DISEÑO TÉCNICO, CONFIGURACIÓN BÁSICA Y CREACIÓN DEL CSIRT EN CIBERSECURITY DE COLOMBIA LTDA

OMAR TIQUE MASMELA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C.
2021

DISEÑO TÉCNICO, CONFIGURACIÓN BÁSICA Y CREACIÓN DEL CSIRT EN CIBERSECURITY DE COLOMBIA LTDA

OMAR TIQUE MASMELA

Trabajo de grado, proyecto aplicado de desarrollo tecnológico presentado para optar el título de ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Asesor
JHON FREDY QUINTERO T.
M.Sc. Seguridad Informática.
Esp. Seguridad Informática.
Ing. de Sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C.
2021

NOTA DE ACEPTACIÓN:

_____

_____

_____

_____

_____

_____

_____

_____

_____

Nombre director, orientador, asesor

_____

Firma jurado (Nombres)

_____

Firma Jurado (Nombres)

Bogotá, D.C. Febrero, 2021

DEDICATORIA

Dedico ante todo este trabajo a Dios, quien es la fortaleza, la salud, la perseverancia y la vida misma, permitiéndome continuar creciendo profesionalmente, contar con el incondicional apoyo de mi esposa y familia; a mi padre, aunque ausente proyectó mi visión por alcanzar los objetivos propuestos, con fe, sabiduría y motivación a través de su apoyo incondicional y las palabras de aliento cuando niño manifestadas.

AGRADECIMIENTOS

El autor de este trabajo expresa su más profunda gratitud a los ingenieros; Jhon Fredy Quintero T., Martin Camilo Cancelado, Director y Tutor de la Especialización en Seguridad Informática de la Universidad Nacional Abierta y a Distancia UNAD, por la disposición, su constante colaboración, comentarios y sugerencias que han permitido la elaboración de este trabajo.

Mi más sincero agradecimiento a todos y cada uno de los docentes que hacen parte de la Especialización en Seguridad Informática por contribuir con su paciencia, disponibilidad y grandiosa generosidad para compartir sus conocimientos, experiencia y apoyo, fortaleciendo con ellos mí formación académica y ampliar el horizonte de oportunidades en mi vida profesional.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

GLOSARIO

ISO	Organización Internacional para la Normalización
IEC	La Comisión Electrotécnica Internacional
IRT	Equipo de Respuesta a Incidentes
IRC	Capacidad de Respuesta a Incidentes
IHT	Equipo de Manejo de Incidentes
IMT	Equipo de Gestión / Gestión de Incidentes
SOC	Centro de Operaciones de Seguridad
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
UTM	Unified Threat Management/ Gestión Unificada de Amenazas
LAN	Local Area Network
SIP	Session Initiation Protocol
UPS	Uninterruptible Power Supply **=** Sistemas de Potencia Ininterrumpida
UTP	Unshielded Twisted Pair
TIA	Telecommunications Industry Association
UIT	Unión Internacional de Telecomunicaciones
ANSI	Instituto Nacional Estadounidense de Estándares
CIRT	Equipo Informático de Respuesta a Incidentes
CIRC	Capacidad o Centro de Respuesta a Incidentes Informáticos
SIRT	Equipo de Respuesta a Incidentes de Seguridad

SERT	Equipo de Respuesta a Emergencias de Seguridad
CCTV	Circuito Cerrado de Televisión
SIEM	Security Information and Event Management
NMAP	Aplicación de código abierto usado para escaneo de puertos en los equipos de computo
GDPR	Reglamento General de Protección de Datos
DDoS	Distributed Denial of Service/Ataque de Denegación de Servicio Distribuido
I+D+i	Innovación + Desarrollo + Investigación
TIC´s	Tecnologías de la Información y comunicación
ENISA	Agencia Europea de Seguridad de las Redes de la Información
CSIRT	Computer Security Incident Response Team
OSSIM	Open Source Security Information and Event Management
DARPA	Defense Advanced Research Projects Agency
MINTIC	Ministerio de Tecnologías de la Información y la Comunicación
NESSUS	Aplicación usada para la detección de vulnerabilidades en equipos de cómputo.
ROUTER	Equipo activo de red que permite enrutar el paquete de datos entre las diferentes redes, incluyendo el Internet
SWITCH	Equipo activo de red que permite el acceso a la red de dispositivos que posean una tarjeta de red (computador, teléfonos IP, etc.)
CERT/CC	Computer Emergency Response Team/ Coordination Center
ARPANET	Advanced Research Projects Agency Network
PROXMOX	Entorno de virtualización de servidores publicado bajo la licencia de software libre GNU AGPL, v3, está disponible gratuitamente para descargar, usar y compartir.

MALWARE Software malicioso y dañino que infiltra un sistema informático con el objeto de sustraer, alterar o suprimir información

FIREWALL Cortafuegos, hardware o software, o la combinación de ambos que por su estructuración y/o programación permite el bloqueo, filtro de amenazas por software malicioso a través de las redes, permitiendo mantener la integridad de la información y la infraestructura en una empresa, sus equipos de cómputo, dispositivos electrónicos y equipos móviles. previniendo accesos sin autorización al interior de red.

e-Banking Todas las formas posibles de interactuar con un banco de manera electrónica y en línea**.**

CIBERSEGURIDAD Es la práctica de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos.

VMware ESXi vSphere Es una completa suite de virtualización, diseñada para virtualizar a través de hardware servidores y centros de datos.

RESUMEN

La realización del presente trabajo como proyecto final de grado, para obtener el título de especialista en seguridad informática mediante la transferencia de conocimiento, esto es realizando el desarrollo de un trabajo aplicado orientado a lograr el “DISEÑO TÉCNICO, CONFIGURACIÓN BÁSICA Y CREACIÓN DEL CSIRT EN CIBERSECURITY DE COLOMBIA LTDA”**.** El proyecto ha sido elaborado con tres variantes fundamentales a saber y contiene en su estructura la parte de investigación realizada frente a las definiciones en si sobre lo que es un CSIRT, su estructuración y administración a nivel técnico; posteriormente esta la investigación y el análisis de las herramientas a nivel de software y aplicaciones que son viables usar y aplicar para la creación del mismo al interior de una empresa, para el caso específico y de acuerdo con la respectiva guía y requerimientos académicos se enfoca a la empresa “CIBERSECURITY DE COLOMBIA LTDA”, finalmente se encuentra la realización de la parte técnica en cuanto a infraestructura, software de aplicaciones y/o herramientas a usar, instalación y configuración de estas en un red creada como prueba de funcionamiento, las cuales han sido realizadas y plasmadas mediante un video creado sobre acceso y administración de las que fueron implementadas.

Lo que resalta en este proyecto aplicado y por ende de transferencia de conocimiento ha sido comprobar que, si es posible el uso de software de tipo OpenSource con la finalidad de proteger los activos intangibles de las empresas y que lo puede soportar el profesional de TI, sin incurrir en costos innecesarios o infraestructuras propietarias y demasiado costosas.

INTRODUCCIÓN

Estando de acuerdo con el hecho de que es una propuesta de “Transferencia de Conocimiento” orientado a desarrollar las competencias del saber y el saber hacer, se puede afirmar que el DISEÑO TÉCNICO, CONFIGURACIÓN BÁSICA Y CREACIÓN DEL CSIRT EN CIBERSECURITY DE COLOMBIA LTDA a nivel empresarial y/o institucional, es un proyecto en el cual se compilan y convergen diferentes líneas de conocimiento, en el cual se agrupan diferentes tecnologías y procedimientos necesarios que permiten culminar una determinada tarea, en este caso si al interior del CSIRT se ofrecen servicios de diferentes líneas dentro de la infraestructura del área de TIC´s de cualquier institución; teniendo como un fin el establecimiento adecuado de canales de comunicación con los diferentes actores involucrados que son los especializados en cada uno de los servicios que puede ofrecer, permitiéndoles culminar sus tareas de forma ordenada y sistemática.

Es evidente que en la actualidad 6 de cada 10 profesionales y específicamente para el componente de TIC´s y aún lo es más crítico en el campo de la seguridad informática y para el DISEÑO TÉCNICO, CONFIGURACIÓN BÁSICA Y CREACIÓN DEL CSIRT EN CIBERSECURITY DE COLOMBIA LTDA, no poseen herramientas metódicas aplicadas, que permitan realizar el diseño y configuración de este tipo de infraestructura en pro de lograr la contención de las amenazas de los delincuentes informáticos que existen en el ciberespacio cuando se atiende un incidente de este tipo.

Una institución que no pueda contar con este tipo de herramientas y centro de atención a incidentes informáticos y el personal idóneo puede significar, la realización de procedimientos erróneos y que el incidente en si sea desatendido o que en el peor de los casos no se den por enterado los administradores de infraestructura tecnológica ocasionando la perdida de información y los datos.

En países como España, Estados Unidos de Norteamérica, Reino Unido han realizados las acciones necesarias por parte de los organismos gubernamentales para hacer frente a los ataques del crimen organizado cibernético, una de las más importantes y que ha sido el referente de otros estados es el Reglamento General de Protección de Datos (GDPR), por sus siglas en inglés) de la Unión Europea); de igual forma han contribuido con las directrices que han permitido la creación de los CSIRT en el sector gobierno y los organismos de investigación de delitos informáticos, y respuestas a los incidentes informáticos.

