DISEÑO TÉCNICO DEL EQUIPO DE RESPUESTA ANTE INCIDENCIAS DE SEGURIDAD INFORMÁTICAS (CSIRT) EN LA EMPRESA “CYBERSECURITY DE COLOMBIA LTDA”

JOSÉ ENRIQUE DURÁN GRANADOS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PAMPLONA
2020

DISEÑO TÉCNICO DEL EQUIPO DE RESPUESTA ANTE INCIDENCIAS DE SEGURIDAD INFORMÁTICAS (CSIRT) EN LA EMPRESA “CYBERSECURITY DE COLOMBIA LTDA”

JOSÉ ENRIQUE DURÁN GRANADOS

Proyecto de Grado – Proyecto aplicado presentado para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMATICA

Katerine Márceles Villalba.
Tutora de Curso
Katerine Márceles Villalba
Asesora

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PAMPLONA
2020

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

El desarrollo de este documento de trabajo de grado para optar el título de Especialista en Seguridad Informática lo dedico principalmente a Dios todo poderoso por ser mi guía y soporte en el camino, también a mi familia por el apoyo, ánimo y paciencia durante todo este proceso formativo.

AGRADECIMIENTOS

Agradezco a la Universidad Nacional Abierta y a Distancia UNAD por brindarme la oportunidad de poder hacer parte de la especialización en Seguridad Informática y además por la construcción de un plan de estudios tan completo y concordante con las necesidades actuales en esta materia.

Agradezco a todos los directores de curso y tutores, quienes con sus valiosos aportes, orientación, motivación y constancia me han brindado las herramientas suficientes para comprender y alcanzar las habilidades necesarias en materia de seguridad informática y sus campos complementarios.

Agradezco a la directora del trabajo de grado profesora Katerine Marceles Villalba, ya que gracias a su constante motivación y apoyo dio lugar al avance y consecución del proyecto a pesar de las adversidades que se dieron durante su construcción y ejecución.

CONTENIDO

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

GLOSARIO

Autenticación: Procedimiento para la verificación de la identidad del actor que reclama el acceso a un sistema o componente digital.

Autorización: Acciones mediante las cuales se le otorgan permisos a un usuario para acceder a un sistema informático.

Certificado digital: Componente que permite la validación de la identidad mediante una llave de cifrado pública.

Cifrar: Transformación de un elemento digital en otro con el fin de ocultar su significado real.

Confidencialidad: Pilar de la seguridad informática que se encarga de evitar que usuarios no autorizados accedan a la información.

Controles: Elementos o acciones que buscan evitar o identificar violaciones a los componentes de un sistema estos pueden ser detectados o disuasivos.

Criptografía: Ciencia encargada de la investigación construcción y validación de procesos de cifrado de información.

CSIRT: Equipo de atención a incidentes de seguridad informática

Descifrado: Proceso inverso al cifrado de información mediante el cual se obtiene acceso al mensaje original.

Disponibilidad: Pilar de la seguridad informática enfocado en garantizar que la información contenida en un sistema esté siempre disponible.

Dirección IP: Acrónimo de “Internet Protocol”, correspondiente a un número único que no se puede repetir en una red ya que este identifica el host correspondiente.

Dirección MAC: Control de acceso al medio, corresponde a un valor de 48 bits que permite la identificación de todos los dispositivos conectados a una red.

Firewall: Componente físico o lógico que permite el control de tráfico en las redes de comunicaciones.

FTP: El protocolo de transferencia de archivos es un servicio que permite enviar archivos sobre una red de comunicaciones.

Hardware: Parte física y tangible de los componentes de un sistema informático conformado por los componentes eléctricos, electrónicos y de protección.

HTTPS: Protocolo que permite la trasferencia de información entre un navegador Web y un servidor Web de forma segura mediante el uso de un algoritmo de cifrado simétrico.

Información: Recursos electrónicos desarrollados con el fin de documentar a los usuarios en una temática específica o el almacenamiento estructurado de datos.

Informática forense: Proceso investigativo sobre un sistema informático que permita obtener evidencia para el desarrollo de procesos judiciales o administrativos asociados a incidentes de seguridad informática.

Incidente de seguridad: Suceso relacionado con el incumplimiento o intento de incumplimiento de cualquiera de los pilares de la seguridad informática Integridad, Disponibilidad o Confidencialidad en el contexto de un sistema.

IDS: Sistema de detección de intrusos dentro de un sistema informático o una red de comunicaciones.

Integridad: Pilar de la seguridad informática que permite garantizar la completitud y exactitud de la información contenida en un sistema.

Plataforma tecnológica: Conjunto de hardware y software usado por entidades, compañías o empresas.

Servidor: Entendido como hardware o software que realiza tareas previamente diseñadas encaminas a facilitar las tareas de los usuarios.

Sistema operativo: Programa informático que se encarga de la gestión de los recursos hardware y facilitar la interacción con el usuario.

Software: Conjunto de instrucciones hechas para realizar una tarea específica en un computador de forma fácil y amigable.

SSL: Capa de seguridad que proporciona un protocolo criptográfico que permite la comunicación segura a través de redes de datos de extremo a extremo.

Virtualización: Mecanismo que permite la implementación dentro de un entorno virtual de algún recurso físico como una computadora u otro dispositivo.

Vulnerabilidad: Deficiencias o fallos dentro de un sistema informático que dan oportunidad a los agresores de realizar acciones no legítimas aprovechándose de estas debilidades.

RESUMEN

Siendo de vital importancia comprender que los sistemas informáticos se ven constantemente amenazados por las diferentes formas de espionaje, vandalismo, fraude, accidentes o sabotaje presentes en la actualidad por medio de diferentes riesgos entre los cuales se destacan los virus, los ataques a la infraestructura, daños voluntarios, daños involuntarios, accidentes, fallas técnicas o catástrofes naturales.

La empresa Cybersecurity de Colombia LTDA, que es una empresa Colombiana que presta servicios de seguridad para la protección de la Información, se plantea el diseño y creación de un Equipo de Respuesta ante Emergencias Informáticas (CSIRT) para dar respuesta a incidentes o de gestión de vulnerabilidades a sus clientes.

Lo anterior, con motivo de que se pueda brindar mejor soporte y tratamiento a los incidentes de seguridad que en la época actual no cesan y que además logren crear mecanismos para la prevención y corrección de vulnerabilidades.

Por lo tanto en el presente trabajo se realizan diferentes acciones encaminadas en la consecución y puesta en funcionamiento inicial del CSIRT de Cybersecurity de Colombia LTDA entre las cuales se encuentran la revisión de herramientas tecnológicas disponibles para el desarrollo de las funciones, la selección de las herramientas de acuerdo a los tipo de licenciamiento, uso y disponibilidad, la propuesta de estructura organizacional tomando como referente diferentes casos de éxito en procesos similares y finalmente la construcción de un laboratorio basado en la formulación de un escenario problema que atendiera a necesidades cercanas a las presentadas en la realidad usando un entorno controlado y verificable.

ABSTRACT

Being of vital importance to understand that computer systems are constantly threatened by the different forms of espionage, vandalism, fraud, accidents or sabotage present today through different risks, among which viruses, attacks on the infrastructure, voluntary damages, involuntary damages, accidents, technical failures or natural catastrophes.

The company Cybersecurity de Colombia LTDA, which is a Colombian company that provides security services for the protection of Information, considers the design and creation of a Computer Emergency Response Team (CSIRT) to respond to incidents or management of vulnerabilities to your customers.

The foregoing, because it is possible to provide better support and treatment to security incidents that do not cease at the current time and that also manage to create mechanisms for the prevention and correction of vulnerabilities.

Therefore, in the present work, different actions are carried out aimed at the achievement and initial implementation of the CSIRT of Cybersecurity de Colombia LTDA, among which are the review of technological tools available for the development of the functions, the selection of tools According to the type of licensing, use and availability, the proposed organizational structure taking as a reference different cases of success in similar processes and finally the construction of a laboratory based on the formulation of a problem scenario that would meet needs close to those presented in reality using a controlled and verifiable environment.

INTRODUCCIÓN

El mundo de hoy se rige por el uso de los sistemas informáticos en la mayor parte de los aspectos de la vida tanto cotidiana como empresarial, es así como estos están influenciando cada vez más la forma de cómo funciona todo el entorno en el que se encuentran las personas, las organizaciones, las empresas, las instituciones y los estados.

Cabe entonces preguntarse cuál sería el impacto que la sociedad / tecnología tendría en caso de presentarse un fallo o ataque a los sistemas informáticos y si en su contexto se han establecido equipos de expertos en materia de seguridad informática que puedan por una parte tratar los incidentes informáticos y por otra llevar a cabo los procesos de actualización e investigación necesarios para mantener a los usuarios informados de las diferentes amenazas, como actuar frente a los incidentes, como minimizar su impacto y como prevenir que estos vuelvan a ocurrir.

Atendiendo lo manifestado anterior mente, la empresa “Cybersecurity de Colombia LTDA” cuyo campo de operación es la seguridad informática se propone consolidarse como un Centro de Respuesta a Incidentes Cibernéticos en el ámbito de **CSIRT** a partir del año 2021, por lo cual se encuentra en el proceso de reunir las capacidades necesarias para alcanzar este objetivo y por esta misma vía buscará crear y gestionar las funciones de respuesta a incidentes cibernéticos, ofreciendo servicios que permitan dar soporte a sus clientes teniendo presente el nivel de servicio ya sea en respuesta a incidentes o en gestión de vulnerabilidades.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Los activos de información y su operatividad en muchos contextos son de incalculable valor; razón por la que estos deben ser administrados de la mejor forma posible motivo por el que durante algún tiempo han surgido producto de la experiencia y de las tecnologías modelos, estándares, equipamiento físico, campos de estudio, instituciones y mecanismos que faciliten el desarrollo de este proceso.

En atención a esto las grandes organizaciones y los gobiernos de todo el mundo han enfilado considerables capitales, humanos, tecnológicos y económicos, atendiendo a la creciente amenaza y riesgo al que se enfrentan los sistemas ya sea por factores accidentales, catástrofes o agresores tecnológicos[1].

En el contexto colombiano el estado por medio del Ministerio de las Tecnologías de Información y Comunicación (MinTIC) a través de diferentes estrategias entre las que se destaca la Política de Gobierno Digital[2], la cual contempla y prioriza la seguridad de la información en su componente Seguridad y Privacidad de la Información y el Modelo de Seguridad y Privacidad de la Información; Políticas de estado que buscan lograr fortalecer la seguridad de la informática en las entidades públicas intentando garantizar la protección de los sistemas informáticos y la información digitalizada del uso, divulgación, destrucción, modificación o interrupción desautorizada.

Es así como desde diferentes escenarios se visibiliza la necesidad de adoptar y contar con instrumentos que permitan garantizar, atender y ofrecer mecanismos bien estructurados que el lugar que corresponde a la protección de los datos desde el punto de vista correctivo pero sin hacer a un lado la prevención de posibles incidentes que puedan afectar a las organizaciones.

De esta forma las empresas que brindan servicios de seguridad de la información requieren del diseño de equipos de trabajo altamente competentes en esta materia;

---

[1] **OSPINA JARRO, Eduardo Andres. 2018.** Modelo de protección de activos de información estratégica: una lectura desde la dirección y gerencia de la seguridad de la información. [En línea] 2018. [Citado el: 28 de 11 de 2020.] https://repository.urosario.edu.co/bitstream/handle/10336/20003/UR-ArtInvestigacion-EduardoAndresOspinaJarro.pdf?sequence=1&isAllowed=y

[2] **COLOMBIA. MINISTERIO DE LAS TIC. 2019.** Manual de gobierno digital. [En línea] 04 de 2019. [Citado el: 30 de 11 de 2020.] https://www.mintic.gov.co/portal/604/articles-81473_recurso_1.pdf

los cuales tendrán la responsabilidad de dar un a manejo optimo a las vulnerabilidades e incidentes de seguridad y contribuir con la mejora continua de las actividades de protección orientadas a la prevención de agresiones futuras y la reducción del impacto de las que logren materializarse[3].

1.2 FORMULACIÓN DEL PROBLEMA

Los activos de información y la operación de servicios de tecnología representan hoy día para las organizaciones, las instituciones, las empresas y las personas factores fundamentales en el desarrollo de actividades convirtiéndose estos continuamente en el blanco de agresiones informáticas razón por la cual el presente proyecto se plantea el siguiente interrogante.

¿Qué tan importante es para la empresa Cybersecurity de Colombia LTDA, contar con Equipo de Respuesta ante Emergencias Informáticas (CSIRT)?

[3] **ESPAÑA. CENTRO CRIPTOLÓGICO NACIONAL. 2011.** Guía de Creación de un CERT/CSIRT. [En línea] 09 de 2011. [Citado el: 27 de 11 de 2020.] https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-sep11.pdf

2 JUSTIFICACIÓN

En la actualidad el mundo se rige indudablemente por el control, operación y funcionamiento eficiente de los sistemas informáticos, los cuales, de diferentes maneras, afectan la vida y el comportamiento de las personas, llegando a tal punto que los sistemas informáticos combinados con sistemas de otros campos intervienen en aspectos tan fundamentales como el procesamiento del agua, la producción de alimentos, el comportamientos de los grupos sociales, la toma de decisiones políticas o simplemente la forma de pensar y actuar de un individuo.

En concordancia con lo anterior, y debido a la fuerte necesidad de garantizar la operación ininterrumpida de los sistemas y el resguardo de la información, la seguridad informática juega un papel fundamental en el aseguramiento, control y operación de los procesos, permitiendo implementar al interior de las organizaciones políticas, normas, planes, estrategias y herramientas con el objetivo de minimizar los riesgos y aumentar las posibilidades de cumplir con sus metas y objetivos de valor.

Es así, como en los últimos años el estado colombiano a través del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) ha realizado grandes esfuerzos enfocados en la protección de la información de los ciudadanos y las entidades estatales por medio de la reglamentación y la implementación de modelos y estándares de seguridad informática que permiten la reducción de los incidentes causados por accidentes de usuarios autorizados o de agentes externos con la intención de llevar a cabo acciones de saboteo, robo o delincuencia, conocidos como transgresores informáticos.

Ante esta situación se hace necesario que las instituciones, empresas, organizaciones o entidades de los diferentes sectores adopten y las apliquen los diferentes estándares, políticas, lineamientos, y recomendaciones existentes en la actualidad, con el objetivo de que estos contribuyan a alcanzar las metas y propósitos en el ámbito de seguridad de datos, la prestación continua, eficiente y confiable de los servicios que proveen.

Motivos por los cuales es necesario que se creen equipos de trabajo altamente competentes en capacidades afines con la seguridad informática por medio de los cuales se dé un tratamiento adecuado a los incidentes informáticos partiendo del punto de la recepción hasta la entrega de la respuesta de los mismos; además de la divulgación de información que permita a la comunidad tecnológica tomar acciones de prevención de agresiones informáticas.

Es allí donde cobra gran importancia el diseño y planificación de un Equipo de Respuesta ante Emergencias Informáticas (CSIRT), que se encargue de dirigir por el camino correcto los procesos de recepción, análisis y respuesta de informes referentes a acciones de seguridad informática y más aun teniendo en cuenta el quehacer de Cybersecurity de Colombia LTDA, que presta servicios de seguridad para la protección de la Información.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Diseñar técnicamente el Equipo de Respuesta ante Incidencias de Seguridad Informáticas (CSIRT) en la empresa “Cybersecurity de Colombia LTDA”.

3. 2 OBJETIVOS ESPECÍFICOS

1. Realizar la recopilación de información referente a herramientas software que den lugar al desarrollo de los servicios reactivos y proactivos del CSIRT.

2. Definir el mapa de la estructura TI del CSIRT teniendo como base las mínimas dependencias para su correcto funcionamiento.

3. Consolidar la información necesaria acerca de las herramientas software para que el CSIRT pueda ejecutar sus actividades correctamente.

4. Desarrollar el diseño de un laboratorio controlado por medio del uso de máquinas virtuales que permita la ejecución de pruebas del software que se utilizarán en el CSIRT.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 La importancia de un CSIRT en una organización. El crecimiento y materialización constante de amenazas y agresiones informáticas que se ha presentado en los últimos tiempos según lo mencionado en el Informe de las tendencias del Cibercrimen en Colombia (2019 - 2020)[4], demuestra que las organizaciones, los entes gubernamentales, empresas privadas y cualquier otro actor fijen su mirada con mayor cuidado hacia los incidentes de seguridad teniendo en cuenta que la era en la que nos encontramos, un alto porcentaje de información y operaciones son almacenadas y realizadas en sistemas computacionales lo cual obliga a los mismos a pensar en la protección de sus activos, dar tratamiento a los incidentes, plantear salvaguardas, identificar impactos y determinar nuevas o ya existentes amenazas.

Según esto en los distintos niveles de las organizaciones deben comprender que los asuntos relacionados con la seguridad informática requieren de un conjunto de disciplinas y personas que cuenten con las capacidades necesarias para dar un manejo de los incidentes de seguridad informática, esto partiendo del hecho de que aunque se hagan ejercicios bien elaborados de prevención de riesgos estos a su vez no logran contrarrestar todas las amenazas, ya que por su misma naturaleza estas cambian todo el tiempo y es allí donde los CSIRT dejan ver su gran valor frente al tratamiento especializado y centralizado de los casos de agresiones informáticas así como del manejo adecuado y eficiente de diferentes evidencias derivadas de procesos de investigación[5].

[4] **CCIT- POLICIA NACIONAL DE COLOMBIA. 2020.** Informe de las tendencias del cibercrimen en Colombia (2019-2020). [En línea] 20 de 10 de 2020. [Citado el: 28 de 11 de 2020.] https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf.

[5] **GARCÍA, Mónica Alexandra. 2014**. Propuesta de diseño de un área informática forense para un equipo de respuestas ante incidentes de seguridad informáticos, CSIRT. [En línea] 2014. [Citado el: 28 de 11 de 2020.] http://repositorio.espe.edu.ec/bitstream/21000/8063/1/T-ESPE-047639.pdf.

4.1.2 Cómo afectan el impacto de las agresiones informáticas en un ambiente organizacional. Según lo mencionado por el Ministerio de las TIC[6], la materialización de las agresiones informáticas causan diferentes tipos de impacto al interior de las organizaciones estos se derivan de la evaluación y el análisis de los riegos dando como resultado los siguientes grados:

- **Alto impacto:** Hace referencia a la materialización de amenazas sobre activos de información o de servicios que influyen directamente sobre el desarrollo de los objetivos misionales de la organización los cuales deben ser atendidos de forma inmediata.

- **Medio impacto:** Hace referencia a la materialización de amenazas sobre activos de información o de servicios que influyen directamente sobre el desarrollo de procesos determinados no relacionados con los objetivos misionales de la organización.

- **Bajo impacto:** Hace referencia a la materialización de amenazas sobre activos de información o de servicios de grado menor o poca significancia, pero a los cuales se les debe realizar seguimiento y monitoreo para evitar que se conviertan en incidentes de grado más alto.

Tal como se describió anteriormente, los incidentes de seguridad se pueden presentar en cualquier nivel o proceso de las organizaciones y por ello es fundamental contar con los mecanismos suficientes que den lugar a la prevención y manejo técnico de cada uno de ellos con el fin de mantener baja la probabilidad de que las entidades sean sometidas a pérdidas de información, traumatismos en la prestación de servicios o falta de operación.

4.1.3 El problema de no gestionar los incidentes de seguridad informática. El manejo inadecuado por la no gestión de los incidentes de seguridad informática pueden llegar a generar impactos serios dentro el desarrollo de las actividades normales de las organizaciones, ya que según el grado al que corresponda éste se puede llegar a causar la detención total de las actividades desarrolladas por la organización.

Además, de esto también es importante mencionar que por más que un incidente de seguridad informática no haya causado daños significativos o haya sido dirigido

[6] **MINTIC. 2016.** Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. [En línea] 2016. [Citado el: 28 de 11 de 2020.] https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf.

hacia activos de poco valor el no tratamiento de estos puede generar impactos más fuertes e inclusive llegar a convertirse en un incidente mayor como es el caso de algunos virus que no causan daños inicialmente pero luego van creciendo y transmitiéndose por las redes de comunicaciones y los dispositivos de almacenamiento hasta el punto de afectar recursos de todo tipo y valor.

Es por esto que la no gestión de los incidentes de seguridad informática y la falta de monitoreo a los recursos pueden llegar ser catastróficos en términos de continuidad del negocio, cumplimiento de metas y objetivos de valor.

Desde este punto de vista según lo expresado en reportes de impacto de incidentes de seguridad digital en el caso de sector financiero apuntan a un valor promedio de 210 dólares por registro y una inversión aproximada entre el 1% y el 5% del EBITDA (Ganancias antes de intereses, impuestos, depreciación y amortización)[7], lo que representa un costo bastante representativo.

4.1.4 La necesidad de asistencia técnica especializada en gestión de incidentes de seguridad informática. Muchas empresas, organizaciones entidades o personas que son víctimas de agresiones informáticas en la mayoría de los casos no cuentan con el personal experto o el personal de los equipos de informática no tiene la formación necesaria para dar la atención a adecuada a estos incidentes motivo por el cual en un alto porcentaje estos se quedan sin el debido tratamiento y con los riegos vigentes.

Siendo este punto donde sobresale la necesidad de contar con mecanismos bien definidos que cuenten tanto con la estructura técnica y operacional suficiente para cumplir con estas actividades de forma sencilla y accesible teniendo en cuenta que en esta materia los procesos de formación, operación e investigación generalmente no están en la medida de muchas organizaciones o personas que estas representan y a su vez la necesidad importante que representan al momento de la atención de agresiones informáticas o la detección de amenazas.

[7] **SÁNCHEZ, Héctor Mauricio y RODRÍGUEZ PARRA, Alexander. 2019.** Constitución de un CSIRT para una Entidad Financiera en Colombia. [En línea] 12 de 2019. [Citado el: 28 de 11 de 2020.] https://proyectosmaestrias.virtual.uniandes.edu.co/images/TNQzugjz0p1d26AM6aQVaAs8MbHg9RzfnHBnKmhf.pdf.

4.2 MARCO CONCEPTUAL

4.2.1 Seguridad informática. La seguridad informática es el conjunto de procesos orientados a la protección y prevención del uso no autorizado de los activos tecnológicos por agentes con malas o buenas intenciones o por simple accidente[8].

La seguridad informática se compone de cuatro pilares fundamentales:

Confidencialidad: Se ocupa de garantizar que los usuarios accedan exclusivamente a los recursos asignados y que usuarios no autorizados no logren ingresar.

Integridad: Se encarga de garantizar que los recursos solo sean modificados por los usuarios autorizados logrando de esta forma mantener la información original y solo con los cambios realizados por los usuarios autorizados.

Disponibilidad: Es responsable de mantener los recursos tecnológicos disponibles cuando estos sean necesarios, lo cual se traduce en brindar las garantías requeridas para la continuidad del negocio.

Autenticación: Es el llamado a brindar las garantías necesarias para asegurar a los usuarios que se están comunicando efectivamente con quien piensan que lo están haciendo.

4.2.2 CSIRT. El término CSIRT proviene de inglés (Computer Emergency Response Team) y que en idioma español traduce Equipo de Respuesta ante Emergencias Informáticas, el cual se puede entender como una organización dedicada a la recepción, análisis y respuesta de informes referentes a acciones de seguridad informática[9].

Es así que con el aumento constante de las amenazar informáticas que se encuentran hoy en día y con el crecimiento constante presentado en los últimos tiempos, se ha creado un escenario propicio para que las organizaciones, los entes gubernamentales, empresas privadas y demás; fijen su mirada con mayor cuidado

[8] **QUINTERO TAMAYO, John. 2016.** Introducción a la seguridad informática - OVA. [En línea] 2016. [Citado el: 28 de 11 de 2020.] http://stadium.unad.edu.co/ovas/10596_9956/seguridad_informtica.html

[9] **GORGONA, Luis. 2015.** Primera respuesta: antes de que llegue la policía. [En línea] 2015. [Citado el: 28 de 11 de 2020.] https://www.oas.org/juridico/spanish/cyber/cyb46_csirts_sp.pdf

hacia los incidentes de seguridad teniendo en cuenta que la era en la que nos encontramos, un alto porcentaje de información y operaciones son almacenadas y realizadas en sistemas computacionales lo cual obliga a los mismos a pensar en la protección de sus activos[10].

Por lo anteriormente mencionado los distintos niveles de las organizaciones han logrado comprender que los asuntos relacionados con la seguridad informática requieren de un conjunto de disciplinas y personas que cuenten con las capacidades necesarias para dar un manejo de los incidentes de seguridad informática, esto partiendo del hecho de que aunque se hagan ejercicios bien elaborados de prevención de riesgos estos a su vez no logran contrarrestar todas las amenazas ya que por su misma naturaleza estas cambian todo el tiempo y es allí donde el concepto de CSIRT deja ver su gran valor frente al tratamiento especializado y centralizado de los casos de agresiones informáticas así como del manejo adecuado y eficiente de diferentes evidencias derivadas de procesos de investigación[11].

4.2.3 Amenaza. Son todas aquellas circunstancias, personas o eventos que pueden llegar a tener la capacidad de ocasionar afectación de algún tipo a uno o varios sistemas informáticos; tales como el acceso no autorizado, modificación, eliminación o ingreso de datos, deterioro o pérdida de disponibilidad. [12]

4.2.4 Vulnerabilidad. Las vulnerabilidades son entendidas como todos aquellas debilidades presentes en los sistemas informáticos, estas provienen de diferentes factores entre los que se encuentran principalmente los fallos en los diseños, la no aplicación adecuada de prácticas de desarrollo o la no aplicación de los controles necesarios; estos fallos de seguridad pueden causar que los posibles agresores informáticos violen los principios de la seguridad informática la disponibilidad, la integridad y la confidencialidad[13].

Actualmente existen muchos tipos diferentes de vulnerabilidades, las cuales se agrupan en tres grupos Vulnerabilidades como en: recursos instalados,

[10] **MENDOZA, Miguel Ángel. 2015.** ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes? [En línea] 18 de 05 de 2015. [Citado el: 01 de 05 de 2020.] https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

[11] **GARCÍA, Mónica Alexandra. 2014.** Propuesta de diseño de un área informática forense para un equipo de respuestas ante incidentes de seguridad informáticos, CSIRT. [En línea] 2014. [Citado el: 28 de 11 de 2020.] http://repositorio.espe.edu.ec/bitstream/21000/8063/1/T-ESPE-047639.pdf.

[12] **MINTIC. 2016.** Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. [En línea] 2016. [Citado el: 28 de 11 de 2020.] https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

[13] **MARKER, Graciela. 2020.** Vulnerabilidades informáticas. [En línea] 22 de 07 de 2020. [Citado el: 28 de 11 de 2020.] https://www.tecnologia-informatica.com/vulnerabilidades-informaticas/.

Vulnerabilidades ya conocidas en recursos no instalados y Vulnerabilidades no conocidas; sumado a esto la vulnerabilidades se clasifican de acuerdo a su grado de impacto estas son: Gravedad baja, Gravedad media, Gravedad de gran importancia y Gravedad critica[14].

4.2.5 Riesgo. Es entendido como la posibilidad o probabilidad de que una amenaza sea materializada o aprovechada por parte de un atacante o factor adverso[15].

4.2.6 Análisis de riesgos. Proceso mediante el cual se lleva a cabo la identificación de activos informáticos, la determinación posibles vulnerabilidades, la definición del tratamiento de las vulnerabilidades y la decisión conjunto con los responsables del activo sí el riesgo se acepta, se disminuye la probabilidad de ocurrencia o se mitiga[16].

4.2.7 Impacto. Es el proceso de cálculo previo o posterior a la ocurrencia de un incidente de seguridad informática mediante el cual se determina el grado de afectación que tendrán los activos informáticos involucrados en caso de materializarse una amenaza.

4.2.8 Incidente de seguridad informática. Son eventos que ocurren a un entorno informático en los que se ven comprometidos los pilares fundamentales de la seguridad informática (Confidencialidad, Integridad o Disponibilidad), esto por medio de la materialización de una amenaza que viola inminentemente las políticas de seguridad o los controles establecidos para el activo o activos afectados[17].

4.2.9 Ataque. Evento adverso que atenta sobre el funcionamiento normal de un sistema informático y que puede generar o no afectación sobre el funcionamiento normal del activo o grupo de activos agredidos.

---

[14] **UNIVERSIDAD INTERNACIONAL DEL VALENCIA. 2018.** www.universidadviu.com. *Vulnerabilidad informática, tipos y debilidades principales.* [En línea] 24 de 04 de 2018. [Citado el: 28 de 11 de 2020.] https://www.universidadviu.com/vulnerabilidad-informatica-tipos-debilidades-principales/

[15] **PARRA MORENO, Duver Augusto. 2012.** Gestión del riesgo en la seguridad informática: "Cultura de la auto-seguridad informática". [En línea] 2012. [Citado el: 28 de 11 de 2020.] https://repository.unimilitar.edu.co/bitstream/handle/10654/6821/ParraMorenoDuverAugusto2012.pdf;jsessionid=C43AFCD7F74F007A88D99FB1613DB1E8?sequence=2

[16] **LAGORIO, Florencia y PAYERO, Abril. 2016.** Riesgos Informaticos. [En línea] 2016. [Citado el: 29 de 11 de 2020.] https://sites.google.com/site/tecnologiadigital20/home/riesgos-informaticos

[17] **ECURED. 2010.** Seguridad Informática. [En línea] 2010. [Citado el: 29 de 11 de 2020.] https://www.ecured.cu/Seguridad_Inform%C3%A1tica

4.2.10 Desastre. Ocurre posteriormente a la materialización exitosa de una amenaza generando como consecuencia la ruptura de la capacidad normal de operación de los activos informáticos comprometiendo uno o varios de los pilares fundamentales de la seguridad informática (Confidencialidad, Integridad o Disponibilidad)

4.3 MARCO HISTÓRICO

Colombia, es uno de los países de la región en el cual se ha incrementado considerablemente el uso de las tecnologías de la información y las comunicaciones en los últimos años en los diferentes sectores económicos y sociales con lo cual se han alcanzado altos niveles de inversión en el país desde los sectores privados y también los públicos.

