DESARROLLO DEL DISEÑO TÉCNICO DE UN CENTRO DE INCIDENTES CIBERNÉTICOS PARA EL CASO DE ESTUDIO EMPRESA CIBERSECURITY DE COLOMBIA LTDA.

TANIA BARRERA RODRÍGUEZ
YEXON VALBUENA SANABRIA

Director
John Freddy Quintero Tamayo

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
BOGOTÁ
2020

PROYECTO APLICADO: DESARROLLO DEL DISEÑO TÉCNICO DE UN CENTRO DE INCIDENTES CIBERNÉTICOS PARA EL CASO DE ESTUDIO EMPRESA CIBERSECURITY DE COLOMBIA LTDA

TANIA BARRERA RODRÍGUEZ
YEXON VALBUENA SANABRIA

Proyecto presentado como requisito para obtener el título de
"ESPECIALISTA EN SEGURIDAD INFORMÁTICA"

Director
John Freddy Quintero Tamayo

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
BOGOTÁ
2020

DEDICATORIA

A DIOS por darme las capacidades para poder cumplir mis anhelos, a mi familia por su paciencia y ejemplo, a Juan Felipe mi hijo por ser el motor de mi vida y a Yexon mi compañero que me impulsa día a día a ser mejor y a no desfallecer a pesar de las dificultades.

Tania Barrera Rodríguez

Este proyecto está dedicado a mi hijo Andrés David Valbuena Villamil por ser él parte fundamental en mi vida, por ser el motor que me impulsa a ser mejor como padre, persona y estudiante. A mi compañera Tania Barrera Rodríguez por su conocimiento, dedicación y constante lucha para sacar este proyecto adelante, por tantos días y noches dedicadas a la investigación y desarrollo de este documento y por permitirme compartir sus conocimientos.

Yexon Valbuena Sanabria

AGRADECIMIENTOS

A los tutores y directores de curso quienes, a través de su retroalimentación, orientación, aportaron en la construcción de las habilidades y conocimiento adquiridos. A la UNAD por ofrecer planes de estudio virtuales de calidad que se adaptan a las necesidades de muchos que tenemos que laborar y a la vez responder por los requerimientos del hogar y especialmente por hacer presencia a nivel nacional brindando oportunidades de estudio a todo aquel que sin importar su ubicación quiera crecer profesionalmente.

RESUMEN

Debido al crecimiento acelerado de los delitos informáticos en los últimos años, donde personas y compañías tanto públicas como privadas han visto comprometida su información, su privacidad, o de alguna manera han sido víctimas de algún delito en la internet, la empresa CIBERSECURITY de Colombia LTDA tiene como propósito crear y gestionar las funciones de atención de requerimientos a delitos cibernéticos, ofreciendo servicios que permitan dar soporte a sus clientes teniendo presente el nivel de servicio contratado los cuales pueden ser de respuesta a incidentes o de gestión de vulnerabilidades. Para ello, el presente proyecto estará orientado al diseño técnico de un centro de respuesta a incidentes cibernéticos, cuyos resultados serán: el mapa de la infraestructura tecnológica del CSIRT, identificando las herramientas de hardware y software requeridas para el desarrollo del CSIRT, las cuales se probarán en un laboratorio controlado, donde se podrá simular la operación de la tecnología necesaria para la puesta en marcha del laboratorio del CSIRT.

El desarrollo de este proyecto está soportado en el marco teórico, tecnológico y legal requeridos para la construcción del CSIRT, cuya metodología de desarrollo consistirá en técnicas de recolección de datos de portales especializados en la seguridad informática, entrevistas a personal vinculado a un CSIRT existe en Colombia y consulta de documentación de procesos (lineamientos, procedimientos, guías, manuales, formatos) relacionados con la operación del mismo.

Palabras clave: Incidentes cibernéticos, respuesta, CSIRT, seguridad, diseño técnico, ataques, amenazas, evidencias, eventos, vulnerabilidad, activos.

ABSTRACT

Due to the accelerated growth of computer crimes in recent years, where both public and private individuals and companies have been compromised their information, their privacy, or have somehow been victims of any crime on the internet, the company CIBERSECURITY de Colombia LTDA. has a purpose to create and manage the functions of response to cyber incidents, offering services that allow to support its customers taking into account the level of service contracted which can be incident response or vulnerability management. For this, the present project will be oriented to the technical design of a cyber incident response center, the results of which will be: the map of the technological infrastructure of the CSIRT, identifying the hardware and software tools required for the development of the CSIRT, in order to testing them in a controlled laboratory, where the operation of the infrastructure required for the perfomance of the CSIRT laboratory can be simulated.

The development of these results will be supported in the theoretical, technological and legal framework required for the construction of the CSIRT, whose development methodology will consist of data collection techniques of specialized portals in computer security, interviews with personnel linked to a CSIRT in Colombia and review of process documentation (guidelines, procedures, guides, manuals, formats) related to its operation.

Keywords: Cyber incidents, response, CSIRT, security, technical design, attacks, threats, evidence, events, vulnerability, assets.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

INTRODUCCIÓN

Con el desarrollo de la tecnología se han incrementado los incidentes de ciberseguridad. Suceden a cada instante y afectan a un gran número de personas y organizaciones públicas y privadas; por esta razón, este proyecto se enfocará en la creación de un laboratorio para un CSIRT que tiene como fin probar las diferentes herramientas requeridas para su operación, que permitirán más adelante gestionar los incidentes de seguridad en la red por medio de mecanismos y software de vanguardia.

Cientos de personas y organizaciones que hacen uso de alguna manera de los servicios de internet se ven cada vez más inconformes y con un alto grado de prevención debido a los constantes ataques que minuto a minuto están ocurriendo en la red y que pueden afectar la integridad de la información dispuesta en los diferentes portales a los que tienen que acceder y que, a pesar que estos incidentes se reportan, las acciones para controlar a los delincuentes no es suficiente por lo que el problema sigue en constante crecimiento.

Esta problemática se debe tratar de manera inmediata, debido a que representa un peligro constante para la información de los usuarios y organizaciones y por ser internet uno de los servicios que más se están usando y que va en constante crecimiento, es trascendental contar con herramientas para la seguridad informática que brinden confianza al estar navegando por la red realizando algún tipo de consulta o solicitando algún servicio. Por lo anterior, es necesario contribuir con una propuesta que aporte conocimiento relacionado con el diseño técnico de un CSRIT el cual permitirá mitigar los delitos en la red y de gestionar los incidentes de seguridad cuando estos ocurran.

El presente proyecto tiene como fin la documentación e implementación de un laboratorio para un CSIRT con el propósito de simular la operación de un CSIRT con las herramientas de software que permitirán gestionar los incidentes de ciberseguridad (servidor de monitoreo, servidor de copias de respaldo, servidor sandbox, correlacionador de eventos, herramientas forenses y pentesting).

Para este proyecto se realizará una consulta del software libre necesario para el desarrollo e implementación del laboratorio del CSIRT. Con base en la identificación de las herramientas para el laboratorio se generará el diseño de la estructura tecnológica necesaria donde se identificarán las dependencias necesarias que conforman el CSIRT.

Por último, se realizarán pruebas de funcionalidad a las herramientas seleccionadas con el fin de confrontar los requerimientos mínimos necesarios para el funcionamiento del laboratorio del CSIRT.

1 DEFINICIÓN DEL PROBLEMA

Según cifras del Centro Cibernético Policial[1], en el año 2018 se registraron 24.400 denuncias por delitos informáticos en Colombia, de ellos más de 6.000 se realizaron en Bogotá seguido por Cali y Medellín. Los delitos más comunes son transacciones electrónicas, pagos a través de las diferentes plataformas en línea y web spoofing (suplantación); lo anterior, a través del engaño a los ciudadanos. Con base en lo anterior, ¿cómo llevar a cabo el desarrollo técnico de un centro de incidentes cibernéticos que permita prevenir, gestionar y responder a éstos?

De acuerdo con cifras publicadas en la página MediaCloud, en su artículo "Predicciones de ciberseguridad de aquí al 2020"[2], se estima a nivel mundial que:

- El 99% de las vulnerabilidades explotadas seguirán siendo aquellas que ya se conocen desde hace al menos 1 año.
- Un tercio de los ataques exitosos experimentados por las empresas será debido a los recursos TIC sombra (recursos usados dentro de una empresa sin aprobación o consentimiento).
- Más del 25% de los ataques identificados realizados a empresas, implicará al IoT (Internet of Technology).

Por otro lado, de acuerdo con predicciones publicadas por Computer World[3], John Galindo CEO de Digiware, estima que:

- Uno de cada mil ciberataques serán incidentes nunca antes vistos o "Zero Day Attack".
- Al menos un incidente de ciberseguridad cobrará vidas humanas.
- El 40% de las organizaciones usarán técnicas de Data Masking para proteger sus BD y evitar la pérdida de sus activos de información.

---

[1] CONEXIÓN CAPITAL. "En Bogotá se registraron más 6.000 denuncias por delitos cibernéticos en 2018". {En línea}. 5 de febrero de 2019. {Consultado el 29 de noviembre de 2019}. Disponible en: https://conexioncapital.co/bogota-denuncias-delitos-ciberneticos/

[2] MEDIACLOUD - #ADNCLOUD. "Innovación en la sociedad digital. Predicciones de ciberseguridad de aquí al 2020". {En línea}. {Consultado el 29 de marzo de 2020}. Disponible en: https://blog.mdcloud.es/predicciones-ciberseguridad-aqui-al-2020/.

[3] COMPUTERWORLD. "Predicciones de seguridad para 2020". {En línea}. 26 de noviembre de 2018. {Consultado el 29 de marzo de 2020}. Disponible en: https://computerworld.co/predicciones-de-seguridad-para-2020/

Finalmente, de acuerdo con publicación Revista Dinero - ¿Cuáles son las tendencias y retos este año en materia de ciberseguridad? (2019), donde se presenta reporte de la firma consultora EY (junio 2019) que consultó a 1.400 líderes de riesgo y seguridad cibernética de algunas de las organizaciones más grandes del planeta, se encontró que el 80% de las juntas directivas no hacen de la ciberseguridad un tema estratégico para sus compañías, el 87% de las organizaciones todavía operan con niveles limitados de ciberseguridad y resiliencia, el 77% trabaja con medidas de protección básicas en materia de ciberseguridad y buscan avanzar hacia capacidades más alineadas con la realidad.

Adicionalmente, dentro de las principales preocupaciones de las organizaciones, se encontraron: a) empleados inconscientes se clasifican como la mayor debilidad (34%) y b) organizaciones podrían no identificar todas las violaciones e incidentes de las que son víctimas (82%).

2 JUSTIFICACIÓN

Debido a la continua presentación de incidentes de seguridad generados por amenazas permanentes sobre las organizaciones (públicas y privadas) y personas, se hace necesario contar con un equipo de expertos que diseñe técnicamente la conformación de la infraestructura tecnológica requerida para el laboratorio del CSIRT que prestará los servicios de respuesta a incidentes cibernéticos y la gestión de vulnerabilidades, con el fin de controlar los daños que pueda afectar la información de la organización, coordinar una recuperación rápida, preservar la evidencia, documentar el incidente y prevenir incidentes similares a futuro o contar con plan de respuesta o posible solución y divulgar este conocimiento para fortalecer la seguridad informática en las organizaciones y las personas y así dar un manejo efectivo a incidentes futuros.

El éxito de un CSIRT depende de los recursos técnicos disponibles, del nivel de conocimiento y las habilidades de los recursos humanos, de los procesos que se aplican al interior del CSIRT y de la cooperación interna y entre organizaciones, es decir un gran trabajo en equipo donde se comparte información de amenazas, vulnerabilidades, ataques, estrategias y métodos para la gestión de incidentes. Adicionalmente un CSIRT debe adaptarse fácilmente a los nuevos requerimientos en seguridad informática de las organizaciones y usuarios, manteniendo el ciclo de mejora continua.

De acuerdo con el artículo *Computer Security Incident Response Team Effectiveness: A Needs Assessment*[4], las empresas están motivadas a proteger su reputación y para ellas es importante que los incidentes se resuelvan de forma rápida y silenciosa, por lo que el visibilizar los incidentes y compartir información de los mismos ha resultado ser una tarea muy difícil. Por lo anterior, es importante sensibilizar a las organizaciones y a los ciudadanos respecto a la relevancia de informar oportunamente los eventos e incidentes de seguridad para su manejo.

En este artículo se muestran los resultados de la encuesta que fue diligenciada por varios CSIRT de países bajos, quienes manifiestan la necesidad de medir la efectividad de la gestión de incidentes y la efectividad del equipo de trabajo, puesto que no cuentan con métricas para ello, aunque se cuenta con indicadores tales como la velocidad de la respuesta, el tiempo de identificación, la cantidad de errores, los costos, entre otros; pero es importante contar con otros indicadores tales como las tasas de incidentes a lo largo del tiempo y el tiempo medio de reparación.

[4] VAN DER KLEIJ, Rick, KLEINHUIS, Geert y YOUNG, Heather. “Computer Security Incident Response Team Effectiveness: A Needs Assessment”. {En línea}. 12 de diciembre de 2017. {Consultado en 29 de noviembre del 2020}. Disponible en: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5733042

En el mercado de la informática se encuentra una variedad de herramientas (libres y propietario) al servicio de la seguridad informática, pero para la implementación de un CSIRT con un presupuesto limitado se hace necesario acudir a herramientas libres. Estas presentan una gran ventaja si se comparan con los precios que tienen las herramientas propietario, además, se tiene la posibilidad de modificar el software (open source) y así implementarlo de acuerdo a las necesidades técnicas del CSIRT.

Dado lo anterior, se hace necesario seleccionar las mejores herramientas de software open source que faciliten la gestión de los requerimientos en seguridad informática y probar su funcionamiento.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar la documentación técnica para la empresa CIBERSECURITY de Colombia LTDA que le permita llevar a cabo las actividades propias de un Centro de respuesta a incidentes cibernéticos en el ámbito de un CSIRT.

3.2 OBJETIVOS ESPECÍFICOS

1. Identificar las herramientas de hardware y software disponibles en el mercado tecnológico, requeridas para el desarrollo de las actividades del CSIRT.

2. Diseñar el mapa de la estructura tecnológica del CSIRT donde se puedan identificar las dependencias mínimas para el funcionamiento del CSIRT.

3. Ejecutar y documentar pruebas de cada una de las herramientas de software instaladas para verificar que éstas cumplen con los requerimientos para el laboratorio del CSIRT.

4 MARCO REFERENCIAL

4.1 MARCO CONCEPTUAL

Un CSIRT para atender incidentes de seguridad es un equipo, organismo u entidad que brinda servicios de seguridad informática e igualmente de seguridad de la información; su propósito es prevenir y gestionar cuando se presente un incidente de seguridad. Estos equipos están conformados por grupos interdisciplinarios y su actuar va ligado a procedimientos y políticas con el fin de responder de manera oportuna y efectiva ante un incidente de seguridad, además colaboran con la mitigación de los riesgos de los ataques cibernéticos.

Para la gestión de servicios, estos centros cuentan con una infraestructura básica (hardware y software) y con procedimientos operativos, todo esto soportado en marcos de trabajo.

Los conceptos básicos relacionados con seguridad de la información están en la norma ISO 27000, y en la guía de gestión y clasificación de incidentes del Ministerio de las TIC[5]. Algunos de los términos más utilizados en la gestión de incidentes de seguridad de la información se describen a continuación:

Amenaza: ejercicio u objeto capaz de provocar un incidente en la seguridad informática y/o de la información[6].

Cracker: posee las mismas cualidades de encontrar vulnerabilidades en sistemas informáticos de hacker, pero a diferencia de este, es que esta en el lado del mal, su propósito va desde infiltrase en un sistema causando daños hasta el secuestro de la información de una organización, persona natural con el fin de cobrar un beneficio económico o por el simple reconocimiento de la comunidad[7].

---

[5] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

[6] DEPARTAMENTO DE SEGURIDAD INFORMÁTICA. {Consultado el 29 de noviembre de 2019}. Disponible en: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

[7] Ibíd

Evento: una situación reconocida con el estado o funcionamiento normal de un sistema informando una violación a la seguridad de la información[8].

Hacker: Persona con enorme conocimiento en el campo de la seguridad informática, su pasatiempo consiste en detectar fallas (vulnerabilidades en las herramientas tecnológicas) para luego repararlas. También, se dedican al desarrollo de aplicaciones libres con el fin de luchar por alguna causa[9].

Incidente: es la trasgresión perentoria a los activos de información. De acuerdo con la ISO 27035. Los incidentes de seguridad de la información se llevan a cabo por medio de unos eventos de seguridad que tienen como fin comprometer las operaciones de la organización y poner en riesgo la información de la organización[10].

Incidente de seguridad de la información[11]: es un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de la información; se refiere a un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información de la entidad.

Phishing: es una forma de hurto en la web y que consiste en engañar a una víctima en potencia mediante el envío de correos a nombre de empresas reconocidas solicitándole información de sus tarjetas de crédito[12].

Virus: es un programa o código creado con el fin de provocar daño en un sistema, consumiendo recursos innecesarios, alterando la información y el funcionamiento del activo atacado[13]. Es diferente a malware, debido a que el virus está en la capacidad de reproducirse e infectar todos los equipos que se encuentren conectados en una red.

---

[8] Ibíd

[9] MÁSQUENEGOCIO. “8 conceptos de seguridad informática que deberías conocer”. {En línea}. 23 de mayo de 2017. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.masquenegocio.com/2017/05/23/conceptos-seguridad-informatica/

[10] CENTRO NACIONAL DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA. “Qué es un incidente”. {En línea}. 5 de octubre de 2018. {Consultado el 29 de noviembre de 2019}. Obtenido de https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/comunicacion/publicaciones/que-es-un-incidente

[11] IBID.

[12] IBID

[13] TORRES, Gonzalo. “¿Qué es un virus informático?”. {En línea}. 18 de diciembre de 2017. {Consultado el 29 de noviembre de 2019}. Obtenido de https://www.avg.com/es/signal/what-is-a-computer-virus

Vulnerabilidad: una debilidad que se presenta en una herramienta tecnológica (Sistema Operativo, servidor, red, etc.) y permite que un delincuente pueda acceder al mismo violando la confidencialidad integridad y la disponibilidad del activo[14].
Estas se ocasionan por la ausencia de buenas prácticas en los desarrollos, por falta de actualización y parcheo en servidores y aplicación etc.

4.2 MARCO TEÓRICO

Los CSIRT cobran mayor importancia debido al incremento de los ataques a los activos de información de las organizaciones y ciudadanos.

La gestión de incidentes de seguridad de la información de acuerdo con la norma ISO27035[15] y con la Guía para la gestión y clasificación de incidentes de seguridad de la información[16], se desarrolla en un proceso conformado por 4 etapas, como se observa en la figura 1:

Figura 1. Etapas gestión de incidentes de seguridad informática

[14] TECNOLOGIA & INFORMATICA. “Vulnerabilidades informáticas”. tecnologia-informatica.com. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://tecnologia-informatica.com/vulnerabilidades-informaticas/

[15] ICONTEC INTERNACIONAL. “Guía Técnica Colombiana GTC-ISO/IEC 27035 Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información”. {En línea}. 12 de diciembre de 2012. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.academia.edu/37861509/GU%C3%8DA_T%C3%89CNICA_GTC-ISO_IEC_COLOMBIANA_27035_TECNOLOG%C3%8DA_DE_LA_INFORMACI%C3%93N._T%C3%89CNICAS_DE_SEGURIDAD._GESTI%C3%93N_DE_INCIDENTES_DE_SEGURIDAD_DE_LA_INFORMACI%C3%93N

[16] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información”. {En línea}. 6 de noviembre de 2016. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

Fuente: MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información”. {En línea}. 6 de noviembre de 2016. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

a) Preparación: En esta etapa se tienen en cuenta los recursos que permitan la atención de los incidentes y la infraestructura para ello, creando los procedimientos necesarios y gestionando las capacitaciones requeridas. Para esta etapa se pueden realizar las siguientes actividades: actualización de parches, hardening de la plataforma, seguridad en las redes, protección contra malware, capacitación y transferencia de conocimiento a usuarios. Estas actividades buscan prevenir que ocurran incidentes.

b) Detección, evaluación y análisis: La detección se refiere a los eventos reportados a través de indicadores que pueden señalar de la existencia de un posible incidente. Estos indicadores pueden ser: alertas de sistemas, reportes de usuarios, informes de software de antivirus, reporte de funcionamiento fuera de lo normal; estos indicadores pueden alimentarse de la información de los logs de servidores, aplicaciones, herramienta de seguridad, entre otros. Estos indicadores sirven de alertamiento y pueden ayudar a gestionar la prevención de la ocurrencia de un incidente o el establecimiento de acciones que permitan minimizar su impacto. Para la realización del análisis del incidente se requiere contar con el personal que tenga el conocimiento de las condiciones estándar de operación de las redes y los sistemas, conocimiento del comportamiento de la infraestructura y, por ejemplo, apoyados en una herramienta de correlación de eventos detectar comportamientos anormales. Por otra parte, la información que permitirá analizar el incidente, debe estar centralizada y se debe contar con una única fuente de tiempo. Entre la información con la que se debe contar se encuentran las lecciones aprendidas, información de nuevas vulnerabilidades, información de la infraestructura actual y los servicios habilitados.

c) La evaluación del incidente se refiere a establecer el nivel de impacto, basados en insumos provistos en el análisis de riesgos y en la clasificación de los activos de la organización. Respecto a la clasificación de los incidentes, se puede tomar en consideración la siguiente: acceso no autorizado, alteración no autorizada de los activos, uso inapropiado de los activos, no disponibilidad de los activos, multicomponente (para el caso de los incidentes que corresponden a más de una categoría), otros (son clasificación establecida). Adicionalmente, se establece su prioridad basados, por ejemplo, en las siguientes variables: prioridad, criticidad de impacto, impacto tanto actual como futuro. Los niveles de prioridad pueden ser: inferior, bajo, medio, alto, superior. Por cada nivel de prioridad se define un tiempo máximo de atención del incidente y no el tiempo máximo de solución, ya que este último puede variar.

d) Contención, erradicación y recuperación: La contención se refiere a la detección del incidente para evitar su propagación, para lo cual la organización puede adoptar una estrategia específica, por ejemplo: apagar el sistema, desactivar los servicios, desconectar la red, entre otros. Esta estrategia se puede adoptar dependiendo del tipo de incidente presentado, para lo que se deben establecer claramente los criterios que permitan la correcta toma de decisiones, por ejemplo: criterios forenses, preservación de la evidencia, daño potencial, tiempo y recursos para la implementar la estrategia adoptada, disponibilidad del servicio, efectividad de estrategia, duración de la aplicación de la solución. La erradicación y recuperación se refiere a eliminar cualquier rastro generado por el incidente y proceder a la restauración de los sistemas/servicios y finalmente realizar el endurecimiento de los mismos para evitar que se vuela a presentar.

e) Actividades post-incidente: Consiste en el reporte del incidente, la identificación y documentación de las lecciones aprendidas, la determinación de las medidas tecnológicas, disciplinarias y penales y el registro de toda esta información en la base de conocimiento; esta información será insumo para los indicadores. La generación de lecciones aprendidas permite conocer: la situación presentada, cómo sucedió, en qué momento sucedió, cómo se gestionó, los procedimientos aplicados, las medidas tomadas que afectaron su recuperación, cómo debería gestionarse la próxima vez que suceda y con qué personal, qué acciones correctivas se requieren para evitar que el incidente se pueda volver a presentar, herramientas requeridas para su detección, análisis y mitigación futura. Es necesario revisar la documentación de gestión de incidentes para realizar las actualizaciones que correspondan a intervalos periódicos y así garantizar la mejora continua.

4.3 MARCO LEGAL Y JURÍDICO

- Constitución Política de Colombia[17].

- Ley 734 de 2002 (Código Disciplinario Único)[18]

[17] SENADO DE LA REPÚBLICA. “Constitución Política De Colombia”. Citado por el MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “Modelo de gestión de riesgos de seguridad digital” {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.mintic.gov.co/portal/604/articles-61854_documento.docx

[18] SENADO DE LA REPÚBLICA. “Código Disciplinario Único”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0734_2002.html

- Circular Externa SFC 052 de 2007[19]. Por la cual la Superintendencia Financiera de Colombia incrementa los estándares de seguridad y calidad para el manejo de la información a través de medios y canales de distribución de productos y servicios que ofrecen a sus clientes y usuarios las entidades vigiladas por esta.

- Ley Estatutaria 1266 de 2008 (Habeas data)[20]. Contempla las disposiciones generales en relación con el derecho de habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

- Ley 1273 de 2009[21]: Código Penal. Por medio de esta Ley se modifica el Código Penal, se crea 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, entre otras disposiciones.

- Ley 1336 de 2009[22] (Explotación, pornografía y el turismo sexual con niños). Se adiciona y robustece la ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. Esta ley establece dos medidas para contrarrestar la explotación sexual y la pornografía infantil que se relacionan tangencialmente con las TIC. En primer lugar, establece en el artículo 4 (autorregulación de café internet códigos de conducta) que todo establecimiento abierto al público que preste servicios de internet o de café internet deberá colocar en un lugar visible un reglamento de uso público

---

[19] SUPERINTENDENCIA FINANCIERA DE COLOMBIA. “Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios”. Citado por el MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “Modelo de gestión de riesgos de seguridad digital” {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.mintic.gov.co/portal/604/articles-61854_documento.docx

[20] CONGRESO DE LA REPÚBLICA DE COLOMBIA. “Ley Estatutaria 1266 de 2008” (Habeas Data). Citado por el MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “Modelo de gestión de riesgos de seguridad digital” {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.mintic.gov.co/portal/604/articles-61854_documento.docx

[21] CONGRESO DE LA REPÚBLICA. “Ley 1273 de 2009”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[22] CONGRESO DE LA REPÚBLICA. Ley 1336 de 2009. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.oas.org/dil/esp/LEY_1336_DE_2009_Colombia.pdf

adecuado de la red, y deberá indicar que la violación a este genera la suspensión del servicio al usuario.

- Ley 1341 de 2009[23]: (Sector TIC). Mediante esta Ley se definen principios y conceptos sobre la sociedad de la información y la organización de las TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones. Especialmente los artículos 4, 11 y 26.

- Decreto 1727 de 2009[24] (Habeas Data). Se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros Países, deben presentar la información de los titulares de la información.

- Ley 1437 de 2011[25]: (Uso de medios electrónicos procedimiento administrativo). Consagra la utilización de medios electrónicos en el procedimiento administrativo y permite adelantar los trámites y procedimientos administrativos, el uso de registros electrónicos, de documentos públicos en medios electrónicos, notificaciones electrónicas, archivos electrónicos de documentos, expedientes electrónicos y sedes electrónicas. Lo anterior, con el fin de que los ciudadanos interactúen con validez jurídica y probatoria. Especialmente los artículos 59 al 64.