De acuerdo con lo expuesto anteriormente, resulta necesario el DISEÑO TÉCNICO, CONFIGURACIÓN BÁSICA Y CREACIÓN DEL CSIRT EN CIBERSECURITY DE

COLOMBIA LTDA al interior de una empresa o institución o su contratación en la modalidad de prestación de servicios, con áreas, procedimientos y procesos bien definidos que permitan ser ejecutados y realizados por el personal que lo componen y sin el temor a cometer errores en la investigación de incidentes informáticos.

1. FORMULACION DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

¿Se hace necesario conocer cuáles son los aspectos técnicos, estándares, normas y legislación que debe tenerse en cuenta para realizar la creación y/o el diseño técnico y configuración básica para poner en funcionamiento el CSIRT al interior de CIBERSECURITY DE COLOMBIA LTDA, para la investigación de incidentes de tipo informático en el componente de TIC´s, en razón a los riesgos y amenazas que presenta la información de esta y los ataques de los que han sido víctimas?

2. JUSTIFICACIÓN

Ante la ausencia de un conocimiento especializado del personal de administradores de la infraestructura de TIC´s a nivel lógico y físico en las instituciones y empresas; la misma transferencia de ese conocimiento técnico que aborda la problemática que hoy día tiene la información y los datos (Seguridad Informática), como lo es el aseguramiento de la misma, las herramientas que deben ser implementadas para su protección y la minimización del riesgo de su perdida, hurto y alteración a través de estas, ha mostrado la necesidad de generar un cambio en este campo que sea el adecuado, a su vez vanguardista, teniendo presente los avances tecnológicos y la evolución de las Tecnologías de la Información y las Comunicaciones (TIC´s), se hace evidente la carencia de un fortalecimiento institucional y empresarial en los procedimientos de prevención, atención, investigación y seguimiento adecuado a los incidentes de seguridad que se susciten al interior de estas o de los clientes que buscan su ayuda ante casos similares, recordemos la transversalidad y la incidencia de este tipo de incidentes en cualquier tipo de empresa o institución que hoy día hace uso de las tecnologías para administrar cualquier tipo de proceso, el DISEÑO TÉCNICO, CONFIGURACIÓN Y LA CREACION DEL CSIRT EN CIBERSECURITY DE COLOMBIA LTDA, será un respaldo al personal de administradores de infraestructura de TIC´s, dentro de los procesos y procedimientos de aseguramiento e investigación de los incidentes informáticos, donde puede hacer uso de herramientas adecuadas en la obtención de información amplia y necesaria sobre el incidente presentado y las acciones a seguir en la protección de la información o hasta presentar las pruebas ante un estrado judicial llegado el caso, el diseño, montaje y configuración de un CSIRT tiene el firme propósito en una empresa o institución prepararse frente a los avances tecnológicos, la mutación y evolución de delitos, la investigación de estos que afectan su infraestructura informática y la ciberseguridad.

La población directamente beneficiada por el DISEÑO TÉCNICO, CONFIGURACIÓN BÁSICA Y CREACION DEL CSIRT EN CIBERSECURITY DE COLOMBIA LTDA, es el personal de administradores de infraestructura de TIC´s, las empresas y/o instituciones que realizan el aseguramiento, la prevención, la investigación de incidentes informáticos y aportación de pruebas ante estrados judiciales dentro de un posible proceso penal.

Después de una revisión realizada, se ha validado la ausencia de referentes documentales que aporten significativamente al desarrollo de actividades propias de un CSIRT en Colombia su creación y configuración, se ha revisado en el portal del MINTIC y no se encontró documento alguno o una guía que demuestre el paso a paso técnico o general para la creación del CSIRT, se ha podido evidenciar la existencia de un CSIRT nacional en el portal de colCERT hallándose la creación del

mismo pero a nivel gerencial e intersectorial pero no un documento que guie a nivel administrativo y técnico su formación y configuración básica, así como los servicios que debe prestar; en pro de solucionar en algo esta falencia y carencia de aspectos técnicos se realiza el presente proyecto con el objeto de disminuir márgenes de errores y tiempo en la realización de esta tarea convirtiéndose en una experiencia simulada mediante la virtualización de equipos que soporten las herramientas principales.

Una condición innovadora es la de soportar la transferencia de conocimientos aprendidos, ligados a los desafíos siempre impuestos por el desarrollo y los avances tecnológicos y su transversalidad en el funcionamiento de las instituciones y las empresas dentro de un territorio globalizado, permitido y hecho posible mediante el uso y la aplicación de la tecnología, las comunicaciones de datos y la infraestructura evolucionada y que la soporta, bajo este concepto y dentro de esta infraestructura, surge la necesidad de contar con un equipo de respuesta a los incidentes informáticos que se suscitan y a los cuales se les debe hacer frente con procedimientos plenamente definidos e identificados que eliminen cualquier manto de duda al momento de realizarlos y dar respuestas pronta y oportuna a estos.

3. DELIMITACIÓN

Para lograr la realización del presente proyecto se debió acudir a la revisión documental de los estándares internacionales ISO 27000, ISO/IEC 27001, ISO/IEC 27035/2016, ANSI/TIA 568-D, así como la legislación Colombiana Constitución Política de Colombia, Código de procedimiento penal, Ley 1273 de 2009, Código de procedimiento civil, Ley 527 de 1999, Ley 1266 de 2008. Protección de Datos Financieros, Ley 1341 del 30 de Julio de 2009 “Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones- TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones”. Ley 1266 de 2008. Protección de Datos Financieros “Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”.

Ley Estatutaria 1581 de 2012, Protección de datos personales, Por la cual se dictan disposiciones generales para la protección de datos personales, que hacen referencia al objeto de esta investigación.

Esto con el objeto de cumplir con la legislación nacional, los estándares, recomendaciones y mejores prácticas para este tipo de infraestructura y que inicialmente tendrá funcionamiento local (dentro del territorio nacional) en la empresa de CIBERSECURITY DE COLOMBIA LTDA, de acuerdo con las condiciones del proyecto aplicado.

4. OBJETIVOS DEL PROYECTO

4.1 OBJETIVO GENERAL

Realizar el DISEÑO TÉCNICO, CONFIGURACIÓN BÁSICA Y LA CREACION DEL CSIRT al interior de una empresa o institución, en este caso la empresa CIBERSECURITY DE COLOMBIA LTDA.

4.2 OBJETIVOS ESPECÍFICOS

- Identificar cuáles son las herramientas necesarias que deben ser instaladas y configuradas en la realización de las actividades propias frente a la investigación de un incidente informático por parte del equipo del CSIRT al interior de una empresa o institución.
- Analizar los procedimientos, las mejores prácticas y las necesidades técnicas a satisfacer que han sido adoptados en otros países en la creación de un centro de respuesta a incidentes informáticos (CSIRT) que sirva de referente para la creación del formulado en este proyecto.
- Documentar el procedimiento, mejores prácticas y la configuración de las herramientas tecnológicas a nivel técnico que son necesarias para la puesta en funcionamiento del centro de investigación de incidentes informáticos CSIRT.
- Realizar la creación y configuración de un CSIRT con los elementos más básicos que permitan su funcionamiento.

5. MARCO REFERENCIAL

De acuerdo con la documentación hallada y la recolección de datos realizada, experiencias particulares y entrevista realizada a ingeniero que han participado en la creación e implementación de un CSIRT y que en la actualidad laboran en un equipo de respuesta a incidentes; de igual forma alineado de conformidad con lo estipulado en la Agencia Europea de Seguridad de las Redes de la Información (ENISA), la Comisión de la Unión Europea, la Unión Internacional de Telecomunicaciones (UIT), o la OTAN, que apuntan a la creación de organizaciones altamente especializadas, diseñadas con el fin de garantizar la seguridad de los sistemas y redes de información de una nación de los que depende el correcto funcionamiento de la propia sociedad, también se realizó una referenciación con el CSIRT de Policía Nacional de Colombia para el entendimiento de los procesos y procedimientos básicos, que permitan ser encaminados a la prestación de servicios proactivos de primer nivel.

Se referenció la guía de “Buenas Prácticas para establecer un CSIRT nacional”, creado por la Organización de Estados Americanos (OEA) emitida en el mes de abril de 2016.

De igual forma se realizó referenciación en el documento emitido por el Centro Criptológico Nacional, 2011 bajo el título de GUÍA DE SEGURIDAD (CCN-STIC-810) GUÍA DE CREACIÓN DE UN CERT / CSIRT.

5.1. MARCO CONCEPTUAL

5.1.1 CSIRT

Con el objeto de tener claridad sobre que es en sí un CSIRT, debemos tener presente que sus siglas hacen alusión a un equipo de respuesta frente a Incidentes de Seguridad Informática; dado entonces que es un grupo conformado, capacitado, idóneo, con los equipos, con las herramientas y aplicaciones necesaria para atender este tipo de emergencias a nivel tecnológico.

