** Es un entorno de virtualización de servidores de código abierto, GNU/Linux basado en Debían.
- **Proxy**: Es una tecnología que se utiliza como puente entre el origen (un ordenador) y el destino de una solicitud (Internet). Generalmente se trata de un dispositivo u ordenador intermedio que nos permite conectarnos a Internet de manera indirecta.

R

- **Ralentizar:** Es la acción que permite lograr que algo se vuelva más lento o se desarrolle con menor rapidez. Esto quiere decir que la ralentización consiste en reducir la velocidad o en dotar de lentitud a cierto procedimiento.
- **Root**: Es un framework para el desarrollo de aplicaciones de análisis de datos científicos a gran escala desarrollado por el CERN, orientado a objetos.
- **Rsync**: Sistema de respaldo o copia de archivos. es una aplicación libre para sistemas de tipo Unix y Microsoft Windows que ofrece transmisión eficiente de datos incrementales, que opera también con datos comprimidos y cifrados.

S

- **SIEM**: (Security Information and Event Management) viene de la conjunción de dos términos que algunos usan indistintamente y otros procuran separar: SIM (Security Information Management) y SEM (Security Event Management), ambos para referirse al análisis en tiempo real de alertas de seguridad generadas en la red o en aplicaciones.
- **SOAP**: Protocolo Simple de Acceso a Objetos, el cual es un protocolo basado en XML, que permite la interacción entre varios dispositivos y que tiene la capacidad de transmitir información compleja.
- **Sockets**: designa un concepto abstracto por el cual dos procesos (posiblemente situados en computadoras distintas) pueden intercambiar cualquier flujo de datos, generalmente de manera fiable y ordenada. Además, es una estructura de datos que permite que dos máquinas se comuniquen entre ellas.
- **SSH**: (Secure Shell) es un protocolo de comunicación segura y que además da nombre al propio programa que usa, en el que podemos conectar de forma remota con servidores que estén configurados para este tipo de conexión. La conexión SSH está cifrada de extremo a extremo además de necesitar una autenticación para poder conectar al servidor.
- **Syslog**: Se trata de un protocolo estándar utilizado para enviar mensajes de registro o eventos del sistema a un servidor específico, llamado servidor de syslog. se utiliza principalmente para recopilar varios registros de dispositivos de diversas máquinas diferentes en una ubicación central para la supervisión y su análisis.
- **Snort**: Es un software gratuito de código abierto. También se puede utilizar como rastreador de paquetes para monitorizar el sistema en tiempo real. El administrador de la

red puede usarlo para observar todos los paquetes entrantes y encontrar los que son peligrosos para el sistema.

T

- **Tomcat**: es un contenedor de servlets que se puede usar para compilar y ejecutar aplicaciones web realizadas en Java. Implementa y da soporte tanto a servlets como a páginas JSP (Java Server Pages) o Java Sockets.
- **T-Pot:** Es una plataforma de HoneyPots que tiene como base una distribución. Esta plataforma incluye una gran variedad de HoneyPots ya preparados, configurados y listos para entrar en funcionamiento.
- **Tshark**: Es un analizador de tráfico de red de línea de comando que permite capturar datos de paquetes desde una red activa o paquetes de lectura de un archivo de capturas guardado anteriormente, mediante la impresión de un formulario decodificado de dichos paquetes a la salida estándar o mediante la escritura de los paquetes en un archivo.

W

- **WSDL**: (Web Services Description Language) es una especificación estándar para describir servicios basados en XML de red.

X

- **XML**: (Extensible Markup Language) es un lenguaje de marcado que define un conjunto de reglas para la codificación de documentos.

Introducción

La transformación digital puede ser definida como la integración de tecnologías de información en todas las áreas y aspectos de una organización con el objetivo de optimizar sus procesos, mejorar su competitividad y entregar valor añadido a sus clientes desde el punto de vista de la competitividad. La integración de nuevas tecnologías se ha convertido en una obligación para las empresas que desean continuar estando vigentes, lo que ha hecho que sin importar su objeto social, su ubicación o su tamaño, la gran mayoría le está apuntando a convertirse en empresas de base tecnológica. Es precisamente esa integración de nuevas tecnologías, la búsqueda por implementar y ofrecer a sus clientes servicios digitales, sumada a la cada vez mayor interconexión de dispositivos inteligentes, lo que cada día amplía la probabilidad de que los ciberdelincuentes busquen aprovechar las brechas de seguridad existentes en los servicios digitales que las empresas exponen para vulnerarlos.

La búsqueda por desarrollar y exponer servicios tecnológicos en el menor tiempo posible como una estrategia para mantenerse a la vanguardia del mercado y captar nuevos clientes, está causando que se integren a los ecosistemas digitales de las organizaciones, componentes a los cuales no se les hacen las pruebas de seguridad necesarias para identificar sus vulnerabilidades y los ataques que pueden llegar a recibir mientras están expuestos a la red; adicionalmente se debe tener en cuenta que la interconectividad a la cual se está llegando actualmente hace que, al tener vulnerabilidades no identificadas en un activo, aumente la probabilidad de que un ataque tenga éxito y se ponga en riesgo el todo el ecosistema digital de una organización; en ese sentido, identificar las técnicas, vulnerabilidades y vectores de

ataque utilizados por los ciber delincuentes, es fundamental en la definición de controles que mitiguen el riesgo de materialización de los incidentes.

Una vez en una organización se presentan eventos e incidentes de seguridad, es muy importante contar con mecanismos que permitan mitigar el riesgo de seguridad informática, proporcionando pautas y prácticas para el establecimiento de capacidades al interior de las organizaciones, mediante la generación de planes, políticas y procedimientos que permitan manejar de manera eficiente los incidentes de seguridad de la información una vez estos han sido detectados. La definición proactiva de controles de seguridad no está totalmente contemplada en la mayoría de los modelos de gestión de incidentes de seguridad, pues estos se enfocan en la gestión de los eventos e incidentes una vez estos se han materializado. Contar con mecanismos que permitan anticiparse a los atacantes es fundamental en la protección del ecosistema digital de las organizaciones, en ese sentido, el uso de Honeypots que emulen los diferentes servicios o tecnologías que las organizaciones exponen, permite identificar el comportamiento de los atacantes y sus técnicas, los vectores utilizados y las vulnerabilidades explotadas [1], lo cual facilita la definición de controles que mitiguen la explotación de dichas vulnerabilidades.

Este trabajo se enmarca en el siguiente objetivo general:

Diseñar una mejora a un modelo de gestión de incidentes de seguridad estándar, mediante el uso de una base de conocimiento de ataques a servicios web en ambientes IoT, construida con tecnologías Honeypot, Big data y bases de datos distribuidas sobre Blockchain, que facilite el manejo de eventos de seguridad informática.

Para lograr este objetivo, se plantearon los siguientes objetivos específicos:

- Seleccionar una Honeypot que cubra servicios Web en IoT, permitiendo replicar la explotación de vulnerabilidades a través de diferentes ciberataques.
- Seleccionar una estructura para representar los datos de un evento de seguridad detectado por una Honeypot adecuada para almacenar en Blockchain.
- Seleccionar la herramienta Big Data de código abierto con la capacidad integrarse a la cadena de bloques seleccionada.
- Definir una estrategia para fortalecer un plan de respuesta a un incidente de seguridad alimentado por el conjunto de ataques almacenados en la base de datos de conocimiento.
- Evaluar el modelo integrado y el manejo de incidentes de seguridad, usando un sistema para atacar los servicios informáticos.

El presente proyecto de investigación tiene como **alcance** diseñar una mejora a un modelo de gestión de incidentes de seguridad proactivo utilizando herramientas tecnológicas que permiten exponer, analizar y almacenar de forma segura la información de los ataques recibidos por los activos expuestos y con ella definir e implementar controles que faciliten la mitigación de los incidentes en los ambientes productivos.

Las limitaciones del presente proyecto están dadas por el hecho de que el modelo de gestión de incidentes propuesto debe ser utilizado junto con herramientas tecnológicas que permitan exponer activos para que reciban ataques y se pueda capturar la información con la cual se definen los controles a implementar; sin embargo, las herramientas seleccionadas no son obligatorias y cada organización debe seleccionar la tecnología y herramientas a utilizar.

El presente trabajo está compuesto por los siguientes capítulos:

- Marco Teórico
- Estado del arte
- Metodología utilizada para el cumplimiento de los objetivos.
- Resultados obtenidos en la ejecución de los objetivos.
- Conclusiones y recomendaciones

1. Marco Teórico y Estado del arte

En este capítulo, se hará una breve exposición de los principales conceptos, normatividad, teorías, enfoques, metodologías, antecedentes e investigaciones previas, entre otros aspectos relacionados con el objeto del presente Trabajo de Grado, y que además de sustentarlo, le permitan al lector avanzar con claridad a través de su lectura y tener una mejor comprensión de los objetivos trazados, la metodología utilizada para su logro, el enfoque dado y las soluciones planteadas.

1.1. Marco Teórico

1.1.1. Internet de las Cosas

La búsqueda constante de hacer que los objetos de uso cotidiano sean cada vez más dinámicos y presten servicios que mejoren procesos y faciliten la vida cotidiana, ha llevado al nacimiento y evolución de objetos que interactúan entre sí, sin necesidad que los seres humanos intervengan; esta interacción es posible gracias a las posibilidades prácticamente infinitas que brinda la Internet.

Hace algunas décadas la conexión entre dispositivos solo era posible en ambientes cerrados; esto era debido a que tecnologías como la Internet, las conexiones inalámbricas, la Inteligencia Artificial (IA) o el Big Data entre otros, no existían o eran incipientes. Actualmente todas estas tecnologías han tenido un gran desarrollo y su uso se ha convertido en algo cotidiano; permitiendo la creación de redes de dispositivos físicos que se conectan entre sí y comparten información a través de la red. [2] La conexión e interacción de todos

estos dispositivos físicos es lo que hoy se conoce como Internet de las Cosas (IoT); y los dispositivos que se conectan, se conocen como dispositivos IoT.

1.1.2. Dispositivos IoT

El ingeniero informático Kevin Ashton es considerado la persona que acuño el termino internet de las cosas (IoT) [3]. Hace más de veinte años el ingeniero Ashton necesitaba ponerle un nombre para una presentación hecha en PowerPoint que había preparado para un grupo de ejecutivos de la empresa P&G; con la presentación Ashton quería lograr que se agregaran etiquetas de identificación de radiofrecuencia en diferentes productos, el nombre que finalmente utilizo para su presentación fue "*Internet de las cosas*". Años después Ashton llego a trabajar en el MIT (Massachusetts Institute of Technology) donde cofundo y dirigió Auto-ID Center, el laboratorio de investigación que ayudó a construir la base del Internet de las cosas.

Un dispositivo IoT es un artefacto electrónico común al cual se le ha agregado tecnología tal como conexión a internet, protocolos de comunicación, sensores y software, con el fin de convertirlo en un objeto inteligente capaz de recolectar información de su entorno circundante, analizarla y transmitirla a otros dispositivos sin que en todo el proceso sea necesaria la intervención humana [4].

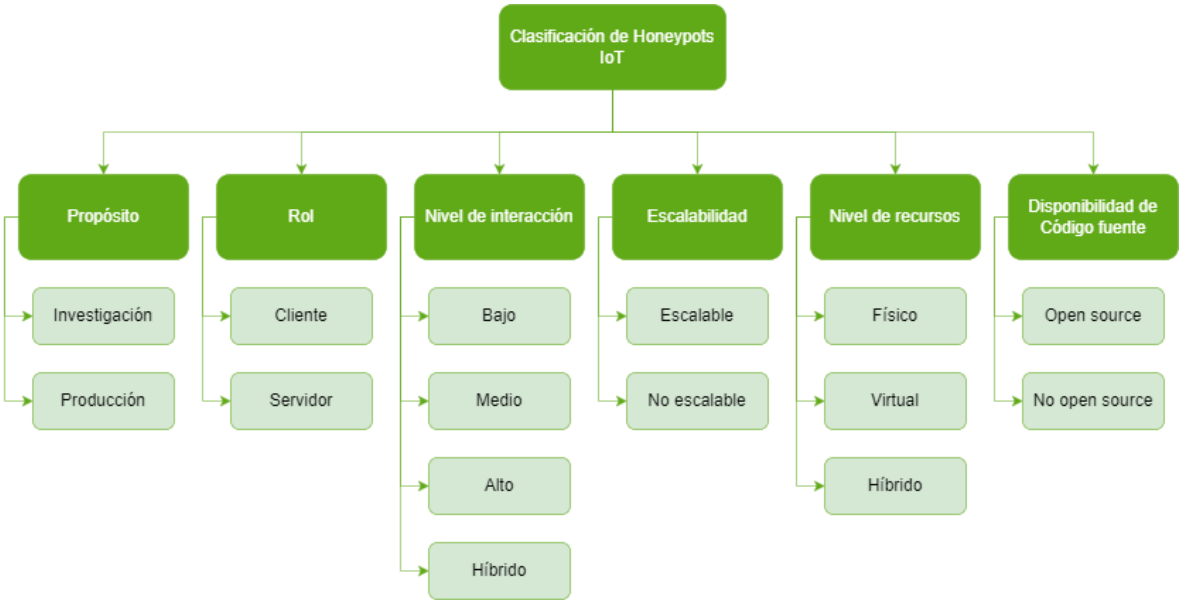
Los dispositivos IoT han sido adoptados en prácticamente todos los sectores de la economía y la vida cotidiana, su adopción ha introducido notables mejoras en la calidad de vida de sus usuarios y en los procesos productivos en los que se les ha integrado. Es una de las tecnologías con mayor crecimiento y adopción en la historia de la computación, con un

estimado de 50 billones de dispositivos para finales del año 2020 [2]. Los dispositivos IoT tendrán en los próximos años un papel fundamental en sectores tan importantes como la agricultura, la medicina, la educación, el desarrollo de ciudades inteligentes y el transporte. El acelerado crecimiento que ha tenido la tecnología IoT desde su aparición, ha introducido nuevos desafíos en materia de seguridad. En los últimos años, mediante el uso de botnets compuestas por miles de dispositivos IoT infectados con software malicioso, se han ejecutado ataques a la infraestructura tecnológica de diferentes organizaciones a nivel mundial, generando pérdidas millonarias. Si bien la mayoría de los dispositivos IoT cuentan con capacidades de procesamiento y almacenamiento limitados, al ser integrados en una Botnet como Mirai, pueden generar incidentes graves de seguridad en el ecosistema digital. Dada la importancia de IoT, es necesario implementar nuevas medidas y modelos de seguridad que permitan reducir los riesgos de ataques a gran escala usando estos dispositivos. El reto es que a medida que se implementan nuevas medidas, los atacantes buscan nuevas formas de vulnerar la seguridad y en consecuencia siempre se puede esperar que los nuevos ataques, sean más sofisticados y destructivos [4]. Entender los vectores de ataque utilizados por los ciber delincuentes para vulnerar la seguridad de IoT permite mantener actualizados los métodos y mecanismos de defensa y activar los modelos de gestión de incidentes necesarios para reducir el riesgo de eventos adversos e incidentes de seguridad.

1.1.3. Honeypot

Una Honeypot es un sistema informático diseñado para atraer atacantes, haciéndoles creer que lograron obtener acceso a sistemas productivos reales. Pueden implementarse integrándolos con otros controles de seguridad como firewalls e IDS, obteniendo así un IPS que ayuda a capturar información sobre los atacantes y los métodos que estos utilizan para lograr acceso a los sistemas, lo cual permite definir e implementar controles, mejorando la seguridad de los sistemas y así evitar que los ataques futuros sean exitosos [5]. Las Honeypot permiten entre otras cosas, mantener la interacción con los atacantes, registrar información sobre los métodos y técnicas utilizadas para vulnerar el sistema, ralentizar el avance del ataque, alejar los atacantes de los sistemas reales e implementar controles en los sistemas reales de forma proactiva [6]. Los criterios de clasificación de las Honeypot pueden ser muy variados; para el propósito específico del presente trabajo de investigación, se utilizarán los criterios definidos en el trabajo [5], en el cual clasificaron las Honeypots de acuerdo con su propósito, rol, nivel de interacción, escalabilidad, nivel de recursos, disponibilidad del código fuente y su aplicación:

Ilustración 1. Clasificación Honeypots IoT



Fuente: [7]

1.1.3.1. Clasificación por propósito:

En este criterio se encuentran las Honeypots de investigación y Honeypots productivas; las de investigación se implementan con el propósito de recopilar información sobre los atacantes y los métodos que estos utilizaron para acceder a los sistemas informáticos, esto se hace generalmente con el fin de definir e implementar controles que protejan dichos sistemas de ataques futuros; en contraste, los Honeypots productivos, se implementan con el fin de proteger de accesos no autorizados los sistemas productivos de las organizaciones que los implementan [5].

1.1.3.2. Clasificación por rol

En esta categoría se encuentran las Honeypots clientes y servidor; las Honeypots cliente son aquellas que detectan activamente los ataques, son más complejas de detectar por parte de los atacantes y más efectivas en la recolección de información de los atacantes y sus métodos; las Honeypots servidor, esperan de manera pasiva a que ocurran los ataques [5].

1.1.3.3. Clasificación por nivel de interacción

La interacción, se refiere a lo que le permite o no la Honeypot al atacante; en esta categoría se encuentran las Honeypots de interacción baja, media, alta e hibrida:

- **Baja interacción:** Trabajan únicamente emulando servicios y sistemas operativos, es decir que las aplicaciones y servicios que simula no son completamente funcionales. Son de fácil puesta en funcionamiento y mantenimiento, su riesgo es prácticamente nulo. Son fácilmente identificadas por el atacante y normalmente son blanco de ataques automatizados, por lo que la información que registran es bastante limitada [8].
- **Media Interacción:** Tienen una mayor capacidad de comunicación con el atacante que los de interacción baja, tienen menos funcionalidades que los de interacción alta [6], están desplegados en sistemas operativos emulados con un nivel de despliegue parcial, su nivel de riesgo es medio. La cantidad de información que puede ser recolectada depende directamente de la habilidad del atacante.
- **Alta interacción:** Son normalmente aplicaciones reales corriendo en sistemas reales, la información que se puede obtener de los atacantes es mucho mayor que los de baja interacción. Como desventaja, los atacantes podrían utilizar el Honeypot como punto de

entrada al resto de sistemas y, por lo tanto, requieren de una configuración de seguridad adicional para evitar que ningún sistema se pueda ver comprometido [8].

- **Interacción Hibrida:** Son aquellas que presentan una combinación de los diferentes niveles de interacción; generalmente se encuentran diferentes niveles de interacción cuando se tiene una Honeynet, es decir, una red de Honeypots [5].

1.1.3.4. Clasificación por escalabilidad

En esta categoría se encuentran las Honeypots escalables y no escalables; la escalabilidad indica la capacidad que tiene una Honeypot de aumentar la cantidad de señuelos que se le puede añadir, cuando se habla de una Honeypot con muchos señuelos, se está hablando de una red de Honeypots, es decir, de una Honeynet. A mayor cantidad de Honeypots implementadas en la red, mayor será la capacidad de detección, recopilación de información y seguridad. La escalabilidad de una Honeypot depende de si sus recursos son físicos y del nivel de interacción; las Honeypots cuyos recursos son físicos y son de alta interacción son menos escalables que aquellas que son virtuales y de baja interacción [5].

1.1.3.5. Clasificación por niveles de recursos

En esta categoría se encuentran las Honeypots que son desplegadas y ejecutadas en máquinas físicas, virtuales e hibridas; el despliegue de Honeypots en máquinas físicas es más costoso que aquellas que se despliegan en máquinas virtuales, son de alta interacción y por lo tanto su capacidad de captura de información es mejor que las desplegadas en máquinas virtuales; por su parte, las Honeypots desplegadas y ejecutadas en una combinación de máquinas físicas y virtuales logran un mejor equilibrio en costos de implementación y captura de información [5].

1.1.3.6. Clasificación por disponibilidad de código fuente

En esta categoría se encuentran las Honeypots cuyo código fuente es abierto, es decir, que sus creadores ponen a disposición el código fuente de la Honeypot, esto permite que otras personas puedan hacer mejoras y personalizaciones en la Honeypot; caso contrario ocurre con las Honeypots cuyo código fuente es creado, mantenido y actualizado por una organización o grupo cerrado de personas. Las Honeypots de código abierto son más económicas en su implementación y generalmente al tener una comunidad abierta de desarrolladores, tienen mejor documentación, lo que al final se traduce en fácil mantenibilidad y mejoras continuas [5].

1.1.4. Big Data

A medida que la humanidad incrementaba la cantidad de datos que podía generar cada día, la necesidad de ejecutar análisis de los datos para obtener información valiosa que pudiera ser utilizada en la toma de decisiones y en la aplicación de mejoras en procesos y modelos popularizó el termino Big Data.

No existe una definición universal para el término Big Data. De acuerdo con estudio realizado por Favaretto, de Clercq y otros [9] en el cual entrevistaron 39 investigadores norteamericanos y suizos, no fue posible encontrar una definición univoca de Big Data entre los entrevistados, incluso muchos de ellos admitieron incertidumbre en el momento de entregar una definición. De acuerdo con el estudio, algunos de los participantes dieron una definición de Big Data basados en la definición tradicional de las Vs, sin embargo, no se

pusieron de acuerdo en la cantidad de Vs, mientras que otros investigadores dieron una definición basada en la recopilación y procesamiento de datos.

Para el objetivo del presente trabajo de investigación se adoptará la definición de Big Data mencionada por [10], la cual indica que Big Data son volúmenes de datos a gran escala que sobrepasa las capacidades y métodos analíticos y de gestión de datos convencionales utilizados generalmente para capturar, almacenar, acceder, gestionar, compartir, procesar, analizar y visualizar la información en un periodo de tiempo aceptable; dicha definición se encuentra basada en la dada por Doug Laney, quien caracterizo Big Data en termino de tres Vs y definió Big Data como una circunstancia en la que el volumen, la velocidad y la variedad de datos almacenados por una organización van más allá de la capacidad de cálculo para una toma de decisiones precisa y oportuna [11].

1.1.4.1. Las Vs de Big Data

- **Volumen**: El volumen hace referencia a la cantidad de datos que se generan y recopilan en una organización, es decir, si un conjunto de datos se considera o no Big Data. Respecto al tamaño necesario para que un conjunto de datos sea considerado Big Data no existe en la actualidad un consenso y es algo que cambia constantemente [12].
- **Variedad**: La variedad hace referencia a los diferentes tipos de datos que la organización genera y recopila; estos pueden estar representados por datos estructurados, semiestructurados y no estructurados, es decir, que dentro de los datos se pueden encontrar videos, textos, imágenes, logs de aplicaciones, comentarios de redes sociales, entre otros [12].

- **Velocidad**: Esta hace referencia a la velocidad con la que una organización genera y recopila datos, es decir la generación de grandes volúmenes de datos en espacios cortos de tiempo [12].

A medida que las investigaciones respecto a Big Data han aumentado, se han agregado Vs a la definición original de Laney, algunas de estas corresponden a valor, variabilidad, visualización, entre otras [10].

- **Veracidad**: La veracidad hace referencia a la calidad que tienes los datos generados y recopilados; la veracidad es de gran importancia, pues teniendo en cuenta que los datos pueden provenir de fuentes diversas, estos pueden ser de baja calidad, lo que al final se traduce en generación de información poco importante o que no es verídica [12].
- **Valor**: El valor hace referencia a la capacidad para limpiar y analizar grandes volúmenes de datos, para extraer información que genere conocimiento a través del cual se generan acciones o decisiones. La recopilación de grandes volúmenes de datos no genera valor hasta que se limpia y analiza para obtener algo útil, lo cual puede ser uno de los retos más grandes de Big Data, pues los costos asociados al almacenamiento y análisis son altos y se corre el riesgo de no lograr obtener datos útiles [12].
- **Visualización**: La visualización hace referencia a la forma como se muestra la información obtenida del análisis de grandes volúmenes de datos; al utilizar elementos visuales como cuadros, gráficos, mapas y otros, se proporciona una manera accesible de ver y comprender tendencias, valores atípicos y patrones en los datos [12].

1.1.4.2. Los retos de Big data

- **Datos multi estructurados:** La enorme cantidad de fuentes generadoras de datos hace que cada día sea más complejo almacenar y procesar los datos para obtener información valiosa o relevante, las fuentes generadoras crecen día y a día y cada una crea datos en formatos diversos; debido a esto, las organizaciones caen en el dilema de la aguja en el pajar, pues requieren analizar información durante semanas o meses, a un coste extremadamente alto para generar un dato importante, lo cual hace insostenible el proceso pues no se cuenta ni con el dinero ni el tiempo, y más teniendo en cuenta que mientras se hace el análisis, se están generando volúmenes enormes de datos[12].
- **Seguridad de los datos e información**: la privacidad y la protección de los datos y la información es otro de los grandes desafíos que enfrenta el Big Data; La exposición de la información por parte de Hackers supone pérdida de credibilidad y confianza hacia las organizaciones, además de la enorme preocupación por saber con precisión qué información han conseguido los ciberdelincuentes durante sus ataques; las organizaciones deben invertir en la seguridad en función de lo valiosos, sensibles o críticos que sean los datos que recopilan; proteger la información pasa por implementar estrategias para proteger la confidencialidad, integridad y disponibilidad de dicha información [12].

1.1.5. Blockchain

Blockchain se hizo público en el año 2008, cuando Satoshi Nakamoto presentó su documento “Bitcoin”; hasta le fecha se desconoce si el nombre hace referencia a una persona

o a un grupo de personas. En esencia, Blockchain puede ser definido como un libro mayor descentralizado en el cual se registran transacciones de forma sincronizada; en esencia, un libro mayor descentralizado o distribuido puede definirse como una tecnología que permite registrar, compartir y sincronizar las transacciones que son realizadas desde múltiples ubicaciones y por múltiples usuarios [13]. En la actualidad Blockchain es conocido por ser una plataforma de almacenamiento distribuido, utilizado para la administración de criptomonedas; sin embargo, es posible utilizar Blockchain para almacenar otro tipo de información de forma totalmente segura. En Blockchain, la información se almacena en bloques que están compuestos por una cabeza o block head y un cuerpo o block body. En la cabeza se almacenan datos como la marca de tiempo, la cual indica el tiempo de escritura en el bloque, el hash del bloque anterior, el nonce, el cual es un número aleatorio que evita que los hashes antiguos no puedan volver a ser utilizados, y el merkle root, el cual es un hash especial, que facilita la verificación de los datos en el bloque.

La primera aplicación que se le dio a la tecnología Blockchain fueron las criptomonedas, la más conocida es Bitcoin, aunque existen muchas otras que han seguido sus pasos, entre ellas se destaca Ethereum, la cual no solo adopto su tecnología, sino que con el fin de convertirla en una plataforma de aplicaciones distribuidas le agregaron contratos inteligentes o smart contracts; estos pueden definirse como un fragmento de código inmodificable que tiene la capacidad de ejecutarse automáticamente sin necesidad que un humano intervenga; esta autonomía proviene del hecho que las Blockchain deben operar sin una entidad centralizada. Tanto Bitcoin como Ethereum hacen parte de lo que se conoce como Blockchain publica sin

permiso, eso quiere decir que cualquier persona puede entrar y utilizarlas sin necesidad de identificarse de ninguna manera, lo cual las hace totalmente anónimas [14].

La gran popularidad que con el tiempo han alcanzado las criptomonedas ha hecho que crezca el interés por aplicar la tecnología subyacente de la cadena de bloques, el libro mayor distribuido y la plataforma de aplicaciones distribuidas a casos de uso empresarial más innovadores; sin embargo, en la mayoría de los casos, dichas aplicaciones empresariales requieren que las Blockchain cuenten con características adicionales de las que originalmente poseen; un ejemplo de ello es el sistema financiero, donde la identificación de los participantes o el alto rendimiento a nivel transaccional, la baja latencia en la confirmación de las transacciones, entre otras, es absolutamente necesaria y algo que utilizando las Blockchain Bitcoin o Ethereum, por citar solo algunos casos, no es posible tener [14]. Las Blockchain pueden ser categorizadas en públicas, privadas y mixtas o federadas, cada una de ellas cuenta con capacidades y características que se adaptan a diferentes necesidades.

Las Blockchain públicas son totalmente abiertas al público; esto quiere decir que cualquier persona puede hacer parte de la misma, estas cuentan con controles de seguridad que garantizan que su funcionamiento no puede ser alterado de forma maliciosa; su funcionamiento es totalmente descentralizado, esto quiere decir que no existe una entidad que regule su funcionamiento, el cual depende en gran medida del número de participantes, por lo cual se motiva su uso mediante un sistema de incentivos; como ejemplo de Blockchain públicas, podemos citar entre otras, a Bitcoin y Ethereum.

Las Blockchain privadas por su parte, cuentan con una entidad centralizada que regula su funcionamiento y define quienes pueden ingresar a la red y que permisos tendrá cada persona dentro de la misma; generalmente este tipo de Blockchain tiene fines corporativos, por lo que los costos de funcionamiento dependen de la entidad central que la controla; como ejemplos de este tipo de Blockchain tenemos Hyperledger, Corda y Quorum.

Finalmente están las Blockchain mixtas o híbridas, este tipo congrega lo mejor de las Blockchain públicas y privadas, generalmente este tipo es controlado por una o varias entidades que regulan el funcionamiento y definen quienes pueden participar, sin embargo, el acceso a la información contenida en la Blockchain es pública. Algunos ejemplos de Blockchain híbridas son BigchainDB y Evernym, una Blockchain que quiere facilitar la gestión de la identidad digital soberana.

1.1.5.1. Características principales de Blockchain

- **Inmutabilidad**: La inmutabilidad se refiere a la imposibilidad de modificar la información almacenada en la Blockchain, esto quiere decir, que es prácticamente imposible de modificarla, debido a que la infraestructura de la Blockchain está compuesta por una colección de nodos, en la cual cada uno contiene una copia del libro mayor digital, en la cual para que la información sea modificada es necesario que a cada transacción sea verificada, es decir, las transacciones solo son registradas en el libro mayor, una vez se alcance el consenso entre todos los nodos, respecto a la autenticidad de la transacción .
- **Seguridad**: La seguridad de la Blockchain está muy relacionada con la inmutabilidad, pues se refiere a la imposibilidad de modificar la información contenida en ella mediante

ataques a sus nodos; esto se debe a que se emplea criptografía con algoritmos asimétricos complejos para cifrar la información y el uso de hash para identificar cada nodo y la información que este contiene, lo cual implica que para corromper la red, es necesario intervenir cada uno de los nodos que la componen, tarea prácticamente imposible.

- **Descentralización**: La Blockchain por su naturaleza e infraestructura no es gobernada por una autoridad que pueda manipular la información almacenada en ella, en otras palabras, la red no reside en un solo servidor, sino en colecciones de nodos.
- **Consenso**: El consenso hace referencia a la verificación que la Blockchain hace de cada una de las transacciones, donde cada nodo dentro de la red debe validar la autenticidad de la transacción, antes de registrarla en el libro mayor.

1.1.6. Base de conocimiento

Una base de conocimiento puede ser definida como una colección de datos organizados que pueden ser utilizados por todos los miembros de una organización para la toma de decisiones; la generación de una base de conocimientos requiere que se lleve a cabo la recopilación, procesamiento, almacenamiento y explotación de la información que se genera al interior de la organización, con el fin de elevar y fortalecer aspectos como la productividad, innovación, incremento de las competencias de los trabajadores y un mejor aprovechamiento del conocimiento existente y su aplicación en todos los procesos organizacionales [15].

1.1.7. Servicios Web

Es un componente software que es distribuido a través de una red como intranet o internet, y funciona en un servidor Web como uno de los recursos disponibles, para lo cual es accedido a través de una página u otro servicio Web. Los servicios Web son desarrollados con lenguajes de programación tales como Java, PHP, entre otros, usando protocolos como SOAP y WSDL [16].

1.1.8. Servidor Web

Conjunto de hardware y/o softwares capaces de almacenar y administrar recursos y servicios Web (estilos, archivos, URL, control de acceso, publicadores, etc.), entregando dichos recursos y accesos a aplicaciones Web o usuarios finales que los consume. Algunos servidores Web son FilleZilla, IIS, Apache, Jboss, entre otros. El servidor Web puede contener, sin limitarse al hardware (CPU, memoria, red), al sistema de almacenamiento, componentes de procesamiento y las aplicaciones o publicadores que se instalen para la administración de los recursos Web [17].