- Ley 1564 de 2012[26] Código General del Proceso Art. 103, el cual permite el uso de las TIC en todas las actuaciones de la gestión y trámites de los procesos judiciales con el fin de facilitar el acceso a la justicia.

---

[23] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “Ley 1341 de 2009”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.mintic.gov.co/portal/604/articles-3707_documento.pdf

[24] PRESIDENCIA DE LA REPÚBLICA. “Decreto 1727 de 2009”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1338429

[25] CONGRESO DE LA REPÚBLICA. “Ley 1437 de 2011”. Citado por el MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “Modelo de gestión de riesgos de seguridad digital” {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.mintic.gov.co/portal/604/articles-61854_documento.docx

[26] CONGRESO DE LA REPÚBLICA. “Ley 1564 de 2012”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1564_2012.html

- Ley 1581 de 2012[27] (Habeas data) en el cual se dictan disposiciones generales para la protección de datos. Esta ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada, sin embargo, a los datos financieros se les continúa aplicando la ley 1266 de 2008, excepto los principios.

- Decreto 1704 de 2012[28] (Interceptación legal de comunicaciones): Determina que la interceptación legal de comunicaciones es un mecanismo de seguridad pública que busca optimizar la labor de investigación de los delitos que adelantan las autoridades y organismos de inteligencia. De esta manera, se determina que los proveedores que desarrollen su actividad comercial en el territorio nacional deben implementar y garantizar en todo momento la infraestructura tecnológica necesaria que provea los puntos de conexión y de acceso a la captura del tráfico de las comunicaciones que cursen por sus redes, para que los organismos con funciones permanentes de policía judicial cumplan, previa autorización del fiscal general de la nación, con todas las labores inherentes a la interceptación de las comunicaciones requeridas.

- Decreto 2758 de 2012[29] (Modifica la estructura del Ministerio de Defensa): Se reestructura la organización del Ministerio de Defensa Nacional, en el sentido de asignar al despacho del viceministro la función de formular políticas y estrategias en materia de ciberseguridad y ciberdefensa. Adicionalmente, le encarga a la Dirección de Seguridad Pública y de Infraestructura, la función de implementar políticas y programas que mantengan la seguridad pública y protejan la infraestructura, así como hacerle seguimiento a la gestión relacionada con el riesgo cibernético en el sector defensa y diseñar el plan estratégico sectorial en materia de ciberseguridad y ciberdefensa.

---

[27] CONGRESO DE LA REPÚBLICA. “Ley 1581 de 2012”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

[28] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “Decreto 1704 de 2012”. Citado por el MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “Modelo de gestión de riesgos de seguridad digital” {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.mintic.gov.co/portal/604/articles-61854_documento.docx

[29] MINISTERIO DE DEFENSA NACIONAL. “Decreto 2758 de 2012”. Citado por el MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “Modelo de gestión de riesgos de seguridad digital” {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.mintic.gov.co/portal/604/articles-61854_documento.docx

- Decreto ley 019 de 2012[30]: (Entidades de certificación digital) Establece las siguientes actividades que las entidades de certificación acreditadas podrán realizar en el país, tales como: producir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas, emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles, y publicar certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la ley 527 de 1999, entre otras. Especialmente los Art. 70 y 71.

- Resolución SIC No. 76434 de 2012[31]: (Habeas data) Resolución expedida por la SIC, por medio de la cual se imparten instrucciones relativas a la protección de datos personales, en particular acerca del cumplimiento de la ley 1266 de 2008, sobre reportes de información financiera, crediticia, comercial de servicios y la proveniente de terceros países.

- Resolución 3933 de 2013[32] del Ministerio de Defensa Nacional: (Crea y organiza grupos internos de trabajo). Creó el Grupo ColCERT y asignó funciones a la dependencia de La Dirección de Seguridad Pública y de Infraestructura del Ministerio de Defensa Nacional respecto a promover el desarrollo de capacidades locales o sectoriales para la gestión operativa de los incidentes de ciberseguridad y ciberdefensa en las infraestructuras críticas nacionales, el sector privado y la sociedad civil.

- Ley estatutaria 1621 de 2013[33]: (Para la función de inteligencia y contrainteligencia en Colombia). Expide normas para fortalecer el marco jurídico

---

[30] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. “Decreto ley 019 de 2012”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: http://wsp.presidencia.gov.co/Normativa/Decretos/2012/Documents/Enero/10/Dec1910012012.pdf

[31] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Resolución SIC No. 76434 de 2012. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.sic.gov.co/sites/default/files/normatividad/Resolucion_76434_2012.pdf

[32] MINISTERIO DE DEFENSA NACIONAL. Resolución 3933 de 2013. Citado por el MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “Modelo de gestión de riesgos de seguridad digital” {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.mintic.gov.co/portal/604/articles-61854_documento.docx

[33] CONGRESO DE LA REPÚBLICA. “Ley estatutaria 1621 de 2013”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1621_2013.html

que permita a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir adecuadamente con su misión constitucional y legal.

- Decreto 0032 de 2013[34]: (Creación de la Comisión nacional digital y de información estatal) El Ministerio de Tecnologías de la Información y las Comunicaciones en cumplimiento de los lineamientos señalados en el documento CONPES 3701, creó, a través de este decreto, la Comisión Nacional Digital y de Información Estatal cuyo objeto es la coordinación y orientación superior de la ejecución de funciones y servicios públicos relacionados con el manejo de la información pública, el uso de infraestructura tecnológica de la información para la interacción con los ciudadanos y el uso efectivo de la información en el Estado colombiano.

- Decreto 1377 de 2013[35]. Reglamenta parcialmente la Ley 1581 de 2012. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

- CONPES 3701 del 2013[36] Lineamientos de política para ciberseguridad y ciberdefensa, el cual orienta a las entidades públicas y empresas privadas a implementar instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y ciberdefensa nacional.

- Ley 1712 de 2014[37] (Uso de las TIC). Regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantías del derecho y las excepciones a la publicidad de la información. Toda persona puede conocer sobre la existencia y acceder a la información pública en posesión o bajo control

[34] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “Decreto 0032 de 2013”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.mintic.gov.co/portal/604/articles-3602_documento.pdf

[35] MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. “Decreto 1377 de 2013”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: http://wsp.presidencia.gov.co/Normativa/Decretos/2013/Documents/JUNIO/27/DECRETO%201377%20DEL%2027%20DE%20JUNIO%20DE%202013.pdf

[36] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, REPÚBLICA DE COLOMBIA, DEPARTAMENTO NACIONAL DE PLANEACIÓN. “CONPES 3701 del 2013”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: mintic.gov.co/portal/604/articles-3602_documento.pdf

[37] CONGRESO DE LA REPÚBLICA. “Ley 1712 de 2014”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html

de los sujetos obligados. El acceso a la información solamente podrá ser restringido excepcionalmente.

- Circular externa SIC 02 del 3 de noviembre de 2015[38]. Datos personales y Registro Nacional de Bases de Datos (RNBD), donde se imparten instrucciones a los responsables del tratamiento de datos personales, personas jurídicas de naturaleza privada inscritas en las cámaras de comercio y sociedades de economía mixta, para efectos de realizar la inscripción de sus bases de datos en el Registro Nacional de Bases de Datos a partir del 9 de noviembre de 2015.
- Decreto 1078 de 2015[39] Decreto Único Reglamentario del sector TIC. Decreto Único Reglamentario del sector TIC. En particular las normas atinentes a la Estrategia de Gobierno en Línea.

- Decreto 415 de 2016[40] (Lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones). Se adiciona el decreto único reglamentario del sector de la función pública, decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones; Arts. 2.2.35.5; 2.2.35.6.

- Documento CONPES 3854 del 2016[41] de Política nacional de seguridad digital, el cual cita las instancias creadas para fortalecer la institucionalidad en el tema de ciberseguridad y ciberdefensa en Colombia y promueve la generación de

[38] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. “Circular externa SIC 02 del 3 de noviembre de 2015”. Citado por el MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “Modelo de gestión de riesgos de seguridad digital” {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.mintic.gov.co/portal/604/articles-61854_documento.docx

[39] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “Decreto 1078 de 2015”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.mintic.gov.co/portal/604/articles-9528_documento.pdf

[40] PRESIDENCIA DE LA REPÚBLICA. “Decreto 415 de 2016”. Citado por el MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “Modelo de gestión de riesgos de seguridad digital” {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.mintic.gov.co/portal/604/articles-61854_documento.docx

[41] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, REPÚBLICA DE COLOMBIA, DEPARTAMENTO NACIONAL DE PLANEACIÓN. “CONPES 3854 del 2016”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854_Adenda1.pdf

CSIRTS Sectoriales para la adecuada gestión de incidentes digitales en los diversos sectores de la economía.

4.4 MARCO ESPACIAL

Este proyecto se desarrolla en el continente americano, país Colombia, ciudad de Bogotá.

4.5 MARCO TECNOLÓGICO

- UNE 71502 La norma presenta un esquema de certificación que permite acreditar a las empresas en un proceso de mejoramiento continuo de sus indicadores de seguridad.

- ISO/IEC 15443 Define términos y establece un conjunto extenso y organizado de conceptos y sus relaciones para comprender el aseguramiento de la seguridad de TI.

- ISO/IEC 18014 Tecnología de la información. Técnicas de seguridad. Servicios de sellado de tiempo. Parte 4: Rastreabilidad de las fuentes de tiempo.

- ISO/IEC 27001 Norma principal de toda la serie. Incluye requisitos y controles (Anexo A) del SGSI.

- ISO 27002 Manual de buenas prácticas para implementar los controles de la norma ISO27001.

- ISO 27003 Manual para implementar un SGSI.

- ISO 27004 Incluye las técnicas de medida y las métricas para determinar la eficacia de un SGSI y los controles relacionados.

- ISO 27005 Directrices para gestionar los riesgos en la seguridad de la Información.

- ISO 27006 Requisitos para lograr la acreditación de las firmas u organizaciones de auditoría y para obtener la certificación del SGSI.

- ISO 27007 Manual de auditoría de un SGSI.

- ISO 27011 Guía de gestión de seguridad de la información específica para telecomunicaciones

- ISO 27031 Guía de continuidad de negocio basada en las tecnologías de la información y las comunicaciones.

- ISO 27032 Directrices de seguridad para el intercambio de información, el manejo de incidentes y aseguramiento de los procesos.

- ISO 27033 Visión general de seguridad de la red y de los conceptos asociados.

- ISO 37034 Guía de seguridad en aplicaciones.

- ISO 27035 Gestión de la información de incidentes de la seguridad.

- ISO / IEC TR 15446 Tecnología de la información. Técnicas de seguridad. Orientación para la producción de perfiles de protección y objetivos de seguridad.

- La Organización de Estados Americanos publicó en el 2016 un documento de Buenas Prácticas para establecer un CSIRT nacional.

- CONPES 3854 del 2016 de Política nacional de seguridad digital el cual cita las instancias creadas para fortalecer la institucionalidad en el tema de ciberseguridad y ciberdefensa en Colombia y promueve la generación de CSIRTS Sectoriales para la adecuada gestión de incidentes digitales para los diferentes sectores económicos.

5 METODOLOGÍA DE DESARROLLO DEL PROYECTO

Para el desarrollo del diseño de la documentación técnica para la empresa CIBERSECURITY de Colombia LTDA, el cual le permita llevar a cabo las actividades propias de un Centro de respuesta a incidentes cibernéticos en el ámbito de un CSIRT, se tendrán en cuenta las siguientes fases:

Fase 1. En esta fase se abordarán las actividades que permitirán dar cumplimiento al objetivo específico N° 1, relacionado con la identificación de las herramientas de hardware y software disponibles en el mercado tecnológico, requeridas para el desarrollo de las actividades del CSIRT, se desarrollarán las siguientes actividades:

- Recopilación de información relacionada con herramientas de software del CSIRT.
- Generación de cuadro informativo de herramientas de software del CSIRT.
- Relación de la tecnología de Hardware que permita desarrollar las actividades del CSIRT.

Fase 2. En esta fase se abordarán las actividades que permitirán dar cumplimiento al objetivo N° 2, relacionado con el diseño del mapa de la estructura tecnológica del CSIRT donde se puedan identificar las dependencias mínimas para el funcionamiento del CSIRT, se desarrollarán las siguientes actividades:

- Consulta de las dependencias necesarias para la implementación del CSIRT.
- Diseño del mapa de la estructura tecnológica del CSIRT.

Fase 3. En esta fase se abordarán las actividades que permitirán dar cumplimiento al objetivo específico N° 3, relacionado con la ejecución y documentación pruebas de cada una de las herramientas de software instaladas para verificar que éstas cumplen con los requerimientos para el laboratorio del CSIRT, se desarrollarán las siguientes actividades:

- Alistamiento del hardware seleccionado (repotenciar equipos existentes).
- Diseño lógico de laboratorio controlado y virtualización de las siguientes herramientas:
    - Servidor de Monitoreo
    - Correlacionador de Eventos
    - Servidor de Copias de Seguridad
    - Servidor Sandbox
- Ejecución y documentación de pruebas de software

6 RESULTADOS

6.1 FASE 1: DESARROLLO DEL OBJETIVO N° 1 – HERRAMIENTAS DE HARWARE Y SOFWARE - CSIRT

Este objetivo consiste en identificar las herramientas de hardware y software libre disponibles en el mercado tecnológico, requeridas para el desarrollo de las actividades del CSIRT.

6.1.1 Actividad N° 1 – Recopilación información herramientas

Esta actividad consiste en la recopilación de información detallada de las herramientas de software seleccionadas, a continuación, el desarrollo de la misma:

En la tabla 1 se presentan las especificaciones técnicas (funcionalidad/características, plataformas soportadas y recursos requeridos) para el servidor Apache:

Tabla 1. Herramienta CSIRT - Servidor Web

Nombre	Tipo de herramienta	Funcionalidades / Características	Plataformas soportadas	Recursos requeridos
Apache	Herramienta que presta servicios de servidor web HTTPS, gratuito y de código abierto	Su tarea es aceptar peticiones de páginas que provienen de usuarios que están accediendo a cualquier sitio web, gestionan la entrega o denegación del servicio de acuerdo con las políticas configuradas de acuerdo con los requerimientos propuestos por el dueño del sitio web. Aquí las tareas más comunes: • Atender las peticiones HTTPS incluyendo ejecuciones de multitarea ya que se puede dar el	Unix Microsoft Windows Macintosh	No aplica

Nombre	Tipo de herramienta	Funcionalidades / Características	Plataformas soportadas	Recursos requeridos
		caso de peticiones al mismo tiempo o simultaneas, peticiones complejas como acceso a bases de datos. • Atender las peticiones HTTPS incluyendo ejecuciones de multitarea ya que se puede dar el caso de peticiones al mismo tiempo o simultaneas, peticiones complejas como acceso a bases de datos. • Restringir el acceso no autorizado a los archivos, gestión de autenticaciones de usuarios o filtrado de peticiones según sea su origen. • Gestionar errores por páginas no encontradas. Informa al usuario para luego redireccionarlo a páginas predeterminadas. • Administrar la información a transmitir de acuerdo con su formato para luego informar de manera adecuada al navegador que está solicitando dicho recurso. • Gestiona los logs (almacena las peticiones que recibe), errores que se producen y toda la información que puede ser registrada para luego ser analizada. • Permite la configuración de hosting virtual que se basa en IPs o DNS, donde se pueden alojar varios sitios web en el mismo servidor. Permite establece distintos niveles de control de acceso a la información como el soporte a cifrado SSL utilizando protocolo seguro HTTPS.		

Fuente: ECURED. “Servidor HTTP Apache”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.ecured.cu/Servidor_HTTP_Apache
Arsys. “Cómo crear un Servidor Cloud para gestionar el correo electrónico con Zimbra”. {En línea}. 27 de enero de 2016. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.arsys.es/blog/soluciones/cloud/cloud-computing/crear-servidor-cloud-gestionar-correo-electronico-zimbra/
DIGITAL LEARNING. “¿Qué hace un Servidor Web como Apache? Configuración”. {En línea}. 17 de marzo de 2012. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.digitallearning.es/blog/apache-servidor-web-configuracion-apache2-conf/
WIKIPEDIA. “Servidor HTTP Apache”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://es.wikipedia.org/wiki/Servidor_HTTP_Apache

En la tabla 2 se presentan las especificaciones técnicas (funcionalidad/características, plataformas soportadas y recursos requeridos) para el servidor de correo Zimbra:

Tabla 2. Herramienta CSIRT - Servidor correo institucional

Nombre	Tipo de herramienta	Funcionalidades / Características	Plataformas soportadas	Recursos requeridos
Zimbra	Servidor de correo institucional	Zimbra conecta a la gente y la información a través de programas de colaboración unificados tales como correo electrónico, gestión de agenda, contactos, tareas, uso compartido de archivos, diálogo en línea (chat) y el video chat. Cuenta con una interfaz fácil e intuitiva. Cuenta con aliados estratégicos como Intel, Red Hat, Novell, Apple, HP. Se presenta en dos versiones: versión libre en la que colabora la comunidad de Software Abierto –que incluye Partners-; y versión comercial (Zimbra Network) que parte de la libre e incluye servicios y	Unix Microsoft Windows Macintosh	Para entornos de evaluación (50 cuentas): CPU Intel/AMD de 32bits a 1.5 GHz o superior. 1 GB de RAM.

Nombre	Tipo de herramienta	Funcionalidades / Características	Plataformas soportadas	Recursos requeridos
		funcionalidades profesionales (soporte y mantenimiento). Ventajas: Flexibilidad: puede ser personalizado de acuerdo con las particularidades empresariales. Libertad: puede usarse con otros programas tradicionales. Estable y confiable. Bajo mantenimiento: cuenta con una interfaz gráfica simple e intuitiva. Compatible con herramientas de escritorio: sincronización entre ZCS y Microsoft Outlook, Thunderbird, Apple Mail, Libreta de direcciones e iCal. Soporte a IMAP/POP.		5 GB de espacio libre en disco para software y logs. Espacio adicional para el almacenamiento del correo y las bases de datos. Para más de 2000 cuentas de usuario: CPU de 64 bits, RAM mínimo 4 GB. Se recomiendo usar discos SCSI.

Fuente: INTERNET YA. “Beneficios de un servidor de correo Zimbra para entidades en Colombia”. {En línea}. Abril 10 de 2019. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.internetya.co/beneficios-de-un-servidor-de-correo-zimbra-para-entidades-en-colombia/

ZIMBRA, A SYNACOR PRODUCT. “Zimbra” {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.zimbra.com/
GÓMEZ PARADELA, Carlos Alberto; MARTÍNEZ GÓMEZ, Mario Tomás. “Manual Instalación Zimbra 6.x.x en Debian Lenny”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://gutl.jovenclub.cu/wiki/doku.php?id=/manuales:zimbra

En la tabla 3 se presentan las especificaciones técnicas (funcionalidad/características, plataformas soportadas y recursos requeridos) para el gestor de contenidos WordPress:

Tabla 3. Herramienta CSIRT - Servidor intranet

Nombre	Tipo de herramienta	Funcionalidades / Características	Plataformas soportadas	Recursos requeridos
Wordpress	WordPress es un sistema de gestión de contenidos que permite mantener un blog	• Es open source, por lo que brinda la posibilidad de acceder a una comunidad de conocimiento de ésta. • Modificable ya que cuenta con plantillas que se pueden agregar a través de plugins. • Permite agregar archivos de multimedia. • Configurable en múltiples idiomas. • Se integra a las redes sociales. • Es multidispositivo. • Diseños modernos y atractivos a través de sus plantillas. • Actualizaciones automáticas y login sencillo.	Linux Server Windows Server	• PHP 5.2.4 o superior • MySQL 5.0.15 o superior • Se recomienda tener el módulo Apache mod_rewrite • Se recomienda que el hosting

Nombre	Tipo de herramienta	Funcionalidades / Características	Plataformas soportadas	Recursos requeridos
				corra en Linux.

Fuente: GIZTAB. “Características principales y primeros pasos”. {En línea}. Septiembre 9 de 2018. {Consultado el 29 de noviembre de 2019}. Disponible en: ttps://www.giztab.com/wordpress-caracteristicas-principales-y-primeros-pasos/
WORDPRESS. “Cuáles son los requerimientos de un servidor para instalar WordPress”. {En línea}. Agosto 14 de 2014 {Consultado el 29 de noviembre de 2019}. Disponible en: http://wordpress.comocreartuweb.com/cuales-son-los-requerimientos-de-un-servidor-para-instalar-wordpress-511.html.

En la tabla 4 se presentan las especificaciones técnicas (funcionalidad/características, plataformas soportadas y recursos requeridos) para el servidor de archivos Samba:

Tabla 4. Herramienta CSIRT - Servidor de archivos

Nombre	Tipo de herramienta	Funcionalidades / Características	Plataformas soportadas	Recursos requeridos
Linux Samba	Servidor de archivos	Programado en: C++, Python y C. Permite compartir archivos e impresoras con PC que utilizan Windows y otros sistemas operativos. Es una suite con aplicaciones Unix que implementa el protocolo SMB (Server Message Block). Comparte diversos sistemas de archivos, impresoras instaladas y configuradas en el servidor y en estaciones de trabajo. Cuenta con un visor de clientes en red, lo que permite la interacción entre usuarios. Permite la autenticación contra un dominio Windows.	Linux Server, OpenVMS, macOS y Unix-like	Requisitos mínimos: Servidor a 250 MHz, 16 GB RAM 120 GB disco duro Requerimientos software: Es necesario contar con los

Nombre	Tipo de herramienta	Funcionalidades / Características	Plataformas soportadas	Recursos requeridos
		Proporciona un servidor de resolución de nombres WINS. Cuenta con dos demonios encargados de gestionar los recursos compartidos: smbd y nmbd. Beneficios: • Seguridad: Protección a través de permisos y contraseñas por usuario sobre un directorio compartido. Dispone de dos modos de seguridad denominados share (contraseña asociada al recurso) y user (el cliente se autentica con un usuario y contraseña para acceder a los recursos de Samba). • Administrable. • Comparte recursos entre sistemas operativos diferentes (Windows y Linux) sin inconveniente.		siguientes paquetes: • samba • samba-client • samba-common • samba-swat • xinetd

Fuente: LIKE GEEKS. “Servidor De Archivos Linux Usando Samba.” {En línea}. 27 de marzo de 2017. {Consultado el 29 de noviembre de 2019}. Disponible en: https://likegeeks.com/es/servidor-de-linux-samba/.

SERVIDOR SAMBA: “conceptos y configuración rápida”. {En línea} 25 de marzo de 2017. {Consultado el 29 de noviembre de 2019} https://www.profesionalreview.com/2017/03/25/servidor-samba-conceptos-y-configuracion-rapida/

CLARET INFORMATICA 2º DE ASIR. “Requisitos necesarios para instalar SAMBA en un sistema Linux”. {En línea}. 24 de enero 24 de 2014. {Consultado el 29 de noviembre de 2019}. Disponible en: http://claretinformaticaasir.blogspot.com/2014/01/requisitos-necesarios-para-instalar.html

En la tabla 5 se presentan las especificaciones técnicas (funcionalidad/características, plataformas soportadas y recursos requeridos) para el servidor de copias de respaldo Bacula:

Tabla 5. Herramienta CSIRT - Servidor copias de seguridad

Nombre	Tipo de herramienta	Funcionalidades / Características	Plataformas soportadas	Recursos requeridos
Bacula	Bacula Enterprise es un software de backup Open Source profesional para su infraestructura de IT.	• Está en la capacidad de realizar respaldos a estaciones de trabajo y servidores con plataformas GNU/Linux, Windows y Mac OS. • Cumple con los niveles de respaldo de la información lo que le permite generar backup completos, Incrementales, diferenciales • Está en la capacidad de realizar respaldos en todo tipo de soportes (librerías de cintas y cabinas de discos) • Soporte VSS en Windows: Permite realizar copia de archivos, aunque estos estén en uso	Windows, Linux, MacOS	SISTEMA OPERATIVO: Ubuntu Server, Windows Server RAM: 8 Gb RAM PROCESADOR: Pentium IV DISCO DURO: 1 Tb

Fuente: RODRÍGUEZ, Marcos. “BACULA BACKUP: Instalación del servidor”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://vivaubuntu.com/bacula-backup-instalacion-del-servidor
ULTIMOBYTE. “BACULA, OPEN SOURCE BACKUP”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.ultimobyte.es/productos/bacula-enterprise-open-source-backup
RODRÍGUEZ, Marcos. “BACULA BACKUP: Instalación del servidor”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://vivaubuntu.com/bacula-backup-instalacion-del-servidor/

En la tabla 6 se presentan las especificaciones técnicas (funcionalidad/características, plataformas soportadas y recursos requeridos) para el servidor DNS OpenDSN:

Tabla 6. Herramienta CSIRT - Servidor DNS

Nombre	Tipo de herramienta	Funcionalidades / Características	Plataformas soportadas	Recursos requeridos
OpenDNS	Servidor DNS	• Es gratuito y abierto. • Es una alternativa al servidor de DNS de su ISP para la resolución de nombres a empresas. • Por estar estratégicamente localizados mantiene en su memoria caché gran cantidad de nombres de dominio, permitiendo que las consultas a los DNS sean muy rápidas, incrementando la velocidad de respuesta. • Incluye filtros de phishing y corrección de errores ortográficos. • Realiza el bloqueo a sitios maliciosos. • Cuenta con accesos directos y control parental.	Linux Server, Windows Server y Mac	No aplica

Fuente: DESDELINUX. “OpenDNS: servidor DNS para navegar más rápido y seguro en Internet”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://blog.desdelinux.net/opendns-servidor-dns-para-navegar-mas-rapido-y-seguro-en-internet/

SEAQ SERVICIOS SAS. “Nagios es una Herramienta Open source de monitoreo”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.seaq.co/nagios.html

COLTRIN, Jason. “Integrate OpenDNS Umbrella with Active Directory”. {En línea}. 5 de septiembre de 2016. {Consultado el 29 de noviembre de 2019}. Disponible en: https://4sysops.com/archives/integrate-opendns-umbrella-with-active-directory/

En la tabla 7 se presentan las especificaciones técnicas (funcionalidad/características, plataformas soportadas y recursos requeridos) para el servidor de monitoreo Nagios:

Tabla 7. Herramienta CSIRT - Herramienta de monitoreo

Nombre	Tipo de herramienta	Funcionalidades / Características	Plataformas soportadas	Recursos requeridos
Nagios	Software para monitoreo hosts (Servidores, redes, routers, Switches)	Esta herramienta realiza seguimiento a los hosts de toda la infraestructura tecnológica de la organización identificando problemas críticos y en tiempo real. • Realiza monitoreo a la red (SMTP, POP3, HTTP, NNTP, ICMP, SNMP, FTP, SSH). • Monitorea la carga del procesador, uso de disco, los registros del sistema de los servidores. • Supervisa equipos remotamente: Por medio de túneles SSL cifrados o SSH. • Notifica a contactos: informa de la caída de un servicio y cuando éste se restablece. • A través de la interfaz web se puede observar el estado de los hosts y la red en tiempo real con la opción de generar informes sobre el comportamiento de lo que se está monitoreando. • Gran variedad de plugins que facilita la labor de los usuarios en la creación de informes con gráficos y seguimiento de acuerdo con los requerimientos. • Cuando un servicio presenta problemas las notificaciones se envían al usuario encargado de las redes o a quien disponga el encargado de gestionar la red. Estas notificaciones se pueden	GNU/Linux, variantes de Unix	Apache 2 PHP Compiler and developmen t libraries Developme nt libraries

Nombre	Tipo de herramienta	Funcionalidades / Características	Plataformas soportadas	Recursos requeridos
		configurar para que se envíen mediante correo electrónico o SMS.		