5.1.2 Orígenes (Estado de arte)

A raíz del incidente acaecido en 1988 a causa del gusano “Morris”, creado por el estudiante de Harvard, Robert Tappan Morris, de 23 años, y que se estima afectó a casi el 10% de los sistemas conectados a **ARPANET**, el antecesor de la actual Internet. El gusano usaba un defecto del sistema operativo Unix para reproducirse hasta bloquear el equipo de cómputo, estimando un costo de 15 millones de dólares para entonces. Este incidente puso de manifiesto la necesidad de coordinar el trabajo de administradores de sistemas y de gestores TIC de una manera ágil y eficiente, a partir de estructuras organizativas que no tuvieran sólo en cuenta los propios sistemas conectados a Internet[1]. (CENTRO CRIPTOLOGICO NACIONAL, 2011).

5.1.3 ¿Qué hay en un nombre? CSIRT

Hay muchas abreviaturas que se han utilizado como base para los nombres de los equipos, así como para caracterizar qué papel tiene el equipo. Por ejemplo;

IRT = Equipo de respuesta a incidentes
IRC = Capacidad de respuesta a incidentes
IHT = Equipo de manejo de incidentes
IMT = Equipo de gestión / gestión de incidentes
Cada una de las anteriores abreviaturas se ha utilizado con otras descripciones, como "Red", "Computadora", "Seguridad", "Seguridad informática" o "Tecnología de la información". Así que escribiremos algunos ejemplos de nombres o títulos.

CSIRT = Equipo de respuesta a incidentes de seguridad informática
CIRT = Equipo de respuesta a incidentes informáticos

[1] CENTRO CRIPTOLOGICO NACIONAL. Guía de seguridad (CCN-STIC-810). Guía de creación de un CERT / CSIRT. Madrid España: ENS, 2011. p.9.

CIRC = Centro o capacidad de respuesta a incidentes informáticos
SIRT = Equipo de respuesta a incidentes de seguridad
SERT = Equipo de respuesta a emergencias de seguridad

Además, el servicio marcado "CERT" (en referencia al Centro de Coordinación CERT), ha sido utilizado en combinación con otras letras por una variedad de otros equipos para caracterizar su equipo específico y construir sobre una marca bien establecida. Sin embargo, como ya se mencionó, aunque los nombres pueden ser similares, los servicios ofrecidos, las tarifas y los niveles de soporte disponibles pueden ser bastante diferentes.

La similitud en los nombres tampoco significa ningún respaldo o relación entre los equipos.

La variedad de nombres utilizados por los equipos a veces dificulta que los usuarios comprendan cuál es la posición de un equipo o cómo se comparan con otros equipos para que el usuario los pueda conocer.

5.1.4 Objetivos de un CSIRT

Su principal objetivo por alcanzar con la creación y configuración de un CSIRT es la investigación y gestión de incidentes que afectan la seguridad de la información, además contar con un enfoque estructurado y planificado que permita manejar de forma adecuada estos incidentes que se presenten al interior de una empresa y/o institución[2] (James Michael Stewart, 2015).

Estos equipos de respuesta han sido creados para lograr la mitigación, la atención y dar respuesta frente a las amenazas de la red, especialmente la Internet, realizar la investigación de incidentes, recolección de pruebas y presentarlas ante instancias judiciales cuando prestan servicios de informática forense; pueden incluso dedicar personal a la capacitación de clientes sobre amenazas que existen en el ciberespacio como parte del servicio[3] (CHRIS PROSISE, 2003).
Estos profesionales actualizan al usuario frente a modalidades, amenazas, riesgos, novedades a nivel de software y hardware junto con sus vulnerabilidades; de igual forma informan sobre malware y código malicioso y virus que aprovechan este tipo de vulnerabilidades presentes… así los clientes que son atendidos pueden realizar

[2] Certified Information Systems Security Professional Study Guide, Seventh Edition, CISSP 7°, James Michael Stewart, Mike Chapple, Darril Gibson. Indianápolis, Indiana New York United States. Septiembre 10 2015. p. 742.

[3] INCIDENT RESPONSE & COMPUTER FORENSICS. Second Edition. Introduction to the Incident Response Process. CHRIS PROSISE, KEVIN MANDIA, Matt Pepe. McGraw-Hill Companies, Inc. San Francisco, New York Chicago United States of América. Enero 20 2003. p. 11

las actualizaciones acertadamente con los paquetes de software requeridos y los orientan sobre las técnicas que usan los delincuentes informáticos.

5.1.5 El CSIRT y sus ventajas

Contar con un equipo propio de respuesta a incidentes informáticos de primera mano y con dedicación completa a mantener la seguridad de las TIC´s al interior de cualquier empresa y/o comercial con prestación de servicios a terceros que permiten la mitigación de incidentes y evitan las perdidas graves de los activos de información de las organizaciones, protegiendo de esta forma su patrimonio, entendiendo que la perdida, supresión, alteración de la información genera graves consecuencias a las empresas.

Otras posibles ventajas de contar con un CSIRT de acuerdo con el ENISA son:

- ✓ Disponer de una coordinación centralizada para las cuestiones relacionadas con la seguridad de las TI dentro de la organización (punto de contacto).
- ✓ Reaccionar a los incidentes relacionados con las TI y tratarlos de un modo centralizado y especializado.
- ✓ Tener al alcance de la mano los conocimientos técnicos necesarios para apoyar y asistir a los usuarios que necesitan recuperarse rápidamente de algún incidente de seguridad.
- ✓ Tratar las cuestiones jurídicas y proteger las pruebas en caso de pleito.
- ✓ Realizar un seguimiento de los progresos conseguidos en el ámbito de la seguridad.
- ✓ Fomentar la cooperación en la seguridad de las TI entre los clientes del grupo atendido (sensibilización)[4]. (Agencia Europea de Seguridad de las Redes y de la Información ENISA, 2006).

5.1.6 Diferentes tipos de CSIRT

Cuando se pone en marcha un CSIRT es muy importante, como con cualquier otro negocio, formarse una idea clara de quiénes forman su grupo de clientes y a qué tipo de entorno se enfocarán los servicios que se presten. Actualmente son distinguidos los «sectores» siguientes:

- ✓ CSIRT del sector académico
- ✓ CSIRT comercial
- ✓ CSIRT del sector de la protección de la información vital y de la información y las infraestructuras vitales (CIP/CIIP)

[4] Agencia Europea de Seguridad de las Redes y de la Información. Como Crear un CSIRT paso a paso. Producto WP2006/5.1 (CERT-D1/D2). Heraklion, Creta: ENISA, 2006. p. 7.

- ✓ CSIRT del sector público
- ✓ CSIRT interno
- ✓ CSIRT del sector militar
- ✓ CSIRT nacional
- ✓ CSIRT del sector de la pequeña y mediana empresa (PYME)
- ✓ CSIRT de soporte

5.1.7 Tipo de servicios según el CSIRT creado

Muchos son los servicios prestados por los equipos de respuesta (CSIRT), sin embrago, de los existentes es imposible certificar que los presta todos, esto en razón a que cada equipo formado al interior de las empresas, o como particulares dedicados a brindar este tipo de soluciones frente a la problemática que suponen las brechas de seguridad en la red y la infraestructura tecnológica se deben adaptar, quiere decir entonces que son customizables, estos son hechos a la medida, además supone que la falta de recursos es una limitante bastante compleja al momento de la decisión; requiere infraestructura propia en equipos de conectividad, servidores, aplicaciones como herramientas informáticas, el espacio adecuado y la seguridad de este. Además, el personal debe ser capacitado, certificado y con amplia experiencia en este tipo de actividades; entonces los servicios no son completos, el solo hecho de incluir servicios de informática forense ya aumenta considerablemente el presupuesto, las herramientas forenses en las que los tribunales confían son costosas y las OpenSource en los tribunales no son aceptadas al 100%.

Tabla 1. Servicios **de los CSIRT del CERT/CC**

Servicios reactivos	Servicios proactivos	Manejo de instancias
Alertas y advertencias	Comunicados	Análisis de instancias
Tratamiento de Incidentes	Observatorio de tecnología	Respuesta a las instancias
Análisis de incidentes	Evaluaciones o auditorías de la seguridad	Coordinación de la respuesta

Fuente: Como crear un CSIRT paso a paso, Producto WP2006/5.1 (CERT-D1/D2), ENISA. Henk Bronk, CERT/CC, mayo de 2020.

Tabla 1. (Continuación)

Servicios reactivos	Servicios proactivos	Manejo de instancias
Apoyo a la respuesta a incidentes	Configuración y mantenimiento de la seguridad	Configuración y mantenimiento de la seguridad
Coordinación de la respuesta a incidentes	Desarrollo de herramientas de seguridad	Análisis de riesgos
Respuesta a incidentes in situ	Servicios de detección de intrusos	Continuidad del negocio y recuperación tras un desastre
Tratamiento de la vulnerabilidad	Difusión de información relacionada con la seguridad	Consultoría de seguridad
Análisis de la vulnerabilidad		Sensibilización
Respuesta a la Vulnerabilidad		Educación / Formación
Coordinación de la respuesta a la vulnerabilidad		Evaluación o certificación de productos

Fuente: Como crear un CSIRT paso a paso, Producto WP2006/5.1 (CERT-D1/D2), ENISA. Henk Bronk, CERT/CC, mayo de 2020.

