DISEÑO DE LA PROPUESTA TÉCNICA PARA CONSOLIDACIÓN DE UN CENTRO DE OPERACIONES DE CIBERSEGURIDAD - SOC EN LA EMPRESA PLATINO SISTEMAS

DANIEL BERNAL HERNANDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2021

DISEÑO DE LA PROPUESTA TÉCNICA PARA CONSOLIDACIÓN DE UN CENTRO DE OPERACIONES DE CIBERSEGURIDAD - SOC EN LA EMPRESA PLATINO SISTEMAS

DANIEL BERNAL HERNANDEZ

Proyecto de Grado – Proyecto aplicado como alternativa de trabajo de grado de ESPECIALISTA EN SEGURIDAD INFORMATICA

Tutor
Luis Fernando Zambrano
Director
Christian Angulo Rivera

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2021

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá., octubre de 2021

AGRADECIMIENTOS

Agradezco a mi familia la cual me ha apoyado siempre en mis estudios y demás decisiones importantes en mi vida.

CONTENIDO

pág.

LISTA DE FIGURAS

LISTA DE CUADROS

LISTA DE ANEXOS

GLOSARIO

- **AD-DC**: Directorio activo – controlador de dominio
- **Aircrack-ng:** suite de software de seguridad inalámbrica
- **Aircrack-ng: S**uite de software para la auditoria en redes inalámbricas
- **Amenaza**: aprovechamiento de una vulnerabilidad para sacar beneficio de ella.
- **Ataque cibernético**: acción premeditada de una o varias personas que causan deterioro a un sistema de información
- **CERT**: Equipo de respuesta para emergencias informáticas
- **Ciberdefensa:** capacidad de neutralizar ataques informáticos y contrarrestar incidentes y amenazas informáticas que afecta la soberanía nacional
- **Confidencialidad:** es la garantía de que la información será protegida para que no sea divulgada sin su respectiva aprobación
- **CSIRT Interno**: se encarga de proporcionar servicios de manejos de incidentes en su propia organización
- **CSIRT**: Equipo de respuestas ante emergencias informáticas
- **Disponibilidad**: propiedad de la información de estar accesible y disponible en el momento en el que sea requerida.
- **Falsos positivos**: detección de virus o malware por parte de los sistemas de seguridad cuando no lo es
- **Hydra:** Programa para crackear contraseñas
- **IDS**: Sistema de detección de intrusiones.
- **Incidente informático**: evento en el cual se ve comprometida la seguridad de un sistema informático, redes u ordenadores.
- **IPS**: Sistema de prevención de intrusiones.
- **Jhon the Ripper:** Programa de criptografía que aplica fuerza bruta para descifrar contraseña

- **Kali Linux:** Distribución de Linux basada en Debian, diseñada para la auditoria y seguridad informática
- **Metasploit:** Programa de ayuda para los test de penetración
- **MISP:** Plataforma de inteligencia contra amenazas
- **Nmap:** Programa para rastrear los puertos lógicos de los equipos de computo
- **Pentesting:** Examen de penetración a un sistema de información
- **RED**: Conjunto de equipo de cómputo y nodos unidos entre sí.
- **Seguridad Informática**: Disciplina que se encarga de proteger la integridad y privacidad de la información.
- **SIEM**: Security Information Event Management
- **SIEM:** Sistema de centralizado para la interpretación de datos y almacenamiento de información distinguida a seguridad informática
- **Snort**: Sistema de detección de intrusos.
- **SO**: Sistema Operativo.
- **SOC**: Centro de operaciones de seguridad
- **Sqlmap:** Herramienta desarrollada para realizar inyección de código sql
- **UPS**: Sistema de alimentación ininterrumpida
- **Vulnerabilidad**: debilidad o fallo de un sistema de información
- **WAZUH:** Sistema de detección de intrusos de código abierto
- **Wireshark:** Programa para analizar protocolos y tráfico de red

RESUMEN

Platino Sistemas es una compañía colombiana la cual presta servicios de seguridad y protección de la información, la cual tiene proyectado crear un SOC (centro de operaciones y seguridad), que tiene como objetivo crear y gestionar las respuestas a ataques informáticos, ofreciendo la mejor respuesta a incidentes y gestión de vulnerabilidades.

El departamento de Tecnologías de la Información y comunicaciones (TIC), como líder del diseño técnico que permite dar desarrollo a las actividades del SOC, presenta la propuesta técnica para la implementación del Centro de Operaciones y Seguridad -SOC[1] para la empresa Platino Sistemas, el cual tiene como objetivo prevenir, monitorear y controlar todo lo relacionado con seguridad informática en la organización.

En el diseño técnico del Equipo de Respuesta a Incidentes de Seguridad, se requiere conocer el estado actual de la seguridad informática, infraestructura, reglas y políticas aplicadas al AD-DC, verificar los filtros de seguridad que se tengan (firewall físico, antivirus, restricciones), perfilamiento de los usuarios y los permisos de cada uno de los perfiles, software y hardware especializado para las actividades a desempeñar.

Después de conocer el estado actual de la empresa Platino Sistemas, se indaga respecto a las mejores herramientas de software libre que se pueda aplicar para el objetivo

[1] B-secure pasión por la seguridad. ¿Cómo elegir un SOC? 3 aspectos que van más allá del costo. Oscar Cortes.[Consulta: 08 de junio de 2021]. Disponible en: https://www.b-secure.co/blog/como-elegir-soc-aspectos-que-van-mas-alla-del-costo-

principal del proyecto, es necesario verificar el alcance del propósito para determinar las mejores herramientas de pentesting e intrusión que se requieren, además del recurso humano para llevar los reportes de incidentes con profesionalismo, conocimiento y ética.[2]

Para el correcto desarrollo legal del proyecto, es necesario tener el conocimiento claro de la legislación colombiana respecto a ataques informáticos, ya que el desconocimiento de la ley no exime de ella, y puede acarrear problemas judiciales, monetarios y penales. Entre estas leyes esta la ley 1273 de 2009 con sus correspondientes artículos para cada uno de los delitos que se contemplan, como lo son el artículo 269A: acceso abusivo a un sistema informático, articulo 269B: obstaculización ilegitima de un sistema de información o red de telecomunicación, articulo 269C: interceptación de datos informáticos, articulo 269D: daño informático, articulo 269E: uso de software malicioso, etc.

También la ley de habeas data (ley 1581 de 2012) es importante ya que trata los datos personales y su protección, los cuales pueden tener repercusiones al momento de analizar vulnerabilidades.

[2] Nsit, Que es un SOC: Funciones y objetivos principales. [Sitio web]. Camila Pachon. [Consulta: 05 de junio de 2021]. Disponible en: https://www.nsit.com.co/que-es-un-soc-funciones-y-objetivos-principales/

ABSTRACT

Platino Sistemas is a Colombian company that provides information security and protection services, which plans to create a CSIRT (cyber incident response center), which aims to create and manage responses to computer attacks, offering the best incident response and vulnerability management.

The Department of Information and Communications Technologies (ICT), as the leader of the technical design that allows the development of CSIRT activities, presents the technical proposal for the implementation of the Security Incident Response Team - CSIRT for the company Platino Sistemas , which aims to prevent, monitor and control everything related to computer security in the organization.

In the technical design of the Security Incident Response Team, it is required to know the current state of computer security, infrastructure, rules and policies applied to the AD-DC, verify the security filters in place (physical firewall, antivirus, restrictions), profiling of users and the permissions of each of the profiles, specialized software and hardware for the CORE to perform.

After knowing the current status of the Platino Sistemas company, it is investigated regarding the best free software tools that can be applied for the main objective of the project, it is necessary to verify the scope of the purpose to determine the best pentesting and intrusion tools In addition to human resources, they are required to carry out incident reports with professionalism, knowledge and ethics.

For the correct legislative development of the project, it is necessary to have a clear knowledge of Colombian legislation regarding computer attacks, since ignorance of the law does not exempt it, and can lead to judicial, monetary and criminal problems. Among these laws is Law 1273 of 2009 with its corresponding articles for each one of the crimes contemplated, such as article 269A: abusive access to a computer system, article 269B:

illegitimate obstruction of an information systems or network of telecommunication, article 269C: interception of computer data, article 269D: computer damage, article 269E: use of malicious software, etc. " http://www.secretariosenado.gov.co/senado/basedoc/ley_1273_2009.html ”The habeas data law (law 1581 of 2012) is also important as it deals with personal data and its protection, which may have repercussions on time to analyze vulnerabilities.

INTRODUCCIÓN

Los equipos de respuesta ante emergencias informáticas (CERT - CSIRT) existe desde 1988 aproximadamente, a partir de la aparición del primer virus informático gusano (autorreplicable) denominado Morris, el cual infecto el 10% de los equipos conectados a internet , afectando 6000 servidores, que en esa época eran pocos los equipos conectados a esa red, el objetivo de este virus era averiguar la contraseña de los equipos afectados, buscando al azar con las contraseñas más comunes, este tipo de ataque no afectaba a todas las computadoras de la época, solo afectaba los equipos VAX y los fabricados por la compañía Sun Microsystem, este último manejaba Unix.

Gracias al aumento de dispositivos electrónicos conectados a internet actualmente para uso empresarial o doméstico, ya que estos presentan una gran ayuda para el desarrollo de las actividades en cada uno de los procesos que se llevan a diario, de la misma manera los ataques informáticos que se presentan a diario han venido en aumento, una de las causas por las cuales aumento el último año, fue por la pandemia del COVID-19, según la revista dinero aumentaron en un 605% los ataques, así mismo los malware tuvieron un crecimiento de 11,5 % según McAfee[3].

La empresa Platino Sistemas es una compañía colombiana la cual presta servicios de seguridad y protección de la información, en sus planes de expansión, está la meta de crear un SOC interno, el cual tendrá como propósito gestionar respuestas a incidentes informáticos y gestión de vulnerabilidades.

[3] Revista Dinero. [Sitio web]. Bogotá. [Consulta 18 noviembre de 2020]. Disponible en:https://www.dinero.com/tecnologia/articulo/cuanto-subieron-las-ciberamenazas-en-el-segundo-trimestre/305962

Dentro de los requerimientos que se necesitan para el funcionamiento del SOC están las herramientas de software, las cuales para el caso de Platino Sistemas se recomienda:

Kali Linux - Es una distribución de Linux basada en Debian
Nmap – Programa de código abierto que funciona para análisis de puertos
Metaesploit – Proyecto de código abierto para seguridad informática
Sqlmap – Herramienta automática de inyección sql
Aircrack-ng – suite de software de seguridad inalámbrica
Entre otras. [4]

[4] Ballesteros Cárdenas Alex, Propuesta técnica para la creación de un centro de respuestas a incidentes cibernéticos para la empresa caso de estudio Cibersecurity de Colombia LTDA. Especialización en Seguridad Informática. Bogotá. Universidad Nacional Abierta y a Distancia (UNAD). 2020. 125 pag. Disponible en: https://repository.unad.edu.co/handle/10596/36671

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Los SOC realizaron su primera aparición a mediados de 1988 en el mes de noviembre, cuando apareció el primer virus catalogado como gusano “Morris” el cual por poco colapsa el servicio de internet de la época (Arpanet) infectando alrededor de 6000 servidores, los cuales prestaban servicio de internet, Motores de Bases de datos, alojamiento de páginas web de la época, etc, desde dicha fecha, se han establecido CSIRT y SOC en los diferentes continentes con el fin de mitigar los ataques de delincuentes cibernéticos que se presentan a nivel global, asegurando la infraestructura tecnológica, la cual presta servicios informáticos usados a diario en las compañías, y compartir información de vulnerabilidades y su mitigación con los demás SOC, con el propósito de tener la información de ciberseguridad más actualizada a nivel internacional, gracias a los incidentes de seguridad informática que se presentan a diario, las técnicas que emplean, los nuevos dispositivos de hardware que aparecen en el mercado, esto permite la constante evolución de los SOC, ya que la información recolectada al momento de analizar una vulnerabilidades, es estudiada y difundida ante los demás SOC con el fin de buscar la mejor manera de mitigar su impacto, con el pasar del tiempo la relevancia con la cual se utiliza los Equipos de Respuesta Ante Emergencias informáticas es mayor, ya que la información hace parte importante del esquema de seguridad informática en las compañías.[5]

[5] ZDnet;The Morris wrom: Interrnet Malware turns 25. [Sitio web].United Kingdom:[Consulta: 4 de junio de 2021]. Disponible en: https://www.zdnet.com/article/the-morris-worm-internet-malware-turns-25/

Para la actualidad son más de 30 años desde que surgió el virus gusano Morris, el cual fue directamente el culpable de la aparición de primer equipo de respuestas a incidentes informáticos, de esta manera han surgido los diferentes SOC gracias a incidentes informáticos que han ocurrido, las avanzadas técnicas de ataques, ingeniería social entre otras.

1.2 FORMULACIÓN DEL PROBLEMA

¿Como la empresa Platino Sistemas lograra cumplir el objetivo organizacional del diseño de la propuesta técnica para la consolidación del Centro de Operaciones de Seguridad - SOC?

2 JUSTIFICACIÓN

El objetivo por el cual se realiza la propuesta para el desarrollo de actividades que comprenden un SOC interno en la empresa Platino sistemas, se enfoca en el diseño técnico para la construcción e implementación del equipo de respuestas a incidentes de seguridad informática, cumpliendo con los recursos mínimos para prestar un óptimo servicio, dando respuesta a incidentes reportados y análisis de vulnerabilidades, gracias a las técnicas especializadas utilizadas para detectar este tipo de brechas informáticas.[6]

Para la empresa Platino Sistemas es muy importante crear este tipo de área en su entorno laboral, ya que presta servicios de seguridad para la protección de la información, lo que daría profesionalismo y aferraría más su Core de negocio con este tipo de apoyo por parte del Centro De Operación De Seguridad-SOC, Estos procesos serán realizados por profesionales especializados, herramientas de software y hardware óptimas para la prestación de estos servicios

Los reportes de los incidentes se manejarán con un tiempo de respuesta (alto, medio y bajo) adecuado a la urgencia del caso, dependiendo del resultado que arroje la matriz de riesgo, lo anterior con el respaldo de la documentación de hardware y software para justificar los servicios prestados por el SOC, dando la suficiente confianza al cliente y poder realizar el seguimiento a su proceso paso a paso, teniendo la tranquilidad de que su petición están en manos de profesionales con las mejores herramientas para prestar este servicio.

[6] Oracle, ¿Qué es un SOC?. [Sitio web]. Oracle. [Consulta: 01 de junio de 2021]. Disponible en: https://www.oracle.com/es/database/security/que-es-un-soc.html

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Diseñar la propuesta técnica para la consolidación del Centro de Operaciones y Seguridad – SOC de la empresa Platino Sistemas, con el fin de cumplir con las metas proyectadas por la organización.

3.2 OBJETIVOS ESPECÍFICOS

- Esquematizar los recursos del software y hardware como propuesta técnica para la consolidación del Centro de Operaciones de Seguridad – SOC

- Simular la infraestructura de software en un entorno controlado con el fin de seleccionar las herramientas que apoyen los servicios del Centro de Operaciones de Seguridad – SOC

- Adaptar la estructura organizacional con roles y funciones, que den soporte al desarrollo de las actividades Centro de Operaciones de Seguridad - SOC.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

Desde la aparición del virus gusano autorreplicable Morris en el año 1988, se ha venido generando la creación de los CSIRT, los cuales se han encargado de dar respuestas a las emergencias informáticas, con el fin de mitigar dichas vulnerabilidades y que generen el menor impacto posible a los victimarios, una de las ventajas que tienen el equipo de respuesta ante emergencias informáticas y lo cual ha permitido su constante evolución, es la comunicación y trasmisión de información con los demás SOC a nivel mundial, lo que permite anticiparse a posibles ataques realizados con anterioridad en otra parte del mundo y mitigarlo de la manera correcta. Con la evolución de los equipos de cómputo y de los softwares, los delincuentes informáticos son cada vez más ingeniosos al momento de realizar sus ataques, lo que ha conllevado a la constante evolución de los SOC y los obliga a estar a la vanguardia en lo que a seguridad informática se trata.[7]

El diseño técnico del SOC en la empresa Platino Sistemas, con el cual se pretende dar cumplimiento a las necesidades que tienen sus clientes con todo lo referente a incidentes y vulnerabilidades cibernéticas, se tiene como referencia algunos proyectos los cuales se utilizaron para el diseño e implementación de un SOC con metodologías libres, como lo es el trabajo de grado para la Especialización en Seguridad Informática de la UNAD (Universidad Nacional Abierta y a Distancia), el cual se titula: Propuesta Técnica para la Creación de un Centro de Respuesta a Incidentes Cibernéticos para la Empresa Caso de Estudio Cibersecurity de Colombia LTDA[8], presentado por Alex Augusto Ballesteros

[7] Ministerio de defensa de España, Guía de creación de un CERT /CSIRT. España: Editor y Centro Criptológico Nacional, 2011. 60 pag. Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-sep11.pdf

[8] Ballesteros, Alex Augusto. Propuesta Técnica Para La Creación De Un Centro De Respuesta A Incidentes Cibernéticos Para La Empresa Caso De Estudio Cibersecurity De Colombia Ltda. Trabajo de grado para

Cárdenas, el cual se puede consultar en el siguiente link https://repository.unad.edu.co/bitstream/handle/10596/36671/aballesterosc.pdf?sequence=1&isAllowed=y , de igual manera, se toma como referencia el trabajo de grado para post-grado en Seguridad Informática, presentado por Jaidur Cano Vargas, el cual titula Propuesta de los documentos administrativos para la Creación de un Centro de Respuesta a Incidentes Cibernéticos para la empresa caso de estudio Cibersecurity de Colombia LTDA[9]. Y se puede consultar en el enlace https://repository.unad.edu.co/bitstream/handle/10596/36488/jjcanov.pdf?sequence=1&isAllowed=y, además de los documentos para postulación de grado, también se analizara la Guía de Creación de CERT-CSIRT[10], la cual fue creada por el Ministerio de Defensa de España en el 2011 y puede ser consultada en https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-sep11.pdf. El proyecto Aurora, como referente importante al momento de realizar la investigación, también sirvió como guía para el entendimiento de las funciones del SOC- CSIRT, dicho proyecto fue creado por Julio Balderrama, Mariela García, Mateo Martínez, Adrián Acosta, Aurora Valinote, el link de consulta es : https://www.proyecto-aurora.org/ , por ultimo pero no menos importante esta la pagina web de Yolanda Corral, la cual un apartado llamado Construye y gestiona un SOC con herramientas Open Source, y su enlace de consulta es: https://www.yolandacorral.com/construye-y-gestiona-un-soc-con-herramientas-open-source/.