Fuente: Fuente: NORTH NETWORKS. “Que es Nagios?”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.north-networks.com/fabricante/que-es-nagios/
SYSADM.ES. “Instalación y configuración de Nagios”. {En línea}. Abril 23 de 2018. {Consultado el 29 de noviembre de 2019}. Disponible en: https://sysadm.es/instalacion-y-configuracion-de-nagios/
ROMERO GONZÁLEZ, Rafael. “Instalación y configuración de nagios core 4.0.4.” {En línea}. Junio de 2015. {Consultado el 29 de noviembre de 2019}. Disponible en: https://exchange.nagios.org/components/com_mtree/attachment.php?link_id=6527&cf_id=24

En la tabla 8 se presentan las especificaciones técnicas (funcionalidad/características, plataformas soportadas y recursos requeridos) para el servidor Sandbox Firejail:

Tabla 8. Herramienta CSIRT - Servidor sandbox

Nombre	Tipo de herramienta	Funcionalidades / Características	Plataformas soportadas	Recursos requeridos
Firejail	Servidor Sandbox	Es un programa SUID (S et propietario U Ser ID tras la ejecución, es un tipo especial de permisos de archivo que permite que el programa se ejecute como root, en lugar del usuario que inició el programa) Escrito en C. Gracias a su kernel permite que cada proceso tenga su propia vista privada. Firejail está en la capacidad de ejecutar cualquier proceso: sesiones de usuarios, servidores Linux y aplicaciones con alto componente gráfico.	Su ejecución se realiza en todas las computadoras Linux con una versión de kernel 3.x o posterior.	Información no disponible

Nombre	Tipo de herramienta	Funcionalidades / Características	Plataformas soportadas	Recursos requeridos
		Esta herramienta cuenta con perfiles de seguridad para la gestión de programas configurados en Gnu/Linux: Mozilla Firefox, Chromium, VLC, Transmisión, etc Todas las características de seguridad de Firejail se implementan dentro del kernel de Linux. El programa sandbox configura el kernel y se va a dormir. La configuración es muy rápida, generalmente decenas de milisegundos. En configuraciones muy complicadas puede llegar hasta 1 segundo. Los requisitos de memoria son bajos, todo lo que necesita es unos pocos MB de memoria. Características: Debido a su peso permite la ejecución de programas a la misma velocidad dentro y fuera de Sandbox. Al momento de arrancar el computador solo se cargan los procesos necesarios en la memoria, solo se consumen recursos al momento de cargar un programa en el servidor Sandbox; éstos no tienen dependencias por lo cual solo se instalan los paquetes necesarios requeridos por el sistema. Muy fácil de usar. Fragmentación de procesos: los programas que se encuentran en ejecución los oculta de mamera automática. Se cuenta con soporte para diferentes sistemas de archivos: local, overlay y system chroot.		

Nombre	Tipo de herramienta	Funcionalidades / Características	Plataformas soportadas	Recursos requeridos
		Modo privado, donde aísla el directorio del usuario /home, de procesos en ejecución en el sandbox creando un sistema de archivos temporal. Perfiles de seguridad: la configuración de los perfiles de seguridad se realiza de manera sencilla en el sistema de archivos. Soporte para redes: con el firejail se pueden usar interfaces TCP/IP en programas en ejecución. Se usa para establecer DMZ y para la configuración de redes temporales. Espacios de nombres de Linux Filtros de seguridad Asignación de recursos Formatos de embalaje universal Auditoría de caja de arena Estadísticas y monitoreo Interfaz gráfica del usuario		

Fuente: Firejail Security Sandbox. “Firejail Usage”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://firejail.wordpress.com/documentation-2/basic-usage/

WORDPRESS. “Firejail security sandbox”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://firejail.wordpress.com/features-3/

HARDLIMIT. “Firejail, Un sandbox universal para Linux”. {En línea}. 20 de febrero de 2015. {Consultado el 29 de noviembre de 2019}. Disponible en: https://hardlimit.com/firejail-un-sandbox-universal-para-linux/

AMOEDO, Damián. “Ubunlog. Firejail, ejecuta de forma segura aplicaciones no confiables en Ubuntu”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://ubunlog.com/firejail-ejecuta-aplicaciones-ubuntu/

GEEKLAND. “Firejail, un sandbox para Linux para ejecutar programas de forma segura”. {En línea}. 4 de septiembre de 2017. {Consultado el 29 de noviembre de 2019}. Disponible en: https://geekland.eu/firejail-sandbox-para-linux/

En la tabla 9 se presentan las especificaciones técnicas (funcionalidad/características, plataformas soportadas y recursos requeridos) para la herramienta de correlación de eventos Snort:

Tabla 9. Herramienta CSIRT - Herramienta de correlación de eventos

Nombre	Tipo de herramienta	Funcionalidades / Características	Plataformas soportadas	Recursos requeridos
Snort	Sistema de detección de intrusos en la red	Tiene un motor de detección de ataques y escaneo de puertos. Registra, alerta y responde a anomalías asociadas a patrones de ataque, en tiempo real. Dispone filtros o patrones ya predefinidos; esto es, las reglas proporcionadas por Snort son los patrones de ataque definidos. Cuando identifica nuevos ataques distribuye los patrones asociados para permitir su detección posterior. Recibe actualizaciones constantes según los informes generados a través de boletines de seguridad. Puede escanear paquetes que entran/salen, dentro del Firewall, fuera del Firewall. El lugar ideal para ubicar Snort es detrás del firewall, para que analice sobre el tráfico de internet toda la información entrante. Snort tiene la capacidad de funcionar como un sniffer permitiendo verificar los registros en tiempo real de todo el tráfico que está pasando por la red, también actúa como registro de paquetes permitiendo guardar en archivos los logs para ser analizados después, y también funciona como un IDS, lo que significa que cuando un paquete está coincidiendo con un patrón configurado en las reglas esto hace que cuando	Linux, Windows	Linux, Openbsd, MacOS, Windows IRIX

Nombre	Tipo de herramienta	Funcionalidades / Características	Plataformas soportadas	Recursos requeridos
		suceda un ataque saber cuándo se produjo y como sucedió. Si encuentra una conexión con tráfico malicioso puede darla de baja (envía paquete con flag: RST activa).		

Fuente: SNORT.ORG. “Snort”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.snort.org/

ECURED. “Snort”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.ecured.cu/Snort

ORTEGO DELGADO, Daniel. “Qué es Snort: Primeros pasos”. {En línea}. 21 de marzo de 2017. {Consultado el 29 de noviembre de 2019}. Disponible en: https://openwebinars.net/blog/que-es-snort/

En la tabla 10 se presentan las especificaciones técnicas (funcionalidad/características, plataformas soportadas y recursos requeridos) para el servidor de gestión de requerimientos e incidentes GLPI:

Tabla 10. Herramienta CSIRT - Gestor de incidentes

Nombre	Tipo de herramienta	Funcionalidades / Características	Plataformas soportadas	Recursos requeridos
GLPI	Registro y seguimiento de incidentes	Cuenta con una interfaz para la administración del inventario informático y con un sistema para la gestión de requerimientos. Fue desarrollada para ambientes Apache-PHP, MySQL Su instalación es sencilla, su manejo permite administrar el soporte y mantenimiento de las organizaciones de manera ágil y simple. Su despliegue y puesta en producción son sencillos. Se puede configurar con el directorio LDAP por lo cual se puede sincronizar las credenciales con el LDAP. Su interfaz permite la administración de solicitudes de requerimientos de todo tipo ya que cuenta con una interfaz para configurar diferentes tipos de solicitudes y requerimientos. Una vez creado el caso se envía un correo al usuario que hizo la solicitud con la información del requerimiento (número	Windows, LinuxServer, MacOS	GLPI usa: PHP MySQL versión mayo o igual a 4.23 HTML CSS CSV, PDF y SLK AJAX SVG y PNG Web Server Prerrequisitos: Apache 2 o superior (http://httpd.apache.org) Microsoft IIS (http://www.iis.net). PHP versión 5.3 o inferior (http://www.php.net).

Nombre	Tipo de herramienta	Funcionalidades / Características	Plataformas soportadas	Recursos requeridos
		asignado, técnico asignado y tiempo en resolver el caso). Cuenta con platillas para tickets para solicitudes, incidentes, soluciones y tareas. Cuenta con una base de conocimiento enlazado con los tickets. Genera formatos configurables de acuerdo con las necesidades. Debido a sus reglas complejas permite un flujo de trabajo automático. Permite la gestión de acuerdo de niveles de servicio, objetivo de nivel de servicio, y acuerdo de nivel operacional. Permite configurar encuesta de satisfacción de acuerdo con las necesidades de la organización para luego cerrar el ticket.		

Fuente: ECURED. “GLPI”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.ecured.cu/GLPI

LANCHEROS PADILLA, Lizeth Katherine. “Implementación de la herramienta de software libre GLPI para sistematizar la mesa de ayuda (help desk) del hospital infantil Universitario de San José”. {En línea}. 2016. {Consultado el 29 de noviembre de 2019}. Disponible en: https://repository.libertadores.edu.co/bitstream/handle/11371/1339/lancheroslizath2016.pdf?sequence=1

En la tabla 11 se presentan las especificaciones técnicas (funcionalidad/características, plataformas soportadas y recursos requeridos) para la herramienta de análisis forense Autopsy:

Tabla 11.Herramienta CSIRT - Herramienta informática forense

Nombre	Tipo de herramienta	Funcionalidades / Características	Plataformas soportadas	Recursos requeridos
Autopsy	Informática Forense	Cuenta con una interfaz gráfica intuitiva Realiza auditorías forenses no intrusivas. Analiza sistemas de archivos, discos con sistemas operativos windows y unix, archivos en formatos NTFS, FAT, UFS1 / 2, Ext2 / 3. Los resultados se despliegan en un solo árbol. Incluye módulos básicos y otros que se pueden adquirir de terceros. Visualiza los eventos en el tiempo. Hash Filtering: identifica archivos conocidos que presentan defectos. Realiza búsquedas indexadas. Artefactos web: muestra el historial, los marcadores y las cookies de Firefox, Chrome e IE. Multimedia: extrae EXIF de imágenes y videos. Indicadores de compromiso. Ejecuta tareas en segundo plano en paralelo utilizando múltiples núcleos y proporciona los resultados tan pronto como se encuentran.	Mac, Solaris, Open & FreeBSD y Linux.	Remover o deshabilitar cualquier software antivirus. La versión de 64 bits de Autopsy requiere un mínimo de 8 GB de RAM (se recomiendan 16 GB). Cuando se instala la versión de 64 bits de Autopsy en Windows, se limitará a un tamaño de almacenamiento dinámico máximo de 4 GB, dejando la memoria

Nombre	Tipo de herramienta	Funcionalidades / Características	Plataformas soportadas	Recursos requeridos
				restante para el sistema operativo, el servicio interno de indexación de texto Solr y otras aplicaciones. Si se desea cambiar el tamaño máximo de almacenamiento dinámico, puede hacerlo después de la instalación cambiando el valor de Memoria máxima de JVM en la sección Tiempo de ejecución en Herramientas -> Opciones -> Aplicación.

Fuente: SLEUTHKIT. “autopsy User Documentation”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://sleuthkit.org/autopsy/docs/user-docs/4.8.0/installation_page.html

AUTOPSY DIGITAL FORENSICS. “Online Autopsy Forensics Tool Training”. {En línea}. 26 de junio de 2014. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.autopsy.com/online-autopsy-forensics-tool-training-sept-24-2014/

En la tabla 12 se presentan las especificaciones técnicas (funcionalidad/características, plataformas soportadas y recursos requeridos) para la herramienta de análisis forense Access Data FTK Imager:

Tabla 12. Herramienta CSIRT - Complementaria informática forense

Nombre	Tipo de herramienta	Funcionalidades / Características	Plataformas soportadas	Recursos requeridos
Access Data FTK Imager	Informática Forense	FTK proporciona búsquedas y filtros de archivos ubicando fácilmente una evidencia. De fácil uso. Contiene 270 formatos de archivos que pueden ser consultados fácilmente desde un explorador. Permite generar logs e informes. Ofrece compatibilidad con otras herramientas forenses. Realiza búsquedas avanzadas sobre imágenes y textos en Internet. Recupera archivos y particiones borradas de un disco de manera automática. Realiza el análisis de emails y archivos comprimidos. Otras funcionalidades: Clona discos, valida la integridad criptográfica de las evidencias, visualiza información del sistema, presenta imágenes en vivo, recupera contraseñas, recupera correos borrados, realiza el análisis forense en navegadores, analiza discos IDE y SATA, repara sectores de discos	Debian, Ubuntu, Fedora, Windows, Red Hat, Mac OS	

Nombre	Tipo de herramienta	Funcionalidades / Características	Plataformas soportadas	Recursos requeridos
		defectuosos, repara particiones dañadas, recupera información dañada por virus, recupera imágenes ocultas.		

Fuente: ACCESS DATA. “LIT FTK specification guide 6.3”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://support.accessdata.com/hc/en-us/article_attachments/360004988813/LIT_FTK_specification_guide_6.3.pdf
ACCESS DATA. “Imager User Guide”. {En línea}. 31 de marzo de 2016 {Consultado el 29 de noviembre de 2019}. Disponible en: https://ad-pdf.s3.amazonaws.com/Imager/3_4_3/FTKImager_UG.pdf

En la tabla 13 se presentan las especificaciones técnicas para los dispositivos de conectividad:

Tabla 13. Dispositivos de conectividad para un CSIRT

Dispositivos de conectividad	
Nombre del dispositivo	**Descripción**
Router ZTE 660	Es uno de los más grandes proveedores global en cuanto al equipamiento de telecomunicaciones y soluciones en redes.
Cableado: Marca Utp Cat6 Patch Cord	Cable De Red - Buy Utp Cat6, Cat6 Patch Cord, Cat6 Cable.

Dispositivos de conectividad	
Nombre del dispositivo	**Descripción**
Tarjeta de Red: Intel(R) Centrino(R) Wireless-N 1000	Tarjeta de Red Qualcomm Atheros AR8151 PCI-E Gigabit Ethernet Controller (NDIS 6.30) (192. [TRIAL VERSION])
	Tarjeta de Red VirtualBox Host-Only Ethernet Adapter (192. [TRIAL VERSION])
	Tarjeta de Red VMware Virtual Ethernet Adapter for VMnet1 (192. [TRIAL VERSION])
	Tarjeta de Red VMware Virtual Ethernet Adapter for VMnet8 (192. [TRIAL VERSION])
Proveedor de Internet:	Empresa de telecomunicaciones de Bogotá (ETB)

Fuente: Los autores.

6.1.2 Actividad N° 2 – Cuadro informativo herramientas de software CSIRT

Esta actividad comprende la generación del cuadro informativo de herramientas de software para el CSIRT. Para ello, se presenta en la tabla 14 dos opciones para los diferentes tipos de herramientas de software y la herramienta propuesta para este proyecto:

Tabla 14. Opciones herramientas Open Source para un CSIRT

Tipo de herramienta	Opción 1	Opción 2	Herramienta propuesta
Servidor web	Apache	Jboss	Apache
Servidor de correo institucional	Zimbra	Roundcube	Zimbra
Servidor de intranet	Wordpress	Drupal	Wordpress
Servidor de archivos	Linux Samba	Windows Server	Linux Samba
Servidor de copias de seguridad	Bacula	Uranium Backup Free	Bacula
Servidor DNS	OpenDNS	Quad9	OpenDNS
Servidor de monitoreo	Nagios	Zabbix	Nagios
Servidor sandbox	Firejail	Glimpse	Firejail
Correlacionador de eventos	OSSEC	Snort	Snort
Registro y seguimiento de incidentes	OSTicket	GLPI	GLPI
Informática forense	FTK	Autopsy	Autopsy y FTK
Dispositivos de conectividad	Ver Tabla N° 13 “Dispositivos de conectividad para un CSIRT”		

Fuente: Los autores

6.1.3 Actividad N° 3 – Cuadro informativo herramientas de hardware CSIRT

Esta actividad comprende la relación de las especificaciones técnicas para la tecnología de Hardware que permita desarrollar las actividades del CSIRT. Para esto, se presenta en la tabla 15 la tecnología de hardware propuesta para el CSIRT, que incluye la configuración básica, la herramienta de virtualización, el sistema operativo, la memoria, el procesador y la capacidad de almacenamiento por servidor:

Tabla 15. Tecnología Hardware para el CSIRT

Servidor físico	Configuración	Herramienta virtualización	Servidor Virtual	Sistema Operativo	Memoria (GB)	Procesador (CPU)	Almacenamiento
Servidor1	100 GB RAM Procesador Intel Core i9 8 núcleos 16 subprocesos 4.40 GHTz Almacenamiento: 4 TB Linux CentOS Server	Virtualbox	Servidor Web [42]	Linux	Min 64 MB o más	Pentium o más	50 MB
			Servidor de Correo Institucional [43]	Linux	Mínimo 8GB de RAM o más	2 GHZ, CPU 64-bit o más	10 GB de espacio en disco o más

[42] ECURED. “Servidor HTTP Apache”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.ecured.cu/Servidor_HTTP_Apache

[43] ARSYS. “Cómo crear un Servidor Cloud para gestionar el correo electrónico con Zimbra”. {En línea}. 27 de enero de 2016. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.arsys.es/blog/soluciones/cloud/cloud-computing/crear-servidor-cloud-gestionar-correo-electronico-zimbra/

Servidor físico	Configuración	Herramienta virtualización	Servidor Virtual	Sistema Operativo	Memoria (GB)	Procesador (CPU)	Almacenamiento
Servidor2	100 GB RAM Procesador Intel Core i9 8 núcleos 16 subprocesos 4.40 GHTz Almacenamiento: 4 TB Linux CentOS Server	Virtualbox	Servidor de Intranet [44]	Linux	2 GB de RAM	Un núcleo o más	20 GB o más
			Servidor de Archivos (Linux Samba)[45]	Linux	256 MB	250 Mhz	8 GB
			Servidor de Copias de Seguridad [46]	Linux	8 GB de RAM o más	Pentium IV o más	1 Tb
			Servidor DNS (OpenDNS) [47]	Linux	1.5 GB	4 CPU cores	7 GB
			Servidor de Monitoreo [48]	Linux	2 GB de RAM	Procesador de 2+ GHz	40 GB HD

[44] WORDPRESS. “Cuáles son los requerimientos de un servidor para instalar WordPress”. {En línea}. Agosto 14 de 2014 {Consultado el 29 de noviembre de 2019}. Disponible en: http://wordpress.comocreartuweb.com/cuales-son-los-requerimientos-de-un-servidor-para-instalar-wordpress-511.html

[45] CLARET INFORMATICA 2º DE ASIR. “Requisitos necesarios para instalar SAMBA en un sistema Linux”. {En línea}. 24 de enero 24 de 2014. {Consultado el 29 de noviembre de 2019}. Disponible en: http://claretinformaticaasir.blogspot.com/2014/01/requisitos-necesarios-para-instalar.html.

[46] RODRÍGUEZ, Marcos. “BACULA BACKUP: Instalación del servidor”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://vivaubuntu.com/bacula-backup-instalacion-del-servidor

[47] COLTRIN, Jason. “Integrate OpenDNS Umbrella with Active Directory”. {En línea}. 5 de septiembre de 2016. {Consultado el 29 de noviembre de 2019}. Disponible en: https://4sysops.com/archives/integrate-opendns-umbrella-with-active-directory/

[48] ECURED. “Nagios”. {En línea}. {Consultado el 17 de mayo de 2020}. Disponible en: https://www.ecured.cu/Nagios

Servidor físico	Configuración	Herramienta virtualización	Servidor Virtual	Sistema Operativo	Memoria (GB)	Procesador (CPU)	Almacenamiento
			Servidor Sandbox (Firejail) [49]	Linux	2 GB de RAM	Intel Core 2 Duo T5200	2 GB
			Correlacionador de Eventos (Snort) [50]	Linux	4GB	2 Core	20 GB
			Registro y seguimiento de Incidentes [51]	Linux	4 GB de RAM	2.5 Ghz, un núcleo o más	26 GB HD
			Informática Forense (Autopsy) [52]	KaliLinux	8 GB	3 GHtz	10 GB

[49] PCGAMEBENCHMARK. “Universe Sandbox System Requirements”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.pcgamebenchmark.com/universe-sandbox-system-requirements

[50] SÁNCHEZ LORENTE, Olga. Detección de intrusiones con SNORT. {En línea}. Junio de 2015. {Consultado el 17 de mayo de 2020}. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/43090/6/osanchezloTFM0715memoria.pdf

[51] ECURED. “GLPI”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.ecured.cu/GLPI

[52] SLEUTHKIT. “autopsy User Documentation”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://sleuthkit.org/autopsy/docs/user-docs/4.8.0/installation_page.html

Servidor físico	Configuración	Herramienta virtualización	Servidor Virtual	Sistema Operativo	Memoria (GB)	Procesador (CPU)	Almacenamiento
			Informática Forense (FTK) [53]	KaliLinux	8 GB	4 cores	500 MB

Fuente: Los autores

[53] ACCESS DATA. “LIT FTK specification guide 6.3”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://support.accessdata.com/hc/en-us/article_attachments/360004988813/LIT_FTK_specification_guide_6.3.pdf

6.2 FASE 2: DESARROLLO DEL OBJETIVO N° 2 – MAPA ESTRUCTURA TECNOLÓGICA CSIRT

Este objetivo consiste en diseñar el mapa de la estructura tecnológica del CSIRT donde se puedan identificar las dependencias mínimas para el funcionamiento del CSIRT.

6.2.1 Actividad N° 1 – Dependencias para la implementación de un CSIRT

Esta actividad comprende la consulta de las dependencias necesarias para la implementación del CSIRT.

Se propone un espacio físico disponible para el CSIRT de aproximadamente 120 m^2, dividido en áreas.

A continuación, la descripción de cada una de estas áreas o dependencias[54]:

1) **Centro de Datos:** el centro de datos será un espacio donde se alojan servidores para el almacenamiento, gestión y protección de la información. De acuerdo con lo anterior, se deberán aplicar los siguientes controles de seguridad:

   - Seguridad física:

     - Control de accesos: Validar la entrada mediante tarjetas personales, con sistemas más exhaustivos como los biométricos o incluso ambos.
     - Vigilancia: Zonas exteriores e interiores bien vigiladas por el personal de seguridad y circuito cerrado de televisión.
     - Climatización de los servidores: es importante contar con aires acondicionados, sensores de temperatura y humedad y la monitorización periódica de éstos.
     - Protección contra incendios: Contar con equipos contra incendios acordes a las necesidades del Data center.
     - Sistemas de alimentación alternos (UPS, planta eléctrica).

   - Seguridad lógica:

     - DCIM: Monitorización a tiempo real.
     - Gestión de riesgos.
     - Segmentación de redes y equipos críticos.

[54] OEA. “Buenas Prácticas para establecer un CSIRT nacional”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.sites.oas.org/cyber/Documents/2016 - Buenas Prácticas CSIRT.pdf

- Adecuación de permisos.

2) **I+D+i:** en esta área se desarrollará la capacidad de investigación, desarrollo e innovación tanto del recurso humano del CSIRT como de sus usuarios, la cual se mantiene en permanente actualización respecto a los avances en el campo de la ciberseguridad (alertas, las amenazas en evolución, los vectores de ataque que emergen, mejores prácticas, mantenimiento y la operación de dispositivos, estrategias de defensa, entre otros).

   En esta área se gestionarán evaluaciones y auditorías de seguridad a los sistemas o a los usuarios, que incluyen el análisis de la infraestructura, aplicaciones, la revisión de las políticas de seguridad, el análisis de vulnerabilidades, las pruebas de penetración y el cumplimiento de los estándares o normas internacionales.

   Adicionalmente, en esta área se implementarán funciones secundarias tales como la realización de cursos de formación y se podrán detectar amenazas o vulnerabilidades emergentes inherentes a las nuevas tecnologías y distribuir información relevante que pueda mejorar los niveles de seguridad en la comunidad.

3) **Centro de Operaciones (SOC):** en esta área se realizará la gestión de incidentes, el monitoreo y el análisis de incidentes, donde se centralizan e integran componentes tecnológicos para gestionar eventos de seguridad, donde se canalizan las alertas y eventos de seguridad.

   Su gestión estará orientada al monitoreo de eventos 7x24 en tiempo real de los activos de información a través de equipos tecnológicos, a su aseguramiento y defensa, contando con un equipo de profesionales especializados.

   Funciones del SOC [55]:

   - **Prevención**: disminuir la probabilidad de aparición de incidentes.

   - **Detección**: monitorear constantemente los activos para detectar amenazas, vulnerabilidades, intrusiones, ataques y demás situaciones que impliquen un posible incidente de seguridad.

[55] MORALES, Carlos, MORENO, Omar Enrique, ORTIGOZA, Johanna. Propuesta de un modelo de centro de operaciones de seguridad (SOC) para Fuerza Aérea Colombiana. {En línea}. 2014. {Consultado el 29 de noviembre de 2019}". Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2786/trabajo%20de%20grado1627.pdf?sequence=1

- **Análisis**: realizar el estudio de los incidentes que surgen durante la detección para determinar si son incidentes reales o falsos positivos.

- **Respuesta**: generar los planes de acción a realizar para atender los incidentes reales analizados.

Para dar cumplimiento a estas funciones se prestarán los siguientes servicios [56]:

- **Monitorización**: observación permanente de los controles de seguridad implementados para detectar posibles incidentes de seguridad.

- **Detección y gestión de vulnerabilidades**: identificación de las debilidades de la infraestructura tecnológica y de las acciones correctivas apropiadas.

- **Centralización, tratamiento y custodia de logs**: dada la gran cantidad de logs que se reportan de los diferentes dispositivos, es necesario hacer uso de un correlacionador de eventos, el cual, analizará estos logs, para detectar situaciones poco comunes o sospechosas para su gestión.