5.1.8 Servicios Básicos

Estos se encuentran en dos grupos a saber: los orientados a sensibilizar a los usuarios y/o clientes, realizar capacitación para alertarlos frente a las amenazas de la red y los deberes frente a la seguridad de la información (datos), siendo por consiguiente estos los proactivos.

Por otro lado, se encuentran los orientados a tratar incidentes e intentar mitigar el daño ocasionado en la infraestructura y/o la información (datos).
Como se ha podido observar no se incluyen aquellos de investigación y presentación de pruebas ante estrados judiciales, no prestan servicios de informática forense, que es el común de estos equipos.

5.1.9 Manejo de Instancias

El **manejo de instancias** incluye el análisis de cualquier fichero u objeto encontrado en un sistema que pueda intervenir en acciones maliciosas, como restos de virus, gusanos, secuencias de comandos, troyanos, etc. También incluye el tratamiento y la difusión de la información resultante entre los proveedores y otros interesados, con el fin de evitar que el software malicioso se siga extendiendo y mitigar los riesgos.

5.1.10 Gestión de Seguridad y Calidad

En la gestión de seguridad y calidad de esta**,** se trazan objetivos en el tiempo, (el plazo es mayor), la consultoría hace parte de estos equipos (CSIRT) de igual forma proyectan e incluyen programas educativos como una de las medidas, que permita su evolución y trascendencia.

5.1.11 Definición de Servicios Iniciales en el CSIRT

5.1.12 Modelo de Costos

Se ha definido la forma y horario en que se prestara inicialmente los servicios de respuesta e investigación a incidentes informáticos por el equipo, laborando y atendiendo en horas de oficina, con acceso remoto al grupo de herramientas con las que cuenta para atender este tipo de incidentes y movilidad por parte de cada miembro del equipo.
De igual forma fuera del horario de oficina se contratará personal que este alerta y preste los servicios de operador y vigilancia, en este horario se prestaran servicios clasificados, aplicaran para casos de incidentes y/o cuando se materialice un riesgo de tipo medioambiental (Desastres Naturales).

5.1.13 Modelo de ingresos

Se ha definido para la subsistencia y continuidad del equipo conformado, a la investigación de incidentes en infraestructuras tecnológicas, presupuestalmente se ha tomado la decisión de realizarlo con los recursos existentes, tanto en equipos

como con el personal que se encuentre capacitado en las áreas concernientes a las TIC´s y que apliquen por sus conocimientos en el equipo de trabajo.

5.1.14 Uso de los recursos existentes

De acuerdo con la necesidad que tiene la empresa CIBERSECURITY DE COLOMBIA LTDA de realizar la creación del CSIRT, y partiendo del hecho que esta empresa se encuentra constituida y en ella existe un departamento de TI y personal que administra la infraestructura y brinda el soporte técnico a su clientes internos y externos, se usaran recursos de hardware y recursos humanos que existen en esta empresa para implementar el equipo de respuesta de investigación de incidentes informáticos.

5.1.15 Aportes por suscripción de soporte y contención

Una vez alcanzada cierta madurez y estabilidad, se brindarán estos servicios de soporte técnico e investigación de incidentes informáticos a personal y empresas externas mediante aportes por suscripción con un periodo anual que permita dar continuidad a nuestro CSIRT.

5.1.2.1 Definición de la estructura organizacional

Como en cualquier empresa tener una estructura organizada y con la jerarquía acertada para el funcionamiento del CSIRT, va a depender en gran medida a como se ha estructurado la organización que presta servicios y/o vende productos siendo el caso o si su enfoque es único a la atención de clientes de tecnología y que grupo pertenece los clientes que atenderá, la contratación referente a los expertos que se necesiten, será enfocada a la necesidad de empresa a atender y a satisfacer sus condiciones particulares; teniendo en cuenta estos aspectos, se enumera una organización típica recomendada.

5.1.2.2 Estructura y funciones del CSIRT

Dirección General

Director General

Personal de Asesoría y Administrativa

Director Oficina Administrativa
Contador

Asesor en TIC’s
Asesor Legal y Jurídico

Grupo operativo y técnico de soporte

Jefe del equipo técnico
Técnicos del Equipo (CSIRT), atienden los servicios requeridos por sus clientes.
Investigadores, quienes tienen el reto de hallar el origen del incidente.

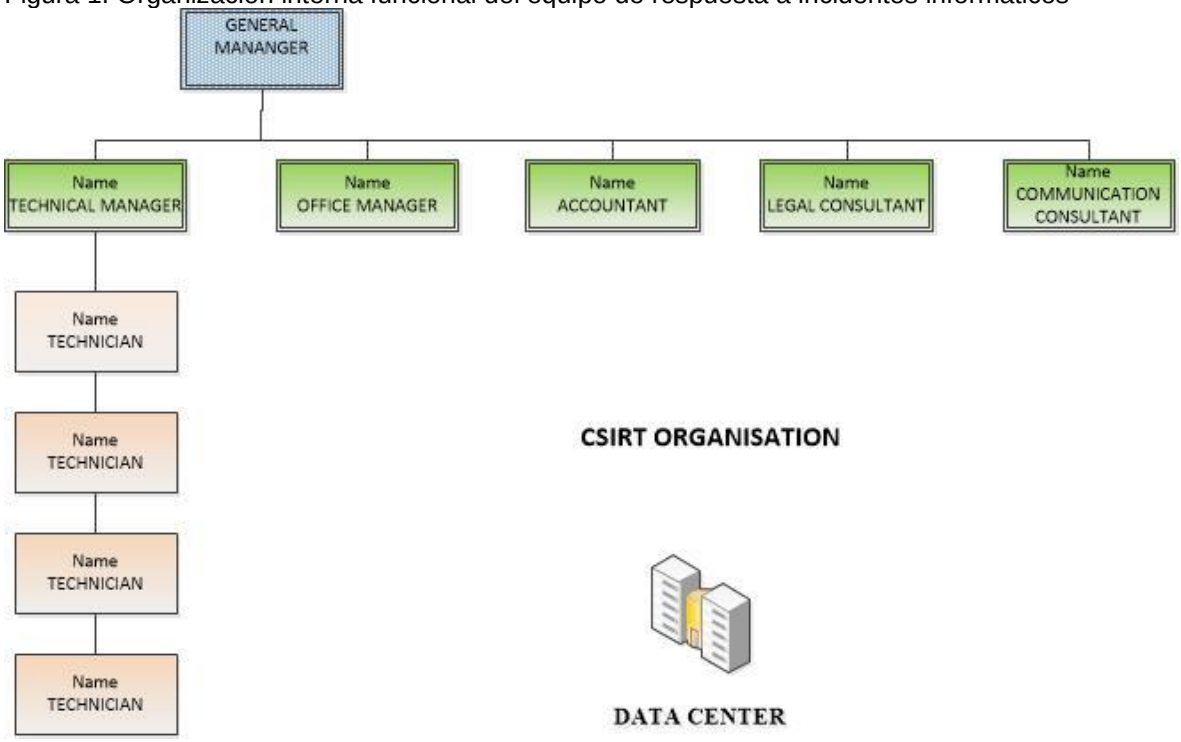
Personal externo de consultorías.

El personal para contratar debe tener un perfil específico para el equipo de respuesta a incidentes informáticos y a quienes se atienden.

5.1.2.3 Diagrama del modelo organizacional de la empresa.

A continuación, se muestra, como en cualquier empresa la estructura organizacional del CSIRT propuesto a manera de ejemplo de lo mínimo que debe contener frente a la respuesta y satisfacción de la necesidad de sus clientes.

Figura 1. Organización interna funcional del equipo de respuesta a incidentes informáticos



Fuente: Software de diseño Visio demo 30 días, Omar Tique M., mayo de 2020

5.1.2.4 Personal calificado y capacitado

El jefe del CSIRT debe tener experiencia en seguridad y apoyo de primer y segundo nivel y ha de haber trabajado en el ámbito de la gestión de crisis. Los otros tres miembros del equipo son especialistas en seguridad. Los miembros del equipo procedentes del departamento de TI que intervienen a tiempo parcial son especialistas en su parte de la infraestructura de la empresa.

Es de tener en cuenta el perfil ocupacional de quien será el encargado de liderar el equipo, de ser idóneo, capacitado y contar con la experiencia necesaria para orientar y que lidere actividades de primer y segundo nivel cuando se necesite brindar soporte y tomar decisiones, saber tomar decisiones bajo incertidumbre, manejo de inteligencia emocional, gestionando adecuadamente una crisis, para los demás profesionales es aplicable la especialización; todo ello enfocado al manejo de seguridad Informática y seguridad de la información.

5.1.2.5 Uso, equipos, oficina, y equipo de respuesta

Hace referencia al sitio o lugar donde va a ser instalados los equipos y donde funcionará la oficina desde donde se atenderá a los clientes internos y externos y en el cual se deberá tener en cuenta las siguientes consideraciones de seguridad tales como: control de acceso, seguridad perimetral, sistema de CCTV, sistemas de detección, control y extensión de incendios, etc.

5.1.2.6 Adecuación del sitio o instalaciones físicas

En razón a que los activos de negocio para el CSIRT es la información y los datos, siendo estos a su vez bastante delicada, se hace necesario que el equipo de respuesta a incidentes informáticos asuma el control de la seguridad física a las áreas de su oficina e instalaciones, teniendo de presente la viabilidad de hacerlo o no.