Especialista. Bogotá D.C; UNAD (Universidad Nacional Abierta y a Distancia), 2020. [Consultado: 10 de enero de 2021]. Disponible en https://repository.unad.edu.co/bitstream/handle/10596/36671/aballesterosc.pdf?sequence=1&isAllowed=y

[9] Cano, Jaidur. Propuesta de los documentos administrativos para la Creación de un Centro de Respuesta a Incidentes Cibernéticos para la empresa caso de estudio Cibersecurity de Colombia LTDA. Trabajo de grado para Especialista. Bogotá D.C; UNAD (Universidad Nacional Abierta y a Distancia), 2020. [Consultado: 15 de enero de 2021]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/36488/jjcanov.pdf?sequence=1&isAllowed=y

[10] Ministerio de Defensa de España. GUIA DE CREACION DE UN CERT / CSIRT. [Sitio web]. España.[Consultado: 20 enero de 2021]. Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-sep11.pdf.

4.1.1 ISO 27001

La Norma ISO 27001 desarrollada por la organización internacional para la Normalización (ISO) la cual tiene como propósito ayudar a gestionar la seguridad de la información en cualquier compañía sin importar su tamaño, Core de negocio, actividad económica, etc.

La primera versión de esta norma se dio a conocer en el año 2005, tomando como base la norma británica BS 7799-2 la cual ya no existe; la nomenclatura correcta para identificar esta norma es ISO/IEC 27001, en la actualidad cuenta con la versión 2 llamada ISO/IEC 27001:2013.[11]

Esta norma puede ser instaurada en cualquier tipo de compañía, el factor a tener en cuenta para la implementación de la norma, es la importancia de los activos de la información de la compañía en la cual se va a implementar, para el caso de Platino Sistemas, la cual es una empresa que presta servicios de seguridad de la información, es de vital importancia establecer dicha normatividad, ya que genera confianza en los clientes y permite tener un buen control de los activos de información de la empresa[12], conjuntamente detecta riesgos y sus posibles controles para mitigarlos, igualmente incluye la alta gerencia en la estructuración de la norma y difusión de los elementos y políticas para la ejecución, puesto que deben conocer la norma y su implementación[13].

---

[11] ISO, Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información – Requisitos. ISO. [Consulta: 13 de junio de 2021]. Disponible en : https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1

[12] Normas-iso, ISO 27001 Gestión de la seguridad de información. [Consulta: 09 de junio de 2021]. Disponible en: https://www.normas-iso.com/iso-27001/

[13] ISO tools, Sistema de Gestión de riesgo y seguridad. ISO Tools. [Consulta: 11 de junio de 2021]. Disponible en: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

En la actualidad la norma ISO/IEC 27001 es el referente mundial para certificar la seguridad de la información en cualquier tipo de empresa, con la implementación de un SGSI (Sistema de Gestión de Seguridad de Información) el cual es el núcleo central de la norma ISO/IEC 27001, y este compuesto por procesos de implementación, mantenimiento y mejora de manera continua, teniendo como base los riesgos de la seguridad de la información[14].

4.1.2 ISO 27035-1:2016

La norma ISO/IEC 27035-1: 2016, tecnología de la información-técnicas de seguridad – Gestión de incidentes de seguridad de la información, tiene los principios básicos y genéricos con el propósito de ser aplicable a cualquier tipo de empresa, ya sea pública o privada, grande o pequeña, etc, una de las ventajas que tiene esta norma, es que tiene la capacidad de adaptarse a cualquier Core de negocio sin importar la criticidad que pueden tener los activos de información[15].

Esta norma es un instructivo para la evaluación , localización y análisis de vulnerabilidades e incidentes informáticos, a los que se puede ver expuesta una compañía, además de esto, dicha norma se puede ser aplicada por terceros o directamente por un área específica de la compañía, esta guía de gestión de incidentes de seguridad de la información, ayudara afrontar los incidentes de seguridad de la

[14] ISO 27001, Normas ISO 27001.ISO 27001. [Consulta: 11 de junio de 2021]. Disponible en: https://normaiso27001.es/

[15] ISO, ISO /IEC 27035-1 : 2016 ; Tecnología de la información – Técnicas de seguridad -Gestión de incidentes de seguridad de la información – parte 1- Principios de gestión de incidentes. [sitio web] . ISO [Consulta: 10 de abril de 2021] . Disponible en : https://www.iso.org/standard/60803.html

información definiendo controles efectivos, lo que conlleva a la reducción del impacto derivado de los incidentes[16].

4.1.3 SIEM

Dado que la mayoría de las empresas tienen una conexión de comunicación interna con el exterior (internet), lo cual permite un mejor desempeño laboral y operativo gracias a las herramientas ofimáticas y entornos web para la gestión de información, esto también genera un aumento en los ataques informáticos y su impacto en las compañías, para mitigar este tipo amenazas, existen los gestores de información y correlacionador de eventos de seguridad, con el fin de que la compañía pueda detectar cualquier tipo de fallo que comprometa la seguridad de la información por medio de un sistema de estandarización de datos, es una buena herramienta ya que permite una visión global de la magnitud de la compañía y de los activos de información a proteger[17].

Los SIEM funcionan mezclando la interpretación de datos y registros gestionando los mismo e interpretándolos, con el fin de encontrar patrones inusuales o comportamientos atípicos y tomar medidas al respecto, evitando en su mayoría la aparición de falsos positivos los cuales pueden ser alertas del antivirus, formatos específicos, programas ejecutables, etc. Este tipo de SIEM centraliza la información recolectada con el fin de analizar la información reportada como peligrosa para analizar las tendencias y patrones y saber qué tipo de archivo se está gestionando[18].

---

[16] SGSI; ISO/IEC 27035 Gestión de incidentes de seguridad. [Sitio web]. [Consulta: 1 de julio de 2021]. Disponible en:https://www.pmg-ssi.com/2020/07/iso-iec-27035-gestion-de-incidentes-de-seguridad/

[17] *Viewnext and IBM Subsidiary;¿Qué es un SIEM?.[Sitio web].[Consulta: 1 de junio de 2021]. Disponible en:* https://www.viewnext.com/que-es-un-siem/

[18] Exabeam, 10 características imprescindibles para un SIEM moderno. [Sitio web]. Exabeam. [Consulta: 01 de junio de 2021]. Disponible en:https://www.exabeam.com/siem/next-gen-siem

4.1.4 SOC

Los SOC (Centro de operaciones de seguridad), son las entidades encargadas de la seguridad de la información e informática por medio de monitoreos y administración de incidentes reportados, lo anterior se realiza por medio de herramientas de recogida y correlación de eventos, como lo es el SIEM, quien es el principal actor dentro del SOC, puesto que ayuda a la administración de eventos de seguridad de los sistemas de información.

La principal tarea de un SOC es analizar, detectar y recoger sucesos de seguridad informática por medio de herramientas de software y hardware con el propósito de analizar y supervisar las redes, periféricos, servidores, bases de datos, equipos de cómputo, aplicaciones web y demás sistemas de información, en busca de patrones y anomalías las cuales permite detectar si se trata de un ataque o incidente de seguridad informática, el SOC debe avalar que los reportes de seguridad arrojados por las distintas herramientas deben ser identificados, analizados e investigados para mitigarlos de la mejor manera.

La manera correcta para definir un SOC, es definiendo los objetivos de la compañía (Platino Sistemas) e integrarlos en cada uno de los departamentos de la empresa, una vez integrada toda la compañía, se analiza y define la infraestructura necesaria para la implementación del SOC la cual mínimamente debe contar con firewall físico y de software, IDS/IPS, detector de vulnerabilidades, SIEM, correlacionador de eventos, medidores y demás herramientas para recolección y análisis de datos, todo lo anterior cumpliendo las normas legales que corresponden[19], también es de suma importancia el personal que tendrá la responsabilidad en cada una de las áreas del SOC, este personal

[19] Oracle, ¿Qué es un SOC?. [Sitio web]. Oracle. [Consulta: 01 de junio de 2021]. Disponible en: https://www.oracle.com/es/database/security/que-es-un-soc.html

debe ser técnicos en sistemas con conocimientos en seguridad informática, ingenieros de sistemas especialistas en seguridad informática, Magister en ciberseguridad o profesionales con post- grados en seguridad informática, con el fin de dar seguridad a los clientes que esta en manos de profesionales y dar soluciones definitivas a los incidentes reportados en el SOC[20].

Existen varios tipos de SOC los cuales se definen de la siguiente manera:

- **SOC Interno:** Es el modelo normalmente constituido en grandes empresas, donde tiene su propio SOC para el tratamiento de incidentes de seguridad de su empresa, cuentan con la infraestructura y personal adecuado para prestar este tipo de servicios.

- **SOC Externo:** Son empresas que se dedican a prestar servicios de seguridad informática a empresas las cuales no cuentan con este tipo de servicio, o no tienen la infraestructura o personal adecuada para ello.

- **SOC Hibrido:** Son empresas que subcontratan otras empresas (SOC) para que presten parcial o totalmente sus servicios, ya sea contratación de personal o infraestructura para obtener el alcance de la compañía[21].

4.1.5 CSIRT

Los CSIRT son los equipos de respuesta a incidentes de seguridad, los cuales se encargan de minimizar y controlar los daños presentados por ataques cibernéticos en los

[20] Nsit, Que es un SOC: Funciones y objetivos principales. [Sitio web]. Camila Pachon. [Consulta: 05 de junio de 2021]. Disponible en: https://www.nsit.com.co/que-es-un-soc-funciones-y-objetivos-principales/
[21]

sistemas de información de una compañía, documentando todo lo ocurrido en el incidente de seguridad, de esta manera se tendrá el contexto de la amenaza lo cual permitirá definir su origen y consecuencias a nivel empresarial.

Dentro de las funciones que debe cumplir el CSIRT, está la rápida reacción ante los incidentes reportados, sin afectar el flujo de trabajo de la compañía o teniendo el menor impacto posible, también debe prevenir que incidentes equivalentes que se presenten en el futuro, ya que se tiene documentación previa de las lecciones aprendidas y de esta manera poder mitigar el ataque cibernético realizado, además de esto, el CSIRT tiene la función de compartir la información relacionada con los incidentes de seguridad informática reportados con los demás CSIRT a nivel mundial, con el fin de difundir información que pueda ser útil para mitigar los ataques reportados en los demás equipos de respuesta a incidentes de seguridad[22].

4.1.6 Blue team

Dentro de los equipos del SOC que prestan servicio de seguridad informática, se encuentra el equipo de trabajo Blue team (Seguridad defensiva), es el equipo encargado de prestar seguridad en las organizaciones de manera proactiva, realizando monitorización de redes, servidores, bases de datos, etc, de manera constante y analizando los comportamientos y patrones inusuales tanto a los software como de los usuarios de los sistemas de información, también rastrean los incidentes de seguridad reportados en los sistemas, con el fin de verificar si tiene vulnerabilidades y verificando las salvaguardas que se tienen para mejorar la seguridad de la información, realizando

[22] Welifesecurity.[Sitio web].Eset.[Consulta 25 noviembre de 2020].Disponible en: https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

las recomendaciones necesarias para mitigar de la mejor manera posible las posibles brechas informáticas que se detecten[23].

4.1.7 Red team

Los miembros del grupo Red team (Seguridad ofensiva), este equipo se encarga de suplantar a los atacantes informáticos utilizando técnicas y herramientas para intrusión de igual manera que lo haría un ciberdeincuente, poniendo a prueba las vulnerabilidades encontradas en los sistemas de información, lo anterior con el fin de dar la información suficiente al equipo Blue team para que se pueda defender ante las vulnerabilidades encontradas por este equipo, con este grupo de trabajo se evalúa la capacidad real de una compañía para defender sus activos de información y de dar respuesta asertiva y oportuna a los incidentes que puedan ocurrir.

4.1.8 Purple team

El objetivo de este equipo de trabajo es aumentar la eficacia de los grupos blue team y red team, se realiza utilizando las técnicas defensivas del blue team con las técnicas ofensivas del red team, normalmente no es un equipo sino una interacción entre los dos equipos de trabajo, su principal objetivo es gestionar la seguridad de los activos de la información realizando pruebas para verificar la eficacia de los mecanismos y procedimientos de seguridad, este tipo de equipo de trabajo normalmente se ven en las empresas pequeñas, ya que el presupuesto no se presta para tener un equipo Blue team y un Red team independientemente[24].

---

[23] Unir la Universidad en Internet; Red Team, Blue team y purple team, ¿Cuáles son sus funciones y diferencias?. [Sitio web]. España.[Consunta en: 19 de julio de2021]. Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

[24] Ibid., p 29.

4.2 MARCO CONCEPTUAL

Los SOC son equipos de personas encargados de realizar medidas preventivas , reactivas y de seguridad informática y de la información, además de esto permite la administración y supervisión de los sistemas de información por medio de las diferentes herramientas que existen para recolectar, correlacionar e intervenir en la interacción de eventos reportado en el SOC, también es el encargado de estudiar el estado de todas las redes a nivel mundial, servidores que generan respuestas ante incidentes tecnológicos.

Para la empresa Platino sistemas el objetivo es implementar un SOC interno para la organización el cual prestara dichos servicios de respuesta a incidentes de seguridad informática.

Una de las ventajas de implementar un SOC interno es:

- Planificación a largo plazo
- Conocimiento a la medida según las necesidades internas
- Conformado por empleados internos de la compañía
- Registros de logs localmente
- Visibilidad de amenazas
- Vigilancia 24 horas, 7 días
- Respuesta rápida

Diseñar: se define como “hacer un plan detallado para la ejecución de una acción o una idea”[25]

[25] *Léxico. [Sitio web].Powered by Oxford.[Consulta 20 noviembre de 2020].Disponible en: https://www.lexico.com/es/definicion/ disenar*

Propuesta: definida por Oxford como “proyecto o idea que se presenta a una persona para que lo acepte o de su conformidad para realizarlo”[26]

Técnica: está definido como “Destreza y habilidad de una persona en un arte, deporte o actividad que requiere usar estos procedimientos o recursos, que se desarrollan por el aprendizaje y la experiencia”[27]

SOC: se define como “Centro de Operaciones y Seguridad[28]”

4.3 MARCO HISTÓRICO

La implementación de los SOC ha venido evolucionando, ya que las herramientas para el análisis de debilidades informáticas son cada vez más exactas desde sus primeras implementaciones en la década de los 80´s, y encuentran nuevas vulnerabilidades en los sistemas de información, bases de datos, servidores web, activos de información, etc. A medida que pasa el tiempo el paradigma de ataques informáticos ha cambiado de manera sustancial, en sus primeras apariciones de ataques informáticos los cuales normalmente eran Malware, Phising, gusanos, etc, en la actualidad los ataques son más sofisticados ya que se habla de APT, Ransomeware, cryptojacking, etc, el análisis de las últimos ciberataques permite tener claridad respecto hacia donde pueden ir los próximos ataques, y crear un perfilamiento del tipo de atacante y sus técnicas, también consiente tener un indicio de reacción respecto a los ataques y realizar su mitigación de la mejor

---

[26] Léxico. [Sitio web].Powered by Oxford.[Consulta 20 noviembre de 2020].Disponible en: https://www.lexico.com/es/definicion/propuesta

[27] Léxico. [Sitio web].Powered by Oxford.[Consulta 20 noviembre de 2020].Disponible en: https://www.lexico.com/es/definicion/tecnica

[28] Oracle, ¿Qué es un SOC?. [Sitio web]. Oracle. [Consulta: 01 de junio de 2021]. Disponible en: https://www.oracle.com/es/database/security/que-es-un-soc.html

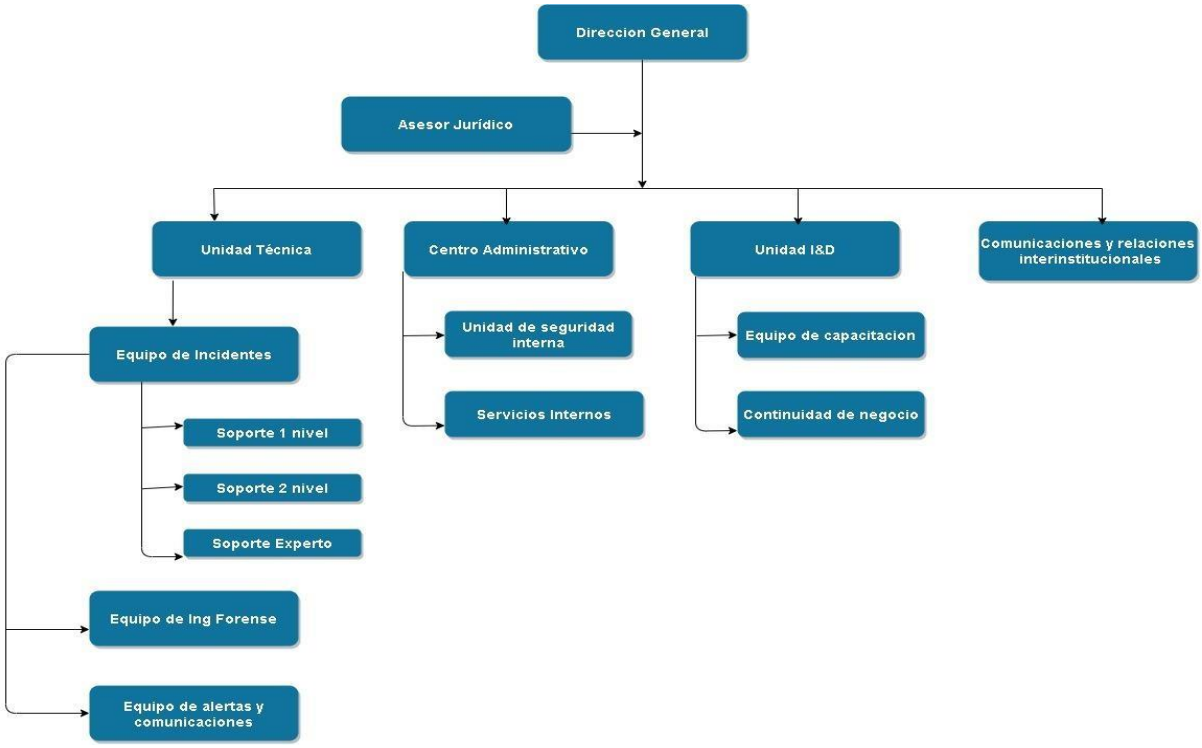
manera posible. así mismo, los delincuentes informáticos evolucionan en sus técnicas de explotación de brechas informáticas. De esta manera los equipos de respuesta ante emergencias informáticas deben estar en constante evolución y mejora dependiendo de los resultados obtenidos con los análisis de vulnerabilidades; cabe resaltar la trasmisión de información que se tiene entre los SOC a nivel mundial, esto con el fin de anticiparse a posibles ataques y permite obtener las ultimas noticias y actualizaciones referente a seguridad informática[29].