Es de esta forma que Colombia ha despertado la atención de gigantes tecnológicos de cobertura global como lo son: Facebook, Alphabet, Amazon Huawei y otras más[18]. Unas de ellas por interés propio y otras por la invitación del estado Colombiano como lo es el caso de Microsoft[19].

El gobierno de Colombia no ha sido ajeno a esta situación, ya que se ha evidenciado que a través del Ministerio de las Tecnologías de la Información y la Comunicación MINTIC, ha realizado importantes inversiones en materia de conectividad, capacitación, asistencia técnica e incentivo en el aumento de las capacidades de infraestructura TI (Tecnologías de información) principalmente en las áreas de la innovación, formación del talento humano y la apropiación de la tecnología[20].

Por lo tanto, se hace necesario inicialmente comprender que en la medida que se adoptan las TI (Tecnologías de información), en el país en función de ello se incrementan los riesgos y es allí donde se manifiestan las oportunidades acompañadas de sus grandes desafíos en la atención, prevención y tramite de los incidentes informáticos que según los datos reportados en el informe

[18] **HERNÁNDEZ, Miguel. 2015.** ¿Qué tanto aporta la industria TIC a la economía nacional? [En línea] 2015. [Citado el: 10 de 05 de 2020.] https://www.eltiempo.com/archivo/documento/CMS-15618752.

[19] **PRESIDENCIA DE LA REPUBLICA DE COLOMBIA. 2019.** Declaración del Presidente Iván Duque sobre su visita a Microsoft en Seattle. [En línea] 09 de 05 de 2019. https://id.presidencia.gov.co/Paginas/prensa/2019/190509-Declaracion-del-Presidente-Ivan-Duque-sobre-su-visita-a-Microsoft-en-Seattle.aspx

[20] **MIN TIC DE COLOMBIA. 2019.** Proyectos de inversión 2020 FUTIC. [En línea] 31 de 12 de 2019. [Citado el: 28 de 11 de 2020.] https://www.mintic.gov.co/portal/604/articles-1783_Proyectos_inversion_2020.pdf.

"TENDENCIAS DEL CIBERCRIMEN 2019-2020"[21] estos van en incremento y diversificación con el pasar del tiempo.

Lo expresado anteriormente, entrega a CYBERSECURITY DE COLOMBIA LTDA los argumentos necesarios para pensar en el aporte que puede realizar en el mejoramiento de los factores que componen el ecosistema de seguridad informática en Colombia y en el cómo actuar frente a las necesidades existentes de formación y asistencia técnica en el país por medio del diseño del Equipo de Respuesta ante Incidencias de Seguridad Informáticas (CSIRT) de la empresa, por medio del cual se atenderán las necesidades de tratamiento y prevención de incidentes de seguridad informática que se presentan a los usuarios que requieren de los servicios de seguridad de la empresa y adicional mente fortalecer sus procesos de seguridad informática desarrollados en el país y si es el caso en la empresa misma.

4.4 ANTECDENTES O ESTADO ACTUAL

Los CSIRT son organismos utilizados a nivel mundial para el trámite y manejo de incidentes de seguridad informática aunque no en todas partes son conocidos con este término, por ejemplo: en Europa se conocen como CERT el cual es un organismo registrado en los Estados Unidos pero su operación radica de igual forma recibir, revisar, responder, seguir y realizar informes en asuntos relacionados con el combate de actos que afecten la seguridad informática.

Otro punto de gran interés es que los CSIRT pueden pertenecer a organizaciones, entidades, instituciones, gobiernos y demás, este grupo de expertos en materia de seguridad tienen como objetivo atender situaciones de seguridad informática presentados dentro de su comunidad pero a su vez pueden operar en conjunto con otros CSIRT los cuales se pueden ver afectados por incidentes presentados dentro de este[22].

Existen diferentes tipos de CSIRT, entre ellos:

- **Centros de Coordinación:** Encargados de manejar los incidentes por medio del uso de diferentes CSIRT.

[21] **CCIT- POLICIA NACIONAL DE COLOMBIA. 2020.** Informe de las tendencias del cibercrimen en Colombia (2019-2020). [En línea] 20 de 10 de 2020. [Citado el: 28 de 11 de 2020.] https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf.

[22] **GARCÍA, Mónica Alexandra. 2014**. Propuesta de diseño de un área informática forense para un equipo de respuestas ante incidentes de seguridad informáticos, CSIRT. [En línea] 2014. [Citado el: 28 de 11 de 2020.] http://repositorio.espe.edu.ec/bitstream/21000/8063/1/T-ESPE-047639.pdf.

- **Nacionales:** Estos se ocupan del manejo de incidentes informáticos a un país en particular.

- **Internos**: son los encargados del manejo de incidentes en las organizaciones, empresas, entidades, instituciones y demás.

- **Equipos de proveedores:** este tipo de CSIRT se encarga del manejo de reportes de vulnerabilidades e incidentes presentados en los propios productos de hardware y software construidos por la organización misma.

- **Proveedores de respuesta a incidentes:** Estos equipos llevan a cabo el manejo de los incidentes de seguridad a terceros ofreciendo este como un servicio a contratar. [23]

Los modelos para el desarrollo de las funciones del CSIRT son:

- **Modelo Centralizado:** este modelo es recomendado para empresas pequeñas en las que se programe la existencia de un solo CSIRT, el cual se ocupe de la totalidad de los incidentes.

- **Modelo distribuido:** en este modelo se debe contar con varios equipos que atiendan los incidentes según su tipo o ubicación geográfica, pero todos finalmente deben constituir un único CSIRTY que requiere ser coordinado.

- **Combinado:** este modelo resulta de la combinación del modelo centralizado con el modelo distribuido.

- **Coordinador:** se encarga de trabajar en equipo con CSIRT de otras entidades a los cuales les ofrece servicios de asesoría, análisis de incidentes, acciones de prevención entre otras actividades que se pacten mutuamente.

Los servicios de un CSIRT son los que se describen a continuación:

- **Servicios reactivos:** Estos servicios constituyen el elemento central de trabajo de los CSIRT, ya que son activados debido a un incidente o evento de seguridad informática.

[23] **LANFRANCO, Einar.** ¿De qué se trata?, modelos posibles,servicios y herramientas. [En línea] [Citado el: 01 de 05 de 2020.] https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2016/15551-EC/4B%201.pdf

- **Servicios proactivos:** Estos servicios contribuyen a la prevención de incidentes de seguridad por medio de la divulgación de información que ayuda a mejorar los métodos de prevención**.**

- **Servicios de Gestión de Calidad de Seguridad:** Estos se enfocan en el aprovechamiento del conocimiento y experiencia de CSIRT con motivo de mejorar constantemente los servicios que ya existen, son similares a los servicios proactivos por eso representan una menor incidencia en la reducción de próximos ataques.

Seguidamente se encuentra que los CSIRT están clasificados en categorías que están acorde al sector al que pertenece la organización, institución, país y demás; esta clasificación permite al modelo brindar servicios de acuerdo al campo que se requiera con diferentes grados de calidad y lograr establecer equipos en los cuales se exploten de mejor forma las capacidades de sus integrantes[24], las categorías son:[25]

- CSIRT ACADÉMICOS
- CSIRT COMERCIALES
- CSIRT DE INFRAESTRUCTURAS CRÍTICAS
- CSIRT GUBERNAMENTALES
- CSIRT NACIONALES
- CSIRT DEL SECTOR MILITAR
- CSIRT DE PROVEEDORES
- CSIRT DEL SECTOR DE PEQUEÑAS Y MEDIANAS EMPRESAS (PYME)

Con todos los elementos anteriormente expresados se evidencia con claridad que los CSIRT son organismos de operación de incidentes de seguridad informática que intervienen fuertemente no solo en la prevención, sino que también robustecen las líneas de seguridad por medio de las difusión de información y el aprovechamiento de las capacidades de los equipos; también permite la participación de todo tipo de organizaciones desde las más pequeñas hasta las de mayor complejidad es por medio del uso de los sistemas de organización propuestos.

[24] **MUÑOZ, Mirna y RIVAS, Lizbeth. 2015.** Estado actual de equipos de respuesta a incidentes de seguridad informática. [En línea] 03 de 2015. http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1646-98952015000100002

[25] **ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA). 2016.** Buenas prácticas para establecer un CSIRT nacional. [En línea] 04 de 2016. [Citado el: 6 de 1 de 2020.] https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf.

Para el desarrollo del proyecto se tomaron como referencia trabajos y documentos afines al diseño, puesta en funcionamiento y operación CSIRT y las diversas aplicaciones que estos tienen al momento de la atención de incidentes de seguridad informática.

Documento "Memoria anual CSIRT financiero ASOBANCARIA 2019", documento elaborado y publicado por el Programa de ciberseguridad del sector - CSIRT Financiero - de ASOBANCARIA[26]. Este documento presenta una clara visión de las actividades desarrolladas por CSIRT financiero de ASOBANCARIA así algunos apartes sobre su operación y presenta valiosa información frente a la amenazas informáticas existentes actualmente y las tendencias que se esperan para el próximo año, sirviendo este como referente para el desarrollo de las actividades del proyecto.

Documento "Buenas prácticas para establecer un CSIRT nacional", documento elaborado y publicado por la OEA (Organización de los Estados Americanos)[27]. El documento presenta un análisis principalmente el proceso de gestión de un proyecto para la creación y la puesta en marcha de un CSIRT nacional. Este documento ofrece una visión clara frente a las diferentes acciones y criterios a tener en cuenta para la el diseño y puesta en operación de un CSIRT; razón por la cual se hace muy afín con el propósito trazado en el proyecto.

Proyecto "Estrategia y diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la Universidad de las Fuerzas Armadas ESPE"[28], La tesis plantea la propuesta para la creación de un CSIRT de tipo académico en la universidad de las Fuerzas Armadas ESPE de Ecuador; motivo por el cual el documento plantea temáticas afines y aplicables al contexto del proyecto.

[26] **ASOBANCARIA. 2019.** ASOBANCARIA. [En línea] 2019. https://www.asobancaria.com/wp-content/uploads/2020/06/CRT-MA_2020_compressed.pdf.

[27] **ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA). 2016.** Buenas prácticas para establecer un CSIRT nacional. [En línea] 04 de 2016. [Citado el: 6 de 1 de 2020.] https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf.

[28] **DE LA TORRE MOSCOSO, Hugo Marcelo y PARRA ROSERO, Mario Andrés. 2018.** Estrategia y diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la Universidad de las Fuerzas Armadas ESPE. [En línea] 2018. [Citado el: 28 de 11 de 2020.] http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/15071/T-ESPE-040447.pdf?sequence=1&isAllowed=y

4.6 MARCO LEGAL

4.6.1 Constitución Política de Colombia. El artículo número 15 de la Constitución política de Colombia establece que las personas tiene el derecho a su intimidad tanto personal como familiar y además al manteniendo de su buen nombre; además obliga al estado a respetar y hacer respetar este derecho, lo cual convierte a la seguridad informática en un componente supremamente valioso teniendo en cuenta que la sociedad actual se rige por el uso de los sistemas informáticos por los cuales circula la mayor cantidad de los datos de las personas y a los cuales se les debe garantizar la integridad, disponibilidad y principalmente la privacidad que exige la carta magna[29].

4.6.2 Ley 87 de 1993. Esta ley establece la normativa para el ejercicio del control interno en Colombia tanto para las entidades como para los organismos del estado Colombiano; esta normativa es uno de los factores valiosos dentro del funcionamiento propio de un CSIRT, ya que allí se disponen diferentes herramientas jurídicas que dan lugar a la toma de decisiones, como a la implementación de estrategias ante la atención y prevención de incidentes informáticos principalmente en los organismos del estado pero también en los demás que sea aplicable[30].

4.6.3 Ley 599 del 2000. El código penal Colombiano establece un bien jurídico tutelado denominado "De la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones lo que se representa en el establecimiento de una herramienta jurídica importante para el tratamiento y gestión y penalización de los autores de los incidentes informáticos acción que es valiosa para en el que hacer de un CSIRT principalmente en los aspectos de asesoramiento y tramite[31].

4.6.4 Ley 1273 de 2009. Esta es una de la herramientas jurídicas más valiosas dispuestas por el estado Colombiano para el manejo, tramite y judicialización de aquellos individuos que cometan agresiones tecnológicas; ya que esta ley modifica el Código Penal creando un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones[32] entre otras disposiciones, siendo esta

---

[29] **COLOMBIA. ASAMBLEA NACIONAL CONSTITUYENTE. 1991.** Constitución Política de la República de Colombia. [En línea] 20 de 07 de 1991. [Citado el: 29 de 11 de 2020.] http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

[30] **COLOMBIA. EL CONGRESO DE COLOMBIA. 1993.** Ley 87 de 1993. [En línea] 29 de 11 de 1993. [Citado el: 29 de 11 de 2020.] http://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=300

[31] **COLOMBIA. EL CONGRESO DE COLOMBIA. 2000.** Ley 599 De 2000. [En línea] 24 de 7 de 2000. [Citado el: 28 de 11 de 2020.] https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

[32] **COLOMBIA. CONGRESO DE COLOMBIA. 2009.** Ley 1273 de 2009. [En línea] 05 de 01 de 2009. [Citado el: 29 de 11 de 2020.] https://mintic.gov.co/portal/604/articles-3705_documento.pdf.

la razón por la cual la ley 1273 de 2009 da una base jurídica solida al CSIRT para el desarrollo de sus actividades en el país.

4.6.5 Ley estatutaria 1581 de 2012. Ley que plantea el desarrollo del derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma[33], la cual aplica como soporte jurídico base en el marco del desarrollo de las actividades del CSIRT.

[33] **COLOMBIA. CONGRESO DE LA REPÚBLICA. 2012.** Ley estatutaria 1581 de 2012. [En línea] 18 de 10 de 2012. [Citado el: 29 de 11 de 2020.] http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

5 DISEÑO METODOLÓGICO

El desarrollo del proyecto se lleva a cabo usando la Metodología Aplicada, debido a que esta se caracteriza principalmente por la aplicación de conocimientos adquiridos previamente y la obtención de otros complementarios durante el desarrollo del proceso.

Es este sentido este método aplicado es bastante apropiado para el desarrollo del proyecto teniendo en cuenta que este es aplicable para para la resolución o intervención en problemas en los que se hace participe la innovación en diferentes aspectos como la industria, el arte y la técnica.[34]

En concordancia con lo dicho el presente proyecto surge de la elección del escenario propuesto por la universidad "Enfoque técnico – Estrategico Cybersecurity de Colombia LTDA", el cual plantea la resolución de un problema estructurado bajo el enfoque técnico y que otorga las características y acotaciones necesarios para responder a las preguntas y problemas que se enmarcan en la ejecución del caso de estudio.

Sumado a lo anterior y de acuerdo a las características expuestas en el escenario, al tratarse de un enfoque técnico el enfoque metodológico aplicado se alinea de mejor forma con el propósito del proyecto y el campo de aplicación.

Por otro lado el desarrollo del proyecto se estructura en fases que se adecúan a la metodología seleccionada; tomando como punto de partida cada uno de los objetivos específicos los cuales se separaran en sub-faces que luego de realizadas permitirán dar cumplimiento del objetivo general.

Posteriormente, se toman los objetivos específicos y se describe cada una de las actividades a desarrollar para el cumplimiento de cada uno.

Fase 1: La recopilación de información referente a herramientas software que den lugar al desarrollo de los servicios reactivos y proactivos del CSIRT.

Actividad 1. Recolección de información: En esta actividad se realizará la recopilación de información y consulta de literatura disponible que permita identificar

[34] **VARGAS CORDERO, Zoila Rosa.** *La investigación aplicada: Una forma de conocer las realidades con evidencia científica.* **2009.** 1, San Pedro, Costa Rica : s.n., 2009, Vol. 33. 0379-7082

las herramientas software libre disponibles en el mercado para poder desarrollar los procesos de CSIRT.

Actividad 2. Análisis de la información: En esta actividad se realizará el análisis detallado de la información que permita definir de forma objetiva las mejores y más adecuadas herramientas que permitirán el desarrollo óptimo de las actividades de CSIRT.

Actividad 3. Consolidación de la información: Consolidar en un documento las herramientas seleccionadas plasmando en él las características, ventajas, desventajas y como cada uno de ellos puede favorecer la ejecución de las actividades propias del CSIRT de acuerdo al análisis realizado.

Fase 2: Definición del mapa de la estructura TI del CSIRT teniendo como base las mínimas dependencias para su correcto funcionamiento.

Actividad 4. Recolección de información: En ésta actividad se llevará a cabo la recolección de la información necesaria para la construcción del mapa de la estructura TI del CSIRT.

Actividad 5. Construcción del mapa: En esta actividad se construirá el mapa de la estructura TI del CSIRT teniendo en cuenta los elementos obtenidos en la recolección de información.

Fase 3: Consolidación de la información necesaria acerca de las herramientas Software necesarios para que el CSIRT pueda ejecutar sus actividades correctamente.

Actividad 6. Recolección de información: En esta actividad se realizará la recopilación de información y consulta de literatura disponible que dé lugar a la obtención de los datos necesarios de Software que requiere el CSIRT para su óptimo funcionamiento.

Actividad 7. Clasificación de la información: En esta actividad se realizará la clasificación de la información obtenida que permita seleccionar las mejores herramientas software a usar en el CSIRT.

Actividad 8. Consolidación del informe: En esta actividad se consolidará el informe, el cual debe contener toda la información referente a las herramientas software seleccionados así como los detalles de los mismos.

Fase 4: Desarrollo del diseño de un laboratorio controlado por medio del uso de máquinas virtuales que permita la ejecución de pruebas del software que se utilizara en el CSIRT.

Actividad 9. Recolección de información: En esta actividad se realizará la recolección de la información de las diferentes herramientas software a utilizar en el CSIRT lo cual se será el insumo primario para el diseño del laboratorio

Actividad 10. Diseño del laboratorio: En esta actividad se llevará a cabo el diseño del laboratorio el cual se soportará en el planteamiento de un escenario problema en el que se dará uso a algunas de las herramientas, se propondrán e implementaran acciones de mejora sobre las capacidades técnicas instaladas en la empresa fortaleciendo de esta manera los procesos y procedimientos propios del CSIRT

Actividad 11. Implementación y prueba del laboratorio: En esta actividad se llevará a cabo la implementación y el desarrollo de las pruebas del laboratorio que darán lugar a la verificación de su funcionamiento de acuerdo al objetivo del mismo.

6 DESARROLLO DE LOS OBJETIVOS

A continuación se presenta la ejecución de las fases y actividades que permitieron el desarrollo del proyecto y dieron vía para alcanzar el objetivo general del mismo.

6.1 FASE 1: RECOPILACION INFORMACIÓN RELACIONADA CON HERRAMIENTAS DE SOFTWARE QUE PERMITAN DESARROLLAR LAS ACTIVIDADES DEL CSIRT, TENIENDO PRESENTE QUE SUS SERVICIOS SON REACTIVOS Y PROACTIVOS.

Para el desarrollo de las actividades del CSIRT se han encontrado diferentes tipos de herramientas destinadas a la detección de vulnerabilidades de los sistemas, la realización de ataques que permitan evaluar la seguridad, sistemas operativos destinados a la seguridad, herramientas para actividades forenses y de elaboración de informes.

Estas herramientas son de los más diversos y variados tipos en función del procedimiento que quieran realizar, incluso se encuentran herramientas que tienen la capacidad de hacer varias funciones en una sola, en el mercado es posible encontrar herramientas propietarias y herramientas libres; pero en atención a los establecido en el presente se toman las herramientas que tienen mayor aceptación en la comunidad y aquellas que tienen mejor documentación y soporte

A continuación se presenta la información de las diferentes herramientas que se seleccionaron en función que facilitar los servicios reactivos y proactivos del CSIRT de la empresa “Cybersecurity de Colombia LTDA”, entre ellas se encuentran:

NESSUS: Es una herramienta basada en la consola de comandos Linux, la cual realiza escaneos de vulnerabilidades en la Web y es catalogado por muchos como uno de los más utilizados a nivel mundial en la industria cuenta con amplio grupo de expertos investigadores en vulnerabilidades que dan respaldo y una gigantesca base de datos, que le permite adaptarse con facilidad tanto a pequeñas como grandes organizaciones; además, sus reportes son bastante detallados y los tiempos de respuesta ajustados a las necesidad de los usuarios[35].

OPENVAS: Es una herramienta para realizar escaneo de vulnerabilidades de código abierto con licencia (GNU/GPL), el cual abarca una gran cantidad de funcionalidades que le permiten realizar pruebas con y sin autenticación, usar

[35] **OBBAYI, Lester. 2019.** A Brief Introduction to the Nessus Vulnerability Scanner. [En línea] 26 de 07 de 2019. [Citado el: 28 de 11 de 2020.] https://resources.infosecinstitute.com/topic/a-brief-introduction-to-the-nessus-vulnerability-scanner/

diferentes protocolos, escaneos en diferentes niveles y además cuenta con un lenguaje de programación propio que le permite al usuario implementar pruebas de vulnerabilidad no contempladas por la herramienta y se caracteriza por el uso de fuentes de información externas que permiten ampliar su rango de análisis[36].

VEGA: Es una herramienta Open Source,[37] la cual provee una interfaz gráfica amigable al usuario y con la que se pueden elaborar escaneos automáticos a las aplicaciones de forma sencilla pero con resultados de auditoria de alta calidad y con la que se acceden a un análisis profundo de vulnerabilidades[38].

SURICATA: Es una herramienta que permite la detección de las diversas amenazas que pueden existir dentro de las redes de comunicaciones, este es un motor detección es muy veloz, completo y de larga trayectoria, con el cual es posible realizar acciones de prevención de intrusos en línea IPS, detección de intrusos (IDS) en tiempo real, hacer monitoreo de red y cuenta con la capacidad para realizar procesamiento fuera de línea.

Este motor de detección de amenazas revisa la red por medio del uso de lenguaje de firma y potentes reglas con lo que se logra el descubrimiento de amenazas poderosas.

Su desarrollo permanente enfocado en la seguridad, el uso, la eficiencia y la integración permiten a Suricata la integración con otras herramientas; ya que usa formatos de amplia aceptación como lo son: JSON y YAML para sus entradas y salidas[39].

Kali Linux: Sistema operativo Kali Linux es una herramienta que se construye en base a la distribución de Linux Debian, la cual tiene como propósito principal proporcionar al usuario un conjunto enorme de utilidades en un ambiente controlado, amigable y de fácil utilización para la realización de actividades más sencillas hasta las más avanzadas en materia de seguridad informática tales como: auditorias de seguridad, pentesting, informática forense, ingeniería inversa o investigación en asuntos relacionados con la seguridad informática.

---

[36] **OPENVAS. 2020.** Open Vulnerability Assessment Scanner. [En línea] 2020. [Citado el: 28 de 11 de 2020.] http://www.openvas.org

[37] **FERREIRO CANOSA, Alejandro. 2017.** Escaneo de vulnerabilidades con Vega. [En línea] 03 de 01 de 2017. https://backtrackacademy.com/articulo/escaneo-de-vulnerabilidades-con-vega-parte-1

[38] **PAUS, Lucas. 2015.** Cómo auditar la seguridad de tu sitio web con Vega. [En línea] 03 de 03 de 2015. [Citado el: 28 de 11 de 2020.] https://www.welivesecurity.com/la-es/2015/03/03/como-auditar-la-seguridad-sitio-web-vega

[39] **SURICATA-IDS. 2020.** Suricata Open Source IDS / IPS / NSM engine. [En línea] 2020. [Citado el: 30 de 11 de 2020.] https://suricata-ids.org

Dentro de las principales características con las que cuenta el sistema operativo Kali Linux se tiene que es un sistema operativo de uso libre; pero que a su vez por razones de seguridad algunos elementos del código están restringidos, utiliza el árbol de Git para código abierto, parchado constante del Kernel para procesos de inyección, soporte grande para dispositivos inalámbricos, sus paquetes (más de 600) son revisados previamente a la publicación y firmados con GPG, cuenta con un entorno de desarrollo altamente seguro, tiene soporte multilenguaje, es multiplataforma y cuenta con una comunidad de soporte enorme a nivel mundial[40].

Metaesploitable3: Es una máquina virtual adaptada para ser vulnerable que se implanta y estructura según las necesidades del usuario, tiene como base el sistema operativo Microsoft Windows Server 2008 R2; en versiones anteriores Metaesploitable se basaba en versiones GNU/Linux, pero debido a las fuertes políticas de aseguramiento de estos sistemas se tornaba muy complejo tener éxito en la realización de pruebas y simulaciones lo que hacía difícil de cumplir el propósito principal siendo esta una de las razones por las que los desarrolladores de Metaespliotable3 consideraron el desarrollo de un ambiente controlado basado en Windows Server 2008 R2 para el planteamiento, hallazgo y explotación de vulnerabilidades y que estos se acerquen lo más posible a la realidad[41].

Nikto: Es una herramienta destinada para el escaneo de vulnerabilidades en los servidores Web, cuenta con la capacidad de revisar múltiples componentes entre los cuales se encuentran programas que pueden representar peligro, versiones obsoletas de los servidores, configuraciones inapropiadas entre otras características[42].

Nmap: La herramienta NMAP permite llevar a cabo procesos de auditorías de seguridad, cuenta con la capacidad de revelar redes, facilita la realización de inventarios de red y la supervisión de la actividad de las redes[43].

Commix: Es una herramienta que permite la realización automatizada de pruebas y explotación de errores, vulnerabilidades y fallas relacionadas con la inyección de comandos en el entorno de las aplicaciones Web[44].

---

[40] **KALI - OFFENSIVE SECURITY . 2019.** What is Kali Linux? [En línea] 26 de 10 de 2019. [Citado el: 19 de 02 de 2020.] https://www.kali.org/docs/introduction/what-is-kali-linux/

[41] **DRAGON JAR. 2018.** Metasploitable 3, Instalación en GNU/Linux, Windows y Mac OS. [En línea] 2018. [Citado el: 28 de 11 de 2020.] https://www.dragonjar.org/metasploitable-3-instalacion-en-gnulinux-windows-y-mac-os.xhtml

[42] **SULLO, Chris; LODGE, David. 2020.** Nikto2. [En línea] 2020. [Citado el: 21 de 02 de 2020.] https://cirt.net/Nikto2

[43] **NMAP. 2017.** Nmap ("Network Mapper"). [En línea] 2017. [Citado el: 21 de 02 de 2020.] https://nmap.org/

[44] **KALI TOOLS. 2020.** Commix package description. [En línea] 2020. [Citado el: 21 de 02 de 2020.] https://tools.kali.org/exploitation-tools/commix

Sqlmap: Esta herramienta permite tomar el control de los servidores de bases de datos, automatizar la realización de pruebas de penetración y explotación de fallas con el método de inyección de SQL[45].

Sqlmap cuenta con soporte para un amplio rango de sistemas de bases de datos entre los que se destacan Oracle, PostgreSQL, MySQL, Firebird, MariaDB, Apache ignite entre otros.

Hydra: Es una herramienta elaborada con el fin de romper contraseñas de inicio de sesión en paralelo y con la cual es posible llevar a cabo ataques a diferentes protocolos como por ejemplo: FTP, HTTP, HTTPS, Oracle, Postgresql, Mysql, SMB, SHH, entre otros muchos[46].

Cewl: Con esta herramienta es posible realizar seguimientos a las URL hasta una profundidad específica con el fin de lograr capturar paquetes de palabras que pueden ser usados para posteriormente descifrar contraseñas[47].

Ncrack: Herramienta para llevar a cabo actividades de descifrado de claves de red muy rápidamente, contribuye en el mejoramiento de la protección de las redes empresariales en lo referente a contraseñas débiles teniendo en cuenta que permite realizar evaluaciones frente a la fortaleza de las contraseñas y la posibles vulnerabilidades que estas mismas puedan tener[48].

Es muy útil para procesos de auditorías internas y externas, ataques de fuerza bruta y cuenta con soporte para muchos protocolos como por ejemplo: SSH, FTP, HTTP, POP3, MongoDB, entre otros.

Aircrack-ng: Esta herramienta contiene un grupo amplio de herramientas que permiten la evaluación de las redes WiFi cuenta con cuatro enfoques principales que son: el monitoreo, el ataque, las pruebas y el agrietamiento; todo ésto se usa a través de comandos, lo cual le permite mayor flexibilidad y grosor en la ejecución[49].

---

[45] **DAMELE, Bernardo y STAMPAR, Miroslav. 2020.** SQLMAP introduction. [En línea] 2020. [Citado el: 22 de 02 de 2020.] http://sqlmap.org

[46] **KALI-TOOLS. 2020.** Hydra package description. [En línea] 2020. [Citado el: 22 de 02 de 2020.] https://tools.kali.org/password-attacks/hydra

[47] **KALI LINUX. 2020.** CeWL package description. [En línea] 2020. [Citado el: 22 de 02 de 2020.] https://tools.kali.org/password-attacks/cewl

[48] **NMAP ORG. 2020.** Ncrack is a high-speed network authentication cracking tool. [En línea] 2020. [Citado el: 22 de 02 de 2020.] https://nmap.org/ncrack

[49] **AIRCRACK NG. 2020.** Aircrack-ng is a complete suite of tools to assess WiFi network security. [En línea] 2020. [Citado el: 23 de 02 de 2020.] https://www.aircrack-ng.org

Wifite: Herramienta parametrizable que permite auditar y atacar las redes WiFi que se encuentran encriptadas en los protocolos Web, Wpa y Wps; su uso se da por medio de la línea de comandos y permite realizar procesos de una forma sencilla y en poco tiempo[50].