Dentro de la implementación de las políticas de seguridad y control de acceso a la información se ha de tener presente los siguientes aspectos.

5.1.2.7 Controles generales concernientes a las instalaciones.

Debe hacerse y validarse la seguridad física de las instalaciones de la empresa o institución en donde se cumple con las políticas y recomendaciones dadas; se

instaura una sala de crisis y monitoreo de los sistemas que integran la empresa y con las que se permiten hacer seguimiento permanente a la infraestructura tecnológica a través del componente de la seguridad perimetral.

Se ha de realizar la adquisición de una caja fuerte para resguardar la documentación de alto valor, material de encriptación, credenciales de usuarios y equipos de altos privilegios. Se ha configurado y adquirido una línea telefónica de exclusividad a la atención de clientes y con la posibilidad de realizar llamadas a móviles y la realización de teleconferencias.

5.1.2.8 Controles y políticas referidas a los equipos de TI

Se tiene en cuenta en primera línea las recomendaciones consignadas en los estándares de la ISO/IEC 27000, ISO/IEC 27001 e ISO/IEC 27035

5.1.2.9 Mantenimiento de canales de comunicaciones.

Generar canales de comunicación efectiva entre el equipo CSIRT a nivel organizacional y los clientes a quienes prestan sus servicios, siendo estos externos a su organización y brindad soporte técnico frente a incidentes informáticos.

5.1.2.10 Sistemas localización de registros.

Crear una aplicación integrada a una base de datos que permita realizar el registro y la consulta de usuarios externos a quienes se presta el servicio de soporte ante la ocurrencia de cualquier incidente de tipo informático.

5.1.2.11 Uso corporativo de nombre “marca”

En este caso usando el nombre de nuestra empresa es posible usar el nombre CSCL-CERT (CIBERSECURITY DE COLOMBIA LTDA)

5.1.2.12 Minimización de riesgos otras consideraciones.

Al interior de la empresa, organización o institución, respecto al componente de infraestructura tecnológica, en sus componentes de hardware, software y aplicaciones se debe evaluar que acciones son viables aplicar para la minimización de los riesgos tales como eliminación del riesgo, minimización del riesgo o transferir

el riesgo a un tercero, es de tenerse en cuenta, además evaluar cuales son susceptibles de trasferir o no y que debe ser asumidos por la propia empresa.

5.2 MARCO TEÓRICO

"Un equipo de respuesta a incidentes en seguridad informática (CSIRT por sus siglas en inglés) es una organización cuyo propósito principal consiste en brindar servicios de respuesta a incidentes de seguridad informática a una comunidad en particular"[5].

Basado en la definición, la funcionalidad de un equipo de respuesta a incidentes de tipo informático, los aspectos de tipo procedimental y los procesos que son implementados al interior, y la concepción del mismo desde su aspecto teórico y filosófico en el que apunta a la prevención, el monitoreo, el seguimiento y la investigación de cualquier incidente de tipo informático que pueda presentarse al interior de una empresa en el componente y/o infraestructura tecnológica a nivel lógico, cuya razón de su existencia es la protección de la información y de los datos como el activo más importante en la funcionalidad de cualquier empresa.

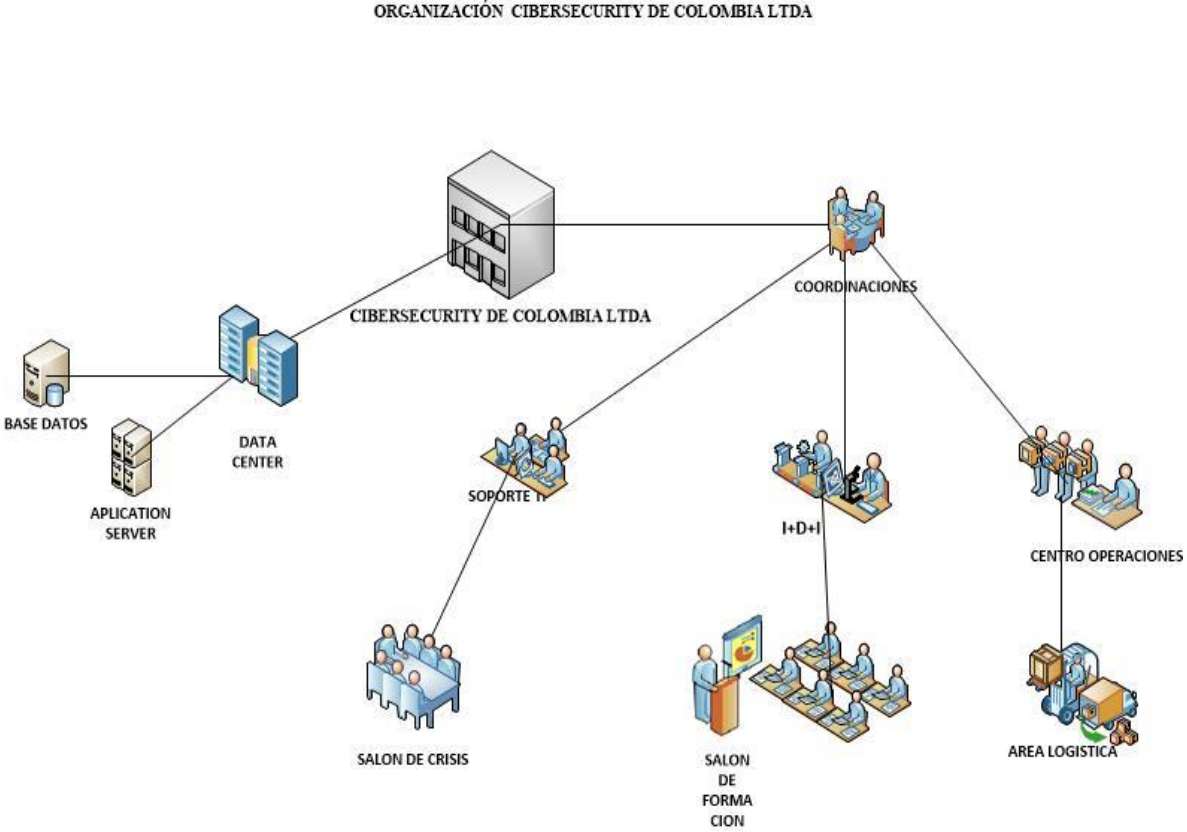
Se ha decidido realizar la creación del **CSIRT** EN **CIBERSECURITY DE COLOMBIA LTDA,** el cual tendrá la organización que se relaciona a continuación y puede observarse en la figura siguiente, de igual forma la organización de grupos con el personal administrativo y de soporte.

De igual forma se atenderá teóricamente los aspectos relevantes tales como la naturaleza y el objetivo que tiene un CSIRT, la comunidad que será su objetivo y a la cual atenderá, teniendo en cuenta (sector gobierno, sector privado o ambos grupos), se definirá la misión y la visión del equipo creado y acogerá un marco legal que permita ajustar las actuaciones conforme a las leyes y los reglamentos regionales y estándares internacionales y mejores prácticas en los procesos y procedimientos.

5.2.1 ORGANIGRAMA DEL CSIRT PROPUESTO

[5] Organización de los Estados Americanos OEA, Buenas prácticas para establecer un CSIRT nacional. 1889 F Street, N.W., Washington, D.C., 2006, U.S.A. 20 Abril 2016. p. www.oas.org/cyber/

Figura 2. Organización Cybersecurity de Colombia LTDA para *el CSIRT.*



Fuente: Software diseño gráfico diagrama de red, Omar Tique M., mayo de 2020.

5.2.2 Centro de Datos (Data Center)

Contará con un lugar físico donde se aloja la infraestructura de tecnología de la información, tales como racks, en el cual se alojarán los equipos servidores, equipos activos de red (routers, switchs, firewalls, planta telefónica, etc.), será el centro de operaciones del componente tecnológico de nuestro CSIRT y de la organización y/o empresa.

5.2.3 I+D+i.

Se ubicará una oficina con el talento humano necesario para el componente de **Investigación, desarrollo e innovación** dentro de nuestra organización, específicamente para hacer frente a los desafíos de nuevas tecnologías emergentes y modalidades del crimen, adaptando este un nuevo concepto a los estudios relacionados con el avance tecnológico e investigativo centrados en el avance de la sociedad, siendo una de las partes más importantes dentro de las tecnologías informáticas.

5.2.4 Centro de Operaciones

Es el lugar donde converge toda la solución tecnológica de un CSIRT, en si es la plataforma de las capacidades de respuesta frente a la investigación y contención de incidentes; en este se cuenta con un portal de informes, la detección de amenazas, la monitorización de la infraestructura tecnológica, la recolección de evidencias para ser analizadas y aportadas en un proceso judicial, la clasificación, la correlación, la investigación, el análisis, la notificación y la auditoria.

5.2.5 Soporte TI

Encargados de realizar las coordinaciones de comunicaciones entre el coordinador de incidentes, el resto del grupo de TI; es igualmente quien debe contactar al personal responsable de cada una de las aplicaciones que funcionan en una empresa u organización, esto en razón a que es posible que no tenga el conocimiento especifico y las configuraciones de cada una de estas aplicaciones informáticas internas o en el caso de las demás empresas que son sus clientes.