1.1.9. Raspberry Pi

Una Raspberry Pi, es una computadora de tamaño pequeño y bajo costo. Fue desarrollada por la fundación Raspberry Pi, organización benéfica cuya sede principal se encuentra localizada en el Reino Unido. Su desarrollo se llevó a cabo bajo el concepto de que por su pequeño tamaño y bajo costo podría ser utilizada para enseñar informática básica; en ella los estudiantes podrían cargar sistemas operativos sencillos, conectar periféricos como ratón

y teclado o agregar almacenamiento adicional, todo ello con el objetivo de poder diseñar, desarrollar y ejecutar aplicaciones informáticas livianas sobre ella. Desde su aparición en el año 2006 la Raspberry Pi ha causado gran impacto en la comunidad académica, esto gracias a sus múltiples usos y su excelente relación costo – beneficio, si se le compara con dispositivos similares en el mercado [18].

Los dos primeros modelos de la Raspberry Pi fueron el modelo A y el modelo B, ambos fabricados en el Reino Unido. Sus primeras ventas al público se dieron a partir del 29 de febrero de año 2012. Los modelos posteriores fueron ensamblados en China; esto se hizo con el único objetivo de disminuir los costos de producción de forma tal que pudieran destinar más recursos a investigación y desarrollo. En diciembre del año 2015 se lanza la Raspberry Pi 2 y poco tiempo después fue lanzada la Raspberry Pi 3; el último modelo, la Raspberry Pi 4 fue lanzado en el año 2019 [19].

A continuación se presenta una tabla con las características técnicas de los modelos Raspberry Pi 3 modelo A+, Raspberry Pi 3 modelo B+, Raspberry Pi 3 modelo B y Raspberry Pi 4 modelo B.

Tabla 1. Características de los diferentes modelos de Raspberry Pi

Raspberry Pi 3 modelo A+	Raspberry Pi 3 modelo B+	Raspberry Pi 3 modelo B	Raspberry Pi 4 modelo B
Procesador Broadcom Quad-Core de 1.4GHz.	Procesador Broadcom Quad-Core de 1.4Ghz,	Procesador Broadcom Quad-Core de 900MHz a 1.20GHz	Procesador Broadcom Quad-Core de 1.5GHz,
Memoria RAM 512 MB compartidos con la GPU.	Memoria RAM de 1GB.	Memoria RAM de 1GB,	Memoria RAM de 2GB, 4GB y de 8GB.
Video Core IV.	Conectividad inalámbrica incorpora doble banda a 2,4GHz y 5GHz.	Wi-Fi y Bluetooth 4.1 Low Energy sin necesidad de adaptadores.	Dos puertos micro HDMI.
Un puerto USB y sin puerto de conexión de red por cable RJ-45.	Puerto Ethernet 300 Mbits/s,		Capacidad de manejar una pantalla 4K a 60Hz o dos pantallas 4K a 30Hz.

			Puerto USB 3.0
	Bluetooth 4.2 Low Energy.		Puerto Ethernet no limitado a 300 Mbps.

Fuente: Elaboración Propia

1.1.10. Eventos de seguridad

Los eventos son cualquier situación observable dentro de un sistema o red de la organización, es decir, la operación normal de los componentes, el uso e interacción de los usuarios con estos o con sistemas, las conexiones a recursos compartidos, el envío de correos electrónicos, el bloqueo de conexiones por parte del firewall, las conexiones o intentos de conexión a los diferentes servidores al interior de la compañía, entre otros [20].

Dentro de los eventos de seguridad de la información podemos también identificar aquellos en los cuales existe la posibilidad de que hayan sido violadas las políticas de seguridad o fallado o vulnerado controles [21]; a este tipo de eventos se les conoce como eventos adversos, en este contexto no todos los eventos adversos pueden ser considerados incidentes de seguridad.

1.1.11. Incidentes de seguridad

Los incidentes de seguridad pueden ser definidos como la violación o la amenaza inminente de violación de las políticas de seguridad informática, políticas de uso aceptable o practicas estándar de seguridad dentro de la organización [20]. Como ejemplo de incidentes de seguridad podemos citar entre muchos otros el envío de múltiples peticiones a servidores con el fin de causar su indisponibilidad, la descarga de archivos maliciosos que infectan con Malware el ecosistema, la exposición de información confidencial de la organización.

Cuando al interior de las organizaciones se presentan eventos o incidentes de seguridad, es necesario que el equipo de respuesta a incidentes active los planes, políticas y procedimientos definidos en el modelo de gestión de incidentes, a fin de lograr el adecuado tratamiento de la situación presentada.

1.1.12. Modelo de gestión de incidentes

Los modelos de gestión de incidentes buscan mitigar el riesgo de seguridad informática, proporcionando pautas y prácticas para el establecimiento de capacidades al interior de las organizaciones, mediante la generación de planes, políticas y procedimientos que permitan manejar de manera eficaz y eficiente los incidentes de seguridad de la información una vez estos han sido detectados [22].

1.1.13. Modelo de gestión de incidentes NIST SP-800-61

NIST es la sigla del National Institute of Standards and Technology, una agencia que pertenece al departamento de comercio de los Estados Unidos de Norte América; su misión

es promover la innovación y la competitividad industrial de los Estados Unidos mediante el avance de la ciencia, los estándares y la tecnología de la medición de manera que mejoren la seguridad económica y su calidad de vida.[23].

1.1.14. Modelo de gestión de incidentes ISO 27035

La Organización Internacional para la Normalización (ISO), es una federación que agrupa organismos de normalización a nivel mundial. La organización tiene como objetivo proponer y desarrollar las normas requeridas por el comercio, la sociedad y los gobiernos. La ISO, está formada por 165 países miembros y en su interior cuenta con aproximadamente 793 comités y subcomités técnicos, estos son los encargados del desarrollo de estándares y terminología [24].

El modelo de gestión de incidentes ISO 27035:2011 tiene como objetivo brindar orientación sobre la gestión de incidentes de información y las vulnerabilidades de la seguridad de la información mediante la definición de controles efectivos para lograr la reducción o mitigación de los impactos derivados de estos incidentes. Para ello propone 5 fases: Planificación y preparación, detección y reporte, evaluación y decisión, respuestas, y la última, lecciones aprendidas [25].

1.1.15. MINTIC: Guía para la Gestión y clasificación de Incidentes de Seguridad de la Información

Fue desarrollada por Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, tiene como objetivo entregar los elementos necesarios para implementar en las

organizaciones un sistema de gestión de incidentes de seguridad de la información de manera estructurada y bien planificada, de forma que se puedan manejar los incidentes de seguridad de la información de forma adecuada. Para el desarrollo de esta guía, se recogieron aspectos importantes de mejores prácticas y documentos de uso libre por parte del NIST (National Institute of Standards and Technology – (Computer Security Incident Handling Guide), tomando como base los lineamientos recomendados en Norma la ISO IEC 27001 – 2013 Numeral 16 de la misma, para la gestión de incidentes.

1.2. Estado del arte

A continuación se presenta una síntesis de las fuentes de información consultadas en la literatura especializada, relacionada con las investigaciones previas y avances en los temas de mayor interés para el presente Trabajo de Grado y que además apoyan la metodología desarrollada, el logro de sus objetivos y el desarrollo de la investigación misma.

En el año 2018 Dinael y Castro [1] exploraron las vulnerabilidades en dispositivos IoT que con mayor frecuencia son explotadas por los atacantes cuando intentan vulnerar su seguridad; entre las vulnerabilidades analizadas se encuentran: interface web insegura, autenticación/autorización insuficiente, servicios de red inseguros, falta de cifrado en el transporte, privacidad, interfaz de nube insegura, firmware inseguro y seguridad física. Los autores, además instalaron una Honeypot sobre una Raspberry pi 3 con el objetivo de emular dichas vulnerabilidades; como resultado, lograron identificar el comportamiento de los atacantes, los vectores utilizados y las vulnerabilidades explotadas.

El trabajo demostró que los dispositivos IoT son especialmente vulnerables a ataques, debido a que en su mayoría son dispositivos desatendidos y gran parte de los ataques que reciben los dispositivos IoT se encuentran automatizados. Los dispositivos vulnerados son en su mayoría utilizados para ejecutar ataques a otros sistemas. En el proyecto no se utilizó Syslog para el manejo de logs, toda la información generada por el Honeypot durante su periodo de exposición y ataque fue almacenada directamente en la Raspberry, la cual tiene capacidad limitada de almacenamiento, situación que llevo a que se perdiera información valiosa para el análisis final.

Por su parte Acien, Fernández y López [26] propusieron una metodología pensada para dar solución a interrogantes como: ¿qué dispositivos simular de cara a los atacantes?, ¿cómo evaluar su funcionamiento?, ¿cómo obtener información útil de las evaluaciones para usarla en futuras mejoras? La metodología propuesta fue divida en fases. En la primera fase, se hace la búsqueda del dispositivo IoT a utilizar, teniendo en cuenta que este no debe ser muy simple, porque puede hacer que para el atacante sea obvio que es una trampa, ni muy complejo porque el atacante puede perder interés en él, para la selección del dispositivo IoT se valieron de algunos motores de búsqueda especializados en esta tecnología, entre los cuales están Shodan, Censys y Wigle. En la segunda fase se centran en la construcción de la Honeypot, para ello utilizan la información recolectada en la fase de búsqueda del dispositivo. En la tercera fase despliegan la Honeypot en un entorno controlado, lo cual les permite evaluar si la Honeypot puede ser infectada. En la cuarta fase la Honeypot es publicada en internet para que los atacantes la encuentren; uno de los puntos más importantes durante esta fase es lograr que la Honeypot sea lo suficientemente parecida al

sistema real que está emulando, esto ayuda a que los motores de búsqueda la indexen correctamente. En la última fase, se evalúa la información recolectada por la Honeypot durante el despliegue público y se correlaciona con la información obtenida durante el despliegue en ambiente controlado.

En su trabajo de investigación, Boukhalfa, Hmina y Chaoui [27], manifestaron preocupación por la seguridad de los sistemas de información de las compañías a nivel mundial; exponen que cada día los ciber delincuentes mejoran sus métodos de ataque, con el fin de vulnerar los sistemas de seguridad de estas. Los autores propusieron la implementación de un sistema automático de monitoreo de seguridad basado en exponer una Honeypot que les permita recolectar en un servidor de Big Data información sobre los ataques, para posteriormente analizarlos usando una Red Neuronal Recurrente (RNN), la cual utiliza Deep Learning para aprender de los ataques y consecuentemente lograr frenar ataques similares en el futuro. Los autores no plantearon el uso de Blockchain para almacenar la información analizada sobre los ataques, ni proponen el uso del conocimiento adquirido para mejorar un modelo gestión de incidentes de seguridad, como lo pretende hacer el presente trabajo de investigación.

Los investigadores Zhang, Weizhe y otros [28] desarrollaron e implementaron una Honeynet hibrida formada por: una Honeypot de interacción media-alta, capaz de implementar interacción con servicio SOAP, grabación y almacenamiento de logs, descarga de muestras de malware y autocomprobación de servicios, una Honeypot de alta interacción, la cual ejecuta el firmware real de un dispositivo IoT, responsable por dar respuesta a las peticiones no procesadas por la Honeypot de interacción media-alta, y, una Honeypot multipuerto desarrollada utilizando el puerto de servicio SOAP más expuesto en 2018 y simulando

diferentes tipos de dispositivos IoT; la Honeypot multipuerto amplía la capacidad de procesamiento de la Honeynet. Con el objetivo de facilitar el despliegue de la Honeynet, los investigadores empaquetaron la Honeynet como una imagen Docker.

En su trabajo los investigadores se centraron en las vulnerabilidades de los protocolos UPnP y SOAP identificada como CVE-2017-17215; dichas vulnerabilidades permiten ejecutar comandos arbitrarios en el proceso "device upgrade". Una de las particularidades del proyecto fue el uso de un modelo hibrido en el cual implementaron una Honeypot emulada y un dispositivo IoT real, esto les permitió mejorar la respuesta entregada a los atacantes, disminuyendo la posibilidad de ser detectados como una trampa.

Tripathi y Kumar [29], proponen el uso de una Raspberry PI 3 como dispositivo de hardware para la instalación de herramientas para el monitoreo y detección de intrusos. Analizan el rendimiento y fiabilidad del dispositivo, instalando sobre este herramientas como el analizador de paquetes Tshark. De igual forma, validaron la respuesta del IDS Snort y la Honeypot Cowrie al registrar peticiones y alertas ICMP, escaneo de puertos mediante Nmap y ataques de fuerza bruta ejecutados desde una terminal con sistema operativo Kali Linux cuyo objetivo era lograr acceso al dispositivo por medio de SSH. Como resultado, obtuvieron una respuesta adecuada de todas las herramientas instaladas y del dispositivo. Los investigadores concluyen que el uso de dispositivos de bajo costo y facilidad de uso como Raspberry Pi 3 y herramientas de software como los IDS, Honeypots y analizadores de paquetes implementados de forma correcta, ayudan a afrontar ataques, mejorando la seguridad, integridad y disponibilidad de la información.

Al-garadi y Mohammed Ali [4] presentaron un estudio de los últimos métodos de aprendizaje profundo para aplicarlos en la seguridad de los dispositivos IoT. En su investigación identificaron las ventajas y desventajas de los diferentes métodos al ser utilizados para mejorar la seguridad del ecosistema IoT. Los autores hacen un análisis comparativo entre los métodos tradicionales de Machine Learning y los nuevos métodos y enfoques de Deep Learning que utilizan varias capas de procesamiento no lineal para la abstracción y transformación de características discriminatorias o generativas para el análisis de patrones, a fin de entregar el conocimiento necesario para que de acuerdo a su visión, en futuros trabajos se desarrollen métodos eficaces para mejorar la seguridad del ecosistema IoT usando el aprendizaje automático y teniendo en cuenta los nuevos desafíos en materia de seguridad. De igual forma, los investigadores presentan la posibilidad de integrar el aprendizaje automático con otras tecnologías como computación de borde y Blockchain. De manera similar a la propuesta por los autores, en el presente trabajo, se presenta la integración de tecnologías como Honeypots, Big data y Blockchain para mejorar la seguridad y la respuesta a incidentes de seguridad dentro del ecosistema IoT.

En su trabajo de investigación Zamfir, Carabas y Tapus [30] propusieron la creación de un marco de monitoreo capaz de manejar y procesar logs en tiempo real. Para ello implementaron Elastic Search, Logstach y Kibana (ELK) con una configuración básica con la cual buscaban confirmar que las tres herramientas cumplen con los requisitos generales para construir un marco de monitoreo sólido. El monitoreo de sistemas informáticos complejos en tiempo real permite a los administradores detectar fallas que pueden tener consecuencias negativas para una empresa si no se detectan a tiempo; para ello, requieren

tener información que les muestre el estado del sistema en tiempo real, con el objetivo de poder reaccionar de forma rápida y oportuna cuando se presenten situaciones detectadas como anormales. Las aplicaciones modernas generan grandes cantidades de logs que son utilizados para monitorear los parámetros del sistema, diagnosticar problemas, rastrear eventos y mitigar fallas, mediante su almacenamiento, administración y procesamiento.

Bandara, Keong y otros [31] adoptaron un enfoque diferente al de muchos proyectos, en los cuales han intentado agregar características de Big Data a Blockchain; en su trabajo los investigadores agregaron características Blockchain a la base de datos NoSQL Apache Cassandra, como resultado obtuvieron un nuevo sistema Blockchain orientado al uso privado, al cual llamaron Mystiko, este fue diseñado siguiendo el principio de mantenerlo simple para que el sistema sea fácil de entender, fácil de configurar y fácil de implementar. Al utilizar Apache Cassandra y ELK (Elasticsearch, Logstash y Kibana), se le dio a Mystiko características tales como: una mayor escalabilidad y rendimiento a nivel transaccional, arquitectura basada en micro servicios y Dockerizados e implementados mediante Kubernetes, consenso federado, eficiencia en la comunicación lograda al evitar la replicación completa de todos los nodos e implementando una replicación fragmentada, y capacidad de búsqueda de texto completo a través del uso de las herramientas (ELK).

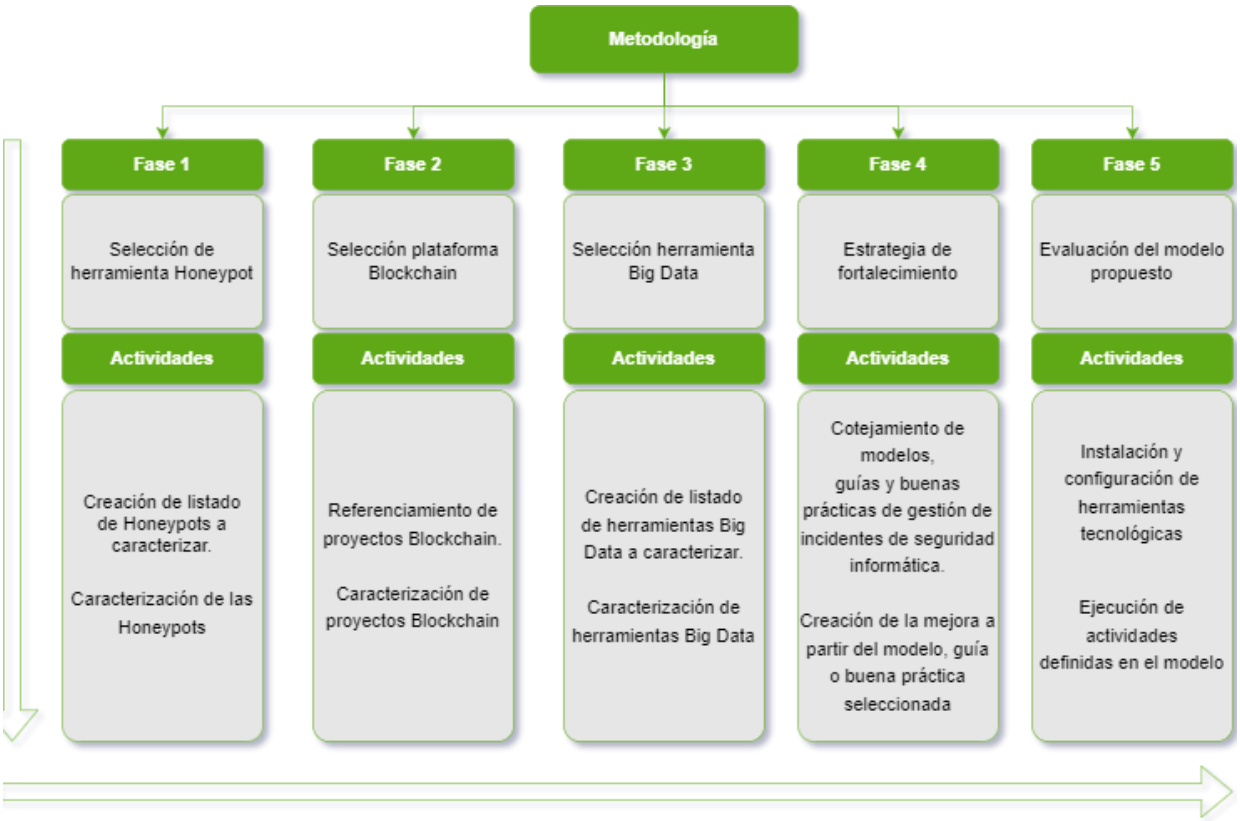
Gómez y Valencia [32] mencionaron que, teniendo en cuenta que no todos los incidentes se pueden prevenir, es necesario que las organizaciones desarrollen capacidades que les permitan detectar rápidamente los incidentes de seguridad, minimizar las pérdidas y la destrucción, mitigar las debilidades que fueron explotadas y restaurar los servicios de TI; en ese sentido, los investigadores estudiaron y analizaron los 5 principales referentes en materia

de gestión de incidentes de seguridad de la información: La guía para la gestión y clasificación de incidentes de seguridad de la información de MINTIC, la guía nacional de notificación y gestión de Ciber incidentes de INCIBE, ll NIST Cybersecurity Framework, el estándar NIST SP 800-61 Rev. 2 y la norma ISO/IEC 27035 – 1 y 2. De su estudio y análisis, infirieron que las normas y guías antes mencionadas tienden a ser **reactivas**, es decir, se centran entre otras cosas en mejorar los tiempos de respuesta de la detección de los incidentes, minimizar las pérdidas y la destrucción, mitigar las debilidades que fueron explotadas y restaurar los servicios de TI, acciones que son aplicables y necesarias, debido a que el incidente de seguridad ya se ha materializado.

2. Metodología

Para lograr el objetivo general propuesto, el proyecto fue dividido en 5 fases (figura 1), donde cada una de ellas corresponde a un objetivo específico; a su vez, cada fase cuenta con actividades que generan entregables que soportan el cumplimiento del objetivo general.

Figura 1. Fases y actividades desarrolladas en la metodología



Fuente: Elaboración propia

A continuación, se describen cada una de las fases desarrolladas para dar cumplimiento al objetivo general:

2.1. Fase 1: Selección de Honeypot

Objetivo: Seleccionar una Honeypot que permita exponer servicios web con el fin de recolectar información sobre los atacantes y los vectores de ataque que estos utilizan para explotar las vulnerabilidades del servicio expuesto. Para llevar a cabo esta fase se ejecutaron las siguientes actividades: (1) Creación de listado de herramientas Honeypot a caracterizar, (2) Caracterización de las herramientas Honeypot.

2.1.1. Actividad 1: Creación de listado de Honeypots a caracterizar

Se creó un listado con las diferentes Honeypots Open source que pueden ser instaladas en un dispositivo IoT; dicho listado se obtuvo como resultado de búsqueda en sitios especializados en seguridad, información obtenida de la página web oficial de las herramientas Honeypot mencionadas en foros de seguridad en bibliografía indexada.

En el proceso de creación de listado de las Honeypot a caracterizar, solo se tuvieron en cuenta aquellas que cumplen los dos requerimientos mínimos definidos. A continuación se presentan los requerimientos mínimos y el motivo por el cual fueron definidos:

Requerimientos mínimos definidos:

- **Honeypots open source:** Al ser un proyecto de investigación aplicado desde el punto de vista académico, se consideró importante contar con una solución que se pudiera adecuar a las necesidades del proyecto y cuyo costo de implementación fuera bajo o inexistente.

- **Honeypots que puedan ser instaladas en un dispositivo IoT:** El proyecto requiere la recolección de datos desde un dispositivo IoT, por lo cual, la Honeypot debía poder ser instalada en dichos dispositivos.

Dado lo anterior, una vez creado el listado de Honeypots, la evaluación del cumplimiento de requerimientos mínimos de cada una será tabulado usando la siguiente tabla a continuación; el resultado de la evaluación será presentado en el capítulo de resultados (capitulo 3):

Tabla 2 Cumplimiento de requisitos mínimos por Honeypot

Honeypot	Open Source	Instalable en IoT

Fuente: Elaboración propia

2.1.2. Actividad 2: Caracterización de las Honeypots

Se evaluarán las Honeypots que cumplen con los dos requerimientos mínimos definidos en la actividad 1 de la presente fase; para el proceso de evaluación de las Honeypots, se definieron cinco criterios y el método de evaluación a utilizar, se seleccionara para su instalación en el laboratorio de pruebas la Honeypot que obtenga el mayor puntaje total en la evaluación.

A continuación, se presentan a) los criterios de evaluación a utilizar en la evaluación y b) la metodología de evaluación a utilizar:

a) Criterios de evaluación

- **Integración con el protocolo Syslog o similar:** Syslog es el acrónimo de System Logging Protocol, se trata de un protocolo que es utilizado para enviar registros o eventos de un sistema a un servidor para su almacenamiento y posterior análisis. La integración con Syslog, permite que la Honeypot pueda enviar al servidor central los eventos que se generaron cuando esta fue expuesta a internet y recibió ataques; el análisis de estos eventos permite entender los vectores de ataque utilizados y sus orígenes; lo cual lleva a la generación de una base de conocimiento. La integración con Syslog fue seleccionada como una de las características, debido a la necesidad que se tenía de poder obtener los logs generados por la Honeypot y llevarlos a un servidor para su posterior análisis mediante el uso de otras herramientas visuales como ELK.
- **Disponibilidad de los archivos instaladores:** Los instaladores permiten desplegar la Honeypot en el dispositivo IoT seleccionado; esto es fundamental en el montaje del laboratorio de pruebas, sin los instaladores no es posible instalar la Honeypot y, por ende, no se puede dar cumplimiento a las pruebas. Esto demuestra la importancia que tiene contar con los instaladores de la Honeypot, pues la fuente de la información son los eventos de seguridad que se registren.
- **Calidad de la documentación:** La documentación permite estudiar cómo hacer la instalación y configuración de la Honeypot y conocer mejor sus características y

capacidades; al igual que en punto anterior “Disponibilidad de los instaladores” sin una documentación adecuada la dificultad para instalar la Honeypot se hubiese elevado, motivo por el cual se consideró esta característica como fundamental en la selección de la Honeypot.

- **Emulación de servicio Web:** Esta característica fue definida debido a que está directamente relacionada con el objetivo general del proyecto, pues se pretende mejorar un modelo de gestión de incidentes basado en ataques a servicios web instalado sobre un dispositivo IoT; por lo cual era fundamental que la Honeypot seleccionada tuviera la capacidad de emular un servicio web; si la Honeypot no cuenta con esta característica no tendría ningún sentido seleccionarla para ser utilizada en el proyecto.

b) Metodología de evaluación

En la evaluación de los criterios “**integración con Syslog o similar**, **disponibilidad de instaladores** y **emulación de servicios web”** se asignará 1 punto a aquellas Honeypots que cuentan con la característica y 0 puntos a aquellas que no, en la evaluación de la característica “**calidad de la documentación**” se definió la siguiente escala de puntos:

- 3 puntos: Buena documentación: La documentación describe paso a paso el proceso de instalación de la Honeypot.
- 2 puntos: Mediana documentación: La documentación describe de manera general el proceso de instalación de la Honeypot.
- 1 punto: Baja documentación: La documentación no describe el proceso de instalación, por lo cual se requiere dedicar un tiempo y esfuerzo considerable para

lograr la instalación y configuración de la Honeypot, se corre el riesgo de mal funcionamiento debido a la falta de guía.

Dado lo anterior, la evaluación del cumplimiento de los criterios definidos de cada una será tabulado usando la siguiente tabla; el resultado de la evaluación será presentado en el capítulo de resultados (capitulo 3):

Tabla 3. Evaluación de criterios por cada Honeypot

Honeypot	Integración con Syslog	Código fuente	Calidad de la documentación	Emulación de servicios Web	Totales

Fuente: Elaboración propia

2.2. Fase 2: Selección de la cadena de bloques y definición de estructura de datos

Objetivo: Seleccionar una plataforma Blockchain que permita almacenar la información resultante del análisis de los Logs generados por la Honeypot seleccionada en la fase 1. La información resultante del análisis de los logs se almacenará en la Blockchain, con el fin de compartirla con otras organizaciones y garantizar su disponibilidad, integridad y

confidencialidad. Para llevar a cabo esta fase se ejecutaron las siguientes actividades: (1) Referenciamiento de proyectos Blockchain (2) Caracterización de tecnologías Blockchain.

2.2.1. Actividad 1: Referenciamiento de plataformas Blockchain

Se hizo una exploración de diferentes fuentes de información (Internet, sitio web oficiales, documentos técnicos) con el fin de determinar cuáles son los proyectos Blockchain más importantes en la actualidad. Se seleccionaron para su posterior caracterización aquellos que cumplían los dos requerimientos mínimos definidos; A continuación, se presentan dichos requerimientos mínimos y el motivo por el cual fueron definidos:

- **Plataformas Blockchain open source:** Al igual que con la selección de la Honeypot, al ser un proyecto de investigación aplicada desde el punto de vista académico, es importante contar con una solución que se pueda adecuar a las necesidades en cuanto a instalación y cuyo costo de implementación fuera bajo o inexistente.
- **Plataformas Blockchain Privadas – Autorizadas:** Igual que en el punto anterior (open source), al ser un proyecto de investigación aplicada desde el punto de vista académico, se requiere hacer una implementación para uso privado que permita mantener control sobre la red.

Dado lo anterior, la evaluación del cumplimiento de los criterios mínimos será tabulado usando la siguiente tabla; el resultado de la evaluación será presentado en el capítulo de resultados (capitulo 3):

Tabla 4. Evaluación de cumplimiento de requisitos mínimos

Blockchain	Open Source	Privada - Autorizada

Fuente: Elaboración propia

2.2.2. Actividad 2: Caracterización de proyectos Blockchain

Para el proceso de evaluación de las plataformas Blockchain, se definieron tres criterios y el método de evaluación a utilizar, se seleccionará para su uso en el laboratorio de pruebas la plataforma que obtenga el mayor puntaje total en la evaluación.

A continuación, se presentan a) los criterios de evaluación y b) la metodología de evaluación de cada uno de ellos:

a) Criterios de evaluación

- **Plataformas Blockchain privadas – autorizadas:** Las Blockchain con permisos o autorizadas operan de forma individual o bajo un conjunto de participantes conocidos; esto proporciona una forma de asegurar las interacciones entre un grupo de entidades que tienen un objetivo común pero que pueden no confiar plenamente entre sí. La autorización permite controlar quien puede acceder a la red, lo cual quiere decir que solo las personas con permiso o autorizadas pueden crear nuevos bloques y procesar transacciones. Las redes privadas con autorizadas o con permiso generalmente están bajo el control de una o varias organizaciones que tienen la gobernanza sobre los datos y los participantes en la red. Esta característica fue

seleccionada debido a la necesidad de almacenar los datos importantes generados por la Honeypot al recibir ataques y que dada su naturaleza es considerada de carácter confidencial.

- **Plataformas Blockchain con soporte de contratos inteligentes:** Los contratos inteligentes o smart contracts tienen como objetivo eliminar intermediarios, simplificar procesos y bajar costos. Los contratos inteligentes son pequeños programas con instrucciones que son almacenados en la Blockchain y que tienen la capacidad de ejecutar automáticamente acciones basadas en parámetros previamente programadas de forma inmutable, transparente y segura; los contratos inteligentes son el equivalente a la lógica de negocio de las aplicaciones de software y al igual que los contratos convencionales determinan qué se puede hacer, cómo se debe hacer y qué ocurre si no se hace, es decir, define la interacción que tendrán los involucrados en una transacción sin que sea necesaria la intervención humana. Esta característica fue seleccionada debido a que se requiere mediante la implementación de un contrato inteligente determinar qué se almacena en la Blockchain y quién tienen permisos de acceder a la información; aunque inicialmente solo una organización participará en la red, en futuras investigaciones puede llegar a ser necesario abrir la red para que otras organizaciones almacenen información en la red.
- **Plataformas Blockchain diseñada para uso corporativo:** A medida que las criptomonedas se han popularizado y se conoce más sobre la tecnología Blockchain, ha crecido también el interés en aplicar la tecnología subyacente de la cadena de bloques, el libro mayor distribuido y la plataforma de aplicaciones distribuidas a

casos de uso empresarial más innovadores, sin embargo, en la mayoría de los casos de uso empresarial se requiere conocer la identidad de los participantes y contar con mayores capacidades a nivel de rendimiento, cosas que las Blockchain públicas no pueden satisfacer. Teniendo lo anterior en cuenta, se determinó que, para el proyecto, lo más adecuado era utilizar una Blockchain específicamente diseñada para uso corporativo y no una adaptación de una red pública para satisfacer los casos de uso en los que las organizaciones deben utilizarla. Uno de los puntos fundamentales en la definición de esta característica es que se trata de un caso de uno en el cual inicialmente solo una organización participa en la red y que los datos que se almacenan solo son de interés de esta organización.

b) Metodología de evaluación

En la evaluación de los criterios **plataformas Blockchain privadas - autorizadas**, **plataformas Blockchain con soporte de contratos inteligentes** y **plataformas Blockchain diseñadas para uso corporativo**, se asignó 1 punto a aquellas que cumplen con la característica y 0 puntos a aquellas que no.

Dado lo anterior, la evaluación del cumplimiento de los criterios definidos de cada una será tabulado usando la siguiente tabla; el resultado de la evaluación será presentado en el capítulo de resultados (capitulo 3):

Tabla 5. Evaluación Caracterización de plataformas Blockchain

Blockchain	Privada Autorizada	Soporte contratos inteligentes	Diseñada para uso corporativo	Totales

Fuente: Elaboración propia

2.3. Fase 3: Selección de la herramienta Big Data

Objetivo: Seleccionar una herramienta Big Data que permitiera analizar en tiempo real los logs generados por la Honeypot seleccionada en la fase 1. Para llevar a cabo esta fase se ejecutaron las siguientes actividades: (1) Creación de listado de herramientas Big Data a caracterizar, (2) Caracterización de las herramientas Big Data.