Reaver: Con esta herramienta es posible la realización de ataques de fuerza bruta contra los PIN de las redes WiFi WPS; siendo este el método mediante el cual se logra extraer las frases de las claves de WPA o WPA2 en texto plano terea en la que la herramienta usa entre 4 y 10 horas aproximadamente dependiendo del equipo objetivo[51].

Clang: Es un proyecto que facilita una infraestructura robusta de herramientas y front end de lenguaje para la familia de C la cual es compuesta por C, C ++, Objective C / C ++, OpenCL, CUDA y RenderScript para un proyecto denominado LLVM[52].

El objetivo principal de la herramienta es proporcionar al usuario un compilador que realice un mejor diagnóstico, integración con IDE´s y con licencia de compatibilidad universal esto a través de un compilador ágil y de fácil desarrollo y mantenimiento.

Radare2: Es un framework de ingeniería inversa multiplataforma, el cual incluye con muchas capacidades que permiten al usuario extraer una gran cantidad de información de una amplia variedad de ejecutables entre las cuales se encuentran: .exe, .java, filesystem, entre otros más. Adicionalmente la herramienta da lugar a realizar análisis dinámicos y estáticos de los datos obtenidos[53].

Metasploit framework: Esta es una herramienta que proporciona un conjunto de herramientas para la realización de pentesting, es usado ampliamente a nivel mundial, permite la identificación, explotación y validación de vulnerabilidades, la administración de las evaluaciones de seguridad y el incremento de conocimiento en asuntos de seguridad informática.

Las principales características que incorpora el framework son la ingeniería social, validación de vulnerabilidades, evasión de antivirus, escape de IPS / IDS,

---

[50] **KALI LINUX NET. 2020.** Kali Linux en español. *Automated wireless auditor.* [En línea] 2020. [Citado el: 23 de 02 de 2020.] https://kali-linux.net/article/wifite

[51] **TOOLS.KALI.ORG. 2020.** Reaver Package Description. [En línea] 2020. [Citado el: 23 de 02 de 2020.] https://tools.kali.org/wireless-attacks/reaver

[52] **CLANG.LLVM.ORG. 2020.** Getting Started: Building and Running Clang. [En línea] 2020. [Citado el: 23 de 02 de 2020.] https://clang.llvm.org/get_started.html

[53] **PEREZ, Diego. 2016.** Radare2: abriendo las puertas al reversing. [En línea] 17 de 08 de 2016. [Citado el: 23 de 02 de 2020.] https://www.welivesecurity.com/la-es/2016/08/17/radare2-reversing

reutilización de credenciales, generación de informes, pruebas de sistemas Web, apoyo para phishing, entre otro amplio grupo de capacidades[54].

Searchsploit: Es una aplicación de búsqueda de vulnerabilidades que funciona a través de la línea de comandos de Linux, con la cual se pueden realizar búsquedas tanto en redes con o sin acceso a internet por medio de la combinación con herramientas de almacenamiento de bases de datos de explotación[55].

Autopsy: Esta herramienta permite la extracción y detección de datos importantes para investigaciones y auditorias informáticas desde los principales componentes de gestión de datos como lo son los discos duros, captación de trafico de red, memorias USB o derivados, hasta información volcada en la memoria RAM dando lugar así a la captación de la información necesaria para la elaboración de análisis forense[56].

Finalmente se puede concluir que el ecosistema de herramientas tecnológicas que facilitan los procesos de aseguramiento, estudio y apropiación de componentes de la seguridad informática al interior de las organizaciones es muy amplio, variado y adaptable, ya que se encuentran herramientas tanto de uso libre como privativo que en muchas ocasiones se complementan y que además están en permanente evolución y adecuación a las demandas del mercado lo que por una parte facilita las actividades de aseguramiento pero que a su vez entrega a los actores maliciosos presentes todo el tiempo en el entorno las mismas capacidades; situación que de cierta forma dificulta la labor de protección, ya que los encargados de proteger tienen la responsabilidad sobre los activos mientras que los atacantes desarrollan sus acciones desde el anonimato y generalmente sin ningún tipo de responsabilidad y de ahí la importancia de dar el uso correcto a cada una de estas como es el caso del CSIRT de Cybersecurity de Colombia.

6.2 FASE 2: DEFINICIÓN DEL MAPA DE LA ESTRUCTURA TI DEL CSIRT TENIENDO COMO BASE LAS MÍNIMAS DEPENDENCIAS PARA SU CORRECTO FUNCIONAMIENTO

Para el correcto desarrollo de las actividades que se llevarán a cabo en el CSIRT de la empresa “Cybersecurity de Colombia LTDA”, se plantea el establecimiento de las dependencias que se describen a continuación las cuales en algunos casos se

[54] **RAPID7-METASPLOIT. 2020.** Getting Started Metasploit . [En línea] 2020. [Citado el: 23 de 02 de 2020.] https://metasploit.help.rapid7.com/docs/getting-started
[55] **EXPLOIT DATABASE. 2020.** SearchSploit - The Manual. [En línea] 2020. [Citado el: 23 de 02 de 2020.] https://www.exploit-db.com/searchsploit
[56] **POROLLI, Matías. 2013.** Cómo realizar un análisis forense con Autopsy. [En línea] 23 de 09 de 2013. [Citado el: 23 de 02 de 2020.] https://www.welivesecurity.com/la-es/2013/09/23/como-realizar-analisis-forense-autopsy

subdividen para poder darles el grado de independencia que necesitan según la función que cumplan:

1. DIRECCIÓN GENERAL

Se encarga del desarrollo de las actividades de gestión y coordinación de los diferentes servicios ofrecidos por el CSIRT.

2. COORDINACIÓN ADMINISTRATIVA

Dirige las áreas operativas del CSIRT, tales como: las finanzas, las comunicaciones, los aspectos legales y demás funciones necesarias para la operación.

2.1 CONTABILIDAD

Se encarga de la administración y el control de las finanzas del CSIRT.

2.2 COMUNICACIONES

Es el encargado de la generación de la información que se entrega desde el CSIRT, así como de recibir esta misma y entregarla de forma clara, oportuna y responsable al destinatario correspondiente.

2.3 JURÍDICA

Dirige el CSIRT en los aspectos legales de forma que no se lleven a cabo actividades que incumplan los aspectos legales y las normativas vigentes.

3. COORDINACIÓN TÉCNICA

Responsables del desarrollo de la prestación de los servicios ofrecidos por del CSIRT

3.1 EQUIPO TÉCNICO

Responsable de que todas las operaciones técnicas se lleven a cabo basándose en las políticas, normativas, protocolos y demás aspectos que sean necesarios para el desarrollo de actividades con un alto nivel de calidad.

3.2 EQUIPO FORENSE

Equipo que se encarga de la obtención de los datos necesarios desde las diferentes fuentes de información y la organización de reportes que serán el insumo base para los procesos de análisis, tratamiento y prevención de los incidentes de seguridad que se presenten.

3.3 SOPORTE TI

Equipo de expertos en servicio al cliente con énfasis en seguridad informática que bajo el uso de estándares de calidad, constituye la primera línea de atención a las organizaciones que se les proporcionan los servicios ofrecidos por el CSIRT "Cybersecurity de Colombia LTDA", dado que la atención de incidentes de seguridad o asesoramiento técnico son uno de los ejes fundamentales para garantizar la continuidad, la prevención y el trámite de los incidentes de seguridad que se presenten al interior de las mismas.

3.4 CONSULTORES EXTERNOS

Expertos en áreas específicas de la seguridad informática o campo profesional que se requieran para la atención de situaciones específicas que puedan surgir en los procesos de atención, tratamiento y prevención de los incidentes de seguridad informática.

4 COORDINACIÓN I+D+I

Equipo encargado de llevar a cabo los procesos investigativos necesarios para el conocimiento de nuevas vulnerabilidades, riesgos, agresiones, técnicas, modelos e incidentes propios de la seguridad informática; así como la divulgación y capacitación a los diferentes equipos técnicos de los resultados de los procesos de investigación para su posterior aplicación.

5 COORDINACIÓN DE INFRAESTRUCTURA TI

5.1 CENTRO DE DATOS

Es una o varias instalaciones que se establecen con el objetivo de realizar acciones de almacenamiento y procesamiento de datos, el centro de datos es uno de los componentes más valiosos del CSIRT, ya que allí se concentran todos los datos de los diferentes procesos y además albergara los procesos de investigación y formación que se realizan al interior de CSIRT como es el caso de los laboratorios, las simulaciones y demás actividades que se requieran para el cumplimiento de las funciones.

5.2 CENTRO DE OPERACIONES

El centro de operaciones o comúnmente conocido como (SOC), es una instalación física e informática en la que se desarrollan actividades de control y monitoreo tanto de sistemas, como de redes y recursos TI.

Es esta instalación se concentran las acciones críticas que se desarrollan en el CSIRT “Cybersecurity de Colombia LTDA” en donde principalmente se destacan el diagnóstico, la recuperación de desastres (RTO y RPO), la gestión de incidentes, contrarrestar ataques, alertas tempranas y el establecimiento de planes y programas de prevención de incidentes de seguridad informática.

El centro de operación tiene un fuerte vínculo con el centro de datos teniendo en cuenta que éste requiere de la mayoría de los elementos dispuestos allí como lo son los sistemas de detección de intrusos (IDS), los sistemas firewall, la documentación técnica o forense, los sistemas de pruebas, los servicios de procesamiento de datos, entre otros.

Con lo anteriormente descrito es importante aclarar que ésta instalación debido a los procesos que se desarrollan en su interior y a su funcionamiento en tiempo real obligatoriamente requiere de una operación 7/24 durante todos los días del año y debe contar con la participación de expertos calificados en materia de seguridad informática.

5.3 SALÓN DE CRISIS

Instalación adecuada para la coordinación de acciones orientadas en la atención de emergencias de seguridad informática, la cual debe contar con todas las herramientas y métodos necesarios para dar respuesta rápida y oportuna a todas las situaciones que necesiten de especial atención.

5.4 SALÓN DE FORMACIÓN

Espacio que se establece con la intención de llevar a cabo las actividades de formación que sean requeridas tanto para el ingreso de nuevo personal como para los procesos de I+D+I; esta instalación debe contar con los elementos y herramientas para impartir conocimiento de tipo teórico, técnico y procedimental, como para el desarrollo de prácticas de laboratorio en ambientes controlados.

6 ÁREA LOGÍSTICA

Esta área se encarga de los procesos de administración de los métodos y medios necesarios para la organización del CSIRT; es allí donde se gestionan las necesidades de tecnología y otros implementos que se requieran para el desarrollo correcto de las actividades; además se encarga de la evaluación de la viabilidad de la adquisición de equipos y de los servicios de distribución de componentes de seguridad informática que se requieran con los usuarios.

Con base en las dependencias descritas anteriormente se presenta el diseño del mapa de la estructura tecnológica del CSIRT de la empresa “Cybersecurity de Colombia LTDA” representado gráficamente en la Figura 1, orientado al cumplimiento de los objetivos y metas de consolidarse para el año 2021 como un CSIRT altamente reconocido en Colombia.

Figura 1 Diseño del mapa de la estructura tecnológica del CSIRT de la empresa “Cybersecurity de Colombia LTDA”

Fuente: Propia del autor

6.3 FASE 3: CONSOLIDACIÓN DE LA INFORMACIÓN NECESARIA ACERCA DE LAS HERRAMIENTAS SOFTWARE NECESARIAS PARA QUE EL CSIRT PUEDA EJECUTAR SUS ACTIVIDADES CORRECTAMENTE.

Se realiza la revisión de viabilidad de las herramientas identificadas en el sector de la seguridad informática frente a las necesidades y enfoque del proyecto lo cual permitirá contar con las aplicaciones necesarias para la operación del CSIRT en la empresa “Cybersecurity de Colombia ltda”.

Atendiendo a esto se propone implementar servicios sobre los cuales establecer métodos, herramientas e infraestructura de tecnología con el objetivo de orientar la operación del CSIRT por la ruta de la prevención de incidentes de ciberseguridad; pero sin dejar a un lado la identificación, el tratamiento, el estudio la solución de las agresiones tecnológicas que se pueden presentar a los usuarios de los servicios ofrecidos por el CSIRT.

Con base en lo anterior se clasifican las herramientas tecnológicas en cuatro categorías diferentes tomando como referentes el licenciamiento, el uso en las comunidades a nivel mundial, referentes estadísticos y aplicación a las necesidades del CSIRT tal como se muestra a continuación:

6.3.1 Infraestructura de tecnología. La infraestructura tecnológica corresponde al componente base de las actividades de sistematización ya que sobre ella reposa toda la operación, el procesamiento y la gestión de los sistemas informáticos siendo este el motivo por el que este valioso activo se debe mantener en constante monitoreo, control y mejora con el objetivo de identificar vulnerabilidades, darle tratamiento a los riesgos o solucionar eventualidades presentadas.[57]

Con esto en mente se presentan las herramientas seleccionadas de acuerdo a grupo al que estas pertenecen.

- **Virtualización**: Se plantea el uso de Virtualbox que es una herramienta potente para la virtualización de sistema operativo con capacidad de uso tanto en el grado doméstico como empresarial, además VirtualBox es una herramienta software con licencia GNU/GPLv2.

  Además tomando como soporte el artículo "**Performance Evaluation of VMware and VirtualBox**"[58], en el cual se hacen diferentes evaluaciones de rendimiento entre VirtualBox y Vmware siendo estas de las más usadas en el mercado; se logra identificar que de diferentes formas en algunos casos una cuenta con mejores resultados que la otra y viceversa.

  Dado a lo anterior y de acuerdo a la necesidad de reducir los costos de operación del proyecto se plantea la decisión de usar VirtualBox, como sistema de virtualización a usar para actividades técnicas del CSIRT en la empresa "Cybersecurity de Colombia ltda".

- **Diagramación de topología de red**: Con motivo de lograr plasmar gráficamente la estructura de red se define el uso de la herramienta draw.io;

[57] **REDHAT. 2020.** ¿Qué es la infraestructura de TI? [En línea] 2020. [Citado el: 13 de 12 de 2020.] https://www.redhat.com/es/topics/cloud-computing/what-is-it-infrastructure.

[58] **DEEPAK, Damodaran, y otros. 2012.** Performance Evaluation of VMware and VirtualBox. [En línea] 2012. http://www.ipcsit.com/vol29/006-ICSST2012-S015.pdf.

la cual cuenta con las capacidades para la elaboración de diagramas sencillos y complejos no solo de red sino de una amplia gama de opciones como: la exportación en diferentes formatos almacenamiento en la nube, compatibilidad con servicios externos como Dropbox, Google Drive, GitHub, GitLab, entre otras capacidades adicionales.

Otra característica importante de draw.io es que esta ópera de forma online, es de uso abierto y no requiere de instalación de software adicionales en los clientes.

- **Seguridad**: Para el aseguramiento de los servicios de red se define el uso de la herramienta IPTABLES, la cual ofrece una importante cantidad de capacidades seguras, confiables, maduras y ampliamente utilizadas a nivel mundial; para aseguramiento y control de servicios de red.

  Esta herramienta siendo de bajo nivel requiere un esfuerzo mayor en términos de administración, pero garantiza mayor nivel de control, flexibilidad en la configuración y reducción de vulnerabilidades por configuraciones por defecto, ya que estas se elaboran de acuerdo a la medida del sistema a implementar.

  Adicional las mediciones de las capacidades de IPTABLES logran demostrar su alto rendimiento frente a diversas amenazas comúnmente conocidas como es el caso de la los ataques DDos según se expone en el artículo "**Performance Evaluations of IPTables Firewall Solutions under DDoS attacks**"[59]

- **Monitoreo**: Para la supervisión de los servicios de red se define la herramienta Suricata la cual contribuye a el CSIRT la capacidad de lograr implementar la detección de las diversas amenazas que pueden existir dentro de las redes de comunicaciones, **Suricata** es un motor detección es muy veloz, completo y de larga trayectoria con el cual es posible realizar acciones de prevención de intrusos necesarios dentro de las operaciones a realiza por el CSIRT de Ciber Secutity de Colombia ltda.

[59] **HURAJAND ČERŇANSKÝ, Šimon. 2015.** Performance Evaluations of IPTables Firewall Solutions under DDoS attacks. [En línea] 2015. https://content.sciendo.com/downloadpdf/journals/jamsi/11/2/article-p35.pdf

Lo anterior tomando como punto de referencia artículo "**Selección de indicadores para la implementación de un IDS en PYMES**"[60]; en el cual se logra evidenciar inicialmente la existencias de diferentes sistemas de monitoreo de tráfico malicioso y que estos a su vez cuentan con capacidades que los hacen importantes en diferentes escenarios; y es así que con el objeto de satisfacer la necesidad del CSIRT de Ciber Security de Colombia Ltda, se opta por el uso de Suricata ya que en muchos de los casos cuenta con características que lo hacen más eficiente y usable que otras de las opciones disponibles.

6.3.2 Servicios tecnológicos. La selección de los servicios tecnológicos a implementar y soportar por parte del CSIRT se realiza en función de la disponibilidad del uso en sistemas UNIX, uso en servicios de producción y necesidades de los usuarios, que sean herramientas de uso libre en cualquiera de las versiones de licenciamiento con el objetivo que se ajusten a las capacidades de Ciber Security de Colombia Ltda; las cuales se presentan a continuación de acuerdo grupo al que pertenecen.

- **Servicio conexión remota**: El protocolo de Secure Shell es la herramienta predilecta para el desarrollo de conexiones remotas hacia host Linux, ya que facilita el proceso de comunicación segura entre diferentes usuarios en multimodal; además SSH brinda grandes garantías de aseguramiento de las comunicaciones, debido a que éste encripta las sesiones de conexión robusta de mínimo 128 bits y ofrece las opciones de usar algoritmos más fuertes o recientes, lo cual hace bastante improbable que un tercero logre obtener las contraseñas .

  SSH cuenta con un gigantesco grupo de usuarios a nivel mundial ya sea por sus capacidades de aseguramiento, así como la disponibilidad de forma nativa en los sistemas Linux objetivo del presente proyecto.

  Finalmente el MIT (Massachusetts Institute of Technology), recomienda en su documentación el uso de SSH, debido a que soporta control de amenazas de intercepción de la comunicación, personificación de host, envenenamiento de DNS, y entre otras[61].

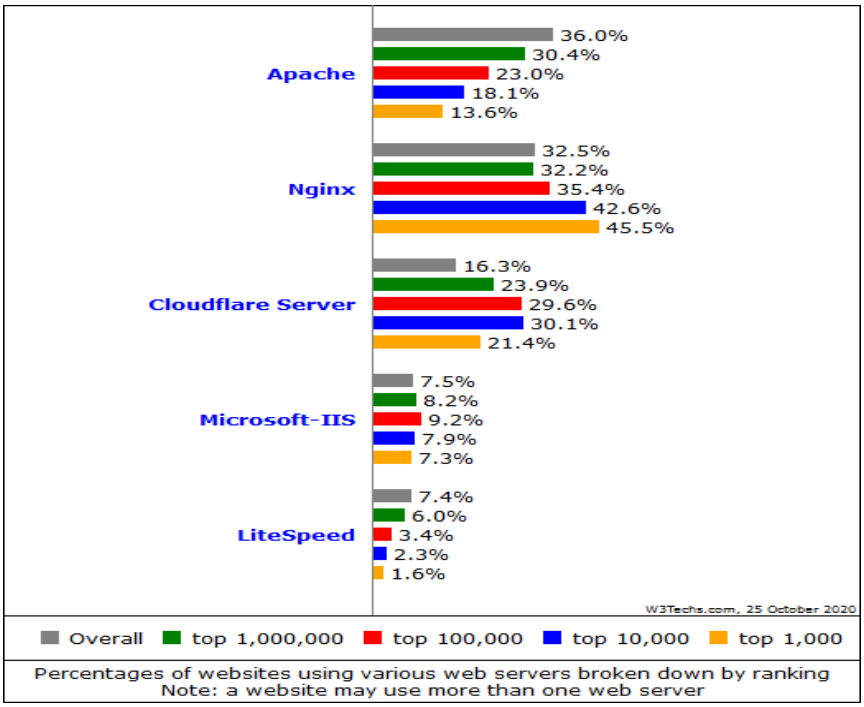
[60] **MÁRCELES VILLALBA, Katerine, PANTOJA, Nelson Darío y AMADOR DONADO, Siler. 2019.** Selección de indicadores para la implementación de un IDS en PYMES. [En línea] 2019. https://search.proquest.com/scholarly-journals/selección-de-indicadores-para-la-implementación/docview/2385759537/se-2?accountid=201395

[61] **MIT, Massachusetts Institute of Technology.** Red Hat Enterprise Linux: Manual de referencia. [En línea] [Citado el: 13 de 12 de 2020.] https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ssh.html.

Por estas razones se opta por el uso de SSH para el desarrollo de los procesos de conexión remota en el CSIRT de Ciber Secutity de Colombia ltda

- **Servicio Web**: Para el desarrollo de las actividades referentes a servicios Web se selecciona el servidor http Apache teniendo en cuenta que este es uno el servidores de este tipo más usado a nivel general en el mundo según el reporte de uso de servidores web presentado por "w3techs.com", el cual evidencia que el 36% de los sitios web a los que se logra identificar el servidor web usan Apache http server este reporte presenta además datos significativos frente a otras opciones disponibles como: Nginx, Cloudflare Server, Microsoft IIS y LiteSpeed[62], tal como se muestra en la Figura 2.

Figura 2 Uso de servidores web desglosado por ranking



Fuente: **W3TECHS. 2020.** Usage of web servers broken down by ranking. [En línea] 2020. [Citado el: 13 de 12 de 2020.] https://w3techs.com/technologies/cross/web_server/ranking.

[62] **W3TECHS. 2020.** Usage of web servers broken down by ranking. [En línea] 2020. [Citado el: 13 de 12 de 2020.] https://w3techs.com/technologies/cross/web_server/ranking.

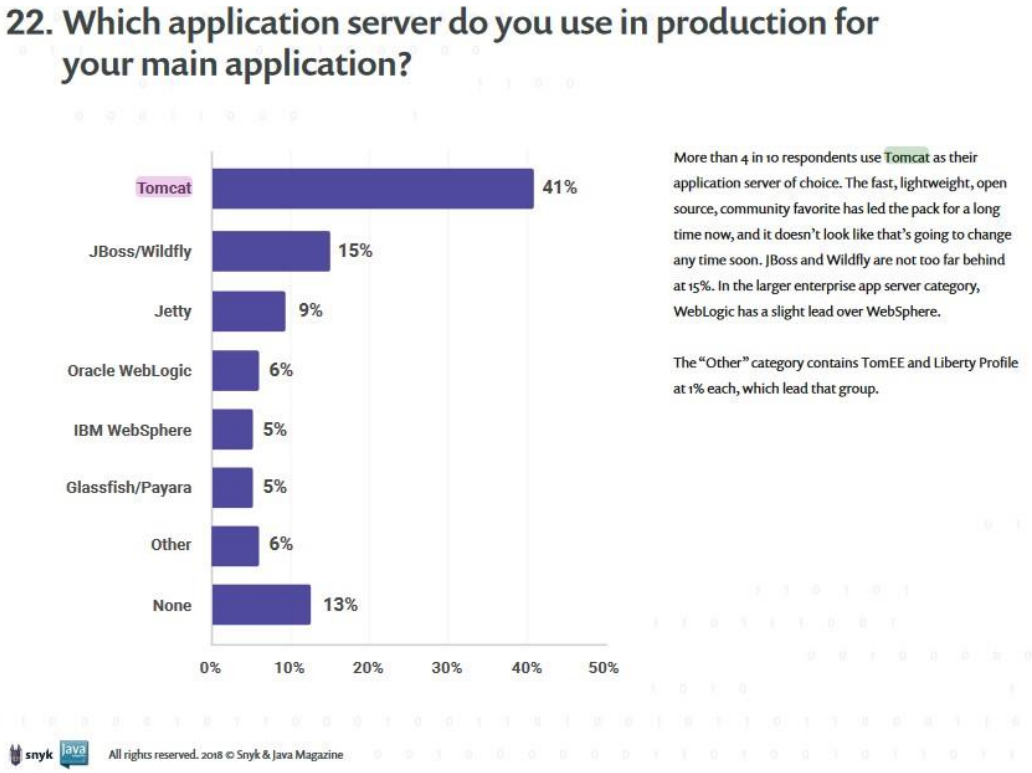
- **Procesamiento de datos**: Java es una de las tecnologías de desarrollo de más amplio uso a nivel mundial en diferentes aspectos, como las aplicaciones de escritorio, dispositivos electrónicos, aplicaciones financieras, aplicaciones Web, entre otros muchos usos según los reportes presentados por Oracle Tecnology Network[63] y otros reportes de cómo el presentado por Skyn & Java Magazine en el que se demuestra alto uso a nivel mundial de la tecnología Java desde la perspectiva de los desarrolladores y los ambientes de producción mismos.

  Según lo mencionado en el reporte del ecosistema JVM[64], 4 de cada 10 encuestados utilizan Apache Tomcat en sus servicios de producción resaltando sus capacidades velocidad, bajo consumo de recursos y el hecho de ser de código abierto ventajas que le permiten abarcar el 41% del mercado frente a otras opciones como JBoss/Wildfly, Jetty, Oracle WebLogic, IBM WebSphere, Glassfish, y entre otras opciones disponibles tal como se detalla en la Figura 3.

[63] **ORACLE TECHNOLOGY NETWORK.** Java. [En línea] [Citado el: 13 de 12 de 2020.] https://www.java.com/es/about/.

[64] **Snyk & Java Magazine. 2018.** res.cloudinary.com. [En línea] 2018. https://res.cloudinary.com/snyk/image/upload/v1539774333/blog/jvm-ecosystem-report-2018.pdf.

Figura 3 ¿Qué servidor de aplicaciones utiliza en producción para su aplicación principal?



Fuente: **Snyk & Java Magazine. 2018.** res.cloudinary.com. [En línea] 2018. https://res.cloudinary.com/snyk/image/upload/v1539774333/blog/jvm-ecosystem-report-2018.pdf.

Por estas razones se consideró importante que el CSIRT de Cybersecurity de Colombia Ltda incorporara dentro de sus servicios la evaluación y construcción del material documental de laboratorio relacionada con el contenedor de tecnologías Java (Java Servlet, JavaServer Pages, WebSocket y Java Expression Languaje), Apache Tomcat teniendo en cuenta que puede presentar una alta demanda de este servicio debido a su alto uso.

- **FTP:** El servicio FTP cuenta con un amplio uso a nivel mundial, debido a la necesidad de poder transferir archivos desde los clientes hacia los servicios ya sean Web, de almacenamiento, copias de seguridad entre otros.

De igual forma es importante tener en cuenta que existen servicios más seguros en éste aspecto como lo es SFTP provisto por el protocolo SSH, pero este presenta un fuerte vínculo con el acceso SSH que en la mayoría de los casos no es viable compartir, por lo cual hoy en día los servicios de

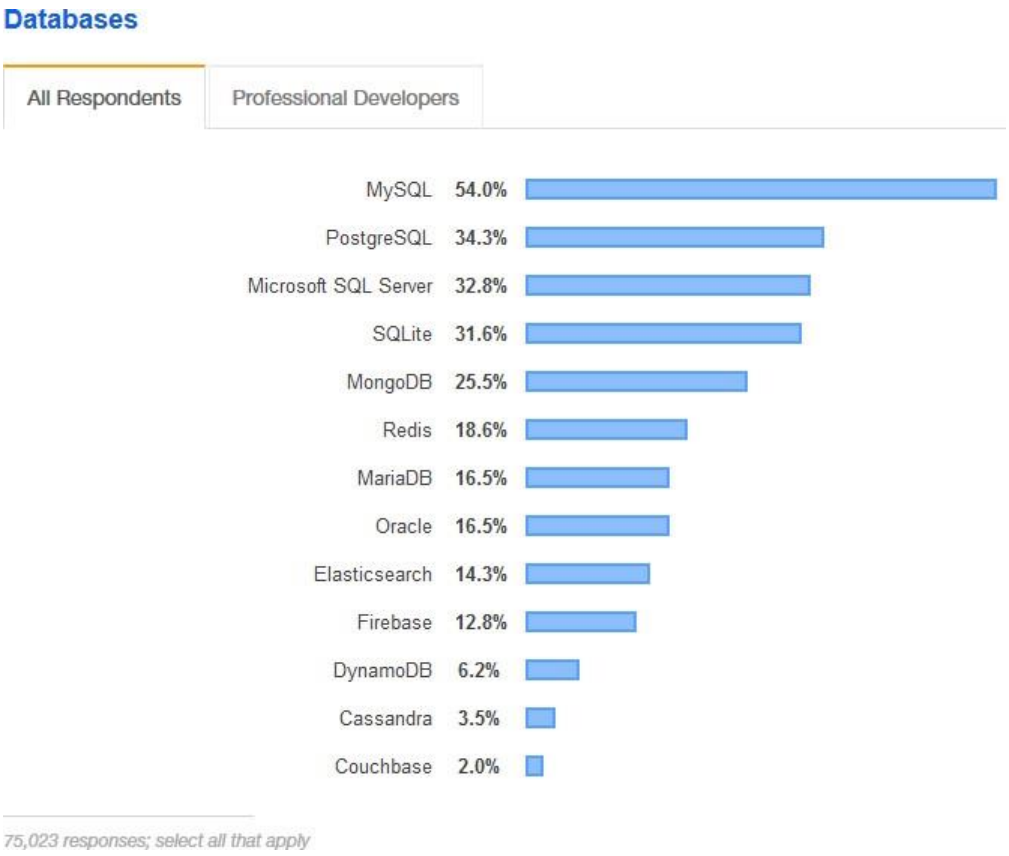
Hosting compartido o dedicado, servidores dedicados y otras implementaciones optan por el uso de FTP para atacar esta necesidad.