5.2.6 Coordinaciones

Conformado por el coordinador del equipo CSIRT quien es el responsable de las actividades del Grupo CSIRT y estará encargado de coordinar las revisiones de sus acciones, las cuales no siempre serán las mismas; de otra parte se encuentra el coordinador de incidentes, el cual será el responsable de coordinar la respuesta, este será el propietario del incidentes o en su defecto del conjunto de incidentes los cuales le hayan sido asignados, será el encargado de cualquier tipo de comunicación que haga referencia al incidente que se le ha asignado y representara a todo el grupo, solo el conoce la información y es el autorizado para divulgar cualquier comunicado referido al o los incidentes presentados y asignados[6]. (Zajicek, 2003).

5.2.7 Área Logística

Es la encargada de la dotación de equipos y tecnología para el funcionamiento del CSIRT, así como la proyección de nuevas adquisiciones, mobiliario, transporte, etc., en representación del funcionamiento y desempeño eficaz del grupo.

---

[6] Zajicek, Moira J. West-Brown Don Stikvoort Klaus-Peter Kossakowski Georgia Killcrece Robin Ruefle Mark. Handbook for Computer Security Incident Response Teams (CSIRTs), First release: December 1998 2^{nd} Edition: April 2003. 10 abril 2003. P 27. Disponible en: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305

5.2.8 Salón de Formación

Se designa personal de capacitación o se contrata con expertos sobre las nuevas tendencias tecnológicas y los desafíos que esas nuevas tecnologías supone a corto y largo plazo; de igual se capacita a miembros del grupo CSIRT sobre nuevas áreas o actividades a desarrollar, capacitaciones sobre Ethikal Hacking, Redes, telefonía bajo protocolos IP y SIP, servidores, Cloud, virtualización e hypervisores, técnicas de intrusión, técnicas de ataque, informática forense y algunas de sus herramientas, etc.

5.2.9 Salón de crísis

Lugar donde es posible llevar la visualización y administración de las herramientas con las cuales cuenta el CSIRT, se reúne la totalidad del grupo de expertos y se toma una decisión frente a un incidente de gran magnitud y complejidad que este afectando a toda la organización en sus procesos más críticos, sobre infraestructuras críticas, sistema bancario, sector salud y ciberdefensa, incidentes en los cuales se hace necesario la toma de decisiones frente a posible afectaciones de este tipo y que puede generar consecuencias desastrosas.

5.3 MARCO LEGAL

La siguiente es la normatividad aplicada a los medios informáticos, procedimientos y aspectos que regulan la interacción del ser humano con la tecnología, hoy día sociedad de la información y sus aspectos que la rigen y es extensiva a las dimensiones del actuar humano.

5.3.1 Constitución Política de Colombia

Constitución Política de 1991, el texto del artículo 15, modificado por el Acto Legislativo 2/2003 declarado inexequible mediante sentencia C-816 de 2004 Corte Constitucional “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo

pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley[7]. (Asamblea Nacional Constituyente , 1991).

Artículo 20, que expresa: "Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación"[8]. (Asamblea nacional Constituyente, 1991)

Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.

Artículo 61, que expresa: "El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley"[9]. (1991, 1991).

5.3.2 Ley 1341 del 30 de Julio de 2009

"Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones- TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones".

5.3.3 Ley 1266 de 2008. Protección de Datos Financieros

Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

5.3.4 Ley Estatutaria 1581 de 2012, Protección de datos personales.

Por la cual se dictan disposiciones generales para la protección de datos personales, y reglamentada parcialmente por el Decreto Nacional 1377 de 2013, Reglamentada Parcialmente por el Decreto 1081 de 2015. De acuerdo con sentencia C-748 de 2011.

---

[7] Asamblea Nacional Constituyente. Constitución Política de Colombia. Bogotá D.C. Colombia: Constituyente. 1991. p.3.

[8] Asamblea Nacional Constituyente. Constitución Política de Colombia. Bogotá D.C. Colombia: Constituyente. 1991. p.3.

[9] Asamblea Nacional Constituyente. Constitución Política de Colombia. Bogotá D.C. Colombia: Constituyente. 1991. p.11.

5.3.5 Ley 1273 DE 2009

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

5.3.6 Directiva (UE) 2016/1148

DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

5.3.7 Estándares

En este caso se ha de tener en cuenta dos aspectos importantes tales como lo es la normalización referente o que rige para el CSIRT y la normalización que es aplicable a las mejores prácticas a la instalación y aseguramiento de la infraestructura y los medios de transmisión de datos.

ISO (la Organización Internacional para la Normalización) e IEC (Comisión Electrotécnica Internacional) forman el sistema especializado de normalización mundial; el estándar norteamericano como lo es la ANSI/TIA con sus recomendaciones y mejores prácticas, referidas a la infraestructura de TI, su aseguramiento y administración.
Los organismos nacionales que son miembros de la ISO o de la IEC participan en el desarrollo de normas internacionales a través de los comités establecidos por la respectiva organización para tratar los campos particulares de la actividad técnica.
Otras organizaciones internacionales, gubernamentales y no gubernamentales, en unión con la ISO e la IEC, también toman parte en el trabajo. En el campo de la tecnología de la información, ISO e IEC han establecido un comité técnico conjunto, el comité ISO/IEC JTC 1.

5.3.8 ISO/IEC 27035 // ISO/IEC 27000/ ISO/IEC 27001-2013 ISO 27002 2014

La ISO/IEC 27035 es una extensión de la serie de normas ISO/IEC 27000 y se centra en la gestión de incidentes de seguridad de la información que se identifica en ISO/IEC 27000 como uno de los factores críticos de éxito para el sistema de gestión de seguridad de la información. (SO/IEC, 2016).

La norma proporciona un enfoque estructurado para:

- Identificar, comunicar y evaluar los incidentes de la seguridad de la información

- Contestar, gestionar los incidentes de la seguridad de la información
- Identificar, examinar y gestionar las vulnerabilidades de seguridad de la información
- Aumentar la mejora de la continuidad de la seguridad de la información y de la gestión de los incidentes, como respuesta a la gestión de incidentes de la seguridad de la información y de las vulnerabilidades[10].

La orientación de la seguridad de la información en (**ISO/IEC-27035-2 Guidelines to plan and prepare for incident response),** se puede aplicar a todas las organizaciones, ya sean pequeñas, medianas o grandes. Además, se da orientación de forma específica para las empresas que presten servicios de gestión de incidentes de seguridad de información[11].

5.3.9 ISO/IEC 27035-2

Esta constituye un proceso con cinco etapas que son claves:

- Preparase para enfrentarse a los incidentes.
- Reconocer los incidentes de seguridad de la información.
- Examinar los incidentes y tomar las decisiones sobre la forma en que se han llevado a cabo las cosas.
- Dar respuesta a los incidentes, lo que quiere decir, investigarlos y resolverlos.
- Aprender de las lecciones[12]. (Excellence, 2014.

5.3.10 ISO/IEC 27000-2018

Information Technology — Security techniques — Information security management systems — Overview and vocabulary. Establece una implementación efectiva de la seguridad de la información empresarial; Un sistema de administración de seguridad de la información consiste en las políticas, procedimientos, pautas, recursos y actividades asociados, administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información. Un sistema de gestión de seguridad de la información es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y

[10] ISO/IEC 27035-1:2016. Information Technology — Security techniques — Information Security Incident Management — Part 1: Principles of Incident Management. Ginebra Suiza: 2016.

[11] ISO/IEC 27035-1:2016. Information Technology — Security techniques — Information Security Incident Management — Part 1: Principles of Incident Management. Ginebra Suiza: 2016.

[12] ISO/IEC 27035-1:2016. Information Technology — Security techniques — Information security Incident Management — Part 1: Principles of Incident Management. Ginebra Suiza: 2016.

mejorar la seguridad de la información de una organización para lograr los objetivos comerciales[13]. (ISO/IEC , 2018).

5.3.11 ISO/IEC 27001

Estándar de Gestión de la Seguridad de la Información, en la cual se "especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización"[14].

5.3.11.1 Principios

Es la preservación e investigación de los incidentes de seguridad presentados en los sistemas informáticos; investigar sobre la perdida de información a causa de virus, accesos no autorizados, las vulnerabilidades que puede presentar una infraestructura de TI y/o un sistema informático, el robo de información protegida[15] (ISO/IEC_INCONTEC INTERNACIONAL, 2015).

Referido a la infraestructura de tecnologías de la información, se considera tres premisas básicas en cuanto al cableado estructurado para el manejo de las telecomunicaciones en un edificio a saber.

- Los edificios y los sistemas de comunicaciones son dinámicos, durante la vida útil del edificio.
- Los equipos de comunicación y los medios de transmisión cambian dinámicamente.
- Telecomunicaciones es más que voz y datos, telecomunicaciones involucra otros servicios en el edificio como son control ambiental, seguridad, audio, TV, alarmas etc.