2.3.1. Actividad 1: Creación de listado de herramientas Big Data a caracterizar

Se creó un listado con las diferentes herramientas Big Data con capacidad de procesar información en tiempo real; dicho listado se obtuvo como resultado de búsqueda en sitios

especializados en seguridad, información obtenida de la página web oficial de las herramientas Big Data mencionadas en foros de seguridad y en bibliografía indexada.

En el proceso de creación de listado de las herramientas Big Data a caracterizar, se tuvieron en cuenta solo aquellas que cumplían el requerimiento mínimo definido; a continuación, se presentan el requerimiento mínimo y el motivo por el cual fue definido:

Requerimiento mínimo definido:

- **Herramientas Big Data open Source:** Al igual que con la selección de la Honeypot y la Blockchain, al ser un proyecto de investigación aplicada desde el punto de vista académico, es importante contar con una solución que se pueda adecuar a las necesidades en cuanto a instalación y cuyo costo de implementación fuera bajo o inexistente. Dado lo anterior, la información recolectada fue tabulada en la tabla 6.

Dado lo anterior, una vez creado el listado de herramientas Big Data, la evaluación del cumplimiento de requerimiento mínimo de cada una será tabulado usando la tabla a continuación; el resultado de la evaluación será presentado en el capítulo de resultados (capitulo 3):

Tabla 6. Cumplimiento de requisito mínimo de las herramientas Big Data

Honeypot	Open Source	URL

Fuente: Elaboración propia

2.3.2. Actividad 2: Caracterización de herramientas Big Data

Para el proceso de evaluación de las herramientas Big Data, se definieron tres criterios, el método de evaluación a utilizar se seleccionará para su uso en el laboratorio de pruebas la herramienta Big Data que obtenga el mayor puntaje total en la evaluación.

A continuación, se presentan a) los criterios de evaluación y b) la metodología de evaluación de cada uno de ellos:

a. Criterios de selección de las herramientas Big Data

- **Capacidad de procesamiento en tiempo real:** El procesamiento de Big Data en tiempo real se refiere a la capacidad que tiene una herramienta de procesar (analizar, almacenar y visualizar) de manera analítica parte o la totalidad de los datos en espacios de tiempo muy corto. Esta característica se seleccionó porque se requiere que la información que se genera en la Honeypot sea procesada en el menor tiempo posible, de tal forma que se tenga información sobre lo que ocurre a medida que ocurre.
- **Especializado en análisis de logs**: Los logs o registros del sistema son archivos de texto o XML en los cuales se registran la información de los eventos y comportamientos que tienen los sistemas que los generan a medida que estos están en operación. El análisis de logs es fundamental en la seguridad de las compañías, su análisis ha permitido desarrollar herramientas para la gestión de eventos de seguridad de la información como

lo son las herramientas SIEM. En el proyecto, es fundamental el análisis de los logs que genera la Honeypot, de su análisis de pueden obtener datos de gran importancia para la gestión de eventos de seguridad, por lo cual, es fundamental que la herramienta Big data seleccionada sea especializada en el manejo de logs.

- **Uso en nodo simple (no clúster):** La característica uso de nodo simple se refiere a la posibilidad que la herramienta Big data sea instalada en un solo sistema de procesamiento; esta característica es importante debido a que facilita el montaje del laboratorio de pruebas y se mantienen los costos bajo control.

b. Metodología de evaluación

En la evaluación de todos los criterios "**capacidad de procesamiento en tiempo real"**, "**especializado en análisis de logs"** y "**uso en nodo simple"**, se asignó 1 punto a aquellas que cumplen con la característica y 0 puntos a aquellas que no.

Dado lo anterior, la evaluación del cumplimiento de los criterios definidos de cada una será tabulado usando la siguiente tabla; el resultado de la evaluación será presentado en el capítulo de resultados (capitulo 3):

Tabla 7. Evaluación de criterios de las herramientas Big Data

Honeypot	Open Source	Procesamiento en tiempo real	Especializado en análisis de logs	Nodo simple	Totales

Fuente: Elaboración propia

2.4. Fase 4: Definir estrategia de fortalecimiento del modelo de gestión de incidentes

Objetivo: Proponer una mejora a un modelo de gestión de incidentes de seguridad, que permita, mediante el conocimiento de los vectores de ataque usados para explotar las vulnerabilidades de un activo, generar de manera proactiva controles mitiguen los incidentes de seguridad informática antes que estos se materialicen en los ambientes productivos de la compañía. En este sentido, se realizaron dos actividades: (1) Cotejar los modelos, guías y buenas prácticas de gestión de incidentes de seguridad informática, (2) Creación de la mejora a partir del modelo, guía o buena práctica seleccionada.

2.4.1. Actividad 1: Cotejar modelos y guías de gestión de incidentes de seguridad de la información.

Se hizo una búsqueda de los modelos, guías, estándares y buenas prácticas para la gestión de incidentes de seguridad, con el fin de seleccionar aquellos que desde la óptica y experiencia de los investigadores pueden servir como base para la creación de la mejora que se pretende proponer en el presente trabajo de investigación. Una vez efectuada la búsqueda de los modelos, guías, estándares y buenas prácticas para la gestión de incidentes de seguridad se seleccionaron los siguientes:

- **ISO/IEC 27035 – 1 y 2:** Tecnología de la información - Técnicas de seguridad - la información de gestión de incidentes de seguridad – parte 1, principios y parte 2, directrices para planificar y prepararse para la respuesta a incidentes, 11/01/2016.
- **Estándar NIST SP 800-61 rev 2:** Computer Security Incident Handling Guide, Agosto 2012.
- **MINTIC:** Guía para la Gestión y clasificación de Incidentes de Seguridad de la Información, 6/11/2016.
- **ISO IEC 27001 2013 - A16** Gestión de incidentes de la seguridad de la información.

Se cotejaron las normas seleccionadas con el fin de entender sus fases y actividades, y seleccionar aquella(s) que puede(n) ser utilizada(s) y/o potenciada(s) como parte de la propuesta de mejora.

Dado lo anterior, la información obtenida en el cotejamiento será tabulada en la siguiente tabla que se presentará en el capítulo de resultados.

Tabla 8. cotejamiento de modelos, normas y buenas practicas

Modelo, norma o Buena Practica 1		Modelo, norma o Buena Practica 2		Modelo, norma o Buena Practica 3	
Fase 1	Actividades	Fase 1	Actividades	Fase 1	Actividades
Fase 2	Actividades	Fase 2	Actividades	Fase 2	Actividades

Fase 3	Actividades	Fase 3	Actividades	Fase 3	Actividades

Fuente: Elaboración propia

2.4.2. Actividad 2: Creación de la mejora a partir del modelo o guía seleccionada.

Se definieron las Fases y actividades que deben llevarse a cabo en la gestión proactiva de eventos e incidentes de seguridad; para llevar a cabo esta actividad se tuvo en cuenta el resultado del cotejamiento efectuado de los modelos, guías y buenas prácticas de gestión de incidentes de seguridad efectuado en la actividad 1.

Dado lo anterior, las fases y actividades que componen la mejora propuesta serán tabuladas en la siguiente tabla que se presentara en el capítulo de resultados:

Tabla 9. Fases y Actividades nuevo modelo de gestión de incidentes de seguridad

Fase 1	Actividades clave
Fase 2	Actividades clave
Fase n	Actividades clave

Fuente: Elaboración propia

2.5. Fase 5: Evaluación del modelo de gestión de incidentes

Objetivo: Evaluar el modelo de gestión de incidentes de seguridad propuesto, a través de la validación de la eficiencia y efectividad del proceso proactivo de tratamiento de las

amenazas y vulnerabilidades mediante los controles definidos e implementados sobre el ambiente productivo de una organización. Para lograrlo se realizaron dos actividades: (1) Instalación y configuración de las herramientas tecnológicas (Honeypot, Big Data, Blockchain), (2) Ejecución de fases y actividades definidas en el modelo propuesto.

2.5.1. Actividad 1: Instalación y configuración de herramientas tecnológicas

En esta actividad se instalaron y configuraron las herramientas tecnológicas que conforman el componente activo necesario en el proceso de identificación de las amenazas y vulnerabilidades de los activos expuestos.

2.5.2. Actividad 2: Ejecución de actividades definidas en el modelo

En esta actividad se ejecutaron las actividades definidas en las fases del modelo propuesto; para su ejecución se contó con el apoyo y soporte de la empresa T.I RESCUE (https://tirescue.com/) especialista en desarrollo e instalación de soluciones de ciberseguridad, quienes pusieron a prueba el modelo propuesto.

3. Resultados

A continuación, se presentan los resultados obtenidos en la ejecución de las actividades de las fases definidas en la metodología.

3.1. Fase 1: Selección de Honeypot

Objetivo: Seleccionar una Honeypot que permita exponer a internet un servicio web, con el fin de recolectar información sobre los atacantes y los vectores de ataque que estos utilizan para explotar las vulnerabilidades del activo expuesto.

3.1.1. Actividad 1: Creación de listado de Honeypots a caracterizar

Se género listado con las Honeypots mencionadas en diversas fuentes consultadas a través de internet. A continuación, se presenta el listado de algunas de las fuentes consultadas:

Tabla 10. Listado de URL consultadas para creación de listado de Honeypots a caracterizar

URL
https://www.hackplayers.com/2015/12/gran-recopilacion-de-honeypots.html
https://blog.elhacker.net/2021/01/los-mejores-honeypots-ejemplos-y-tipos-trampas-rdp-ssh-cowrie-docker-rdpy.html
https://blog.segu-info.com.ar/2015/12/recopilacion-de-honeypots.html
https://github.com/paralax/awesome-honeypots

Fuente: Elaboración propia

Una vez obtenido el listado inicial, se buscó la página web oficial del proyecto y/o en documentos que permitieran ampliar la información de cada una. A continuación, se presenta el listado de Honeypots y los documentos y/o páginas web en los cuales se encontró información sobre cada una:

Tabla 11. Listado de Honeypots inicial y sitio web/documento para ampliación de información

Honeypot	Sitio web / Documento
Telnet IoT Honeypot	https://github.com/Phype/telnet-iot-honeypot
HoneyThing	https://github.com/omererdem/honeything
MTPot	https://github.com/Cymmetria/MTPot
IoTPot	https://github.com/IoTPOT/IoTPOT
Shipon Honeypot	SIPHON: Towards Scalable High-Interaction Physical Honeypots [33].
IoTCandyJar	IoTCandyJar: Towards an Intelligent-Interaction Honeypot for IoT Devices [34]
Thing Pot	ThingPot: an interactive Internet-of-Things honeypot [35] https://github.com/Mengmengada/ThingPot
Dionaea	Capturing attacks on IoT devices [36] https://communityhoneynetwork.readthedocs.io/en/stable/dionaea/
Cowrie	Capturing attacks on IoT devices [36] https://github.com/cowrie/cowrie

Fuente: Elaboración propia

El listado inicial se depuro teniendo en cuenta los dos requisitos mínimos definidos para el proyecto. Durante el proceso de depuración del listado inicial, se consultaron las páginas web y/o documentos con el fin de estudiar la información técnica de cada Honeypots; a continuación, se presenta el listado de las fuentes consultadas por cada Honeypot:

De acuerdo en lo definido en la Metodología, en la tabla 12 se presenta el listado de las Honeypots que cumplieron con los requisitos mínimos definidos: Honeypots open source y Honeypots instables en un dispositivo IoT:

Tabla 12. Evaluación de cumplimiento de requisitos mínimos Honeypots

Honeypot	Open Source	Instalable en IoT
Telnet IoT Honeypot	Si	Si
HoneyThing	Si	Si
MTPot	Si	Si
IoTPOT	Si	Si
Siphon	Si	Si
IoT Candy Jar	Si	Si
Thing Pot	Si	Si
Dionaea	Si	Si
Cowrie	Si	Si

Fuente: Elaboración propia

3.1.2. Actividad 2: Caracterización de las Honeypots

Para la caracterización de las Honeypots, se partió del listado creado en la actividad 1 de la fase 1; a cada una de las Honeypots del listado se le evaluó el cumplimiento de las cinco

características definidas en la metodología; como resultado de la evaluación se obtuvieron las tablas 13 y 14.

Tabla 13. Evaluación de cumplimiento de criterios Honeypots

Honeypot	Open Source	Integración con Syslog	Código Fuente	Calidad Documentación	Emulación de Servicios Web	Totales
Telnet IoT Honeypot	1	1	1	2	0	5
HoneyThing	1	1	1	2	0	5
MTPot	1	1	1	2	0	5
IoTPOT	1	0	1	1	0	3
Siphon	1	0	0	2	1	4
IoT Candy Jar	1	0	0	2	1	4
Thing Pot	1	1	0	1	1	4
Dionaea	1	1	1	3	1	7
Cowrie	1	1	1	3	0	6

Fuente: Elaboración propia

Como se puede observar en la tabla 13, la Honeypot **Dionaea** obtuvo un total de siete puntos (7 puntos); por lo cual fue seleccionada como la Honeypot a ser utilizada en el proyecto.

Tabla 14. Descripción y características generales de las Honeypots evaluadas

Honeypot	Descripción	Protocolos	Arquitectura	Interacción
Telnet IoT Honeypot	El objetivo principal del proyecto Telnet IoT Honeypot fue analizar automáticamente las conexiones de Botnet y mapearlas vinculando diferentes conexiones e incluso redes. El proyecto implementó un servidor telnet de Python que intenta actuar como un Honeypot para detectar Malware IoT que se propaga a través de contraseñas predeterminadas e inseguras en servidores telnet en Internet. El Honeypot funcionó emulando un entorno de caparazón de la misma forma que lo hace la Honeypot Cowrie.	Telnet	Cliente - Servidor	Baja
HoneyThing	HoneyThing es una Honeypot para IoT (TR-069). Se diseñó para actuar completamente como un módem/enrutador que tiene un servidor web integrado (RomPager) y es	TR-064	Cliente	Baja

	compatible con el protocolo TR-069 (CWMP).			
MTPot	Proyecto específicamente diseñado para comprender cómo opera el Bot Mirai en la infección de dispositivos IoT como cámaras y Routers para su posterior uso en ataques DoS y DDoS.	Telnet	Cliente	Baja
IoTPOT	IoTPOT características hibridas; como servicio principal implementa Telnet de cara a los atacantes externos simulando ser un dispositivo IoT conectado a Internet, pero en una segunda capa considerada de alta interacción, es capaz de procesar los comandos del malware en diversos entornos simulados con distintas arquitecturas (ARM, MIPS o X86 por ejemplo). Esta herramienta fue desarrollada por un grupo de investigadores japoneses tras los ataques de la Botnet Mirai.	Telnet	Cliente	- Baja - Alta

Siphon	Siphon es una plataforma Honeypot escalable de alta interacción para dispositivos IoT. Siphon aprovecha los dispositivos IoT que se encuentran físicamente en una ubicación y están conectados a Internet a través de los llamados agujeros de gusano distribuidos por todo el mundo. La arquitectura resultante permite exponer pocos dispositivos físicos sobre una gran cantidad de direcciones IP distribuidas geográficamente.	- SSH - HTTP	Cliente	- Alta
IoT Candy Jar	Proyecto que buscó crear una Honeypot de interacción inteligente utilizando dispositivos publicados en internet para recopilar las respuestas a las solicitudes. La interacción inteligente se refiere a la capacidad de emular Honeypots de alta y baja interacción, emulando el comportamiento de los dispositivos IoT y logrando que las peticiones y el código	- HTTP - SSH -Telnet -TR-064 -XMPP -MQTT -UPnP -CoAP -MS-RDP	Cliente	- Baja y Alta (interacción inteligente)

	enviado al Honeypot sean procesadas como lo haría el dispositivo real, obteniendo como ventaja que el Honeypot no puede ser comprometido.			
Thing Pot	Thing Pot se consideró un MIH o una plataforma IoT de interacción híbrida Honeypot, cuya plataforma comprende XMPP/MQTT como módulos HIH, mientras que la emulación de dispositivos LIH se realizó a través de una API REST. Thing Pot simula el Front End, el Back End, los dispositivos IoT y los servicios XMPP/MQTT existentes (servidores, clientes, bibliotecas). Todos estos componentes componen la plataforma IoT con la que los piratas informáticos pueden interactuar.	-HTTP - MPP	Cliente - Servidor	- Alta - Media - Baja
Dionaea	Es un Honeypot de baja interacción (emula servicios), sucesor del proyecto Nepenthes, escrito en C pero que además incorpora Python como lenguaje de scripting, utiliza la biblioteca Libemu para	- Blackhole - EPMAP - FTP - HTTP -	Cliente	- Baja

	emular la ejecución de instrucciones Intel x86 y detectar shellcodes. Además, cuenta con soporte para IPv6 y protocolo TLS. El objetivo del Honeypot Dionaea es obtener una copia del Malware que intenta propagarse por la red al brindar servicios que pretenden ser vulnerables.	Memcache - Mirror - MQTT - MSSQL - MYSQL - PPTP - SIP - SBM - TFTP		
Cowrie	Cowrie es una Honeypot de interacción media SSH y Telnet diseñado para registrar ataques de fuerza bruta e interacción de proyectiles realizados por un atacante. Cowrie también funciona como un proxy SSH y telnet para observar el comportamiento del atacante a otro sistema. Cowrie fue desarrollado a partir de Kippo	- SSH - SFTP - SCP	Cliente	- Media

Fuente: Elaboración propia

3.1.2.1. Descripción general de la Honeypot Seleccionada (Dionaea)

- **Objetivo de Dionaea:** La intención de Dionaea es atrapar el Malware que explota las vulnerabilidades expuestas por los servicios ofrecidos a una red, el objetivo final es obtener una copia del malware.
- **Requisitos de instalación:** A continuación, se presentan los requerimientos que fueron necesarios para la instalación de la Honeypot Dionaea:

Plataforma	Opciones
Sistema operativo	• **Ubuntu 18.04 LTS (recomendado) (usado para desarrollo)** • **Debian 10 (recomendado)**
Tiempo de ejecución de Python	• **3.9 (recomendado)** • **3.8 (recomendado)** • **3.7** • **3.6**

Fuente: Elaboración propia

- **Configuración predeterminada Dionaea:** El archivo de configuración de Dionaea se llama dionaea.cfg; a continuación, se presenta la configuración predeterminada de la Honeypot:

```
# SPDX-FileCopyrightText: none
# SPDX-License-Identifier: CC0-1.0
[dionaea]
download.dir=@DIONAEA_STATEDIR@/binaries/
```

#modules=curl,python,nfq,emu,pcap

modules=curl,python,emu

processors=filter_streamdumper,filter_emu

listen.mode=getifaddrs

 # listen.addresses=127.0.0.1

 # listen.interfaces=eth0,tap0

 # Use IPv4 mapped IPv6 addresses

 # It is not recommended to use this feature, try to use nativ IPv4 and IPv6 adresses

 # Valid values: true|false

 # listen.use_ipv4_mapped_ipv6=false

 # Country

 # ssl.default.c=GB

 # Common Name/domain name

 # ssl.default.cn=

 # Organization

 # ssl.default.o=

 # Organizational Unit

 # ssl.default.ou=

 # Provide certificate files

 # The provided certificate must be in the PEM format.

 # The certificates must be sorted starting with the server certificate

 # followed by intermediate CA certificates if applicable and ending at

 # the highest level CA.

 # ssl.default.cert=@DIONAEA_CONFDIR@/ssl/your-certificate-with-chain.crt

 # The provided key must be in the PEM format.

 # ssl.default.key=@DIONAEA_CONFDIR@/ssl/your-private-key.key

[logging]

default.filename=@DIONAEA_LOGDIR@/dionaea.log

default.levels=all

default.domains=*

errors.filename=@DIONAEA_LOGDIR@/dionaea-errors.log

errors.levels=warning,error

errors.domains=*

[processor.filter_emu]

name=filter

config.allow.0.protocols=smbd,epmapper,nfqmirrord,mssqld

next=emu

[processor.filter_streamdumper]

name=filter

config.allow.0.types=accept

config.allow.1.types=connect

config.allow.1.protocols=ftpctrl

config.deny.0.protocols=ftpdata,ftpdatacon,xmppclient

next=streamdumper

[processor.streamdumper]

name=streamdumper

config.path=@DIONAEA_STATEDIR@/bistreams/%Y-%m-%d/

[processor.emu]

name=emu

config.limits.files=3

*#512 * 1024*

config.limits.filesize=524288

config.limits.sockets=3

config.limits.sustain=120

config.limits.idle=30

config.limits.listen=30

config.limits.cpu=120

*#// 1024 * 1024 * 1024*

config.limits.steps=1073741824

[module.nfq]

queue=2

[module.nl]

 # set to yes in case you are interested in the mac address of the remote (only works for lan)

lookup_ethernet_addr=no

[module.python]

imports=dionaea.log,dionaea.services,dionaea.ihandlers

sys_paths=default

service_configs=@DIONAEA_CONFDIR@/services-enabled/*.yaml

ihandler_configs=@DIONAEA_CONFDIR@/ihandlers-enabled/*.yaml

[module.pcap]

any.interface=any

– **Ejecutando Dionaea:** A continuación, se presentan las opciones que puede utilizar al correr Dionaea:

```
$ /opt/dionaea/bin/dionaea -H
  -c, --config=FILE               use FILE as configuration file
                                    Default value/behaviour: /opt/dionaea/etc/dionaea/dionaea.cfg
  -D, --daemonize                 run as daemon
  -g, --group=GROUP               switch to GROUP after startup (use with -u)
                                    Default value/behaviour: keep current group
  -G, --garbage=[collect|debug]   garbage collect,  usefull to debug memory leaks,
                                  does NOT work with valgrind
  -h, --help                      display help
  -H, --large-help                display help with default values
  -l, --log-levels=WHAT           which levels to log, valid values
                                  all, debug, info, message, warning, critical, error
                                  combine using ',', exclude with - prefix
  -L, --log-domains=WHAT          which domains use * and ? wildcards, combine using ',',
                                  exclude using -
  -u, --user=USER                 switch to USER after startup
                                    Default value/behaviour: keep current user
  -p, --pid-file=FILE             write pid to file
  -r, --chroot=DIR                chroot to DIR after startup
                                    Default value/behaviour: don't chroot
  -V, --version                   show version
  -w, --workingdir=DIR            set the process' working dir to DIR
                                    Default value/behaviour: /opt/dionaea

examples:
    # dionaea -l all,-debug -L '*'
    # dionaea -l all,-debug -L 'con*,py*'
    # dionaea -u nobody -g nogroup -w /opt/dionaea -p /opt/dionaea/var/run/dionaea.pid
```

3.2. Fase 2: Selección de la cadena de bloques y definición de estructura de datos

Objetivo: Seleccionar una plataforma Blockchain que permita almacenar la información resultante del análisis de los Logs generados por la Honeypot seleccionada en la fase 1.

3.2.1. Actividad 1: Referenciamiento de proyectos Blockchain

Se realizaron búsquedas en internet con el fin de referenciar las diferentes plataformas Blockchain; como resultado de dicha búsqueda se creó un listado inicial de plataformas Blockchain; A continuación, se presenta dicho listado:

Tabla 15. Listado de plataformas Blockchain a caracterizar y URL página oficial

Plataforma Blockchain	URL
Ethereum	https://ethereum.org/en/
Ripple	https://ripple.com/
Cardano	https://ripple.com/
Stellar	https://www.stellar.org/?locale=en
Hyperledger Fabric	https://openblockchain.readthedocs.io/en/latest/
EOS	https://eos.io/
Corda	https://www.corda.net/
Tron	https://tron.network/
Multichain	https://www.multichain.com/

Hyperledger Sawtooth	https://sawtooth.hyperledger.org/
Quorum	https://docs.qbs.consensys.net/

Fuente: Elaboración propia

De acuerdo con lo definido en la Metodología, se seleccionaron las plataformas Blockchain que cumplieron los dos requisitos mínimos definidos en la metodología (Plataformas Blockchain open Source y Plataformas Blockchain Privadas – Autorizadas).

A continuación, se presenta el listado de las plataformas Blockchain que cumplieron con los dos requisitos mínimos:

Tabla 16. Evaluación de cumplimiento de requisitos mínimos plataformas Blockchain

Plataforma Blockchain	Open Source	Privada - Autorizada
Corda	Si	Si
Hyperledger Fabric	Si	Si
Multichain	Si	Si
Enterprise Ethereum	Si	Si
Quorum	Si	Si
Hyperledger Sawtooth	Si	Si

Fuente: Elaboración propia

Como se puede observar, de las once plataformas Blockchain analizadas, seis cumplieron con los requisitos mínimos, y en ese sentido, son las que se evalúan para la selección final.

3.2.2. Actividad 2: Caracterización de plataforma Blockchain

En la caracterización de las plataformas Blockchain, se evaluó el cumplimiento de los dos criterios definidos para el proyecto: Plataformas Blockchain con soporte de contratos inteligentes y Plataformas Blockchain diseñadas para uso corporativo.

A continuación, se presenta el listado de las plataformas Blockchain y la evaluación del cumplimiento de características:

Tabla 17. Evaluación de cumplimiento de características por Blockchain

Plataforma Blockchain	Open Source	Privada Autorizada	Soporte contratos inteligentes	Diseñada para uso corporativo	Totales
Corda	1	1	1	1	4
Hyperledger Fabric	1	1	1	1	4
Multichain	1	1	1	0	3
Quorum	1	1	1	0	3

Fuente: Elaboración propia

Una vez se hizo la evaluación, se obtuvo como resultado que de las cinco plataformas Blockchain evaluadas, dos (2) cumplen con todos los criterios definidos para el proyecto; lo cual quiere decir que las dos plataformas son aptas para ser utilizadas en el proyecto, por

lo cual, para seleccionar una, fue necesario tener en cuenta la experiencia de los investigadores en la implementación de proyectos usando la plataforma; dado lo anterior, fue seleccionada la plataforma Hyperledger Fabric como herramienta a ser utilizada en el proyecto.

Tabla 18. Descripción y características generales de las Blockchain evaluadas

Blockchain	Descripción	Tipo	Descentralizado	Protocolo	Minería
Ethereum	Ethereum es una tecnología que le permite validar las transacciones que se hacen a través de la cadena de bloques de un modo muy ágil, descentralizado y seguro. También potencia aplicaciones que cualquiera puede usar y nadie puede derribar.	Publico	Si	PoW	si
Ripple	La plataforma Ripple es un protocolo de código abierto que está diseñado para permitir transacciones rápidas y baratas. También conocido como XRP, es un sistema de cambio local o procesador de pagos en sí mismo.	Publico	No	RPCA	Pre minado

	La utilidad del protocolo XRP es conectar los sistemas de pago tradicionales y alternativos en una sola red.				
Cardano	Cardano es una plataforma pública de Blockchain de naturaleza descentralizada. Está desarrollada como Open Source, por lo que una amplia comunidad le da respaldo. Utiliza la prueba de participación (Proof of Stake) como protocolo de consenso.	Privada	Si	Proof of Stake	No
Stellar	Stellar (XLM) es un protocolo parcialmente descentralizado cuya funcionalidad permite el intercambio de Bitcoins o Ether por su criptomoneda Lumen (XLM).	Público y Privada	Si	FBA, SCP	No

Hyperledger Fabric	Hyperledger Fabric es una plataforma de código abierto, probada, de nivel empresarial y distribuida. Tiene controles de privacidad avanzados, por lo que solo los datos que se desea compartir se comparten entre los participantes de la red "con permisos" (conocidos).	Privada	Si	CTF,BFT	si
EOS	EOS es una plataforma Blockchain diseñada para habilitar el escalamiento vertical y horizontal de aplicaciones descentralizadas. Esto se logra a través de un constructo tipo sistema operativo sobre el cuales pueden construir aplicaciones. En este sentido, EOS es similar a Ethereum.	Publico	Si	DPoS,aBFT	No

Corda	Corda es una plataforma de Blockchain privada autorizada que permite a las empresas realizar transacciones directamente y en estricta privacidad entre sí mediante contratos inteligentes. En esta plataforma, a diferencia de las cadenas de bloques públicas, las transacciones son privadas solo para las partes incluidas en la transacción.	Privada	Si	CorDapp,PoW	No
Tron	TRON es una plataforma de cadena de bloques, descentralizada de código abierto. con más rápido crecimiento y destaca entre la multitud porque tiene su propia plataforma de contenido descentralizada de igual a igual. TRON se posiciona como la red pública con más rápido	Publico	Si	P2P,DPoS	No

	crecimiento en el mundo. Utiliza tecnología peer-to-peer (P2P) y prueba de participación delegada (DPoS) como mecanismo de consenso.				
Multichain	Multichain se refiere a una bifurcación de código abierto de bifurcación extendida de Bitcoin. Esta tecnología puede emplearse para soportar Blockchain personalizados, ya sean públicos o privados. Además, promete simplicidad cuando se trata de configuración, asimismo proporciona una buena selección de características y mejoras dirigidas a usuarios empresariales.	Publico o privado	Si	CRP	No

Hyperledger Sawtooth	Hyperledger Sawtooth. Es un framework modular que nos permitirá crear y ejecutar Blockchain altamente configurables. Dispone de un consenso propio denominado PoET y ejecución de Smart Contract en diferentes lenguajes. Uno de sus puntos fuertes es la creación de pruebas de concepto para trazabilidad.	Privada	Si	PoET	si

Quorum	Quorum utiliza un algoritmo de consenso basado en la votación y logra la privacidad de los datos mediante la introducción de un nuevo identificador de transacción "privado". Uno de los objetivos de diseño de Quorum es reutilizar tanta tecnología existente como sea posible, minimizando los cambios necesarios para ir a Ethereum a fin de reducir el esfuerzo necesario para mantenerse sincronizado con futuras versiones del código base público de Ethereum.	Privada	Si	stanbul BFT,Raft Consensus	si

Fuente: Elaboración propia

3.2.2.1. Descripción general de la Blockchain seleccionada

- ¿Qué es Hyperledger Fabric?: Hyperledger Fabric es una plataforma de libro mayor abierta, probada, de nivel empresarial y distribuida. Tiene controles de privacidad

avanzados, por lo que solo los datos que se desea compartir se comparten entre los participantes de la red "con permisos" (conocidos).

- Beneficios de Hyperledger Fabric:
    - Red con permisos: Establecer confianza descentralizada en una red de participantes conocidos en lugar en de una red abierta de participantes anónimos.
    - Transacciones confidenciales: Exponer solo los datos que desee compartir con las partes con las que desee compartirlos.
    - Arquitectura conectable: Adaptar el Blockchain a las necesidades del sector con una arquitectura conectable en lugar de un enfoque único.
    - Empiece fácilmente: Programar contratos inteligentes en los lenguajes con los que trabaje su equipo actualmente, en lugar de aprender arquitecturas y lenguajes personalizados.

- Otras ventajas de Hyperledger Fabric:
    - Diseño modular: Disponibilidad de módulos para diferentes usos, tales como contratos inteligentes, almacenamiento de registros, identidad, criptografía, consenso, políticas y comunicación.

- Plataforma extremadamente segura: Los protocolos, algoritmos y criptografía de Hyperledger se auditan con regularidad.
- Interoperable: Permite comunicarse con otros sistemas sin problemas.
- Criptomoneda-angosta: La red no necesita ninguna criptomoneda para funcionar.
- Soporte API de gama alta: Todas las API que proporcionan son capaces de manejar la interoperabilidad y le permitirán comunicarse con su sistema central desde una red y una aplicación de cliente externa.

3.3. Fase 3: Selección de la herramienta Big Data

Objetivo: Seleccionar una herramienta Big Data que permita analizar en tiempo real los logs generados por la Honeypot seleccionada en la fase 1.

3.3.1. Actividad 1: Creación de listado de herramientas Big Data a caracterizar

Se creó una lista con las herramientas Big Data mencionadas en sitios web especializados, foros de la comunidad y documentos académicos consultados a través de internet, de igual manera se agregaron a la lista las herramientas conocidas por los investigadores. Una vez

obtenido el listado inicial, se buscó información adicional de cada herramienta, y se seleccionaron solo aquellas que cumplieron con el requerimiento mínimo defino: herramientas Big Data open source.

A continuación, se presenta el listado de herramientas que cumplieron con el criterio mínimo y la URL de su sitio web.