Es por esto que para la operación de los servicios del CSIRT de Cybersecurity de Colombia Ltda se selecciona una de las opciones disponibles en el mercado de las herramientas para la aplicación en sistemas GNU/Linux; en este caso particular se optó por VSFTPD, debido a su disponibilidad de forma nativa en el sistema operativo, su licenciamiento GNU/GLPLv2 y sus características de aseguramiento del servicio como por ejemplo el encerramiento usuarios (chroot), la posibilidad de implementación de SSL, y entre otras características[65].

- **Servicios de bases de datos**: En este aspecto particular con soporte en los resultados de la encuesta para desarrolladores elaborada por el portal para desarrolladores y entusiastas del desarrollo de software "Developer Survey Results 2019"[66]; aplicada a 75.025 usuarios muestra que las dos bases de datos más utilizadas durante el año 2019 son MySQL y PostgreSQL respectivamente tal como se muestran en la Figura 4.

[65] **EVANS, Chris.** Probably the most secure and fastest FTP server for UNIX-like systems. [En línea] [Citado el: 11 de 12 de 2020.] https://security.appspot.com/vsftpd.html#features.
[66] **STACKOVERFLOW. 2019.** Developer Survey Results 2019. [En línea] 2019. [Citado el: 02 de 12 de 2020.] https://insights.stackoverflow.com/survey/2019#technology.

Figura 4 resultados de la encuesta para desarrolladores en el uso de bases de datos



Fuente: STACKOVERFLOW. 2019. Developer Survey Results 2019. [En línea] 2019. [Citado el: 02 de 12 de 2020.] https://insights.stackoverflow.com/survey/2019#technology.

Pero según el enfoque que se plantea para el funcionamiento del CSIRT se descarta MySQL, debido a su licenciamiento privativo a diferencia de PostgreSQL que cuenta con licenciamiento BSD o también conocido como MIT licence que permiten el uso libre del software, pero no comparten el código fuente en este caso particular por razones de aseguramiento del código, el cual debe ser aprobado y probado para su liberación por el equipo global de desarrollo para su publicación oficial.

6.3.3 Herramientas de diagnóstico, testing e informes. La selección de las herramientas se realiza en función de las capacidades y necesidades planteadas para el correcto funcionamiento del CSIRT de Cybersecurity de Colombia Ltda, el licenciamiento, el uso dentro de las comunidades técnicas y las capacidades ajustadas a los servicios tecnológicos a usar.

A continuación se presenta la relación de herramientas de diagnóstico, testing e informes que se plantean usar en el CSIRT de la empresa "Cybersecurity de Colombia Ltda"

- **Openvas**: Cuenta con licenciamiento GNU/GPL, es un escáner de vulnerabilidades con comunidad de desarrollo y soporte a nivel mundial; lo que hace que se mantenga en constante actualización y monitoreo, cuenta con más de 50.000 pruebas de vulnerabilidades lo que lo hace útil el desarrollo de escaneos de diferente índole en los sistemas informáticos presentes en los usuarios del CSIRT de Ciber Secutity de Colombia Ltda[67].

- **Vega**: Es una herramienta de escaneo de vulnerabilidades Web de código abierto licenciado bajo el modelo EPL (Eclipse Public Licence), el cual provee una plataforma para el desarrollo de prueba de seguridad a sistemas Web en los que es posible determinar entre otras, vulnerabilidades SQL injection, inclusión de archivos remotos, Cross-Site, Scripting XSS, además de esto permite la generación de informes claros y detallados de los escaneos[68].

- **Kali Linux**: Es tal vez la herramienta más valiosa de uso libre GNU/GPL v2 con la que se puede contar en el CSIRT, ya que esta ofrece un amplio abanico de opciones para desarrollar tanto pruebas de vulnerabilidad, como ataques controlados a diferentes servicios que permiten tener opciones frente al diverso ecosistema de la seguridad informática y la gran variedad de frentes que se pueden llegar a tener en esta materia[69].

- **Nikto**: Escáner de vulnerabilidades de servicios http licenciado bajo el esquema GNU/GPL, el cual cuenta con más de 8000 pruebas dirigidas a identificar vulnerabilidades potencialmente peligrosas; además de buscar versiones de los servidores instalados y el software complementario presente en estos[70].

  Con soporte en lo anterior se considera Nikto una herramienta importante para la validación de vulnerabilidades en el CSIRT en la empresa "Cybersecurity de Colombia Ltda

---

[67] **GREENBONE NETWORKS GMBH. 2020.** Greenbone Security Manager with Greenbone OS 20.08 – User Manual. [En línea] 30 de 11 de 2020. [Citado el: 12 de 12 de 2020.] https://docs.greenbone.net/GSM-Manual/gos-20.08/en/

[68] **SUBGRAPH. 2020.** Vega helps you find and fix cross-site scripting (XSS), SQL injection, and more. [En línea] 2020. [Citado el: 30 de 11 de 2020.] https://subgraph.com/vega/.

[69] **KALI - OFFENSIVE SECURITY . 2019.** What is Kali Linux? [En línea] 26 de 10 de 2019. [Citado el: 19 de 02 de 2020.] https://www.kali.org/docs/introduction/what-is-kali-linux/.

[70] **SULLO, Chris; LODGE, David. 2020.** Nikto2. [En línea] 2020. [Citado el: 21 de 02 de 2020.] https://cirt.net/Nikto2

- **Nmap:** Escáner de red con licencia GNU/GPL v2 el cual se constituye en una importante herramienta para la verificación de vulnerabilidades y configuraciones de red dentro de las operaciones a realizar en la CSIRT[71]

- **Metasploit framework:** Provee un gigantesco paquete de información de seguridad informática, ayudas para la elaboración de pruebas de penetración, con licencia BSD motivo por el cual es una herramienta importante para el desarrollo de las actividades del CSIRT[72].

- **Autopsy:** Herramienta de código abierto que representa gran importancia para el CSIRT, debido a que permite la extracción de la información que se encuentra en los computadores, servidores y otros dispositivos a través de imágenes bit a bit para el desarrollo de análisis forenses, la generación de diferentes informes y la recuperación de meta data de los archivos, cuenta con una gran comunidad a nivel mundial y está en constante desarrollo lo que le da gran valor a las actividades desarrolladas en la CSIRT[73].

El proceso de selección de las herramientas correspondió a un ejercicio inicial de construcción el CSIRT, pero debido a la naturaleza misma de la seguridad informática es necesario que en el trascurso del tiempo y la evolución de las vulnerabilidades, los riesgos y las agresiones este ecosistema de aplicaciones se robustezca y se mejoren las implementaciones con forme avanza la tecnología con el propósito de afianzar cada más el CSIRT de Cybersecurity de Colombia y fortalecer los servicios que presta.

6.4 FASE 4: DESARROLLO DEL DISEÑO DE UN LABORATORIO CONTROLADO POR MEDIO DEL USO DE MÁQUINAS VIRTUALES QUE PERMITA LA EJECUCIÓN DE PRUEBAS DEL SOFTWARE QUE SE UTILIZARA EN EL CSIRT.

El desarrollo de la presente fase se dio por medio de la consecución de dos sub fases que permitieron llevar a cabo la actividad de forma integrada y siguiendo la

[71] **NMAP ORG.** Chapter 15. Nmap Reference Guide. [En línea] [Citado el: 30 de 11 de 2020.] https://nmap.org/book/man.html.

[72] **DOCS RAPID7. 2020.** Quick Start Guide. [En línea] 2020. [Citado el: 25 de 11 de 2020.] https://docs.rapid7.com/metasploit/.

[73] **BASIS TECHNOLOGY. 2018.** Fast, Thorough, and Efficient Investigations. [En línea] 2018. [Citado el: 20 de 11 de 2020.] https://s3.amazonaws.com/resources.autopsy.com/datasheets/Autopsy-EN.pdf.

línea general planteada por el objetivo a cumplir las cuales se muestran a continuación.

- **SUB FASE 1:** Se compone de la construcción de un escenario problema en el que se detallan las características de un incidente de seguridad informática, el contexto en el que este se desarrolla y se establecen las actividades que se deben llevar a cabo en el marco del desarrollo del objetivo propuesto.

  De esta sub fase se genera el documento entregable: Anexo A. Escenario problema

- **SUB FASE 2:** Se compone del desarrollo del laboratorio basado en el escenario problema en el cual se enmarcan las actividades, la correspondiente propuesta de solución a cada una de las actividades planteadas en el escenario problema y su correspondiente prueba de validación; este laboratorio se presenta en función del cumplimiento del objetivo propuesto.

  De esta sub fase se genera el documento entregable: Anexo B. Laboratorio del escenario problema

7 CONCLUSIONES

Con la recopilación de la información referente a las herramientas software que permitirán el desarrollo de los servicios reactivos y proactivos del CSIRT; se logra determinar que en el mercado del software se encuentran disponibles opciones de todo tipo, situación que es favorable al CSIRT, ya que esto facilita en gran medida el adecuado desarrollo de sus actividades y como valor agregado poder imprimirles el sello de calidad que se necesita.

La planeación del mapa de la estructura TI del CSIRT es uno de los elementos fundamentales dentro de la consolidación de este, ya que de esta forma se logra la determinación clara de cada una de las áreas que se necesitan para su optima operación, sumado a esto por esta misma vía se logra avanzar en la construcción de los diferentes perfiles que se requieren para lograr cumplir con el propósito de cada dependencia establecida.

La selección de las herramientas software a utilizar para el desarrollo de las actividades del CSIRT permitió a partir de un grupo de herramientas; identificar diferencias y capacidades individuales que dieron lugar a que cada una de estas se seleccionara en un primer ejercicio con motivo de enfocar más estrechamente los esfuerzos iniciales en el marco de dar los primeros pasos en la construcción del CSIRT; dejando claro que en el futuro las herramientas descartadas u otras no tenidas en cuenta dentro del proceso pueden ser incluidas para la correspondiente adopción y uso.

El diseño del laboratorio generó como resultado una experiencia altamente favorable tanto para la empresa como para el recién creado CSIRT ya que este permitió limpiar el camino y obtener un visión inicial importante alrededor de las actividades que se desarrollan en el CSIRT teniendo en cuenta que dentro de este se buscó englobar el problema desde su concepción inicial, pasando por la revisión, la propuesta de solución y la prueba de operación; elementos que son fundamentales para el cumplimiento del objetivo de Cybersecurity de Colombia como empresa que ofrece servicios de seguridad.

8 RECOMENDACIONES

La consolidación de las posibles herramientas software planteadas para el desarrollo inicial del CSIRT corresponde a una revisión de las herramientas que se adaptan mejor en la actualidad para su funcionamiento; pero de igual forma es recomendable la constante revisión de nuevas herramientas o de las mejoras de la ya existen teniendo en cuenta que tanto las herramientas como la amenazas evolucionan día tras día.

La computación tal como la conocemos hoy día está en constante desarrollo, mejora y modernización razón por la cual se recomienda que los procesos realizados en el CSIRT ya sea desde el enfoque técnico como en el enfoque administrativo evolucionen lo más acorde posible al avance de la tecnología con el fin de lograr garantizar a los usuarios que las acciones que se llevan a cabo permiten minimizar, tratar y prevenir los riesgos de la forma más acertada posible y haciendo uso de los métodos con mayor nivel efectividad disponible.

Se invita a cada uno de quienes participen dentro de las propuestas, acciones o revisiones desarrolladas en presente documento a la construcción, aporte o mejora de componentes similares que permitan el fortalecimiento y crecimiento de este tipo de procesos que son fundamentales para la creación de entornos virtuales mucho más seguros, responsables y sanos para los usuarios de las diferentes tecnologías con las que se cuenta en la actualidad y de las cuales dependen muchas de las acciones que realizamos en nuestro diario vivir.

BIBLIOGRAFÍA

AIRCRACK NG. 2020. Aircrack-ng is a complete suite of tools to assess WiFi network security. [En línea] 2020. [Citado el: 23 de 02 de 2020.] https://www.aircrack-ng.org/.

ASOBANCARIA. 2019. Memoria anual CSIRT financiero ASOBANCARIA 2019. [En línea] 2019. [Citado el: 28 de 11 de 2020.] https://www.asobancaria.com/wp-content/uploads/2020/06/CRT-MA_2020_compressed.pdf.

BASIS TECHNOLOGY. 2018. Fast, Thorough, and Efficient Investigations. [En línea] 2018. [Citado el: 20 de 11 de 2020.] https://s3.amazonaws.com/resources.autopsy.com/datasheets/Autopsy-EN.pdf.

CCIT- POLICIA NACIONAL DE COLOMBIA. 2020. Informe de las tendencias del cibercrimen en Colombia (2019-2020). [En línea] 20 de 10 de 2020. [Citado el: 28 de 11 de 2020.] https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf.

CLANG.LLVM.ORG. 2020. Getting Started: Building and Running Clang. [En línea] 2020. [Citado el: 23 de 02 de 2020.] https://clang.llvm.org/get_started.html.

COLOMBIA. ASAMBLEA NACIONAL CONSTITUYENTE. 1991. Constitución Política de la República de Colombia. [En línea] 20 de 07 de 1991. [Citado el: 29 de 11 de 2020.] http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html.

COLOMBIA. CONGRESO DE COLOMBIA. 2009. Ley 1273 de 2009. [En línea] 05 de 01 de 2009. [Citado el: 29 de 11 de 2020.] https://mintic.gov.co/portal/604/articles-3705_documento.pdf.

COLOMBIA. CONGRESO DE LA REPÚBLICA. 2012. Ley estatutaria 1581 de 2012. [En línea] 18 de 10 de 2012. [Citado el: 29 de 11 de 2020.] http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html.

COLOMBIA. EL CONGRESO DE COLOMBIA. 2000. Ley 599 De 2000. [En línea] 24 de 7 de 2000. [Citado el: 28 de 11 de 2020.] https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388.

COLOMBIA. EL CONGRESO DE COLOMBIA. 1993. Ley 87 de 1993. [En línea] 29 de 11 de 1993. [Citado el: 29 de 11 de 2020.] http://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=300.

COLOMBIA. MINISTERIO DE LAS TIC. 2019. Manual de gobierno digital. [En línea] 04 de 2019. [Citado el: 30 de 11 de 2020.] https://www.mintic.gov.co/portal/604/articles-81473_recurso_1.pdf.

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. 2016. colaboracion.dnp.gov.co. [En línea] 2016. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf.

DAMELE, Bernardo y STAMPAR, Miroslav. 2020. SQLMAP introduction. [En línea] 2020. [Citado el: 22 de 02 de 2020.] http://sqlmap.org/.

DE LA TORRE MOSCOSO, Hugo Marcelo y PARRA ROSERO, Mario Andrés. 2018. Estrategia y diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la Universidad de las Fuerzas Armadas ESPE. [En línea] 2018. [Citado el: 28 de 11 de 2020.] http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/15071/T-ESPE-040447.pdf?sequence=1&isAllowed=y.

DEEPAK, Damodaran, y otros. 2012. Performance Evaluation of VMware and VirtualBox. [En línea] 2012. http://www.ipcsit.com/vol29/006-ICSST2012-S015.pdf.
DOCS RAPID7. 2020. Quick Start Guide. [En línea] 2020. [Citado el: 25 de 11 de 2020.] https://docs.rapid7.com/metasploit/.

DRAGON JAR. 2018. Metasploitable 3, Instalación en GNU/Linux, Windows y Mac OS. [En línea] 2018. [Citado el: 28 de 11 de 2020.] https://www.dragonjar.org/metasploitable-3-instalacion-en-gnulinux-windows-y-mac-os.xhtml.

ECURED. 2010. Seguridad Informática. [En línea] 2010. [Citado el: 29 de 11 de 2020.] https://www.ecured.cu/Seguridad_Inform%C3%A1tica.

ESPAÑA. CENTRO CRIPTOLÓGICO NACIONAL. 2011. Guía de Creación de un CERT/CSIRT. [En línea] 09 de 2011. [Citado el: 27 de 11 de 2020.] https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-sep11.pdf.

EVANS, Chris. Probably the most secure and fastest FTP server for UNIX-like systems. [En línea] [Citado el: 11 de 12 de 2020.] https://security.appspot.com/vsftpd.html#features.

EXPLOIT DATABASE. 2020. SearchSploit – The Manual. [En línea] 2020. [Citado el: 23 de 02 de 2020.] https://www.exploit-db.com/searchsploit.

FERREIRO CANOSA, Alejandro. 2017. Escaneo de vulnerabilidades con Vega. [En línea] 03 de 01 de 2017. https://backtrackacademy.com/articulo/escaneo-de-vulnerabilidades-con-vega-parte-1.

GARCÍA, Mónica Alexandra. 2014. Propuesta de diseño de un área informática forense para un equipo de respuestas ante incidentes de seguridad informáticos, CSIRT. [En línea] 2014. [Citado el: 28 de 11 de 2020.] http://repositorio.espe.edu.ec/bitstream/21000/8063/1/T-ESPE-047639.pdf.

GORGONA, Luis. 2015. Primera respuesta: antes de que llegue la policía. [En línea] 2015. [Citado el: 28 de 11 de 2020.] https://www.oas.org/juridico/spanish/cyber/cyb46_csirts_sp.pdf.

GREENBONE NETWORKS GMBH. 2020. Greenbone Security Manager with Greenbone OS 20.08 – User Manual. [En línea] 30 de 11 de 2020. [Citado el: 12 de 12 de 2020.] https://docs.greenbone.net/GSM-Manual/gos-20.08/en/.

HERNÁNDEZ, Miguel. 2015. ¿Qué tanto aporta la industria TIC a la economía nacional? [En línea] 2015. [Citado el: 10 de 05 de 2020.] https://www.eltiempo.com/archivo/documento/CMS-15618752.
HURAJAND ČERŇANSKÝ, Šimon. 2015. Performance Evaluations of IPTables Firewall Solutions under DDoS attacks. [En línea] 2015. https://content.sciendo.com/downloadpdf/journals/jamsi/11/2/article-p35.pdf.

KALI - OFFENSIVE SECURITY . 2019. What is Kali Linux? [En línea] 26 de 10 de 2019. [Citado el: 19 de 02 de 2020.] https://www.kali.org/docs/introduction/what-is-kali-linux/.

KALI LINUX. 2020. CeWL package description. [En línea] 2020. [Citado el: 22 de 02 de 2020.] https://tools.kali.org/password-attacks/cewl.

KALI LINUX NET. 2020. Kali Linux en español. *Automated wireless auditor.* [En línea] 2020. [Citado el: 23 de 02 de 2020.] https://kali-linux.net/article/wifite/.

KALI TOOLS. 2020. Commix package description. [En línea] 2020. [Citado el: 21 de 02 de 2020.] https://tools.kali.org/exploitation-tools/commix.

KALI-TOOLS. 2020. Hydra package description. [En línea] 2020. [Citado el: 22 de 02 de 2020.] https://tools.kali.org/password-attacks/hydra.

La investigación aplicada: Una forma de conocer las realidades con evidencia científica. VARGAS CORDERO, Zoila Rosa. 2009. 1, San Pedro, Costa Rica : s.n., 2009, Vol. 33. 0379-7082.

LAGORIO, Florencia y PAYERO, Abril. 2016. Riesgos Informaticos. [En línea] 2016. [Citado el: 29 de 11 de 2020.] https://sites.google.com/site/tecnologiadigital20/home/riesgos-informaticos.

LANFRANCO, Einar. ¿De qué se trata?, modelos posibles,servicios y herramientas. [En línea] [Citado el: 01 de 05 de 2020.] https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2016/15551-EC/4B%201.pdf.

MÁRCELES VILLALBA, Katerine, PANTOJA, Nelson Darío y AMADOR DONADO, Siler. 2019. Selección de indicadores para la implementación de un IDS en PYMES. [En línea] 2019. https://search.proquest.com/scholarly-journals/selección-de-indicadores-para-la-implementación/docview/2385759537/se-2?accountid=201395.

MARKER, Graciela. 2020. Vulnerabilidades informáticas. [En línea] 22 de 07 de 2020. [Citado el: 28 de 11 de 2020.] https://www.tecnologia-informatica.com/vulnerabilidades-informaticas/.

MENDOZA, Miguel Ángel. 2015. ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes? [En línea] 18 de 05 de 2015. [Citado el: 01 de 05 de 2020.] https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/.

MIN TIC DE COLOMBIA. 2019. Proyectos de inversión 2020 FUTIC. [En línea] 31 de 12 de 2019. [Citado el: 28 de 11 de 2020.] https://www.mintic.gov.co/portal/604/articles-1783_Proyectos_inversion_2020.pdf.

MINTIC - Colombia. 2016. mintic.gov.co. [En línea] 2016. https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf.

MINTIC. 2016. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. [En línea] 2016. [Citado el: 28 de 11 de 2020.] https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf.

MIT, Massachusetts Institute of Technology. Red Hat Enterprise Linux: Manual de referencia. [En línea] [Citado el: 13 de 12 de 2020.] https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ssh.html.

MUÑOZ, Mirna y RIVAS, Lizbeth. 2015. Estado actual de equipos de respuesta a incidentes de seguridad informática. [En línea] 03 de 2015. http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1646-98952015000100002.

NMAP. 2017. Nmap ("Network Mapper"). [En línea] 2017. [Citado el: 21 de 02 de 2020.] https://nmap.org/.

NMAP ORG. Chapter 15. Nmap Reference Guide. [En línea] [Citado el: 30 de 11 de 2020.] https://nmap.org/book/man.html.

NMAP ORG. 2020. Ncrack is a high-speed network authentication cracking tool. [En línea] 2020. [Citado el: 22 de 02 de 2020.] https://nmap.org/ncrack/.

OBBAYI, Lester. 2019. A Brief Introduction to the Nessus Vulnerability Scanner. [En línea] 26 de 07 de 2019. [Citado el: 28 de 11 de 2020.] https://resources.infosecinstitute.com/topic/a-brief-introduction-to-the-nessus-vulnerability-scanner/.

OPENVAS. 2020. Open Vulnerability Assessment Scanner. [En línea] 2020. [Citado el: 28 de 11 de 2020.] http://www.openvas.org/.

ORACLE TECHNOLOGY NETWORK. Java. [En línea] [Citado el: 13 de 12 de 2020.] https://www.java.com/es/about/.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA). 2016. Buenas prácticas para establecer un CSIRT nacional. [En línea] 04 de 2016. [Citado el: 6 de 1 de 2020.] https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf.

OSPINA JARRO, Eduardo Andres. 2018. Modelo de protección de activos de información estratégica: una lectura desde la dirección y gerencia de la seguridad de la información. [En línea] 2018. [Citado el: 28 de 11 de 2020.] https://repository.urosario.edu.co/bitstream/handle/10336/20003/UR-ArtInvestigacion-EduardoAndresOspinaJarro.pdf?sequence=1&isAllowed=y.

PARRA MORENO, Duver Augusto. 2012. Gestión del riesgo en la seguridad informática: “Cultura de la auto-seguridad informática”. [En línea] 2012. [Citado el: 28 de 11 de 2020.] https://repository.unimilitar.edu.co/bitstream/handle/10654/6821/ParraMorenoDuverAugusto2012.pdf;jsessionid=C43AFCD7F74F007A88D99FB1613DB1E8?sequence=2.

PAUS, Lucas. 2015. Cómo auditar la seguridad de tu sitio web con Vega. [En línea] 03 de 03 de 2015. [Citado el: 28 de 11 de 2020.] https://www.welivesecurity.com/la-es/2015/03/03/como-auditar-la-seguridad-sitio-web-vega/.

PEREZ, Diego. 2016. Radare2: abriendo las puertas al reversing. [En línea] 17 de 08 de 2016. [Citado el: 23 de 02 de 2020.] https://www.welivesecurity.com/la-es/2016/08/17/radare2-reversing/.

POROLLI, Matías. 2013. Cómo realizar un análisis forense con Autopsy. [En línea] 23 de 09 de 2013. [Citado el: 23 de 02 de 2020.] https://www.welivesecurity.com/la-es/2013/09/23/como-realizar-analisis-forense-autopsy/.

PRESIDENCIA DE LA REPUBLICA DE COLOMBIA. 2019. Declaración del Presidente Iván Duque sobre su visita a Microsoft en Seattle. [En línea] 09 de 05 de 2019. https://id.presidencia.gov.co/Paginas/prensa/2019/190509-Declaracion-del-Presidente-Ivan-Duque-sobre-su-visita-a-Microsoft-en-Seattle.aspx.

QUINTERO TAMAYO, John. 2016. Introducción a la seguridad informática - OVA. [En línea] 2016. [Citado el: 28 de 11 de 2020.] http://stadium.unad.edu.co/ovas/10596_9956/seguridad_informtica.html.

Rapid7. 2019. github.com/rapid7/metasploitable3. [En línea] 2019. https://github.com/rapid7/metasploitable3.

RAPID7-METASPLOIT. 2020. Getting Started Metasploit . [En línea] 2020. [Citado el: 23 de 02 de 2020.] https://metasploit.help.rapid7.com/docs/getting-started.

REDHAT. 2020. ¿Qué es la infraestructura de TI? [En línea] 2020. [Citado el: 13 de 12 de 2020.] https://www.redhat.com/es/topics/cloud-computing/what-is-it-infrastructure.

SÁNCHEZ, Héctor Mauricio y RODRÍGUEZ PARRA, Alexander. 2019. Constitución de un CSIRT para una Entidad Financiera en Colombia. [En línea] 12 de 2019. [Citado el: 28 de 11 de 2020.] https://proyectosmaestrias.virtual.uniandes.edu.co/images/TNQzugjz0p1d26AM6aQVaAs8MbHg9RzfnHBnKmhf.pdf.

Snyk & Java Magazine. 2018. res.cloudinary.com. [En línea] 2018. https://res.cloudinary.com/snyk/image/upload/v1539774333/blog/jvm-ecosystem-report-2018.pdf.

SNYK; JAVA MAGAZINE. 2018. JVM Ecosystem Report 2018. A snapshot of the JVM landscape. [En línea] 2018. [Citado el: 09 de 12 de 2020.] https://res.cloudinary.com/snyk/image/upload/v1539774333/blog/jvm-ecosystem-report-2018.pdf.

STACKOVERFLOW. 2019. Developer Survey Results 2019. [En línea] 2019. [Citado el: 02 de 12 de 2020.] https://insights.stackoverflow.com/survey/2019#technology.

SUBGRAPH. 2020. Vega helps you find and fix cross-site scripting (XSS), SQL injection, and more. [En línea] 2020. [Citado el: 30 de 11 de 2020.] https://subgraph.com/vega/.

SULLO, Chris; LODGE, David. 2020. Nikto2. [En línea] 2020. [Citado el: 21 de 02 de 2020.] https://cirt.net/Nikto2.

SURICATA-IDS. 2020. Suricata Open Source IDS / IPS / NSM engine. [En línea] 2020. [Citado el: 30 de 11 de 2020.] https://suricata-ids.org/.

TOOLS.KALI.ORG. 2020. Reaver Package Description. [En línea] 2020. [Citado el: 23 de 02 de 2020.] https://tools.kali.org/wireless-attacks/reaver.

UNIVERSIDAD INTERNACIONAL DEL VALENCIA. 2018. www.universidadviu.com. *Vulnerabilidad informática, tipos y debilidades principales.* [En línea] 24 de 04 de 2018. [Citado el: 28 de 11 de 2020.] https://www.universidadviu.com/vulnerabilidad-informatica-tipos-debilidades-principales/.

W3TECHS. 2020. Usage of web servers broken down by ranking. [En línea] 2020. [Citado el: 13 de 12 de 2020.] https://w3techs.com/technologies/cross/web_server/ranking.

wordpress.org. wordpress.org. [En línea] [Citado el: 21 de 2 de 2020.] https://es.wordpress.org/support/article/new-to-wordpress-where-to-start/#paso-uno-leer.

wpscan.org. wpscan.org. [En línea] [Citado el: 21 de 2 de 2020.] https://wpscan.org/.

ANEXOS

Anexo A. Escenario problema

Datos generales	
Usuario:	Cybersecurity de Colombia LTDA
Tipo de proceso:	Gestión de incidente en el entorno de pruebas controlado
Situación problema:	Manipulación de registros en el departamento financiero
Nota:	Cybersecurity de Colombia LTDA y GEST-Financia son componentes ficticios usados para el desarrollo del proceso académico.

1. CONTEXTO AL PROBLEMA.

Cybersecurity de Colombia LTDA, es una compañía que ofrece servicios de seguridad para la protección de información la cual cuenta con diferentes servicios tecnológicos para el desarrollo de sus actividades misionales y administrativas entre las que se encuentran.

- Sistema ERP (Sistema de planificación de recursos empresariales), "GEST-Financia".
- Red de comunicaciones y video vigilancia.
- Centro de servidores.
- Otros sistemas de apoyo a los procesos.

La anterior infraestructura es mantenida y soportada por el área de sistemas que consta de 2 ingenieros que se especializan principalmente en la gestión en el nivel de usuario final de los servicios.

Dicho ésto en días anteriores se presentó un incidente de seguridad informática identificado y reportado al equipo de sistemas por un funcionario del área de contabilidad en el que manifestó que los datos registrados en uno de los movimientos financieros fue modificado y que esta alteración se realizó con su usuario del sistema "GEST-Financia".

De forma inmediata el personal de sistemas acompañado por personal delegado de la alta gerencia procede a desarrollar la evaluación inicial de la situación reportada ejecutando las siguientes actividades.

- Apertura de un proceso de indagación interno en el que participan los funcionarios del equipo de sistemas, la funcionario del área contable, los jefes inmediatos del funcionario y el personal de vigilancia; esto con el fin de recopilar la mayor cantidad de información.
- Se solicitan y revisan las grabaciones del sistema de video vigilancia con 30 días de anterioridad a la fecha del reporte del incidente.
- Se genera reporte de hallazgos a la alta gerencia para su análisis.

Al finalizar el ejercicio anterior; se establecen las siguientes conclusiones iniciales.

Los sistemas de información solo pueden ser accedidos dentro de las instalaciones de "Cybersecurity de Colombia LTDA", por lo tanto la agresión se realizó internamente.