4.4 ANTECEDENTES O ESTADO ACTUAL

Dado el caso que la empresa Platino sistemas en la actualidad presta servicios de seguridad para la protección de la información, cuenta con las herramientas básicas para la implementación del SOC, puesto que el core de negocio se enfoca en el alcance de la propuesta de implementación de SOC, es de tener en cuenta que dicha ejecución necesita herramientas informáticas más sofisticadas y orientadas a dar respuesta a las emergencias informáticas, de igual manera es necesario tener el personal idóneo para la prestación de los servicios dada la estructura organizacional a tener.

[29] UST; La evolución del SOC ante el nuevo modelo de amenazas. [Sitio web]. España. [Consulta: 15 de junio de 2021]. Disponible en:https://www.ust.com/es/insights/la-evolucion-del-soc-ante-el-nuevo-modelo-de-amenazas

Figura 1 Estructura Organizacional



Fuente: Propia

4.5 MARCO LEGAL

Dada la normativa Colombia, la cual reglamenta el uso y manejo de los recursos informáticos. La ley 1273 de 2009 contiene el artículo 269, el cual divide en los artículos 269A: acceso abusivo a un sistema informático, articulo 269B: obstaculización ilegitima de un sistemas de información o red de telecomunicación, articulo 269C: interceptación de datos informáticos, articulo 269D: daño informático, articulo 269E: uso de software malicioso, etc. y normaliza los actos informáticos ilícitos que se generen en Colombia[30],

[30] *Congreso de la república. [Sitio web]. Bogotá secretaria del senado. [Consulta 15 noviembre de 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html*

además de estos se debe tener en cuenta la ley 1581 de 2012 (Habeas data) respecto a protección de datos.

Colombia también se ratificó en el convenio de Budapest el día 20/06/2018, en este convenio también llamado convenio de ciberseguridad fue el primero de su tipo y hace referencia a los delitos informáticos y ciberdelitos con el fin de armonizar las leyes entre las naciones participantes[31], además del anterior convenio, se cuenta con el documento Conpes 3854, el cual trata la política nacional de seguridad digital, la cual tiene como propósito cambiar tradicionalmente la gestión de riesgo como uno de los compendios más importante en la seguridad digital[32], también se tiene como referencia el documento Conpes 3995 y 3920 los cuales hace referencia a la política nacional de confianza y seguridad digital y la explotación de datos (Big data)[33] respectivamente, y trata el tema de establecer medidas para mejorar la seguridad y confianza digital con el finde que Colombia sea más competitiva digitalmente[34].

La ley 527 de 1999 la cual hace referencia al comercio electrónico, también define y reglamenta el uso y acceso de los datos y firmas digitales, además instituye las entidades de certificación. Esta ley aplica para todo tipo de información que se maneje en forma de datos, salvo las siguientes 2 excepciones:

- a) En las obligaciones contraídas por el Estado colombiano en virtud de convenios o tratados internacionales;

---

[31] Cancillería de Colombia, Colombia se adhiere al convenio de Budapest contra la ciberdelincuencia. [Sitio web]. Bogotá. Cancillería de Colombia. [Consulta 10 de junio de 2021]. Disponible en: https://www.cancilleria.gov.co/newsroom/news/colombia-adhiere-convenio-budapest-ciberdelincuencia

[32] *Consejo Nacional de Política Económica y Social; Documento CONPES 3854. Bogotá 01 de Julio de 2021. 91 pag. Disponible en:* https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

[33] *Departamento Nacional de planeación; Documento CONPES 3920. Bogotá 1 de julio de 2021. 116 pag. Disponible en:* https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3920.pdf

[34] Documento Conpes 3995, Departamento nacional de planeación. Bogotá. 01 de julio de 2020. 51 pag. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

- b) En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo[35].

La ley 1341de 2009 la cual determina el contexto para la elaboración de políticas públicas que presidirán en el sector de las TIC'S, con esta ley se crea la Agencia Nacional del Espectro, también es la ley que vela para que la planeación, gestión, administración, regulación y control de libre acceso al espectro electromagnético sea administrado de la mejor manera.

El decreto 1727 de 2009 determina la manera en la que la entidades bancarias, financieras, crediticias, comerciales y la provenientes de estas mismas entidades de otros países, dan a conocer la información de los titulares de la información[36].

El decreto 1704 de 2012 el cual contempla la interceptación legal de comunicaciones, tiene como objetivo interceptar cualquier tipo de comunicación sin importar su origen o tecnología, con el fin de maximizar el trabajo investigativo de las entidades competentes en los delitos que se estén procesando, lo anterior teniendo en cuenta el marco constitucional y legal. Este decreto contempla 8 artículos en los cuales están los deberes de los proveedores de ISP, el transporte de la información sustraída por los terceros, información de los suscriptores, la ubicación de las partes interesadas y la confidencialidad de la información[37].

---

[35] El Congreso de Colombia; Ley 527 de 1999. [Sitio web]. Bogotá. [Consulta: 20 de mayo de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html.

[36] Secretaria Jurídica Distrital; Decreto 1727 de 2009 Nivel Nacional. [Sitio web]. Bogotá. [Consulta: 23 de abril de 2021]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36251

[37] Departamento administrativo de la función pública; Decreto 1704 de 2012; [Sitio web]. Bogotá. [Consulta: 13 mayo de 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=48863

5 DISEÑO METODOLÓGICO

La metodología de investigación que se utilizará será cuantitativa, la cual toma estudios individuales ya realizados como resultados para verificar los beneficios y desventajas de una intervención, este tipo de metodología es una forma de análisis secundaria ya que los datos son recolectados por otras investigaciones que ya han sido publicadas y orientadas al mismo objetivo.

Dentro de la metodología de investigación optada para el desarrollo del proyecto, se tomará el tipo, **-** *Estudio del caso* **-** el cual analiza muy detalladamente el comportamiento de algunos de los objetos de investigación, para que este tipo de metodología sea aceptada, los informes estudiados deben estar orientados al mismo objetivo, en este caso la implementación técnica del SOC[38]. Además de esto, también se tendrá en cuenta la investigación descriptiva, ya que el enfoque del SOC es la recolección, análisis e intervención de los datos por medio de condiciones y excepciones, los cuales son tratados por el personal experto en seguridad informática, utilizando las herramientas tecnológicas suficientes para dar el mejor resultado.

Todo lo anterior se debe llevar con la documentación necesaria para los roles y responsabilidades, actas y contratos teniendo el detalle de cada una de las incidencias presentadas en el SOC, es de tener en cuenta las incidencias denominadas falsos positivos, ya que pueden ser tareas cotidianas o excepciones que se utilizan a diario en las labores de la empresa[39].

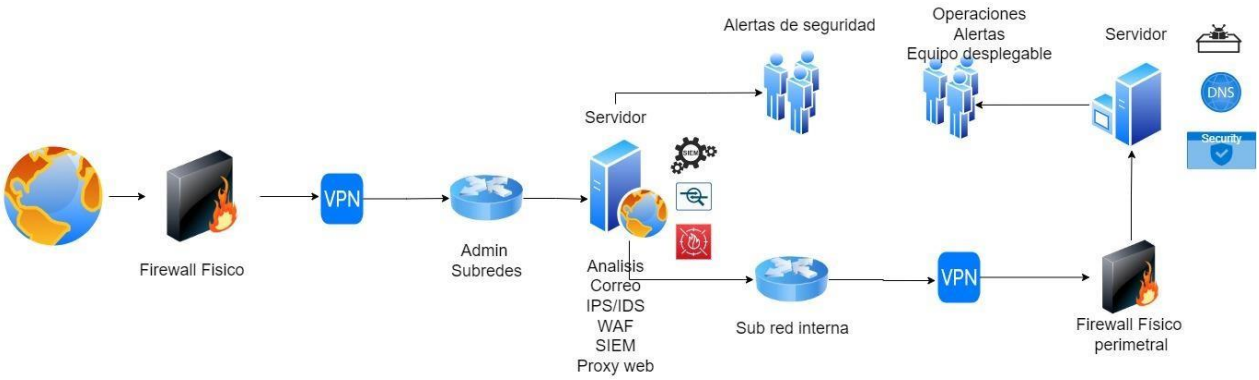
---

[38] *Monje Carlos Arturo, Metodología de la investigación cualitativa y cuantitativa guía didáctica, [en línea]. Neiva-Colombia, Universidad Surcolombiana, facultad de Ciencias sociales y Humanas, 2001. Pag 217.*

[39] Morales González Carlos, Moreno Sánchez Omar, Ortigoza Pérez Johanna. Propuesta para un centro de operaciones y seguridad (SOC) para fuerza Aérea Colombiana. Ingeniería de sistemas. Bogotá. Universidad Piloto de Colombia. 2014. 94 pag. Disponible en: http://polux.unipiloto.edu.co:8080/00001627.pdf

6 DESARROLLO DE LOS OBJETIVOS

6.1 TOPOLOGIA PARA LA IMPLEMENTACION DEL SOC (PLATINO SISTEMAS)



Fuente: Propia

6.2 DESARROLLO DE OBJETVOS ESPECIFICOS

Para llevar a cabo el desarrollo de este proyecto; es necesario conocer el estado actual de la compañía, con que activos de información cuenta la empresa, que tipo de capacitación tiene el personal que maneja los activos de información, tener en conocimiento de cuentas sedes tiene la empresa, saber qué tipo de información maneja la empresa y si tiene terceros que manejen información sensible, con el propósito de tener conocimiento exacto de los recursos que tiene actualmente Platino Sistemas ya que esto permite realizar un análisis de vulnerabilidades en los activos de información, clasificarlos y mitigar sus brechas informáticas con las herramientas necesarias para suplir los requerimientos del SOC. Así mismo, se debe crear la estructura organizacional del SOC para prestar con profesionalismo y de forma eficiente sus servicios, en este caso se utilizará las distintas herramientas para la prestación de servicios reactivos y proactivos de código abierto y permitirá definir de una mejor manera el alcance del SOC[40].

[40] Morales González Carlos, Moreno Sánchez Omar, Ortigoza Pérez Johanna. Propuesta para un centro de operaciones y seguridad (SOC) para fuerza Aérea Colombiana. Ingeniería de sistemas. Bogotá.

A partir de los objetivos específicos se pretende realizar la consolidación del SOC de la siguiente manera:

- Esquematizar los recursos del software y hardware como propuesta técnica para la consolidación del Centro de Operaciones de Seguridad – SOC.

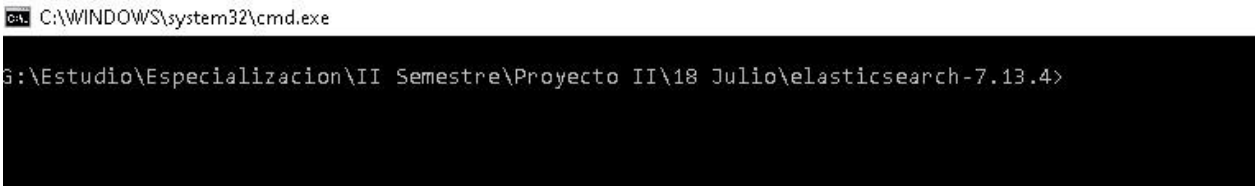
  Es necesario tener claridad respecto a los recursos que se necesitan para desarrollar las actividades del SOC con el profesionalismo que requieren, uno de estos recursos, es el personal, el cual deberá llevar acabo todas las funciones y presentación de servicios, este personal debe tener las competencias necesarias para sus ocupaciones, normalmente son técnicos, ingenieros o especialistas en sistemas y seguridad informática, de la misma manera se debe contar con la infraestructura necesaria para prestar este tipo de servicios; ya que Platino Sistemas por ser una empresa dedicada a la seguridad de la información, cuenta con la infraestructura básica con la cual se puede avanzar en el desarrollo del alcance, esta infraestructura cuenta con un firewall físico, doble servicio de internet (Principal y backup), switch PoE capa 3, cableado estructurado certificado, equipos de cómputo robustos para un mejor desempeño, impresoras de red, Servidor de AD, etc, y de esta manera garantizar su funcionamiento, además de esto, se debe contar con los recursos de software obligatorios para la prestación de los servicios del SOC, algunos de estos recursos son: un servidor Sandbox (Win 10), servidor web (Win server 2016), servidor de archivos (Win server 2016), , servidor de copias de seguridad (Win Server 2016), servicios de informática forense (Kali Linux), SO para pentesting (Kali Linux), etc, con los anteriores recursos se puede garantizar los servicios que se prestaran en el SOC.

Universidad Piloto de Colombia. 2014. 94 pag. Disponible en: http://polux.unipiloto.edu.co:8080/00001627.pdf

Para este proyecto se utilizará el SIEM de Elasticsearch el cual se encuentra instalado sobre un servidor de monitoreo con sistema operativo Windows 10 profesional el cual puede ser instalado de la siguiente manera:

- Descarga de Elasticsearch: Se debe ingresar a la página oficial de elastic[41] y descargar el archivo comprimido dependiendo de SO que se maneje, una vez descargado y descomprimido, se ingresa desde cmd a los archivos descomprimidos.

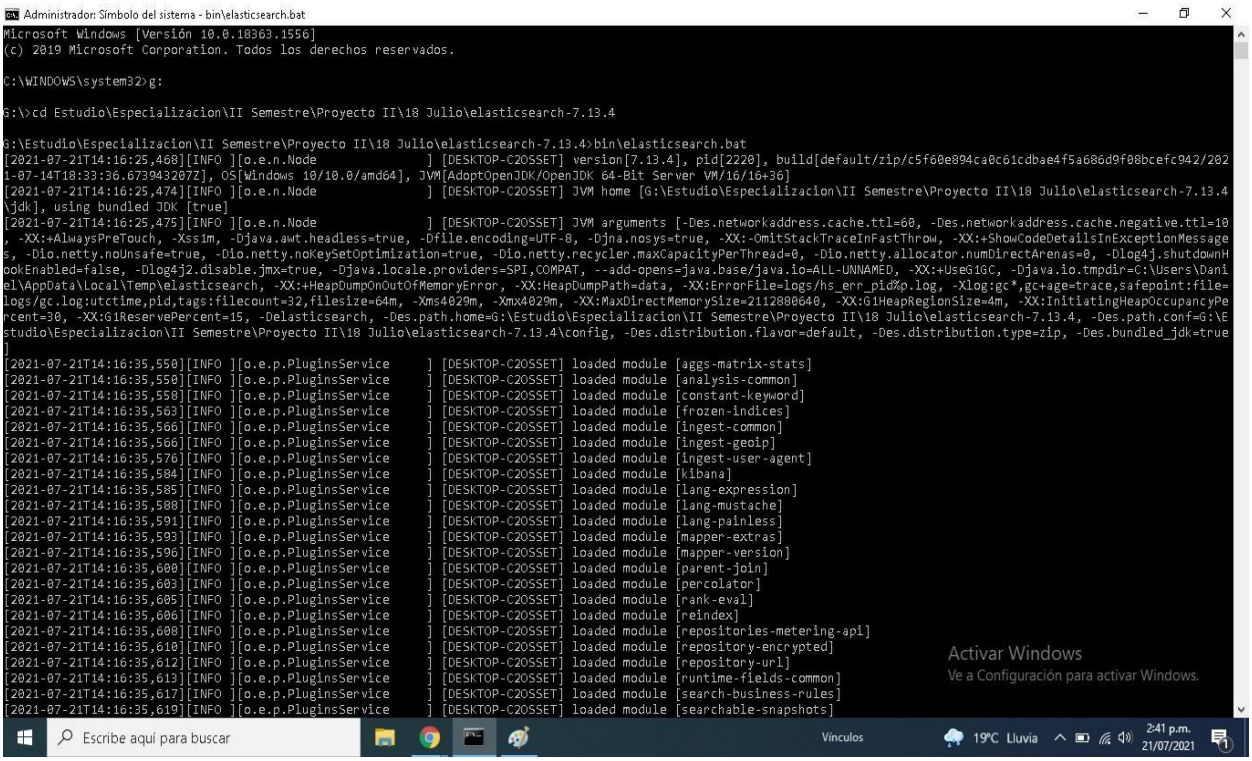
Figura 2 Descarga Elastic cmd



- Instalación de Elasticserch por medio de cmd con privilegios elevados: Una vez en la carpeta donde se encuentra la descarga, se agrega el siguiente código bin\elasticsearch.bat para que empiece la instalación del software[42].