Tabla 19. Evaluación de cumplimiento requerimiento mínimo herramientas Big Data

Herramienta Big Data	Open Source	URL
Apache Hadoop	Si	https://hadoop.apache.org/
MongoDB	Si	https://docs.mongodb.com/
ELK	Si	https://www.elastic.co/es/what-is/elk-stack
Apache Spark	Si	https://spark.apache.org/
Apache Cassandra	Si	https://cassandra.apache.org/_/index.html
Apache Storm	Si	https://storm.apache.org/
Apache Drill	Si	https://drill.apache.org/

Fuente: Elaboración propia

3.3.2. Actividad 2: Caracterización de herramientas Big Data

En la caracterización de las herramientas Big Data, se evaluó el cumplimiento de los tres criterios definidos en el proyecto: **Procesamiento en tiempo real**, **especializado en análisis de logs** y **nodo simple**.

A continuación, se presenta el listado de las herramientas Big Data y la evaluación del cumplimiento de características:

Tabla 20. Evaluación de cumplimiento de criterios herramientas Big Data

Herramienta Big Data	Procesamiento en tiempo real	Especializado en análisis de logs	Nodo simple	Totales
Apache Hadoop	0	0	0	0
MongoDB	1	0	0	1
ELK	1	1	1	3
Apache Spark	1	0	0	1
Apache Cassandra	1	0	1	2
Apache Storm	1	0	0	1
Apache Drill	0	0	1	1

Fuente: Elaboración propia

Como se puede observar la herramienta Big Data que obtuvo en mayor puntaje es ELK; por lo cual fue seleccionada como la herramienta a ser utilizada en el proyecto.

Tabla 21. Descripción y características generales de las herramientas Big Data evaluadas

Herramienta	Descripción	Características Básicas
Apache Hadoop	Es una estructura para componentes de software libre basada en Java, para programar aplicaciones distribuidas que manejen grandes volúmenes de datos, que permite fragmentar tareas de cálculo (jobs) en diferentes procesos y distribuirlos en los nodos de un clúster de ordenadores, de manera que trabajan en alta disponibilidad y manejando grandes volúmenes de Datos.	• Procesamiento distribuido. • Eficiente. • Económico. • Fácilmente escalable. • Tolerante a fallos. • Open source.
MongoDB	Es un sistema de base de datos NoSQL, orientado a documentos y de código abierto,0 guarda la estructura de los datos en documentos BSON con un esquema dinámico, lo que implica que no existe un esquema predefinido. Los elementos de los datos se denominan documentos y se guardan en colecciones. Una colección puede tener un número indeterminado de documentos.	• Open Sourse • Consultas ad hoc. • Indexación. • Replicación. • Balanceo de carga. • Almacenamiento de archivos. • Agregación. • Ejecución de JavaScript del lado del servidor.

ELK	Es la combinación de Elastic Search, Logstach y Kibana que se utiliza para proporcionar un enfoque integral en la consolidación, gestión y análisis de registros de las aplicaciones. ELK Stack simplifica la búsqueda y el análisis de datos al proporcionar información en tiempo real a partir de los datos de registro.	• Open Source • ElasticSearch: Almacena, busca e indexa los datos transformados de Logstash. • Logstash: Recopila los registros, los analiza y los transforma en datos. • Kibana: Usa Elasticsearch para explorar, visualizar y compartir la información.
Apache Spark	Apache Spark es un motor unificado de analíticas para procesar datos a gran escala que integra módulos para SQL, Streaming, aprendizaje automático y procesamiento de grafos.	• Open Source • Está integrado con Apache Hadoop. • Trabaja en memoria y en disco. • Proporciona APIs para Java, Scala, Python y R.
Apache Cassandra	Se trata de un software NoSQL distribuido y basado en un modelo de almacenamiento de «clave-valor», de código abierto que está escrita en Java. Permite grandes	• Open Source • Usa un modelo peer-to-peer. • Gran disponibilidad y tolerancia de partición.

	volúmenes de datos en forma distribuida. Por ejemplo, esta fue desarrollada originalmente para la plataforma Facebook.	• Compatible con el modelo de programación MapReduce de Google.
Apache Storm	Es un sistema de computación en tiempo real distribuido para el procesamiento de grandes volúmenes de datos de alta velocidad. Storm es extremadamente rápido y puede procesar más de un millón de registros por segundo y por nodo en un clúster de tamaño normal. Storm se integra con YARN mediante Apache Slider. YARN administra Storm y también tiene en cuenta los recursos del clúster para los componentes de gobernanza de datos, seguridad y operaciones de una arquitectura de datos moderna.	• Open Source • Rápido: en los análisis de referencia procesa un millón de mensajes de 100 bytes por segundo y por nodo. • Escalable: con cálculos en paralelo que se ejecutan a través de un clúster de equipos. • Tolerante a fallos: cuando un nodo de trabajo deja de funcionar, Storm lo reinicia automáticamente. • Fiable: Storm garantiza que cada unidad de datos (tupla) se procese al menos una vez o exactamente una vez. Los

		mensajes solo se reproducen cuando hay fallos. • Fácil de usar: las configuraciones estándar sirven para la producción desde el primer momento.
Apache Drill	Es un motor de consultas SQL para ser utilizado en entornos Big Data (Hadoop-HDFS, HBase, Hive, MongoDB…) con una baja latencia, sin necesidad de tener definido un esquema de datos previo y permitiendo combinar en una única consulta, datos de distintas fuentes y Bases de datos relacionales o no Relacionales.	• Open Source • Alto rendimiento y baja latencia en ejecución de consultas. • No necesita metadatos centralizados. • No es necesario definir y mantener las tablas, vistas o relaciones entre datos. • Ejecución dinámica de consultas sin necesidad de que haya definido un esquema de datos.

Fuente: Elaboración propia

3.3.2.1. Descripción general de la herramienta Big Data Seleccionada

- ¿Qué es ELK?: ELK es la sigla de tres proyectos open Source: Elasticsearch, Logstash y Kibana donde cada uno de ellos cumple con una tarea especifica: **Elasticsearch** es un motor de búsqueda y analítica. **Logstash** es un pipeline de procesamiento de datos del lado del servidor que ingesta datos de una multitud de fuentes simultáneamente, los transforma y luego los envía a un "escondite", como Elasticsearch. **Kibana** permite a los usuarios visualizar los datos en cuadros y gráficos con Elasticsearch. Se utiliza para proporcionar un enfoque integral en la consolidación, gestión y análisis de registros de las aplicaciones, simplificando la búsqueda y el análisis de datos al proporcionar información en tiempo real a partir de los datos de registro [37].
- Ventajas de ELK [38]
    - Potencia: Ofrecer mucha funcionalidad con un bajo costo técnico, las configuraciones son mínimas para empezar. Las optimizaciones disponibles son amplias.
    - Escalabilidad: Elasticsearch es una herramienta diseñada para manejar terabytes de datos sin ningún problema. Su arquitectura le permite expandirse de forma rápida y fácil.
    - Flexibilidad: La configuración es flexible y puede adaptarse a cualquier necesidad y entorno.
    - Apertura: Elastic fomenta un ecosistema de extensiones (plugins) alrededor de sus herramientas que han creado un número

importante de funcionalidades extras y gratuitas para facilitar el trabajo con ellas.

- Código Abierto: Hoy en día el código abierto ofrece ventajas competitivas sobre otras plataformas porque permite la rápida corrección de errores gracias a la comunidad, la creación de extensiones e incluso incremente la base de usuarios al permitir utilizar las herramientas sin requerir pago alguno, lo que incrementa el conocimiento compartido de las herramientas.

3.4. Fase 4: Definir estrategia de fortalecimiento del modelo de gestión de incidentes

Objetivo: Proponer una mejora a un modelo de gestión de incidentes de seguridad, que permita, mediante el conocimiento de los vectores de ataque usados para explotar las vulnerabilidades de un activo, generar de manera proactiva controles que mitiguen los incidentes de seguridad informática antes que estos se materialicen en los ambientes productivos de la compañía.

Se cotejaron las normas **ISO/IEC 27035 – 1 y 2** (Tecnología de la información - Técnicas de seguridad - la información de gestión de incidentes de seguridad – parte 1, principios y parte 2, directrices para planificar y prepararse para la respuesta a incidentes, 11/01/2016), **NIST SP 800-61 Rev. 2** (Computer Security Incident Handling Guide, Agosto 2012), **ISO IEC 27001 – 2013 capitulo 16** (A16 Gestión de incidentes de la seguridad de la información) y **MINTIC** (Guía para la Gestión y clasificación de Incidentes de Seguridad

de la Información, 6/11/2016); con el fin de entender sus fases y actividades, y seleccionar aquellas que puedan ser utilizadas y/o potenciadas como parte de la propuesta de mejora del modelo.

3.4.1. Actividad 1: Cotejamiento de los modelos y guías de gestión de incidentes de seguridad informática.

A continuación, se presenta un breve resumen de cada uno de los modelos y las etapas que lo conforman, esto, con el fin de tener un mejor entendimiento de cada uno y poder seleccionar las partes que pueden ser utilizadas y/o potenciadas en el diseño de la mejora objeto del presente trabajo de investigación. La actividad de cotejamiento se dividió en tres subactividades: 1) Revisión y resumen de las normas, modelos y guías, 2) Análisis y conclusiones de la revisión de las normas, modelos y guías y 3) Cotejamiento de las normas, modelos o guías seleccionadas.

3.4.1.1. Revisión y resumen de las normas, modelos y guías

A continuación, se presenta un breve resumen de cada uno de los modelos, normas y guías y las fases y actividades que lo conforman, esto, con el fin de tener un mejor entendimiento de cada uno y poder seleccionar las partes que pueden ser utilizadas y/o potenciadas en el diseño de la mejora objeto del presente trabajo de investigación:

a. NIST SP 800-61 Rev. 2

El modelo de gestión de incidentes NIST SP-800-61 tiene como objetivo el proporcionar pautas que le permitan a las organizaciones responder de manera efectiva para mitigar los riesgos de los incidentes de seguridad informática. El modelo entrega los elementos

necesarios la lograr la detección, análisis, priorización y manejo de los incidentes; así como para el establecimiento de un programa de gestión de incidentes de seguridad [20].

El modelo contempla un ciclo de vida compuesto por las fases: preparación; detección y análisis; contención, erradicación y recuperación y finalmente actividades pos incidentes; cada una de las fases tiene un objetivo específico y se llevan a cabo de forma cíclica.

Figura 2 Fases ciclo de vida del modelo de gestión de incidentes NIST SP800-61

Fuente [20]

Fase de preparación

La fase de preparación tiene inmersas dos actividades; la primera es la preparación para manejar incidentes e implica el establecimiento de las capacidades necesarias para que el equipo de respuesta a incidentes responda de manera efectiva ante los incidentes, así como también la definición y selección de las herramientas necesarias para lograrlo; la segunda, es la prevención de incidentes; la cual lleva a seleccionar e implementar los controles necesarios que permitan limitar el número de incidentes de seguridad que se presentarán, y los cuales deben ser seleccionados con base en el análisis de la evaluación de riesgos [20].

- Preparación para manejar incidentes: Durante la preparación para manejar incidentes, el equipo de respuesta selecciona las herramientas y los recursos necesarios para el manejo de los incidentes; el modelo NIST SP 800-61 los agrupa en cuatro categorías: comunicaciones y facilidades, hardware y software de manejo de incidentes, recursos de análisis de incidentes, y software de mitigación de incidentes. La selección de los recursos y herramientas apropiadas es fundamental para tener una respuesta efectiva ante los incidentes.
- Prevención de incidentes: Si bien el equipo de respuesta a incidentes no es responsable por la prevención de incidentes, sus aporten en materia de evaluación de riesgos e identificación de brechas, conduce a hacer que el número de incidentes sea bajo, lo que finalmente se traduce en una mejor respuesta a incidentes. Para la prevención de riesgos es importante llevar a cabo prácticas que ayuden a proteger la infraestructura y las aplicaciones. Algunas de las prácticas recomendadas incluyen actividades como la evaluación de riesgos, seguridad del host, seguridad de las redes, prevención de Malware, y sensibilización y formación a los usuarios finales [20].

Fase de detección y análisis:

La fase de detección y análisis aborda la importancia que tiene para las organizaciones estar preparadas para manejar incidentes que utilizan vectores de ataque comunes y la necesidad de desarrollar procedimientos de manejo más específicos [20]. Se resalta la necesidad de que el equipo tenga la capacitación necesaria que le permita afrontar cualquier tipo de incidente, teniendo en cuenta que los incidentes que se pueden presentar en una organización son muy variados.

De igual forma, se aborda la necesidad de reconocer las señales que permiten detectar los incidentes. Estas señales están divididas en dos categorías: las señales precursoras y las indicadoras. Las señales precursoras, son aquellas que indican que un incidente puede llegar a presentarse en un futuro cercano; y las indicadoras, son aquellas que indican que un incidente ya se presentó o está en curso dentro de la organización. El análisis de las señales por parte de un equipo altamente experimentado facilitará la tarea de detección y permitirá que se tomen decisiones apropiadas. Una vez el equipo de manejo de incidentes sospecha o determina que efectivamente ha ocurrido o está ocurriendo un incidente, es necesario que se disparen actividades tendientes a documentarlo, priorizarlo (en caso de que se presenten varios al mismo tiempo) y notificar a las personas adecuadas la ocurrencia.

Fase de contención, erradicación y recuperación

La contención permite evitar que un incidente sobrepase los recursos y cause más daño. Las estrategias de contención varían de acuerdo con el tipo de incidente, el daño potencial que pueden causar, los sistemas o elementos afectados, la necesidad de preservar evidencias, entre otros [20]. En algunos casos, el equipo de respuesta puede decidir que la mejor estrategia de contención es utilizar un Sandbox; este les permite monitorear la actividad e identificación del atacante, recopilar información que les ayude en la mitigación o para ser utilizada en caso de iniciar acciones legales, en cuyo caso, es necesario que toda la evidencia se obtenga siguiendo procedimientos que cumplan la ley y las regulaciones a fin de asegurar que serán admitidos en los tribunales [20].

Luego que el equipo ha logado contener el incidente, se deben iniciar las actividades de erradicación y recuperación, las cuales contemplan entre otras, la identificación de los nodos

afectados, las cuentas de usuarios violadas y las vulnerabilidades explotadas; al igual que la restauración de los sistemas o elementos afectados para devolverlos a su estado de operación normal [20].

Fase de actividades post incidente

Las actividades post incidentes le permiten al equipo de respuesta darles cierre a los incidentes [20] de seguridad. Las actividades post incidentes se componen básicamente de las lecciones aprendidas, uso de datos de incidentes recopilados y la retención de pruebas.

- Lecciones Aprendidas: En las reuniones de lecciones aprendidas participan todos los miembros de equipo, y aquellas personas que de una u otra forma están involucradas con el incidente y pueden aportar información; en ellas, el equipo intenta dar respuesta a preguntas que le permitan entender lo sucedido, se analizan los precursores y los indicadores y se determina cuáles de estos deben ser vigilados en el futuro para evitar incidentes similares; de igual forma el equipo analiza su desempeño y si las decisiones y acciones efectuadas fueron las apropiadas o si por el contrario se debieron hacer las cosas de una manera diferente.

  Otro de los beneficios que trae la realización de reuniones de lecciones aprendidas, es que la información que se recolecta en ellas puede ser utilizada para capacitar a los miembros menos experimentados del equipo, al igual que la actualización de las políticas y procedimientos de respuesta a incidentes [20]. Una vez se ha llevado a cabo la reunión de lecciones aprendidas, el equipo debe crear un informe de los incidentes analizados, este puede ser utilizado en el futuro para darle un adecuado manejo a incidentes similares.

- **Uso de datos de incidentes recopilados**

El principal objetivo para la recolección de datos es la creación de una base de conocimiento que le permita a la organización mediante su análisis obtener información valiosa para la toma de decisiones futuras.

Los datos recolectados durante las actividades post incidentes le permitirán a la organización justificar las partidas presupuestarias solicitadas por el equipo de respuesta a incidentes, encontrar vulnerabilidades y amenazas que, luego de incluirlos en un proceso de evaluación de riesgos, permitirán definir e implementar controles y obtener métricas como el número de incidentes gestionados, tiempo por incidente, evaluación objetiva de cada incidente, evaluación subjetiva de cada incidente.

- **Retención de pruebas**

Las organizaciones deben crear una política en la cual defina el tiempo que se conservaran las pruebas recolectadas durante los incidentes. El modelo de gestión de incidentes NIST SP800-61 define tres factores que deben ser tenidos en cuenta en la creación de la política: enjuiciamiento, retención de datos y costos.

b. ISO/IEC 27035 – 1 y 2

El modelo de gestión de incidentes ISO 27035:2011 tiene como objetivo brindar orientación sobre la gestión de incidentes de información y las vulnerabilidades de la seguridad de la información mediante la definición de controles efectivos para lograr la reducción o mitigación de los impactos derivados de estos incidentes. Para ello, propone 5 fases: Planificación y preparación, detección y reporte, evaluación y decisión, respuestas, y lecciones aprendidas [25].

Figura 3 Fases ciclo de vida del modelo de gestión de incidentes ISO 27035

Fuente [25]

Fase de planificación y preparación

La fase de planificación y preparación tiene como objetivo lograr que la organización pueda mediante la ejecución de una serie de actividades, poner en uso un esquema eficaz y eficiente de la gestión de eventos, incidentes y vulnerabilidades de seguridad de la información; dentro del listado presentado, una de las actividades más importantes es la generación de la política de gestión de eventos/incidentes/vulnerabilidades de seguridad de la información; y como parte fundamental de esta actividad, se debe lograr que la dirección de la compañía conozca, avale y se comprometa con el esquema de gestión [21].

Otras actividades contempladas en la fase de planificación y preparación son: actividades para la revisión y actualización constante de las políticas de gestión de riesgos y de seguridad de la información, actividades para la creación de formularios de registro de eventos e incidentes y para definir los procedimientos y acciones asociadas con el uso de formatos, actividades para definir el equipo de respuesta a incidentes, al igual que sus procedimientos operativos y listado de personas que lo componen con su respectivo rol y las responsabilidades asignadas, actividades que permitan tener relaciones y comunicación con entidades internas y externas que estén relacionadas con la gestión de eventos e incidentes

de seguridad de la información, actividad para establecer, implementar y operar mecanismos técnicos que den soporte al esquema y permita disminuir la posibilidad de que ocurran incidentes, actividades para crear y fomentar programas de formación sobre eventos e incidentes de seguridad a fin de lograr que todos los funcionarios de la organización entiendan que la seguridad es responsabilidad de todos, y finalmente, actividades que permitan poner a prueba el esquema de gestión de eventos e incidentes de seguridad [21].

Fase de detección y reporte

La fase de detección y reporte es la primera del uso operativo del esquema de gestión de incidentes de seguridad de la información; en esta fase la ISO 27035:2011 contempla tres actividades clave: la detección de los eventos de seguridad de la información, la recolección de la información sobre el evento, y el reporte de los eventos. Otra de las actividades consideradas de gran importancia dentro de la fase, es la detección de vulnerabilidades que aún no hayan sido explotadas.

La detección de eventos o vulnerabilidades puede provenir de fuentes humanas, como personal interno o clientes, o de los diferentes sistemas automáticos desplegados en la organización, entre los cuales pueden estar los sistemas de detección de intrusos (IDS), sistemas de prevención de intrusos (IPS), correlacionadores de eventos (SIEM) o los Honeypots, de alertas generadas por firewalls, de eventos escalados por el área de TI o la mesa de ayuda, entre otros. En todos los casos y sin importar la fuente por la cual fue reportado el evento, la ISO 27035 contempla actividades que permitan recolectar y registrar información sobre los eventos, al igual que toda la evidencia electrónica y las decisiones tomadas respecto de este, el escalamiento llevado a cabo y el seguimiento de los eventos.

Toda la información recolectada y registrada debe ser idealmente almacenada en una base de datos de eventos/incidentes y vulnerabilidades gestionadas por el equipo de respuesta a incidentes, dicha información será utilizada para tomar decisiones y para análisis posterior [21].

Fase de evaluación y decisión

Esta fase es la segunda del uso operativo del esquema de gestión de incidentes de seguridad la información; durante esta fase se evalúa la información recolectada y almacenada relacionada con los eventos y se determina si es un evento o un incidente de seguridad de la información. Al igual que en la fase anterior, la ISO 27035:2011 contempla una serie de actividades clave que deben llevarse a cabo.

La primera de las actividades corresponde con la evaluación que debe hacer el punto de contacto (POC) para evaluar y determinar si un evento es un incidente de seguridad en progreso o finalizado y si es necesario escalarlo, o si se trata de una falsa alarma. Para la evaluación de los eventos de seguridad se debe contar con una escala previamente definida para la clasificación en la cual debe tenerse en cuenta el posible impacto con base en los activos. Otras actividades contempladas en esta fase incluye las evaluaciones que debe efectuar el equipo de respuesta a incidentes para confirmar los resultados obtenidos por el POC, para lo cual, si así se determina, puede efectuarse una segunda evaluación usando la escala de clasificación y finalmente definir el tratamiento apropiado, la priorización y las personas que deben tratar el incidente, así como actividades que aseguren todas las personas involucradas en el manejo de incidentes registrarán adecuadamente las actividades ejecutadas para su análisis posterior.

Fase de respuestas

La fase de respuesta es la tercera del uso operativo del esquema de gestión de incidentes de seguridad la información; esta fase involucra dar respuesta de manera inmediata, en tiempo real o casi real a los incidentes, de acuerdo con las decisiones tomadas en la fase de evaluación y decisión [21]. La ISO 27035 contempla una serie de actividades clave que deben ser garantizadas por la organización.

Entre otras, las actividades recomendadas por la ISO 27035 involucran la activación de la respuesta por parte del equipo de respuesta a incidentes; dichas respuestas dependerán de si el incidente se encuentra bajo control o no. Para incidentes bajo control la respuesta puede ser iniciar el proceso de recuperación, para incidentes no controlados o que tendrán un gran impacto, puede ser iniciar los procedimientos de manejo de crisis, actividades para iniciar análisis forense, actividades para asignación de recursos, actividades para escalamiento del incidente, actividades tendientes a recolectar y almacenar de manera segura y apropiada evidencia electrónica, actividades para asegurar que el control de cambios actualiza los reportes de incidentes y finalmente actividades para comunicar a personas y organizaciones internas y externas la existencia del incidente. Una vez el incidente de seguridad es tratado exitosamente, es necesario dar un cierre formal a este, para ello se debe registrar el incidente en la base de datos de gestión de incidentes de seguridad de la información, al igual que tratar las vulnerabilidades y registrar la información respecto a las mismas [21].

Fase de lecciones aprendidas

La fase de lecciones aprendidas es la cuarta del uso operativo del esquema de gestión de incidentes de seguridad de la información; la fase de lecciones aprendidas se inicia una vez los incidentes han sido solucionados y cerrados, busca generar conocimiento y dar madurez al equipo de respuesta, partiendo de la forma como se manejaron los eventos, vulnerabilidades e incidentes. Al igual que las fases anteriores, la ISO 27035 contempla una serie de actividades clave que deberían ser aseguradas por la organización [21].

Las actividades de lecciones aprendidas involucran validar la eficacia de los procesos, procedimientos, formatos y formularios utilizados durante el tratamiento de los incidentes y el tratamiento de las vulnerabilidades de seguridad de la información, con el objetivo de implementar mejoras al esquema de gestión, que permita mejorar la respuesta y recuperación, así como también llevar a cabo análisis forense e identificar las lecciones aprendidas, y llevar a cabo la actualización de la base de datos de eventos/vulnerabilidades e incidentes [21].

c. ISO / IEC 27035-2, directrices para planificar y prepararse para la respuesta a incidentes

Describe cómo planificar y prepararse para la respuesta a incidentes. Esta parte comprende el “Plan” y preparar las fases “lecciones aprendidas” del modelo presentado en la norma ISO / IEC 27035-1.

d. ISO IEC 27001 2013 - A16 Gestión de incidentes de la seguridad de la información

El capítulo 16 de la norma ISO 27001, está dedicado al establecimiento de controles para la gestión de incidentes de seguridad de la información. El capítulo 16 tiene como objetivo la

gestión de incidentes y mejoras de seguridad de la información y este compuesto por las siguientes actividades o procedimientos:

- 16.1.1 Responsabilidades y procedimientos.
- 16.1.2 Reporte de eventos de seguridad de la información.
- 16.1.3 Reporte de debilidades de seguridad de la información.
- 16.1.4 Evaluación y decisión sobre los eventos de seguridad de información.
- 16.1.5 Respuesta a incidentes de seguridad de la información.
- 16.1.6 Aprendiendo de los incidentes de seguridad de la información.
- 16.1.7 Recolección de evidencia.
- El capítulo 16 contempla las siguientes actividades para la resolución de incidentes:

Figura 4. Pasos para la resolución de incidentes

Fuente: ISO 27001

e. MINTIC: Guía para la Gestión y clasificación de Incidentes de Seguridad de la Información

La guía Mintic contempla 5 fases: Planificación y preparación, detección y reporte, evaluación y decisión, respuestas, y lecciones aprendidas; En el desarrollo de la presente

guía se incorporaron componentes definidos por el NIST alineados con los requerimientos normativos de la NTC–ISO–IEC 27001-2013 en su numeral 16 para la estrategia de Gobierno en Línea.

Figura 5 Fases del ciclo de vida de la guía Mintic

Fuente: [39]

Fase de preparación

Contempla todos los elementos necesarios para la implementación de un modelo de gestión de incidentes que permita a la organización desarrollar la capacidad de responder ante los incidentes de seguridad, así como también la capacidad para para detectar y evaluar las vulnerabilidades de forma que se garantice que todos los sistemas y la infraestructura corporativa es segura, previniendo así la ocurrencia de incidentes de seguridad.

En la etapa de preparación el equipo de respuesta a incidentes debe velar por que se cuente con los recursos necesarios para la adecuada atención de incidentes de seguridad; esto incluye herramientas de hardware y software y recursos de comunicación, así como los procedimientos necesarios para todas las etapas y la capacitación al equipo de respuesta.

Fase de detección y análisis

La fase de detección y análisis presenta la importancia de contar con elementos que permitan identificar y analizar eventos que indiquen que un incidente ha ocurrido o está por ocurrir; la identificación y gestión de dichos eventos permiten que la organización pueda prepararse para mitigar el impacto de la ocurrencia de un incidente de seguridad. Otros procesos contemplados en la fase de detección y análisis son:

- **La evaluación de los incidentes de seguridad:** Busca determinar el nivel de severidad de los incidentes de seguridad teniendo en cuenta los niveles de impacto basado basados en el análisis de riesgos y la clasificación de los activos.
- **La clasificación de los incidentes de seguridad:** Busca determinar el tipo de incidente de seguridad; la clasificación es diferente en cada organización, depende de su infraestructura, su apetito de riesgo, de la clasificación de sus activos entre otras, entre las clasificaciones que pueden presentarse están entre otras: Acceso no autorizado, modificación de recursos, indisponibilidad de recursos.
- **Priorización de los incidentes y tiempos de respuesta:** El nivel de prioridad de cada incidente permite determinar los tiempos máximos para su atención de acuerdo a su criticidad e impacto; para determinar la prioridad de los incidentes que utilizan variables como Prioridad, criticidad de impacto, impacto actual, impacto futuro, entre otras; el nivel de prioridad se determina utilizando la siguiente formula:

Nivel Prioridad = (Impacto actual * 2,5) + (Impacto futuro * 2,5) + (Criticidad del Sistema * 5)

- **Declaración y notificación de incidentes:** La notificación de los incidentes permite al equipo de respuesta a incidentes responder ante estos de forma sistemática y minimizar su ocurrencia, facilitar una recuperación rápida y eficiente de las actividades, minimizando la pérdida de información y la interrupción de los servicios, el proceso de tratamiento de incidentes, y manejar correctamente los aspectos legales que pudieran surgir durante este proceso. La notificación de los incidentes puede provenir de personas internas o externas y puede hacerse utilizando cualquier medio para efectuarse, la organización debe contar con un formulario que debe ser diligenciado por la persona que notifica sobre el incidente para que la persona encargada determine el tipo de incidente y trasmita la información para que se inicie el tratamiento de este.

Fase de contención, erradicación y recuperación

La fase de contención, erradicación y recuperación contempla la implementación de estrategias que permitan minimizar el impacto, disminuir la propagación y los daños causados por los incidentes de seguridad. Esta fase se divide en tres partes:

- **Contención**: Busca que el incidente no se propague y cause más daños en la infraestructura de la organización; para que la contención sea eficaz, se debe contar con una estrategia de contención previamente definida, dicha estrategia varía de acuerdo con el tipo de incidente.
- **Erradicación y recuperación:** Busca eliminar todo rastro dejado por el incidente en los sistemas afectados, una vez se ha erradicado el incidentes se da paso al proceso de recuperación, el cual busca dejar los sistemas afectados en el estado óptimo de

funcionamiento, en muchos casos el proceso de recuperación requiere la activación del DRP (plan de recuperación de desastres) o el BCP (plan de continuidad del negocio), esto generalmente ocurre cuando la afectación causada por el incidente en un sistema es grave.

Fase de actividades post incidentes

La fase de actividades post incidentes es una de las partes más importantes dentro del ciclo de vida de los modelos y guías de gestión de incidentes de seguridad. Esta fase contempla la generación de reportes sobre el incidente, la generación de lecciones aprendidas, la generación de controles, la aplicación de medidas disciplinarias y penales y el registro de todos los eventos y acciones tomadas durante la gestión del incidente para la generación de la base de conocimiento que permita prevenir y mejorar la respuesta ante incidentes futuros.

3.4.1.2. Análisis y conclusiones de la revisión de las normas, modelos y guías

A continuación, se presenta un breve análisis a modo de conclusión sobre cada uno de los tres referentes anteriormente descritos:

a) La Guía Mintic para la gestión y clasificación de incidentes de seguridad de la información, fue elaborada mediante la recopilación de aspectos relevantes de los documentos NIST (National Institute of Standards and Technology (Computer Security Incident Handling Guide) y lineamientos y buenas prácticas presentados en la norma ISO IEC 27001 – 2013 capitulo 16.

b) NIST SP 800-61 Rev. 2, De acuerdo con la norma, el primer paso para lograr una adecuada gestión de incidentes de seguridad es definir de manera clara qué es para la

organización un “incidente”. La norma busca entregar a la organización las pautas necesarias para que la gestión de los incidentes de seguridad sea el más apropiado; en ese sentido recomienda establecer capacidades de respuesta, políticas de respuesta a incidentes, un plan de RI, procedimientos, mecanismos para compartir información, estructura de equipo e incluso colaboración con grupos externos; teniendo en cuenta lo anterior, se concluye que el enfoque de la norma es la gestión de los incidentes una vez estos se han materializado. La norma es útil para el presente trabajo pues proporciona un enfoque reactivo ante los incidentes, lo cual brinda la oportunidad de construir un nuevo procedimiento con enfoque preventivo.

c) ISO IEC 27001 – 2013 capitulo 16, capítulo dedicado al establecimiento de controles para la gestión de incidentes de seguridad, incluyendo la comunicación de eventos de seguridad y debilidades; el capítulo responde a los objetivos: detectar, responder, reportar y aprender; en ese sentido el enfoque del capítulo es la gestión de los incidentes una vez se están o se han presentado.

d) ISO/IEC 27035 – 1 y 2, La guía se centra en entregar las pautas para localización, análisis y evaluación de vulnerabilidades e incidentes a los que puede estar expuesta una organización, lo cual les permite definir controles efectivos para actuar frente a los incidentes de seguridad informática y, por consiguiente, en la reducción o mitigación de los impactos derivados de estos incidentes. La guía es útil para el presente trabajo de investigación, debido a que no se centra en gestionar los incidentes de seguridad, sino que también se ocupa de las posibles vulnerabilidades que pueda tener la organización.

De acuerdo con la estructura de cada una de las normas anteriormente analizadas, se concluye que estas tienden a ser reactivas, pues se aplican una vez el incidente de seguridad de la información se ha materializado.

Con base en el análisis anteriormente expuesto, se concluye que los modelos **ISO/IEC 27035 – 1 y 2** (Tecnología de la información - Técnicas de seguridad – Gestión de incidentes de seguridad de la información – parte 1, principios y parte 2, directrices para planificar y prepararse para la respuesta a incidentes, 11/01/2016), **NIST SP 800-61 Rev. 2** (Computer Security Incident Handling Guide, Agosto 2012), se utilizarán como línea base en el desarrollo de la mejora al modelo de gestión de incidentes de seguridad, el cual tuvo como característica principal la gestión de incidentes de seguridad de la información proactiva, es decir, la gestión de incidentes de seguridad en ambientes no productivos (ambientes señuelo) para utilización de la información recolectada de los estos incidentes a fin de definir controles que permitan mitigar su materialización en ambientes productivos.