- **Respuesta de resolución**: desarrollo de planes de acción para neutralizar la amenaza.

- **Asesoría de seguridad**: apoyo a la Dirección para tomar decisiones por parte de personal especializado (técnicos de sistemas, especialistas en comunicaciones, seguridad física, seguridad lógica, juristas, auditores, analistas de malware).

- **Programas de prevención**: control permanente de nuevas amenazas e implementación de acciones preventivas que mitiguen el riesgo que se presenten incidentes.

Para el desarrollo de estos servicios se hace necesario contar con un equipo de profesionales con diferentes perfiles, los cuales se agruparán para la atención de incidentes de la siguiente manera [57]:

---

[56] MORALES, Carlos, MORENO, Omar Enrique, ORTIGOZA, Johanna. Propuesta de un modelo de centro de operaciones de seguridad (SOC) para Fuerza Aérea Colombiana. {En línea}. 2014. {Consultado el 29 de noviembre de 2019}". Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2786/trabajo%20de%20grado1627.pdf?sequence=1

[57] RAMOS, David. "A fondo: ¿Cómo funcionan los SOC?". {En línea}. 21 de noviembre de 2017. {Consultado el 29 de noviembre de 2019}". Disponible en: https://www.silicon.es/a-fondo-como-funcionan-soc-2362658

- **Nivel 1: Monitorización y análisis:** éste debe estar conformado por uno o más analistas para monitorear las alertas constantes y las amenazas que se pueden presentar, además, deben realizar su clasificación con base en la información que se recopila para ser analizada y luego establecer si estas alertas pudiesen llegar a ser incidentes de seguridad o son falsos positivos.

- **Nivel 2: análisis profundo y respuesta:** este se encarga de dar respuesta a los incidentes tras la clasificación inicial; este nivel cuenta con un nivel de experticia mayor. A partir de unas metodologías y procedimientos se procede con el análisis del incidente verificando la información de las fuentes comprobando si éste involucra a sistemas críticos y cuáles son los bancos de datos posiblemente afectados. También está en la capacidad de hacer recomendaciones y remediar proporcionando soporte para el análisis del incidente.

- **Nivel 3: expertos y 'hunters':** este nivel es superior a los vistos anteriormente y se llega a éste cuando se requieren los servicios de un "expertise" muy alto para dar respuesta y mitigación a los incidentes de seguridad; también está en la capacidad de buscar posibles incidentes.

  Está conformado por personal técnico especializado en las diferentes ramas de la ciber-seguridad, quienes realizan auditorías, proponen planes de acción y remediación y ejecutan servicios avanzados como el análisis forense.

- **Coordinación del SOC:** este es el cerebro del SOC. Éste es el encargado de gestionar al equipo y sus presupuestos; también tiene como tarea ser el punto de contacto para los incidentes críticos, y también diseña y actualiza el catálogo de servicios y rendimiento del grupo de trabajo.

- **Otros roles:** los roles mencionados anteriormente corresponden a los niveles básicos del SOC; al interior del SOC existen muchos expertises que se encargan de los procedimientos y de los equipos técnicos; también se encuentran los que ejercen el rol de jefes de proyecto para los clientes, éstos se encargan del reporte al cliente final y del seguimiento de los SLA.

Finalmente, para el cumplimiento de funciones y prestación de los servicios, el SOC deberá aplicar las mejores prácticas orientadas a proteger la información y los recursos tecnológicos que la procesan, basándose en estándares tales como: ISO27001, para la implementación y operación del SGSI el cual se puede implementar haciendo uso del ciclo de mejoramiento continuo de Deming, PHVA, y el estándar ISO27035 para gestionar los incidentes de seguridad de la información.

4) **Soporte TI:** en esta área se contará con el recurso humano y tecnológico requerido para la administración y soporte de la infraestructura tecnológica del CSIRT, servicios que se ejecutarán bajo las mejores prácticas, como es el caso de ITIL.

5) **Área de coordinadores:** en esta área se coordinará la eficacia de la respuesta a los incidentes de seguridad y la interacción mediante la coordinación de gestiones y colaboración, y se proporcionará el análisis de incidentes y de vulnerabilidades, se generarán los boletines de noticias, estadísticas y documentación de las mejores prácticas, entre otros.

6) **Área Logística:** en esta área se realiza el control del inventario, almacenaje y disposición de los bienes requeridos para prestar los servicios del CSIRT.

7) **Salón de Formación:** en esta área se desarrollarán sesiones de capacitación, ya sean presenciales o virtuales, a través de empresas certificadoras que tienen como propósito la formación o la formación y certificación del talento humano en las siguientes temáticas:

    - Hacking ético.
    - Seguridad Web: Inyección SQL y cross site scripting
    - Seguridad en Linux: Server Hacking
    - Criptografía
    - Hacking Móvil.
    - Informática Forense

8) **Salón de crisis:** en esta área se gestionan los incidentes de seguridad de la información que se consideren situaciones de crisis[58] que precisan una respuesta urgente; esta situación es previamente informada por la Alta Gerencia de la Organización (usuarios del CSIRT), quien solicitará la instalación de la mesa de crisis donde se analizará la situación presentada (de ser posible con expertos y/o aliados estratégicos), se evaluarán los recursos financieros, humanos y tecnológicos requeridos para la atención de la emergencia y se evaluarán las alternativas para la contención, erradicación y solución del incidente.

[58] Un incidente crítico (CI) es un evento o serie de eventos que amenaza seriamente el bienestar del personal, potencialmente resultando en la muerte, lesiones mortales o enfermedades. Un incidente crítico o una serie de tales incidentes se convierte en una crisis cuando su naturaleza, severidad o posibles consecuencias para una organización justifican una respuesta más allá de la capacidad del programa de rutina o mecanismos de gestión, es decir, que requieren liderazgo y coordinación desde el nivel de alta dirección.

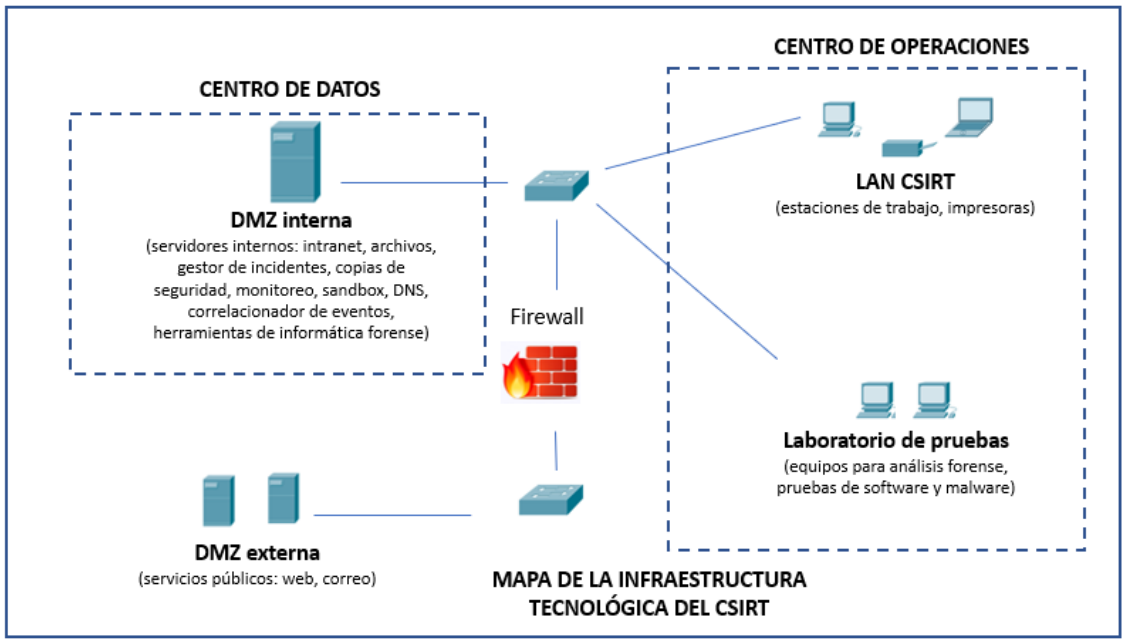
9) **Área para almacenamiento de evidencias:** es un área aislada, con conexión a internet restringida, donde se almacena toda la evidencia o indicio recopilado de los procesos de investigación y que requieren su preservación evitando su deterioro con contaminación, emisiones electromagnéticas, interferencias, humedad, entre otros. En esta área se almacenará información sensible no digital, fichas, discos duros, entre otros. Esta área es supervisada por un Coordinador.

10) **Laboratorio de pruebas:** es un área aislada, con conexión a internet restringida para evitar fuga de información, manipulación de resultados, manipulación o daño de evidencias. En esta área se analiza toda la evidencia o indicio de los procesos de investigación. Adicionalmente llevan a cabo las actividades forenses, pruebas de software y revisión de malware y proporciona servicios de investigación a otras áreas. Esta área es supervisada por un Coordinador.

6.2.2 Actividad N° 2 – Diseño del mapa de la estructura tecnológica CSIRT

Esta actividad comprende el diseño del mapa de la estructura tecnológica del CSIRT. Para esto, en la figura 2 se presenta el mapa de la estructura tecnológica propuesta para el CSIRT:

Figura 2. Mapa de la estructura tecnológica del CSIRT



Fuente: Los autores

6.3 FASE 3: DESARROLLO DEL OBJETIVO N° 3 – PRUEBAS A HERRAMIENTAS DE SOFTWARE – LABORATORIO CSIRT

Este objetivo consiste en ejecutar y documentar pruebas de cada una de las herramientas de software instaladas para verificar que éstas cumplen con los requerimientos para el laboratorio del CSIRT

6.3.1 Actividad N° 1 – Alistamiento de hardware y software seleccionado

Esta actividad comprende el alistamiento del hardware y software seleccionado.

6.3.1.1 Hardware y software requerido

En la figura 16 se presentan los requerimientos técnicos para la instalación de los servidores y software contemplados para el CSIRT:

Tabla 16. Hardware y software requeridos para el laboratorio del CSIRT

Configuración equipos físicos	Herramienta virtualización	Servidor virtual	Sistema Operativo	Memoria (GB)	Procesador (CPU)	Almacenamiento
	Virtualbox	Monitoreo (Nagios) [59]	Linux 1	2 GB	Procesador de 2+ GHz	40 GB HD

[59] ECURED. “Nagios”. {En línea}. {Consultado el 17 de mayo de 2020}. Disponible en: https://www.ecured.cu/Nagios

Configuración equipos físicos	Herramienta virtualización	Servidor virtual	Sistema Operativo	Memoria (GB)	Procesador (CPU)	Almacenamiento
Equipo 1: Linux Elementary	Virtualbox	Gestión de incidentes (GLPI) [60]	Linux 2	4 GB	Procesador 2.5 Ghz, un núcleo o más	26 GB HD
		Escaneo vulnerabilidades (Nmap, OpenVas)	Kalilinux 1	2 GB	2 cores	10 GB
		Correlacionador de Eventos (Snort) [61]	Kalilinux 1	4GB	2 Core	20 GB
		Sandbox (Firejail) [62]	Linux 4	2 GB	Intel Core 2 Duo T5200	2 GB
		Copias de respaldo (Bacula) [63]	Linux 3	8 GB o más	Pentium IV o más	DISCO DURO: 1 Tb

[60] ECURED. “GLPI”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.ecured.cu/GLPI

[6161] SÁNCHEZ LORENTE, Olga. Detección de intrusiones con SNORT. {En línea}. Junio de 2015. {Consultado el 17 de mayo de 2020}. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/43090/6/osanchezloTFM0715memoria.pdf

[62] PCGAMEBENCHMARK. “Universe Sandbox System Requirements”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.pcgamebenchmark.com/universe-sandbox-system-requirements

[63] RODRÍGUEZ, Marcos. “BACULA BACKUP: Instalación del servidor”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://vivaubuntu.com/bacula-backup-instalacion-del-servidor

Configuración equipos físicos	Herramienta virtualización	Servidor virtual	Sistema Operativo	Memoria (GB)	Procesador (CPU)	Almacenamiento
Equipo 2: Windows 10		Analizador de protocolos (Wireshark) [64]	Kalilinux 1	500 MB	Any modern 64-bit AMD64/x86-64 or 32-bit x86 processor	500 MB
		Explotación de vulnerabilidades (Metasploit) [65]	Kalilinux 1	4 GB	2 GHz+ processor.	50 GB

Fuente: Los autores.

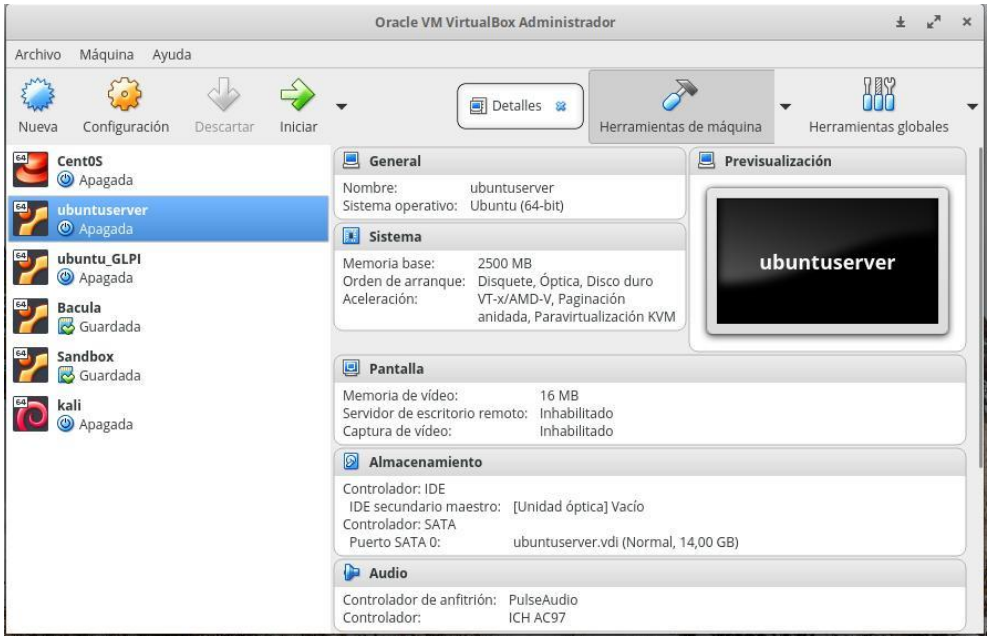
[64] WIRESHARK.ORG. “System Requirements”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.wireshark.org/docs/wsug_html_chunked/ChIntroPlatforms.html

[65] RAPID7. “System Requirements and Documentation”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.rapid7.com/products/metasploit/system-requirements/

6.3.1.2 Instalación de las máquinas virtuales requeridas

a) Monitoreo (Nagios): En la figura 3 se presenta la herramienta con la que se realizará seguimiento y monitoreo los servidores (memora RAM, procesadores, almacenamiento y estado) y aplicaciones del laboratorio CSIRT[66]:

Figura 3. M.V. Monitoreo

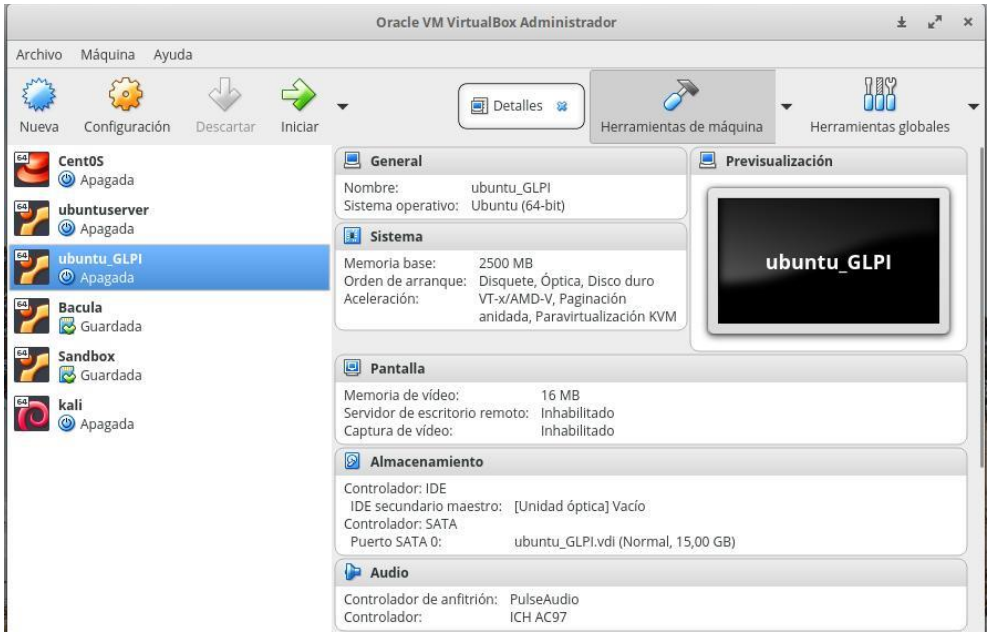


Fuente: Los autores

[66] SYSADM.ES. “Instalación y configuración de Nagios”. {En línea}. Abril 23 de 2018. {Consultado el 29 de noviembre de 2019}. Disponible en: https://sysadm.es/instalacion-y-configuracion-de-nagios/

b) Gestión de incidentes (GLPI): En la figura 4 se presenta la herramienta para la administración de servicios tecnológicos, con ella se gestionarán los requerimientos relacionados con seguridad de la información e informática[67]:

Figura 4. M.V. Gestión de incidentes

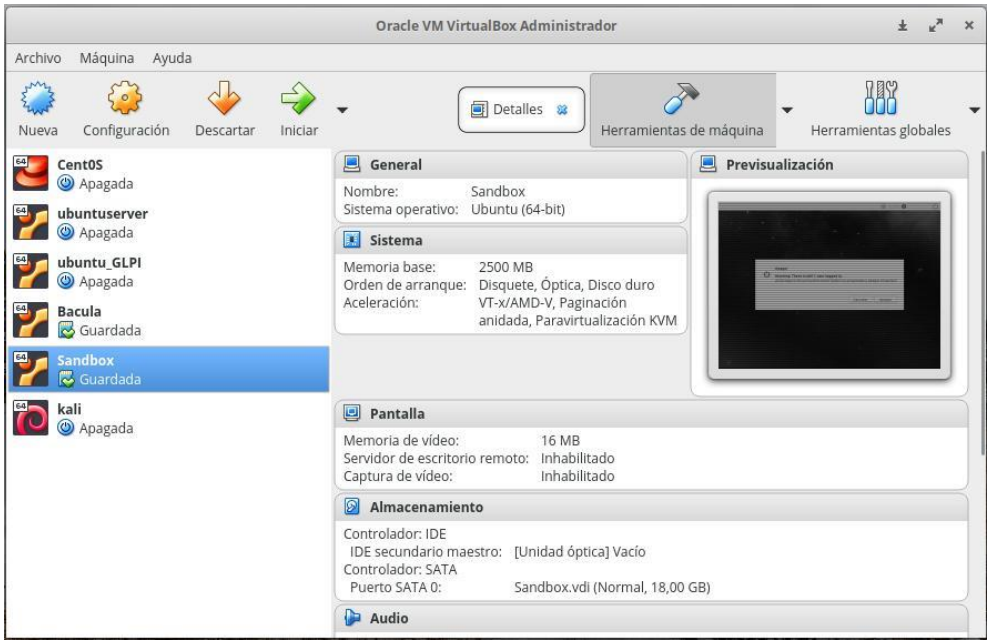


Fuente: Los autores

[67] GLPI PROJECT. "Install the GLPI application". {Consultado el 29 de noviembre de 2019}. Disponible en: https://glpi-project.org/DOC/EN/

c) Sandbox (Firejail): En la figura 5 se presenta la herramienta para la ejecución de programas en un entorno seguro, con esta solución se llevarán a cabo pruebas de seguridad de acuerdo con el tipo de solicitud del requerimiento[68]:

Figura 5. M.V. Sandbox

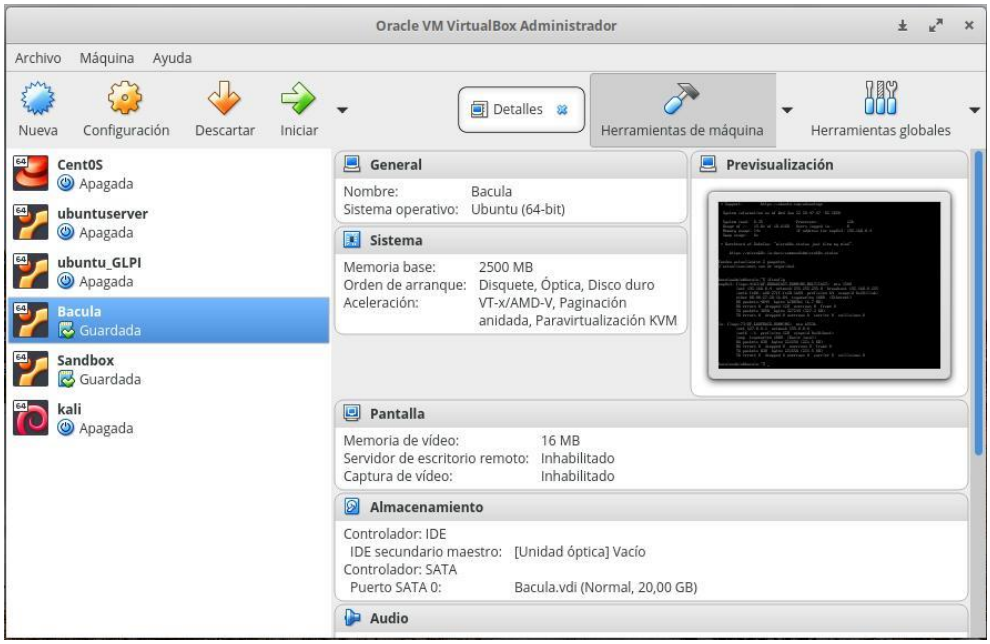


Fuente: Los autores

[68] FIREJAIL SECURITY SANDBOX. “Firejail Usage”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://firejail.wordpress.com/documentation-2/basic-usage/

d) Copias de respaldo (Bacula): En la figura 6 se presenta la herramienta para respaldar información a equipos bajo protocolo IP y con ella se realizarán las copias de respaldo a los servidores[69]:

Figura 6. M.V. Copias de respaldo

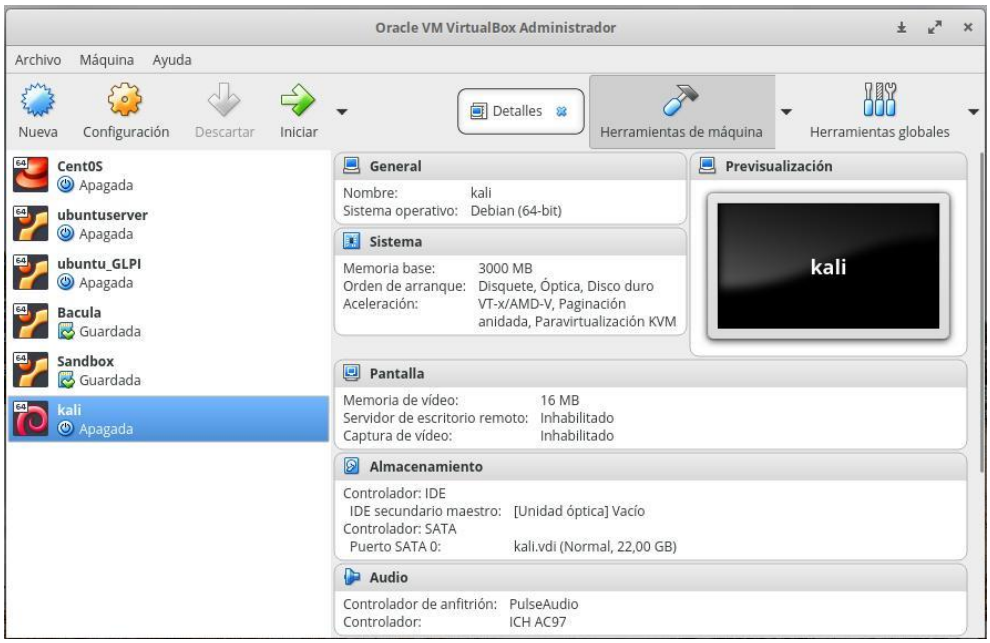


Fuente: Los autores

[69] RODRÍGUEZ, Marcos. "BACULA BACKUP: Instalación del servidor". {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://vivaubuntu.com/bacula-backup-instalacion-del-servidor

e) Kalilinux[70] (Nmap, OpenVas[71], Snort[72], Metasploit): En la figura 7 se presenta la máquina virtual con sistema operativo KaliLinux que incluye las herramientas de auditoría para la seguridad informática. Con estas aplicaciones se atenderán los requerimientos en seguridad de la información e informática:

Figura 7. M.V. para las herramientas de seguridad informática



Fuente: Los autores

[70] PROFESIONALES review. “Como instalar Kali Linux en VirtualBox” 02 de enero de 2019. {en linea}. (Consultado el 29 de noviembre de 2019). Disponible en: https://www.profesionalreview.com/2019/01/02/instalar-kali-linux-virtualbox/

[71] REDES - LABORATORIO DE SEGURIDAD INFORMÁTICA Y REDES. “OpenVAS: Instalación, configuración y prueba”. {En línea}. 11 de mayo de 2018. {Consultado el 29 de noviembre de 2019}. Disponible en: http://redeslinuxinternet.blogspot.com/2018/05/openvas-instalacion-configuracion-y.html

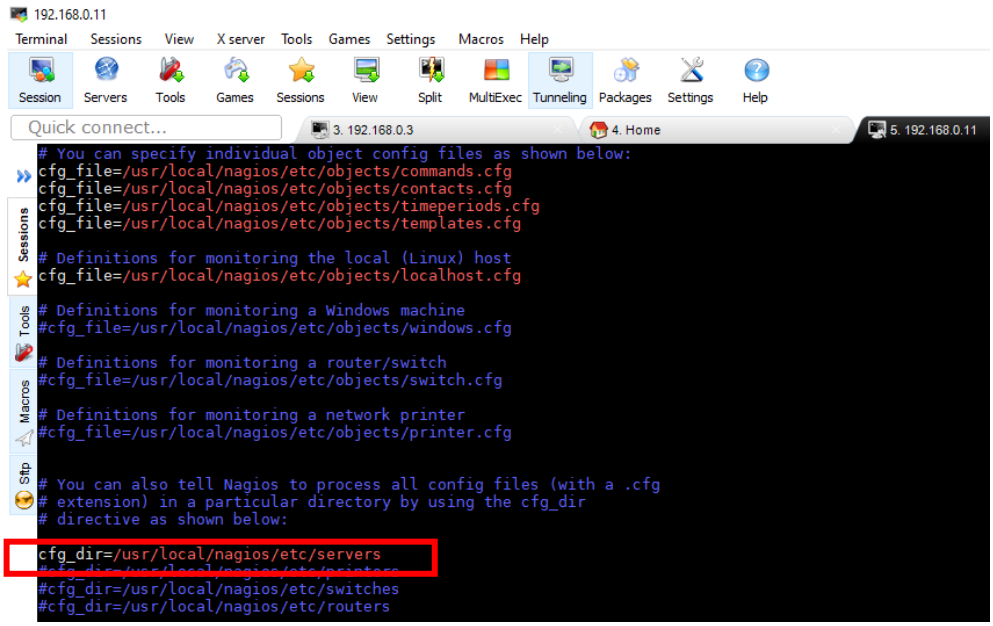
[72] SNORT.ORG. “Snort”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.snort.org/