[41] Elastic; Download Elasticsearch; [Sitio web]. España. [Consulta: 15 de julio de 2021]. Disponible en: https://www.elastic.co/es/downloads/elasticsearch
[42] Ibid., p 38.

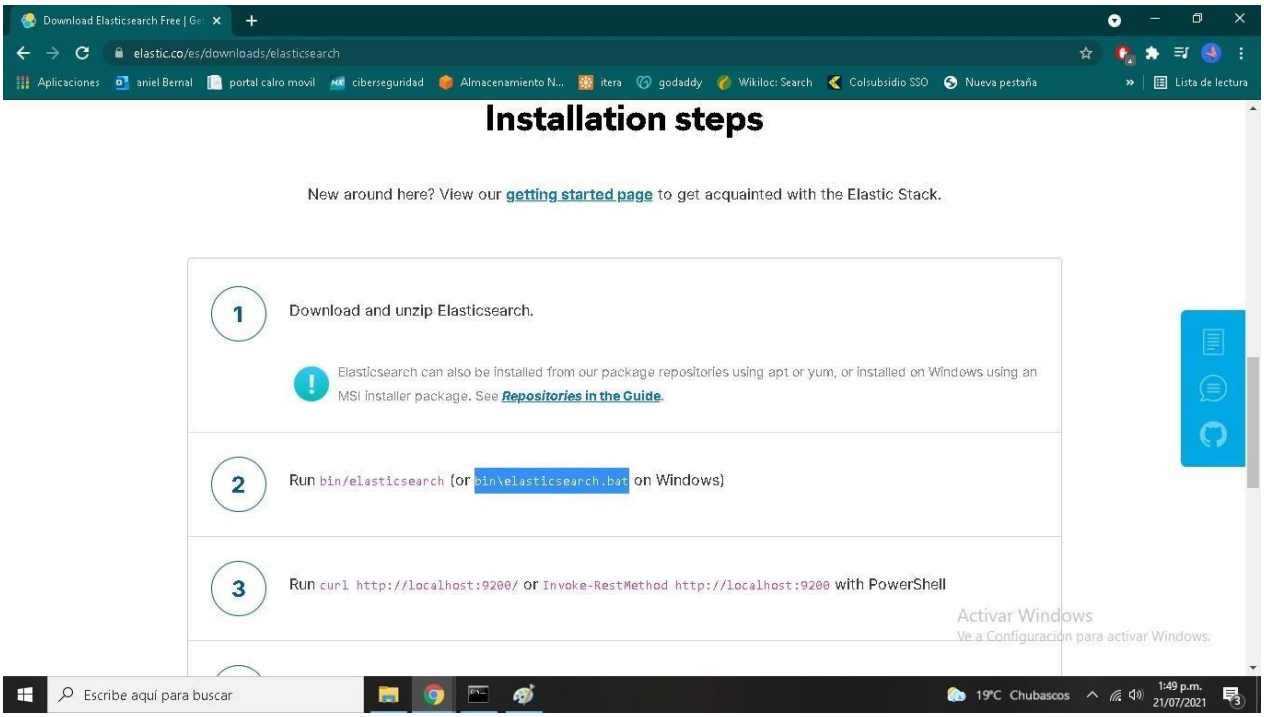
Figura 3 Instalación cmd



- Página web de instalación paso a paso de Elasticsearch[43]: Desde la página oficial es posible descargar los instructivos y software para cada uno de los SO los cuales son compatibles con el SIEM.

[43] Elastic; Download Elasticsearch; [Sitio web]. España. [Consulta: 15 de julio de 2021]. Disponible en: https://www.elastic.co/es/downloads/elasticsearch

Figura 4 Paso a Paso instalación Elasticsearch



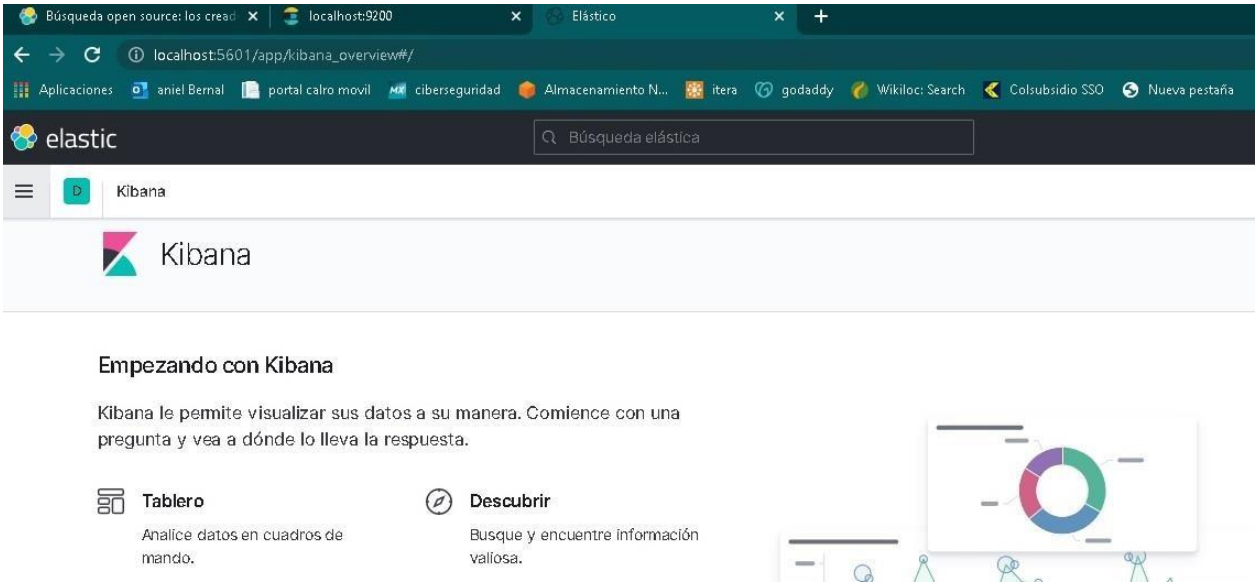
- Verificación de la instalación del SIEM Elasticsearch: Es de aclarar que se verifica desde el navegador web, ingresando en la url “localhost” seguido del puerto lógico 9200, de esta manera se evidencia que está corriendo el software.