3.4.1.3. Cotejamiento de las normas seleccionadas

De acuerdo en lo definido en la Metodología, en la tabla 19 se presentan las fases y actividades clave de los referentes seleccionados que se utilizaran como línea base le aportan al trabajo de investigación y que por consiguiente fueron seleccionados para ser utilizados como punto de partida en la creación de un modelo con enfoque preventivo ante incidentes de seguridad de información:

Tabla 22. Cotejamiento de los modelos de gestión de incidentes de seguridad seleccionados

ISO/IEC 27035 – 1 y 2		NIST SP 800-61 Rev. 2	
Fase	Actividades Clave	Fase	Actividades Clave
Planificación y preparación	✓ **Formular y generar una política de gestión de eventos, incidentes y vulnerabilidades de seguridad de la información y lograr el compromiso de la alta dirección con esa política** ✓ **Actualizar las políticas de gestión del riesgo y de seguridad de la información, a nivel corporativo y a niveles de sistemas, redes y servicios específicos.** ✓ **Definir y documentar un esquema detallado de gestión de incidentes de seguridad de la información** ✓ **Establecer el ISIRT, con un programa adecuado de formación**	Preparación	✓ **Preparación para manejar incidentes.** • **Crear listados con herramientas y recursos necesarios para el manejo de incidentes; los listados se pueden dividir en: i) Comunicaciones y facilidades. ii) hardware y software para manejo de incidentes, iii) recursos de análisis de incidentes, y iv) software de mitigación de incidentes.**

	diseñado, desarrollado y suministrado a su personal ✓ **Establecer y preservar relaciones y conexiones adecuadas con organizaciones internas y externas que están directamente involucradas en la gestión de eventos, incidentes y vulnerabilidades.** ✓ **Establecer, implementar y operar mecanismos técnicos y otro apoyo para brindar soporte al esquema de gestión de incidentes de seguridad de la información.** ✓ **Diseñar y desarrollar un programa de formación y de toma de conciencia en gestión de eventos, incidentes y vulnerabilidades.**		✓ **Implementar practicas recomendadas para revenir incidentes. i) evaluaciones de riesgo, ii) seguridad del host, iii) seguridad de la red, iv) prevención de malware, v) sensibilización y formación del usuario.**

	✓ **Probar el uso del esquema de gestión de incidentes de seguridad de la información, sus procesos y procedimientos.**		
Detección y reporte	✓ **Detectar y reportar la ocurrencia de un evento de seguridad de la información, o la existencia de una vulnerabilidad de la seguridad de la información.** ✓ **Recolectar información sobre un evento o vulnerabilidad de seguridad de la información.** ✓ **Asegurar que todos los involucrados en el PoC (Punto de Contacto) registren adecuadamente todas las actividades, resultados y decisiones relacionadas para análisis posterior.**	Detección y análisis	✓ **Definir procedimientos de manejo de incidentes específicos basados en los vectores de ataque.** ✓ **Determinar mediante el análisis de las señales de un incidente (precursoras e indicadoras): i) si se ha producido un incidente, ii) el tipo de incidente que se ha producido y iii)**

	✓ **Asegurar que se recolecta evidencia electrónica y se almacena en forma segura, y que se hace seguimiento continuo de su preservación segura, en caso de que se requiera para emprender acciones legales o acciones disciplinarias internas.** ✓ **Asegurar que el régimen de control de cambios se mantenga y cubra el seguimiento de los eventos y vulnerabilidades de seguridad de la información** ✓ **Escalar, según se requiera durante toda la fase, para revisión y/o decisiones posteriores.** ✓ **Registrar en un Sistema de Seguimiento de Incidentes.**		**la magnitud del problema.** ✓ **Documentar todos los hechos relacionados con el incidente.** ✓ **Priorizar el manejo de los incidentes de acuerdo con factores relevantes como: i) impacto funcional del incidente, ii) impacto en la información del incidente, iii) recuperación del incidente.**

			✓ **Notificar a las personas adecuadas para que todos los que deban participar desempeñen sus funciones; la política de manejo de incidentes debe especificar como mínimo i) qué se debe informar, ii) a quién y iii) en qué momento).**
Evaluación y decisión	✓ **PoC (Punto de Contacto) evalúa y determina si un evento es un incidente de seguridad de la información posible o concluido, o es una falsa alarma, y si no es una falsa alarma, si se requiere escalarlo.**	Contención, erradicación y recuperación	✓ **Seleccionar estrategia de contención.** ✓ **Definir los criterios de selección de la estrategia de contención.**

	✓ **Evaluación para confirmar los resultados de la evaluación del PoC (Punto de Contacto), ya sea que el evento sea o no un incidente de seguridad de la información, si es aplicable.** ✓ **Escalar, según se requiera durante toda la fase, para evaluaciones y/o decisiones posteriores** ✓ **Asegurar que todos los involucrados, particularmente el ISIRT, registran adecuadamente todas las actividades para análisis posterior** ✓ **Asegurar que se recolecta evidencia electrónica y se almacena en forma segura, y que se hace seguimiento continuo de su preservación segura, en caso de que se requiera para**		✓ **Recopilación y manipulación de pruebas.** ✓ **Identificación de los hosts atacantes:** • **Validación de la dirección IP del host atacante.** • **Investigación del host atacante a través de motores de búsqueda** • **Uso de bases de datos de incidentes.** • **Monitoreo de posibles canales de comunicación del atacante.**

	emprender acciones legales o acciones disciplinarias internas. ✓ **Asegurar que el régimen de control de cambios se mantenga y cubra el rastreo de incidentes de seguridad de la información y las actualizaciones de reportes de incidentes de seguridad de la información.** ✓ **Distribuir la responsabilidad por las actividades de gestión de incidentes de seguridad de la información, a través de la jerarquía de personal adecuada.** ✓ **Suministrar procedimientos formales que debe seguir cada persona notificada, incluida la revisión y corrección del reporte, la**		✓ **Erradicación y recuperación:** • **Eliminar el Malware.** • **Deshabilitar las cuentas de usuario violadas.** • **Identificar y mitigar todas las vulnerabilidades que fueron explotadas.** • **Identificar los hosts afectados dentro de la organización.** • **Restaurar los sistemas para que funcionen normalmente.** • **Confirmar que los sistemas funcionan**

	evaluación de daños y la notificación al personal pertinente. ✓ **Usar directrices para una documentación minuciosa de un evento de seguridad de la información.** ✓ **Uso de directrices para una documentación minuciosa de las acciones posteriores a un incidente de seguridad de la información.** ✓ **Actualización de la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información**		• **Corregir vulnerabilidades explotadas para evitar incidentes similares.** • **Restaurar sistemas a partir de copias de seguridad limpias.** • **Instalar parches.** • **Cambiar contraseñas.** • **Reforzar la seguridad del perímetro de la red.**
Respuestas	✓ **Revisión, por parte del ISIRT, para determinar si el incidente de seguridad de la información está bajo control (promover la respuesta requerida, si está bajo control o promover actividades de crisis al**	Actividades Post incidente	✓ **Lecciones Aprendidas:** • **Celebración de una reunión de**

	llevar el incidente a la función de manejo de crisis, si no está bajo control o si va a tener un impacto severo en los servicios esenciales de la organización). ✓ **Asignar recursos internos e identificar recursos externos para responder a un incidente.** ✓ **Llevar a cabo el análisis forense de seguridad de la información, según se requiera.** ✓ **Escalar el incidente, según se requiera, durante toda la fase, para revisiones o decisiones posteriores.** ✓ **Asegurar que todos los involucrados, particularmente el ISIRT, registran adecuadamente**		**"lecciones aprendidas" con todas las partes involucradas después de un incidente importante y, opcionalmente, periódicamente después de incidentes menores.** • **Actualización de las políticas y los procedimientos de respuesta a incidentes.** • **Creación de informe de seguimiento para cada incidente.** ✓ **Uso de datos recopilados de los incidentes:** • **Estudiar los registros de las**

	todas las actividades para análisis posterior. ✓ **Asegurar que se recolecta evidencia electrónica y se almacena en forma segura.** ✓ **Asegurar que el régimen de control de cambios se mantenga y cubra el rastreo de incidentes de seguridad de la información y las actualizaciones de reportes de incidentes de seguridad de la información.** ✓ **a comunicar la existencia del incidente de seguridad de la información o cualquier detalle pertinente de éste a otras organizaciones o personas internas o externas.**		**características de los incidentes.** • **Generación de métricas por cada incidente: i) número de incidentes majeados, ii) Duración de cada incidente, iii) evaluación objetiva y subjetiva de cada incidente, entre otras.** ✓ **Retención de evidencia:** • **Creación de política de retención de la evidencia recopilada sobre los incidentes.** ✓ **Lista de verificación de**

			manejo de incidentes: • **Diligenciar la lista de chequeo de manejo de incidentes por cada incidente.**
Lecciones Aprendidas	✓ **Llevar a cabo el análisis forense de seguridad de la información, según se requiera.** ✓ **Identificar las lecciones aprendidas de incidentes y vulnerabilidades de seguridad de la información.** ✓ **Revisar, identificar y hacer mejoras a la implementación de controles de seguridad de la información (controles nuevos y/o actualizados), al igual que la política de gestión de incidentes de seguridad de la información.**		

	✓ **Revisar, identificar, y si es posible, hacer mejoras a los resultados de la revisión por la dirección y la evaluación de riesgos para la seguridad de la información existentes, como resultado de las lecciones aprendidas.** ✓ **examinar cómo fue la eficacia de los procesos, procesos, formularios de reporte y/o la estructura organizacional para responder a la evaluación y recuperación de cada incidente de seguridad de la información y tratar las vulnerabilidades de seguridad de la información.** ✓ **actualizar de la base de datos de eventos / incidentes /**		

	vulnerabilidades de seguridad de la información. ✓ **Comunicar y compartir los resultados de la revisión dentro de una comunidad de confianza.**		

Fuente: Elaboración propia

3.4.2. Actividad 2: Construir mejora del modelo de gestión de incidentes a partir de los modelos y/o guías seleccionados

En esta actividad se construyó la mejora al modelo de gestión de incidentes de seguridad, partiendo del entendimiento de las normas ISO/IEC 27035 – 1 y 2 y NIST SP 800-61 Rev. 2; la mejora buscó lograr una gestión proactiva de los incidentes de seguridad de la información; es decir, la gestión de incidentes de seguridad en ambientes no productivos (ambientes señuelo) que permita utilizar la información recolectada de los estos incidentes en dichos ambientes, a fin de definir controles que permitan mitigar su materialización en ambientes productivos; para la mejora se parte de la premisa que los modelos ISO 27035 o NIST SP800-6 brindan orientación de cómo gestionar un incidente de seguridad una vez se ha materializado, es decir, la gestión o manejo reactivo a los incidentes de seguridad informática [40].

Para lograr que las fases y actividades construidas sean efectivas, se incorporó un componente activo, compuesto por herramientas que detectan y registran información de los

ataques que reciben las plataformas señuelo (Honeypot), así como también por herramientas que permiten analizar y almacenar la información generada durante los ataques (logs, Big Data y Blockchain).

Para el diseño y construcción del nuevo modelo de gestión de incidentes de seguridad de la información se tuvieron en cuenta los siguientes aspectos:

- Análisis y entendimiento de las fases y actividades clave de los modelos ISO 27035 y NIST SP 800-61.
- La importancia de la información arrojada por el componente activo en la definición de los controles y acciones.
- La definición, construcción y aplicación de acciones y controles que permitieron mitigar la materialización de incidentes de seguridad en ambientes productivos.

3.4.2.1. Fases del modelo de gestión de incidentes proactivo

a) Planificación y preparación
b) Levantamiento de información y reporte
c) Respuesta (Correlación de ataques, Definición de controles)
d) Implementación y evaluación de controles
e) Reporte y lecciones aprendidas

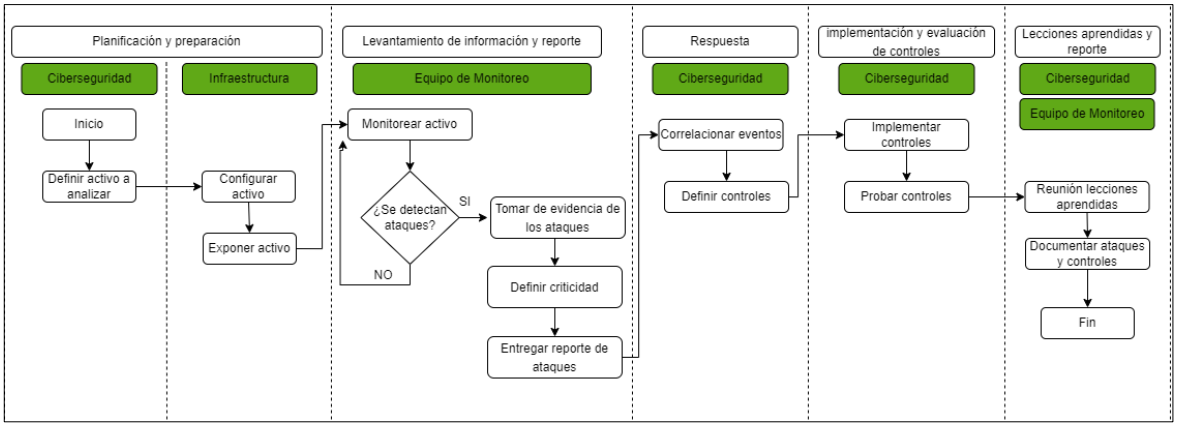
Figura 6. Fases del modelo de gestión de incidentes proactivo

Fuente: Elaboración propia

3.4.2.2. Roles y responsabilidades por fases

El siguiente diagrama muestra las actividades que se llevaron a cabo en cada una de las fases del modelo propuesto y el área responsable de su ejecución:

Figura 7. Actividades y sus responsables por fases



Fuente: Elaboración propia

- **Descripción de equipos y responsabilidades**

– Equipo de ciberseguridad: Tienen la responsabilidad de definir los activos de información que deben ser expuestos mediante la Honeypot a fin de identificar los

vectores de ataque utilizados para vulnerarlos y poder así definir e implementar controles que mitiguen sus vulnerabilidades.

- Equipo de infraestructura de ciber: Tienen la responsabilidad de administrar la(s) Honeypot(s) mediante la(s) cual(es) se exponen los activos.
- Equipo de monitoreo: Tienen la responsabilidad de monitorear los ataques que reciben los activos expuestos en la(s) Honeypots, definir su criticidad y reportarlos al equipo de ciberseguridad.

Figura 8. Matriz de roles y responsabilidades

	Ciberseguridad		Infraestructura		Monitoreo	
Tareas	Lider Ciberseguridad	Analistas de ciberseguridad	Lider Infraestructura	Analistas de Infraestructura	Lider Monitoreo	Analistas de monitoreo
Definir Activo	R	A	-	-	-	-
Configirar activo	R	-	R	A	-	-
Exponer activo	R	C	R	A	-	-
Monitorear activo	R	I	I	I	R	A
Tomar evidencia de ataques	R	I	I	I	R	A
Definir criticidad	R	I	I	I	R	A
Reportar ataques	R	I	I	I	R	A
Correlacionar eventos	R	A	I	I	-	-
Definir controles	R	A	C	C	-	-
Implementar controles	R	A	R	A	I	-
Probar y monitorear controles	R	A	R	A	R	A
Reunion de lecciones aprendidas	R	A	A	A	A	A
Documentar ataques y controles	R	A	R	A	C	C

Fuente: Elaboración propia

Para facilitar el entendimiento de la tabla anterior, a continuación, se describe el significado de cada letra de la matriz RACI.

- Letra R: Indica quien asume la responsabilidad; esta letra define el rol de la persona que se encuentra encargada de realizar una determinada tarea.

- Letra A: La letra A determina quién aprueba; el papel de la persona o rol que actuará como aprobador es aceptar y aprobar la tarea entregada por la persona responsable.
- Letra C: La letra C indica quien es consultado. Por lo general son personas expertas o conocedoras sobre un tema y tarea que son consultadas para que opinen y sugieran sobre algún aspecto de las tareas del proyecto.
- Letra I: La letra I determina quién informa. El rol de estas personas involucra a todo individuo que debe ser informado sobre el proceso de evolución y desarrollo de las tareas.

3.4.2.3. Descripción de las fases del modelo de gestión de incidentes proactivo

A continuación, se presenta el objetivo de cada una de las fases y actividades clave del modelo propuesto:

Tabla 23. Fases y actividades clave del modelo proactivo propuesto

Fase de planificación y preparación	○ Definir el activo de información a analizar. ○ Instalación y configuración del activo a exponer sobre las herramientas señuelo.
Fase de levantamiento de información y reporte	○ Toma de evidencia de los ataques. ○ Entrega de reporte sobre los ataques por cada activo expuesto.

Fase de respuesta	○ Correlación de ataques. ○ Definición de controles.
Fase de implementación y evaluación de controles	○ Despliegue de control. ○ Pruebas de los controles implementados.
Fase reporte y lecciones aprendidas	○ Reunión de lecciones aprendidas. ○ Documentar vectores de ataque y controles definidos e implementados.

Fuente: Elaboración propia

a) Fase de planificación y preparación

La fase de **planificación y preparación** tiene como objetivo definir los activos de información que la organización desea analizar en busca de brechas de seguridad, con el fin de recabar información que le permita al equipo de respuesta a incidentes, definir de manera proactiva, controles que permitan mitigar la materialización de incidentes de seguridad en ambientes productivos. La fase de planificación y preparación tiene inmersas las siguientes actividades clave:

- **Definir el activo de información a analizar:** En esta actividad, el área de Ciberseguridad de acuerdo con necesidades internas de la organización define cuales activos de información serán expuestos en la Honeypot, las vulnerabilidades o fallas de diseño se le configurarán y si los ataques serán internos o externos. Una vez el área de

ciberseguridad define los activos a analizar, solicita al área de infraestructura de ciberseguridad mediante formato la exposición de los activos definidos.

El formato de solicitud debe contener como mínimo la siguiente información:

- Activo.
- Tipo de activo.
- Criticidad del activo.
- Responsable del activo.
- Tipo de exposición (interna o externa)
- Tiempo de exposición.
- Características técnicas del activo.
- Vulnerabilidades o fallas de diseño a configurar.
- Periodicidad de reporte de ataques recibidos.

- **Instalación y configuración del activo a exponer sobre las herramientas señuelo:** En esta actividad, el área de infraestructura de ciberseguridad una vez recibe la solicitud de exposición de los activos de información, debe llevar a cabo la instalación y configuración de las herramientas necesarias para exponer el activo de acuerdo a las especificaciones solicitadas por el área de ciber seguridad; es necesario que se lleven a cabo pruebas de acceso que permitan determinar que el servicio fue expuesto adecuadamente y que los atacantes internos o externos según sea el caso pueden alcanzar el activo. Una vez el activo está expuesto y se ejecutan las pruebas, se debe entregar al SOC o área de monitoreo para este lleve a cabo el seguimiento del activo y entregue

informe de los ataques recibidos de acuerdo con la periodicidad definida por ciberseguridad.

b) Fase de levantamiento de información y reporte

La fase de **levantamiento de información y reporte** tiene como objetivo hacer el seguimiento a los activos expuesto y reportar al área de ciberseguridad sobre los ataques que los activos han recibido de acuerdo con las especificaciones entregadas por el equipo de ciberseguridad; el SOC o el equipo de monitoreo es responsable por la ejecución de esta fase. La fase de levantamiento de información y reporte tiene inmersas las siguientes actividades clave:

- **Toma de evidencia de los ataques:** En esta actividad, el SOC o equipo de monitoreo analiza la información entregada por el componente activo (Honeypot, Big Data y Blockchain), determina si la información efectivamente corresponde a un ataque y determina la criticidad de los ataques que se están recibiendo. La información referente a los ataques debe ser manejada como información sensible y se deben seguir los lineamientos internos definidos por la organización para el tratamiento de esta categoría de información.
- **Entregar reporte sobre los ataques por cada activo expuesto:** En esta actividad, el SOC o equipo de monitoreo debe entregar la información recolectada sobre los ataques que recibió cada activo expuesto al área de ciberseguridad. El reporte de los ataques debe contener, pero sin limitarse la siguiente información:
  - Responsable del SOC o equipo de monitoreo que entrega el reporte.
  - Fecha del ataque.

- Hora del ataque.
- Descripción del ataque.
- Host atacante.
- Tipo de ataque.
- Vector de ataque utilizado
- Datos o aplicaciones de interés para el atacante
- Evidencia de los ataques.

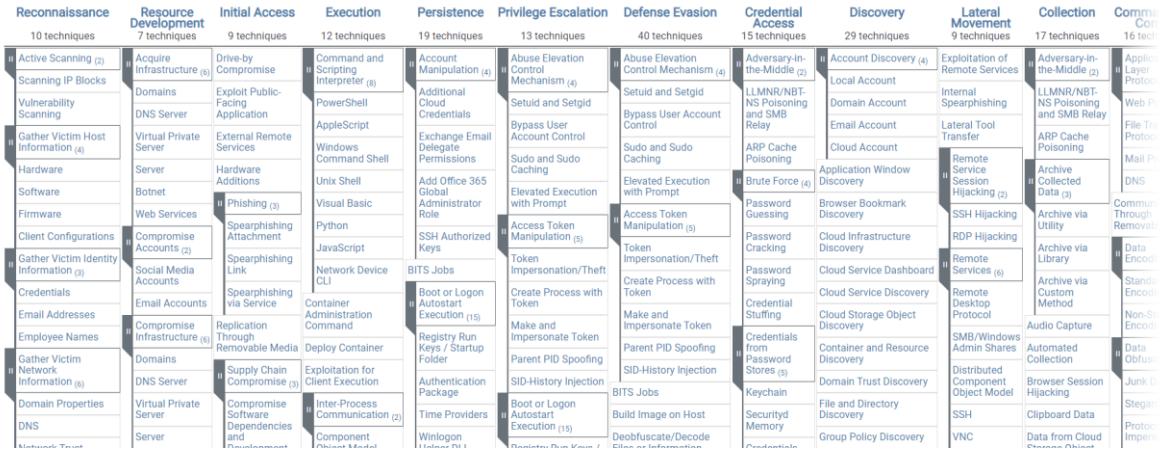
c) Fase de respuesta

La fase de **respuesta** tiene como objetivo analizar la información entregada por el SOC o el equipo de monitoreo sobre los ataques recibidos por los activos expuestos, determinar las tácticas y técnicas utilizadas por los atacantes para vulnerar los activos y con base en el resultado o conclusiones del análisis, definir los controles que deben implementarse en los activos productivos para evitar que se genere un incidente de seguridad. La fase de respuesta tiene inmersas las siguientes actividades clave:

- **Correlación de ataques:** En esta actividad, el equipo de ciberseguridad basado en la información entregada por el SOC o el equipo de monitoreo determina cuales fueron las tácticas, técnicas, sub técnicas y software utilizado por los atacantes para vulnerar los activos.
- **Definición de controles:** En esta actividad, el equipo de ciberseguridad basado en la información enviada por el SOC o el equipo de monitoreo en la identificación de los vectores de ataque utilizados, determina los controles que deben ser implementados para mitigar la materialización de incidentes de seguridad en ambientes productivos. Para la

definición de controles el equipo puede utilizar, pero sin limitarse, las matrices de ataque del Framework de Mitre.

Figura 9. Matriz de ataque Framework Mitre



Fuente: [41]

d) Fase de implementación y evaluación de controles

La fase de **implementación y evaluación de controles** tiene como objetivo ejecutar el despliegue de contramedidas que permitirán mitigar la materialización de los mismos incidentes de los activos expuestos en la infraestructura señuelo en ambientes productivos. La fase de implementación y evaluación de controles tiene inmersas las siguientes actividades clave:

- **Despliegue de control:** En esta actividad, el equipo de ciberseguridad junto con los responsables de activo despliega en ambiente productivo de la organización los controles

definidos para la mitigación de riesgo de materialización de los ataques recibidos por los activos expuestos.

- **Pruebas de los controles implementados:** En esta actividad, el equipo de ciberseguridad junto con los responsables de los activos sobre los cuales se implementaran los controles definidos, ejecutan pruebas que permitan determinar la efectividad de los controles implementados; para la ejecución de las pruebas el equipo debe utilizar pero sin limitarse, los mismos vectores de ataque que fueron detectados por el componente activo (Honeypot, Big Data) y que fueron documentados y estudiados en fases anteriores. Como parte de las pruebas y validaciones que ejecuta el equipo de ciberseguridad se debe tener en cuenta la comprobación de los dispositivos de seguridad perimetral, esto con el fin de determinar el impacto que los controles implementados tienen sobre otros activos del ecosistema y determinar si se requieren ajustes en los controles.

e) Fase reporte y lecciones aprendidas:

La fase de reporte y lecciones aprendidas tiene como objetivo generar una base de conocimiento y darle madurez al equipo de ciberseguridad en el tratamiento proactivo de vulnerabilidades y amenazas. Todas las actividades que deben ser ejecutadas en esta fase buscan validar la eficacia y eficiencia del proceso proactivo de tratamiento de amenazas y vulnerabilidades, al igual que la efectividad de los formatos y herramientas utilizadas durante el proceso; todo lo anterior con el objetivo de implementar mejoras continuas a todo

el proceso. La fase de lecciones aprendidas debe ser vista como una de las más importantes en el tratamiento y cierre proactivo de vulnerabilidades y amenazas. Igual que las otras fases del modelo propuesto, esta fase tiene inmersa las siguientes actividades clave:

- **Reunión de lecciones aprendidas:** En esta actividad deben participar todos los miembros del equipo de ciberseguridad y los miembros seleccionados de otros equipos involucrados en la configuración de los activos expuestos, la definición y despliegue de controles y en general todas las personas que tengan información sobre las vulnerabilidades y amenazas detectadas y tratadas. La reunión tiene como objetivo analizar la información recolectada sobre las amenazas, vulnerabilidades y controles implementados; de igual forma el equipo de ciberseguridad puede determinar si es necesario la definición de políticas internas que lleven a evitar que se presenten vulnerabilidades y amenazas similares en el futuro.
- **Documentar vectores de ataque y controles definidos e implementados**: Una vez se ha llevado a cabo la reunión de lecciones aprendidas, el equipo debe crear un informe que contenga toda la información recolectada sobre las amenazas, vulnerabilidades y controles implementados, dicho informe puede ser utilizado en el futuro para darle un adecuado manejo a situaciones similares y para la definición de políticas, monitoreos y controles adicionales.

3.5. Fase 5: Evaluación del modelo propuesto

Objetivo: Evaluar el modelo de gestión de incidentes de seguridad propuesto, a través de la validación de la eficiencia y efectividad del proceso proactivo de tratamiento de las

amenazas y vulnerabilidades mediante los controles definidos e implementados sobre el ambiente productivo de una organización. Para lograrlo se realizaron dos actividades: (1) Instalación y configuración de las herramientas tecnológicas (Honeypot, Big Data, Blockchain), (2) Ejecución de actividades definidas en el modelo propuesto

3.5.1. Actividad 1: Instalación y configuración de herramientas tecnológicas

En esta actividad se realizó la instalación de las herramientas tecnológicas necesarias para la identificación de amenazas y vulnerabilidades, de acuerdo con las necesidades específicas de la organización. Una adecuada configuración de las herramientas tendrá incidencia directa en la información capturada durante la exposición del activo en la Honeypot y, por consiguiente, en los controles que el equipo de ciberseguridad define para la su implementación en el ambiente productivo del activo.

3.5.1.1. Función de las herramientas tecnológicas que conformaron el componente activo del modelo proactivo propuesto

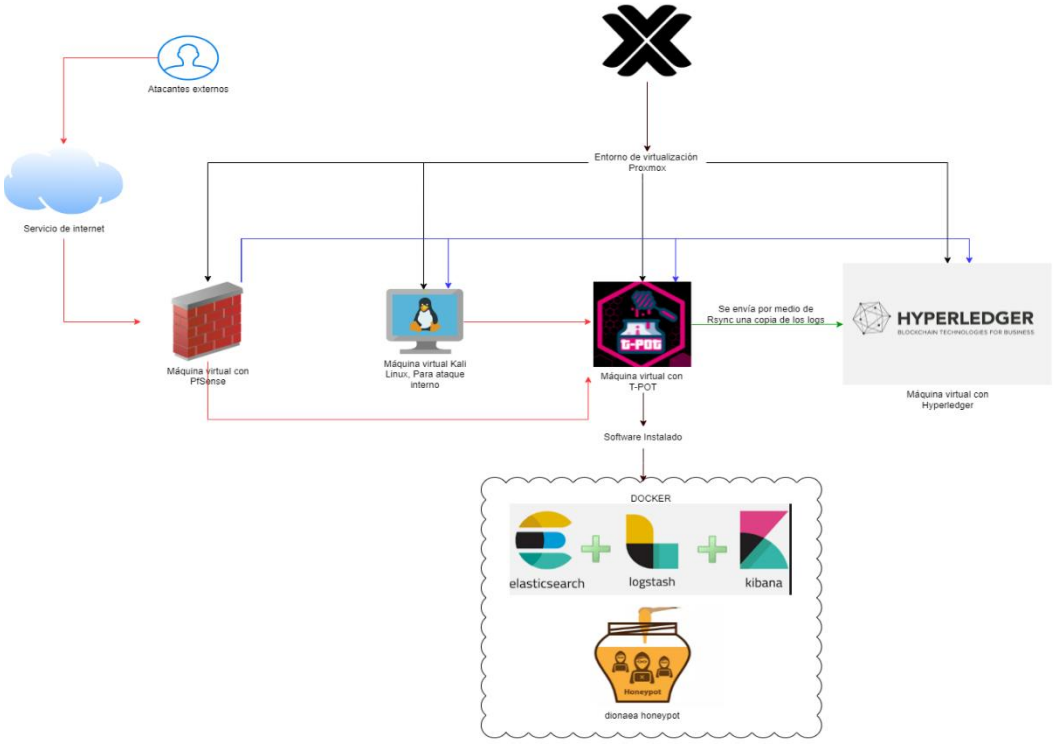
A continuación, se describe la función que tiene cada herramienta tecnológica seleccionada, dentro del componente activo utilizado por el modelo de gestión de incidentes proactivo propuesto:

- **Honeypot T-Pot - Dionaea:** La Honeypot Dionaea tuvo la función de emular los activos tecnológicos (servicios web) que serán expuestos para que reciban ataques con el fin de

recolectar información sobre los vectores utilizados para explotar sus vulnerabilidades. La información que se recolectó durante los ataques fue utilizada en el modelo de gestión de incidentes para definir los controles que deben ser implementados en los ambientes productivos del activo expuesto, con el fin de mitigar el riesgo que se presenten incidentes de seguridad debido al uso de los mismos vectores de ataque utilizados en el ambiente controlado de la Honeypot.

- **Big Data - ELK:** La herramienta ELK permitió realizar búsquedas, analizar y visualizar los datos provenientes de la Honeypot en tableros de información personalizables y aporta un manejo eficientemente de los volúmenes de logs generados por la Honeypot gracias a su gran escalabilidad.
- **Blockchain - Hyperledger Fabric:** La herramienta Hyperledger Fabric tuvo la función de almacenar la información de los incidentes de seguridad generados por la Honeypot durante los ataques y que son visualizados en la herramienta ELK; esto con el fin de garantizar su integridad, disponibilidad y confidencialidad.

Figura 10. Diagrama de arquitectura de la infraestructura instalada



Fuente: Elaboración propia

3.5.1.2. Instalación y configuración de Honeypot y Big Data

– Los requerimientos mínimos a nivel de hardware para la instalación de la plataforma T-POT fueron:

- 10 GB de memoria RAM
- 128 GB de espacio libre en disco.
- 8 Cores.