6.3.1.3 Configuración de servidores

a) Configuración servidor de monitoreo (Nagios 4.0):

En la figura 8 se presenta el contenido del archivo //usr/local/nagios/etc/nagios.cfg donde se habilita la línea cfg_dir para activar el servicio de monitoreo de hosts[73]:

Figura 8. Activación servicio monitoreo

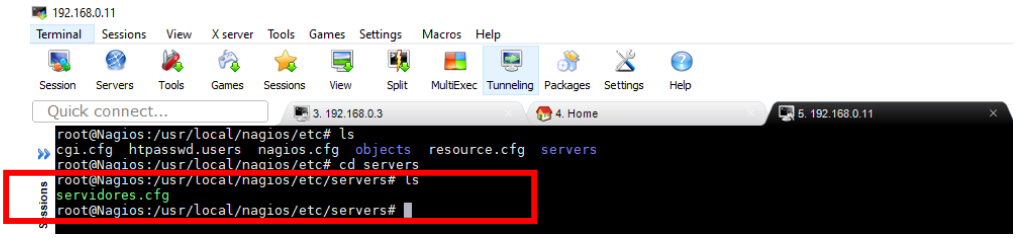


Fuente: Los autores

En la figura 9 se presenta el archivo servidores.cfg creado en una carpeta nueva denominada /usr/local/nagios/etc/servers/, en la cual se ubican los archivos de configuración de alertas de los servidores a monitorear:

[73] ROMERO GONZÁLEZ, Rafael. “Instalación y configuración de nagios core 4.0.4.” {En línea}. Junio de 2015. {Consultado el 29 de noviembre de 2019}. Disponible en: https://exchange.nagios.org/components/com_mtree/attachment.php?link_id=6527&cf_id=24

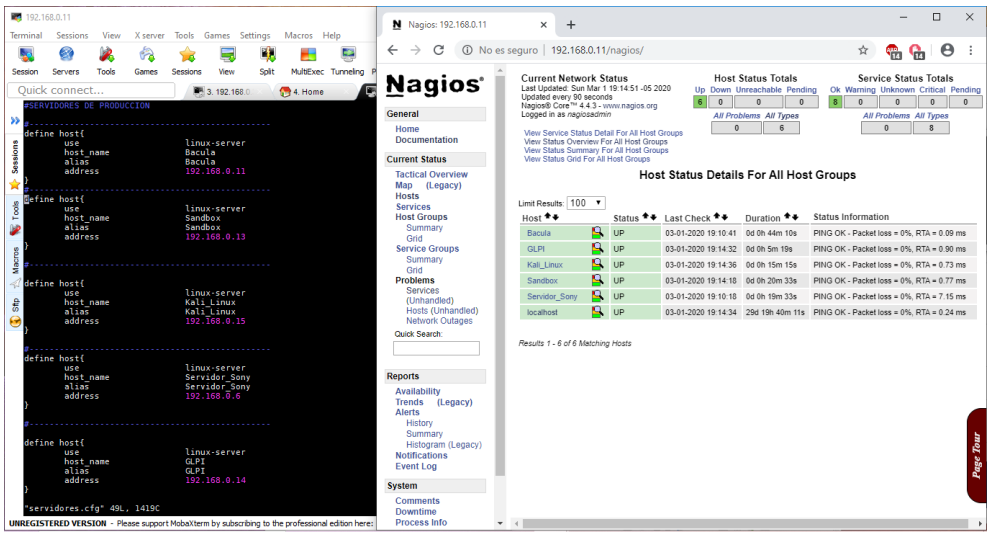
Figura 9. Configuración servicio de monitoreo – archivo servidores.cfg



Fuente: Los autores

En la figura 10 se presenta el archivo servidores.cfg donde se configura cada uno de los hosts a monitorear, como se observa en la terminal y en el servidor Nagios donde se despliegan estos hosts y su estado:

Figura 10. Configuración Nagios

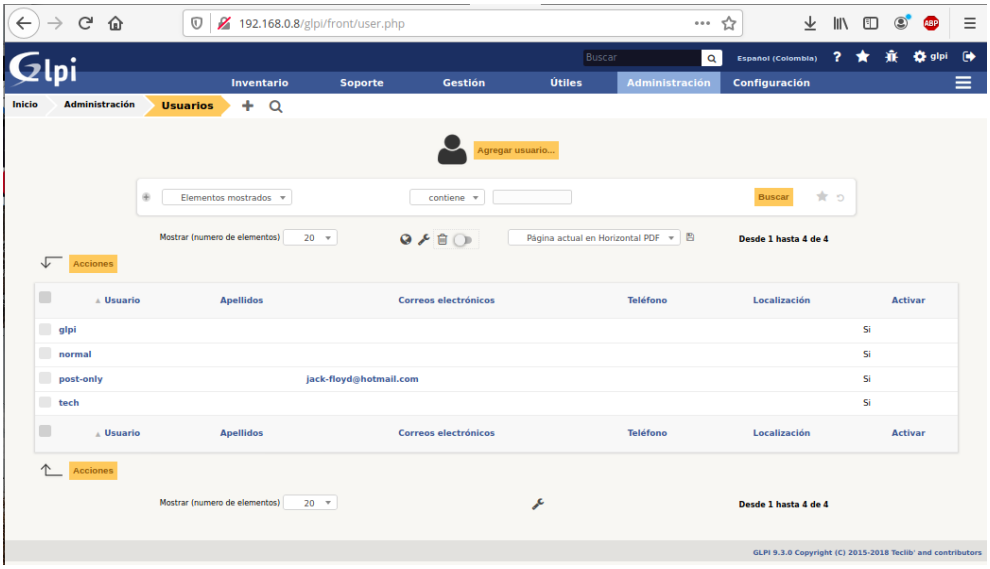


Fuente: Los autores

b) Configuración servidor de gestión de requerimientos e incidentes (GLPI):

En la figura 11 se puede observar la interfaz para la gestión de usuarios, en ella se pueden crear usuarios y asignarles un perfil de acuerdo con su roll en la organización:

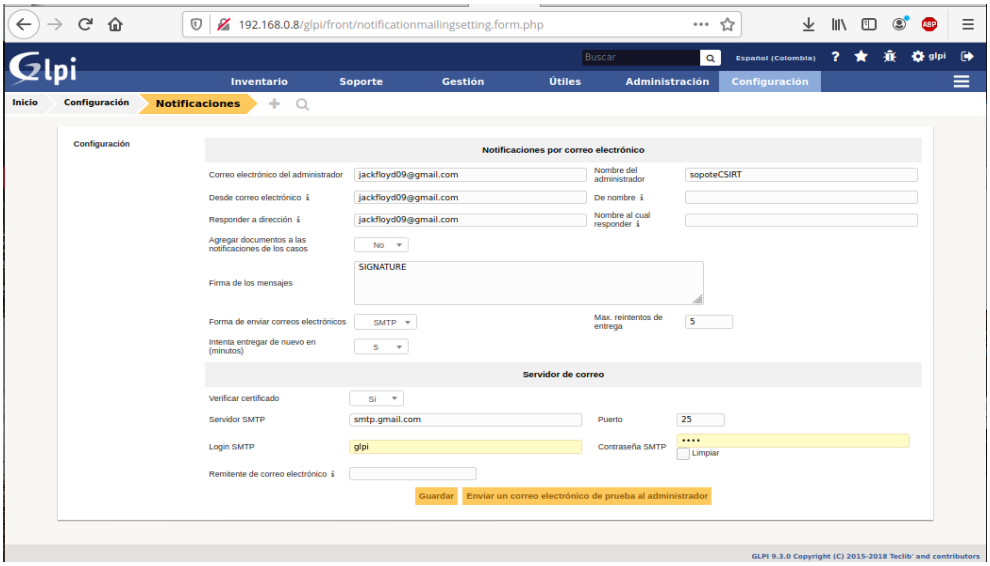
Figura 11. Administración de usuarios - GLPI



Fuente: Los autores

En la figura 12 se observa la interfaz para la configuración de notificaciones; en ésta se agrega el correo que los usuarios usarán para enviar requerimientos:

Figura 12. Configuración de notificaciones - GLPI



Fuente: Los autores

b) Configuración servidor sandbox (Firejail versión: Firetools 0.9.50 QT versión 5.9.2):

Para ejecutar una aplicación en la herramienta Sandbox existes dos formas; una es por medio de una consola shell y la otra por medio de la interfaz gráfica, para este caso y de acuerdo a lo presentado en la figura 13 se utilizará la interfaz gráfica ya que es más fácil de usar[74]:

Figura 13. Interfaz gráfica de sandbox (Firetools)

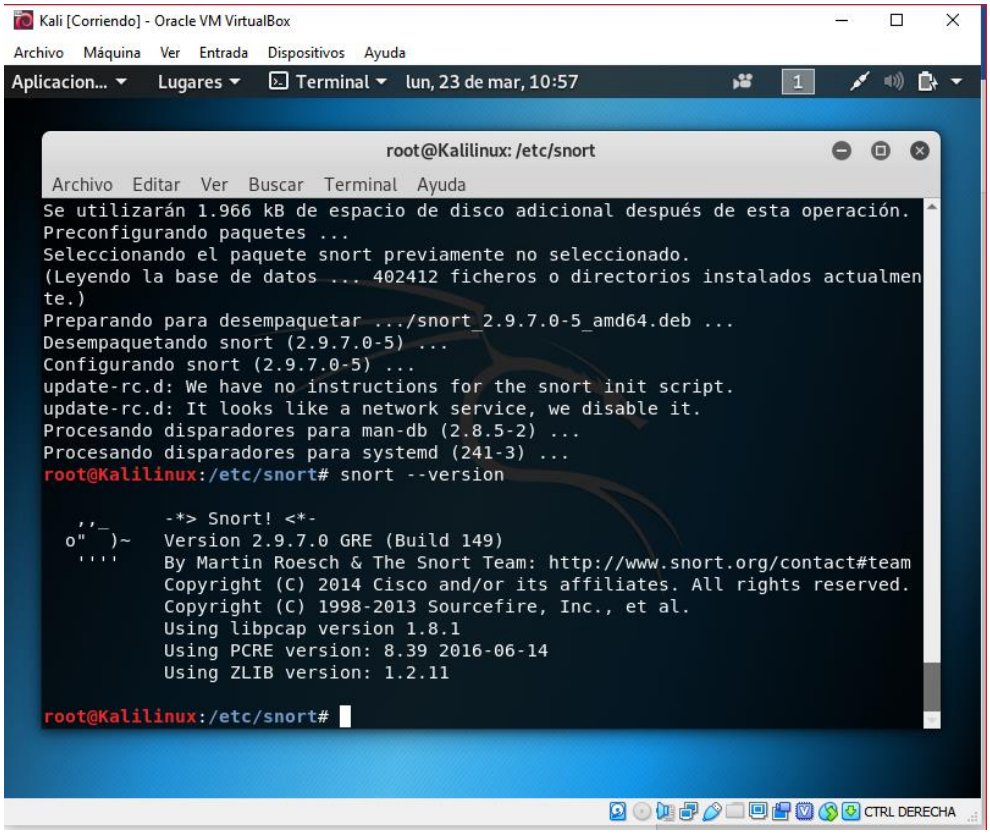
Fuente: Los autores

Se observa el menú de la herramienta sandbox en el modo gráfico el cual es intuitivo y cómodo para gestionar.

[74] FIREJAIL. “Firejail security sandbox”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://firejail.wordpress.com/features-3/

c) Correlacionador de eventos (Snort versión 2.9.7.0): En la figura 14 se presenta la herramienta snort con la que se realizan auditorías de las redes con el fin de detectar intrusos y movimientos poco comunes en la red[75]:

Figura 14. Instalación de correlacionador de eventos Snort



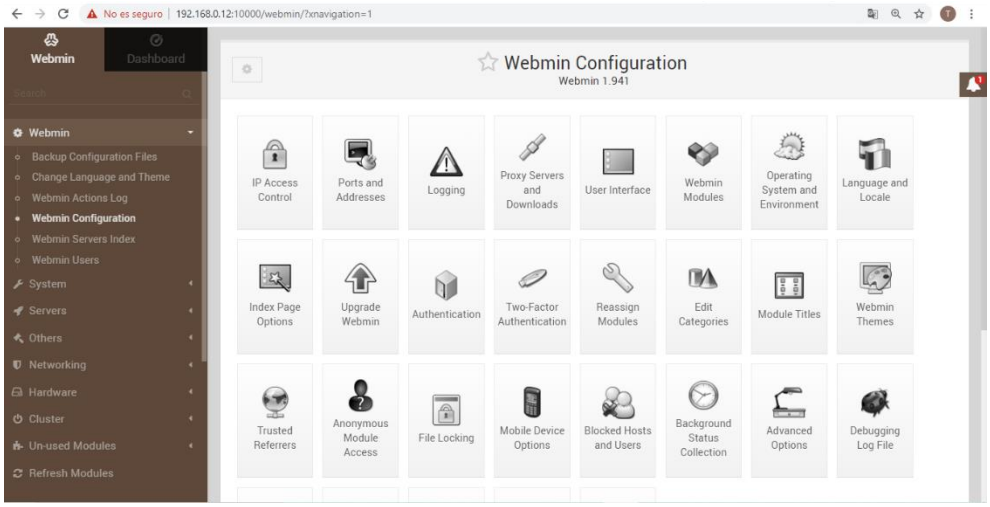
Fuente: Los autores

d) Configuración servidor de copias de respaldo (Bacula): En la figura 15 se presenta la herramienta Bacula que se implementará para respaldar la información de los servidores del CSIRT[76]:

[75] ORTEGO DELGADO, Daniel. “Qué es Snort: Primeros pasos”. {En línea}. 21 de marzo de 2017. {Consultado el 29 de noviembre de 2019}. Disponible en: https://openwebinars.net/blog/que-es-snort/

[76] RODRÍGUEZ, Marcos. “BACULA BACKUP: Instalación del servidor”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://vivaubuntu.com/bacula-backup-instalacion-del-servidor

Figura 15. Interfaz admin - Webmin Configuration - Bacula

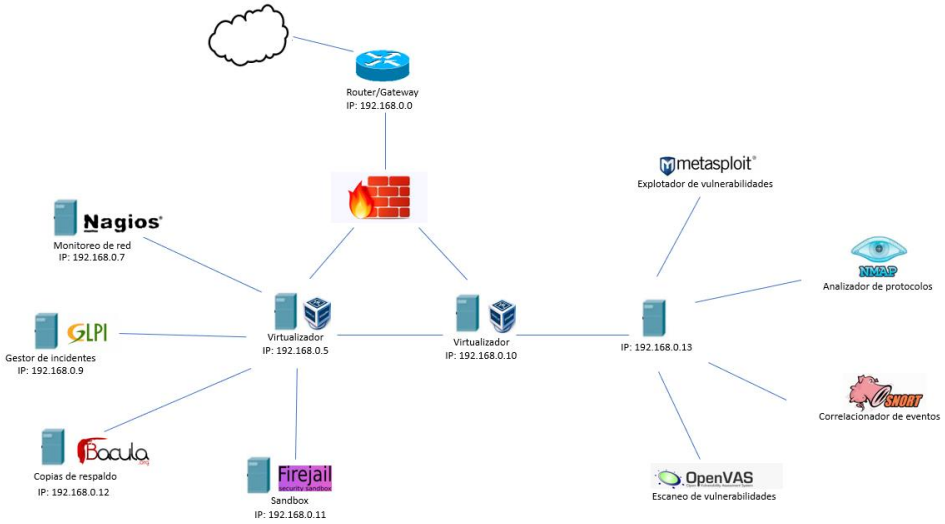


Fuente: Los autores

6.3.2 Actividad N° 2 – Diseño lógico del laboratorio CSIRT

En la figura 16 se presenta el diseño lógico del laboratorio controlado, que incluye dos servidores físicos y cinco servidores virtuales:

Figura 16. Diseño lógico - Laboratorio CSIRT



Fuente: Los autores

6.3.3 Actividad N° 3 – Ejecución y documentación software CSIRT

A continuación, se realiza una breve presentación de cada una de las herramientas a utilizar y su funcionamiento para el laboratorio del CSIRT:

6.3.3.1 Virtualbox

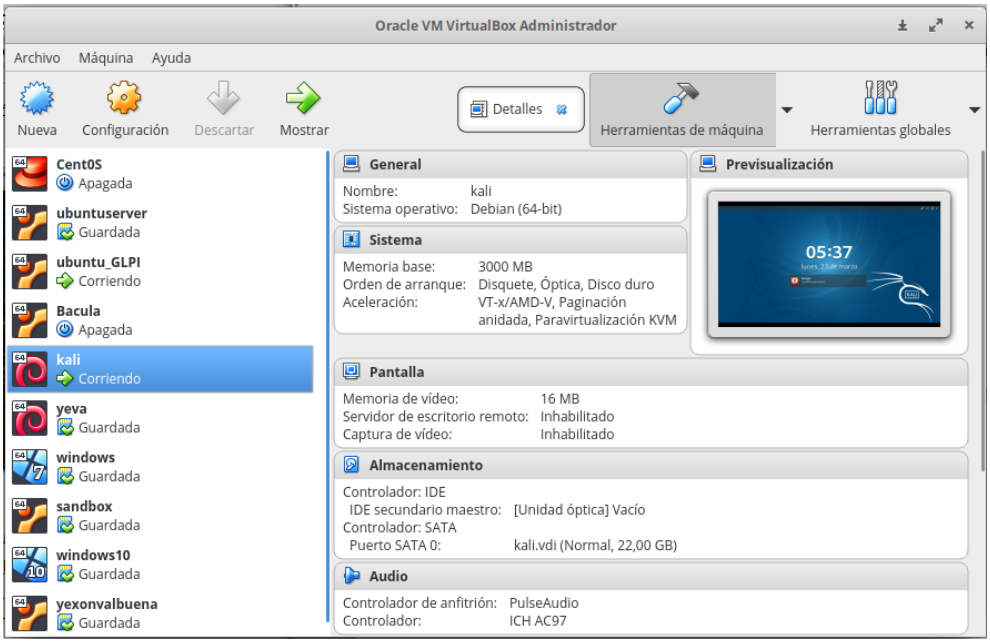
Es una herramienta para virtualización de arquitecturas de 32 y 64 bits; en ella podemos instalar sistemas operativos como invitados en ambientes virtuales en una máquina anfitriona. Virtualbox permite disponer de muchos servidores con características diferentes instalados en un servidor físico y a la vez todos sus recursos puedan ser compartidos entre las máquinas virtuales[77].

[77] PC RESUMEN. “Virtualización con Oracle VM VirtualBox”. {En línea}. 21 de mayo de 2019. {Consultado el 29 de noviembre de 2019}. Disponible en https://www.pcresumen.com/menu-software/31-virtualizacion/41-virtualizacion-con-oracle-vm-virtualbox

A cada una de las máquinas virtuales se les puede asignar recursos como: memoria RAM, procesadores, tarjeta de red, disco entre otros y así poder gestionar el sistema operativo.

En la figura 17 se presenta Virtualbox con una serie de máquinas ya instaladas:

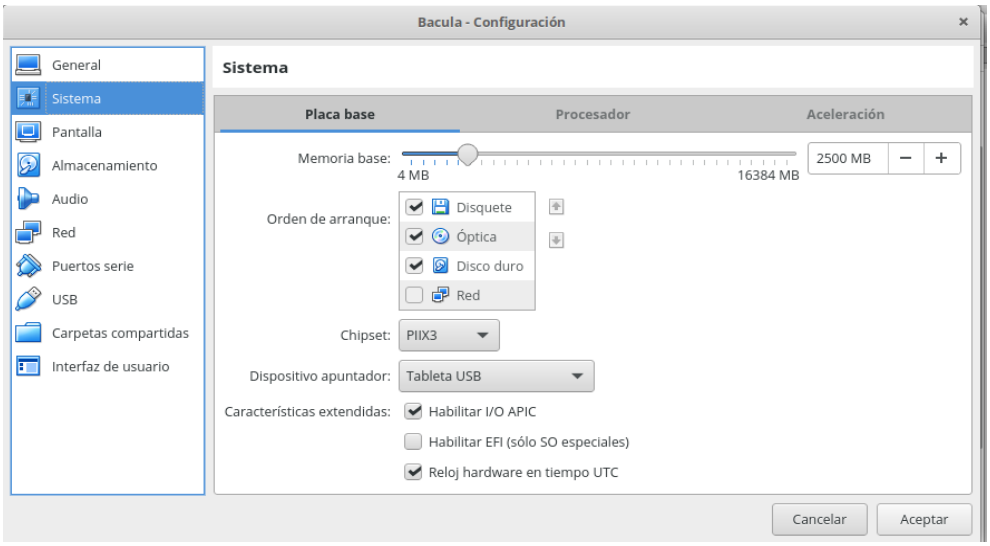
Figura 17. Interfaz gráfica de Virtualbox



Fuente: Los autores

En la figura 18 se observan las características como la memoria RAM, el procesador y la aceleración de una máquina virtual instalada:

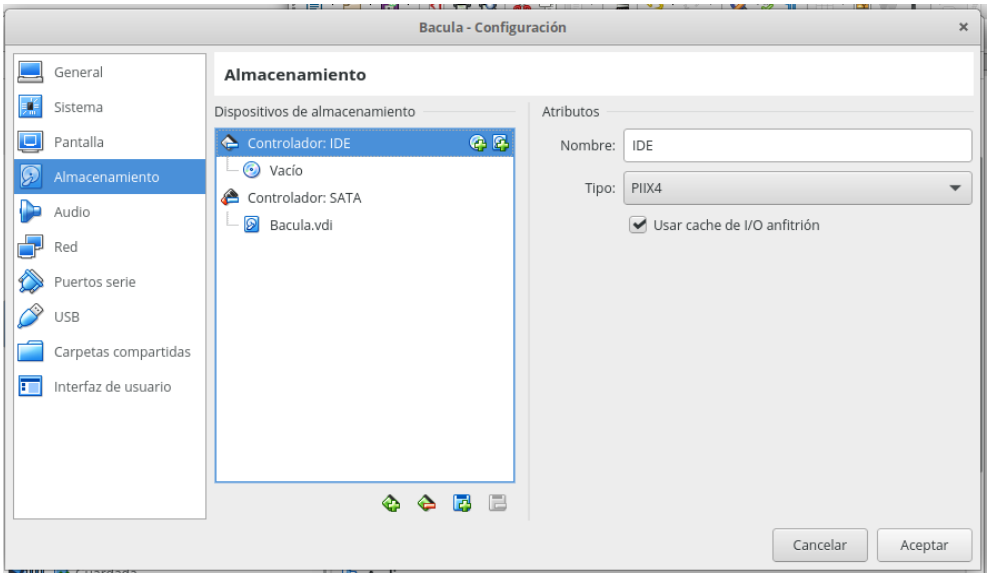
Figura 18. Configuración general de máquina virtual en Virtualbox



Fuente: Los autores

En la figura 19 se observan los dispositivos de almacenamiento y sus atributos:

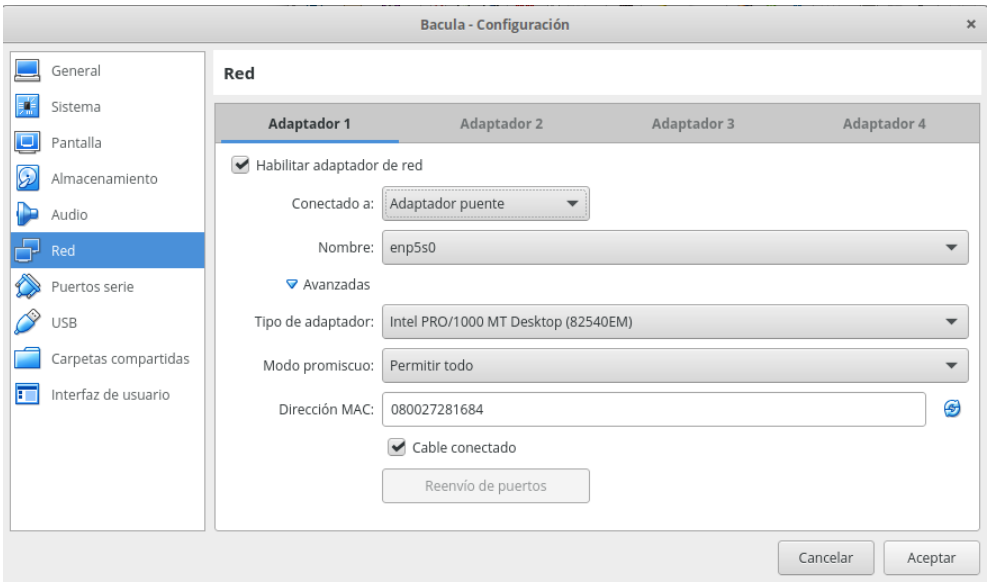
Figura 19. Configuración de dispositivos de almacenamiento en Virtualbox



Fuente: Los autores

En la figura 20 se presenta la configuración de la red para la máquina virtual, donde se observa que está conectada en Adaptador puente, tiene una tarjeta asignada enp5s0 y tiene un adaptador que se encuentra en modo promiscuo:

Figura 20. Configuración del adaptador de red en Virtualbox



Fuente: Los autores

6.3.3.2 Nagios

Es una herramienta para el monitoreo de infraestructura tecnológica de código abierto que tiene como fin vigilar el comportamiento de los equipos (de comunicaciones, host, entre otros) y servicios cuando su comportamiento no es el esperado o muestra un cambio inesperado. Nagios monitoriza servicios como SMTP, POP3, HTTP, SNMP, entre otros[78]; para los recursos de hardware monitorea carga del procesador, gestión de los discos, memoria y el estado de los puertos[79] .

Para este proyecto se tiene instalada la última versión disponible 4.4.3 de Nagios Core.