Figura 5 SIEM Elasticsearch instalado


```
{
  "name" : "DESKTOP-C2OSSET",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "mci1VNf9TlWWfCulSFrJxQ",
  "version" : {
    "number" : "7.13.4",
    "build_flavor" : "default",
    "build_type" : "zip",
    "build_hash" : "c5f60e894ca0c61cdbae4f5a686d9f08bcefc942",
    "build_date" : "2021-07-14T18:33:36.673943207Z",
    "build_snapshot" : false,
    "lucene_version" : "8.8.2",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```


- Elasticsearch – Kibana: Elasticsearch cuenta con varias herramientas que le ayudan a administrar mejor los datos obtenidos en los incidentes de seguridad informática reportados, una de estas herramientas es Kibana, la cual ayuda a visualizar de una mejor manera los eventos que se registran en el software.

Figura 6 Elasticsearch - Kibana



Para tener una Suite de herramientas lo suficientemente óptima para la prestación de los servicios para la mitigación de incidentes informáticos, se prestara el servicio de IDS por medio de la herramienta Wazuh el cual es totalmente compatible con el SIEM utilizado para la monitorización y administración de datos, este software fue instalado de la siguiente manera:

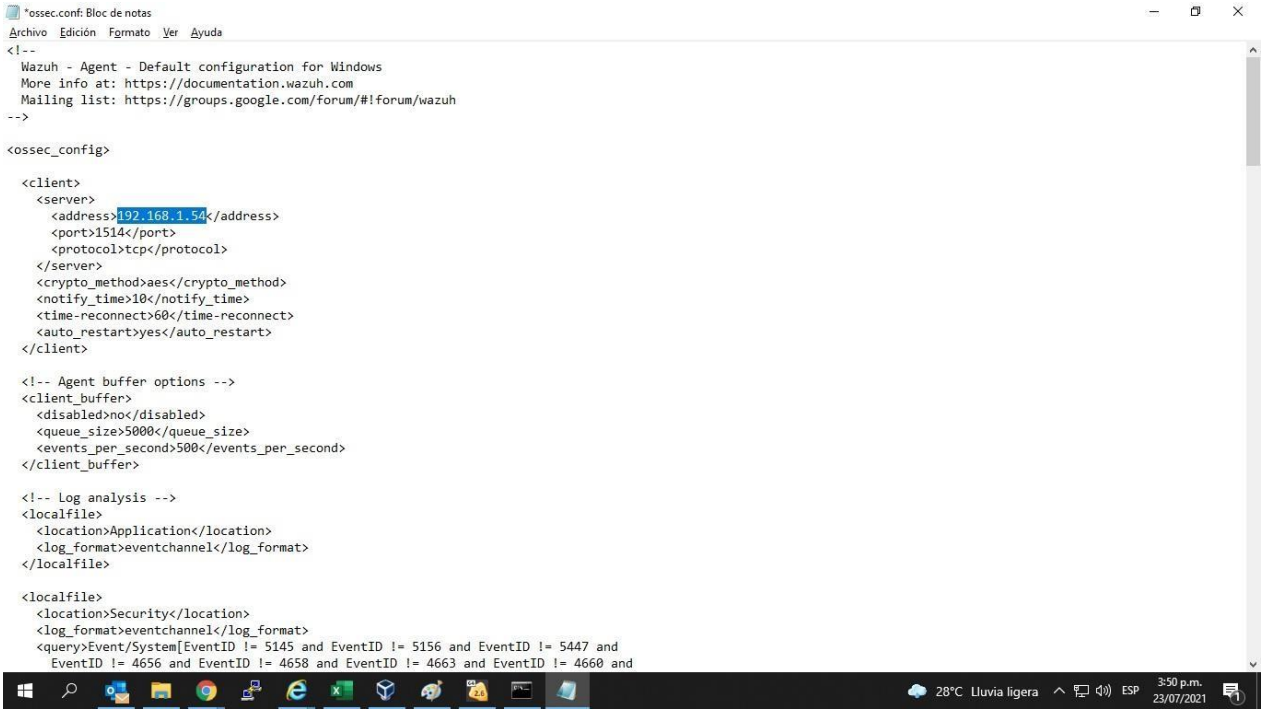
- Instalación de WAZUH: se ingresa a la pagina oficial de wazuh https://wazuh.com/ , después se selecciona la opción instalar wazuh, y selecciona instalar guía dependiendo de la opción que se requiera, una vez en la pagina, se selecciona el sistema operativo en el cual se tiene previsto realizar la instalación y se procede a descargar y ejecutar el instalador del aplicativo[44].

Figura 7 Wazuh Agent Manager

[44] Wazuh; Installation guide. [Sitio web]. [Consulta 21 de julio de 2021]. Disponible en: https://documentation.wazuh.com/current/installation-guide/index.html

Después de ejecutar el aplicativo de wazuh, se sigue la ruta View/ view confg y se procede a modificar el archivo plano de la siguiente manera[45]:

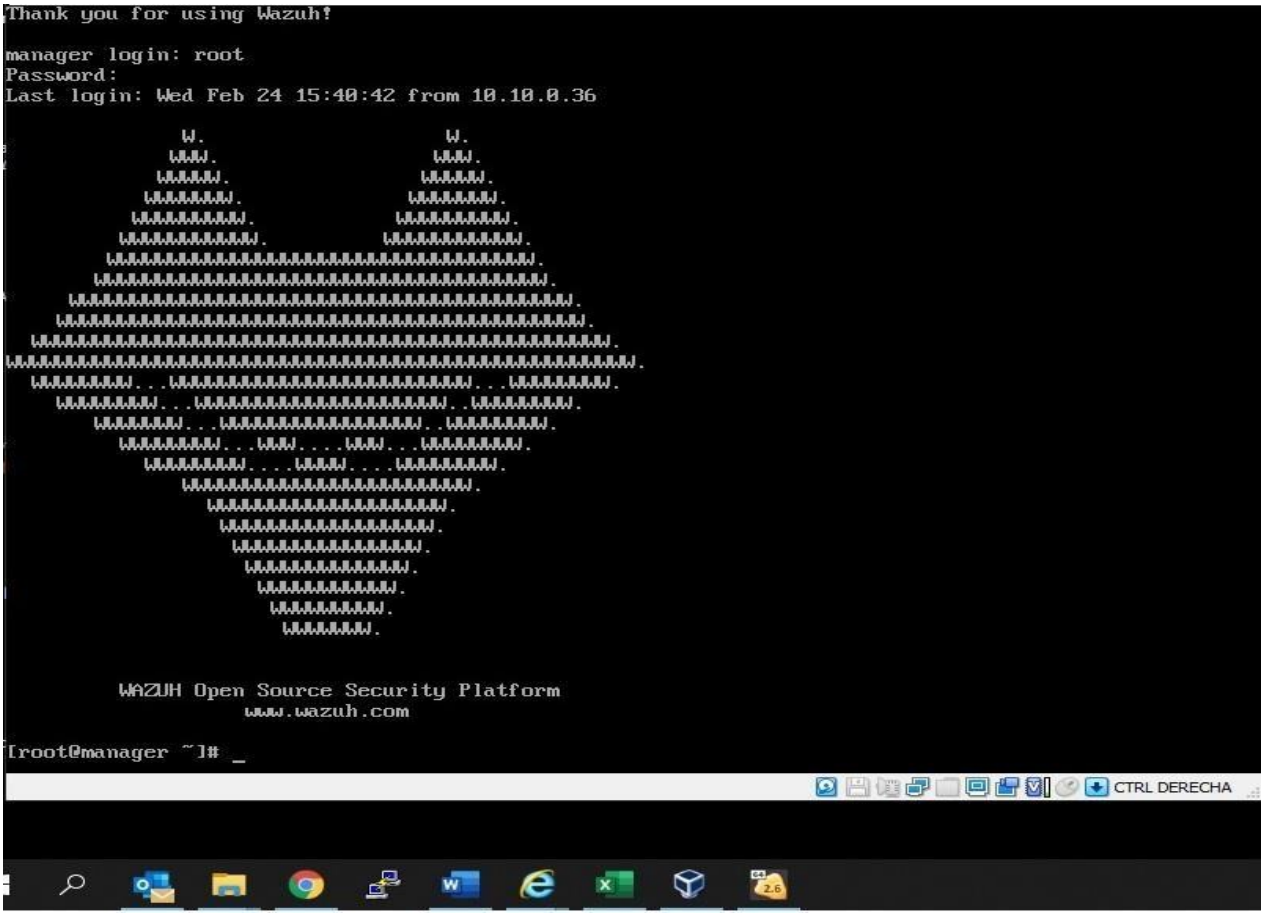
Figura 8 Modificar Ossec.conf



La dirección IP que se debe digitar es la ip en la cual se va alojar el software, después se da guardar, se selecciona la opción Refresh, y se generar la clave de autenticación para el inicio de software.

45 Ibid., p.42

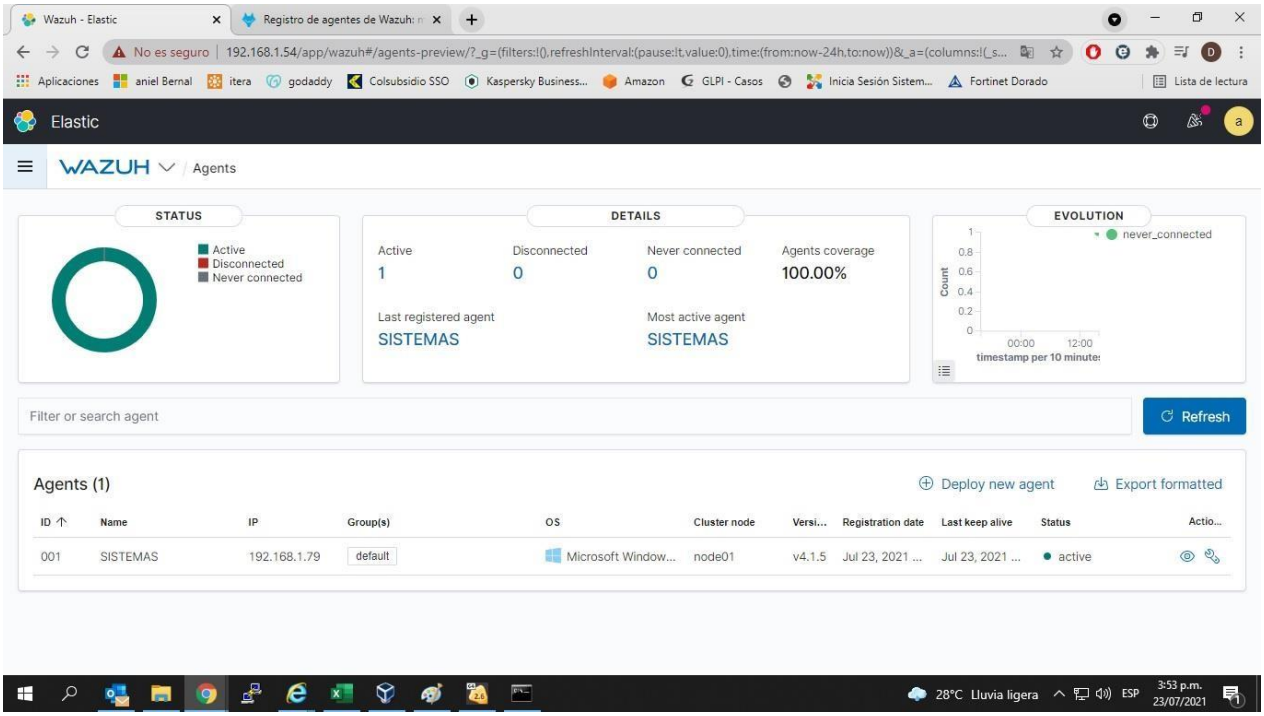
Figura 9 Wazuh Instalado



Una vez finalizado la instalación del software y su registro en el servidor de Wazuh, se ingresa por medio de la ip en el navegador de preferencia en el cual se podrá iniciar sesión y visualizar la interfaz gráfica de wazuh[46].

[46] Ibid., p.42

Figura 10 Wazuh interfaz grafica



- Simular la infraestructura de software en un entorno controlado con el fin de seleccionar las herramientas que apoyen los servicios del Centro de Operaciones de Seguridad – SOC

  Existen en el mercado variedades de herramientas para la implementación de un SOC, ya sea de pago o libres, en el caso de la empresa Platino Sistemas, se utilizarán las herramientas de software de código abierto más adecuadas para desarrollar las actividades de reacción y proactivas, las cuales permiten realizar dichas responsabilidades a cabalidad sin generar ningún costo de licenciamiento para la compañía, también se realizara el montaje de los equipos sobre la máquina virtual VirtualBox, la cual permite instalar varias máquinas virtuales con el propósito de administrarlas todas al mismo tiempo, es necesario tener en cuenta que el rendimiento de esta herramienta depende de la arquitectura de hardware en la cual

se hospedan el VirtualBox, en dicha herramienta se realizara todo el montaje necesario para realizar las distintas pruebas con el fin de poner a prueba la capacidad de respuesta de estas ante la detección de una vulnerabilidad informática[47].

Cabe resaltar que el manejo y la administración de este tipo de herramientas y el reporte de incidentes debe ser controlado por un SIEM, el cual se encarga de hacerle frente a los riesgos informáticos que se reportan en el SOC, proporcionando una vista global de la protección de los sistemas de información, en esta ocasión se utilizara Elasticsearch el cual es un SIEM de analítica y análisis distribuido, el cual es compatible con los formatos más usados, también es una herramienta gratuita abierta a cualquier tipo de empresa, esta solución esta disponible desde el 2010 lo cual indica que tienen más de una década de experiencia en el sector, cabe resaltar que Elasticsearch tiene varias funcionalidades, para el caso de Platino Sistemas, se utilizara para la analítica de seguridad informática. Esta herramienta funciona analizando los datos que pasan por ella sin importar la fuente, ya sea logs, aplicaciones web métricas del sistema, etc, una vez los datos están en Elasticsearch, son parseados, regulados y enriquecidos antes de su clasificación por la aplicación, ya indexados por la herramienta los administradores del sistema podrán hacer consultas complejas de los datos tratados. Para tener una mejor visualización del sistema existe Kibana, el cual es un software de visualización y gestión de información para Elasticsearch, el cual muestra información en tiempo real por medio de histogramas, gráficos y mapas, también cuenta con funciones avanzadas las cuales permiten crear infografías con canvas y visualizar datos geoespaciales en Elastic Maps[48]

[47] Gartner, Las cinco características de un centro de operaciones de seguridad impulsado por inteligencia. [Sitio web]. Gartner. [Consulta: 15 de mayo 2021]. Disponible en: https://www.gartner.com/en/documents/3160820

[48] Elastic;¿Qué es Elasticsearch?[Sitio web]. España. [Consulta: 12 de julio de 2021]. Disponible en: https://www.elastic.co/es/what-is/elasticsearch

Para tener información verídica respecto a como se mueve la seguridad informática a nivel mundial, se cuenta con la herramienta MISP, la cual es de código abierto y se encarga de compartir, recopilar y almacenar datos de ataques dirigidos, información sobre fraude financiero, información de las vulnerabilidades encontradas últimamente, inteligencia de amenazas, etc, con el propósito de contrarrestar cualquier ataque cibernético lo más pronto haciendo el menor daño posible[49].

Cuadro 1 Cuadro Comparativo Software

Cuadro comparativo Software			
Software open source		Software de pago	
Software	costo	Software	costo
Kali Linux- Distribución de Linux (Debian) para auditoria y seguridad informática en general. (contiene variedad de herramientas)	N/A	**Nessus**- Software para escanear vulnerabilidades en varios SO, (Entrega informe de resultados del sistema objetivo)	$ 14,628,235
Nmap- permite realizar el rastreo de puertos del equipo víctima, además del servicio que presta, si está activo, etc. (contiene gran variedad de comandos para las distintas tareas que presta)	N/A	**Fingbox-** hardware que se conecta a la red en la cual se desea analizar, permite el bloqueo de usuarios. (muy fácil de instalar)	US 129
Metasploit libre- software que permite obtener información acerca de vulnerabilidades, además presta servicios de pentesting. (versión libre y de pago)	N/A	**Malwarebytes** (10-99 equipos)- presta seguridad de red, tiene la capacidad de detectar y prevenir amenazas tiene administración centralizada. (basado en la nube)	US 52.49 equipo/año
Wireshark-analizador de tráfico y protocolos de red, permite solucionar problemas en las redes LAN empresariales. (tiene interfaz gráfica amigable con el usuario)	N/A	**PRTG Monitor Network-** permite el monitoreo de red para la optimización de la misma, (se adapta a las necesidades del cliente)	US 11500
Sqlmap-realiza la detección y explotación de fallas en bases de datos SQL. (permite el control de motores de bases de datos)	N/A	**EdgeScan-** solución inteligente que cubre la capa de red, aplicación, detección de API. (cubre toda la pila)	US 15000

[49] Misp Threat sharing; MISP: Plataforma de inteligencia de amenazas de código y estándares abiertos para compartir información sobre amenazas. [Sitio web]. [Consulta: 8 de julio de 2021]. Disponible en: https://www.misp-project.org/

Jhon the Ripper- herramienta para la recuperación de contraseñas, craquear hashes por medio de diccionario o fuerza bruta. (multiplataforma)	N/A	**L0PHTCRACK-** software para la recuperación de contraseñas y auditoria. (verifica la debilidad de una contraseña**)**	US 2395
Hydra- es un “cracker” de inicio de sesión, se puede utilizar en varios protocolos de seguridad. (fácil de manejar)	N/A	**L0PHTCRACK**- software para la recuperación de contraseñas y auditoria. (verifica la debilidad de una contraseña**)**	US 2395
Aircrak-ng- Herramienta para evaluar y auditar la seguridad en redes wifi. (multiplataforma)	N/A	**Wireless WEP Key Password Spy-** Permite recuperar contraseñas de red guardadas en el computador. (permit ever el trafico de red)	US 50
SIEM Wazuh- Permite la detección de amenazas, respuesta a incidentes de seguridad, monitoreo de integridad de la información, etc (presenta informes detallados de los servicios examinados**)**	N/A	**ManageEngine Log360 –** Gestiona los eventos e información de seguridad que se presentan en la red, etc. (realiza seguimiento a los eventos hallados)	US 12000

Fuente: Propia

- Construir la estructura organizacional con roles y funciones, que den soporte al desarrollo de las actividades Centro de Operaciones de Seguridad - SOC.

  Con la construcción del organigrama de la compañía, se puede asignar roles específicos a los profesionales, especialistas técnicos y administrativos de la empresa para que estos desarrollen sus competencias en la prestación de los servicios según la responsabilidad del cargo a desarrollar, con el compromiso del perfil profesional que cada uno, dicho organigrama ayuda a identificar los responsables en cada uno de los procesos los cuales se llevan a cabo en el SOC, lo anterior demuestra que la organización y asignación de responsabilidades y roles ayudan a la mejora continua y tener claro el alcance de la compañía con el centro de operaciones y seguridad.