El funcionario de contabilidad se encontraba en incapacidad médica desde un día antes de la fecha, en la cual se desarrolló el incidente y según las grabaciones no asistió en esos días a la institución.

En las grabaciones se identificó una situación extraña con una persona que pertenece al área de mantenimiento quien había ingresado a la empresa hace un mes aproximadamente y que a la fecha del reporte del incidente ya no trabajaba en la empresa por causa renuncia voluntaria motivada en que por problemas personales no podía continuar este ex empleado se ve en la grabaciones operando continuamente una computadora portátil, dispuesta para el registro de actividades diarias del equipo de mantenimiento y que se conecta a un punto de red, ya que el sistema de registro de información lo requiere por su arquitectura Web.

Frente a esto se interroga al equipo de sistemas sobre la posibilidad de que desde este punto de red se pudiera tener acceso a otros recursos de la compañía a lo que responden los funcionarios:

> "La entidad no cuenta con equipamiento físico para la protección, no se tienen controles lógicos para el control de este tipo de conexiones y no se cuenta con el personal técnico asociado al área

para la implementación de estas características a los sistemas y redes".

Con esta información las directivas de la compañía, solicitan que de manera inmediata el área de sistemas identifique los principales problemas de seguridad y que estos sean remitidos al recién creado CSIRT de la empresa para que proponga y de alternativas de solución mediante una prueba piloto a los diferentes inconvenientes planteados como fase inicial de aseguramiento de la entidad y que a su vez emita algunas conclusiones del incidente presentado con base en la información que se tiene.

2. ACTIVIDADES REQUERIDAS.

Atendiendo a las indicaciones entregadas por la alta dirección el equipo de sistemas de **Cybersecurity de Colombia LTDA** procede a realizar el análisis de las principales vulnerabilidades las cuales se remiten al **CSIRT** para que estas sean revisadas y se propongan las alternativas de solución implementadas bajo un mecanismo controlado de pruebas.

Se presenta a continuación la relación de hallazgos encontrados.

Componente	Vulnerabilidad
Servicio web Apache que soporta el frontend de los sistemas	No cuenta con https
Servicio Apache Tomcat que soporta el backend de los sistemas	Es disponible públicamente. No se controla el acceso a nivel de red.
Servicio de base de datos PostgreSQL que soporta la persistencia de los sistemas.	Es disponible públicamente. No se controla el acceso a nivel de red. No se controla el acceso lógico.

Red de comunicaciones	No cuenta con controles de acceso desde cualquier punto se asigna IP la cual se provee por el enrutador del ISP No se cuenta con IDS (Sistema de detección de intrusos)
Servicio FTP	Los usuarios que tienen acceso a este servicio pueden ver los archivos y carpetas diferentes a los que se le tiene permitido
Usuario final	Se han presentado incidentes menores de seguridad informática como el borrado de archivos o el uso inadecuado de los computadores pero no se conocen herramientas que permitan la verificación y análisis de los mismos.

Anexo B. Laboratorio del escenario problema

CONTENIDO

Tabla de ilustraciones

pag.

1. OBJETIVO.

Proponer alternativas de solución a los problemas de seguridad planteados por el equipo de sistemas de "**Cybersecurity de Colombia**" mediante el desarrollo de una prueba piloto usando máquinas virtuales y se emitan algunas conclusiones frente al incidente planteado en el escenario problema.

2. MATERIALES Y RECURSOS.

Tipo	Descripción	Cantidad
Software	Máquina virtual en VirtualBox en la que se refleje el estado actual de los servicios asociados al sistema "GEST-Financia".	1
Software	Máquina virtual KAli Linux para el desarrollo de pruebas.	1
Software	Cliente SSH	1
Software	Cliente FTP	1
Software	Cliente Microsoft Windows 10	1
Hardware	Computador con 256 Gb de espacio en disco disponible, 8Gb de memoria RAM, procesador mínimo de 4 núcleos y conexión a internet.	1

3. DESARROLLO.

Se implementa máquina virtual en la herramienta VirtualBox en la cual se replican los servicios de producción por medio de la restauración de un disco virtual proporcionado por el equipo de sistemas de Cybersecurity al cual previo a la entrega retiraron los componentes de datos críticos dejando únicamente los servicios pero sin datos.

Otra característica importante es que el servidor no cuenta con instalación de entorno gráfico por lo cual se debe operar en el nivel de consola de comandos.

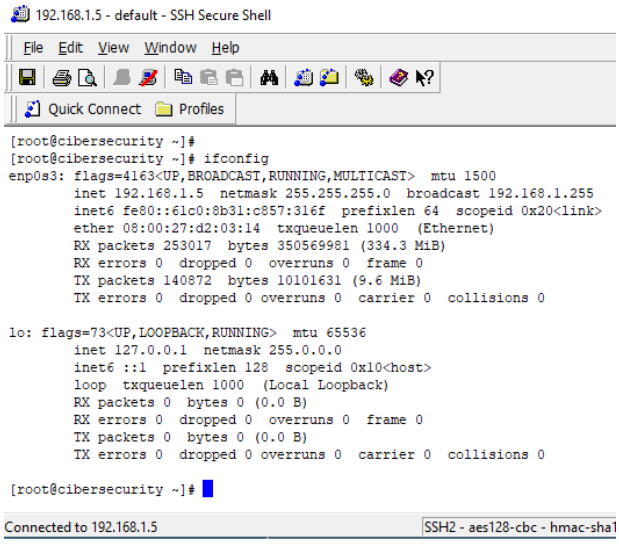
Para facilitar la gestión y la ejecución de comandos el servidor se accederá desde un cliente SSH

3.1. VERIFICACION DE ENTORNO PREVIO

- **Identificación de la IP usada por el servicio dispuesto para el laboratorio.**

  Se utiliza para esto el comando **ifconfig** según lo mostrado en la **Figura 1** el cual arroja como resultado que la IP asignada a la interfaz enp0s3 es 192.168.1.5

Figura 1. Ejecución comando ifconfig

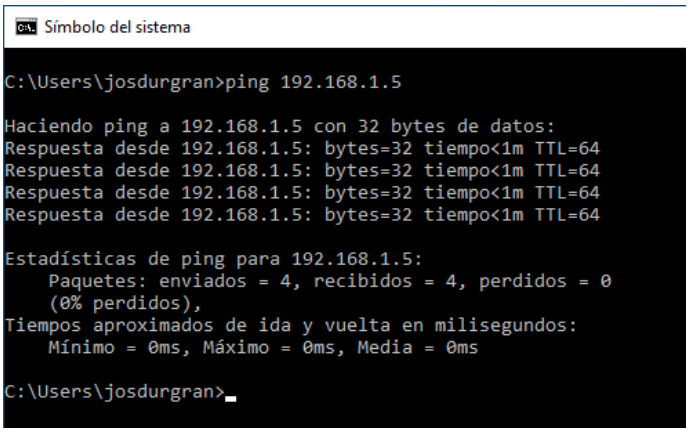


Fuente: Propia del autor

- Verificación de respuesta a ping.

Se utiliza para esto el comando **ping** desde una terminal del equipo cliente tal como se muestra en la **Figura 2** evidenciando que se tiene respuesta.

Figura 2. Ejecución de comando ping desde la terminal cliente.

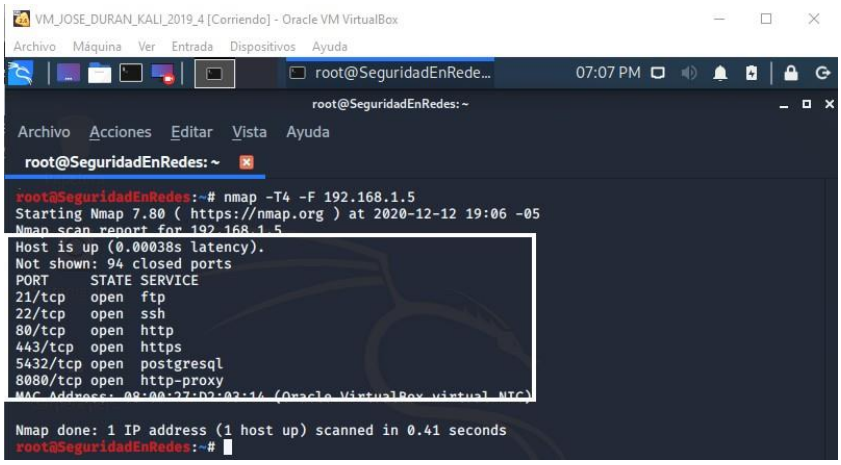


Fuente: Propia del autor

- Ejecución de escaneo de puertos para identificar los puertos disponibles y posibles servicios asociados.

Para esto se hace uso de la herramienta NMAP desde un host Kali Linux al cual se le fija como objetivo la IP 192.168.1.5 identificada en el "Paso 1", buscando captar información referente a la red del servicio.

Figura 3. Escaneo de puertos con NMAP



Fuente: Propia del autor

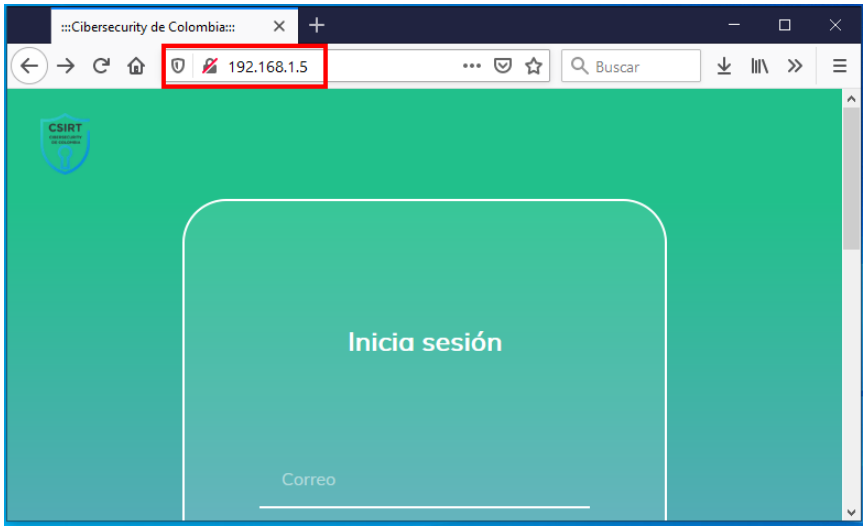
De acuerdo al escaneo de puertos se visualiza que los servicios y sus puertos asociados están disponibles públicamente lo cual representa riesgos de seguridad importantes principalmente en servicios de base de datos puerto 5432 y Apache Tomcat 8080, debido a que éste interactúa y procesa datos sumado ésto se visualizan los servicios SSH y FTP como se muestra en la Figura 3.

3.2. LABORATORIO

Configuración de https al servicio Web Apache

- Se verifica a través del navegador web desde el equipo cliente la dirección 192.168.1.5 obteniendo el siguiente resultado en el que se resalta de color rojo que el servicio responde por http puerto 80.

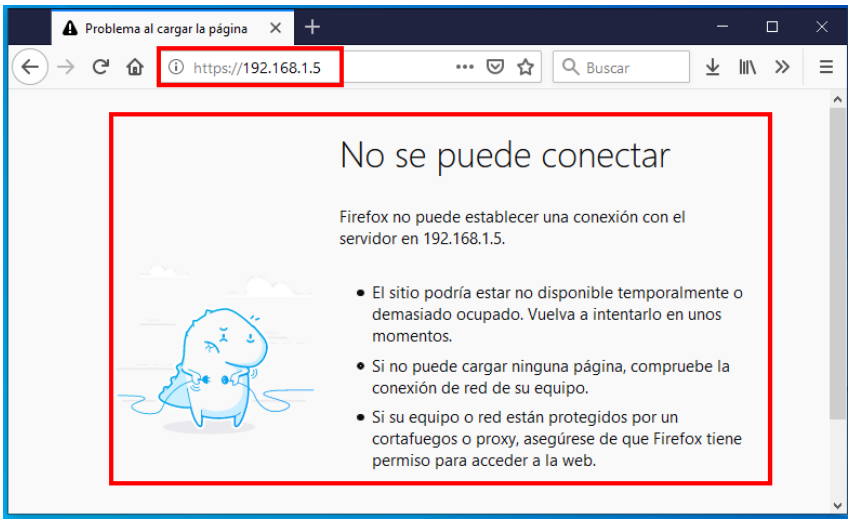
Figura 4. Se verifica que el servicio Web responde por http puerto 80



Fuente: Propia del autor

- Luego se procede a verificar la dirección 192.168.1.5 pero esta vez por https obteniendo como resultado que no se encuentra configurado el servicio por el puerto 433 según se muestra a continuación; se resaltan en rojo la URL y el error correspondiente.

Figura 5. Se verifica que el servicio Web no responde al protocolo https puerto 443



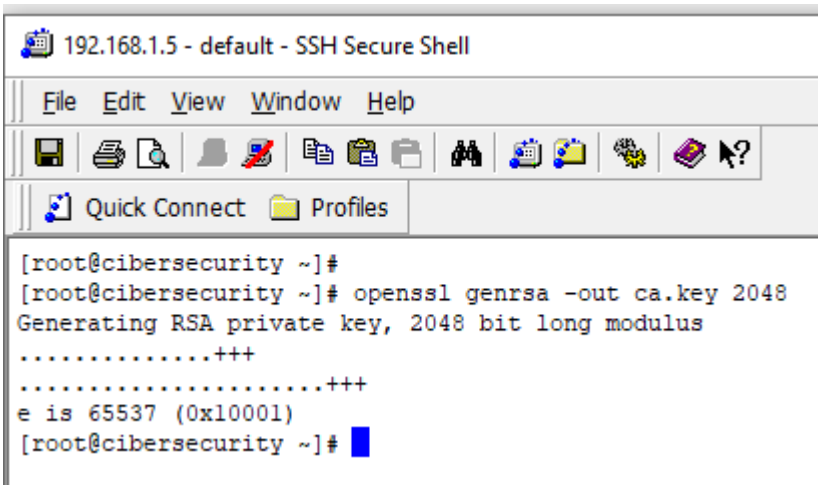
Fuente: Propia del autor

- Seguidamente se inicia con el procedimiento de configuración del certificado SSL al servicio Apache Web Server

  - Crear el certificado SSL

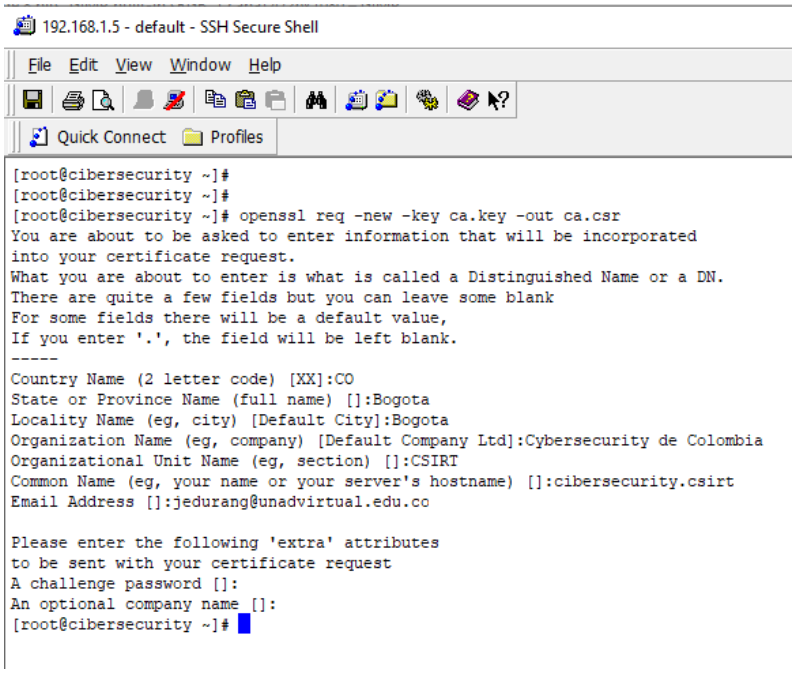
  Se debe crear un par de claves (Pública y privada) y certificado auto firmado usando el comando **OpenSSL**; en este caso se configurará para 365 días de valides y longitud de 2048 bites de la siguiente forma:

Figura 6 Generar llave privada con el comando "openssl genrsa -out ca.key 2048"



Fuente: Propia del autor

Figura 7 Generar el CSR (Solicitud de firma de certificado) con el comando "openssl req -new -key ca.key -out ca.csr"

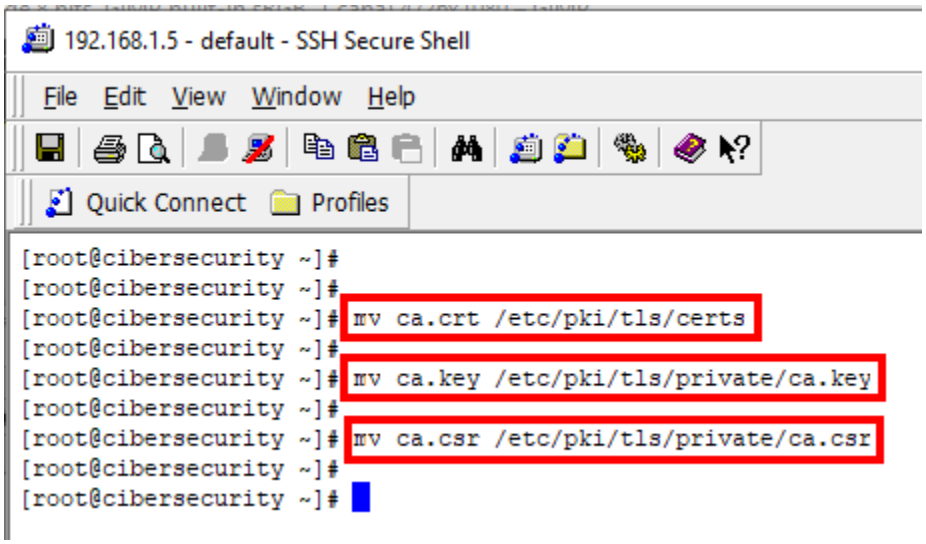


Fuente: Propia del autor

Figura 8 Generar la llave auto firmada con el comando "openssl x509 -req -days 365 -in ca.csr -signkey ca.key -out ca.crt"

Fuente: Propia del autor

Figura 9. Ubicar los archivos en la ruta correcta.



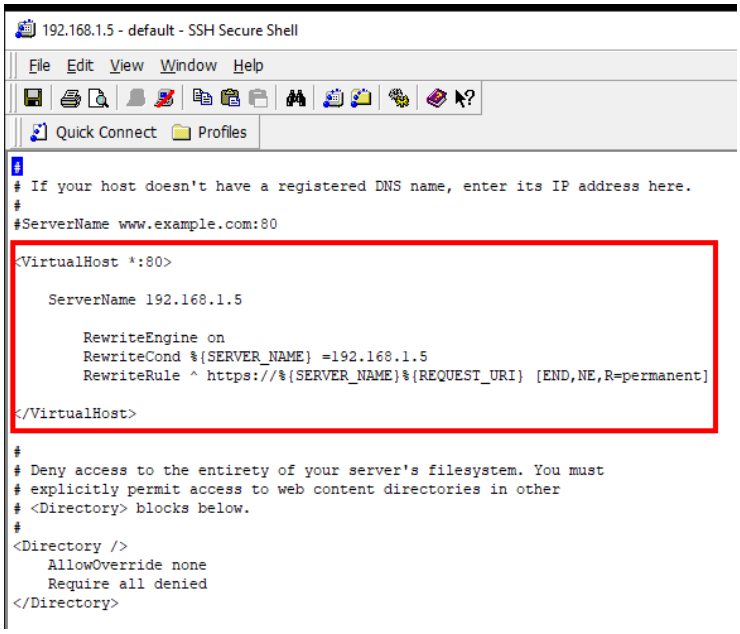
Fuente: Propia del autor

- Implementar certificado SSL en el servicio Apache Web server.

  Se configura una redirección automática desde el host virtual por defecto http establecido en el puerto 80 hacia el virtualhost por defecto para https por el puerto 443 para garantizar que siempre se acceda por https mantener disponibles los dos servicios, facilitar la implementación y no causar traumatismos a los usuarios finales de Cybersecurity de la siguiente forma:

  Inicialmente se debe editar el archivo /etc/httpd/conf/httpd.conf, para configurar la redirección desde el virtualhost puerto 80 hacia el virtualhost puerto 443 colocando la etiquetas señaladas en rojo después de la etiqueta "#ServerName www.example.com:80".

Figura 85. Configuración virtualhost puerto 80

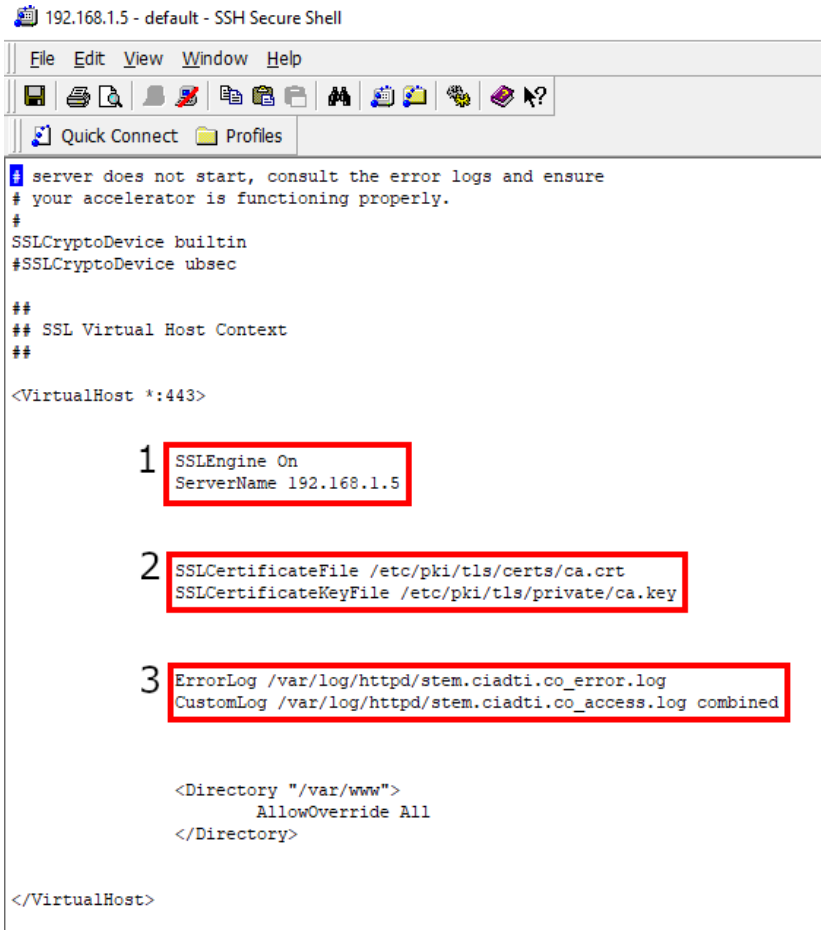


Fuente: Propia del autor

Nota: La IP 192.168.1.5, se debe cambiar ya sea por la IP que corresponda en los servicios de producción de Cybersecurity o el dominio establecido para este.

Luego de esto se debe editar el archivo /etc/httpd/conf.d/ssl.conf, para configurar el certificado SSL para lo que se debe adicionar un nuevo virtualhost por puerto 443 colocando las etiquetas señaladas en rojo después de la línea "**## SSL Virtual Host Context**".

Figura 86. Configuración virtualhost puerto 443



Fuente: Propia del autor

Nota:

1 **SSLEnggine On:** Corresponde a la activación de SSL

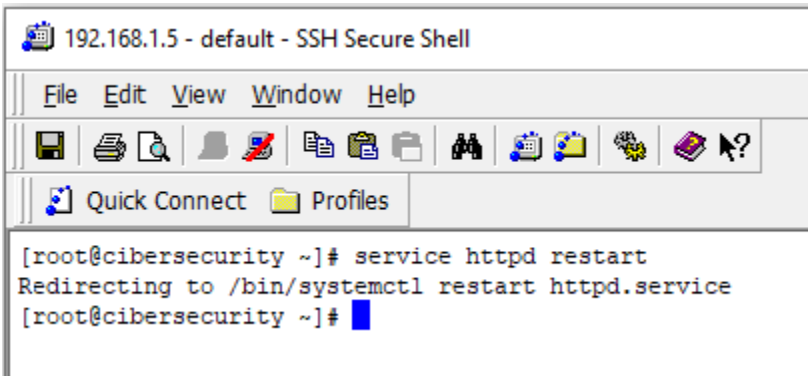
ServerName: Dirección IP del servicio, se debe cambiar ya sea por la IP que corresponda en los servicios de producción de Cybersecurity o el dominio establecido.

2 En este bloque se establece la configuración de los certificados SSL

3 Se configuran los logs tanto de acceso y actividad como los de errores.

Finalmente se debe reiniciar el servicio httpd para que se tomen los cambios.

Figura 12. Reinicio del servicio httpd con el comando "service httpd restart"

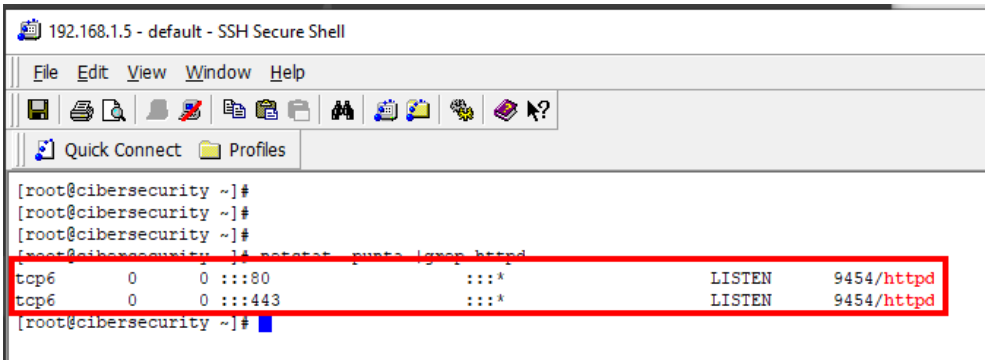


Fuente: Propia del autor

Prueba operación del https en el servicio web Apache

- Verificar qué puertos asociados al servicio httpd están en modo escucha.

Figura 13. Ver Puerto en escucha asociados al servicio httpd con el comando " netstat -punta |grep httpd"

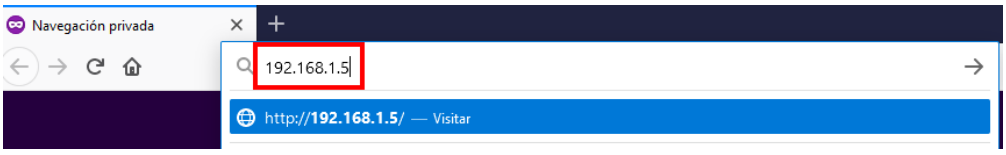


Fuente: Propia del autor

Tal como se muestra en la Figura 13, httpd en este punto está escuchando peticiones por los puertos 80 y 443 lo que hace que se cumpla el propósito inicial.

➢ Verificar por medio del navegador web el funcionamiento de la redirección y el certificado.

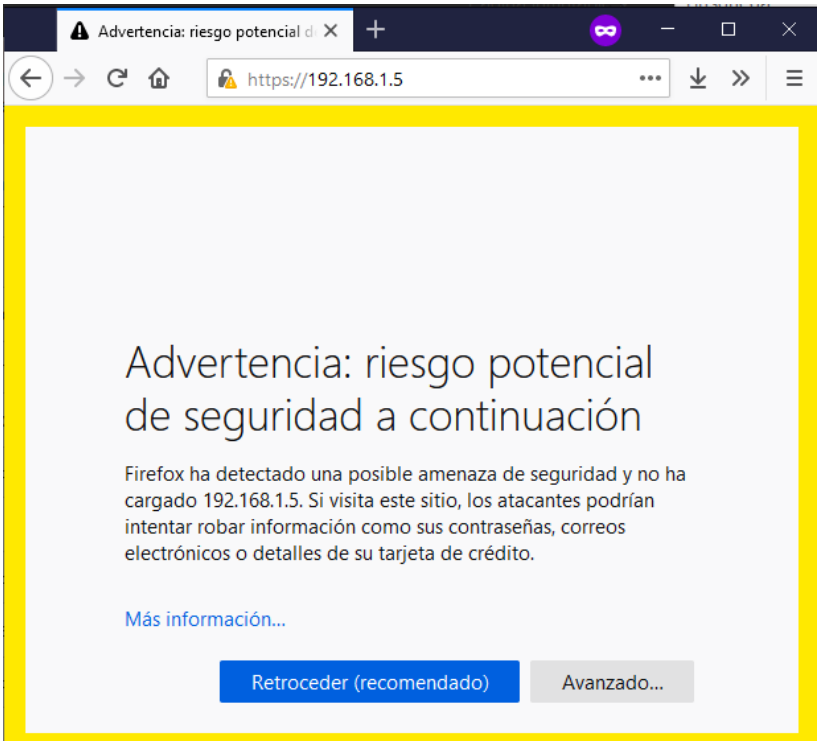
Figura 14. Se ingresa la dirección en el navegador Web 192.168.1.5



Fuente: Propia del autor

Nota: Al digitar la dirección sin especificar https el navegador Web por defecto envía la petición por http puerto 80.