– La preparación de la instalación fue:

- Descargar la imagen ISO de la plataforma T-Pot desde la página oficial del proyecto en GitHub (https://github.com/telekom-security/tpotce/releases/tag/20.06.2).
- Se recomienda ubicar la plataforma T-Pot en una zona sin filtrar, donde todo el tráfico TCP y UDP se reenvíe a la interfaz de red de T-Pot.
- Para evitar sondear los puertos de administración de la plataforma T-Pot, se debe le debe ubicar detrás de un firewall y reenviar todo el tráfico TCP / UDP en el rango de puertos de 1-64000 a T-Pot mientras permite el acceso a puertos > 64000 solo desde IP de confianza y / o solo exponer los puertos relevantes para su caso de uso.
- Para un correcto funcionamiento de la plataforma T-Pot, se deben habilitar los siguientes puertos:

Tabla 24. Puertos requeridos para el funcionamiento de T-Pot

Puerto	Protocolo	Dirección	Descripción
80, 443	TCP	Saliente	T-Pot Management: Instalación, actualizaciones, registros (es decir, Debian, GitHub, DockerHub, PyPi, Sicherheitstacho, etc.

64294	TCP	Entrante	Gestión de T-Pot: Acceso a la consola.
64295	TCP	Entrante	T-Pot Management: Acceso a SSH
64297	TCP	Entrante	T-Pot Management Acceso al proxy inverso NGINX
5555	TCP	Entrante	Honeypot: ADBHoney
5000	UDP	Entrante	Honeypot: CiscoASA
8443	TCP	Entrante	Honeypot: CiscoASA
443	TCP	Entrante	Honeypot: CitrixHoneypot
80, 102, 502, 1025, 2404, 10001, 44818, 47808, 50100	TCP	Entrante	Honeypot: Conpot
161, 623	UDP	Entrante	Honeypot: Conpot
22, 23	TCP	Entrante	Honeypot: Cowrie
19, 53, 123, 1900	UDP	Entrante	Honeypot: Ddospot
11112	TCP	Entrante	Honeypot: Dicompot
21, 42, 135, 443, 445, 1433,	TCP	Entrante	Honeypot: Dionaea

1723, 1883, 3306, 8081			
69	UDP	Entrante	Honeypot: Dionaea
9200	TCP	Entrante	Honeypot: Elástico
22	TCP	Entrante	Honeypot: Endlessh
21, 22, 23, 25, 80, 110, 143, 443, 993, 995, 1080, 5432, 5900	TCP	Entrante	Honeypot: Heraldo
21, 22, 23, 25, 80, 110, 143, 389, 443, 445, 1080, 1433, 1521, 3306, 5432, 5900, 6379, 8080, 9200, 11211	TCP	Entrante	Honeypot: qHoneypots
53, 123, 161	UDP	Entrante	Honeypot: qHoneypots
631	TCP	Entrante	Honeypot: IPPHoney

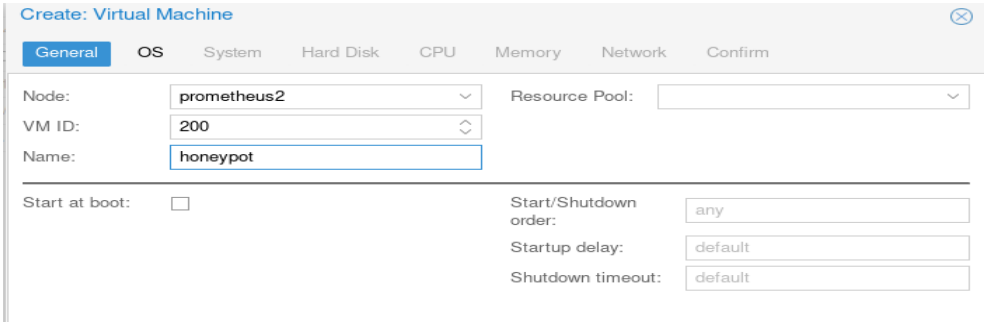
80, 443, 8080, 9200, 25565	TCP	Entrante	Honeypot: Log4Pot
25	TCP	Entrante	Honeypot: Mailoney
2575	TCP	Entrante	Honeypot: Medpot
6379	TCP	Entrante	Honeypot: Redishoneypot
5060	UDP	Entrante	Honeypot: Centinela
80	TCP	Entrante	Honeypot: Trampa (Curtidor)

Fuente: Elaboración propia

– La instalación de la plataforma T-Pot fue:

  - Se creó una máquina virtual utilizando el virtualizador Proxmox.
  - Se definió Honeypot como nombre para la máquina virtual.

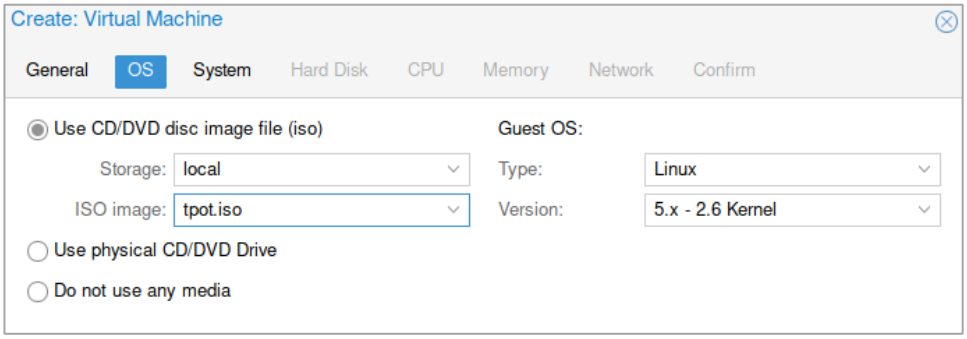
Figura 11. Definición de nombre de la máquina virtual



Fuente: Preparación máquina virtual en Proxmox

– Se carga la imagen ISO de TPot que se instala sobre la máquina virtual.

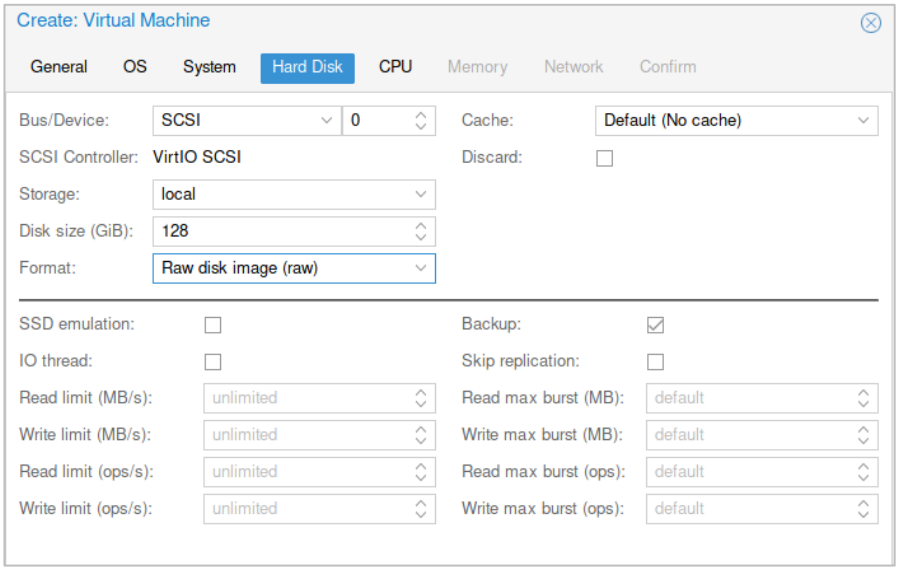
Figura 12. Carga de imagen ISO para ser instalada



Fuente: Preparación máquina virtual

– Se asigna el espacio en disco (No puede ser inferior a 128 GB).

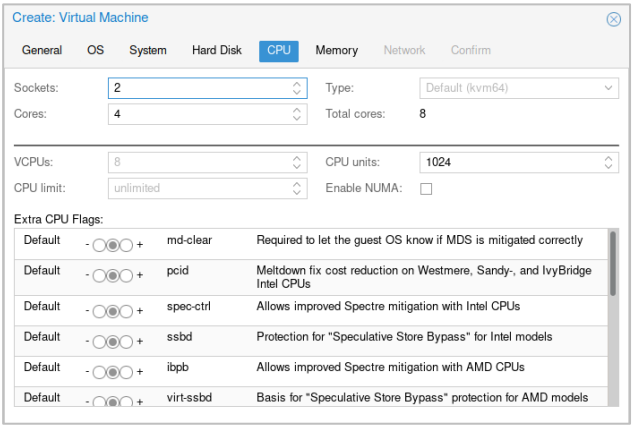
Figura 13. Selección de espacio en disco



Fuente: Preparación máquina virtual

– Asignación de Sockets y Cores: 2 Socket y 4 Core por Socket, para un total de 8 Cores

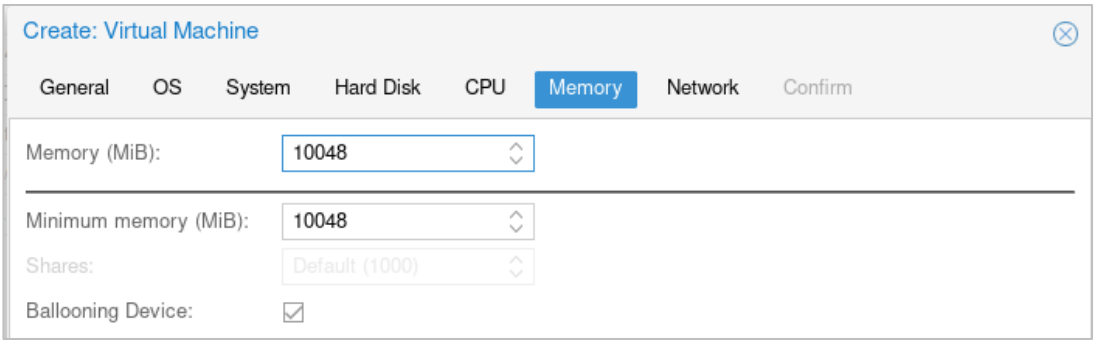
Figura 14. Asignación de Sockets y Cores



Fuente: Preparación máquina virtual

– Asignación de memoria RAM (10 Gb): Se asigna la memoria RAM a la máquina.

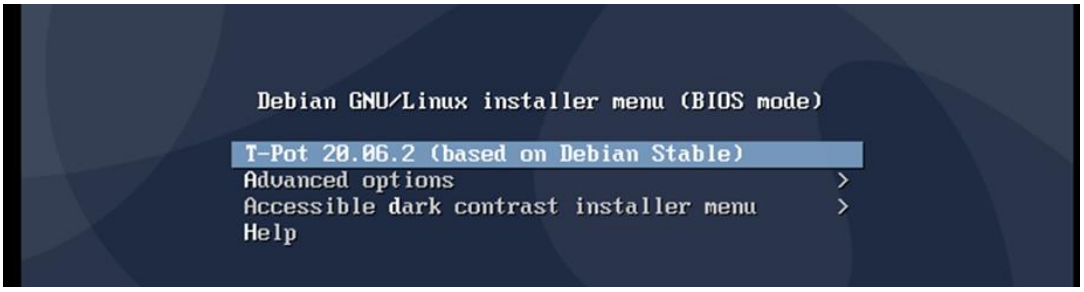
Figura 15. Asignación de memoria RAM



Fuente: Proceso de instalación Tpot

– Selección de opción de instalación: Se selecciona la opción T-Pot 20.06.2

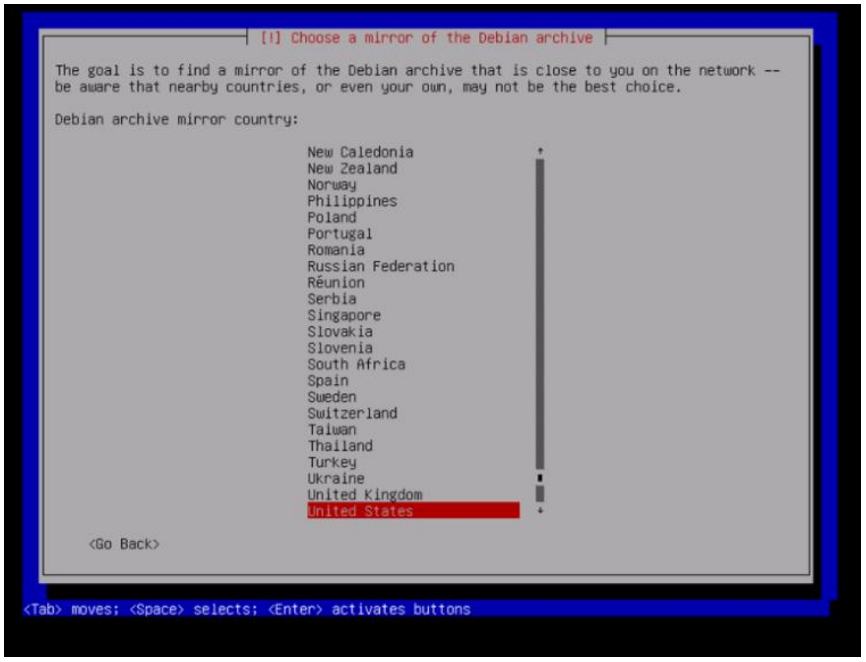
Figura 16. Selección de opciones de instalación



Fuente: Proceso de instalación Tpot

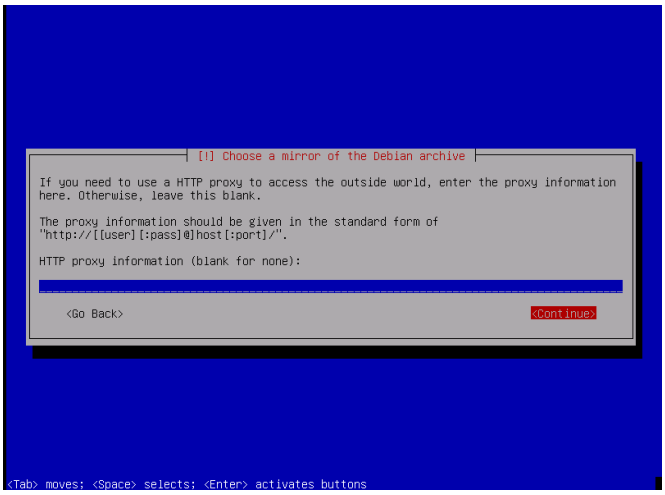
– Configuraciones adicionales.

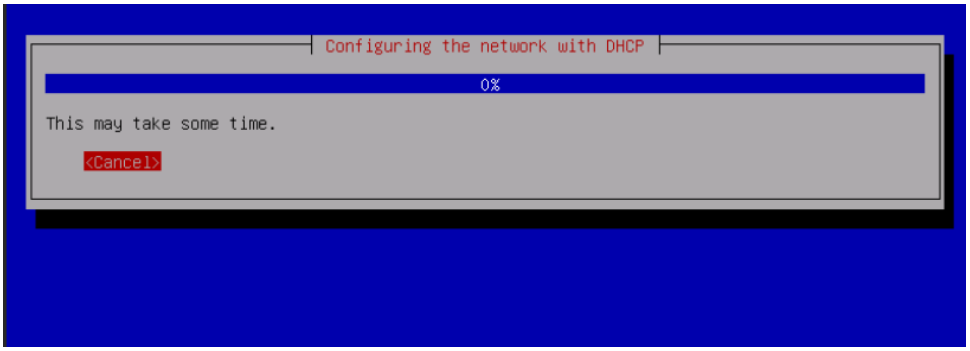
Figura 17. Selección de idioma



Fuente: Proceso de instalación Tpot

Figura 18. Ajustes de Proxy y búsqueda de DHCP

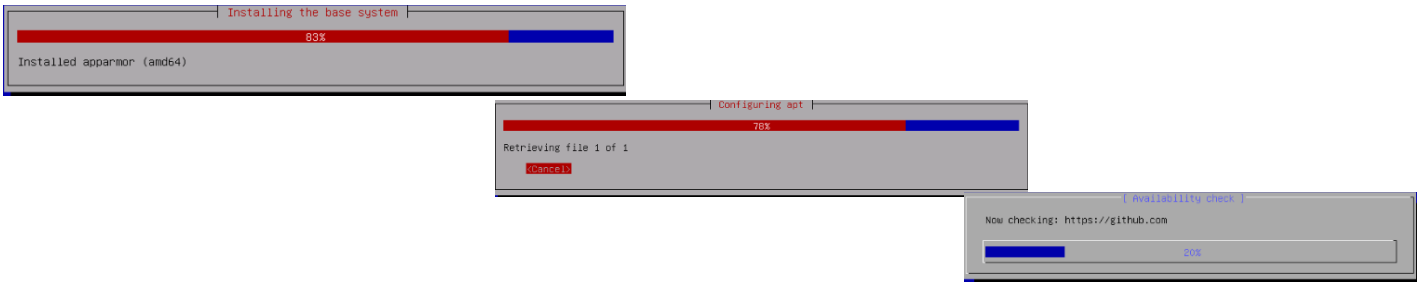




Fuente: Proceso de instalación Tpot

– Instalación desatendida de Docker:

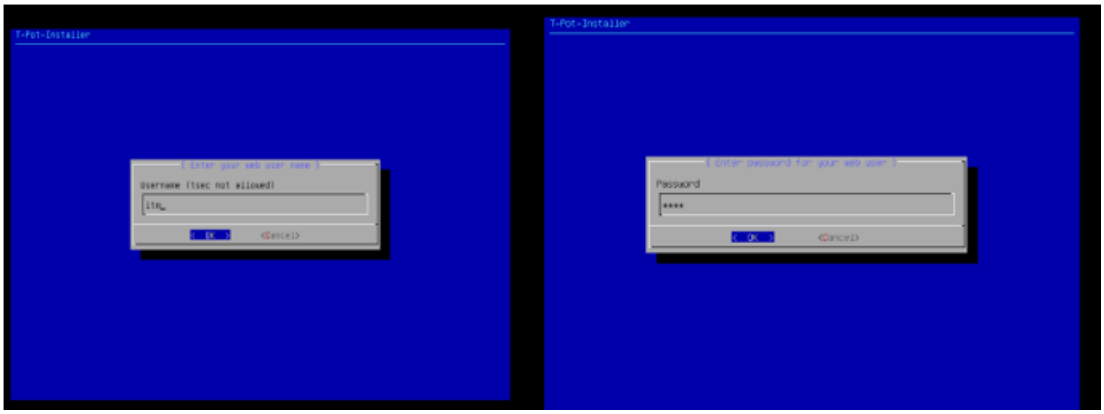
Figura 19. Instalación desatendida de Docker



Fuente: Proceso de instalación Tpot

– Configuración de usuario y contraseña de acceso a la máquina virtual que contiene las Honeypot.

Figura 20. Configuración de credenciales



Fuente: Proceso de instalación Tpot

– Instalación de componentes: En este proceso el sistema instaló todos los componentes necesarios para el correcto funcionamiento de la Honeypot; durante este proceso el sistema se reinició en varias ocasiones.

Figura 21. Instalación de componentes

Fuente: Proceso de instalación T-Pot

– Proceso de carga de la plataforma Honeypot; Todos los servicios de Honeypot fueron preconfigurados y se iniciaron automáticamente durante este proceso.

Figura 22. Carga de SSH con las direcciones IP que asigno el DHCP

Fuente: Proceso de instalación T-Pot

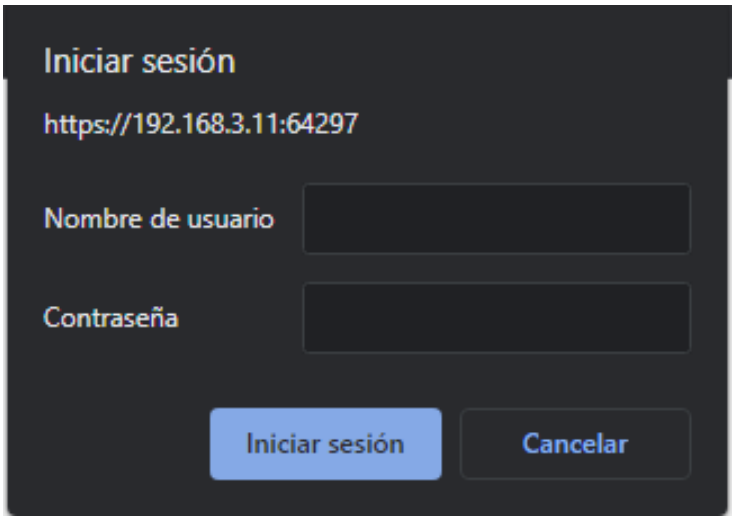
– Arranque e inicio de sesión en Tpot mediante SSH; Por defecto, el demonio SSH permitió el acceso TCP por el puerto 64295; en el inicio de sesión el sistema solicitó el ingreso de las credenciales previamente definidas.

Figura 23. Inicio de sesión SSH TPot

Fuente: Sistema T-Pot

- Inicio de sesión de sesión Web **de** T-Pot**:** en el inicio de sesión el sistema solicitó el ingreso de las credenciales previamente definidas.

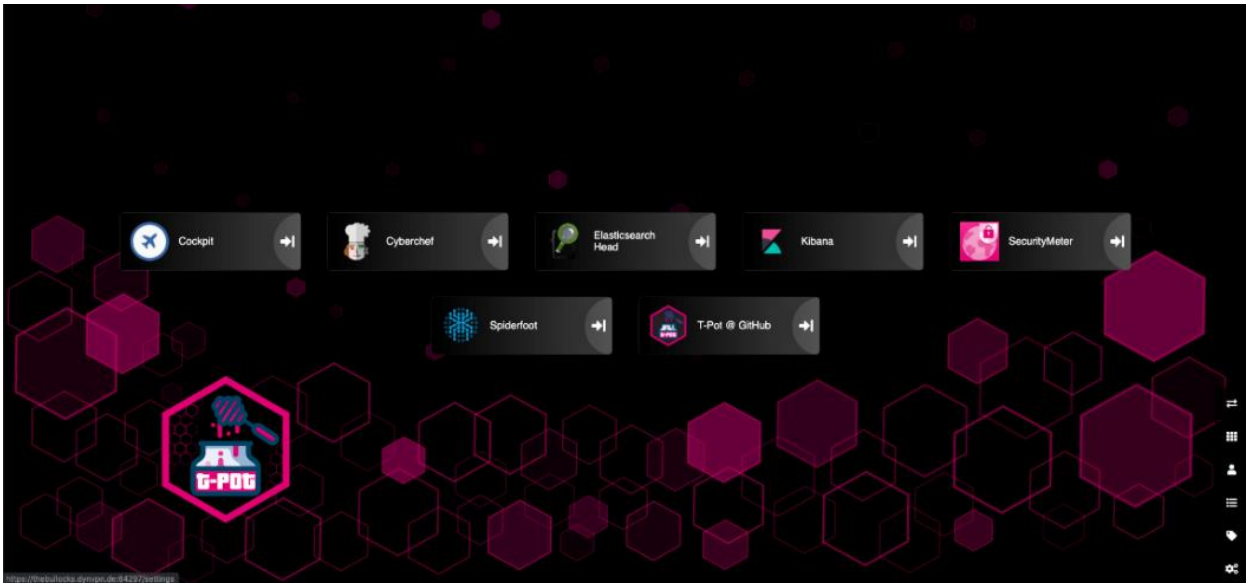
Figura 24. Inicio de sesión web T-Pot



Fuente: Sistema T-Pot

- Menú principal T-Pot: Una vez se ingresaron las credenciales de acceso a la plataforma web de T-Pot, el sistema presentó el menú principal.

Figura 25. Menú principal T-Pot



Fuente: Sistema T-Pot

- Vista general de la Kibana: A esta vista general se accedió mediante opción de menú presentado en el menú principal de T-Pot; en esta vista se observaron las métricas de los ataques que se han presentado.

Figura 26. Vista general Kibana

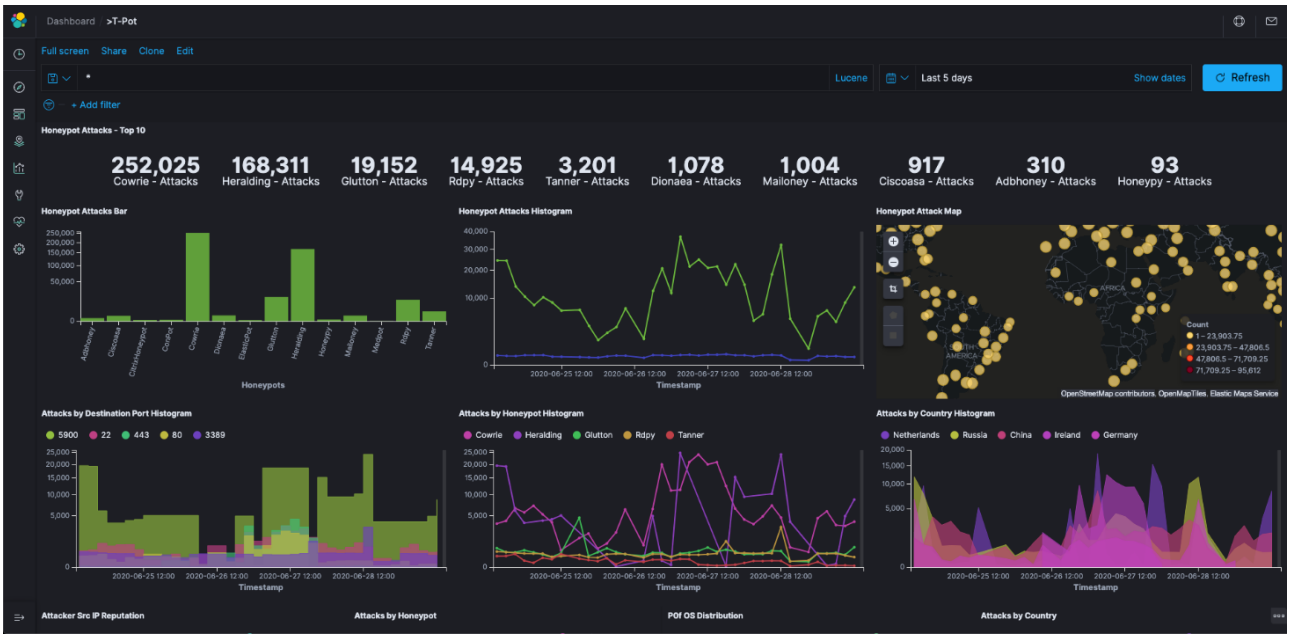
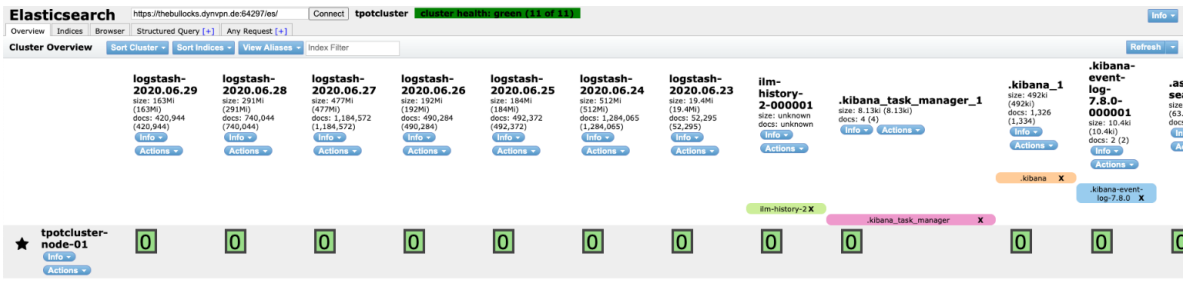


Figura 27. Vista general Elasticsearch



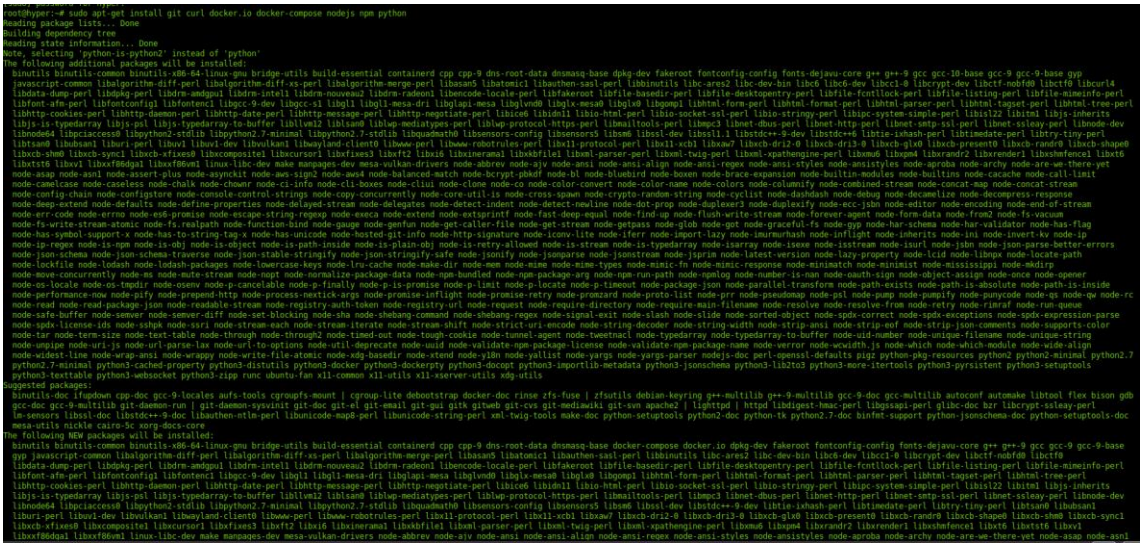
Fuente: Sistema Elasticsearch

3.5.1.3. Instalación de Máquina virtual Hyperledger

– Se ejecutan los siguientes comandos en la terminal con usuario Root; estos comandos instalan las herramientas Git, Curl, Docker, Docker-Compose, Node.js, NPM y Python.