  Para el desarrollo de la propuesta técnica de consolidación del SOC (Centro de operaciones y seguridad) en la empresa Platino Sistemas, se requiere contar con el

recurso humano especializado en seguridad informática, ingenieros de sistemas o a fines, técnicos en sistemas con conocimientos en ciberseguridad50, además de esto, se debe contar con una comunicación asertiva con los demás SOC, con el fin de obtener la información actualizada y así poder contrarrestar de la mejor manera posible las vulnerabilidades informáticas que se presenten, es de resaltar las herramientas de código abierto las cuales se utilizaran para la implementación del SOC como lo son, SIEM (Security Information Event Management) Elasticsearch, Kibana, Kali Linux, Nmap, aircrack-ng, wireshark, metaesploit, hashcat, WAZUH, itop, etc51, las cuales deben ser utilizadas por el personal idóneo para esta labor, es necesario contar con un registro de ticket para llevar control y trazabilidad de las incidencias reportadas, y de esa manera dar prioridad a los incidentes reportados por los usuarios según su criticidad, además de la documentación de cada una de ellas, lo anterior con el objetivo de dar respuesta con mayor rapidez en caso de algún ataque o incidente, lo cual da confianza en la prestación del servicio y asegura un exitoso desarrollo y administración del SOC en la compañía.

Los roles y responsabilidades de cada uno depende del tipo de SOC que se este implementando para prestar el servicio, teniendo en cuenta una organización multinivel, la cual incluye la alta dirección o gerencia y el cuerpo administrativo y técnico, se asignan las responsabilidades de la siguiente manera[52]:

---

[50] Cano Vargas Jaidur, Propuesta de los documentos administrativos para la creación de un centro de respuestas a incidentes cibernéticos para la empresa caso de estudio Cibersecurity de Colombia LTDA. Especialización en Seguridad Informática. Bogotá. Universidad Nacional Abierta y a Distancia (UNAD). 2020. 98 pag. Disponible en: https://repository.unad.edu.co/handle/10596/36488

[51] Méndez Fonseca Víctor Julio. Marco Tecnológico de un SOC de Nueva Generación [En línea]. 1 ed. Colombia Bogotá. 12 pag. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/7937

[52] Incibe-cert; Respondiendo a incidentes industriales, SOC OT.[Sitio web]. España. [Consulta: 1 de julio de 2021]. Disponible en: https://www.incibe-cert.es/blog/respondiendo-incidentes-industriales-soc-ot

- **Dirección General**: Sera la encargada de comunicar y reportar la información e inteligencia creada por cada uno de los grupos que conforman el SOC, también será la encargada de realizar reuniones para comunicar los avances e inconvenientes

- **Equipo de incidentes**: es el área encargada de coordinar los equipos de respuesta inmediata del SOC, dependiendo del tamaño del área técnica se valida si se necesita un coordinador por cada subárea.

- **Soporte 1 nivel**: Esta área se encargan de monitorización y evaluación de incidencias
- **Soporte 2 nivel:** esta área se encarga de las investigaciones básicas, se tratan posibles soluciones a problemas de baja complejidad, se dan recomendaciones para evitar las propagaciones del malware.

- **Soporte 3 nivel:** en esta área se encuentran los profesionales mas especializados en las diferentes áreas de pentesting, entre ellos esta, ingeniero forense, especialistas en seguridad informática, ingenieros de malware, entre sus funciones esta dar solución a las incidencias de mas complejidad.

Debido a la complejidad, o el alcance del SOC, algunas de las tareas que se desarrollan, se pueden tercerizar con algún proveedor dependiendo del caso, los servicios que mas se contratan con agentes externos son recopilación de pruebas (33%), búsqueda de amenazas (44%), Ingeniería forense (38%), monitorización y detección (35%), cabe resaltar que muchas de las responsabilidades si no se pueden cumplir, lo mejor es

delegarla a otra compañía que si preste el servicio, ya que esto puede acarrear un efecto colateral al depender varias áreas de esa tarea o función[53].

[53] Silicon.es; A fondo: ¿Como funcionan los SOC?. [Sitio web]. España. [Consulta en: 5 de julio de 2021]. Disponible en: https://www.silicon.es/a-fondo-como-funcionan-soc-2362658

7 RECOMENDACIONES

Para tener una mejora continua al momento de prestar los servicios en el SOC, se recomiendan los siguientes pasos para evitar falsos positivos (detección de virus o malware por parte de los antivirus cuando no lo es):

- Documentar el flujo de la información
- Crear exclusiones desde el principio de la implementación
- Simular ataques y probar las alertas programadas
- Crear filtro y políticas de descarte

Además, se hace las siguientes recordaciones:

- Delegar funciones a los expertos en seguridad informática
- Visualizar las posibles amenazas
- Vigilancia 7*24*365
- Investigaciones eficaces
- Respuestas rápidas
- Efectividad operacional
- Aprovechar los recursos

Es de tener en cuenta los servicios que prestara el SOC los cuales son:

Servicios proactivos:

- Comunicados
- Auditorías internas de seguridad
- Difusión de información respecto a seguridad informática
- Vigilancia tecnológica

Servicios reactivos:

- Servicio de alertas
- Gestión de incidentes
- Análisis de incidentes
- Apoyo a respuesta a incidentes
- Coordinación de respuesta a incidentes
- Gestión y análisis de vulnerabilidades
- Gestión de herramientas

Para la prestación de los servicios mencionados, es posible utilizar las siguientes herramientas de software; las cuales son de código abierto.

- Kali Linux
- Nmap
- Metasploit
- Wireshark
- Sqlmap
- Jhon the Ripper
- Hydra
- Aircrack-ng
- SIEM
- Itop
- WAZUH
- MISP
- ELASTICSEARCH

De igual manera se recomienda las siguientes herramientas de hardware para la implementación de laboratorios para la realización de pruebas:

- Servidor web
- Servidor de correo institucional
- Servidor de intranet
- Servidor de archivos
- Servidor de copias de seguridad
- Servidor DNS
- Servidor de Monitoreo
- Servidor Sandbox
- Correlacionador de Eventos
- Registro y seguimiento de Incidentes
- Dispositivos de Conectividad
- Tener presente herramientas para un servicio especial de informática forense

También es necesario contar con los siguientes equipos para garantizar la continuidad del servicio, teniendo el menor impacto en el caso de tener una falla de energía, alguna restauración de información o de algún sistema operativo.

- UPS 20 KVA para terminales de usuario y UPS de 6 KVA para los servidores y equipos de respaldo
- Sistema de respaldo de la información físico y en la nube
- Configuración de Backup de información con sus respectivos controles
- Sistema de aire acondicionado para el cuarto de datos.
- Certificación del cableado estructurado (cable UTP Cat 6a)
- Contar con medidor de temperatura y humedad en el centro de datos.

Figura 11 Laboratorio Controlado

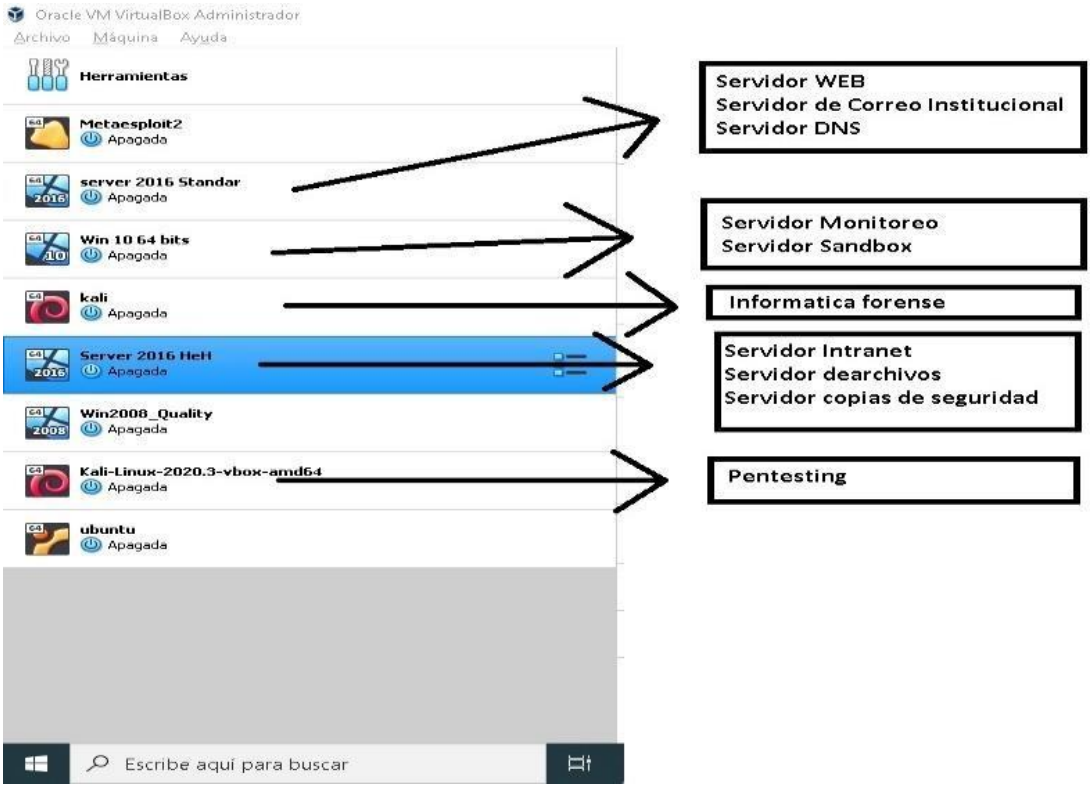
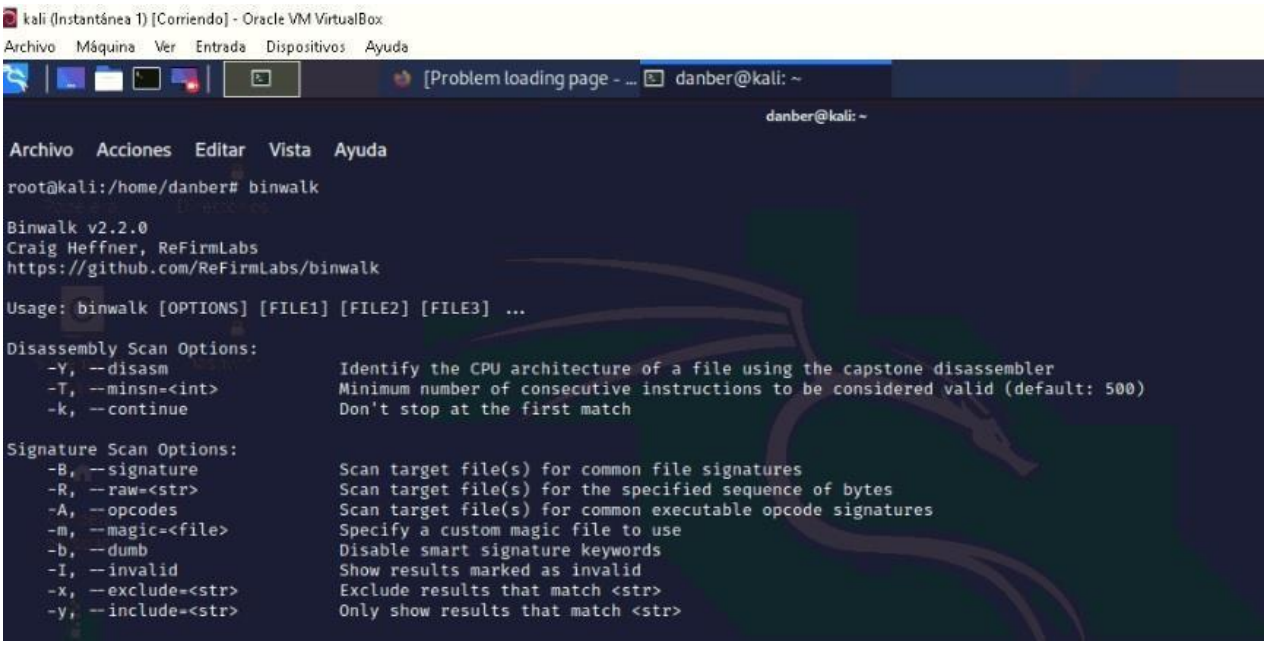


Figura 12 Binwalk - kali Linux

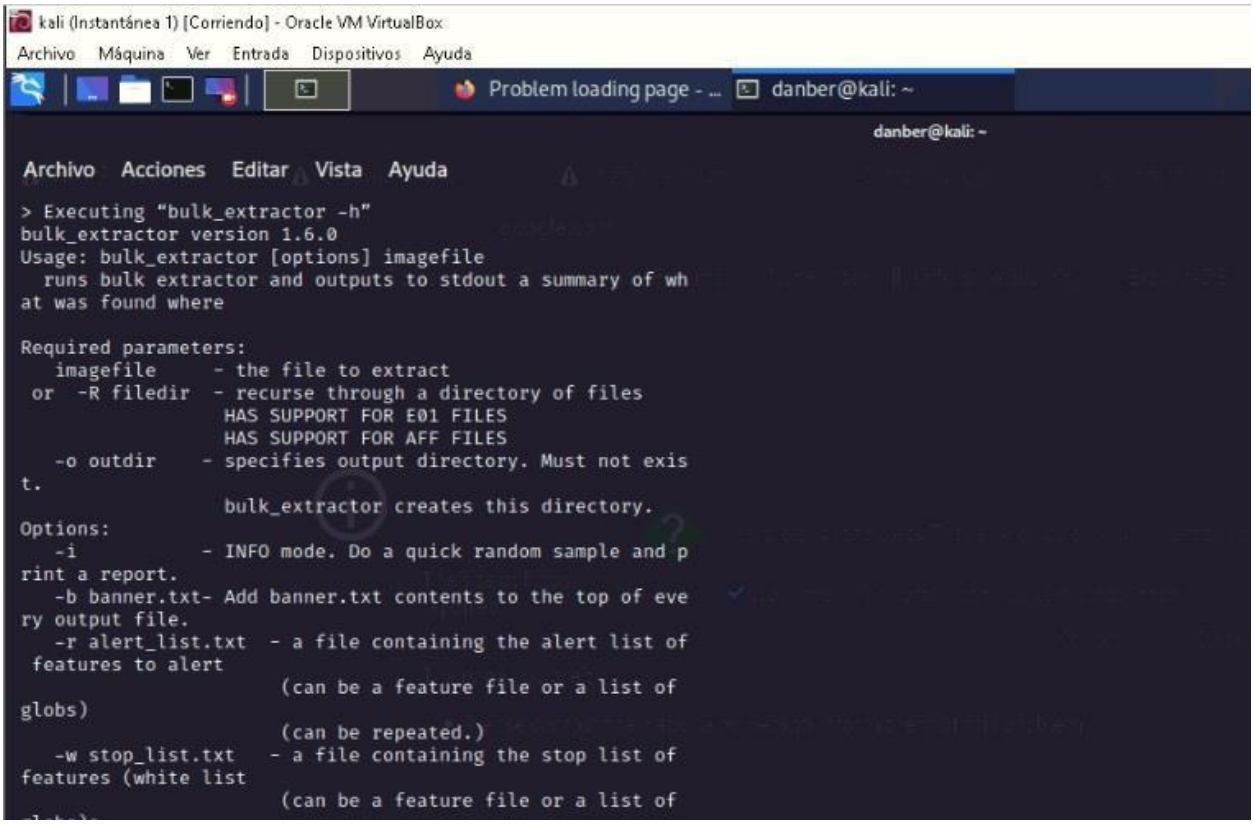


7.1 BINWALK

Es una herramienta para el análisis forense que permite identificar archivos y códigos en las figuras de firmware, esta herramienta hace uso de la biblioteca libmagic, lo cual afirma su compatibilidad con firmas creadas para los archivos Unix[54].

[54] Kali Tools; Descripción del paquete Binwalk;[Sitio web]. [Consulta: 20 de diciembre de 2020]. Disponible en: https://tools.kali.org/forensics/binwalk

Figura 13 Bulk Extractor



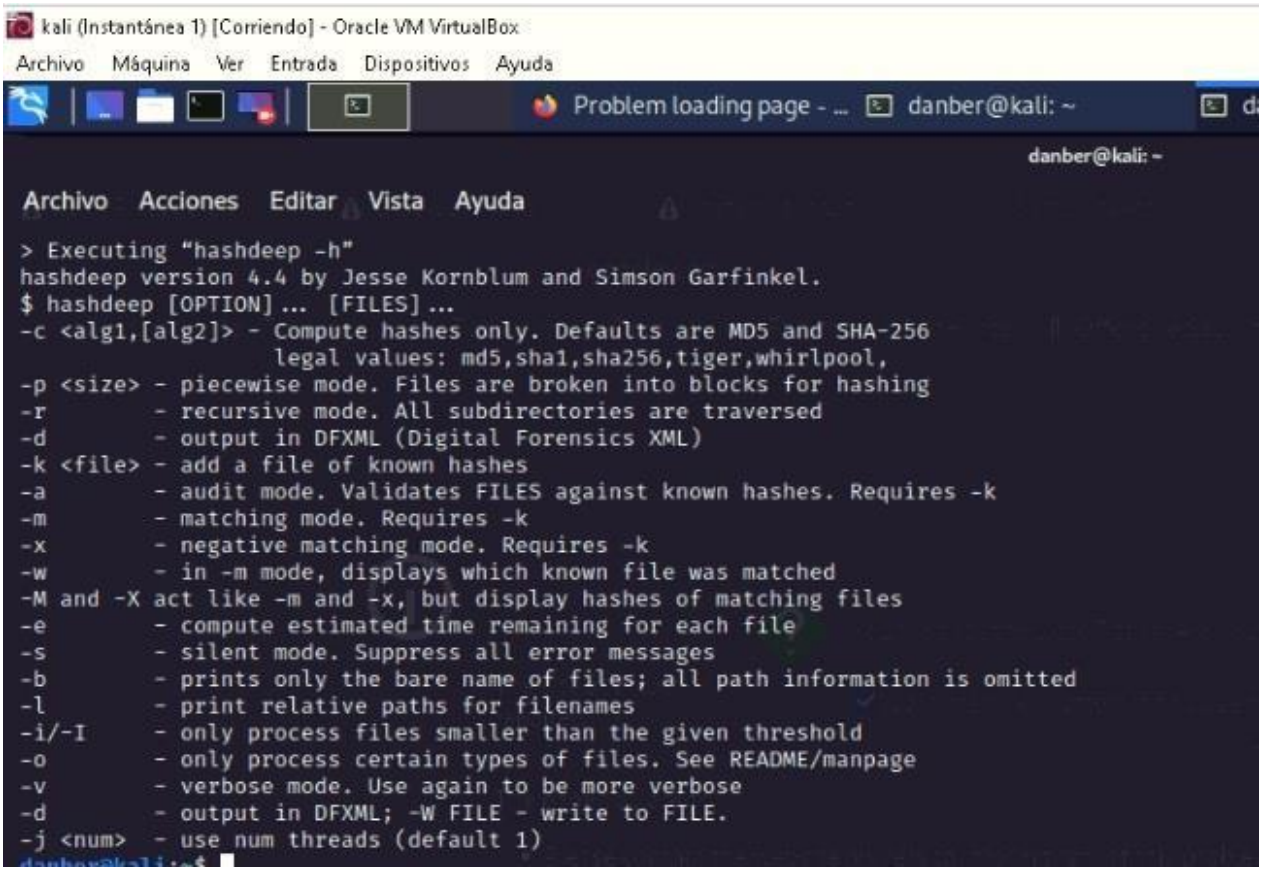
7.2 BULK EXTRACTOR

Esta herramienta es muy útil ya que permite extraer datos importantes como los son correos electrónicos, url, números de tarjetas de crédito y variedad de información digital de sus víctimas, es muy usada en la informática forense para el rastreo de intrusos, malware, investigaciones cibernéticas, unas de las principales características son:

- Eficacia en comparación con otro software que prestan el mismo servicio, ya que puede procesar archivos comprimidos
- Puede crear su propio directorio basándose en las palabras que aparecen en los datos

- Si la maquina tiene varios núcleos en el procesador, más rápida será la labor[55]

Figura 14 hashdeep

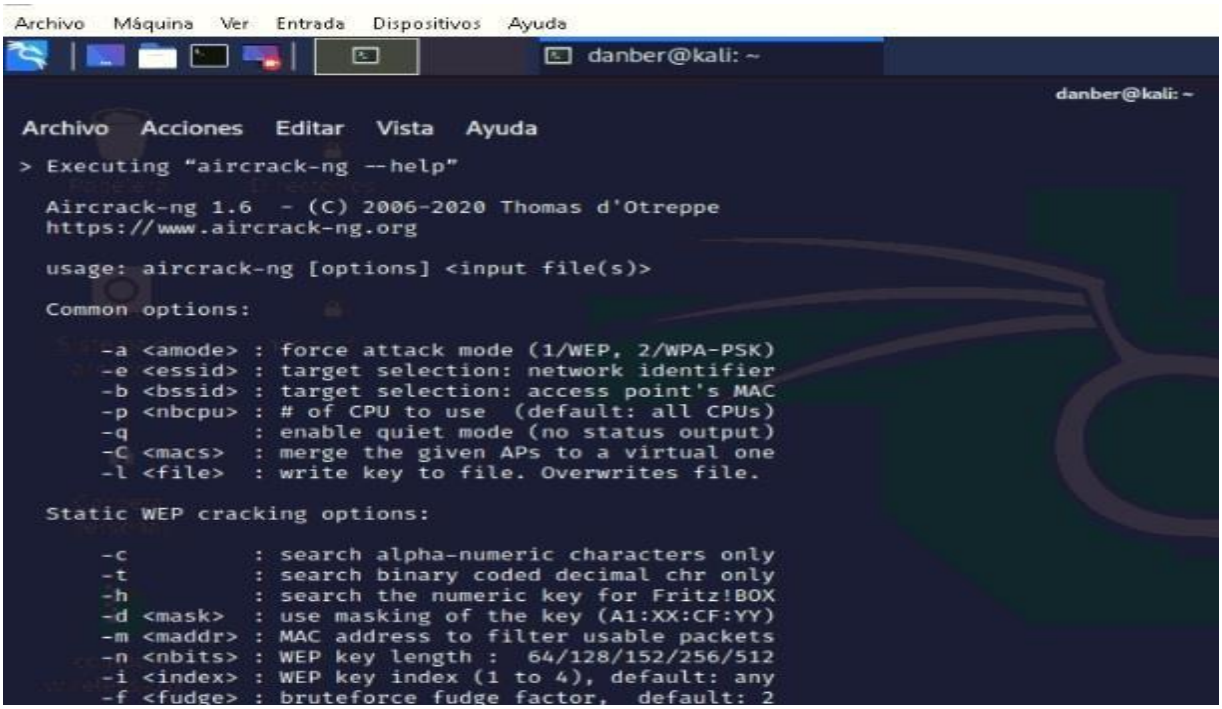


[55] Kali Tools; bulk-extractor package decription; [Sitio web]. [Consulta: 19 de diciembre de 2020]. Disponible en: https://tools.kali.org/forensics/bulk-extractor

7.3 HASHDEEP

Es un instrumento multiplataforma que sirve para descifrar hashes, los tipos de hashes que permite son: SAH 1, SHA256, MD5, Whirlpool y Tigger, Hashddep es la evolución del anterior programa llamado md5deep, el cual agrego varios programas gradualmente.

Figura 15 Aircrack NG

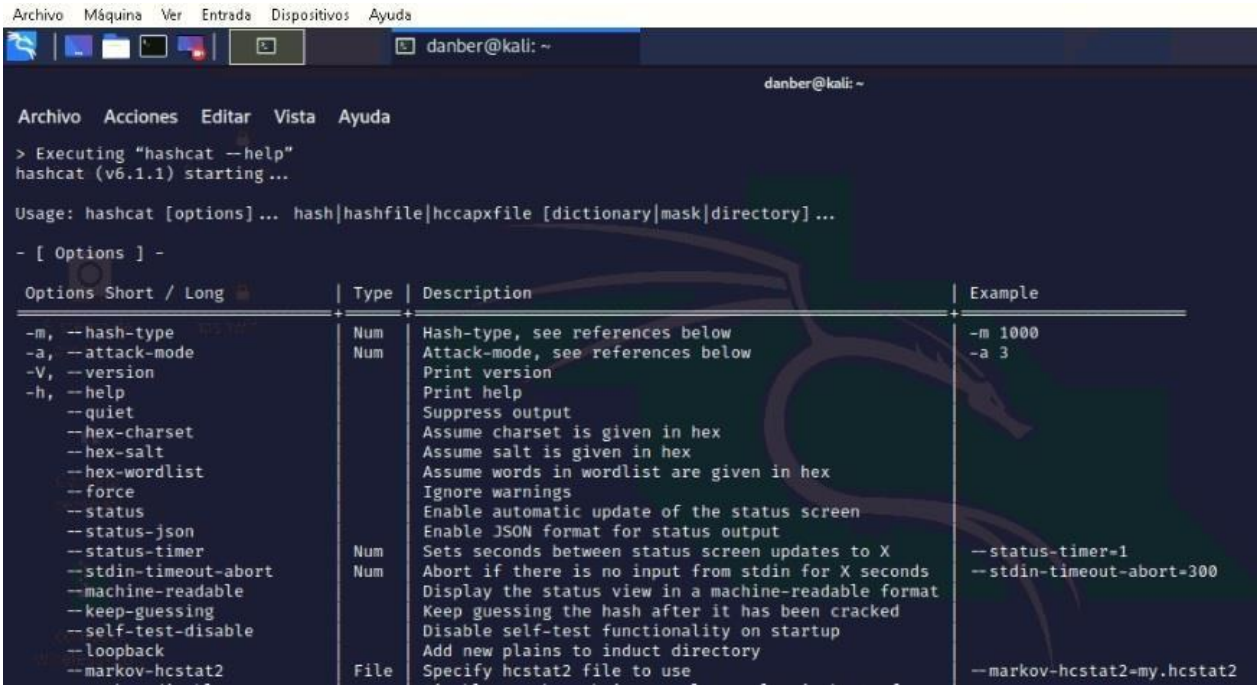


7.4 AIRCRACK-NG

Esta herramienta de la suite que maneja Kali Linux tiene la capacidad de dejar la tarjeta de red en modo monitor, de esta manera puede capturar algo del tráfico inalámbrico, con

el finde obtener información, la cual permitirá realizar algún tipo de ataque, cabe resaltar que no todas las tarjetas de red tienen estas características[56].

Figura 16 HashCat



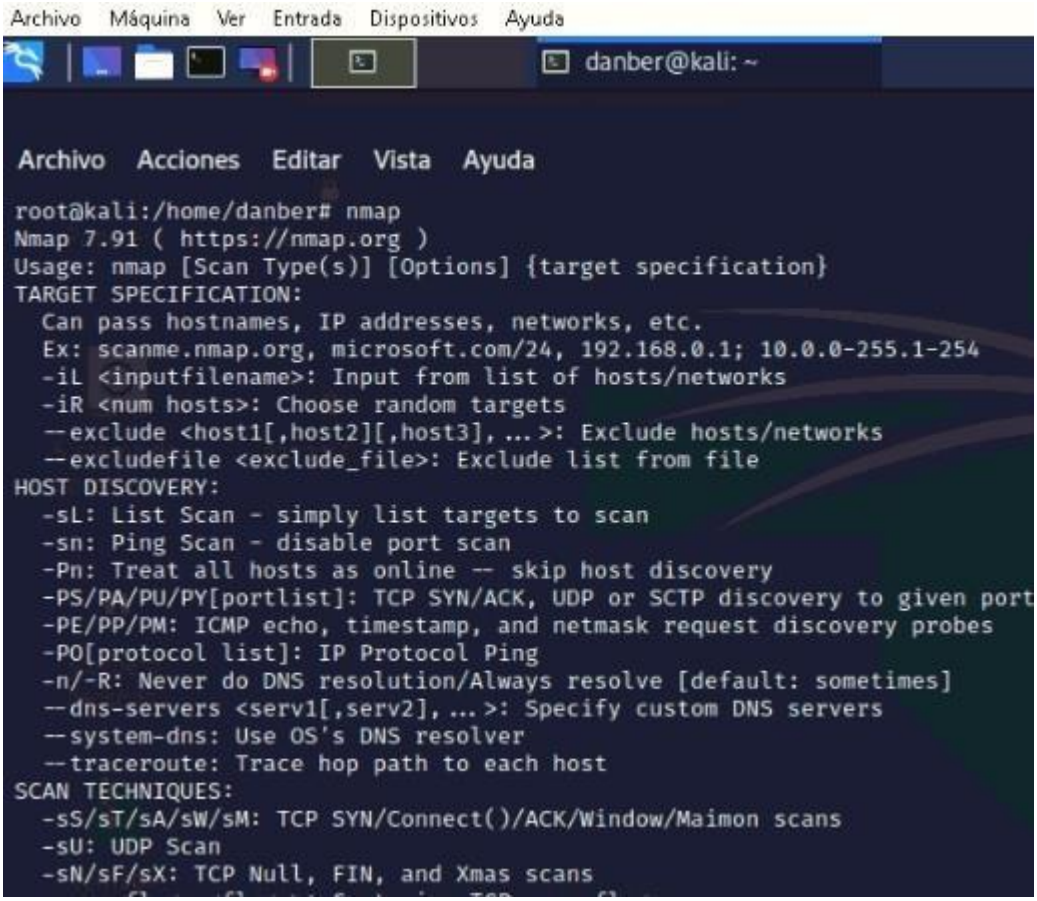
7.5 HASHCAT

Este software permite descifrar contraseñas utilizando varias combinaciones de caracteres con el fin de crackear las credenciales, esta herramienta permite escoger que caracteres utilizar para realizar el ataque, por ejemplo puede utilizar una combinación de letras, números y caracteres especiales, elegir si va o no con mayúsculas, la longitud de la contraseña, etc, es necesario tener en cuenta que se pueden hacer ataques por