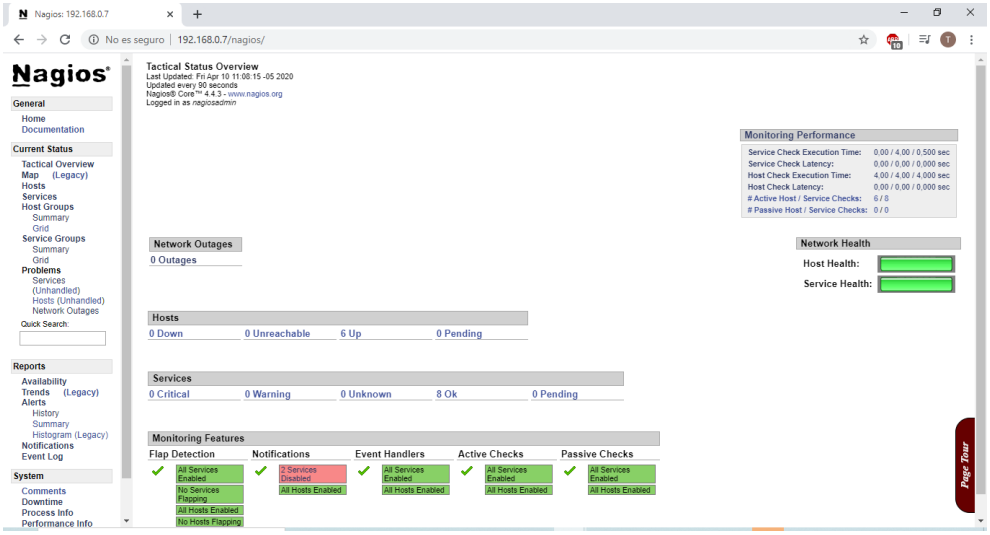
En la figura 21 se presenta la información del performance del servidor Nagios, el estado de los servicios y los hosts monitoreados, las caídas de red, servicios o equipos caídos, y el monitoreo de los servicios activos, los que tienen problemas, los chequeos activos y los chequeos pasivos:

---

[78] ECURED. “Nagios”. {En línea}. {Consultado el 17 de mayo de 2020}. Disponible en: https://www.ecured.cu/Nagios

[79] SEAQ SERVICIOS SAS. “Nagios es una Herramienta Open source de monitoreo”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.seaq.co/nagios.html

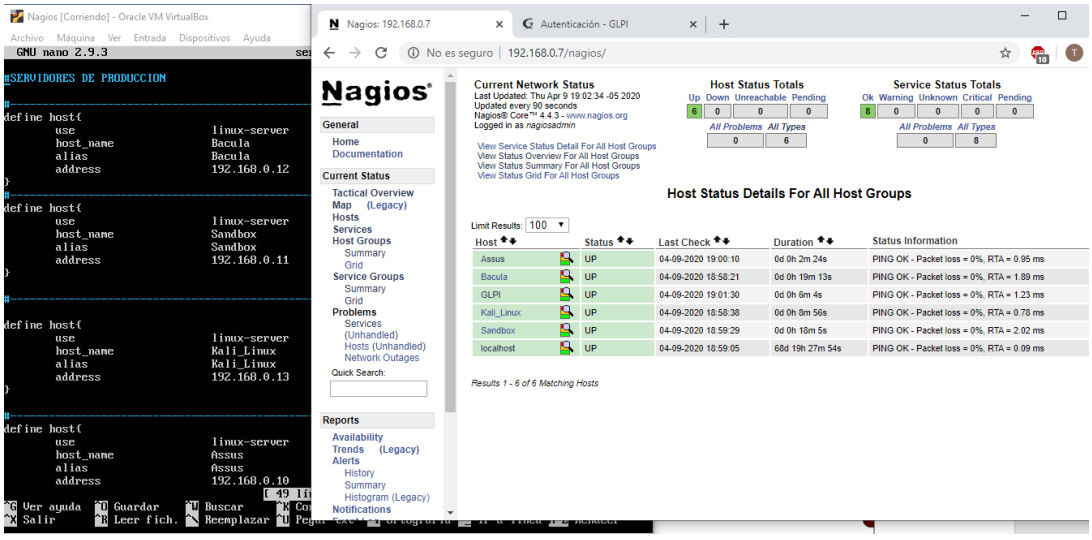
Figura 21. Estado general - Nagios



Fuente: Los autores

Al ingresar a “Hosts”, en la figura 22 se observa que se están monitoreando 6 servidores virtualizados que hacen parte del laboratorio del CSIRT. Estos servidores fueron incluidos previamente en el archivo de /usr/local/nagios/etc/servers/servidores.cfg, donde se incluyó para cada uno su nombre, alias e IP:

Figura 22. Estado de la red - Nagios

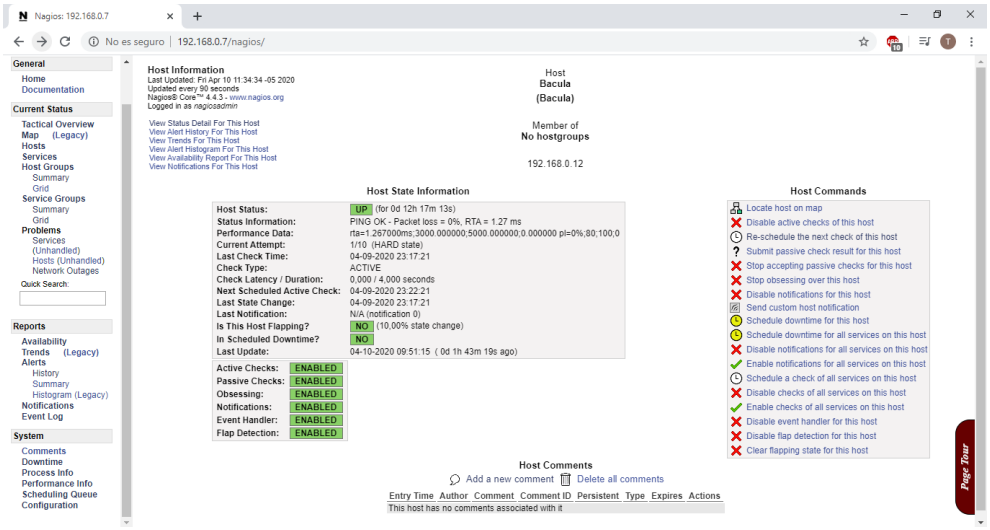


Fuente: Los autores

En la anterior figura se observa para cada equipo monitoreado, su estado, el último chequeo, su duración e información de su estado. Adicionalmente, en la parte superior de la figura, se presenta información general de los hosts y el estado de los servicios.

En la figura 23 se observa para cada host la información detallada del mismo, dando click sobre su nombre, así:

Figura 23. Información de un host - Nagios



Fuente: Los autores

6.3.3.3 Bacula

Es una herramienta open source, que permite realizar copias de respaldo de varios ordenadores por vía red, realizar la recuperación y verificación de dichos datos en caso de pérdida parcial o total de información[80].

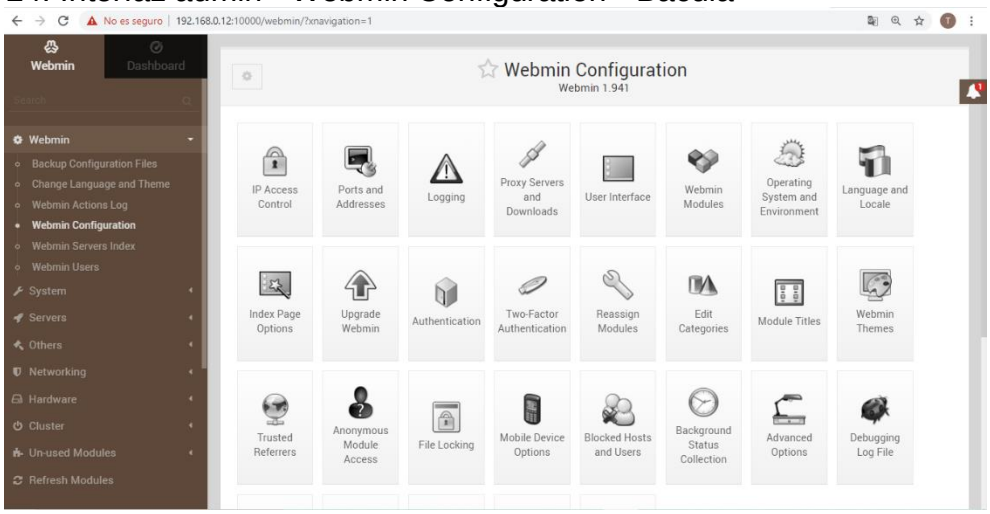
Esta herramienta se compone de tres módulos o servicios: Director (controla todas las tareas de respaldo, restauración y comunicación), almacenamiento (administra los medios de almacenamiento para el backup) y el cliente.

Esta herramienta maneja tres tipos de respaldo: full, diferencial e incremental; adicionalmente, denomina los medios de almacenamiento lógico como volúmenes y los agrupa en Pools.

[80] ULTIMOBYTE. “BACULA, OPEN SOURCE BACKUP”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.ultimobyte.es/productos/bacula-enterprise-open-source-backup

En la figura 24 se observa el menú de todas configuraciones que se pueden realizar con esta herramienta:

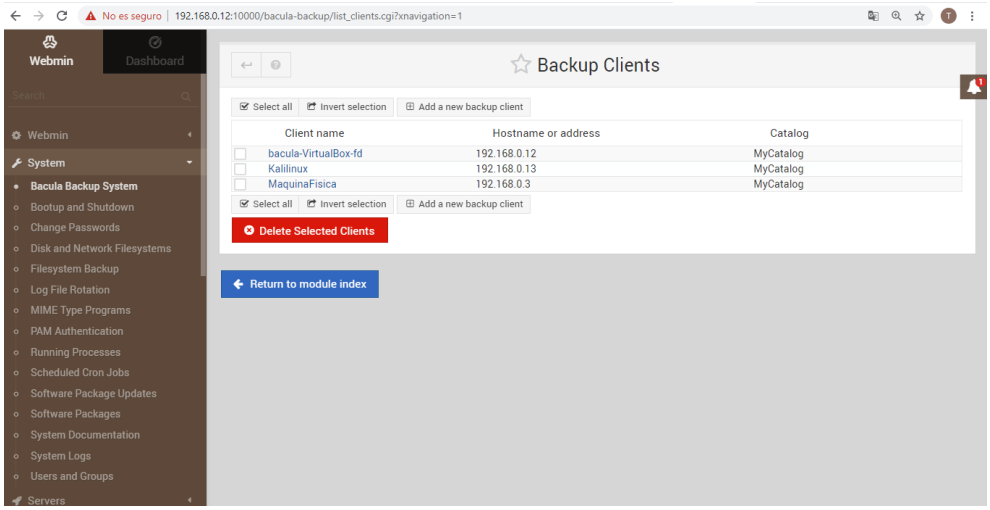
Figura 24. Interfaz admin - Webmin Configuration - Bacula



Fuente: Los autores

En la figura 25 se despliega la interfaz donde se gestionarán las configuraciones necesarias para el respaldo de la información:

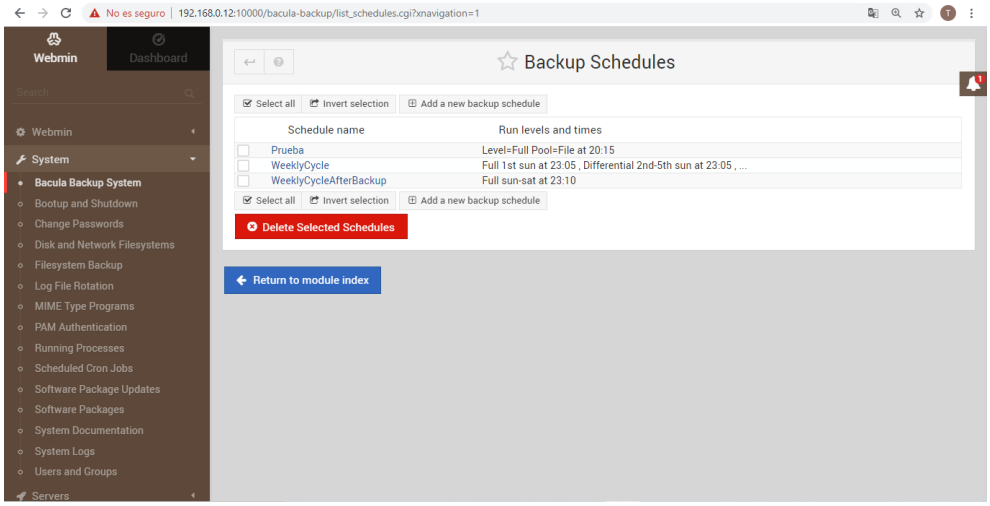
Figura 25. Interfaz admin - Bacula Clients



Fuente: Los autores

En la figura 26 se observa la interfaz donde se encuentran las opciones de configuración para la programación de las copias de respaldo:

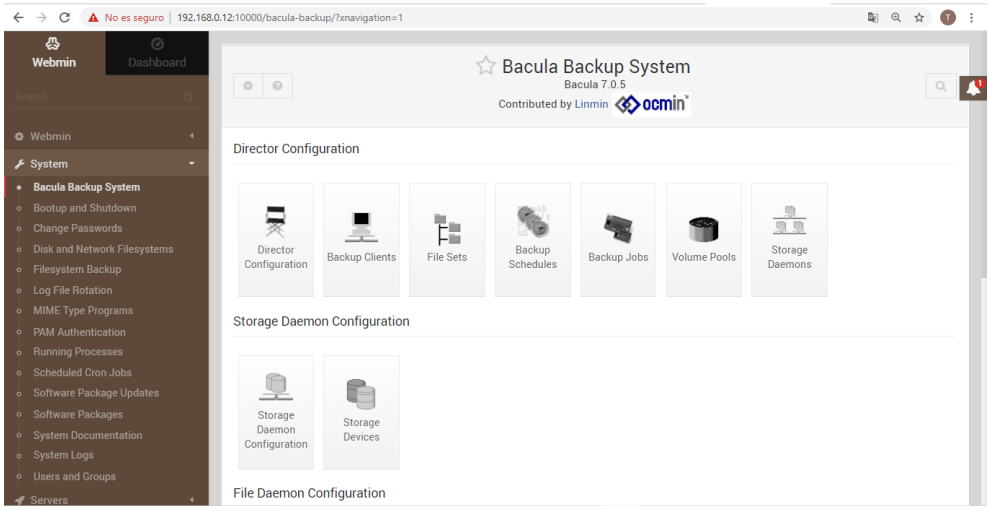
Figura 26. Interfaz admin - Bacula Schedule



Fuente: Los autores

En la figura 27 se presentan los módulos de configuración del administrador de la herramienta Bacula:

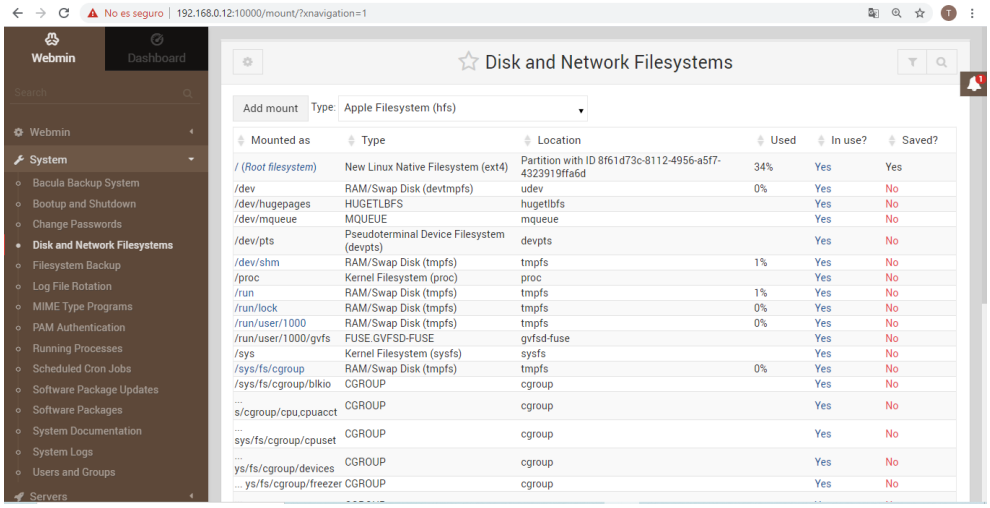
Figura 27. Interfaz admin - Bacula Backup System



Fuente: Los autores

En la figura 28f se configuran los sistemas de archivos que se encuentran en los servidores:

Figura 28. Interfaz admin - Disk and Network Filesystems - Bacula



Fuente: Los autores

6.3.3.4 Sandbox

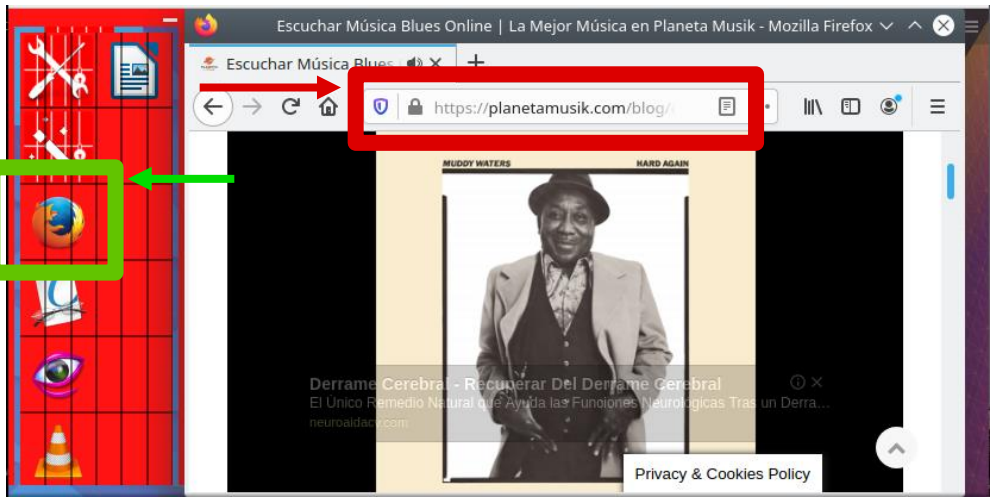
Como el nombre en inglés lo indica es “caja de arena” o herramienta de entorno controlado para proteger la máquina de algún programa que ha sido infectado y para no extender el virus. A la herramienta informática que se necesita analizar, se le asigna un entorno controlado del resto de los sistemas del servidor o incluso de computador personal. Si en el momento de la ejecución del programa que se está analizando en el Firejail de Sandbox tiene algún malware no permite que el resto de la máquina sea infectada.

6.3.3.4.1 Uso de Firejail de Sandbox

En la figura 29 se puede observar la reproducción de música desde un portal web sobre sandbox, ya que no se recomienda acceder en condiciones normales o ejecutar directamente en la máquina, pues es de los que más virus concentra y que se pueden descargar sin que el usuario se entere; pero en esta ocasión, no hay problema ya que se está ejecutando en el Firejail de manera controlada[81]:

[81] HARDLIMIT. “Firejail, Un sandbox universal para Linux”. {En línea}. 20 de febrero de 2015. {Consultado el 29 de noviembre de 2019}. Disponible en: https://hardlimit.com/firejail-un-sandbox-universal-para-linux/ http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

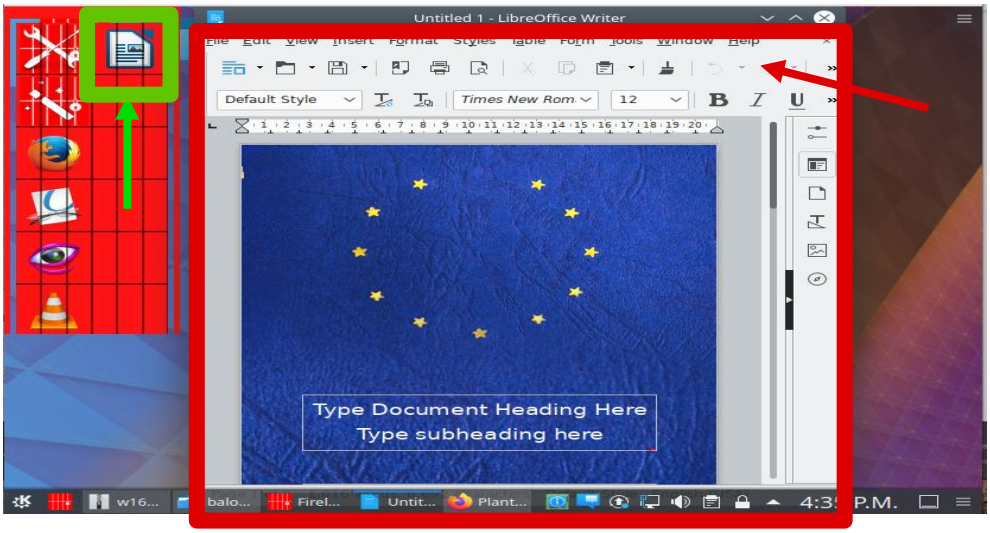
Figura 29. Página web de música desde Sandbox Firejail



Fuente: Los autores

En la figura 30 se observa un documento que se ha descargado desde un sitio en Internet sobre el sandbox ya que en condiciones normales no se recomienda ejecutarlo desde la máquina física, pues este tipo de archivos contiene muchos virus escondidos y una vez el usuario lo ejecuta instala el Malware que viene oculto el documento:

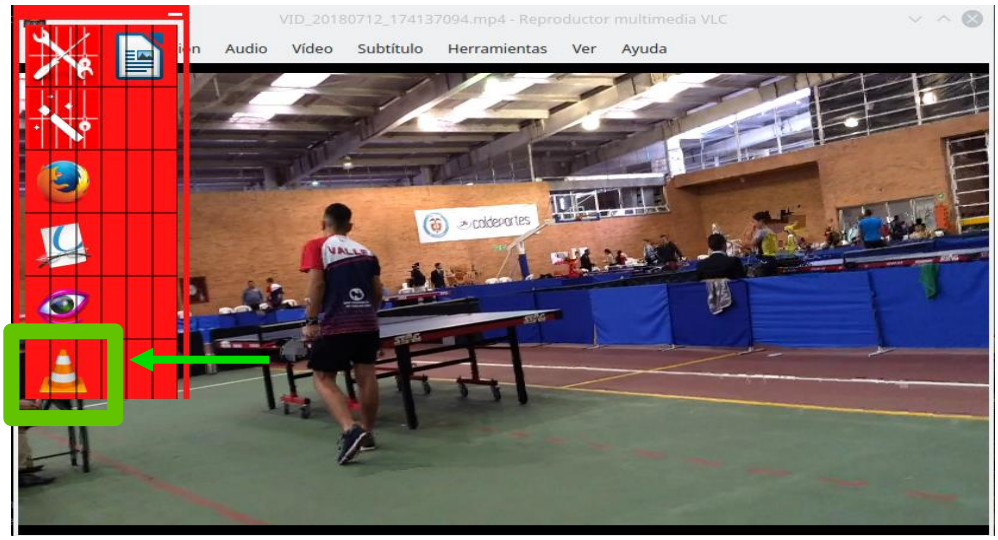
Figura 30. Documento descargado desde internet sobre Sandbox



Fuente: Los autores

Por último, en la figura 31 se muestra la reproducción de un video descargado desde un repositorio en Internet sobre Sandbox; no se recomienda su reproducción en la máquina física ya que los formatos mp4, avi, mpeg-4 mkv, mov, etc. (video) son de los más usados para ocultar virus y que, una vez lo reproduzca un usuario puede infectar su computadora:

Figura 31. Video descargado de repositorio en internet sobre Sandbox



Fuente: Los autores

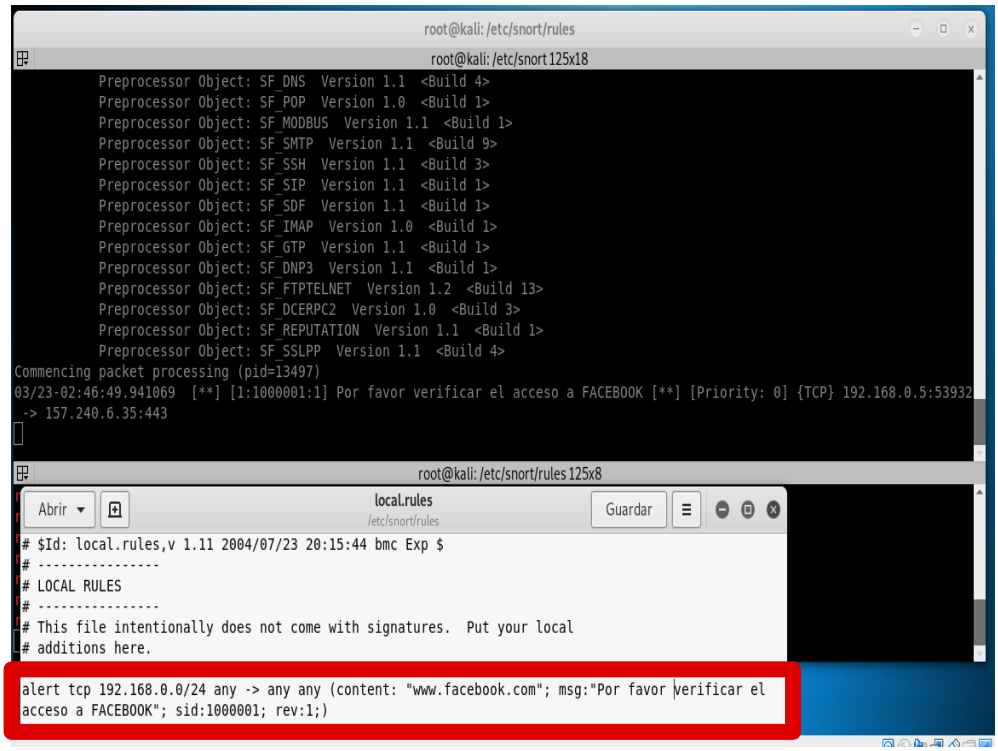
6.3.3.5 Snort

Es un Sistema de detección de intrusiones, contiene un motor para la detección de ataques, además, hace barrido de puertos el cual permite registrar, alertar y responder cualquier movimiento anómalo previamente configurado como posibles ataques, intentos de ataque a una vulnerabilidad, análisis de protocolos, todo en vivo[82].