- sudo apt-get update
- sudo apt-get install git curl docker.io docker-compose nodejs npm python

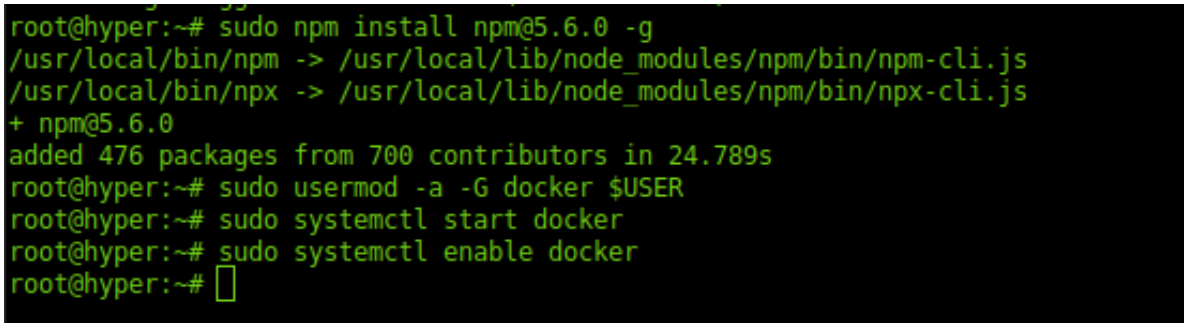
Figura 28. Proceso de instalación de herramientas en terminal



Fuente: Terminal máquina virtual Hyperledger Fabric

- Se ejecutan comandos para actualizar la herramienta NPM y configuración de la herramienta Docker:
  - sudo npm install npm@5.6.0 -g
  - sudo usermod -a -G docker $USER
  - sudo systemctl start docker
  - sudo systemctl enable docker

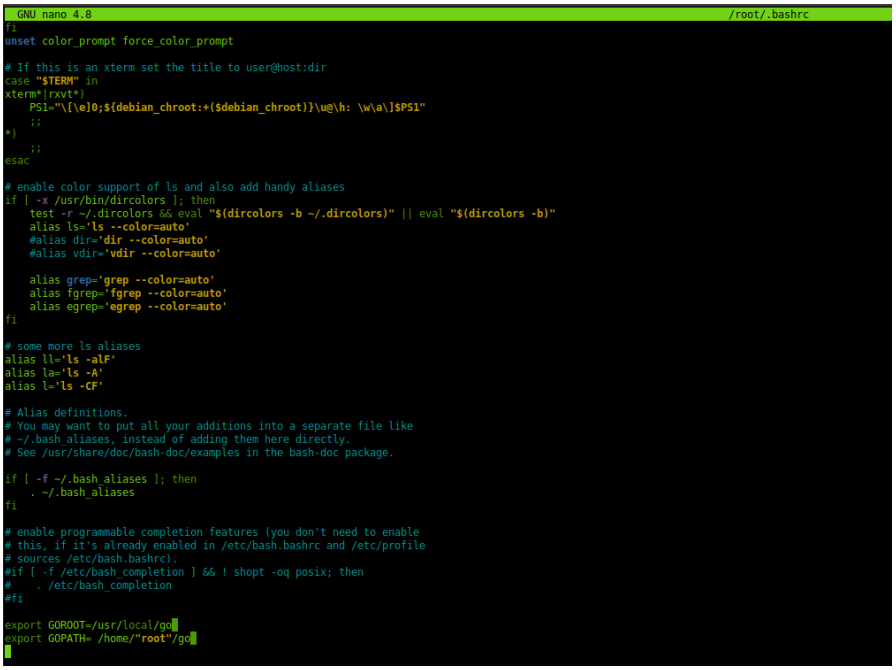
Figura 29. Ejecución de comandos en terminal



Fuente: Terminal máquina virtual Hyperledger Fabric

- Se ejecutaron comandos para descargar, descomprimir y mover los repositorios de Google:
  - wget https://dl.google.com/go/go1.13.6.linux-amd64.tar.gz
  - tar -xzvf go1.13.6.linux-amd64.tar.gz
  - sudo mv go/ /usr/local
- Se ejecutaron comandos para creación de folder, edición de archivo. bashrc y exportación
  - cd ~
  - mkdir go
  - nano ~/.bashrc
  - export GOROOT=/usr/local/go
  - export GOPATH= /home/ root/go
  - export PATH=$PATH:$GOROOT/bin

Figura 30. Ejecución de comandos en terminal

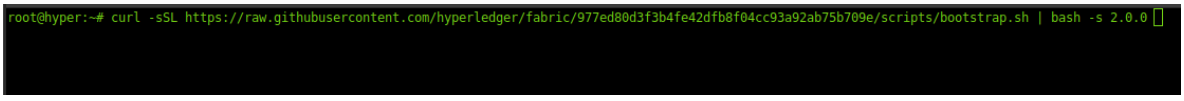


Fuente: Terminal máquina virtual Hyperledger Fabric

- Se ejecutó comando para descarga de repositorio de Hyperledger Fabric para su instalación:
  - Curl–SSL

    https://raw.githubusercontent.com/hyperledger/fabric/977ed80d3f3b4fe42dfb8f04cc93a92ab75b709e/scripts/bootstrap.sh | bash -s 2.0.0

Figura 31. Ejecución de comando de descarga de Hyperledger Fabric



Fuente: Terminal máquina virtual Hyperledger Fabric

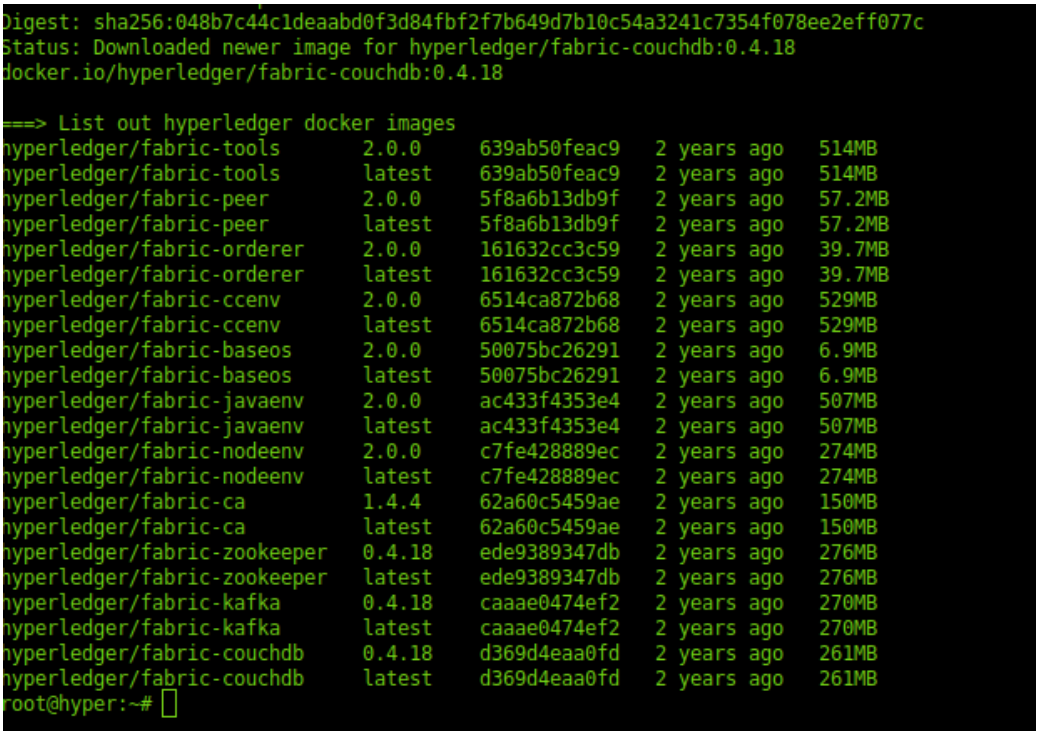
– Se muestró donde están ubicados los logs en el T-Pot para implementar el sistema de copias:

Figura 32. Ubicación de los logs de T-Pot

Fuente: Terminal máquina virtual Hyperledger Fabric

– Evidencia de los contenedores de Docker instalados durante el proceso.

Figura 33. Docker instalados

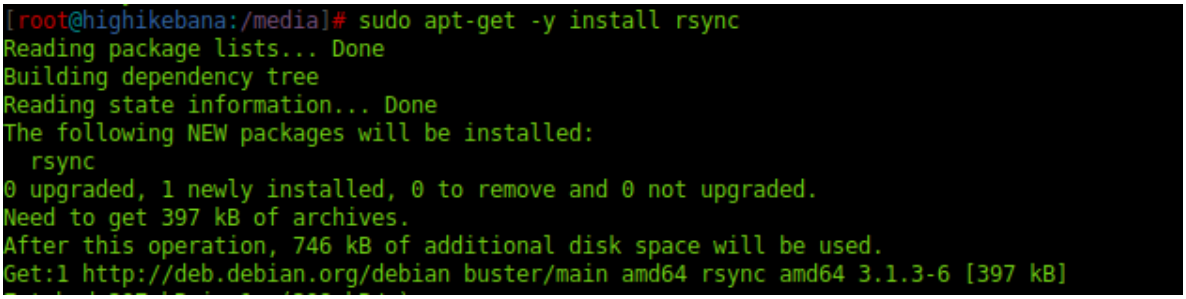


Fuente: Terminal máquina virtual Hyperledger Fabric

– Se ejecutaron comandos para la instalación de Rsync para la copia de los logs desde la Honeypot hasta la plataforma Blockchain.

  - Sudo apt-get –y install rsync

Figura 34. Instalación de herramienta Rsync



Fuente: Terminal máquina virtual Hyperledger Fabric

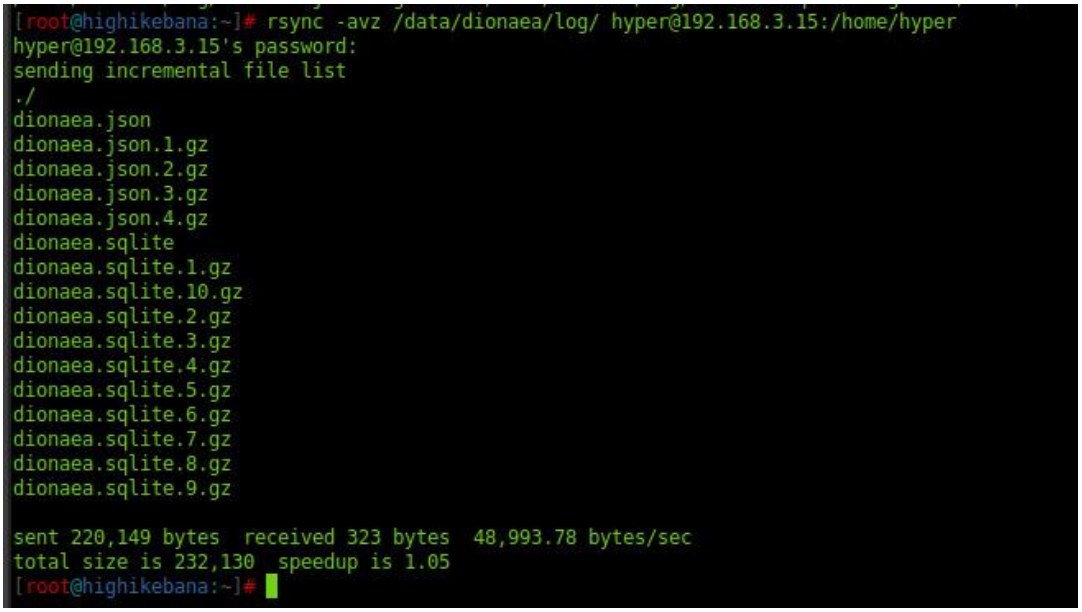
– Se ejecutaron comandos de creación de script para generación de copias de los logs sobre la plataforma Hyperledger Fabric:

Figura 35. Ejecución de comandos para creación de scrip

Fuente: Terminal máquina virtual Hyperledger Fabric

– Ejecución del script Rsync que genera copia de la ruta data/dionaea/log/ a (Hyperledger@192.3.15:/home/hyper):

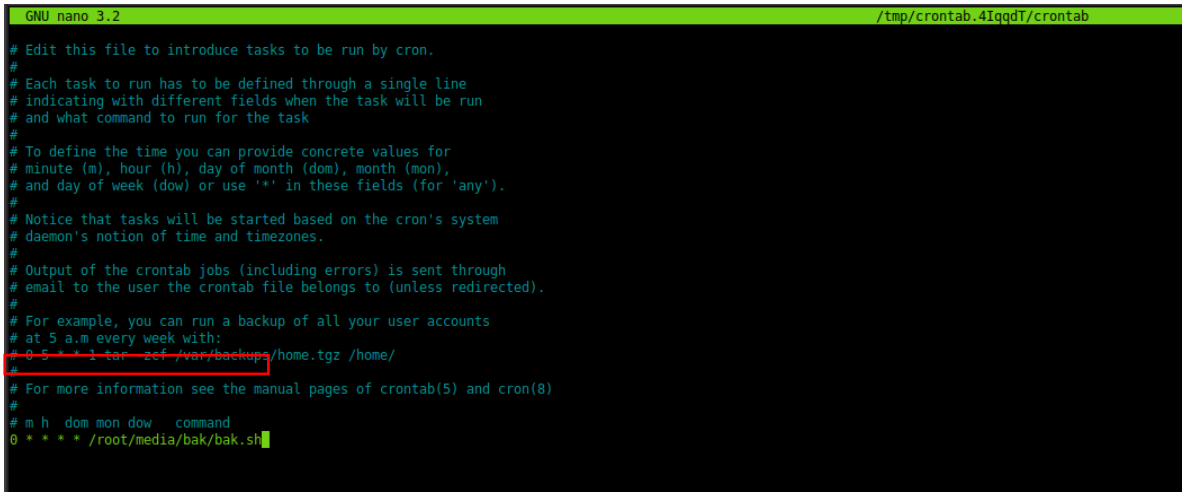
Figura 36. Ejecución de Script Rsync



Fuente: Terminal máquina virtual Hyperledger Fabric

- Configuración de tiempo de ejecución de scrip parta generación de copia de logs desde Honeypot hacia plataforma Hyperledger Fabric:

Figura 37. Configuración de periodicidad de ejecución de script



Fuente: Terminal máquina virtual Hyperledger Fabric

3.5.2. Actividad 2: Ejecución de actividades definidas en el modelo

Para la ejecución de esta actividad se contó con el apoyo de T.I Rescue, empresa con amplia experiencia en soluciones de ciberseguridad, que presta servicios a distintas organizaciones de diversos sectores del país. La empresa T.I Rescue fue la encargada de ejecutar las actividades definidas en el nuevo modelo de gestión de incidentes de seguridad.

3.5.2.1. Fase de planificación y preparación

Actividad 1: Definir el activo de información a analizar: El área de ciberseguridad definió que se requiere analizar un servidor web Apache Tom Cat v. 8.5.32 el cual en ambiente productivo será utilizado por la compañía para la publicar API Rest que serán consumidas por aliados estratégicos de la compañía.

A continuación, se presenta el formato utilizado por el área de ciberseguridad para solicitar la exposición del activo en la Honeypot.

Figura 38. Formato de solicitud de exposición de activos de información

1. ORIGEN DEL ACTIVO			
RESPONSABLE			
Infraestructura			
1. INFORMACIÓN DE LOS ACTIVOS		**2. DESTINO DEL ACTIVO**	
Activo	1. Servidor Web Tomcat versión 8.5.32	**Criticidad del activo**	Alta
Descripción	Contenedor Java Servlet, o contenedor web, que proporciona la funcionalidad extendida para interactuar con Java Servlets.	**Nombre del Responsable del Activo**	Diego Lopez
Rol	Servidor Web Front End	**Tiempo de exposición**	7 Dias
Vulnerabilidades o fallas de diseño a configurar	Contraseñas debiles	**Periodicidad de reporte de ataques recibidos**	Cada 7 dias
Nombre de Analista de Ciberseguridad	Farzad Londoño	**Tipo de exposición (interna o externa)**	Interna y Externa
4. SOLICITUD DE SERVICIOS ADICIONALES			
¿Requiere apoyo para la configuración del activo?	No		
5. OBSERVACIONES			
Ninguna			
*CAMPOS DE DILIGENCIAMIENTO EXCLUSIVO DE LAS ÁREAS RESPONSABLES**			

Fuente: Elaboración propia

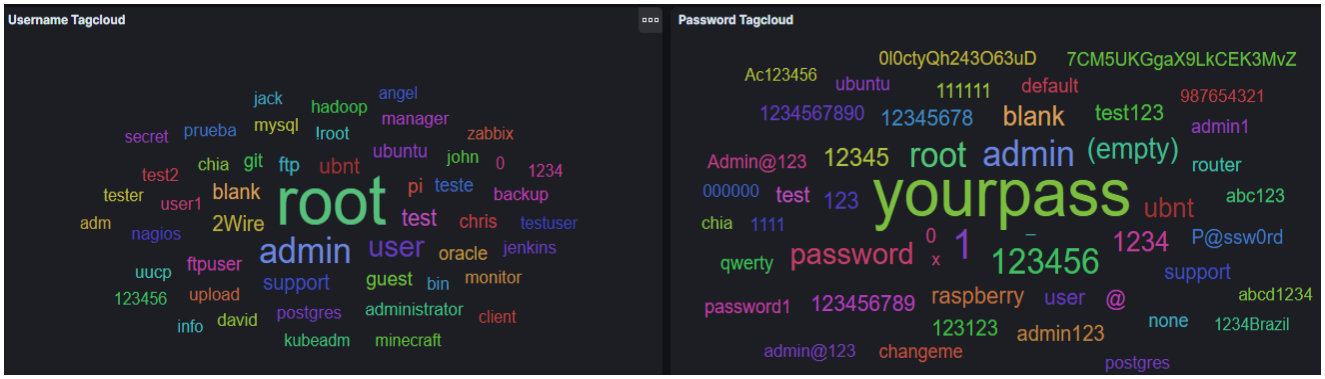
Actividad 2: **Instalación y configuración del activo a exponer sobre las herramientas señuelo:** En esta actividad se utilizó la infraestructura instalada para el laboratorio (ver numeral 3.5.1 Actividad 1: Instalación y configuración de herramientas tecnológicas).

3.5.2.2. Fase de levantamiento de información y reporte

Actividad 1: Toma de evidencia de los ataques: A continuación, se presenta la evidencia tomada por el equipo de monitoreo de la empresa **T.I Rescue** sobre los ataques recibidos por el servidor Apache Tomcat:

- **Evidencia 1:**
  - Tipo de ataque: Ataque de fuerza bruta (Brute Force).
  - Origen: Externo.
  - Descripción del ataque: El atacante está tratando de encontrar las credenciales de acceso del servidor Apache Tomcat.
  - Vector de ataque: Ataque automatizado de diccionario para encontrar las credenciales de acceso a la consola de administración del servidor Apache Tomcat.

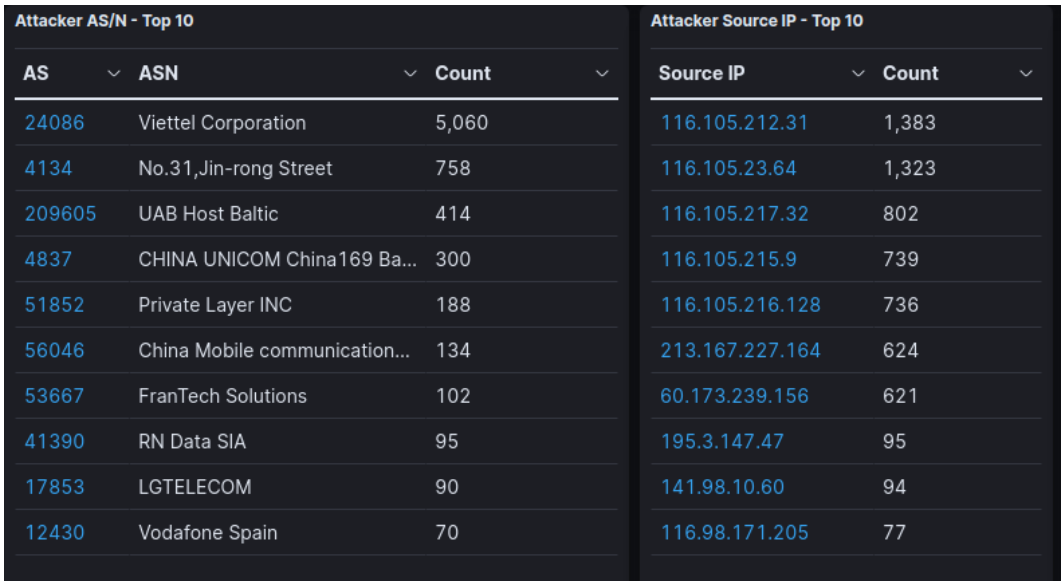
Figura 39. Credenciales probadas en el ataque de diccionario



Fuente: Dashboard Kibana

- **Evidencia 2:**

Figura 40. Evidencia de origen de direcciones IP atacantes



Attacker AS/N - Top 10

AS	ASN	Count
24086	Viettel Corporation	5,060
4134	No.31,Jin-rong Street	758
209605	UAB Host Baltic	414
4837	CHINA UNICOM China169 Ba...	300
51852	Private Layer INC	188
56046	China Mobile communication...	134
53667	FranTech Solutions	102
41390	RN Data SIA	95
17853	LGTELECOM	90
12430	Vodafone Spain	70

Attacker Source IP - Top 10

Source IP	Count
116.105.212.31	1,383
116.105.23.64	1,323
116.105.217.32	802
116.105.215.9	739
116.105.216.128	736
213.167.227.164	624
60.173.239.156	621
195.3.147.47	95
141.98.10.60	94
116.98.171.205	77

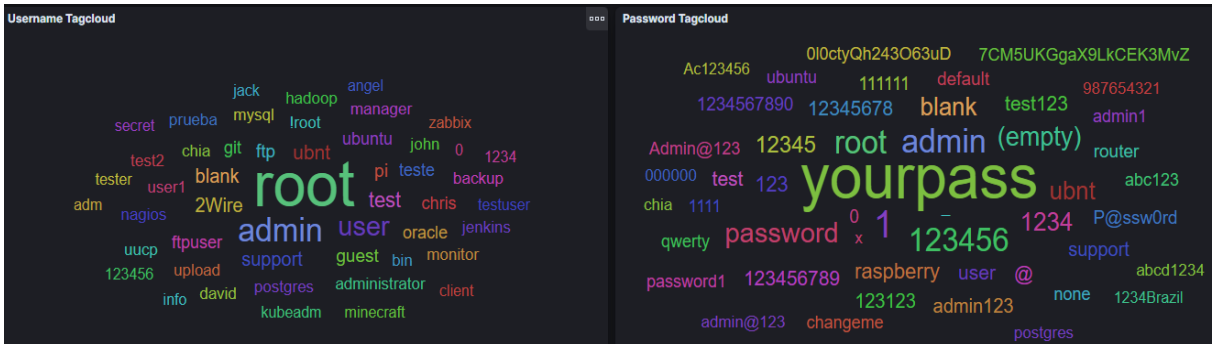
Fuente: Dashboard Kibana

Actividad 2: **Entrega de reporte sobre los ataques por cada activo expuesto:** A continuación, se presenta el informe presentado por el equipo de monitoreo al equipo de ciberseguridad sobre los ataques recibidos por el activo Apache Tomcat:

Tabla 25. Formato de entrega de reporte del equipo de monitoreo al equipo de ciberseguridad

REPORTE SOC	
1. INFORMACIÓN EQUIPO MONITOREO PROACTIVO	
Responsable del SOC o equipo de monitoreo que entrega el reporte.	Juan Camilo Rodríguez
Fecha del Ataque	29/01/2022
Descripción del Ataque	El atacante está tratando de encontrar las credenciales de acceso del servidor Apache Tomcat.
Tipo de Ataque	Fuerza Bruta (Brute Force)
Vector de Ataque	Ataque automatizado de diccionario para encontrar las credenciales de acceso a la consola de administración del servidor Apache Tomcat.
Host o IP Atacante	116.105.212.31 116.105.23.64 116.105.217.32 116.105.215.9 116.105.216.128 213.167.227.164 60.173.239.156 195.3.147.47 141.98.10.60 116.98.171.205
Datos de Interés para el atacante.	Credenciales consola de administración servidor Apache Tomcat.
Evidencia	

Credenciales probadas en el ataque de diccionario



Direcciones IP atacantes

Attacker AS/N - Top 10

AS	ASN	Count
24086	Viettel Corporation	5,060
4134	No.31,Jin-rong Street	758
209605	UAB Host Baltic	414
4837	CHINA UNICOM China169 Ba...	300
51852	Private Layer INC	188
56046	China Mobile communication...	134
53667	FranTech Solutions	102
41390	RN Data SIA	95
17853	LGTELECOM	90
12430	Vodafone Spain	70

Attacker Source IP - Top 10

Source IP	Count
116.105.212.31	1,383
116.105.23.64	1,323
116.105.217.32	802
116.105.215.9	739
116.105.216.128	736
213.167.227.164	624
60.173.239.156	621
195.3.147.47	95
141.98.10.60	94
116.98.171.205	77

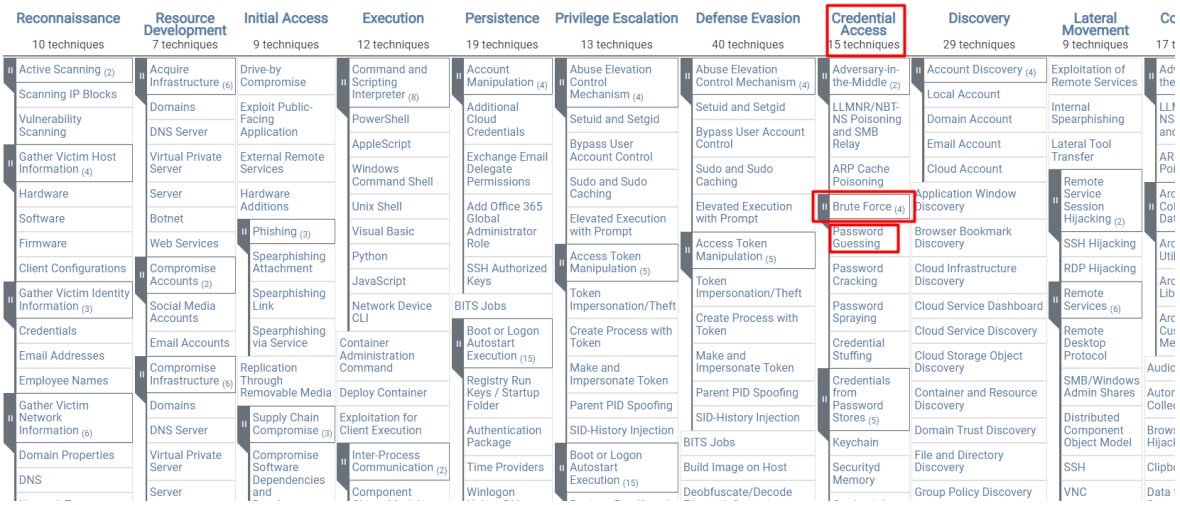
Fuente: Elaboración propia

3.5.2.3. Fase de Respuesta

Actividad 1: Correlación de ataques: A continuación, se presenta la correlación efectuada por el equipo de ciberseguridad de acuerdo con el reporte de los ataques recibidos por el servidor Apache Tomcat expuesto en la Honeypot.

- **Tipo de ataque:** Credencial Access
- **Técnica**: Brute Force
- Sub técnica: Password Guessing

Figura 41. Framework Mitre ATT&CK para correlación de ataque recibido por el activo Apache Tomcat



Fuente: Framework Mitre ATT&CK

Actividad 2: Definición de controles: A continuación, se presenta el listado de controles definidos por el equipo de ciberseguridad de acuerdo con el Framework Mitre ATT&CK:

Control: Políticas de uso de la cuenta (M1036)

Descripción: Establezca políticas de bloqueo de cuentas después de una cierta cantidad de intentos fallidos de inicio de sesión para evitar que se adivinen las contraseñas. Una política demasiado estricta puede crear una condición de denegación de servicio y hacer que los entornos queden inutilizables, con todas las cuentas utilizadas en la fuerza bruta bloqueadas [41].

Control: Uso de listas de DNSBL

Descripción: Establezca listas de DNSBL (Listas negras basadas en DNS) para minimizar la cantidad de ataques que puedan afectar la operación.

3.5.2.4. Fase de implementación y evaluación de controles

Actividad 1: Despliegue de controles 1 y 2: En esta actividad el equipo de ciberseguridad involucró a los encargados de la infraestructura de la empresa (TI Rescue) para que prestaran apoyo en la implementación de controles sobre el activo Apache Tomcat en el ambiente productivo.

Control 1:

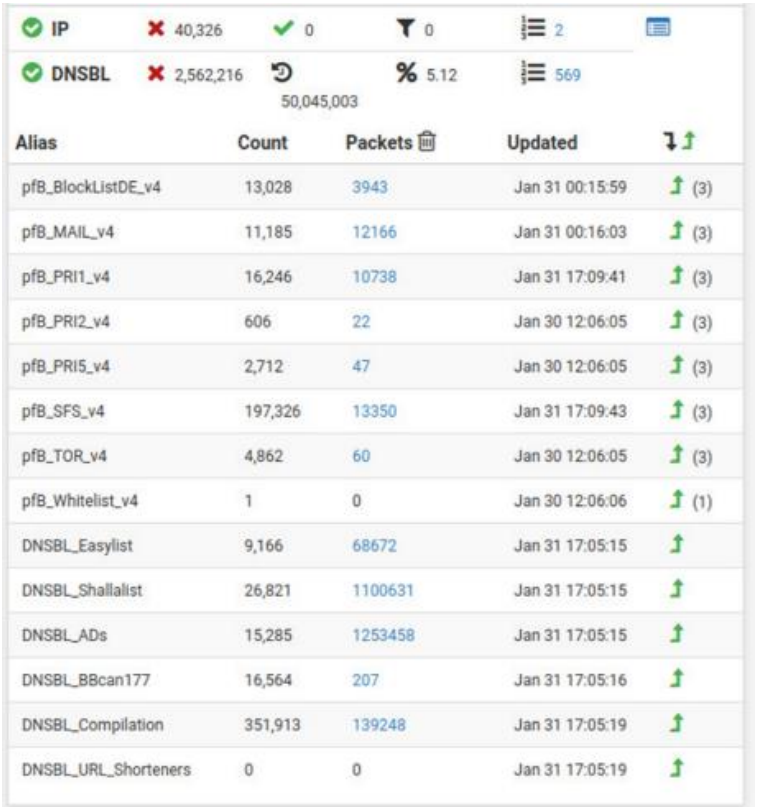
- **Control por desplegar:** Bloqueo por intentos fallidos en el activo ApacheTomcat
- **Plataforma por impactar:** Apache Tomcat.
- **Ejecución:** Usando la consola con usuario administrador, se modifica el archivo de configuración server.xml, agregando la siguiente línea así:
    - sudo nano $CATALINA_BASE/conf/server.xml file
- **Se agregó la siguiente línea:**

- <Realm className="org.apache.catalina.realm.LockOutRealm" lockOutTime="3000" failureCount="5"/>

Control 2:

- **Control por desplegar:** listas de DNSBL (listas negras basadas en DNS)
- **Plataforma por impactar:** FW pfSense.
- **Ejecución:** Ver configuración en el sitio web oficial de [42]

Figura 42. Lista de aplicación control DNSBL

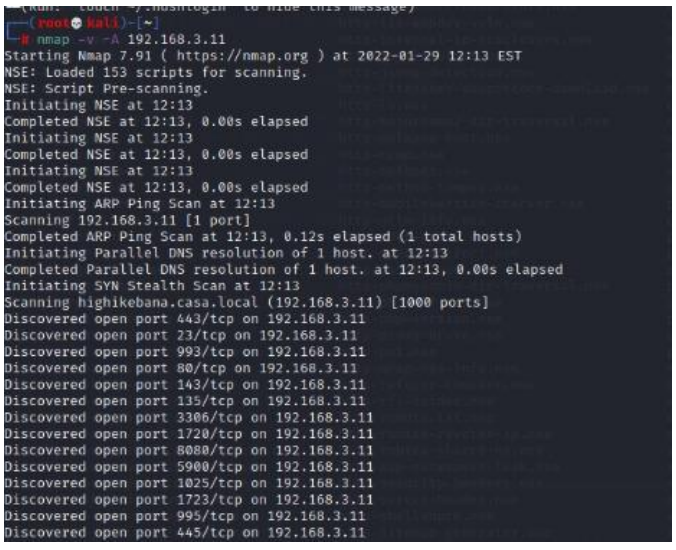


Fuente: Consola pfSense

Actividad 2: Pruebas de los controles implementados: Para realizar las pruebas de los controles instalados, se realizó un ataque interno, para ello el equipo de ciberseguridad utilizó una máquina con SO Kali/Linux; Se utiliza el mismo vector de ataque usado por los atacantes durante la exposición externa del activo. A continuación, se presentan las evidencias del ataque interno realizado y la evidencia que muestra que no se logró adivinar las credenciales del Apache Tomcat:

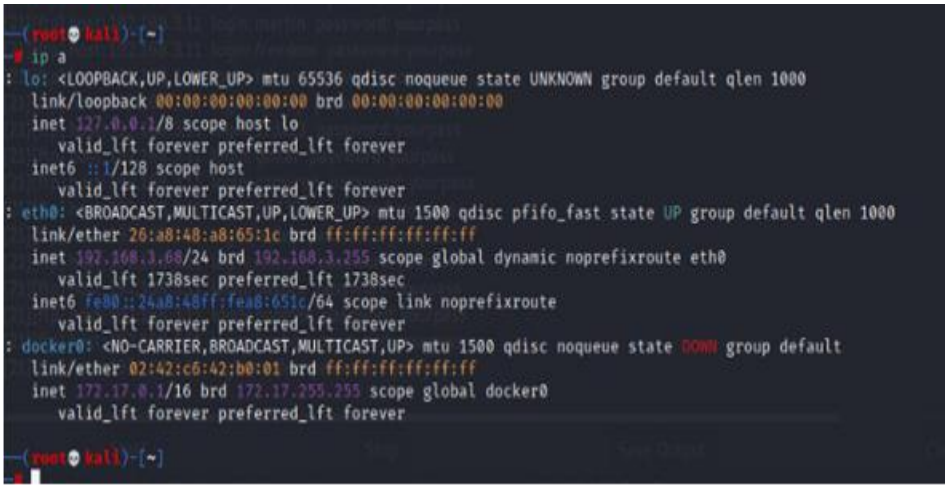
Control probado: Bloqueo por intentos fallidos en el activo ApacheTomcat: A continuación, se presenta la evidencia de la prueba de la efectividad del control implementado:

Figura 43. Escaneo de puerto desde SO Kali Linux al servidor en el cual está instalado en servidor Apache Tomcat