[56] Aircrack – ng; Description; [Sitio web]. [Consulta: 15 de diciembre de 2020]. Disponible en: https://www.aircrack-ng.org/

diccionario, fuerza bruta, etc, y dependiendo de las características del equipo, el tiempo de asertividad será menor o mayor[57].

Figura 17 Nmap



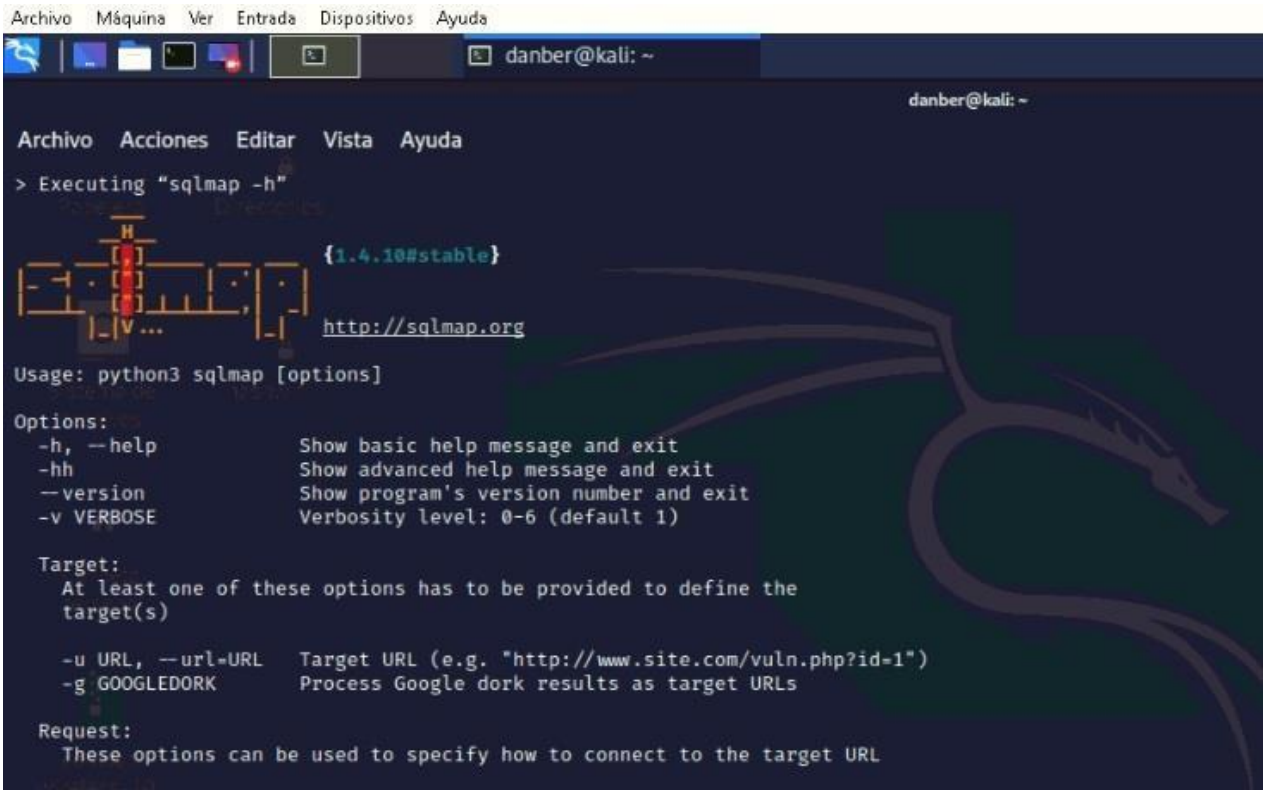
7.6 NMAP

Esta herramienta para la auditoria de redes permite el scanner de puertos de un equipo o de una red corporativa, dentro de sus capacidades esta verificar que puertos están

[57] Kali tools; hashcat package Description; [Sitio web]. [Consulta: 15 de diciembre de 2020]. Disponible en: https://tools.kali.org/password-attacks/hashcat

abiertos o cerrados, que sistema operativo tiene, cual servicio tiene asociado el puerto, etc[58].

Figura 18 SQLmap



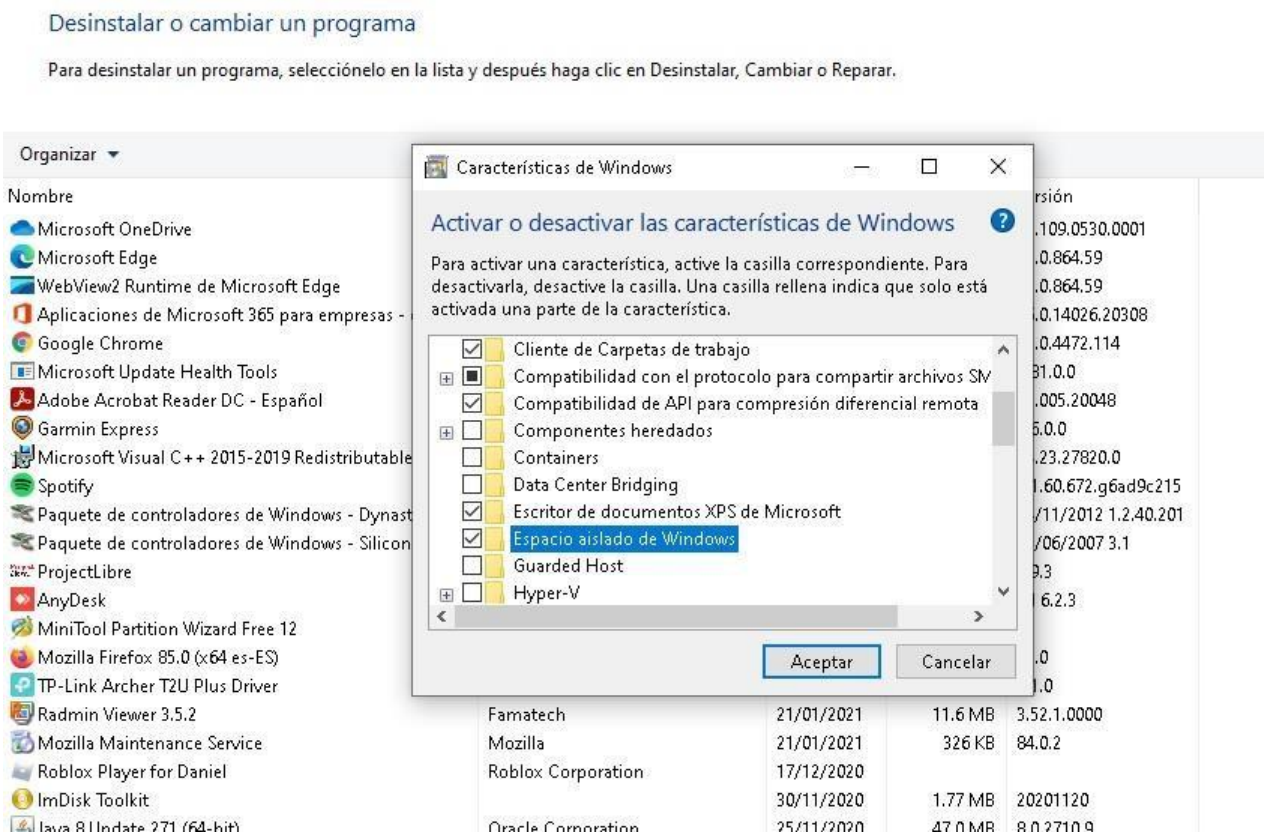
7.7 SQLMAP

Esta herramienta de prueba de penetración detecta y explota las fallas encontradas en las bases de datos SQL, por medio de inyección de código directamente en las bases de datos víctimas, puede ser utilizada en motores de bases de datos como Firebird,

[58] Kali tools; Nmap Package Desciptio; [Sitio web]. [Consulta: 10 diciembre de 2020]. Disponible en: https://tools.kali.org/information-gathering/nmap

PostgreSQL, Oracle, SQL Server, IBM DB2, Acces, soporta 6 tipos de ataques de inyección[59].

Figura 19 Servidor Sandbox Win10



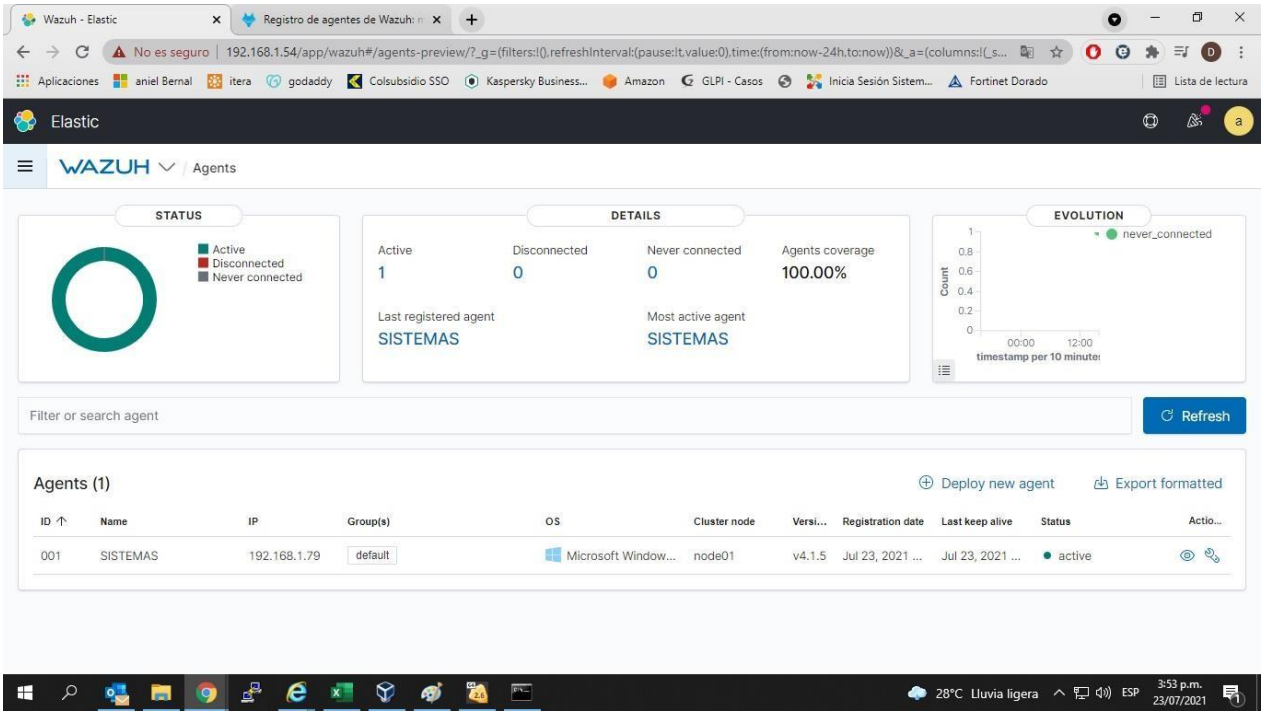
7.8 SERVIDOR SANDBOX

Un servidor Sandbox es un espacio de trabajo seguro, el cual se encuentra aislado de los demás equipos de cómputo de la compañía, este servidor cuenta con unas características estrictas las cuales permiten la ejecución de programas de los cuales no tenemos mucha información sin poner en riesgo el equipo. Existen varios software que

[59] Kali tools; sqlmap Package Description:[Sitio web].[Consulta: 7 de diciembre de 2020]. Disponible en:https://tools.kali.org/vulnerability-analysis/sqlmap

permiten realizar este tipo de prácticas, existen de pago y gratuitos, para el caso problema, se utilizara la herramienta del sistemas operativo Win 10 la cual trae esa opción como se muestra en la anterior imagen[60].

Figura 20 Wazuh



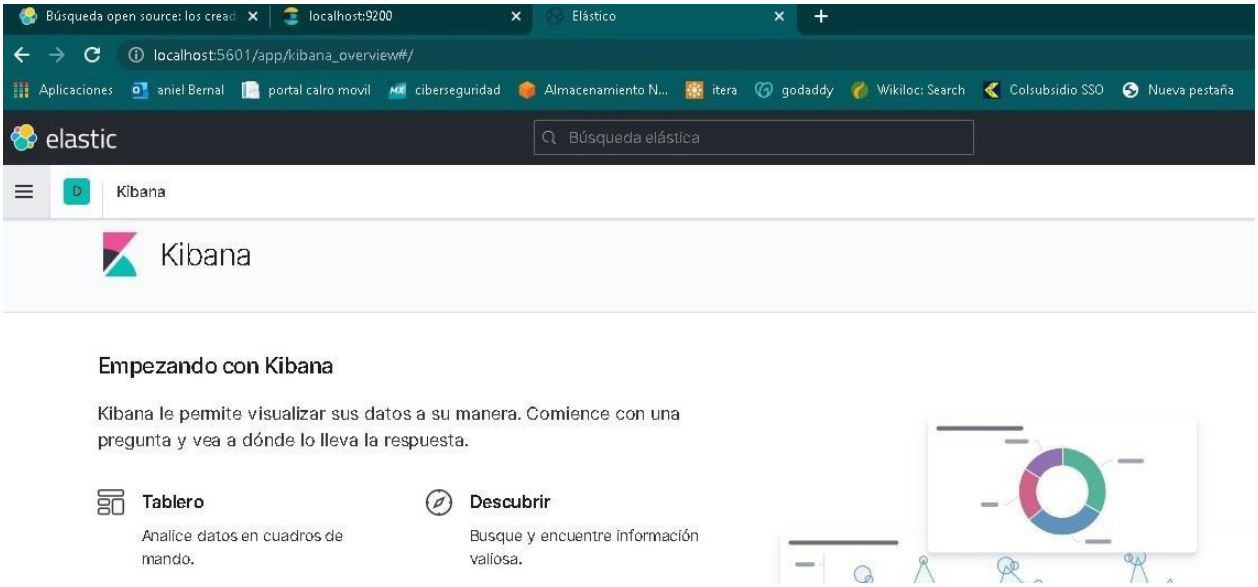
7.9 WAZUH

Este IDS de código abierto para realizar las tareas de monitorización, recopilación y análisis de datos y registros, detección de rootkits, detección de puertos y su estado, integridad de archivos, etc, las cuales son de suma importancia para la implementación

[60] Geeknetic; Como crear un entorno seguro Sanbox con Virtualbox; [Sitio web]. España. [Consulta: 1 julio de 2021]. Disponible en: https://www.geeknetic.es/Guia/1758/Como-crear-un-Entorno-Seguro-Sandbox-con-VirtualBox.html

de un SOC, ya que permiten el control y administración de los riesgos encontrados o reportados al equipo de TI en la empresa Platino Sistemas.

Figura 21 Elasticsearch - Kibana



7.10 ELASTICSEARCH – KIBANA

Este SIEM presta el servicio de analítica y análisis distribuido, además de esto se puede implementar en cualquier tipo de empresa sin importar su tamaño o razón social, una de las ventajas de este software es su gratuidad, también puede analizar cualquier tipo de dato, ya sea numérico, texto, estructurados y no estructurados, cuenta con mas de 10 años en el mercado lo que garantiza una experiencia solida en el sector, este SIEM cuenta con varias herramientas de gratuitas para la monitorización y administración de los incidentes de seguridad informática, una de estas herramientas es kibana la cual permite una buena visualización de métricas de los eventos que transcurren por el software[61].

[61] Elastic;¿Qué es Elasticsearch?[Sitio web]. España. [Consulta: 12 de julio de 2021]. Disponible en:

8 PROPUESTA ECONOMICA

Basados en las necesidades que tiene la empresa Platino sistemas, y en lograr el objetivo empresarial de consolidar la propuesta técnica de un SOC para el año 2022, se tiene en cuenta en este caso en especial, se utilizaran herramientas de código abierto las cuales permiten prestar un buen servicio para los casos que sean reportados por los empleados.

8.1 HERRAMIENTAS SOC

Cuadro 2 Herramientas SOC

	DESCRIPCION	HERRAMIENTA	CATEGORIA	CANTIDAD	UNIDAD	PRECIO
Herramientas SOC	Herramienta SIEM	Wazuh	SIEM	1	und	N/A
	IPS	Snort	Perimetral	1	und	N/A
	Firewall Físico	Fortinet	perimetral	1	und	$ 7.500.000
	Gestión de Incidentes	GLPI	Software	1	und	N/A

Fuente: Propia

8.2 CONSULTORIA Y CERTIFICACION

Cuadro 3 Consultoría y Certificación

	DESCRIPCION	HERRAMIENTA	CATEGORIA	CANTIDAD	UNIDAD	PRECIO
Consultoría y certificación	Consultoría SOC	ARC Software	Asesoría	50	hora	$17.000.000
	Certificación SGSI - ISO 27001:2013	Icontec	Certificación	30	hora	$11.000.000
	Recuperación de Incidentes	Eventum		1	Und	$1.500.000

Fuente: Propia

8.3 PERSONAL

Cuadro 4 Personal

	DESCRIPCION	HERRAMIENTA	CATEGORIA	CANTIDAD	UNIDAD	PRECIO
Personal	Operador SOC	3 turno / 8horas	Personal	4	personal	$1.200.000
	Operador Líder	3 turno / 8horas	Personal	4	personal	$1.600.000
	Analista SOC	3 turno / 8horas	Personal	4	personal	$1.400.000
	Gerente	1 turno / día	Personal	1	personal	$2.500.000
	Jefe Operaciones	1 turno / día	Personal	1	personal	$2.000.000

Fuente: Propia

8.4 PLANTA FISICA E INSTALACIONES

Cuadro 5 Planta Física e Instalaciones

	DESCRIPCION	HERRAMIENTA	CATEGORIA	CANTIDAD	UNIDAD	PRECIO
Planta Física e instalaciones	Control de acceso	Biométrico	Accesos	1	und	$515.000
	Sala de reuniones	Planta física	Planta física	1	und	$4.000.000
	Medidores humedad y temperatura	Medidores	Medición		und	$140.000
	Cableado eléctrico normal y regulado	Planta física	Planta física	15	und	$ 250.000 certificado $200.000 Sin certificado
	Aire acondicionado centro de datos (7000 BTU)	Planta física	Planta física	1	und	$1.200.000
	Detectores de Humo	Planta física	Planta física	1	und	$ 40.000

	ups 20 kva	Planta física	Planta física	1	und	$ 16.000.000

Fuente: Propia

8.5 HERRAMIENTAS HARDWARE

Cuadro 6 Herramientas Hardware

	DESCRIPCION	HERRAMIENTA	CATEGORIA	CANTIDAD	UNIDAD	PRECIO
Herramientas Hardware	*Servidor web *Servidor de correo institucional * Servidor DNS *Servidor AD	Servidor físico Hp Proliant ML 350 – 10 Gen, 64 Gb RAM, Arreglo de discos (RAID 1), de 2 TB 7500 rpm, Procesado Intel Xeon E5-2630 V3, licencia Windows Server 2016/ 2019 standar	Físico	1	Und	$ 18.000.000
	*Servidor de Monitoreo * Servidor Sandbox	VirtuaLBox / Server 2016	Entorno virtual	1	Und	N/A
	*Informática Forense * Pentesting	Procesador Core I 7 Gen 10, 16 Gb Ram, SSD 512 Gb, Tarjeta gráfica	Físico	1	und	$7000000

		de 4 gb, SO Linux				
	*Servidor Copias Seguridad	AWS	Entorno web	1	und	US 0.3 /gb mensual

Fuente: Propia

9 CONCLUSIONES

Gracias al análisis que se realizó para el diseño técnico de SOC para la empresa Platino Sistemas, se concluye que es de suma importancia contar con el conocimiento para realizar dicha implementación, este conocimiento abarca la parte de adquisición de herramientas y personal idóneo para la prestación del servicio, además de tener presente los tipos de CSIRT-CERT y SOC que existen para entender cuál se adapta mejor a las necesidades de la empresa Platino Sistemas. En el mercado existen muchas herramientas que permiten la detección de vulnerabilidades, IDS/IPS, FAW, firewall de bases de datos, pentesting, etc, es de parte de los especialistas elegir las más adecuadas para la prestación del servicio que está plasmada en el alcance de la propuesta.

Cabe recalcar la importancia de la legislación que rige los delitos informáticos, ya que esto puede tener consecuencias graves para la empresa y sus representantes, además de poner en duda la reputación de la compañía al tener malos antecedentes con la ley por este tipo de delitos.

En el presente documento se dan los lineamientos para el Diseño De La Propuesta Técnica Para Consolidación De Un Centro De Operaciones De Ciberseguridad - SOC En La Empresa Platino Sistemas, en la cual se tiene definida la gestión y administración de incidentes de seguridad informática, con el propósito de tener claridad al momento de desarrollar las actividades propias del SOC, de igual forma las políticas establecidas donde se tiene claridad bajo la responsabilidad de que profesional están los procesos de incidentes reportados en el SOC, con la documentación y trazabilidad correspondiente de cada caso atendido, con el fin de evitar reprocesos a futuro, con incidentes de seguridad con técnicas de intrusión similares a las atendidas anteriormente.

Teniendo en cuenta la información que se tiene de la empresa Platino Sistemas, se definieron los roles y responsabilidades para cada uno de los integrantes del grupo de

trabajo del departamento de TI, se definió el tipo de SOC el cual va a prestar los servicios de seguridad informática en la compañía.

Para tener una mejora continua en la prestación de los servicios del SOC, se debe tener en cuenta la constante capacitación a los empleados, ya que las técnicas de intrusión que utilizan los ciberdelincuentes son cada vez más avanzadas, también es necesario tener claridad con el desarrollo de herramientas informáticas ya sean de software o hardware para la prestación de este tipo de servicios, ya que cada vez es más sofisticado y fácil de adquirir por los distintos medios que presta la web

ANEXOS

https://drive.google.com/file/d/1Y4m6uTYz2R9PPZyMT2xrD3klnpOgmHKL/view?usp=sharing

BIBLIOGRAFÍA

Aircrack – ng; Description; [Sitio web]. [Consulta: 15 de diciembre de 2020]. Disponible en: https://www.aircrack-ng.org/