---

[13] INTERNATIONAL STANDARD ISO/IEC 27000:2018, Fifth Edition 2018-02. Information Technology — Security techniques — Information security management systems — Overview and vocabulary. Vernier, Geneva, Switzerland. 10 febrero 2018. P 11. Disponible en: https://www.iso.org/standard/73906.html

[14] ISO/IEC 27001:2013/Cor 2:2015. Information Technology-Security techniques-Information security management systems-Requirements-Technical Corrigendum 2. Edition **:** 2. ISO/IEC JTC 1/SC 27 **.** 2013-10. Disponible en: https://www.iso.org/standard/54534.html .

[15] ISO/IEC_INCONTEC INTERNACIONAL. GUÍA TÉCNICA COLOMBIANA GTC ISO/IEC 27002 TECNOLOGÍA DE LA INFORMACIÓN. Bogotá D.C Cundinamarca Colombia, 22 Julio 2015.

Es de gran importancia que estas consideraciones sean tenidas en cuenta durante la implementación del cableado estructurado y fibra óptica en cualquier proyecto de acuerdo con las recomendaciones del estándar ANSI/TIA 568-D.

5.3.13 ANSI/TIA 568.0-D-2015

Este estándar normaliza el Cableado genérico de telecomunicaciones para las instalaciones del cliente "Generic Telecommunications Cabling for Customer Premises". El propósito de esta Norma es permitir la planificación e instalación de un sistema de cableado estructurado para todo tipo de instalaciones del cliente. Esta norma específica un sistema que admitirá cableado de telecomunicaciones genérico en un entorno de múltiples productos y proveedores.

Esta Norma es la base de la infraestructura de cableado para datos y de telecomunicaciones de las instalaciones.

Los requisitos adicionales se detallan en normas específicas para el tipo de local. Por ejemplo, ANSI/TIA-568.1-D, contiene requisitos adicionales aplicables al cableado de edificios comerciales[16] (ANSI/TIA, 2015).

5.3.14 ANSI/TIA 568.1-D-2015

Este estándar normaliza el Estándar de infraestructura de telecomunicaciones de edificios comerciales, "Commercial Building Telecommunications Infrastructure Standard". El propósito de esta Norma es permitir la planificación e instalación de un sistema de cableado estructurado para edificios comerciales. La instalación de sistemas de cableado durante la construcción o renovación de un edificio es significativamente menos costosa y perjudicial que después de la ocupación del edificio.

Esta Norma establece criterios técnicos y de rendimiento para varias configuraciones de sistemas de cableado para acceder y conectar sus respectivos elementos. Para determinar los requisitos de un sistema de cableado genérico, se consideraron los requisitos de rendimiento para varios servicios de telecomunicaciones[17] (ANSI/TIA, 2015).

---

[16] ANSI/TIA. ANSI/TIA-568.0-D-2015, Generic Telecommunications Cabling for Customer Premises. Courthouse Road, Suite 200 Arlington, VA 22201 U.S.A.. 14 septiembre 2015. p 13.

[17] ANSI/TIA. ANSI/TIA-568.1-D Commercial Building Telecommunications Infrastructure Standard. Courthouse Road, Suite 200 Arlington, VA 22201 U.S.A.. 09 SEPTEMBER 2015.

5.3.15 ANSI/TIA 568.2-D-2015

Este estándar normaliza y aplica las recomendaciones en cuanto a las características eléctricas y desempeño que debe tener el cable UTP y cada uno de los accesorios que hacen parte del canal de transmisión de datos, es el estándar internacional de EE.UU y rige para cualquier tipo de infraestructura que hace parte del continente americano y se certifica bajo las premisas allí establecidas, de igual forma aplica para métodos de instalaciones (mejores prácticas) y aplica para la categoría 6ª y categoría 8 que son las últimas versiones para este tipo de medios de transmisión.

De igual forma está contemplado en el estándar los parámetros de desempeño, mejores prácticas, ancho de canal, para todo el componente de fibra óptica cuando esta es usada como medio de transmisión y se hace extensivo a todos sus componentes que intervienen en el canal.

5.3.16 ANSI/TIA 568 3-D-2016

Este estándar normaliza el estándar de Cableado de fibra óptica y sus componentes "Optical Fiber Cabling and Components Standard". El propósito de esta Norma es especificar los requisitos de cableado y componentes para el cableado de fibra óptica de las instalaciones. Está destinado a ser utilizado por fabricantes; sin embargo, los fabricantes, usuarios, diseñadores e instaladores encontrarán útil esta Norma. Además, esta Norma está destinada a ser utilizada como referencia por los conjuntos de normas comunes y normas de cableado de instalaciones enumeradas en el Prólogo. Esta Norma es aplicable al cableado y componentes de fibra óptica de las instalaciones. En este estándar se especifican los requisitos para los componentes (por ejemplo, cable, conectores, hardware de conexión, cables de conexión), conectividad y cableado. Los requisitos de prueba y medición también se incorporan en esta Norma[18] (NSI/TIA, 2016).

5.3.17 ISO/IEC 11801 II Edición y Adenda

Estándar europeo de cableado genérico para sitios de cliente (múltiples normas)

Estas normas internacionales definen el rendimiento mecánico y eléctrico del cableado de telecomunicaciones por una clase de rendimiento (clase C, clase D, clase E, clase EA, clase F y clase FA) y componentes por categoría o rendimiento (es decir, categoría 3, categoría 5, categoría 6, categoría 6ª, categoría 7, categoría 7ª, categoría 8 y categoría 8 II Edición).

[18] NSI/TIA. NSI/TIA-568.3-D-2016, Optical Fiber Cabling and Components Standard. Courthouse Road, Suite 200 Arlington, VA 22201 U.S.A. 25 octubre 2016. p.

5.3.18 Guía técnica GTC-ISO/IEC Colombiana 27035

Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información.

Esta guía es una adopción idéntica (IDT) de la norma ISO/IEC 27035: 2011.

La representación de todos los sectores involucrados en el proceso de Normalización Técnica está garantizada por los Comités Técnicos y el período de Consulta Pública, este último caracterizado por la participación del público en general.

La guía GTC-ISO/IEC 27035 fue ratificada por el Consejo Directivo de 2012-12-12. (INCONTEC, 2012)

Agencia Europea de Seguridad de las Redes de la Información (ENISA), la Comisión de la Unión Europea, la Unión Internacional de Telecomunicaciones (UIT), o la OTAN, -----apuntan a la creación de organizaciones altamente especializadas, diseñadas con el fin de garantizar la seguridad de los sistemas y redes de información de una nación de los que depende el correcto funcionamiento de la propia sociedad[19].

6. MARCO ESPACIAL

De acuerdo con las condiciones del proyecto, la ubicación de la empresa en donde se creará y aplicará el objeto de este estudio, está enmarcado dentro de la empresa CIBERSECURITY DE COLOMBIA LTDA**,** y este se encuentra en el territorio nacional, donde se desarrolla el proyecto.

7. DISEÑO METODOLÓGICO

Para la presente investigación se ha acudido al método de revisión documental, dado a que se tendrá como referente la experiencia, conocimiento y doctrina que pueda ser hallada en diversas fuentes y/o países en materia de la creación, diseño y configuración de equipos de trabajo como respuesta a la investigación de incidentes informáticos.

[19] ISO/IEC 27035-1:2016. Information Technology — Security techniques — Information Security Incident Management — Part 1: Principles of Incident Management. Ginebra Suiza: 2016.

Este ha sido un proyecto aplicado y proyectivo en razón a que el resultado de este estudio es la materialización y la creación y el DISEÑO TÉCNICO Y CONFIGURACIÓN BÁSICA PARA EL FUNCIONAMIENTO DEL CSIRT al interior de una empresa o institución; se ha realizado la instalación y configuración de equipo servidor y se ha virtualizado las maquinas necesarias que aloja las herramientas básicas.

De igual forma es del tipo analítica, teniendo en cuenta que para desarrollar el presente proyecto se debió efectuar la consulta y el análisis de la literatura a nivel teórico y técnico-practico (documentos, guías, manuales, legislación y posible doctrina aplicada en otros países) que se encontró en los diversos medios referentes al tema objeto del presente proyecto; en este caso se realiza la instalación y configuración de sistemas operativos, herramientas, aplicaciones y se ha seguido la ruta técnica hallada para la configuración y puesta en funcionamiento de las herramientas del CSIRT.

La selección de las herramientas metodológicas, la aplicación de estas en la consecución de información, referenciación, posibles experiencias de terceros, la selección de herramientas técnicas y tecnológicas, así como la instalación y configuración de sistemas operativos y aplicaciones necesarias en la creación y puesta en funcionamiento del CSIRT propuesto, y la población que atenderá.

7.1 Entrevista

Se realiza entrevista a personal de ingenieros que integran o hayan hecho parte de un grupo de respuesta a incidentes informáticos, (CSIRT) en nuestro país con el fin de conocer de cerca cuales son las herramientas informáticas que deben ser incluidas y la posibilidad de configurarlas usando tecnologías Open Source.

7.2 Revisión Documental

Para el desarrollo del presente proyecto se acudió al método de revisión documental de tipo teórico y práctico a nivel técnico, dado que se tendrá como referente la doctrina existente en otros países en materia de la creación, implementación y configuración de las herramientas tecnológicas (servidores de correo, DNS, herramientas de seguridad perimetral, etc.), necesarias en un CSIRT para la investigación de incidentes informáticos.