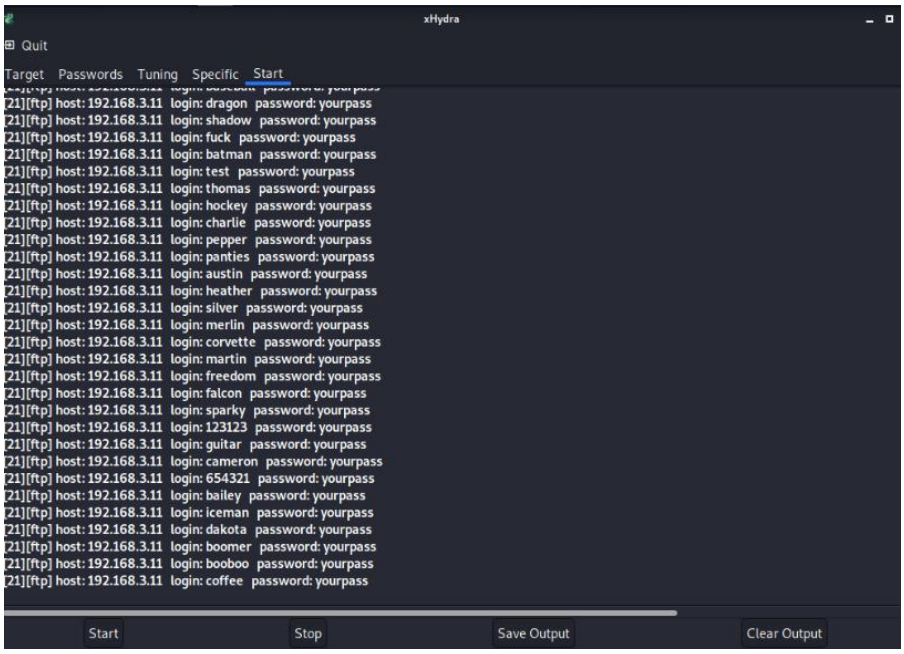
Fuente: Consola Kali Linux

Figura 44. Prueba de conexión entre Kali Linux y servidor Apache Tomcat



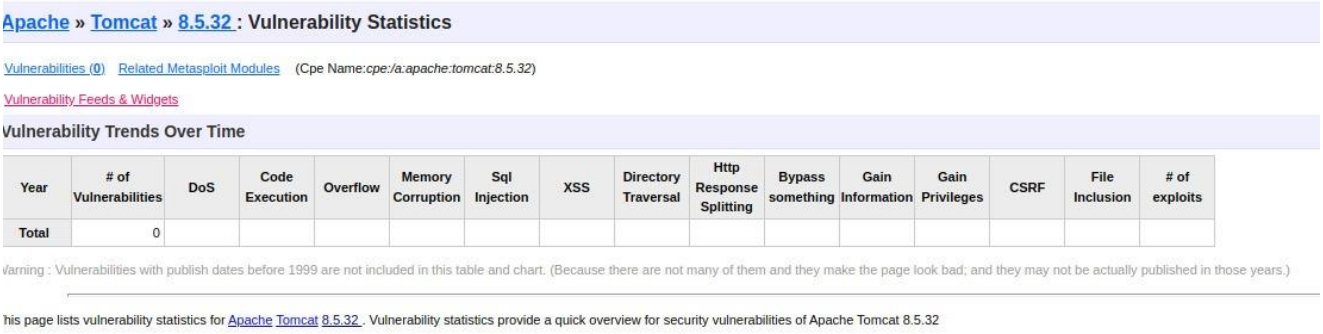
Fuente: Consola Kali Linux

Figura 45. Ataque de fuerza bruta sobre servidor Apache Tomcat



Fuente: Consola Kali Linux

Figura 46. Estadísticas de vulnerabilidades reportadas por Apache Tomcat



Apache » Tomcat » 8.5.32 : Vulnerability Statistics

Vulnerabilities (0) Related Metasploit Modules (Cpe Name:*cpe:/a:apache:tomcat:8.5.32*)

Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
Total	0														

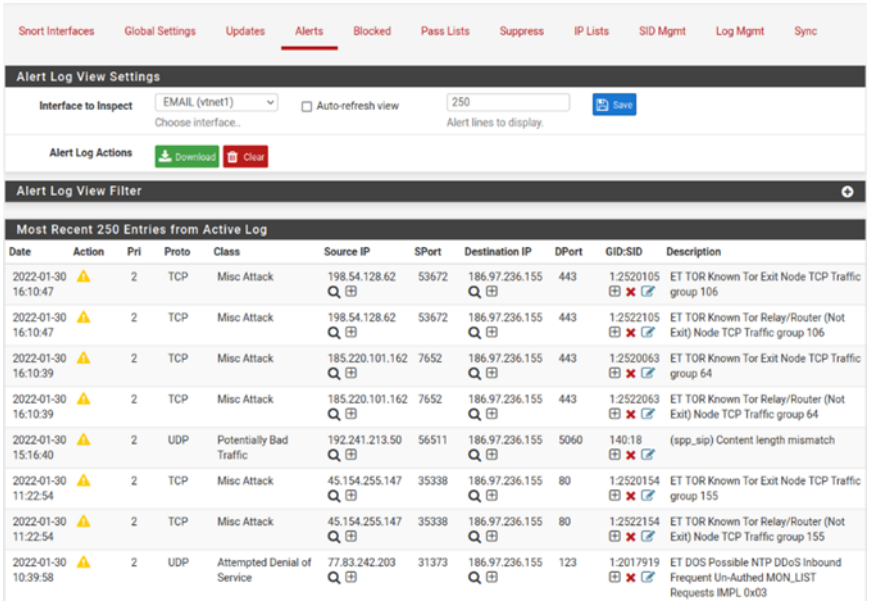
Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

This page lists vulnerability statistics for Apache Tomcat 8.5.32 . Vulnerability statistics provide a quick overview for security vulnerabilities of Apache Tomcat 8.5.32

Fuente: Servidor web Apache Tomcat productivo

Control probado: listas de DNSBL (listas negras basadas en DNS): Con el servicio en ambiente productivo, se evidencia en las alertas de monitoreo del FW que se recibieron ataques a los puertos 443 y 8080 y todos fueron evitados por este. A continuación, se presenta la evidencia de la efectividad del control implementado:

Figura 47. Log de eventos del FW pfSense



Snort Interfaces | Global Settings | Updates | Alerts | Blocked | Pass Lists | Suppress | IP Lists | SID Mgmt | Log Mgmt | Sync

Alert Log View Settings

Interface to Inspect: EMAIL (vtnet1) — Choose interface.. | Auto-refresh view | 250 — Alert lines to display. | Save

Alert Log Actions: Download | Clear

Alert Log View Filter

Most Recent 250 Entries from Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2022-01-30 16:10:47	⚠	2	TCP	Misc Attack	198.54.128.62	53672	186.97.236.155	443	1:2520105	ET TOR Known Tor Exit Node TCP Traffic group 106
2022-01-30 16:10:47	⚠	2	TCP	Misc Attack	198.54.128.62	53672	186.97.236.155	443	1:2522105	ET TOR Known Tor Relay/Router (Not Exit) Node TCP Traffic group 106
2022-01-30 16:10:39	⚠	2	TCP	Misc Attack	185.220.101.162	7652	186.97.236.155	443	1:2520063	ET TOR Known Tor Exit Node TCP Traffic group 64
2022-01-30 16:10:39	⚠	2	TCP	Misc Attack	185.220.101.162	7652	186.97.236.155	443	1:2522063	ET TOR Known Tor Relay/Router (Not Exit) Node TCP Traffic group 64
2022-01-30 15:16:40	⚠	2	UDP	Potentially Bad Traffic	192.241.213.50	56511	186.97.236.155	5060	140:18	(spp_sip) Content length mismatch
2022-01-30 11:22:54	⚠	2	TCP	Misc Attack	45.154.255.147	35338	186.97.236.155	80	1:2520154	ET TOR Known Tor Exit Node TCP Traffic group 155
2022-01-30 11:22:54	⚠	2	TCP	Misc Attack	45.154.255.147	35338	186.97.236.155	80	1:2522154	ET TOR Known Tor Relay/Router (Not Exit) Node TCP Traffic group 155
2022-01-30 10:39:58	⚠	2	UDP	Attempted Denial of Service	77.83.242.203	31373	186.97.236.155	123	1:2017919	ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03

Fuente: Consola FW pfSense

3.5.2.5. Fase reporte y lecciones aprendidas:

Actividad 1: reunión de lecciones aprendidas

- Fecha de la reunión: febrero 1 de 2022
- Hora de la reunión: 5:00 PM
- Lugar: Oficinas T.I Rescue
- Dirección: Cra. 65 #8B - 91 Ofic. 485 Centro comercial terminal del sur
- Participantes: Equipo de ciberseguridad T.I Rescue, Equipo de infraestructura T.I Rescue, Manuel Flórez Lasprilla, Carlos Andrés Pabón y Farzad Londoño.

A continuación, se presentan las opiniones entregadas por integrantes del equipo T.I Rescue respecto a los ataques y controles definidos durante la evaluación del modelo de gestión de inocentes proactivo:

Tabla 26. Opinión entregada por integrante equipo Ciberseguridad T.I Rescue

Opinión	
Rol:	Ciberseguridad
Conclusión vulnerabilidades y controles:	El tener abiertos algunos puertos y no tener unas listas negras de DNS se convierte en un hueco de seguridad. Tener controlado desde firewall los puertos, solo abrir los necesarios para la operación. Tener control de listas negras y mantenerlas actualizadas utilizando sitios confiables.
Propuesta política:	Establecer política de control de cambios a nivel de firewall y la actualización de listas negras de DNS de forma automática.

Fuente: Elaboración propia

Tabla 27. Opinión entregada por integrante equipo Infraestructura T.I Rescue

Sondeo	
Rol:	Infraestructura
Conclusión vulnerabilidades y controles:	Tener cuentas con claves débiles y el umbral de bloqueo muy alto aumenta la oportunidad de que un atacante adivine las credenciales. Disminuir el umbral de bloqueo por intentos de autenticación.
Propuesta política:	Establecer política de bloqueo de cuenta a partir del 5 intento se bloquee.

Fuente: Elaboración propia

Tabla 28. Opinión entregada por integrante equipo Infraestructura T.I Rescue

Sondeo	
Rol:	Infraestructura
Conclusión vulnerabilidades y controles:	Tener cuentas con claves muy fáciles, aumenta la posibilidad de que un atacante las adivine.
Propuesta política:	Establecer política de bloqueo por intentos fallidos y de desbloqueo de cuentas.

Fuente: Elaboración propia

Lecciones aprendidas

- En general hay que tener muy en cuenta los roles de las personas que participaron en este proceso proactivo, para que sus funciones del día a día no se topen con las de estos procesos proactivos.
- Es muy importante siempre tener presente e incluir en las pruebas las posibles limitaciones a nivel de infraestructura o de seguridad que puedan impedir el desarrollo de la actividad.
- Todos los aplicativos y componentes de infraestructura deben ser analizados con herramientas que permitan detectar sus vulnerabilidades antes de sacarlos a producción.
- No se deben dejar las contraseñas que por defecto traen las aplicaciones, consolas, etc.

Actividad 2: Documentar vectores de ataque y controles definidos e implementados:

El informe elaborado por el por el equipo de ciberseguridad a la gerencia de la empresa **T.I Rescue** respecto al incidente que se detectó durante el ejercicio de prueba del modelo de gestión de incidentes proactivo se presenta en el Anexo.

4. Conclusiones

A continuación, se presentan las conclusiones del presente trabajo de investigación:

4.1. Conclusiones objetivo general

El objetivo general del presente proyecto de investigación fue proponer una mejora a un modelo de gestión de incidentes de seguridad estándar, mediante el uso de una base de conocimiento de ataques a servicios web en ambientes IoT, construida con tecnologías Honeypot, Big data y bases de datos distribuidas sobre Blockchain, que facilitara el manejo de incidentes de seguridad de la información; dicho objetivo se logró, a través del diseño de un nuevo modelo de gestión de incidentes de seguridad, formado por cinco fases: Planificación y preparación, levantamiento de información y reporte, respuesta, implementación y evaluación de controles, y reporte y lecciones aprendidas (ver capítulo 3, sección 3.4.2.1 Fases del modelo de gestión de incidentes proactivo).

El nuevo modelo pretende facilitar el manejo de eventos e incidentes de seguridad mediante a) La facilidad en la definición e implementación de controles de forma proactiva en ambientes no productivos (ambientes señuelo), basados en la información generada por el componente activo en el cual se expusieron los activos y, b) aplicando el conocimiento adquirido en el tratamiento de los eventos e incidentes de seguridad en los ambientes no productivos (ambientes señuelo), al tratamiento de eventos e incidentes en caso que se materialicen en el ambiente productivo. Dado lo anterior se puede concluir que, si se aplican las fases definidas en el modelo propuesto, este tiende a ser **proactivo**, a diferencia de los

cotejados en el presente trabajo de investigación que de acuerdo con lo expresado en el estado del arte tienden a ser reactivos. Dado lo anterior, el modelo propuesto ofrece los siguientes beneficios:

- Identificación proactiva de los eventos e incidentes de seguridad que pueden llegar a presentarse en ambientes productivos de la organización.
- Definición e implementación proactiva de controles de seguridad.

El modelo proactivo propuesto no pretende reemplazar los modelos, guía y buenas prácticas evaluados en este trabajo de investigación, dado que estos, a diferencia del modelo propuesto, tienen un enfoque reactivo ante los incidentes de seguridad, cuyo enfoque es proactivo; por el contrario, el nuevo modelo puede ser utilizado como una primera capa de seguridad en la gestión de eventos e incidentes, pues a través de este se definen e implementan controles de seguridad antes de que los eventos e incidentes se materialicen en los ambientes productivos, y los modelos, guías y buenas prácticas evaluados son utilizados una vez se presentan los eventos e incidentes en ambientes productivos.

4.2. Conclusiones objetivos específicos

Respecto a los objetivos 1) Seleccionar herramienta Honeypot, 2) Seleccionar plataforma Blockchain y 3) Seleccionar herramienta Big Data, se puede concluir que se lograron de manera exitosa, al ser seleccionadas las herramientas:

- Dionaea, mediante la evaluación de cumplimiento de características definidas (ver numeral 3.1.2. Actividad 2: Caracterización de las Honeypots) de acuerdo con las necesidades específicas del proyecto (ver numeral 2.1.2. Actividad 2: Caracterización

de las Honeypots); la Honeypot seleccionada cumplió con el objetivo para el cual fue seleccionada (ver numeral 2.1. Fase 1: Selección de Honeypot).

Como resultado, se logró la instalación como parte del componente activo (ver numeral 3.5.1.1. Instalación y configuración de Honeypot y Big Data) y exposición de un activo de información (servicio web) para lograr recolectar información sobre los vectores de ataque utilizados durante su exposición, para la posterior definición e implementación de controles en ambientes productivos.

- Hyperledger Fabric, mediante la evaluación de cumplimiento de características definidas (ver numeral 3.2.2 Actividad 2: Caracterización de proyectos Blockchain) de acuerdo con las necesidades específicas del proyecto (ver numeral 2.2.2. Actividad 2: Caracterización de proyectos Blockchain); la plataforma Blockchain seleccionada cumplió con el objetivo para el cual fue seleccionada (ver numeral 2.2. Fase 1: Selección de la cadena de bloques y definición de estructura de datos).

  Como resultado, se logró la instalación como parte del componente activo (ver numeral 3.5.1.2. Instalación de Máquina virtual Hyperledger) y el envio de información generada por la Big Data para su almacenamiento seguro en la Blockchain (ver Figura 32. Ejecución de Script Rsync).

- ELK (Elasticsearch, Logstash y Kibana), mediante la evaluación de cumplimiento de características definidas (ver numeral 3.3.2 Actividad 2: Caracterización de herramientas Big Data) de acuerdo con las necesidades específicas del proyecto (ver numeral 2.3.2. Actividad 2: Caracterización de herramientas Big Data); la plataforma Blockchain seleccionada cumplió con el objetivo para el cual fue seleccionada (ver numeral 2.3. Fase 1: Selección de herramienta Big Data).

  Como resultado, se logró la instalación como parte del componente activo (ver numeral 3.5.1.1. Instalación y configuración de Honeypot y Big Data) y posterior procesamiento de logs generados por lo Honeypot para ser mostrados en el Dashboard (ver Figura 48. Vista general Kibana y Figura 23. Vista general Elasticsearch)

Respecto al objetivo número cuatro “Definir estrategia de fortalecimiento del modelo de gestión de incidentes”, para su cumplimiento fue necesario hacer una revisión de algunos modelos, guías y buenas prácticas de gestión de incidentes de seguridad, de la cual se obtuvo como resultado una matriz comparativa de las fases y actividades que les componen, se llega a la conclusión que tanto el modelo ISO/IEC 27035 – 1 y 2 y como el NIST SP 800-61 Rev. 2 desde su propio enfoque y estructura aportan elementos a la construcción del nuevo modelo (ver 3.4.1.3. Cotejamiento de las normas seleccionadas) y en ese sentido, se utilizarán como base para la creación del nuevo modelo proactivo de gestión de incidentes de seguridad.

Para poder validar el funcionamiento del modelo propuesto y cumplir con el objetivo específico cinco “Evaluación del modelo propuesto”, fue necesario que la empresa T.I Rescue lo aplicara en el análisis de un activo instalado en su infraestructura corporativa. El equipo de infraestructura de T.I Rescue instalo las herramientas tecnológicas necesarias, selecciono el activo y lo expuso en la Honeypot durante siete días. Como resultado de la ejecución del modelo se definieron e implementaron los controles necesarios en el ambiente de producción de T.I Rescue y se evaluó su efectividad; una vez hecho esto, se concluye:

- Los controles definidos e instalados en ambiente productivo fueron efectivos contra los mismos ataques recibidos por el activo durante su exposición (Ver 3.5.2.3 Fase de respuesta).
- Fue posible ejecutar todas fases y las actividades propuestas por el modelo (Ver 3.5.2. Actividad 2: Ejecución de actividades definidas en el modelo)
- Al aplicar el modelo fue posible mitigar los incidentes de seguridad en los ambientes productivos, mediante la definición e implementación proactiva de controles, basados en la información recolectada durante los incidentes en los activos expuestos en la infraestructura señuelo (Ver 3.5.2.4. Fase de implementación y evaluación de controles)
- El modelo facilita la gestión de los incidentes de seguridad al entregar información valiosa sobre los ataques que puede llegar a recibir un activo de información (Ver 3.5.2.2. Fase de levantamiento de información y reporte)

4.3. Recomendaciones

- Las herramientas que componen la infraestructura señuelo y de análisis de información no tienen que ser las mismas seleccionadas para el presente trabajo de investigación; para su selección cada compañía puede definir los criterios de acuerdo con sus necesidades específicas.
- Para lograr una mayor cobertura de activos que pueden ser expuestos se recomienda usar una colmena de Honeypots.
- El nuevo modelo puede ser utilizado, y se recomienda para cualquier organización cuya gestión de cambios sea constante y por lo tanto quiera identificar las vulnerabilidades, riesgos y ataques a los que estarán expuestos los nuevos componentes, con el fin de tener una gestión proactiva de los eventos e incidentes de seguridad.

4.4. Trabajo futuro

Se propone como trabajo futuro la utilización de una Honeynet, con el fin de mejorar la capacidad de exposición de activos y conectar la Honeypot con el API de virus total, con el fin de lograr una ampliación de la información respecto de los ataques recibidos.

Generar métricas que permitan encontrar el porcentaje disminución de la probabilidad que se presenten incidentes de seguridad en ambientes productivos, logrados con la aplicación del modelo de gestión de incidentes proactivo.

Anexo

Informe gestión proactiva incidentes de seguridad mediante el uso de modelo de gestión de incidentes proactivo.

INFORME DE MANEJO PROACTIVO DE EVENTOS E INCIDENTE DE SEGURIDAD

En este informe se describen las vulnerabilidades y controles implementados, para darle un adecuado manejo a situaciones similares y para la definición de políticas, monitoreos y controles adicionales.

El informe de los incidentes permite responder a los mismos en forma sistemática, minimizar su ocurrencia, facilitar una recolección de posibles amenazas de manera eficiente minimizando la pérdida de información y la interrupción de los servicios, mejorar continuamente los controles.

Este Informe debe entregarse físicamente en la empresa o enviarse mediante correo electrónico en la dirección info@tirescue.com.co

Por cualquier consulta puede comunicarse a los teléfonos +57 604 6073303.

INFORME PROACTIVO DE INCIDENTE DE SEGURIDAD

Fecha de notificación: 29/01/2022	Hora de notificación: 10:00 AM

DATOS DE LA PERSONA QUE NOTIFICA	
Apellido y Nombres:	Farzad Londoño
Área / Dependencia:	Ciberseguridad
Correo electrónico:	info@tirescue.com.co
Teléfono:	57 604 6073303

INFORMACIÓN DEL INCIDENTE (Marque con una X todas las opciones que considere aplicables.**)**	
Fecha del incidente: 29/01/2022	Hora del incidente: 09:00 AM
Activo Afectado: Apache Tomcat ambiente no productivo	

X	Suplantación (Spoofing)		Denegación de Servicio
	Modificación (Tampering)		Elevación de Privilegio
	Repudio		Revelación de información

INFORMACIÓN SOBRE EL INCIDENTE

Describa brevemente cómo detectó el incidente: Por medio de la aplicación de monitoreo Kibana el equipo de ciberseguridad detecto los ataques y luego notifico lo siguiente:

Se presentó un ataque de Ataque de fuerza bruta (Brute Force), este está tratando de encontrar las credenciales de acceso del servidor Apache Tomcat. Este pretendía realizar un ataque automatizado de diccionario para encontrar las credenciales de acceso a la consola de administración.

El equipo del SOC reporta los siguientes hosts que se vieron en la consola de Kibana:

192.168.3.68,116.105.212.31,116.105.23.64,116.105.217.32,116.105.215.9,116.105.216.128,

213.167.227.164,60.173.239.156,195.3.147.47,141.98.10.60,116.98.171.205

- **Se presenta una correlación de ataques de acuerdo con el Framework Mitre ATT&CK e informa los controles a implementar en este tipo de eventos:**
    - **Tipo de ataque: Credencial Access**
    - **Técnica: Brute Force**
    - **Sub técnica: Password Guessing**

A continuación, se informan los controles definidos y su descripción.

Control: Políticas de uso de la cuenta (M1036)

Descripción: Establezca políticas de bloqueo de cuentas después de una cierta cantidad de intentos fallidos de inicio de sesión para evitar que se adivinen las contraseñas. Una política demasiado estricta puede crear una

condición de denegación de servicio y hacer que los entornos queden inutilizables, con todas las cuentas utilizadas en la fuerza bruta bloqueadas

Control: Uso de listas de DNSBL

Descripción: Establezca listas de DNSBL (Listas negras basadas en DNS) para minimizar la cantidad de ataques que puedan afectar la operación

Se aplicó la implementación de controles sobre el activo Apache Tomcat en el ambiente productivo.

Control 1:

- **Control por desplegar: Bloqueo por intentos fallidos en el activo ApacheTomcat**
- **Plataforma por impactar: Apache Tomcat.**
- **Ejecución: Usando la consola con usuario administrador, se modifica el archivo de configuración server.xml, agregando la siguiente línea así:**
  - **sudo nano $CATALINA_BASE/conf/server.xml file**
- **Se agregó la siguiente línea:**
  - **<Realm className="org.apache.catalina.realm.LockOutRealm" lockOutTime="3000" failureCount="5"/>**

Oficial: https://tomcat.apache.org/tomcat-8.0-doc/config/realm.html#LockOut_Realm_-_org.apache.catalina.realm.LockOutRealm

Control 2:

- **Control por desplegar: listas de DNSBL (listas negras basadas en DNS)**
- **Plataforma por impactar: FW pfSense.**

- **Ejecución: Ver configuración en el sitio web oficial https://tech.lobobrothers.com/rematando-con-pfblockerng-en-pfsense/**

El incidente aún está en progreso: [ ] SI [x] NO

Sistema, computadora o red afectada:

En este caso se vio comprometido solo el activo señuelo y la red configurada para ello.

Localización física:

Virtualizador Promox de la compañía

¿Existe copia de respaldo de los datos o software afectado?	x	SI		NO
¿El recurso afectado tiene conexión con la red corporativa?		SI	x	NO
¿El recurso afectado tiene conexión a Internet?	x	SI		NO

Nombres e información de contacto de otras personas que pueden tener información para asistir en la investigación del incidente: equipo Ciberseguridad y el líder.
Apellido y nombres: Farzad Londoño
Datos de contacto: +57 304 378 8390

Bibliografía

[1] D. Antonio and C. Astroz, “HoneyPot de dispositivos IoT usando una Raspberry Pi 3,” p. 52, 2018.

[2] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, “IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182–8201, 2019, doi: 10.1109/JIOT.2019.2935189.

[3] M. Skowron, A. Janicki, and W. Mazurczyk, “Traffic fingerprinting attacks on internet of things using machine learning,” *IEEE Access*, vol. 8, pp. 20386–20400, 2020, doi: 10.1109/ACCESS.2020.2969015.

[4] M. A. Al-garadi, A. Mohamed, A. Al-ali, X. Du, and M. Guizani, “A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security,” *Understanding Communication Research Methods: A Theoretical and Practical Approach*, pp. 222–237, 2019, doi: 10.4324/9780203495735-22.

[5] J. Franco, A. Aris, B. Canberk, and A. S. Uluagac, “A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and Cyber-Physical Systems,” *IEEE Communications Surveys and Tutorials*, vol. 23, no. 4, pp. 2351–2383, 2021, doi: 10.1109/COMST.2021.3106669.

[6] N. Naik, P. Jenkins, N. Savage, and L. Yang, “A computational intelligence enabled honeypot for chasing ghosts in the wires,” *Complex & Intelligent Systems*, Nov. 2020, doi: 10.1007/s40747-020-00209-5.

[7] J. Franco, A. Aris, B. Canberk, and A. S. Uluagac, “A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and Cyber-Physical Systems,” *IEEE Communications Surveys and Tutorials*, vol. 23, no. 4, pp. 2351–2383, 2021, doi: 10.1109/COMST.2021.3106669.

[8] Instituto Nacional de Ciberseguridad, “Guía de implantación de un honeypot industrial,” 2019.

[9] M. Favaretto, E. de Clercq, C. O. Schneble, and B. S. Elger, “What is your definition of Big Data? Researchers’ understanding of the phenomenon of the decade,” *PLoS ONE*, vol. 15, no. 2, pp. 1–20, 2020, doi: 10.1371/journal.pone.0228987.

[10] T. R. Rao, P. Mitra, R. Bhatt, and A. Goswami, *The big data system, components, tools, and technologies: a survey*, vol. 60, no. 3. Springer London, 2019. doi: 10.1007/s10115-018-1248-0.

[11] A. B. Mohd, “Evolution of Big Data and Tools for Big Data,” *Journal of Interdisciplinary Cycle Research*, vol. XII, no. X, p. 309, 2020.

[12] N. Deepa *et al.*, “A Survey on Blockchain for Big Data: Approaches, Opportunities, and Future Directions,” Sep. 2020, [Online]. Available: http://arxiv.org/abs/2009.00858

[13] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, “Blockchain for the IoT and industrial IoT: A review,” *Internet of Things*, vol. 10, no. 66, p. 100081, 2020, doi: 10.1016/j.iot.2019.100081.

[14] “A Blockchain Platform for the Enterprise — hyperledger-fabric docs master documentation.” https://hyperledger-fabric.readthedocs.io/en/release-2.2/ (accessed May 24, 2021).

[15] Y. Rodríguez Cruz, “Gestión de Información y del Conocimiento para la toma de decisiones organizacionales.,” *Bibliotecas. Anales de Investigación*, vol. 11, no. 11, pp. 150–163, 2015.

[16] “Servicios Web - IBM Documentation.” https://www.ibm.com/docs/es/was/9.0.5?topic=services-web (accessed Apr. 18, 2021).

[17] “Que es un servidor WEB? - Aprende sobre desarrollo web | MDN.” https://developer.mozilla.org/es/docs/Learn/Common_questions/What_is_a_web_server (accessed Apr. 18, 2021).

[18] Raspberry Pi Foundation, “Raspberry Pi Foundation - About Us,” *Raspberry Pi Foundation*, 2016. https://www.raspberrypi.org/about/ (accessed Mar. 03, 2021).

[19] Raspberry pi Foundation, “Buy a Raspberry Pi 4 Model B – Raspberry Pi,” *Raspberry Pi*, 2020. https://www.raspberrypi.org/products/ (accessed Mar. 15, 2021).

[20] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, “NIST Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide Recommendations,” *NIST Special Publication*, 2012.

[21] R. T. Sataloff, M. M. Johns, and K. M. Kost, *Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información*. 2012.

[22] National Institute of Standards and Technology, “NIST Mission, Vision, Core Competencies, and Core Values | NIST,” 2017. https://www.nist.gov/about-nist/our-organization/mission-vision-values (accessed Feb. 28, 2021).

[23] Instituto Nacional de Ciberseguridad, “Honeypot, una herramienta para conocer al enemigo | CERTSI,” *Instituto Nacional de Ciberseguridad de España*, Jun. 2018.

[24] A. I. y Peter Bonner and G. Holloway, “Organismos Nacionales de Normalización en Países en Desarrollo,” *Progresar Rapidamente*, p. 88, 2010.

[25] R. Sanchez and J. Enrique, “INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security,” vol. 2016, 2017.

[26] A. Acien, A. Nieto, G. Fernandez, and J. Lopez, “Definición de procedimientos para fabricar honeypots IoT basados en criterios de búsqueda,” 2018.

[27] A. Boukhalfa, N. Hmina, and H. Chaoui, *A Honey Net, Big Data and RNN Architecture for Automatic Security Monitoring of Information System*, Vol 915. S., vol. 3, no. 2. Tangier, Morocco: Springer International Publishing, 2019. doi: 10.1007/978-3-030-11928-7.

[28] W. Zhang, B. Zhang, Y. Zhou, H. He, and Z. Ding, “An IoT Honeynet Based on Multiport Honeypots for Capturing IoT Attacks,” *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3991–3999, 2020, doi: 10.1109/JIOT.2019.2956173.

[29] S. Tripathi and R. Kumar, “Raspberry Pi as an Intrusion Detection System, a Honeypot and a Packet Analyzer,” *Proceedings of the International Conference on*

Computational Techniques, Electronics and Mechanical Systems, CTEMS 2018, pp. 80–85, 2018, doi: 10.1109/CTEMS.2018.8769135.

[30] V. A. Zamfir, M. Carabas, C. Carabas, and N. Tapus, "Systems monitoring and big data analysis using the elasticsearch system," *Proceedings - 2019 22nd International Conference on Control Systems and Computer Science, CSCS 2019*, pp. 188–193, 2019, doi: 10.1109/CSCS.2019.00039.

[31] E. Bandara *et al.*, "Mystiko - Blockchain Meets Big Data," *Proceedings - 2018 IEEE International Conference on Big Data, Big Data 2018*, pp. 3024–3032, 2019, doi: 10.1109/BigData.2018.8622341.

[32] F. Humberto Gómez Orjuela Héctor Valencia Valencia, "Diseño de un procedimiento de gestión de incidentes de ciberseguridad que articule la gestión de riesgos, continuidad, crisis y resiliencia que se pueda integrar a la respuesta corporativa."

[33] A. Z. Tabari and X. Ou, "A First Step Towards Understanding Real-world Attacks on IoT Devices," 2020.

[34] T. Luo, Z. Xu, X. Jin, Y. Jia, and X. Ouyang, "IoTCandyJar: Towards an Intelligent-Interaction Honeypot for IoT Devices," *Black Hat 2017*, pp. 1–11, 2017.

[35] M. Wang, J. Santillan, and F. Kuipers, "ThingPot: an interactive Internet-of-Things honeypot," 2018.

[36] P. Krishnaprasad, "Capturing attacks on IoT devices with a multi-purpose IoT honeypot," no. May, 2017.

[37] "El ELK Stack: de los creadores de Elasticsearch. | Elastic." https://www.elastic.co/es/what-is/elk-stack (accessed May 29, 2022).

[38] “Las herramientas Elastic — documentación de ManualKibanaOCDS - latest.” https://manualkibanaocds.readthedocs.io/es/latest/C2/Seccion1.html#las-ventajas-de-la-plataforma-elk (accessed May 29, 2022).

[39] CCP - MINTIC, “Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.” Accessed: Jan. 21, 2022. [Online]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

[40] S. Q. Tascon and J. Z. Jiménez, “Modelo para la gestión de incidentes de seguridad en redes industriales SCADA a través del algoritmo de predicción Filtro Kalman,” 2019.

[41] “MITRE ATT&CK®.” https://attack.mitre.org/ (accessed Feb. 05, 2022).

[42] “Rematando con pfBlockerNG en Pfsense - Tech LBT.” https://tech.lobobrothers.com/rematando-con-pfblockerng-en-pfsense/ (accessed Feb. 12, 2022).