Ballesteros Cárdenas Alex, Propuesta técnica para la creación de un centro de respuestas a incidentes cibernéticos para la empresa caso de estudio Cibersecurity de Colombia LTDA. Especialización en Seguridad Informática. Bogotá. Universidad Nacional Abierta y a Distancia (UNAD). 2020. 125 pag. Disponible en: https://repository.unad.edu.co/handle/10596/36671

Ballesteros, Alex Augusto. Propuesta Técnica Para La Creación De Un Centro De Respuesta A Incidentes Cibernéticos Para La Empresa Caso De Estudio Cibersecurity De Colombia Ltda. Trabajo de grado para Especialista. Bogotá D.C; UNAD (Universidad Nacional Abierta y a Distancia), 2020. [Consultado: 10 de enero de 2021]. Disponible en https://repository.unad.edu.co/bitstream/handle/10596/36671/aballesterosc.pdf?sequence=1&isAllowed=y

B-secure pasión por la seguridad. ¿Cómo elegir un SOC? 3 aspectos que van más allá del costo. Oscar Cortes. [Consulta: 08 de junio de 2021]. Disponible en: https://www.b-secure.co/blog/como-elegir-soc-aspectos-que-van-mas-alla-del-costo-

Cancillería de Colombia, Colombia se adhiere al convenio de Budapest contra la ciberdelincuencia. [Sitio web]. Bogotá. Cancillería de Colombia. [Consulta 10 de junio de 2021]. Disponible en: https://www.cancilleria.gov.co/newsroom/news/colombia-adhiere-convenio-budapest-ciberdelincuencia

Cano Vargas Jaidur, Propuesta de los documentos administrativos para la creación de un centro de respuestas a incidentes cibernéticos para la empresa caso de estudio Cibersecurity de Colombia LTDA. Especialización en Seguridad Informática. Bogotá. Universidad Nacional Abierta y a Distancia (UNAD). 2020. 98 pag. Disponible en: https://repository.unad.edu.co/handle/10596/36488

Cano, Jaidur. Propuesta de los documentos administrativos para la Creación de un Centro de Respuesta a Incidentes Cibernéticos para la empresa caso de estudio Cibersecurity de Colombia LTDA. Trabajo de grado para Especialista. Bogotá D.C; UNAD (Universidad Nacional Abierta y a Distancia), 2020. [Consultado: 15 de enero de 2021]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/36488/jjcanov.pdf?sequence=1&isAllowed=y

Congreso de la república. [Sitio web]. Bogotá Secretaria del senado.[Consulta 15 noviembre de 2020].Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Consejo Nacional de Política Económica y Social; Documento CONPES 3854. Bogotá 01 de Julio de 2021. 91 pag. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

Departamento administrativo de la función pública; Decreto 1704 de 2012; [Sitio web]. Bogotá. [Consulta: 13 mayo de 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=48863

Departamento Nacional de planeación; Documento CONPES 3920. Bogotá 1 de julio de 2021. 116 pag. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3920.pdf

Documento Conpes 3995, Departamento nacional de planeación. Bogotá. 01 de julio de 2020. 51 pag. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Elastic;¿Qué es Elasticsearch?[Sitio web]. España. [Consulta: 12 de julio de 2021]. Disponible en: https://www.elastic.co/es/what-is/elasticsearch

Elastic; Download Elasticsearch; [Sitio web]. España. [Consulta: 15 de julio de 2021]. Disponible en: https://www.elastic.co/es/downloads/elasticsearch

El Congreso de Colombia; Ley 527 de 1999. [Sitio web]. Bogotá. [Consulta: 20 de mayo de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html.

Exabeam, 10 características imprescindibles para un SIEM moderno. [Sitio web]. [Consulta: 01 de junio de 2021]. Disponible en: https://www.exabeam.com/siem/next-gen-siem

Gartner, Las cinco características de un centro de operaciones de seguridad impulsado por inteligencia. [Sitio web]. Gartner. [Consulta: 15 de mayo 2021]. Disponible en: https://www.gartner.com/en/documents/3160820

Geeknetic; Como crear un entorno seguro Sanbox con Virtualbox; [Sitio web]. España. [Consulta: 1 julio de 2021]. Disponible en: https://www.geeknetic.es/Guia/1758/Como-crear-un-Entorno-Seguro-Sandbox-con-VirtualBox.html

Incibe-cert; Respondiendo a incidentes industriales, SOC OT.[Sitio web]. España. [Consulta: 1 de julio de 2021]. Disponible en:https://www.incibe-cert.es/blog/respondiendo-incidentes-industriales-soc-ot

ISO 27001, Normas ISO 27001.ISO 27001. [Consulta: 11 de junio de 2021]. Disponible en: https://normaiso27001.es/

ISO tools, Sistema de Gestión de riesgo y seguridad. ISO Tools. [Consulta: 11 de junio de 2021]. Disponible en: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

ISO, ISO /IEC 27035-1: 2016; Tecnología de la información – Técnicas de seguridad - Gestión de incidentes de seguridad de la información – parte 1- Principios de gestión de incidentes. [sitio web]. ISO [Consulta: 10 de abril de 2021]. Disponible en: https://www.iso.org/standard/60803.html

ISO, Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información – Requisitos. ISO. [Consulta: 13 de junio de 2021]. Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1

Kali Tools; bulk-extractor package decription; [Sitio web]. [Consulta: 19 de diciembre de 2020]. Disponible en: https://tools.kali.org/forensics/bulk-extractor

Kali Tools; Descripción del paquete Binwalk;[Sitio web]. [Consulta: 20 de diciembre de 2020]. Disponible en: https://tools.kali.org/forensics/binwalk

Kali tools; hashcat package Description; [Sitio web]. [Consulta: 15 de diciembre de 2020]. Disponible en: https://tools.kali.org/password-attacks/hashcat

Kali tools; Nmap Package Desciptio; [Sitio web]. [Consulta: 10 diciembre de 2020]. Disponible en: https://tools.kali.org/information-gathering/nmap

Kali tools; sqlmap Package Description:[Sitio web].[Consulta: 7 de diciembre de 2020]. Disponible en: https://tools.kali.org/vulnerability-analysis/sqlmap

Léxico. [Sitio web].Powered by Oxford.[Consulta 20 noviembre de 2020].Disponible en: https://www.lexico.com/es/definicion/ disenar

Léxico. [Sitio web].Powered by Oxford.[Consulta 20 noviembre de 2020].Disponible en: https://www.lexico.com/es/definicion/propuesta

Léxico. [Sitio web].Powered by Oxford.[Consulta 20 noviembre de 2020].Disponible en: https://www.lexico.com/es/definicion/tecnica

Méndez Fonseca Víctor Julio. Marco Tecnológico de un SOC de Nueva Generación [En línea]. 1 ed. Colombia Bogotá. 12 pag. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/7937

Ministerio de defensa de España, Guía de creación de un CERT /CSIRT. España: Editor y Centro Criptológico Nacional, 2011. 60 pag. Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-sep11.pdf

Ministerio de Defensa de España. GUIA DE CREACION DE UN CERT / CSIRT. [Sitio web]. España. [Consultado: 20 enero de 2021]. Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-sep11.pdf.

Misp Threat sharing; MISP: Plataforma de inteligencia de amenazas de código y estándares abiertos para compartir información sobre amenazas. [Sitio web]. [Consulta: 8 de julio de 2021]. Disponible en: https://www.misp-project.org/

Monje Carlos Arturo, Metodología de la investigación cualitativa y cuantitativa guía didáctica, [en línea]. Neiva-Colombia, Universidad Surcolombiana, facultad de Ciencias sociales y Humanas, 2001. Pag 217.

Morales González Carlos, Moreno Sánchez Omar, Ortigoza Pérez Johanna. Propuesta para un centro de operaciones y seguridad (SOC) para fuerza Aérea Colombiana. Ingeniería de sistemas. Bogotá. Universidad Piloto de Colombia. 2014. 94 pag. Disponible en: http://polux.unipiloto.edu.co:8080/00001627.pdf

Normas-iso, ISO 27001 Gestión de la seguridad de información. [Consulta: 09 de junio de 2021]. Disponible en: https://www.normas-iso.com/iso-27001/

Nsit, Que es un SOC: Funciones y objetivos principales. [Sitio web]. Camila Pachon. [Consulta: 05 de junio de 2021]. Disponible en: https://www.nsit.com.co/que-es-un-soc-funciones-y-objetivos-principales/

Oracle, ¿Qué es un SOC?. [Sitio web]. Oracle. [Consulta: 01 de junio de 2021]. Disponible en: https://www.oracle.com/es/database/security/que-es-un-soc.html

Proyecto Aurora; Proyecto Aurora. [Sitio web].[Consulta: 01 julio de 2021]. Disponible en: Proyecto Aurora ONG (proyecto-aurora.org)

Revista Dinero. [Sitio web]. Bogotá. [Consulta 18 noviembre de 2020]. Disponible en:https://www.dinero.com/tecnologia/articulo/cuanto-subieron-las-ciberamenazas-en-el-segundo-trimestre/305962

Secretaria Jurídica Distrital; Decreto 1727 de 2009 Nivel Nacional. [Sitio web]. Bogotá. [Consulta: 23 de abril de 2021]. Disponible en:

https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36251

SGSI; ISO/IEC 27035 Gestión de incidentes de seguridad. [Sitio web]. [Consulta: 1 de julio de 2021]. Disponible en:https://www.pmg-ssi.com/2020/07/iso-iec-27035-gestion-de-incidentes-de-seguridad/

Silicon.es; A fondo: ¿Como funcionan los SOC?. [Sitio web]. España. [Consulta en: 5 de julio de 2021]. Disponible en: https://www.silicon.es/a-fondo-como-funcionan-soc-2362658

Unir la Universidad en Internet; Red Team, Blue team y purple team, ¿Cuáles son sus funciones y diferencias?. [Sitio web]. España.[Consunta en: 19 de julio de2021]. Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

UST; La evolución del SOC ante el nuevo modelo de amenazas. [Sitio web]. España. [Consulta: 15 de junio de 2021]. Disponible en:https://www.ust.com/es/insights/la-evolucion-del-soc-ante-el-nuevo-modelo-de-amenazas

Viewnext and IBM Subsidiary;¿Qué es un SIEM?.[Sitio web].[Consulta: 1 de junio de 2021]. Disponible en: https://www.viewnext.com/que-es-un-siem/

Wazuh; Installation guide. [Sitio web]. [Consulta 21 de julio de 2021]. Disponible en: https://documentation.wazuh.com/current/installation-guide/index.html

Welifesecurity.[Sitio web].Eset.[Consulta 25 noviembre de 2020].Disponible en: https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

ZDnet;The Morris wrom: Internet Malware turns 25. [Sitio web].United Kingdom:[Consulta:

4 de junio de 2021]. Disponible en: https://www.zdnet.com/article/the-morris-worm-internet-malware-turns-25/