En la figura 32 se puede observar una alerta generaba por Snort debido al acceso a la red social Facebook; esta alerta se genera debido a que previamente fue configurada la herramienta (/etc/snort/rules/local.rules) para que al momento que una máquina dentro del rango de la red configurada en Snort trate de acceder a este portal, se genere dicha notificación al administrador:

[82] ECURED. “Snort”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.ecured.cu/Snort

Figura 32. Ejemplo inclusión regla de alertamiento - Snort



Fuente: Los autores

6.3.3.6 Nmap

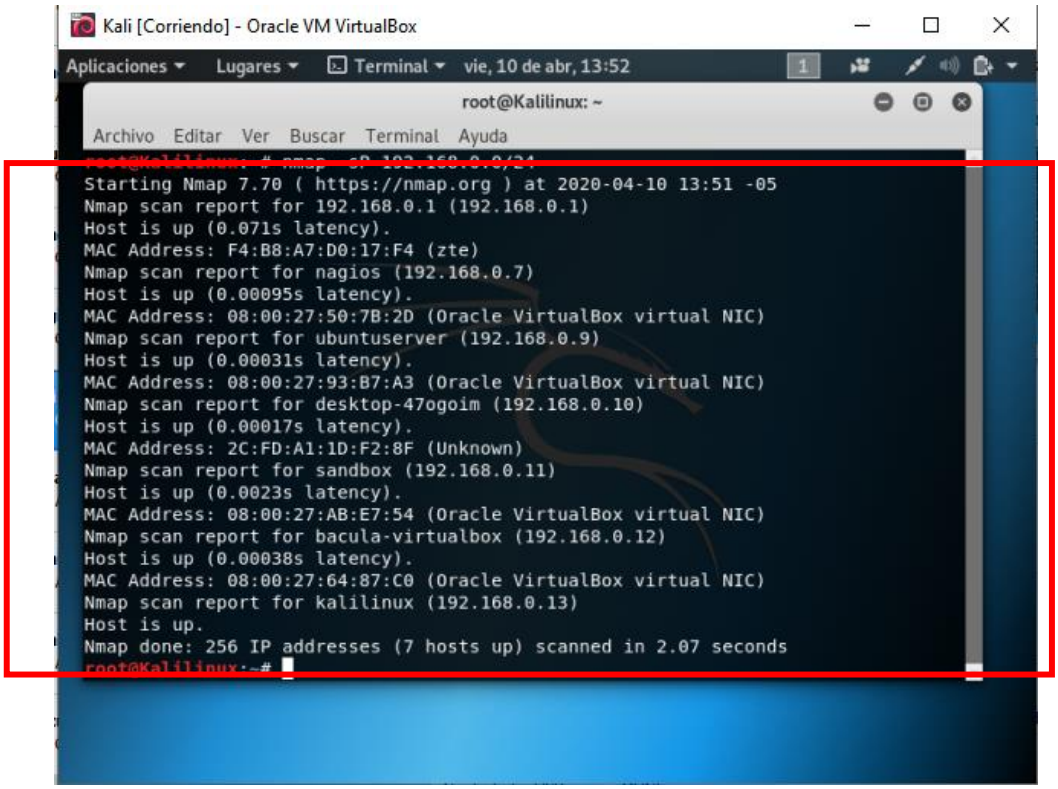
Es una herramienta de código abierto para realizar el descubrimiento de red y auditorías en redes. Adicionalmente, es utilizado para hacer el inventario de la red, planificar actualizaciones, monitorear dispositivos o servicios de red[83].

Para el proyecto se tiene instalada esta herramienta en su versión 7.7., la cual ya viene preinstalada en el sistema Kalilinux.

En la figura 33 se observa la utilización de la instrucción para establecer un ping sobre el segmento de red con máscara 24 y reconocer los equipos que hacen parte del segmento de red:

[83] REPORTE DIGITAL. “Descubre los servicios que ofrece Nmap para detectar riesgos de seguridad” {En línea}. 25 de abril de 2019. {Consultado el 29 de noviembre de 2019}. Disponible en https://reportedigital.com/iot/nmap/

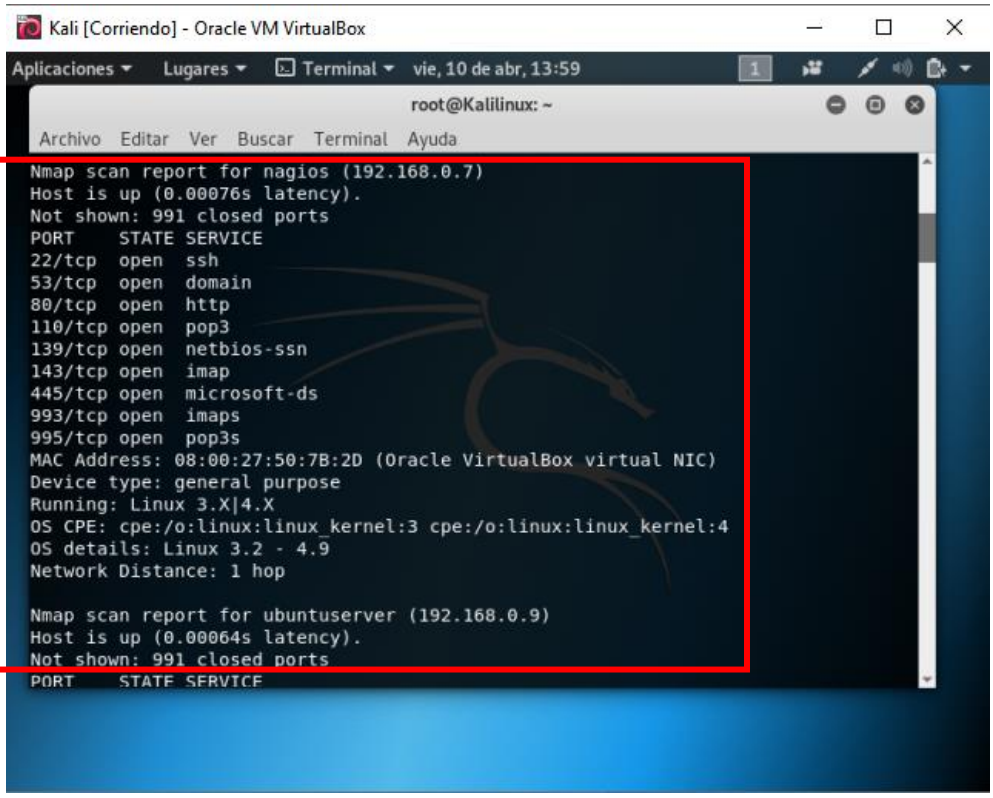
Figura 33. Escaneo de hosts en el segmento de red - Nmap



Fuente: Los autores

En la figura 34 se observa la ejecución de la instrucción para conocer el sistema operativo de los equipos en el segmento de red (Nmap -A 192.168.0.0/24) encontrando, por ejemplo, para el servidor Nagios, la versión del sistema operativo, la MAC address, los puertos escaneados, su estado y el servicio al que están asociados:

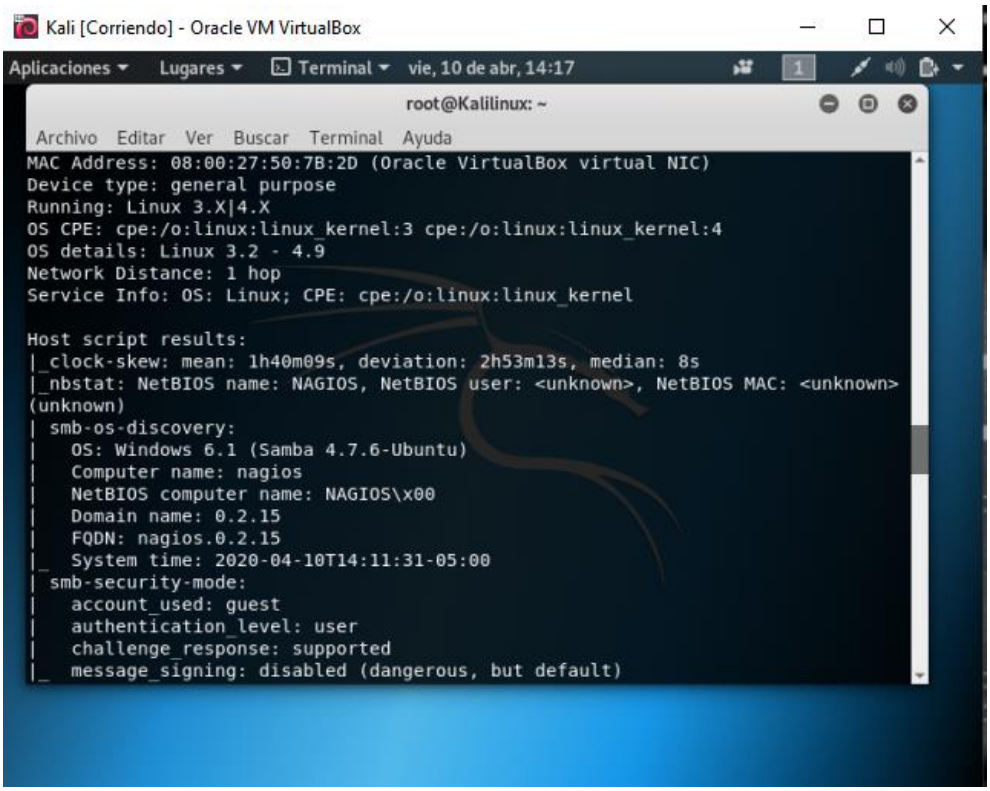
Figura 34. Detección sistema operativo, puertos y servicios - Nmap



Fuente: Los autores

En la figura 35 se observa la ejecución de la instrucción Nmap -A 192.168.0.0/24, para conocer el nombre de los equipos escaneados en el segmento de red, versión del sistema operativo, nombre de los servicios versiones de los servicios, descripción de workgroup, tipo de cuenta usada y su nivel de autenticación, el traceroute, la Mac Address, entre otros:

Figura 35. Detección de S.O. y versión, escaneo de scripts y traceroute - Nmap



Fuente: Los autores

Se pueden utilizar y combinar una variedad de parámetros o argumentos para ejecutar el Nmap, los cuales permiten especificar destinos a escanear, descubrir hosts, aplicar técnicas de escaneo, especificar puertos y orden de escaneo, detectar servicios/versiones, escanear script (tareas personalizadas), detectar sistemas operativos, tiempo y desempeño, realizar evasión y spoofing de firewall/IDS y realizar el control de salidas.

6.3.3.7 OpenVas

Es una herramienta open source para el escaneo de puertos y gestión centralizada de las vulnerabilidades de diversos sistemas e incluye un motor de correlación para cruzar todo lo que se ha identificado/detectado y proponer soluciones asociadas[84].

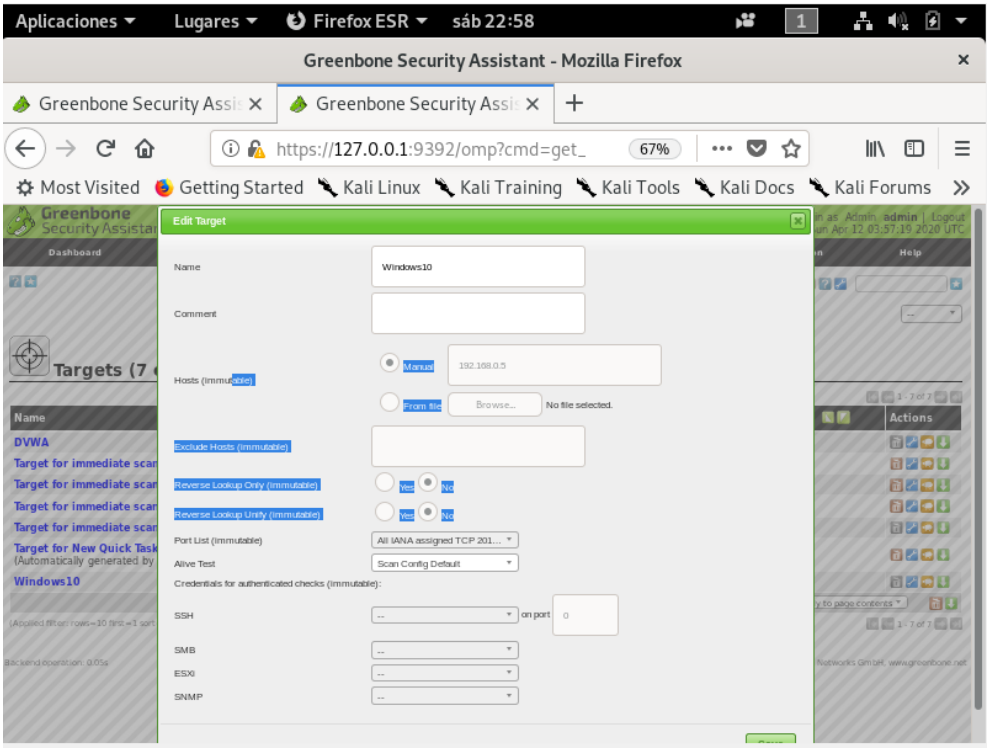
Para el laboratorio del proyecto se tiene instalada la versión 7.0.3 de la interfaz gráfica Greenbone Security Assistant de OpenVas.

---

[84] ALVÁREZ HUERTA, Leopoldo. “OpenVas en Linux: Explorando nuestros sistemas”. {En línea}. 30 de mayo de 2014. {Consultado el 29 de noviembre de 2019}. Disponible en:https://openwebinars.net/blog/openvas-en-linux-explorando-nuestros-sistemas/

En la figura 36 se presenta la interfaz gráfica para configurar los parámetros para el target (host destino):

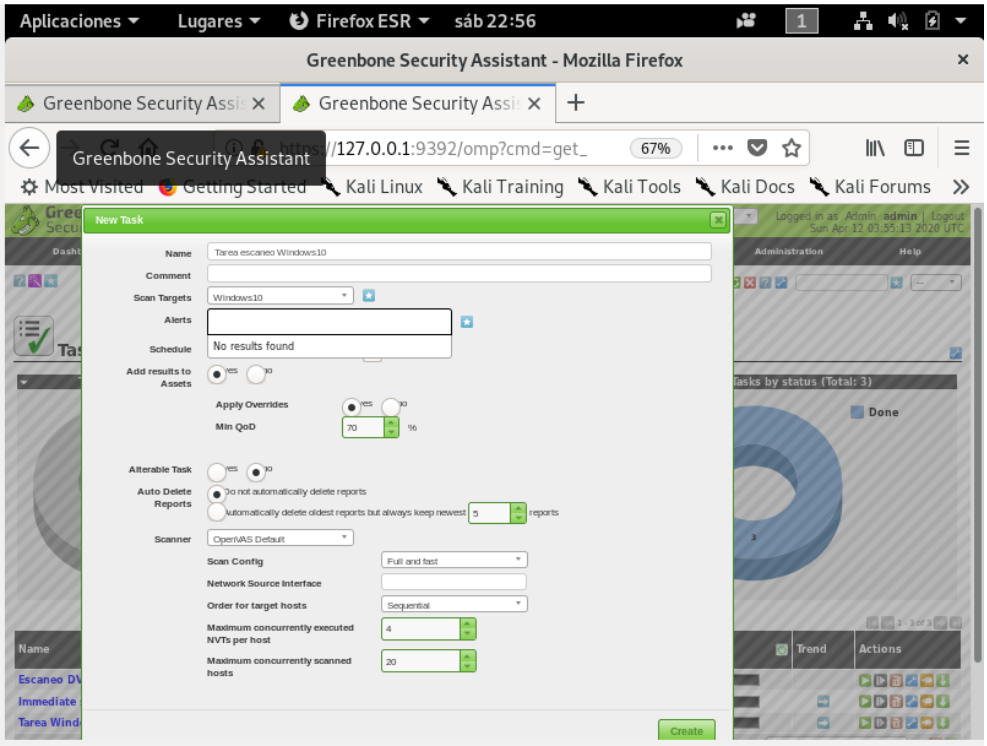
Figura 36. Parametrización target - OpenVas



Fuente: Los autores

En la figura 37 se presenta la interfaz gráfica para configurar los parámetros para la tarea (escaneo del target):

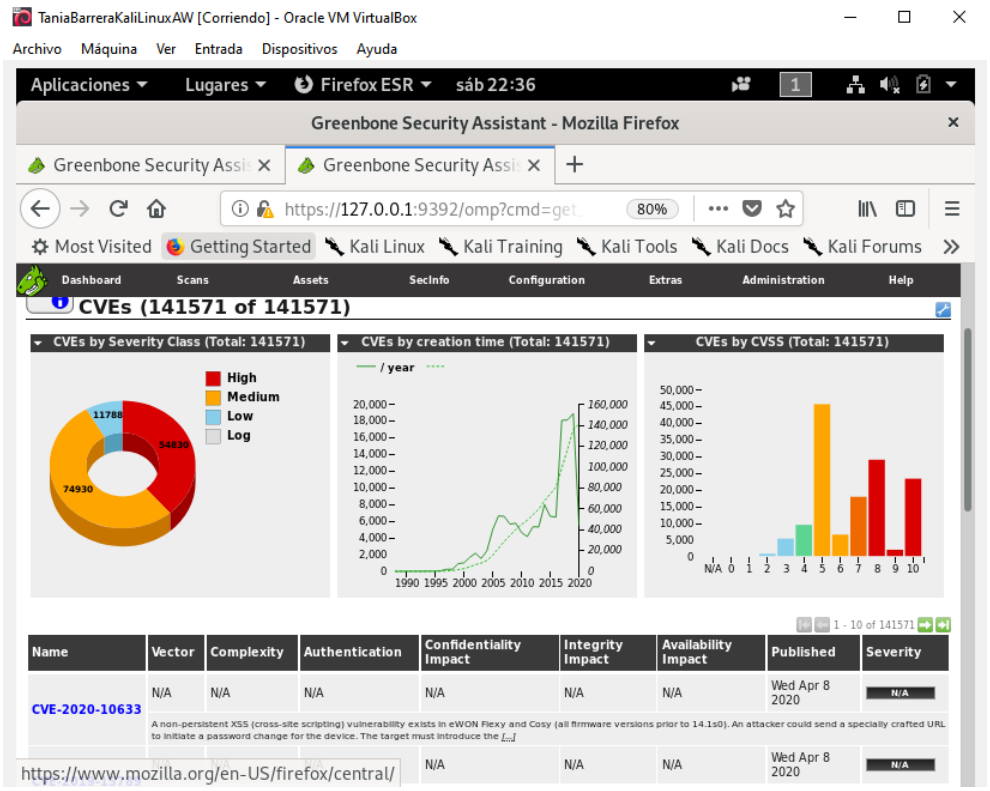
Figura 37. Parametrización tareas de escaneo - OpenVas



Fuente: Los autores

En la figura 38 se observa el listado de vulnerabilidades del CVE, frente a las cuales OpenVas validar las vulnerabilidades del target:

Figura 38. Listado CVE incluido en la base de datos de OpenVas



Fuente: Los autores

Los resultados generados por ésta corresponden a las vulnerabilidades encontradas en los targets escaneados. Le corresponde al administrador de esta herramienta verificar de manera manual si éstos son falsos positivos.

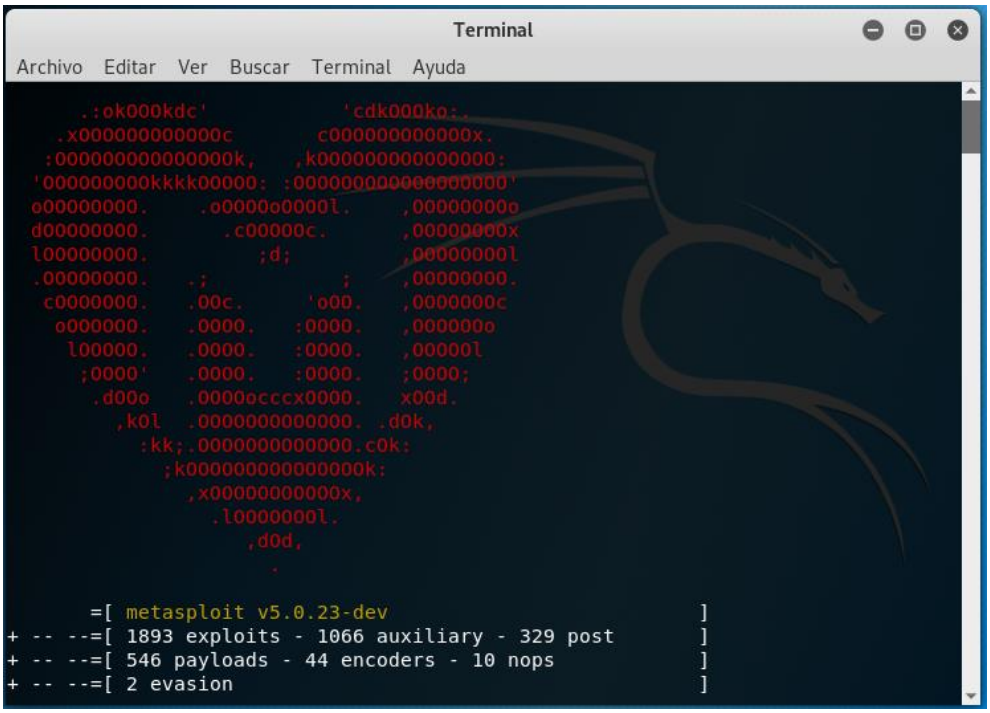
Adicionalmente el módulo “Scan management” permite realizar configuraciones asociadas a las tareas de exploración, realizando invalidaciones especialmente cuando se trate de falsos positivos; de esta forma, en el siguiente escaneo no serán reportados como vulnerabilidades.

6.3.3.8 Metasploit

Es una herramienta de uso libre, usada para llevar a cabo auditorías de seguridad informática. Dentro de sus características principales se encuentran: ofrece una cantidad considerable de exploits y el entorno para poder ejecutarlos, tiene gran flexibilidad de personalización por lo que se puede adecuar de acuerdo con las necesidades del negocio, y, cuenta con el respaldo de una comunidad de más de 200.000 usuarios que a diario brindan soporte y actualización.

En la figura 39 se presenta la consola de gestión de Metasploit, sobre la cual se ejecutan los exploits:

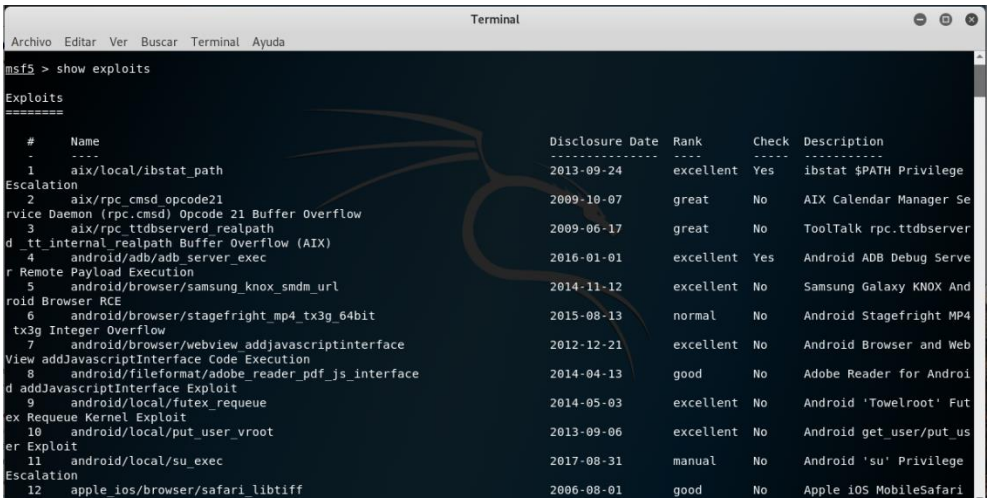
Figura 39. Consola de gestión - Metasploit



Fuente: Los autores

En la figura 40 se presenta la ejecución del comando show exploit muestra los exploits disponibles con nombre, fecha de divulgación, rango, check y una descripción. El listado de exploits es muy extenso y para usarlos es necesario conocer cuál es el target y cuáles son sus debilidades o vulnerabilidades:

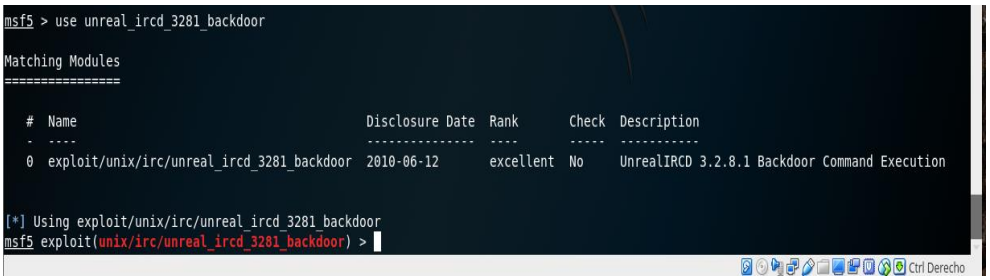
Figura 40. Listado de exploits disponibles - Metasploit



Fuente: Los autores

En la figura 41 se observa la selección de un exploit, para lo cual se debe ejecutar el comando -exploit- y luego el nombre del exploit; para este caso, se utilizará el unreal_ircd_3281_backdoor:

Figura 41. Uso de exploit unreal_ircd_3281_backdoor - Metasploit



Fuente: Los autores

6.3.3.9 GLPI

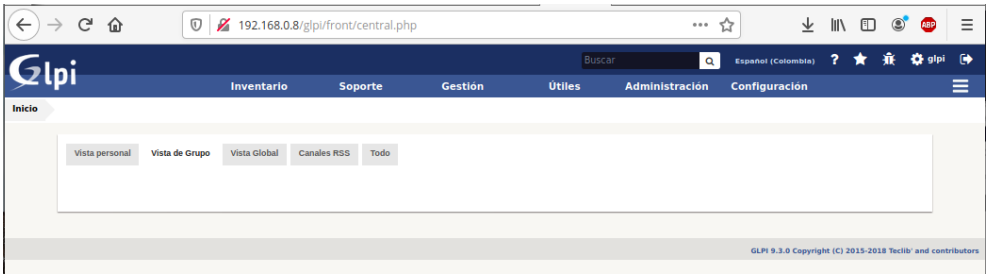
Es una herramienta de software libre que sirve para gestionar el inventario de equipos servidores, licencias etc., y como Helpdesk permite hacer seguimiento a los requerimientos de los usuarios y equipos, generando un historial detallado del mantenimiento[85].

[85] ECURED. “GLPI”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.ecured.cu/GLPI

En la interfaz web está disponible el inventario de los equipos tecnológicos y los usuarios asociados a éstos, los requerimientos desde su entrada, sus intervenciones o seguimientos hasta el cierre de los mismos.