Figura 15. Redirección automática desde el servidor Web a https puerto 443



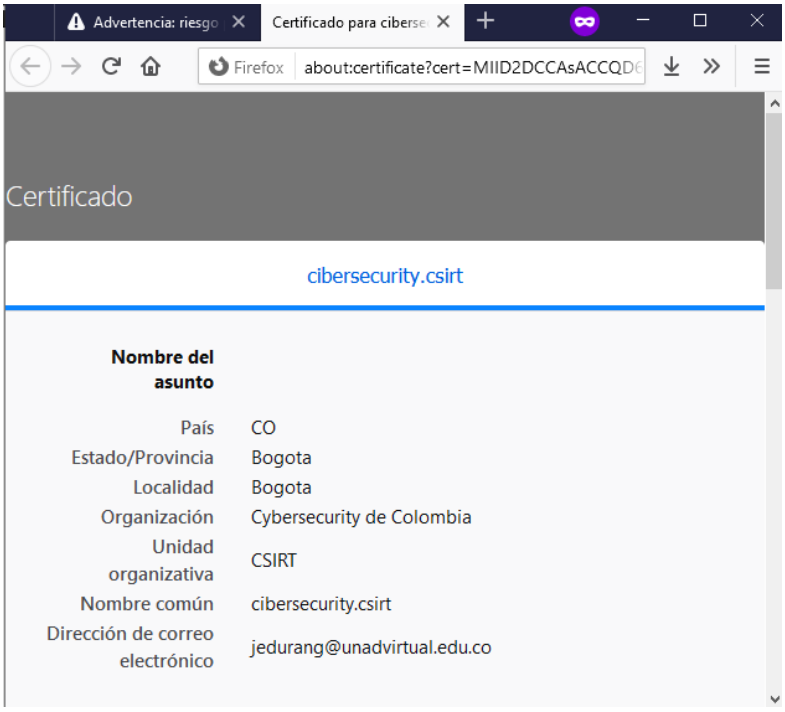
Fuente: Propia del autor

Nota: Se puede comprobar así que la redirección está funcionando, la advertencia de riesgo corresponde a que el certificado SSL asociado al servicio no proviene de una entidad certificadora reconocida por el navegador Web.

✓ Revisar que el certificado que está tomando el servicio corresponda con el generado.

En la escena presentada en la **Figura 15**, se debe ingresar al botón "Avanzado..." y luego "Ver certificado".

Figura 16. Visualización de detalles del certificado SSL

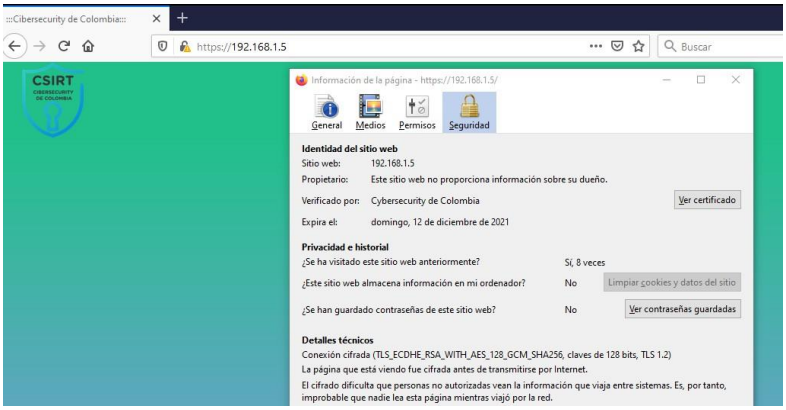


Fuente: Propia del autor

Nota: Se visualizan los datos del certificado que se generó anteriormente.

✓ Verificación final del funcionamiento del certificado SSL en el navegador Web

Figura 17. Funcionamiento y detalles del certificado SSL en el frontend en los sistemas de Cybersecurity



Fuente: Propia del autor

Configuración de Apache Tomcat

- Se verifica a través del navegador web desde el equipo cliente la dirección 192.168.1.5:8080

Se obtiene como resultado que el servicio responde y además proporciona información sensible en su página por defecto como la versión del servidor, además de algunos botones que dirigen a servicios de Apache Tomcat que no se usan y que probablemente generan vulnerabilidades que algún atacante pueda explotar.

Figura 18. Respuesta publica servidor Apache Tomcat

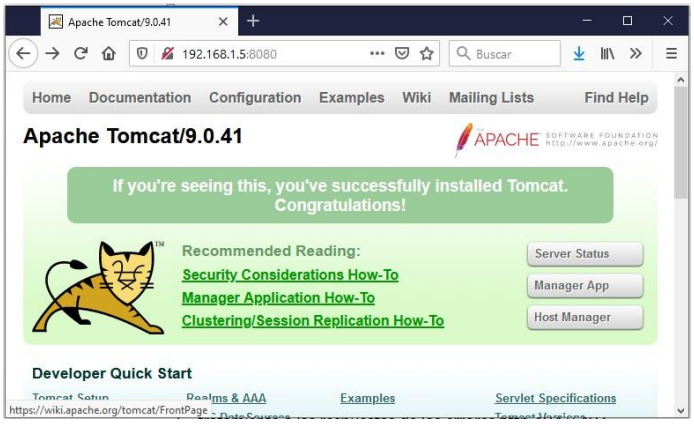
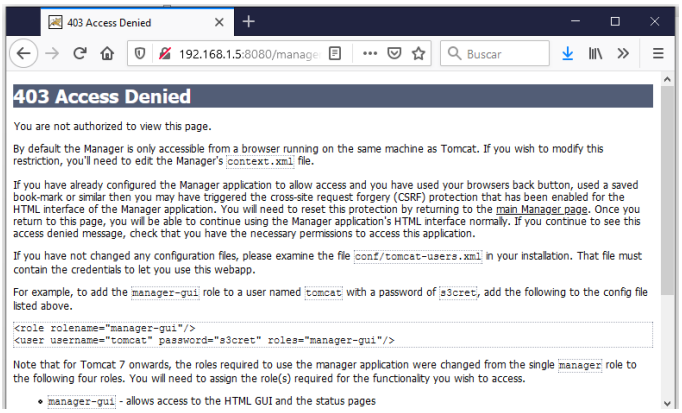


Figura 19. Error no controlado 403 Apache Tomcat



Fuente: Propia del autor

Figura 20. Error no controlado 404 Apache Tomcat

Fuente: Propia del autor

Con esto en mente el CSIRT propone que se retire la publicación del servicio Apache Tomcat del entorno público, que se dé control a través de firewall lógico, el cual se tratará en un aparte exclusivo del presente laboratorio y se de tratamiento a las respuestas de los errores http 404 y 403 para ocultar la información de versionado del servicio.

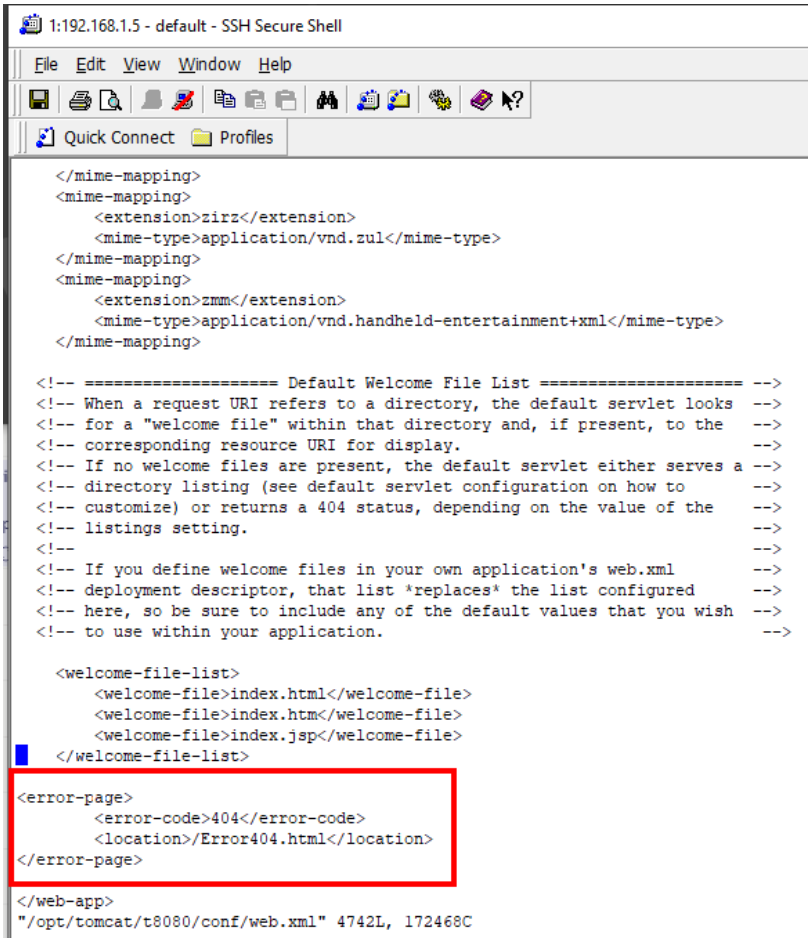
✓ Tratamiento a las respuestas de los errores http 404 y 403

Se debe realizar la edición del fichero $CATALINA_HOME/conf/web.xml que es el descriptor de

implementación estándar de Apache Tomcat donde se controlan de forma general los parámetros de despliegue de los contextos Tomcat

Para controlar el error 404 se debe adicionar el contenido resaltado de color rojo antes de la etiqueta "</web-app>" del fichero $CATALINA_HOME/conf/web.xml

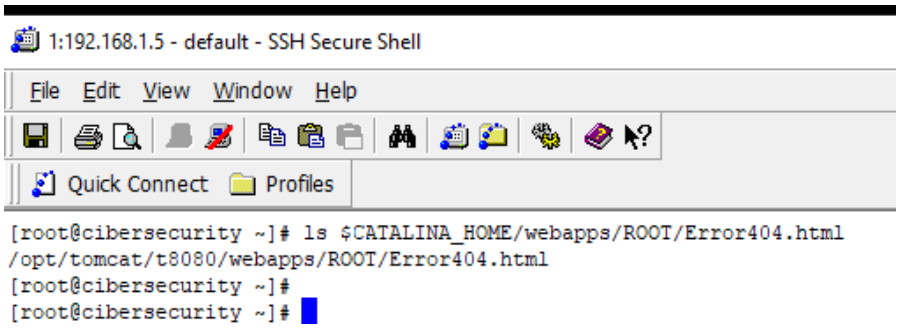
Figura 21. Etiquetas para controlar el error http 404



Fuente: Propia del autor

Posteriormente se debe ubicar en la carpeta raíz de los contextos Tomcat el fichero $CATALINA_HOME/webapps/ROOT/Error404.html que será el que se muestre cuando ocurra este error.

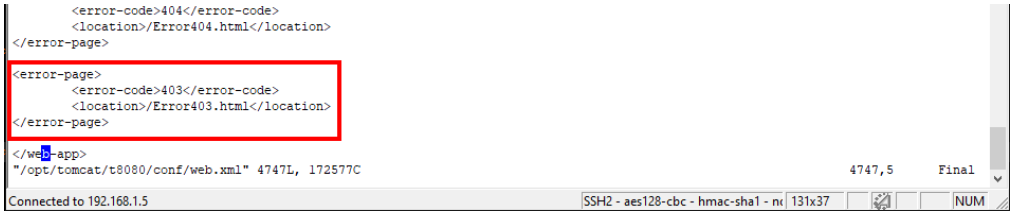
Figura 22. Página por defecto error http 404



Fuente: Propia del autor

Para controlar el error 403 se debe adicionar el contenido resaltado de color rojo antes de la etiqueta "</web-app>" del fichero $CATALINA_HOME/conf/web.xml

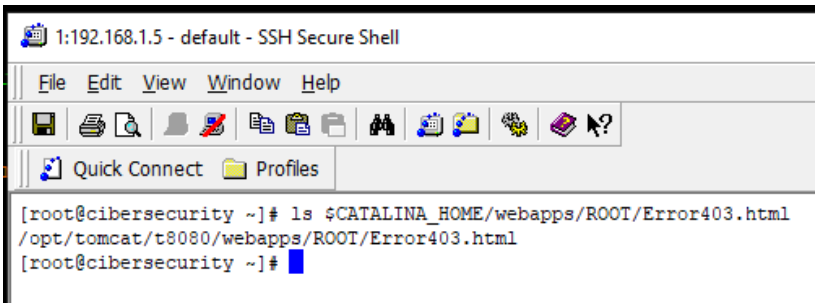
Figura 23. Etiquetas para controlar el error http 403



Fuente: Propia del autor

Ubicar en la carpeta raíz de los contextos Tomcat el fichero $CATALINA_HOME/webapps/ROOT/Error403.html que será el que se muestre cuando ocurra este error.

Figura 24. Página por defecto error http 40



Fuente: Propia del autor

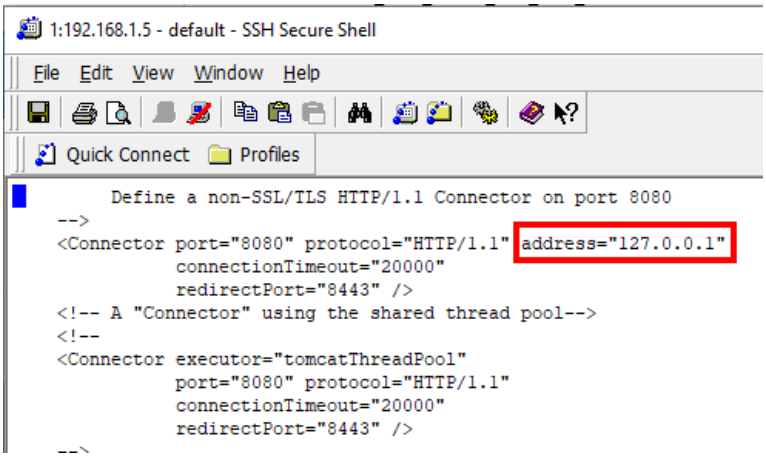
Nota: En caso de tener más contextos dentro de Tomcat se debe realizar este proceso para cada uno.

✓ Retirar el servicio Apache Tomcat del entorno público

Teniendo en cuenta que este es un servicio crítico debido a su naturaleza de gestión y procesamiento de datos y la correspondiente conexión directa con la base de datos el CSRIT recomienda que éste sea aislado del entorno público y que su acceso sea controlado.

Para ello se debe adicionar el contenido resaltado de color rojo en la etiqueta "**Connector**" del fichero $CATALINA_HOME/conf/server.xml

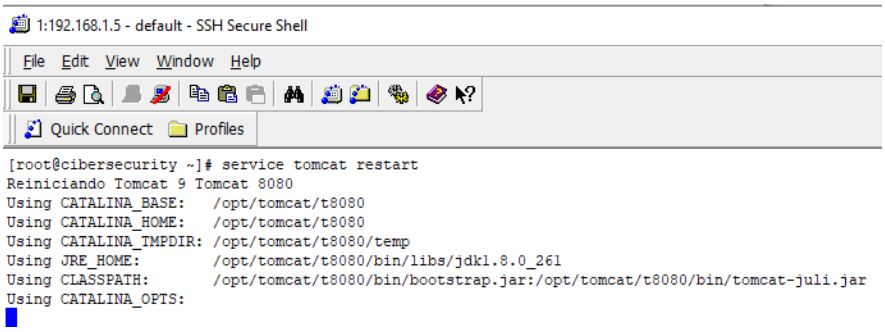
Figura 25. Configuración para limitar el acceso a localhost del servicio Tomcat



Fuente: Propia del autor

Finalmente se debe reiniciar el servicio Tomcat para que se tomen los cambios.

Figura 26. Reinicio del servicio tomcat con el comando "service tomcat restart"

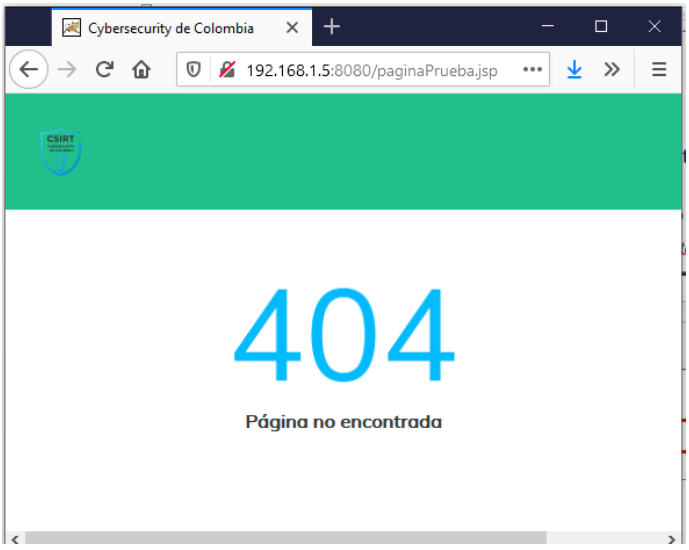


Fuente: Propia del autor

Prueba de las operaciones realizadas al servicio Tomcat

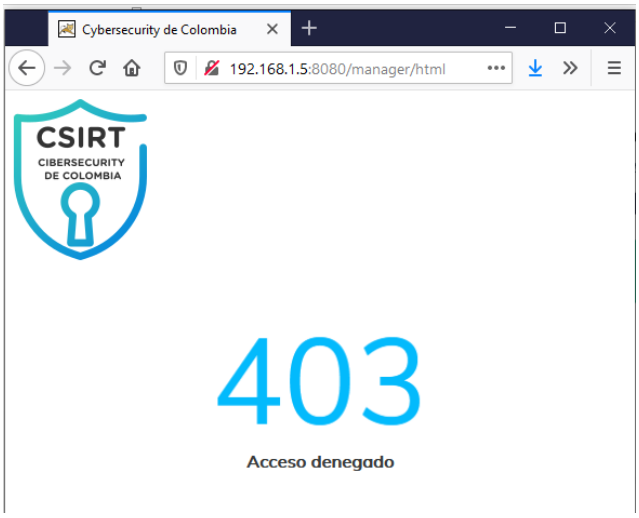
- Verificar el control de los errores http 403 y 404

Figura 27. Prueba de implementación de página de control de error http 404



Fuente: Propia del autor

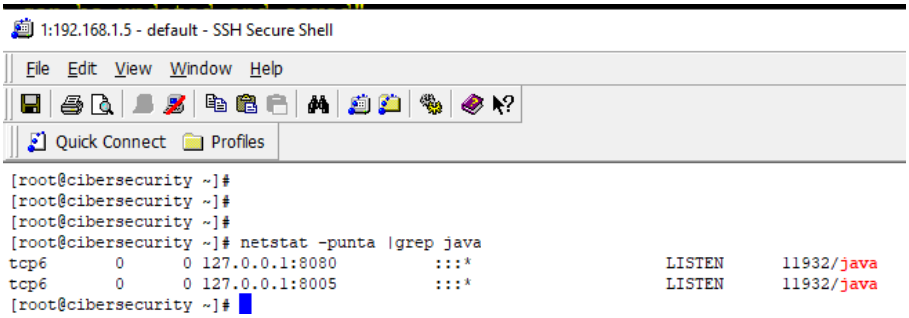
Figura 28. Prueba de implementación de página de control de error http 403



Fuente: Propia del autor

- Consulta a través de la consola de comandos el estado del servicio Tomcat

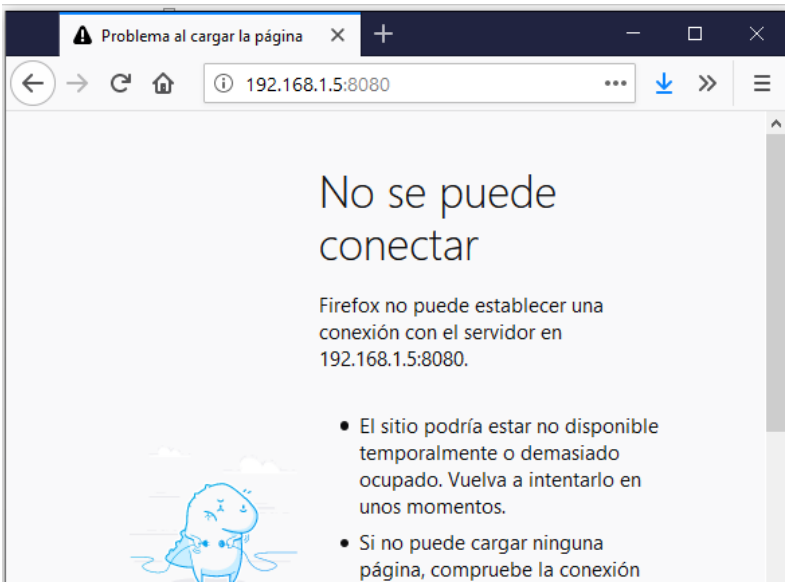
Figura 29. Verificación del estado de los servicios Java asociados tomcar por medio del comando "netstat -punta |grep java"



Fuente: Propia del autor

- Ingreso desde el navegador Web a la dirección 192.168.1.5:8080 la cual corresponde al servicio Apache Tomcat

Figura 30. Verificación del servicio Tomcat desde el navegador Web



Fuente: Propia del autor

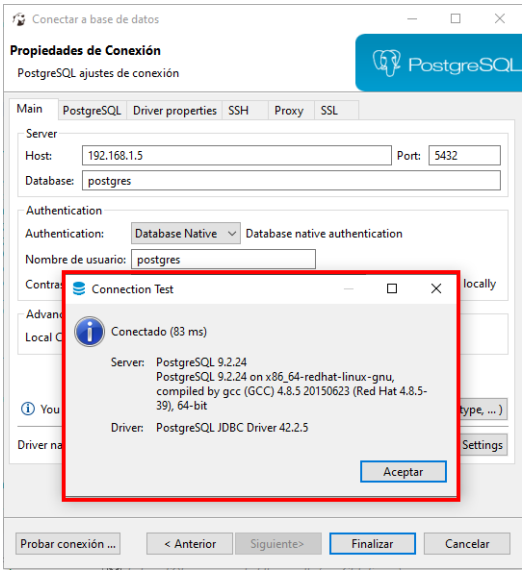
Según lo evidenciado anteriormente se logran objetivos proyectados por el CSIRT en referencia al servicio Tomcat; Controlar los errores http 404 y 403 y aislar el servicio Tomcat del entorno público.

Configuración de PostgreSQL

- **Se verifica a través de un cliente de base de datos la conexión al host 192.168.1.5 por el puerto 5432 y el usuario postgres.**

Se obtiene como resultado conexión exitosa a la base de datos desde el cliente lo que representa un fuerte problema de seguridad teniendo en cuenta que cualquier host puede establecer conexión desde la red de la empresa.

Figura 31. Respuesta pública servidor de base de datos postgresql



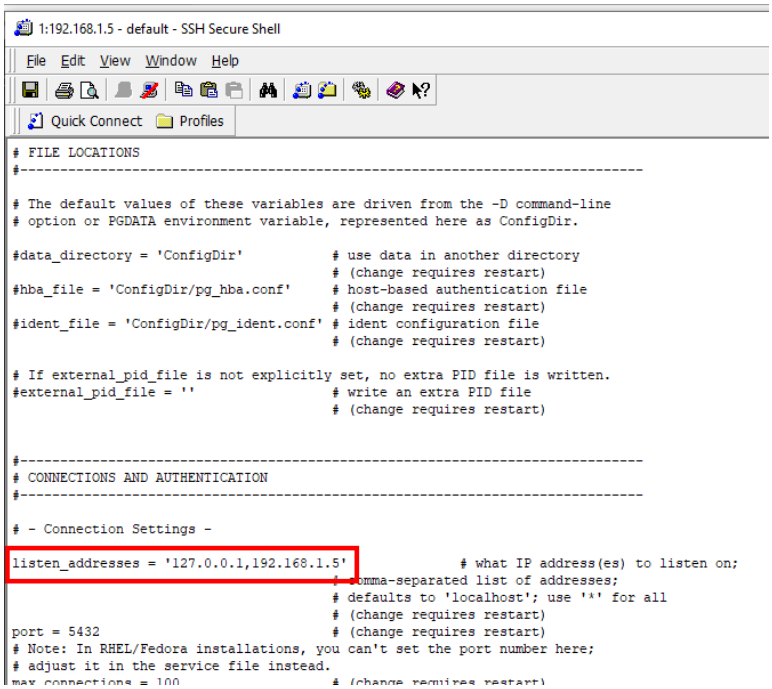
Fuente: Propia del autor

✓ Configurar postgreSQL para que opere únicamente desde las IP de servicio que los administradores autoricen.

Para efectos del laboratorio se permitirán las IP de servicio del servidor 192.168.1.5 para poder dar acceso a los host que requieran acceso en red a la base de datos y localhost para la conexión con el backend.

Para ello se debe establecer la configuración cómo se resalta en color rojo en el fichero $PGDATA/postgresql.conf usando el usuario postgres del sistema operativo, en la siguiente figura se evidencian:

Figura 32. Control de IPs del servicio



Fuente: Propia del autor

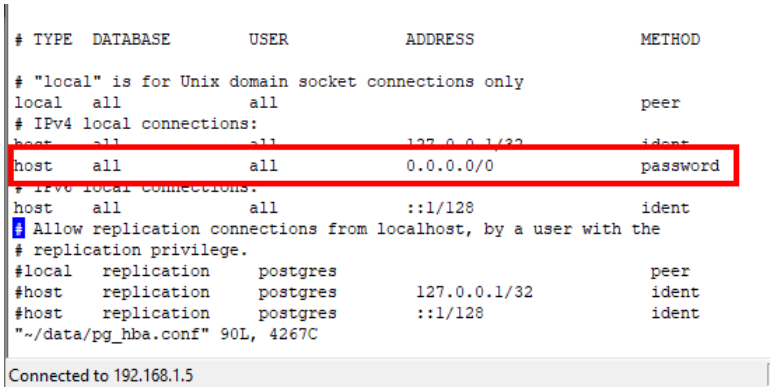
✓ Restringir lógicamente el acceso a postgreSQL para los host que lo requieran.

Para efectos del laboratorio se permitirá el acceso a la IP 192.168.1.6 correspondiente al cliente a autorizar el acceso.

Se debe establecer la configuración en el fichero $PGDATA/pg_hba.conf con el usuario postgres del sistema operativo de la siguiente forma.

Retirar la línea que se señala en color rojo.

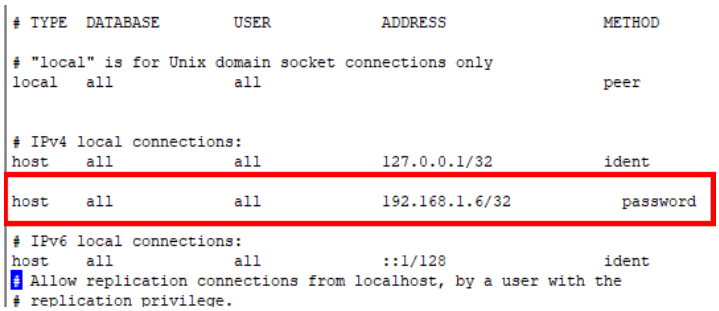
Figura 33. Retirar configuración incorrecta de acceso a postgresql



Fuente: Propia del autor

Autoriza el acceso a la IP 192.168.1.6 correspondiente al usuario de Cybersecurity que realiza consultas y modificaciones a la base de datos.

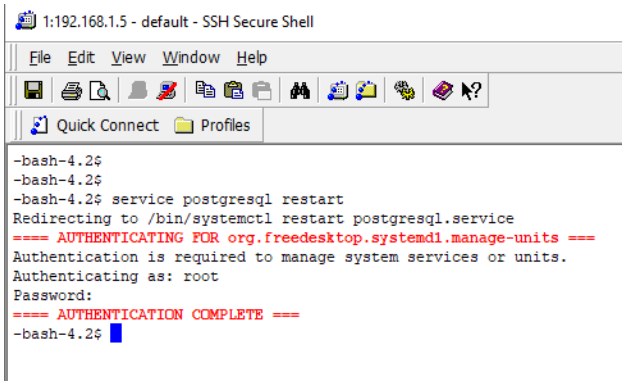
Figura 34. Autorización de acceso lógico a la IP 192.168.1.6



Fuente: Propia del autor

Finalmente se reinicia el servicio postgreSQL

Figura 35. Reinicio PostgreSQL

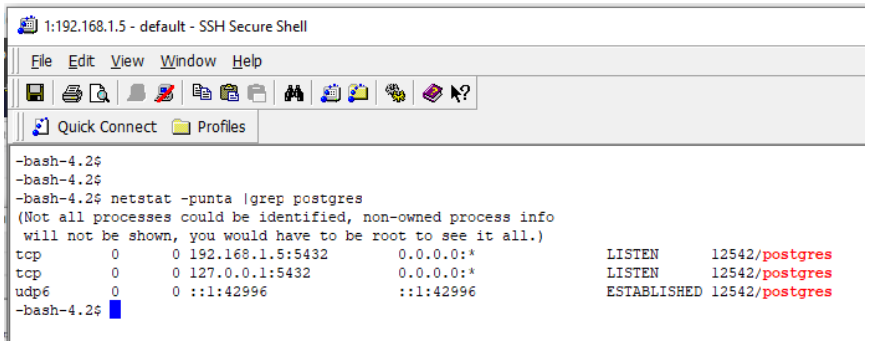


Fuente: Propia del autor

Prueba de las operaciones realizadas al servicio PostgreSQL

- Consulta a través de la consola de comandos el estado del servicio PostgreSQL

Figura 36. Verificación del estado del servicio PosgreSQL por medio del comando "netstat -punta |grep postgres"

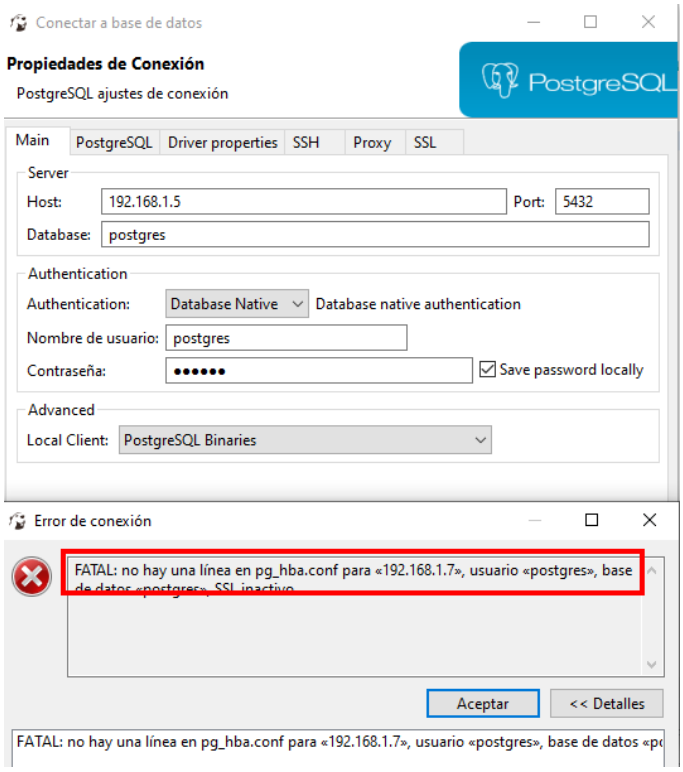


Fuente: Propia del autor

En la Figura 36, se evidencia que el servicio está escuchando por las IP 192.168.1.5 y por la IP 127.0.0.1 tal como se requiere por el equipo de sistemas de Cybersecurity de Colombia.