En la figura 42 se puede observar la interfaz general de GLPI, donde se encuentran todas las opciones de accesos y configuraciones de la herramienta:

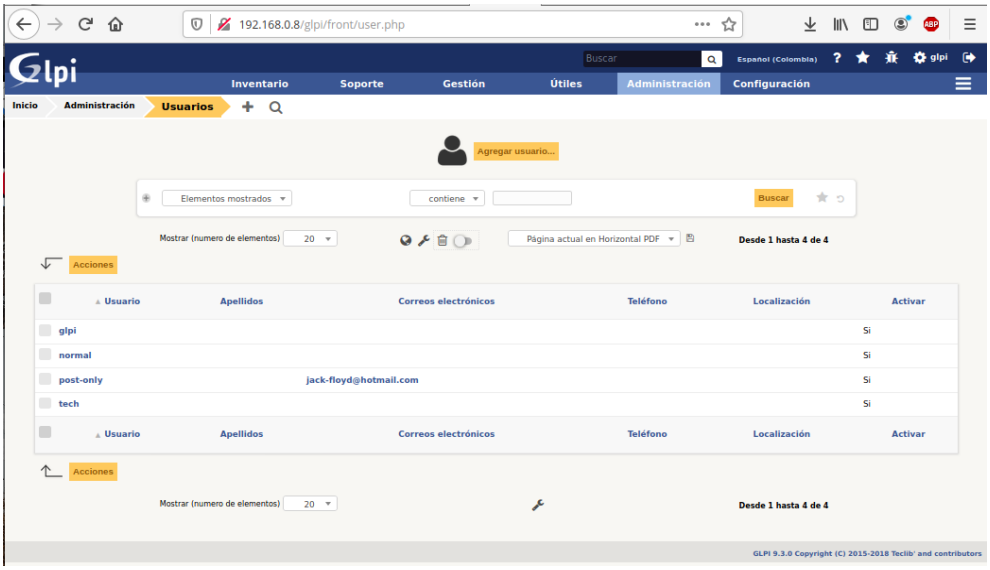
Figura 42. Interfaz web general - GLPI



Fuente: Los autores

En la figura 43 se puede observar la interfaz para la gestión de usuarios, en ella se pueden crear usuarios y asignarles un perfil de acuerdo con su roll en la organización:

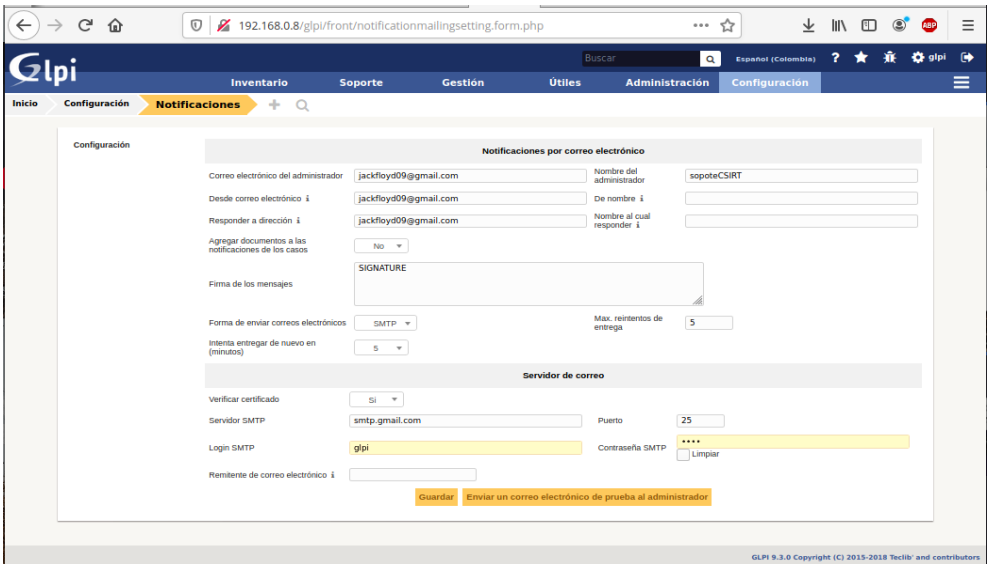
Figura 43. Administración de usuarios - GLPI



Fuente: Los autores

En la figura 44 se observa la interfaz para la configuración de notificaciones, en ésta se agrega el correo que los usuarios usarán para enviar requerimientos:

Figura 44. Configuración de notificaciones - GLPI



Fuente: Los autores

7 RESULTADOS Y DISCUSIÓN

Como resultado del desarrollo de los objetivos del proyecto, se seleccionaron las herramientas de hardware y software requeridas para un CSIRT, se establecieron las dependencias necesarias para su conformación, se definió el mapa de su estructura tecnológica, se elaboró el diseño lógico para el laboratorio y se alistaron y dejaron en funcionamiento los servidores y herramientas de software seleccionadas para el laboratorio del CSIRT.

El Gobierno Colombiano y algunas organizaciones nacionales y multinacionales han venido asignando en las últimas décadas recursos humanos, económicos y tecnológicos para la creación de equipos de trabajo, como los CSIRT, focalizados en atender las necesidades en seguridad de la información de las organizaciones y en la resolución de incidentes de seguridad que se puedan presentar; sin embargo, muchas empresas colombianas aún no conocen la importancia de estos grupos ni acuden a los mismos cuando presentan incidentes de seguridad de consideración.

Cada vez son más las empresas que han sido blanco de ataques informáticos contra sus activos (información, hardware, software, entre otros), lo que demuestra una vez más la poca importancia por la seguridad y protección de los mismos. La falta de recursos asignados a la seguridad informática, la poca cultura de las personas, la falta de políticas, la deficiencia en la aplicación de penas contra delitos informáticos y el poco acompañamiento por parte de grupos y entidades gubernamentales encargadas de liderar estos temas son las causas más comunes al momento de hablar de seguridad de la información.

El debate se debe abrir y enfocar en procura de la creación de políticas claras a nivel nacional que apalanquen la inyección de más recursos económicos para las entidades del estado y grupos especializados, el acompañamiento permanente y oportuno a las empresas privadas y públicas con el fin de robustecer la seguridad informática y convertirla en política de estado al servicio de la comunidad.

8 CONCLUSIONES

Con el desarrollo del presente proyecto, se puede concluir que las herramientas Open Source son fundamentales como apoyo a las operaciones de un CSIRT, puesto que, funcionalmente son competitivas y adicionalmente tienen una continua y gratuita actualización. Dichas herramientas hacen frente a las amenazas crecientes a las que están expuestos los sistemas de información y en la medida que sean actualizadas oportunamente, estas amenazas podrán ser prevenidas, o en caso de configurarse como incidentes, podrán ser contenidos, erradicados y solucionados rápidamente.

Se requiere de una variedad de herramientas, tanto libres como comerciales, para poder cubrir los diferentes aspectos que se gestionan en un CSIRT. Es por esto que el factor económico cobra importancia a la hora de seleccionar las herramientas a implementar en el laboratorio.

9 RECOMENDACIONES

Dada la constante evolución del software (sistemas operativos, herramientas de seguridad, herramientas de comunicaciones, entre otros) se hace cada vez más importante y necesario el uso de software libre y de código abierto, el cual, además de robusto y económico, permite el aporte de comunidades que continuamente están explorando nuevas funcionalidades, actualizaciones y mejoras a los sistemas, que incluyen los parches de seguridad para evitar su exposición a ataques.

Para dar continuidad al presente proyecto, se recomienda gestionar el apoyo del Estado para lograr el patrocinio de las fases siguientes del proyecto para que el mismo sea una herramienta que puedan aprovechas tanto las entidades públicas y privadas. Todo esto apalancado en las nuevas políticas nacionales de seguridad digital que promueven la generación de CSIRTS sectoriales.

Para los proyectos evaluados como sobresalientes y sostenibles, tanto en pregrado como en especializaciones y maestrías, es de vital importancia que la UNAD impulse su implementación en escenarios reales con el fin de que éstos impulsen la generación de conocimiento, fuentes de trabajo, nuevos proyectos y aporten de una manera efectiva a la atención de las necesidades actuales de las instituciones y la comunidad, en los diferentes campos de aplicación en los que se enfoca la Universidad.

10 DIVULGACIÓN

Se autoriza la preservación, conservación, modificación, transformación tecnológica, uso y divulgación del presente documento a la Universidad Nacional Abierta y a Distancia.

11 BIBLIOGRAFÍA

ACCESS DATA. “Imager User Guide”. {En línea}. 31 de marzo de 2016 {Consultado el 29 de noviembre de 2019}. Disponible en: https://ad-pdf.s3.amazonaws.com/Imager/3_4_3/FTKImager_UG.pdf

ACCESS DATA. “LIT FTK specification guide 6.3”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://support.accessdata.com/hc/en-us/article_attachments/360004988813/LIT_FTK_specification_guide_6.3.pdf

ALIBABACLOUD. “How to Install OSSEC on Ubuntu 16.04”. {En línea}. 15 de julio de 2019. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.alibabacloud.com/blog/how-to-install-ossec-on-ubuntu-16-04_595080

ALVÁREZ HUERTA, Leopoldo. “OpenVas en Linux: Explorando nuestros sistemas”. {En línea}. 30 de mayo de 2014. {Consultado el 29 de noviembre de 2019}. Disponible en:https://openwebinars.net/blog/openvas-en-linux-explorando-nuestros-sistemas/

AMOEDO, Damián. “Ubunlog. Firejail, ejecuta de forma segura aplicaciones no confiables en Ubuntu”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://ubunlog.com/firejail-ejecuta-aplicaciones-ubuntu/

ARSYS. “Cómo crear un Servidor Cloud para gestionar el correo electrónico con Zimbra”. {En línea}. 27 de enero de 2016. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.arsys.es/blog/soluciones/cloud/cloud-computing/crear-servidor-cloud-gestionar-correo-electronico-zimbra/

AUTOPSY DIGITAL FORENSICS. “Online Autopsy Forensics Tool Training”. {En línea}. 26 de junio de 2014. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.autopsy.com/online-autopsy-forensics-tool-training-sept-24-2014/

BALDERRAMA, Julio Cesar. “Como crear un CSIRT Fundamentos”. {En línea}. 22 de octubre de 2017 {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.youtube.com/watch?v=2huboveQFLs

BIENESTAR FAMILIAR. “Procedimiento gestión de incidentes de seguridad de La información”. {En línea}. 27 de noviembre de 2018. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.icbf.gov.co/sites/default/files/procesos/p5_gti_procedimiento_gestion_de_incidentes_de_seguridad_de_la_informacion_v5.pdf

CANTOS, Manel. “Servicios de gestión de la seguridad de la información, un caso de éxito.” {En línea}. Agosto 25 de 2016. {Consultado el 29 de noviembre de 2019}. Disponible en: https://blog.altran.es/altran-smart-society/gestion-seguridad-de-la-informacion/.

CLARET INFORMATICA 2º DE ASIR. “Requisitos necesarios para instalar SAMBA en un sistema Linux”. {En línea}. 24 de enero 24 de 2014. {Consultado el 29 de noviembre de 2019}. Disponible en: http://claretinformaticaasir.blogspot.com/2014/01/requisitos-necesarios-para-instalar.html

COLTRIN, Jason. “Integrate OpenDNS Umbrella with Active Directory”. {En línea}. 5 de septiembre de 2016. {Consultado el 29 de noviembre de 2019}. Disponible en: https://4sysops.com/archives/integrate-opendns-umbrella-with-active-directory/

COMPUTER FORENSICS FOR EVERYONE. “Installing FTK Imager Lite in Linux Command Line”. {En línea}. 22 de febrero de 2013{Consultado el 29 de noviembre de 2019}. Disponible en: http://comp4n6.blogspot.com/2013/02/using-sans-siftworkstation-you-have.html

COMPUTERWORLD. “Predicciones de seguridad para 2020”. {En línea}. Noviembre 26 de 2018 {Consultado el 20 de enero de 2020}. Disponible en: https://computerworld.co/predicciones-de-seguridad-para-2020/

CONEXIÓN CAPITAL. “En Bogotá se registraron más 6.000 denuncias por delitos cibernéticos en 2018”. {En línea}. 5 de febrero 5 de 2019. {Consultado el 29 de noviembre de 2019}. Disponible en: https://conexioncapital.co/bogota-denuncias-delitos-ciberneticos/

CONGRESO DE LA REPÚBLICA DE COLOMBIA. “Ley Estatutaria 1266 de 2008 (Habeas Data)”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: http://ticbogota.gov.co/node/137

DEPARTAMENTO NACIONAL DE PLANEACIÓN. “Política nacional de explotación de datos (big data)”. {En línea}. 17 de abril de 2017 {Consultado el 29 de noviembre de 2019}. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3920.pdf

DESDELINUX. “OpenDNS: servidor DNS para navegar más rápido y seguro en Internet”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://blog.desdelinux.net/opendns-servidor-dns-para-navegar-mas-rapido-y-seguro-en-internet/

DIGITAL LEARNING. “¿Qué hace un Servidor Web como Apache? Configuración”. {En línea}. 17 de marzo de 2012. {Consultado el 29 de noviembre de 2019}.

Disponible en: https://www.digitallearning.es/blog/apache-servidor-web-configuracion-apache2-conf/

DINERO. “Guía de ciberseguridad para el 2019 - ¿Cuáles son las tendencias y retos este año en materia de ciberseguridad? (s.f.) Revista Dinero”. {En línea}. 1 de junio de 2019. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.dinero.com/tecnologia/articulo/ciberseguridad-en-el-2019-en-colombia/265858

ECURED. “GLPI”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.ecured.cu/GLPI

ECURED. “Nagios”. {En línea}. {Consultado el 17 de mayo de 2020}. Disponible en: https://www.ecured.cu/Nagios

ECURED. “Servidor HTTP Apache”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.ecured.cu/Servidor_HTTP_Apache

ECURED. “Snort”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.ecured.cu/Snort

EISF BRIEFING PAPER. “Crisis Management of Critical Incidents”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.eisf.eu/wp-content/uploads/2014/09/0121-Buth-2010-Crisis-Management-of-Critical-incident-2010.pdf.

FIREJAIL. “Firejail security sandbox”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://firejail.wordpress.com/features-3/

Firejail Security Sandbox. “Firejail Usage”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://firejail.wordpress.com/documentation-2/basic-usage/

FIREST. “Foro sobre los equipos de seguridad e intervención en caso de incidente”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.first.org/education/FIRST_SIRT_Services_Framework_Version1.0-es.pdf

FIRST. “Forum of incident response and security teams”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.thegfce.com/members-and-partners/partners/forum-of-incident-response-and-security-teams-first

FORENSIC UPDATES. “Comparison of Hardware Requirements”. {En línea}. 15 de marzo de 2012. {Consultado el 29 de noviembre de 2019}. Disponible en:

http://forensicupdates.blogspot.com/2012/03/comparison-of-hardware-requirements.html

GEEKLAND. “Firejail, un sandbox para Linux para ejecutar programas de forma segura”. {En línea}. 4 de septiembre de 2017. {Consultado el 29 de noviembre de 2019}. Disponible en: https://geekland.eu/firejail-sandbox-para-linux/

GIZTAB. “Características principales y primeros pasos”. {En línea}. Septiembre 9 de 2018. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.giztab.com/wordpress-caracteristicas-principales-y-primeros-pasos/

GLPI Project. “Install the GLPI application”. {Consultado el 29 de noviembre de 2019}. Disponible en: https://glpi-project.org/DOC/EN/

GÓMEZ PARADELA, Carlos Alberto; MARTÍNEZ GÓMEZ, Mario Tomás. “Manual Instalación Zimbra 6.x.x en Debian Lenny”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://gutl.jovenclub.cu/wiki/doku.php?id=/manuales:zimbra

HACKING. “Hacking con kali linux”. {en línea}. (Consultado el 29 de noviembre de 2019). Disponible en: https://hackingkalinux.com/

HARDLIMIT. “Firejail, Un sandbox universal para Linux”. {En línea}. 20 de febrero de 2015. {Consultado el 29 de noviembre de 2019}. Disponible en: https://hardlimit.com/firejail-un-sandbox-universal-para-linux/
http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

HUÉRFANO, Sandra y ROBAYO, Omar. “Diseño de un CSIRT”. {En línea} {Consultado el 29 de noviembre de 2019}. Disponible en: https://app.emaze.com/@AOFCRTCTT/csirt#11.

HUERTAS, Leonardo. “Estructura interna de un CSIRT”. {En línea}. 2 de octubre de 2016 {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.youtube.com/watch?v=RaBp3qsxQYY.

ICONTEC INTERNACIONAL. "Guía Técnica Colombiana GTC-ISO/IEC 27035 Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información”. {En línea}. 12 de diciembre de 2012. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.academia.edu/37861509/GU%C3%8DA_T%C3%89CNICA_GTC-ISO_IEC_COLOMBIANA_27035_TECNOLOG%C3%8DA_DE_LA_INFORMACI%C3%93N._T%C3%89CNICAS_DE_SEGURIDAD._GESTI%C3%93N_DE_INCIDENTES_DE_SEGURIDAD_DE_LA_INFORMACI%C3%93N.

IGLESIAS, Leonardo Rafael. “Herramientas Open Source para Informática Forense”. {En línea}. 2015. {Consultado el 29 de noviembre de 2019}. Disponible en: http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0187_IglesiasLF.pdf

INTERNET YA. “Beneficios de un servidor de correo Zimbra para entidades en Colombia”. {En línea}. Abril 10 de 2019. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.internetya.co/beneficios-de-un-servidor-de-correo-zimbra-para-entidades-en-colombia/

LANCHEROS PADILLA, Lizeth Katherine. “Implementación de la herramienta de software libre GLPI para sistematizar la mesa de ayuda (help desk) del hospital infantil Universitario de San José”. {En línea}. 2016. {Consultado el 29 de noviembre de 2019}. Disponible en: https://repository.libertadores.edu.co/bitstream/handle/11371/1339/lancheroslizath 2016.pdf?sequence=1

LASSER. “Cómo proteger información en un data center”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://grupolasser.com/como-proteger-informacion-en-un-data-center/

LIKE GEEKS. “Servidor De Archivos Linux Usando Samba.” {En línea}. 27 de marzo de 2017. {Consultado el 29 de noviembre de 2019}. Disponible en: https://likegeeks.com/es/servidor-de-linux-samba/.

LINKEDIN. “Entendiendo los CSIRT: responsabilidades, roles y diferencias respecto a un SOC y CERT”. {En línea}. 6 de agosto de 2018. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.linkedin.com/pulse/entendiendo-los-csirt-responsabilidades-roles-y-respecto-cargill-1f

MALAGÓN, Chelo. “Organización y operación de un CSIRT”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.rediris.es/cert/doc/reuniones/fs2004/archivo/csirt.pdf.

MANCOMUN. “OSSEC: Sistema de detección de intrusos”. {En línea}. Noviembre 3 de 2017. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.mancutai, omun.gal/es/artigo-tic/ossec-sistema-de-deteccion-de-intrusos/

MENDOZA, Miguel Ángel. “¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes?”. {En línea}. 18 de mayo de 2015 {Consultado 18 de mayo de 2015}. Disponible en: https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “Lineamientos de política para la Ciberseguridad y

Ciberdefensa.”. {En línea}. 14 julio de 2011. {Consultado el 29 de noviembre de 2019}. Disponible en: https://mintic.gov.co/portal/604/articles-3510_documento.pdf

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “Consejo Nacional de Política Económica y Social República de Colombia”. {En línea}. 2016 {Consultado el 29 de noviembre de 2019}. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

MINTIC. “Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

MORALES GONZÁLEZ, Carlos Andrés, MORENO SÁNCHEZ, Omar Enrique y ORTIGOZA PÉREZ, Johanna Nathalie. “Propuesta de un modelo de centro de operaciones de seguridad (SOC) para Fuerza Aérea Colombiana.” {En línea}. 2014. {Consultado el 29 de noviembre de 2019}. Disponible en: http://polux.unipiloto.edu.co:8080/00001627.pdf

MUTAI, Josphat. “How to Install OSSEC HIDS on Ubuntu 18.04 / 16.04 / Debian 9.” {En línea}. 12 diciembre de 2018{Consultado el 29 de noviembre de 2019}. Disponible en: https://computingforgeeks.com/how-to-install-ossec-hids-on-ubuntu-18-04-16-04-debian-9/

NORTH NETWORKS. “Que es Nagios?”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.north-networks.com/fabricante/que-es-nagios/

OEA. “Buenas Prácticas para establecer un CSIRT nacional”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.sites.oas.org/cyber/Documents/2016 - Buenas Prácticas CSIRT.pdf

ORTEGO DELGADO, Daniel. “Qué es Snort: Primeros pasos”. {En línea}. 21 de marzo de 2017. {Consultado el 29 de noviembre de 2019}. Disponible en: https://openwebinars.net/blog/que-es-snort/

PC RESUMEN. “Virtualización con Oracle VM VirtualBox”. {En línea}. 21 de mayo de 2019. {Consultado el 29 de noviembre de 2019}. Disponible en https://www.pcresumen.com/menu-software/31-virtualizacion/41-virtualizacion-con-oracle-vm-virtualbox

PCGAMEBENCHMARK. “Universe Sandbox System Requirements”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.pcgamebenchmark.com/universe-sandbox-system-requirements

PROFESIONALES review. “Como instalar Kali Linux en VirtualBox” 02 de enero de 2019. {en linea}. (Consultado el 29 de noviembre de 2019). Disponible en: https://www.profesionalreview.com/2019/01/02/instalar-kali-linux-virtualbox/

MORALES, Carlos, MORENO, Omar Enrique, ORTIGOZA, Johanna. Propuesta de un modelo de centro de operaciones de seguridad (SOC) para Fuerza Aérea Colombiana. {En línea}. 2014. {Consultado el 29 de noviembre de 2019}”. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2786/trabajo%20de%20grado1627.pdf?sequence=1

RAMOS, David. “A fondo: ¿Cómo funcionan los SOC?”. {En línea}. 21 de noviembre de 2017. {Consultado el 29 de noviembre de 2019}”. Disponible en: https://www.silicon.es/a-fondo-como-funcionan-soc-2362658.

RAPID7. “System Requirements and Documentation”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.rapid7.com/products/metasploit/system-requirements/

REDES - LABORATORIO DE SEGURIDAD INFORMÁTICA Y REDES. “OpenVAS: Instalación, configuración y prueba”. {En línea}. 11 de mayo de 2018. {Consultado el 29 de noviembre de 2019}. Disponible en: http://redeslinuxinternet.blogspot.com/2018/05/openvas-instalacion-configuracion-y.html

REPORTE DIGITAL. “Descubre los servicios que ofrece Nmap para detectar riesgos de seguridad”. {En línea}. 25 de abril de 2019. {Consultado el 29 de noviembre de 2019}. Disponible en https://reportedigital.com/iot/nmap/

RIQUELME, Rodrigo. “¿Qué es un Equipo de Respuesta ante Emergencias Informáticas (CERT)?”. {En línea}. 22 enero de 2018 {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.eleconomista.com.mx/tecnologia/Que-es-un-Equipo-de-Respuesta-ante-Emergencias-Informaticas-CERT-20180122-0009.html

RODRÍGUEZ URIBE, Edson Dirceu y PORRAS MEDINA, Carlos Hernán. “Snort”. {En línea}. Julio 2006. {Consultado el 29 de noviembre de 2019}. Disponible en: http://168.176.47.172/media/files/UIFCE/Otros/Snort.pdf

RODRÍGUEZ, Marcos. “BACULA BACKUP: Instalación del servidor”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://vivaubuntu.com/bacula-backup-instalacion-del-servidor/

ROMERO GONZÁLEZ, Rafael. “Instalación y configuración de nagios core 4.0.4.” {En línea}. Junio de 2015. {Consultado el 29 de noviembre de 2019}. Disponible en:

https://exchange.nagios.org/components/com_mtree/attachment.php?link_id=6527&cf_id=24

SALAZAR CHAMORRO, Liliana Teresa. “Implementación de un servidor linux”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: http://www.fce.unal.edu.co/media/files/UIFCE/Otros/Implementacionde_un_Servidor_Linux.pdf

SÁNCHEZ LORENTE, Olga. Detección de intrusiones con SNORT. {En línea}. Junio de 2015. {Consultado el 17 de mayo de 2020}. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/43090/6/osanchezloTFM0715memoria.pdf

SEAQ SERVICIOS SAS. “Nagios es una Herramienta Open source de monitoreo”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.seaq.co/nagios.html

SECRETARÍA DEL SENADO. “Constitución política de Colombia”. {En línea}. 31 de diciembre de 2019. {Consultado el 29 de noviembre de 2019}. Disponible en:

SENADO DE LA REPÚBLICA. “Código Disciplinario Único”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0734_2002.html

SERVIDOR SAMBA: “conceptos y configuración rápida”. {En línea} 25 de marzo de 2017. {Consultado el 29 de noviembre de 2019} https://www.profesionalreview.com/2017/03/25/servidor-samba-conceptos-y-configuracion-rapida/

SLEUTHKIT. “autopsy User Documentation”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://sleuthkit.org/autopsy/docs/user-docs/4.8.0/installation_page.html

SNORT.ORG. “Snort”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.snort.org/

SUPERINTENDENCIA FINANCIERA DE COLOMBIA. “Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: http://tramites1.suit.gov.co/registro-web/suit_descargar_archivo?A=17433

SYSADM.ES. “Instalación y configuración de Nagios”. {En línea}. Abril 23 de 2018. {Consultado el 29 de noviembre de 2019}. Disponible en: https://sysadm.es/instalacion-y-configuracion-de-nagios/

ULTIMOBYTE. “BACULA, OPEN SOURCE BACKUP”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.ultimobyte.es/productos/bacula-enterprise-open-source-backup

UNIVERSIDAD AUTÓNOMA DE OCCIDENTE. “Elementos de anteproyecto modalidad “pasantía institucional”. {En línea}. 21 de enero de 2011. {Consultado el 19 de noviembre de 1029}. Disponible en: https://www.uao.edu.co/sites/default/files/Anteproyecto_Pasant%C3%Ada_Institucional.pdf

US NATIONAL LIBRARY OF MEDICINE NATIOSAL INSTITUTES OF HEALTH. “Computer security incident response team effectiveness”. {En línea} 12 de diciembre de 2017. {Consultado el 20 de noviembre de 2019}. Disponible en: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5733042/

UYANA, Mónica y ESCOBAR, Milton. “Propuesta de diseño de un área informática forense para un equipo de respuestas ante incidentes de seguridad informáticos (CSIRT)”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://docplayer.es/4456551-Propuesta-de-diseno-de-un-area-informatica-forense-para-un-equipo-de-respuestas-ante-incidentes-de-seguridad-informaticos-csirt.html

WIKIPEDIA. “Servidor HTTP Apache”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://es.wikipedia.org/wiki/Servidor_HTTP_Apache

WORDPRESS. “Cuáles son los requerimientos de un servidor para instalar WordPress”. {En línea}. Agosto 14 de 2014 {Consultado el 29 de noviembre de 2019}. Disponible en: http://wordpress.comocreartuweb.com/cuales-son-los-requerimientos-de-un-servidor-para-instalar-wordpress-511.html

WIRESHARK.ORG. “System Requirements”. {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: .https://www.wireshark.org/docs/wsug_html_chunked/ChIntroPlatforms.html

ZIMBRA, A SYNACOR PRODUCT. “Zimbra” {En línea}. {Consultado el 29 de noviembre de 2019}. Disponible en: https://www.zimbra.com/

ANEXO 1. LINK DEL VIDEO

https://youtu.be/-Xt8EsGV0dY