➢ Restricción lógica de acceso solo por la IP 192.168.1.6 para la prueba correspondiente se intentara el acceso desde la IP 192.168.1.7

Figura 37. Verificación de intento de acceso desde una IP diferente a las autorizadas



Fuente: Propia del autor

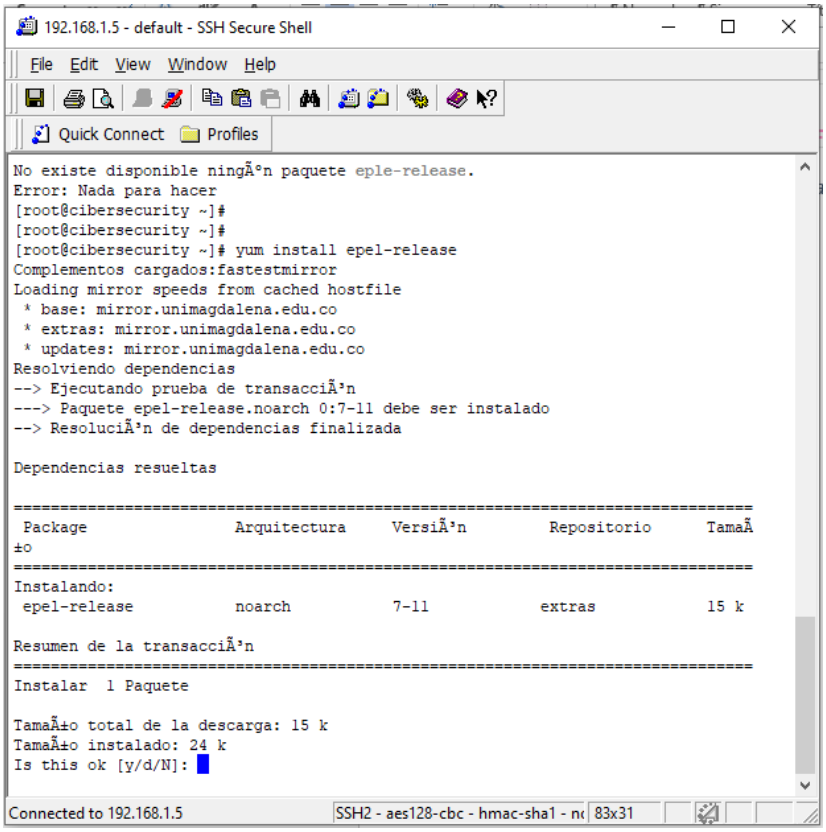
En el bloque resaltado de color rojo se muestra que a pesar qué el intento de conexión se realiza con las credenciales correctas el servidor restringe el acceso solo a las IPs autorizadas.

Instalación y configuración de Suricata IDS

➢ Proceso de instalación del IDS Suricata.

Instalar el repositorio "**epel-release**" necesario para poder tener acceso a las dependencias demandadas por la herramienta.

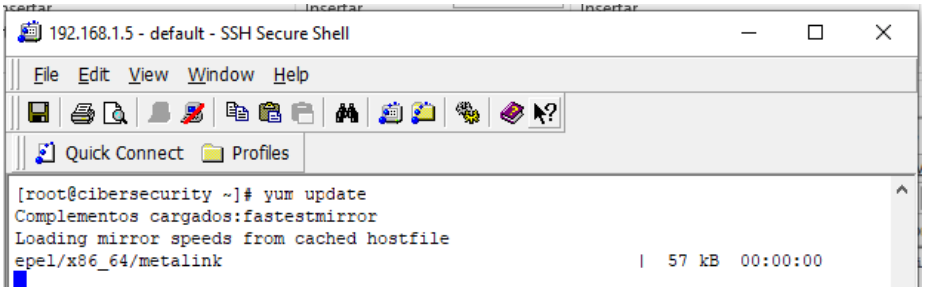
Figura 38. Instalación de repositorio epel-release con el comando "yum install epel-release".



Fuente: Propia del autor

Actualizar la lista de repositorios para que el sistema tome los datos de repositorio "**epel-release**"

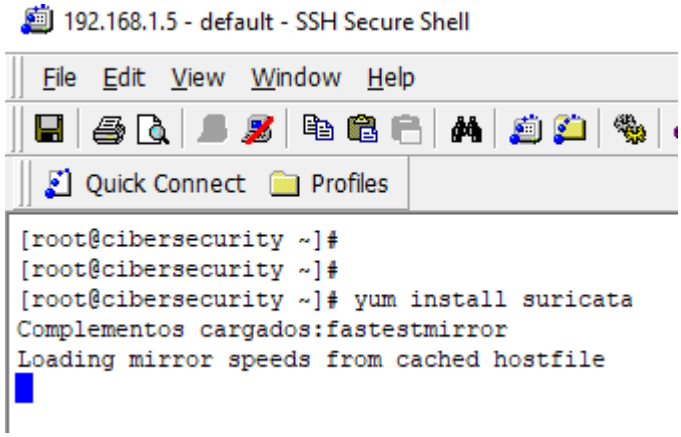
Figura 39. Actualizacion de los repositorios con el comando "yum update"



Fuente: Propia del autor

Instalar la herramienta "**Suricata IDS/IPS/NSM**" por medio del comando "**yum**" del sistema operativo.

Figura 40. Instalación de "Suricata IDS/IPS/NSM" por medio del comando "yum install suricata"

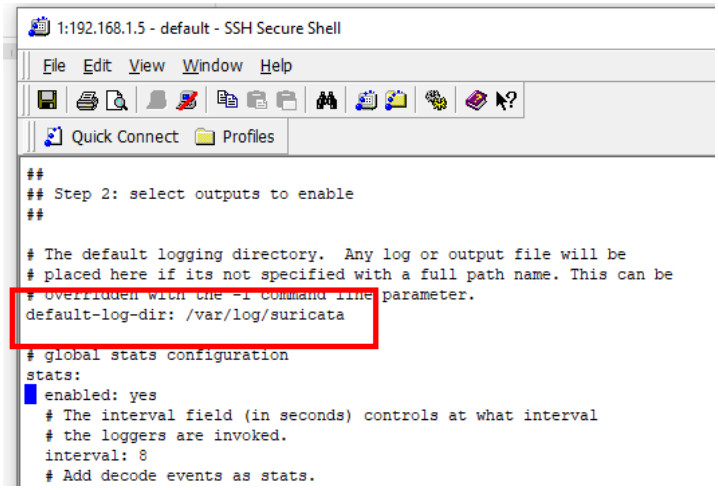


Fuente: Propia del autor

La configuración de "**Suricata IDS/IPS/NSM**", se realiza en el archivo "**/etc/suricata/suricata.yaml**" la cual se muesta a continuación.

Se inicia con la definición de la ubicación por defecto donde se almacenaran los informes por defecto están definidos en la ruta "**/var/log/suricata/**", para efectos del laboratorio se mantendrá esta configuración pero puede ser modificada de acuerdo a la necesidad que se tenga.

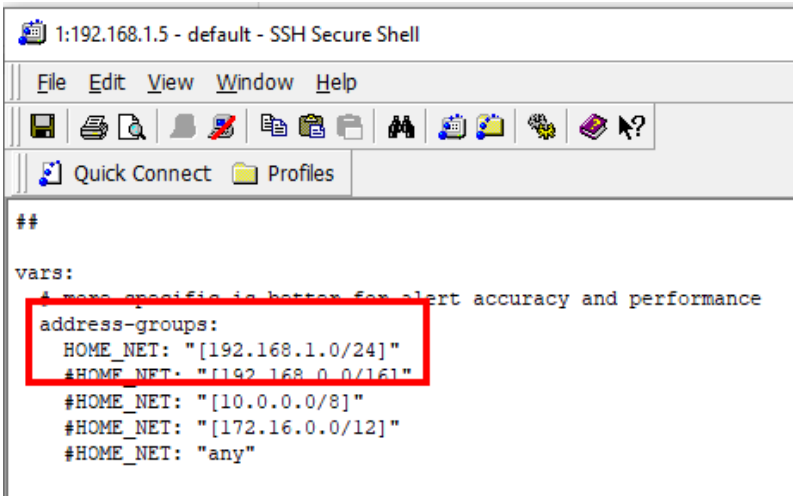
Figura 41. Configuración por defecto de la ubicación de los archivos de informes y registros de Suricata



Fuente: Propia del autor

Luego se configura la red o redes que se desea que suricata escanee en este caso será la red "192.168.1.0/24" a la cual pertenece el servidor de sistemas de Cybersecurity de Colombia; tal como se resalta en color rojo.

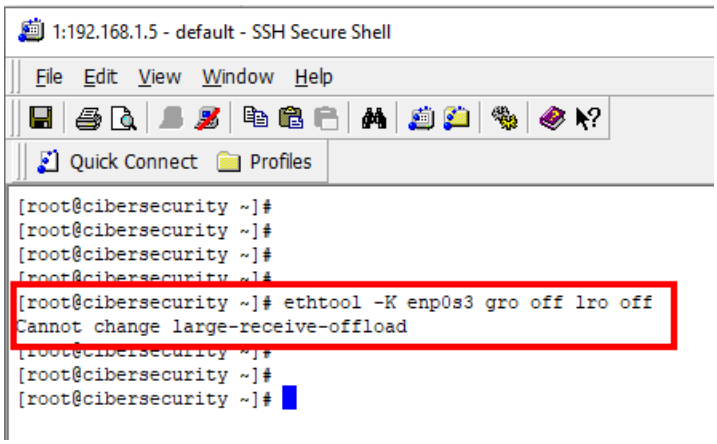
Figura 42. Configuracion de las redes a escanear



Fuente: Propia del autor

Se deben desactivar las funciones que hacen offload de paquetes, debido a que estas pueden causar interferencias con los procesos de detección de "**Suricata IDS/IPS/NSM**" sobre la tarjeta de red del sistema a monitorear en este caso "**enp0s3**"; tal como se resalta en color rojo.

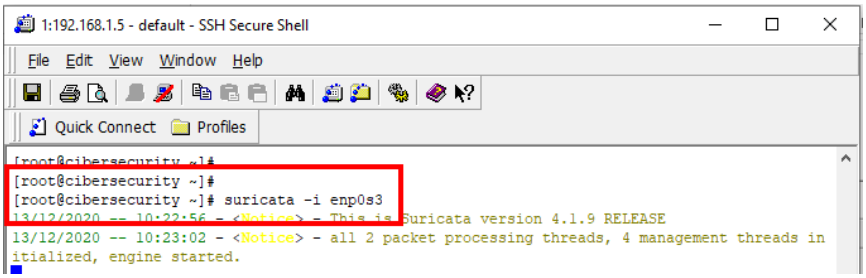
Figura 43. Desactivar funciones que hacer offload de paquetes



Fuente: Propia del autor

Se inicia el servicio "**Suricata IDS/IPS/NSM**" sobre la tarjeta de red del sistema a monitorear en este caso "**enp0s3**"

Figura 44. Inicio del servicio suricata con el comando "suricata -i enp0s3"

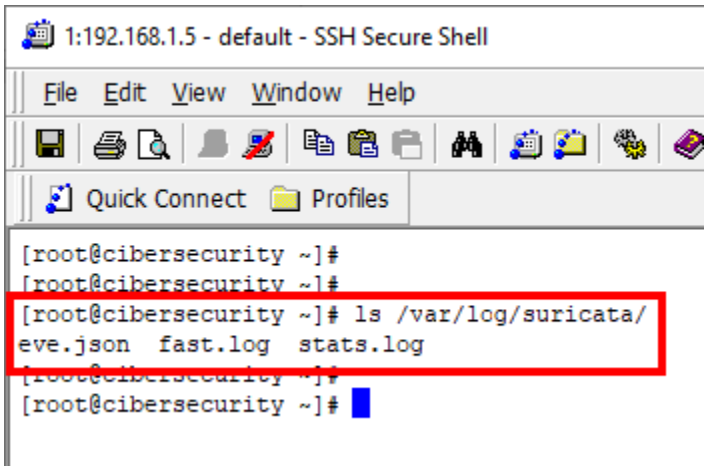


Fuente: Propia del autor

Prueba de funcionamiento de "Suricata IDS/IPS/NSM"

- Verificar que Suricata género y escribe los archivos de informes en la ruta definida "/var/log/suricata/".

Figura 45. Verificación de ficheros de informes de Suricata

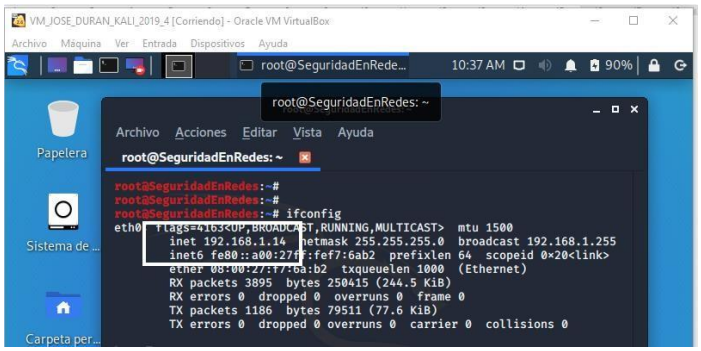


Fuente: Propia del autor

- Verificar realizando un escaneo de puertos desde una terminal remota para verificar el funcionamiento de Suricata.

  Identificar la IP de la terminal remota Kali Linux; la cual se señala en color blanco.

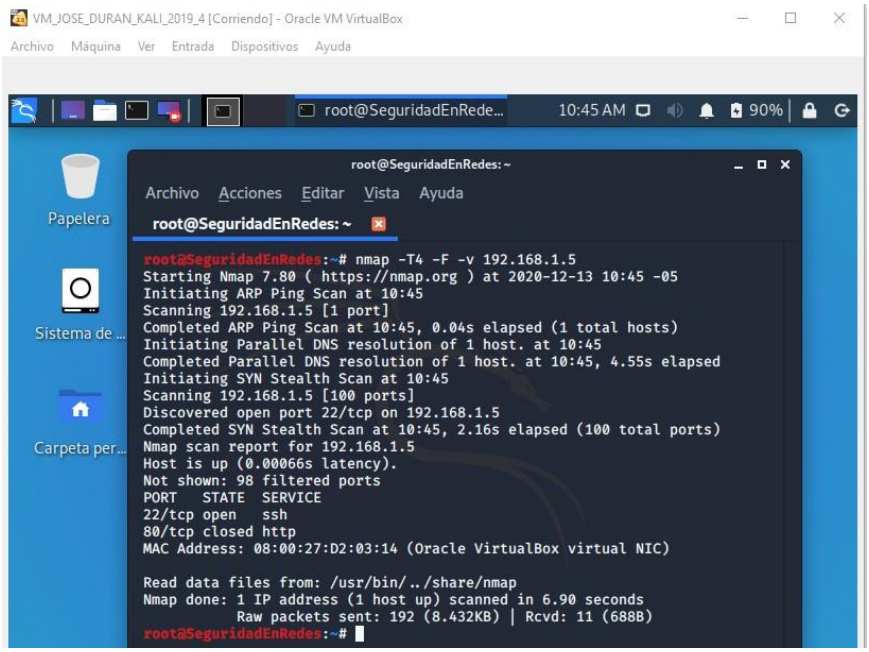
Figura 46. Verificación de la IP de la terminal Kali Linux



Fuente: Propia del autor

Desde una terminar Kali Linux con IP 192.168.1.14, se realiza un escaneo a la IP 192.168.1.5.

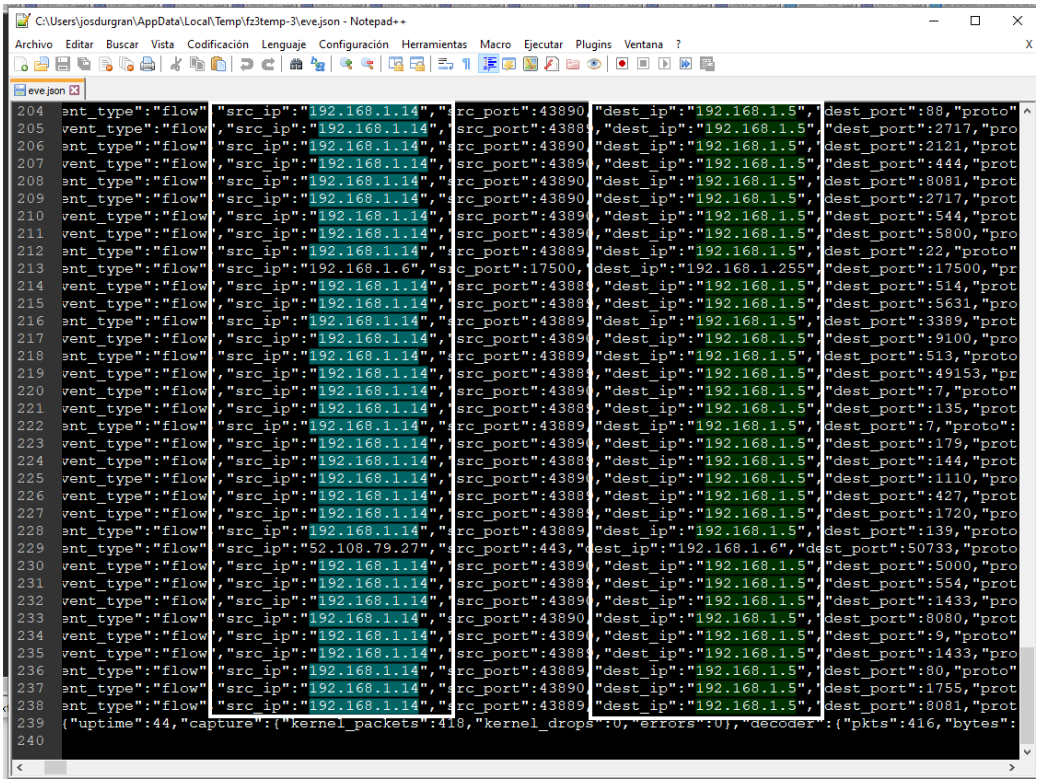
Figura 47. Escaneo de puerto a la IP 192.168.1.5 con el comando NMAP



Fuente: Propia del autor

Revisión de fichero de registro **"eve.json"** e identificación del procedimiento de escaneo de puertos.

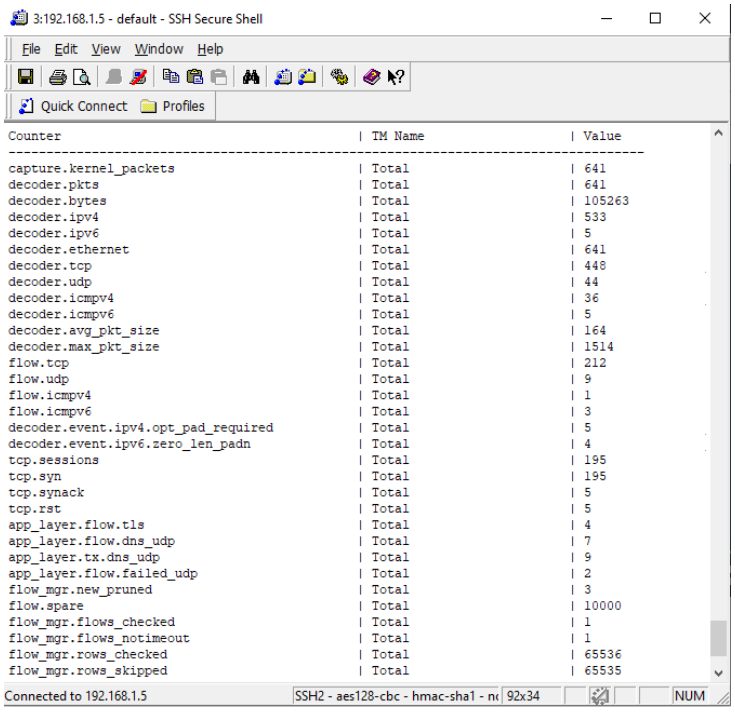
Figura 48. Identificación de registro de Suricata en los ficheros de informes



Fuente: Propia del autor

Revisión de fichero de registro de estadísticas "stats.log" para evidenciar de forma más resumida el tráfico presente en la red.

Figura 49. Registro de estadísticas de Suricata



Fuente: Propia del autor

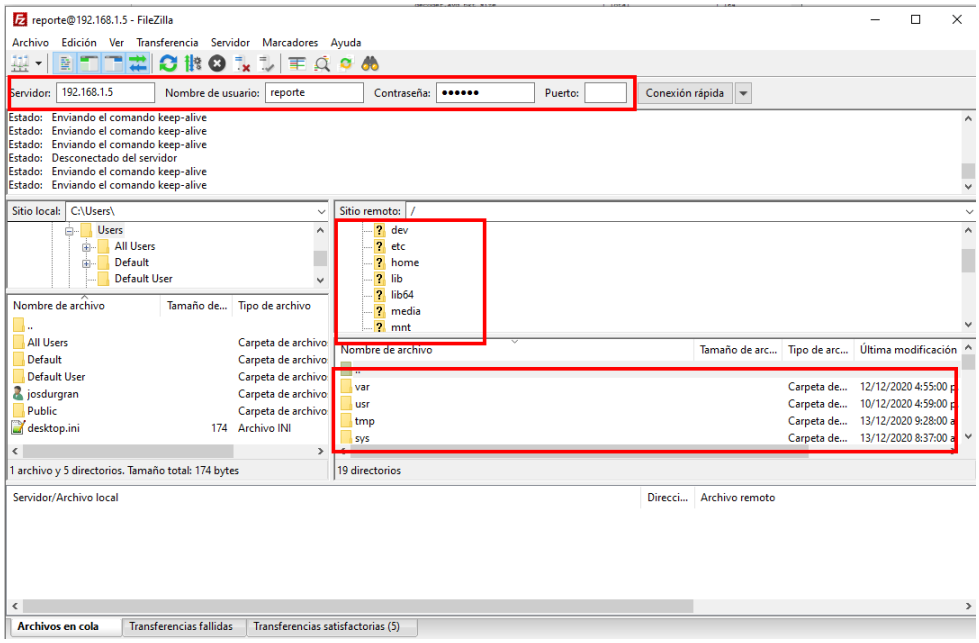
Se evidencia de esta forma que el proceso de implementación de Suricata cumple con el propósito de llevar a cabo el registro y seguimiento en la red en Cybersecurity de Colombia Ltda, con el fin de detectar posible tráfico malicioso.

Configuración de servicio FTP

- **Verificación condición de acceso al servicio ftp**

Se realiza conexión al servidor ftp y se evidencia que el usuario “reporte”, cuenta con acceso al servicio, pero que éste a su vez puede ver otras carpetas del sistema, lo cual representa una vulnerabilidad muy fuerte.

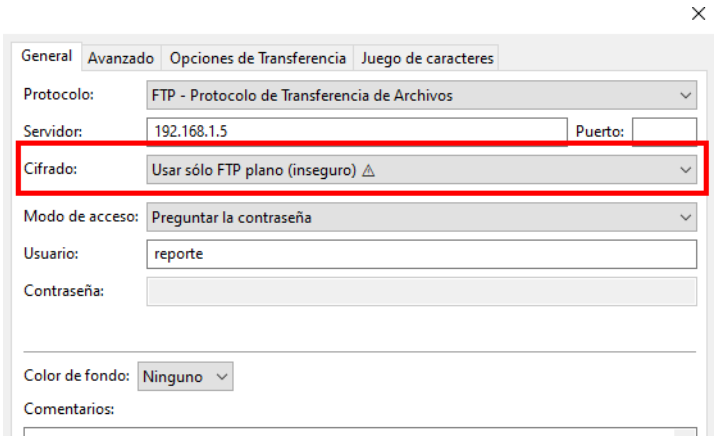
Figura 50. Se evidencia que los usuarios FTP, tienen exeso de privilegios en el servicio.



Fuente: Propia del autor

Por otra parte se encuentra que el servicio no se encuentra cifrado por lo que las trasferencias de información se realizan de forma plana por lo que pueden ser vistas a través de la red en caso de algún ataque de captura de tráfico.

Figura 51. Se evidencia que el servicio FTP no cuenta con cifrado del tráfico.



Fuente: Propia del autor

- Restricción de acceso al usuario final solo a la carpeta autorizada.

Para este proceso se establecerá una jaula al usuario "reporte" de modo que solo pueda visualizar y tener acceso solo al contenido de la capeta que le es asignada.

Este proceso se realiza modificando el archivo de configuración del servidor FTP "**vsftpd**", ubicado en la ruta "**/etc/vsftpd/vsftpd.conf**", des comentando las líneas que se resaltan de color rojo.

Figura 52. Ajuste de líneas de configuración del servicio vsftpd para el control de acceso a carpetas y archivos

```
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd/banned_emails
#
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
# the user does not have write access to the top level directory within the
# chroot)
#chroot_local_user=YES
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd/chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
```

Fuente: Propia del autor

- Implementación en el servicio FTP de los protocolos SSL (Capa de Zócalo Seguro) y TLS (Seguridad en el Nivel de Transporte)

Este proceso requiere obligatoriamente el uso de certificado SSL motivo por el cual se dará uso al mismo ya creado para el servicio Apache Web server haciendo énfasis únicamente en la implementación del mismo.

Se debe modificar el archivo de configuración del servidor FTP "**vsftpd**", ubicado en la ruta "**/etc/vsftpd/vsftpd.conf**", adicionando al final las líneas que se resaltan de color rojo las cuales se anotan luego de acuerdo a la numeración asignada para aclarar las configuraciones realizadas.

Figura 53. Configuración para soporte TLS/SSL del servicio vsftpd

Fuente: Propia del autor

Nota:

1 Corresponde a la activación de TLS/SSL

2 Forzar el uso de TLS/SSL en la transferencia de datos

3 Obliga a que la autenticación sea bajo TLS/SSL.

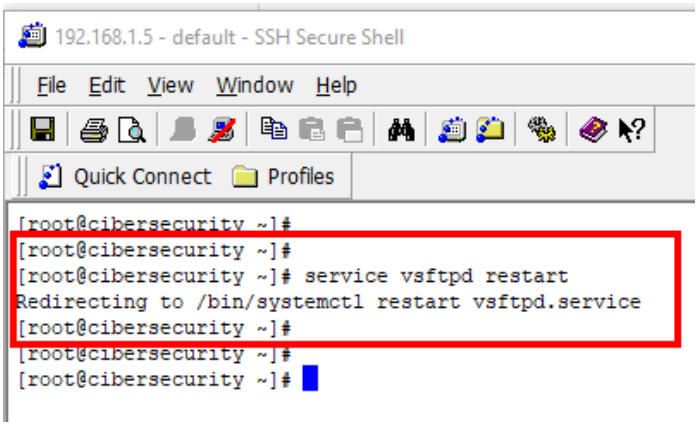
4 Activa el uso de TLS versión 1.2

5 Bloque donde se establecen las rutas del certificado y la firma digital.

6 Configuraciones del comportamiento del cifrado y el reúso de SSL

Finalmente se debe reiniciar el servicio "1" para que se tomen los cambios.

Figura 54. Reinicio del servicio vsftpd por medio del comando "service vsftpd restart"



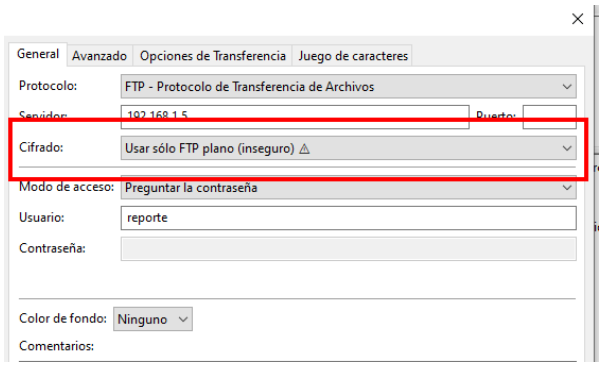
Fuente: Propia del autor

Prueba de las configuraciones aplicadas al servicio FTP

- Verificación del uso de TLS/SSL de forma obligatoria en el servicio.

  Se usa el cliente FTP "Filezilla", desde la terminal remota intentando usar conexión sin TLS/SSL.

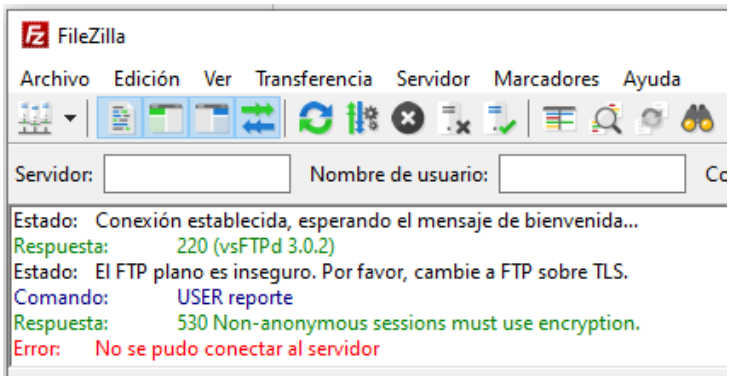
Figura 55. Intento de conexion sin usar TLS/SSL



Fuente: Propia del autor

La situación anterior devuelve como resultado la negación de acceso por parte del servicio informado que debe realizarse con TLS/SSL.

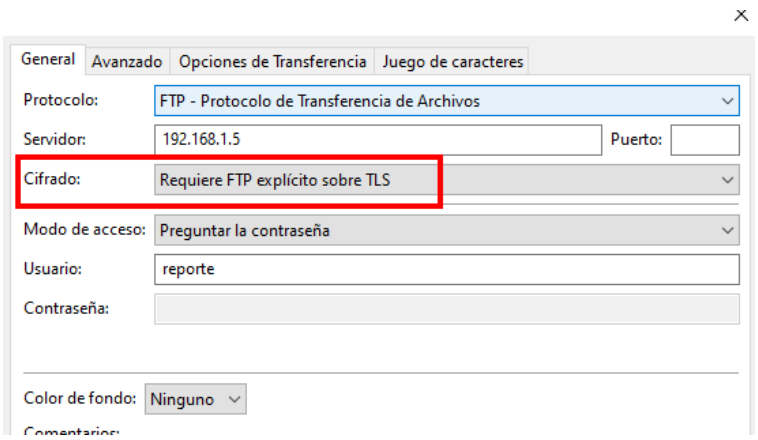
Figura 56. Respuesta del servidor FTP negando la conexión por no usar TLS/SSL



Fuente: Propia del autor

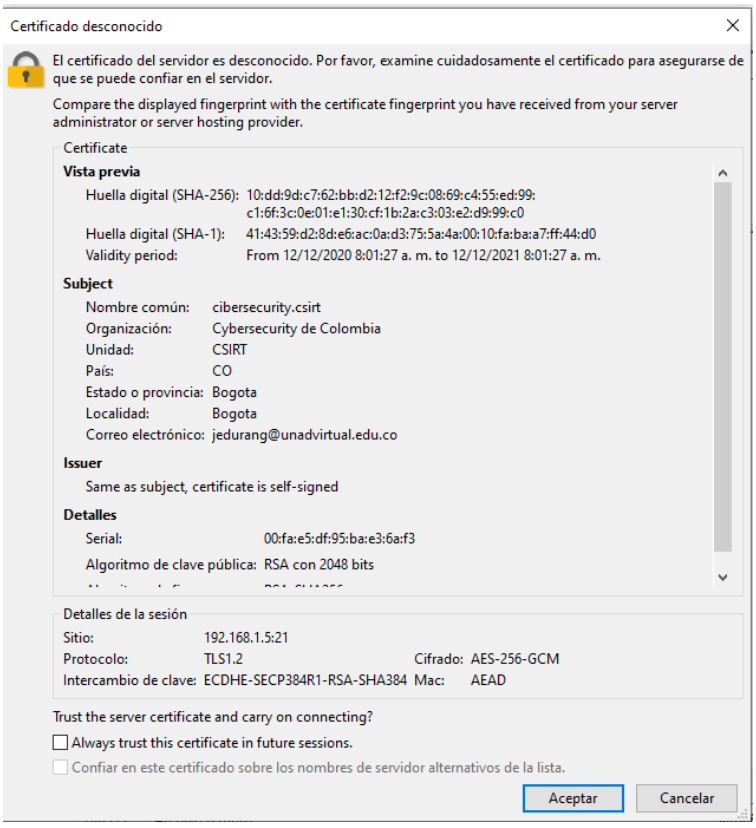
En concordancia con esto se procede a realizar la conexión usando TLS/SSL de la siguiente forma.

Figura 57. Conexión al servicio FTP usando SSL



Fuente: Propia del autor

Figura 58. Certificado SSL asociado al servicio FTP



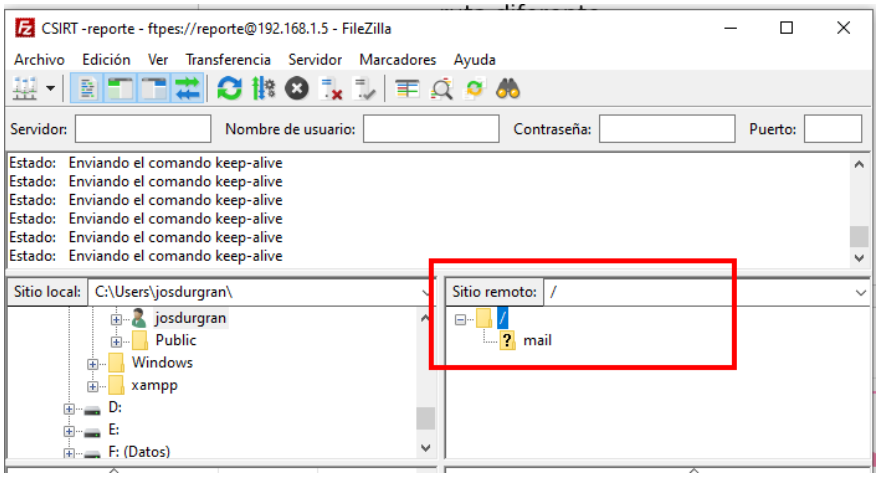
Fuente: Propia del autor

Nota: Se puede comprobar así que la conexión se está desarrollando bajo los protocolos TLS/SSL con el certificado generado por el CSIRT, la advertencia corresponde a que el certificado SSL asociado al servicio no proviene de una entidad certificadora reconocida por Filezilla.

- **Verificación de la restricción de acceso a solo las rutas autorizadas al usuario.**

En esta situación se dio uso al usuario "reporte", cual solo tiene acceso al directorio personal.

Figura 59. Visualización de acceso controlado al usuario reporte del servicio FTP



Fuente: Propia del autor

En la Figura 59, se muestra que el usuario reporte se ha enjaulado en la carpeta autorizada (Carpeta personal), que esta se ha convertido en su raíz y que solo tiene acceso de esta en adelante no puede acceder a ningún recurso alojado en rutas inferiores.

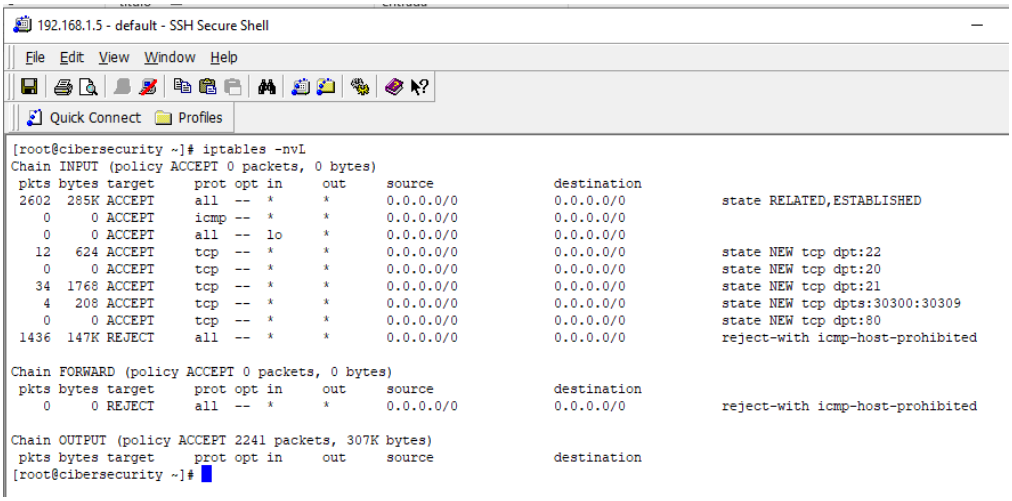
De esta forma se cumple con el propósito trazado para en la configuración del servidor FTP.

Configuración servicio Firewall IPTABLES

- **Verificación condición de firewall IPTABLES**

Para el la verificación inicial del estado del servicio firewall de ejecuta el comando "iptables -nvL" que muestra las reglas aplicadas.

Figura 60. Estado actual del servicio iptables



Fuente: Propia del autor

En la Figura 60, se muestra el resultado del estado actual de firewall IPTABLES en donde se evidencia que este tiene como política por defecto la aceptación de todos los paquetes y se bloquean y se aplican bloqueos a aquellos que el administrador considere.

Con base en lo anterior el CSIRT de Cybersecurity de Colombia Ltda, propone que se aplique la política por defecto inversa es decir negar todas las solicitudes y permitir únicamente las que el administrador considere y requiera de acuerdo a los servicios utilizados.

Lo anterior con soporte en que es más riesgoso permitir todas las entradas y bloquear las que se consideren, ya que de presentarse olvido, no conocimiento o falta de mantenimiento se pueden dejar importantes vulnerabilidades que de ser explotadas causarían daños significativos tanto a los servicios, los datos y la operación misma del sistema.

A continuación, se presenta la configuración propuesta inicialmente por el CSIRT con motivo de reducir el riesgo plateado anteriormente.

Editar el archivo "**/etc/sysconfig/iptables**" colocando las reglas que se resaltan y se explican a continuación.

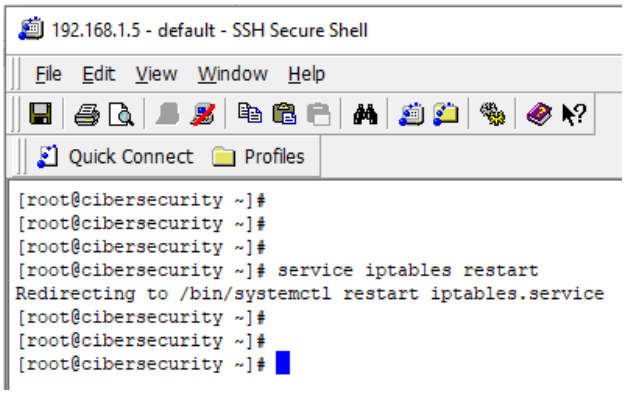
Figura 61. Reglas propuestar por el CSRIT para el firewall IPTABLES

```
*filter

# Política por defecto para entradas: Negada
:INPUT DROP [0:0]

# Política por defecto para redirección: Negada
:FORWARD DROP [0:0]

# Política por defecto para salidas: Permitida
:OUTPUT ACCEPT [3356:6091439]

# Acceso pertimitido completo desde localhost
-A INPUT -i lo -j ACCEPT

# Acceso servicio SSH
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT -m comment --comment "Acceso servicio SSH"

# Acceso servicio FTP
-A INPUT -p tcp -m tcp --dport 20 -m state --state NEW,ESTABLISHED -j ACCEPT -m comment --comment "Acceso servicio FTP"
-A INPUT -p tcp -m tcp --dport 21 -m state --state NEW,ESTABLISHED -j ACCEPT -m comment --comment "Acceso servicio FTP"
-A INPUT -p tcp -m tcp --dport 30300:30309 -m state --state NEW,ESTABLISHED -j ACCEPT -m comment --comment "Acceso servicio FTP"

# Acceso servicio HTTP
-A INPUT -p tcp -m tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT -m comment --comment "Acceso servicio HTTP"

# Acceso servicio HTTPS
-A INPUT -p tcp -m tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT -m comment --comment "Acceso servicio HTTPS"

# Ingreso respuestas DNS tcp y udp
-A INPUT -p tcp -m tcp --sport 53 -m state --state NEW,ESTABLISHED -j ACCEPT -m comment --comment "Ingreso respuestas DNS tcp"
-A INPUT -p udp -m udp --sport 53 -m state --state NEW,ESTABLISHED -j ACCEPT -m comment --comment "Ingreso respuestas DNS udp"

#Acceso a base de datos PostgreSQL
-A INPUT -s 192.168.1.6 -p tcp -m tcp --sport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT -m comment --comment "Acceso a PostgreSQL"

COMMIT
```

Fuente: Propia del autor

Reiniciar el servicio IPTABLES para que se apliquen las reglas

Figura 62. Reinicio del servicio iptables con el comando "service iptables restart"



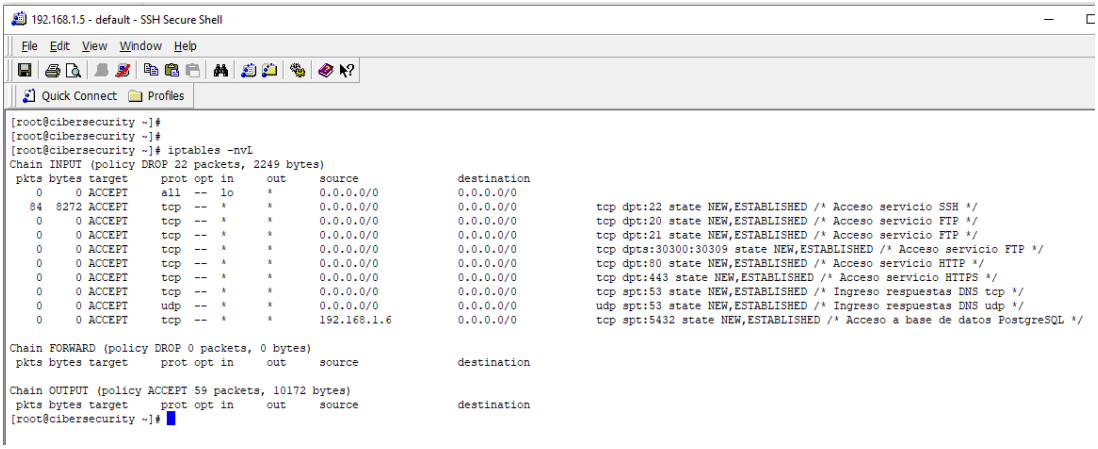
Fuente: Propia del autor

Prueba de las configuraciones aplicadas al servicio firewall IPTABLES

- **Verificación de la aplicación de reglas**

  Para el la verificación del estado del servicio firewall de ejecuta el comando "iptables –nvL" que muestra las reglas aplicadas.

Figura 63. Verificacion del estado de las reglas del firewall IPTABLES



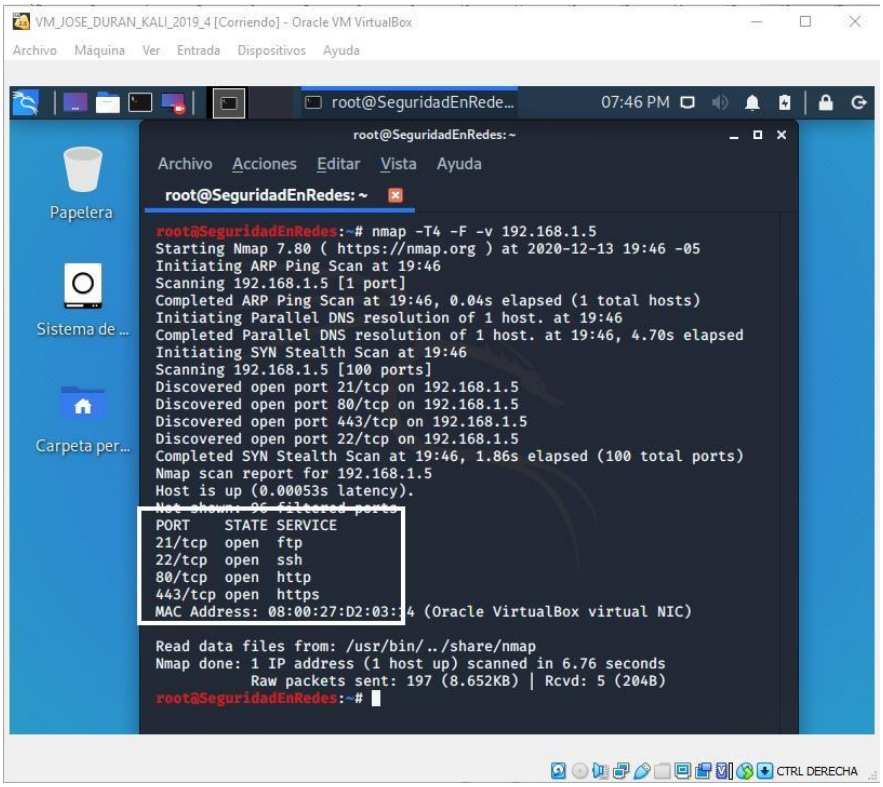
Fuente: Propia del autor

En la Figura 63, se evidencia que la política por defecto de entradas y redirección es negada, que todas las salidas están permitidas y que solo se autoriza el acceso a los servicios que lo requieren (SSH, FTP, HTTP, HTTPS, DNS TCP, DNS UDP y base de datos pero solo a la IP autorizada); logrando de esta forma control más estricto sobre los accesos al servidor y garantizando de esta forma que solo cuentan con acceso los servicios que se necesitan.

- **Ejecución de escaneo de puertos.**

Se lleva a cabo la ejecución de un nuevo escaneo de puertos con NMAP desde Kali Linux, con el propósito de verificar nuevamente el estado de los servicios disponibles públicamente luego de las actividades del CSIRT.

Figura 64. Ejecución de escaneo de puertos de control con NMAP desde Kali Linux



Fuente: Propia del autor

La ejecución del escaneo de puertos revela que el desarrollo de las actividades propuestas por el CSIRT han logrado cumplir con el propósito de mejorar las condiciones de aseguramiento del servidor y los correspondientes servicios que este aloja.

En la sesión resaltada de color blanco en la Figura 64, se evidencia que solo son están disponibles públicamente los servicios que lo requieren y los demás se aíslan de este entorno manteniendo la operatividad de todos ellos pero en el contexto privado, sumado a esto se aplican procesos de mejora a los servicios que lo requieren con el caso de la aplicación de técnicas de cifrado para incrementar las salvaguardas establecidas.

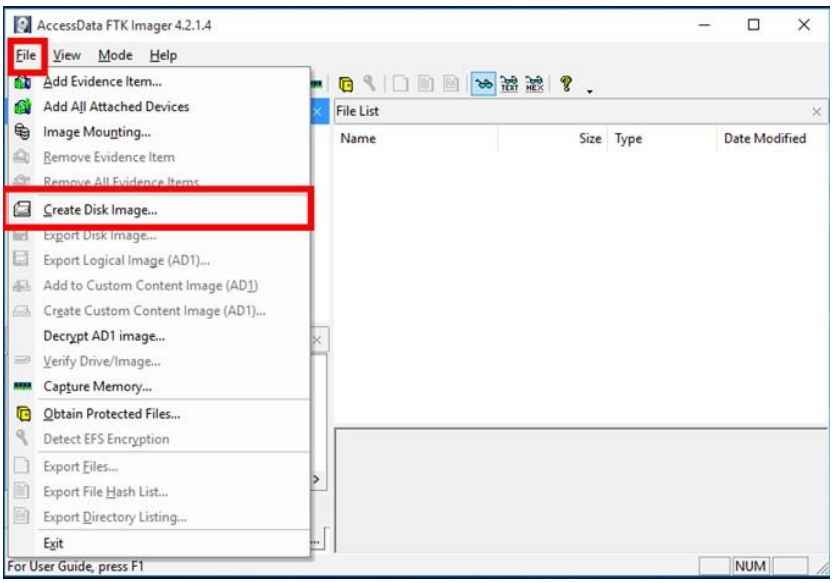
Toma de imágenes bit a bit de los discos duros de los computadores de los usuarios finales con la herramienta "AccessData FTK Imager"

- Toma de copia del disco duro

Inicialmente de debe tener instalada la última versión del programa "**AccessData FTK Imager"**, luego de esto desarrollar los siguientes pasos.

Ingresar al menú "**File**" y a la opción "**Create Disk Image**" esto colocará en escena un asistente para desarrollar el procedimiento.

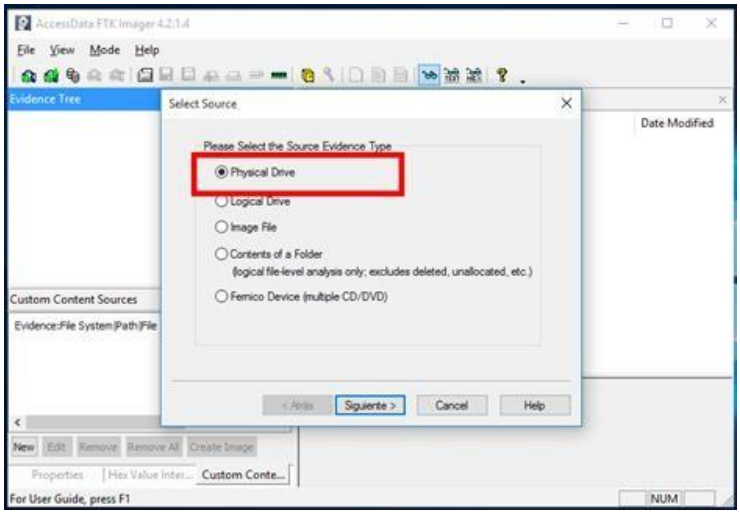
*Figura 65. Inicio del asistente para creacion de imagenes de "**FTK imager**"*



Fuente: Propia del autor

Una vez abierto el asistente se debe seleccionar la opción "**Physical Drive**" y presionar "Siguiente".

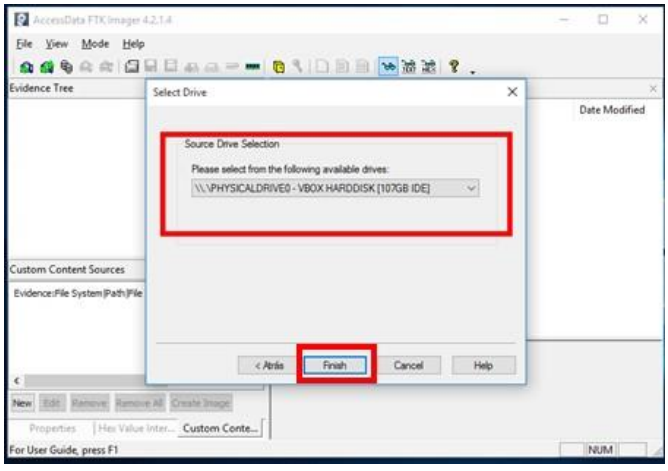
Figura 66. Seleccionar el tipo de fuente a la que se le tomara copia



Fuente: Propia del autor

Seguido a esto se debe elegir el disco al que se le tomará el respaldo y presionar "Finish"

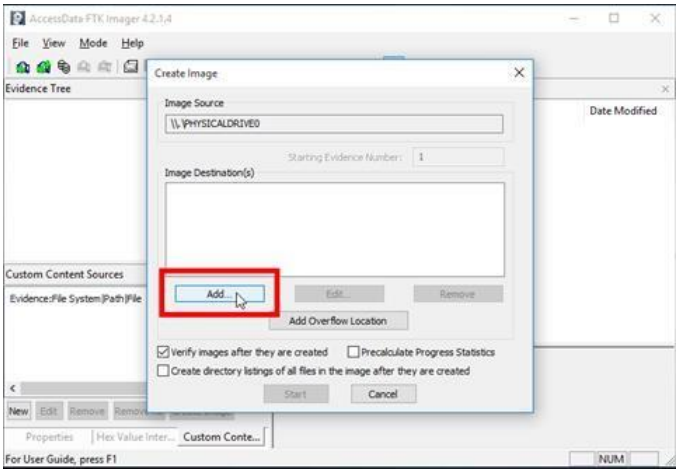
Figura 67. Selección del disco al que se le realizara la copia



Fuente: Propia del autor

Luego se debe configurar la ubicación donde se escribirá la imagen del disco para lo que se debe presionar en el botón "Add".

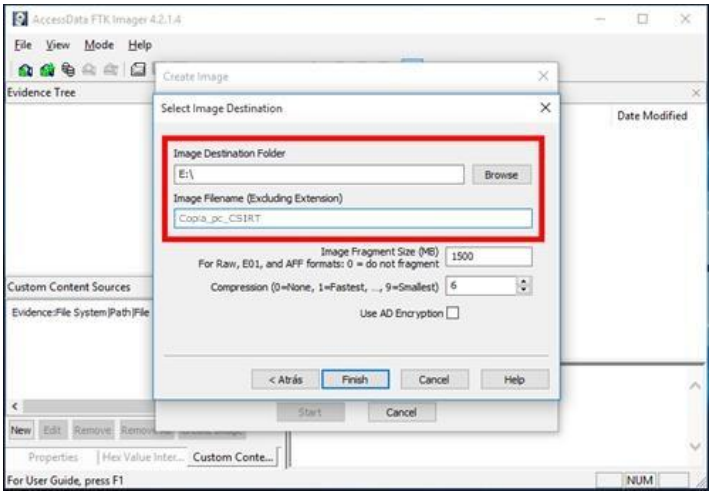
Figura 68. Configuración de la ubicación de la ruta de almacenamiento de la imagen



Fuente: Propia del autor

Establecer el nombre del archivo y la ruta correspondiente esta debe ser diferente al disco que se le realiza la copia.

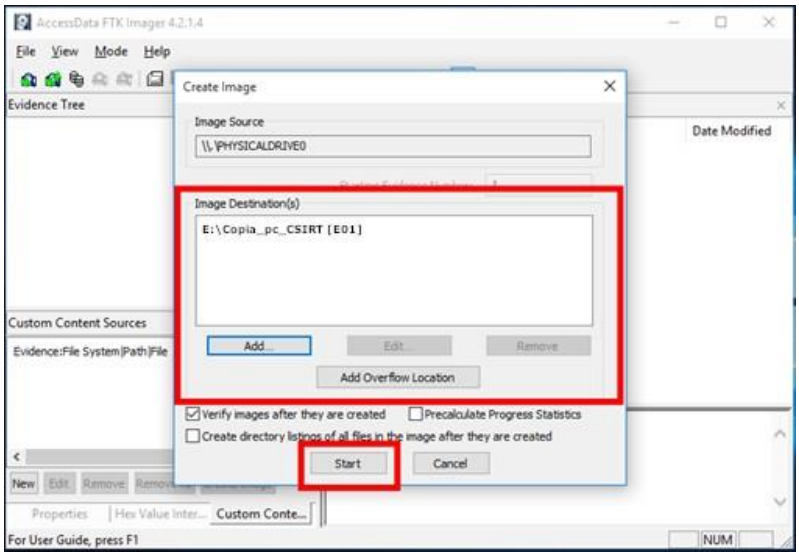
Figura 69. Nombre y ubicación de la copia del disco



Fuente: Propia del autor

Dar inicio al proceso de la toma de la copia del disco.

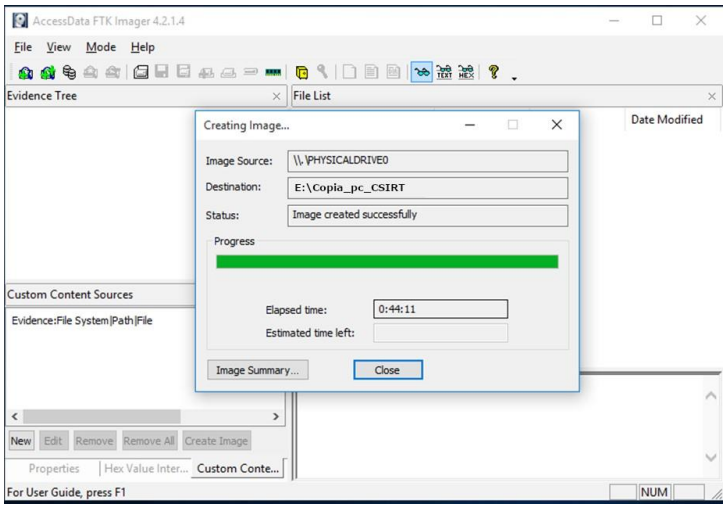
Figura 70. Inicio del proceso de copia del disco



Fuente: Propia del autor

Se finaliza el proceso de toma de la copia del disco

Figura 71. Confirmación del proceso de toma de la copia del disco



Fuente: Propia del autor

Luego de generada la copia del disco; esta debe ser remitida al equipo de experto en informática forense perteneciente a la coordinación técnica del CSIRT con el objetivo que se desarrollen las acciones documentales y procedimentales necesarias con las evidencias digitales y lograr así caracterizar adecuadamente la situación y las posibles agresiones que se pudieron presentar.

4. CONCLUSIONES DEL ESCENARIO PROBLEMA

De acuerdo a los diferentes hallazgos encontrados en los servicios existen muchas opciones que pudieron materializarse en la agresión presentada algunas de estas opciones pudieron ser ingeniería social para lograr tener acceso a los sistema, captura de tráfico para identificar credenciales de acceso lo que podría dar acceso a casi cualquier componente del sistema como la base de datos o el sistema mismo.

Al no contar con mecanismos para identificar el tráfico a los sistemas se puede pensar que pudo tratarse entre otras cosas de un error de gestión.

También existe la posibilidad de explotación combinada de vulnerabilidades que finalmente permitió al posible agresor materializar el ataque.

5. RECOMENDACIONES

Siempre que tenga alguna duda o dificultad en la realización de alguna acción se debe solicitar ayuda al personal técnico del CSIRT.

El presente laboratorio corresponde a un primer ejercicio de aseguramiento en la empresa “Cybersecurity de Colombia”, pero se debe tener absoluta conciencia que pueden existir más vulnerabilidades que requieren tratamiento por lo que se recomienda continuar trabajando de la mano con el CSIRT para lograr fortalecer cada día la seguridad informática en la compañía.

De acuerdo a los datos de la arquitectura de red expresados tanto en el escenario problema como en la configuración del servidor el CSIRT recomienda que se inicie con en "**Cybersecurity de Colombia**", un proceso de evaluación de la red de comunicaciones con el objetivo comprender mejor la arquitectura de ésta y poder pensar en la posible segmentación con motivo de tener mejor control de ella y generar independencia de servicios.

Es importante que se sigan fortaleciendo los diferentes aspectos al interior de la compañía que contribuyan en el mejoramiento de las condiciones de seguridad informática en "**Cybersecurity de Colombia**"