7.3 Población

La realización del presente trabajo aplicado va dirigido a la satisfacción de las necesidades que tiene el personal de ingenieros administradores de infraestructura tecnológicas y de las telecomunicaciones de conocer cómo se realiza la

configuración básica de un CSIRT o equipo de respuesta a incidentes informáticos al interior de una empresa o mediante la modalidad de prestación de servicios a terceros en los aspectos técnicos.

7.4 Diseño del trabajo aplicado

7.4.1 Método de Enfoque Cualitativo.

Se ha aplicado el método cualitativo por perseguir la finalidad de satisfacer una necesidad real, en donde a través de consultar documentos, guías, manuales y doctrina aplicada en otros países a nivel teórico y práctico, referente al componente técnico, ha posibilitado la configuración del CSIRT propuesto en el presente proceso, con las herramientas más básicas a ser usadas.

7.5 Fuentes de obtención de la información

7.5.1 Fuentes primarias

Entrevista realizada a ingenieros especialista en seguridad informática y Magister en seguridad informática.

7.5.2 Fuentes secundarias

Se ha recurrido a las fuentes informativas disponibles en los sitios web (cibergrafía), de las organizaciones que estandarizan los procesos, que han implementado este tipo de infraestructura y equipos de trabajo para hacer frente a la delincuencia, presente en el ciberespacio.

8 DESARROLLO DE LOS OBJETIVOS

Para alcanzar el objetivo propuesto en el presente proyecto y el cual consiste en el "**DISEÑO TÉCNICO, CONFIGURACIÓN BÁSICA Y CREACION DEL CSIRT EN CIBERSECURITY DE COLOMBIA LTDA"**., y el cual se ha logrado realizar e implementar para la prevención y la investigación de incidentes de seguridad de tipo informático.

Ha sido necesario la realización de las actividades descritas en cada uno de los siguientes acápites o ítems y que consisten en una serie de investigaciones, aclaración de conceptos, procesos, y procedimientos, siendo estos a nivel lógico y físico que permiten la integración de componentes, infraestructura, herramientas y

aplicaciones orientadas al uso con sus particularidades al interior de cualquier equipo de respuesta e investigación de incidentes de tipo informático CSIRT.

8.1 Herramientas necesarias en un CSIRT

8.1.1 Aspectos técnicos

Teniendo en cuenta el tipo de proyecto y el desarrollo del mismo, en aras de alcanzar los objetivos propuestos a nivel técnico e implementación de la infraestructura planteada, además de los personales como es la adquisición del título, se hace necesario tener presente los aspectos técnicos necesarios en la implementación, y de que tipo específico serán estos orientados a que realmente funcione lo que se ha proyectado adquirir, instalar, configurar y poner finalmente en funcionamiento, definiendo entonces los aspectos descritos a continuación:

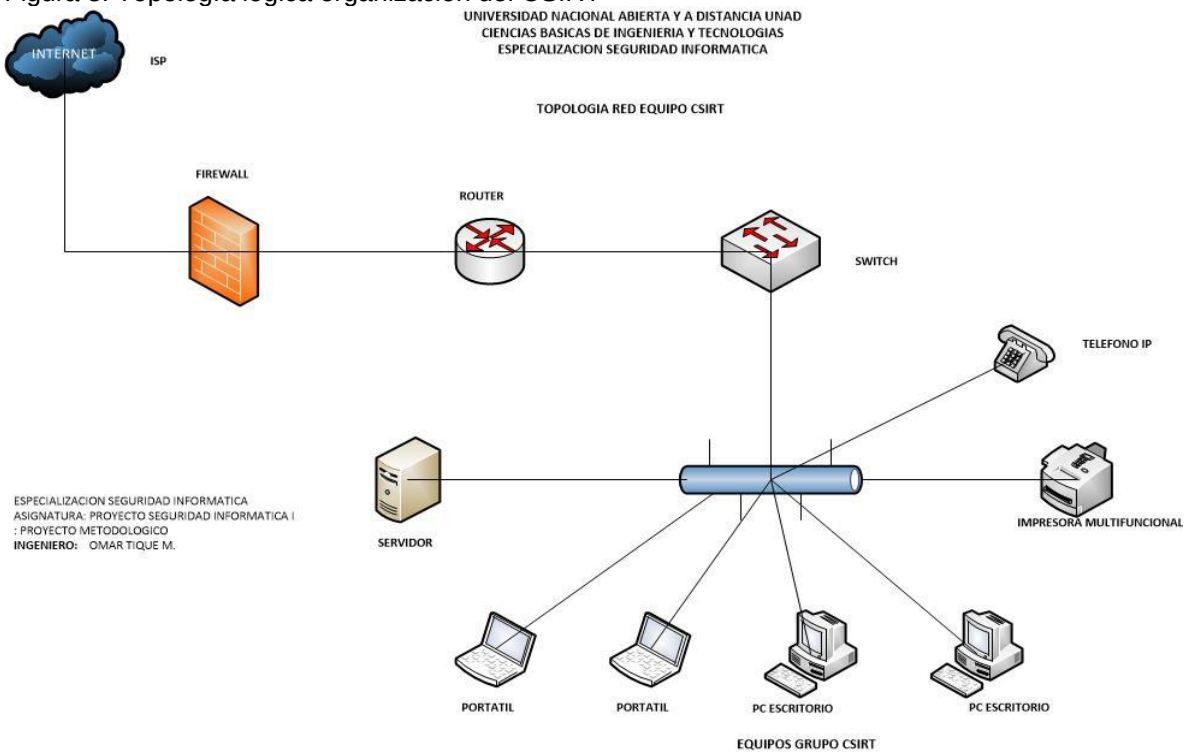
8.1.2 Topología, infraestructura y equipos

Para alcanzar el objetivo propuesto se hace necesario la adquisición, instalación y configuración y puesta en funcionamiento de la siguiente infraestructura tecnológica a nivel físico y lógico (Hardware-software) así como la configuración e integración de aplicaciones que permitan el funcionamiento y la disponibilidad de las herramientas tecnológicas que necesitan frente a la respuesta e investigación de intrusiones, la explotación de una vulnerabilidad informáticas para realizar actividades pertinentes cuando se presenten este tipo de eventos; con el objeto de cumplir con la tarea se hace necesaria la creación de una red LAN que permita la comunicación interna del equipo de respuesta a los incidentes informáticos y el uso de las herramientas necesarias para ello, de tal forma se usó el siguiente diagrama de red para validar su jerarquía.

8.1.3 Topología de Red en el CSIRT Propuesto

A continuación, se presenta la topología a nivel lógico la estructuración de integración del CSIRT propuesto.

Figura 3. Topología lógica organización del CSIRT



Fuente: Software de diseño Visio demo 30 días, Omar Tique M., mayo de 2020

En la configuración de la topología y adquisición de hardware y configuración de equipos se ha tenido en cuenta las consideraciones emitidas por el estándar de seguridad de la información la ISO/IEC 27001 para garantizar disponibilidad, seguridad y confidencialidad de la información (datos).

En tal sentido los siguientes son los ítems para cumplir en la infraestructura, equipos y resguardo de estos.

A.13 Seguridad de las comunicaciones

De acuerdo con la ISO 27001, hace referencia a las políticas y acciones desplegadas en hacer seguras las comunicaciones dentro de una red de datos, que interactúa a nivel interno y externo, usadas por las empresas.

A.13.1.1 Controles de redes

"Son las políticas y acciones desplegadas con el objetivo de lograr el aseguramiento de las red cableada y física; mantener estas alejadas de las intrusiones a nivel físico y lógico".

Control

Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.

A.13.1.2 Seguridad de los servicios de red

Son las políticas y acciones desplegadas por parte de la administración para asegurar los servicios que corren o prestan través de la red, de igual forma mediante que tecnología implementada se asegura el servicio frente a intrusiones.

Control

Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.

A.13.1.3 Separación en las redes

Es la acción de segmentar una red y permitir el acceso a los servicios y aplicaciones únicamente al usuario que corresponde, cuando se trate de usuarios o de equipos cuando se trate de este tipo de implementación, que aunque se encuentre en la misma empresa y lugar no le es posible acceder a los mismos sitios, sino que se configura para que pueda ingresar a donde corresponde, esto es quine accede al área financiera, le es imposible ingresar al manejo de personal.

Control

“Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes”.

8.1.2 HARDWARE

Es parte de la infraestructura física (equipos) destinada a prestar los servicios de conectividad e interoperabilidad de usuarios, aplicaciones, herramientas, administración de la empresa y su interrelación con los clientes externos e internos, aquella donde esta soportada todas las capacidades tecnológicas con que se cuenta para su funcionamiento.

8.1.2.1 Equipos activos de red

Se han adquirido para el proyecto algunos equipos activos de red necesarios, tales como router, Switch, conversores de medios como conectores de fibra óptica o tranceiver para la interconexión de equipos mediante fibra óptica.

8.1.2.2 Router.

Se ha dispuesto de la utilización en el proyecto del equipo router cisco 3860 relacionado en las figuras anteriores como enrutador de nuestra red LAN.

8.1.2.3 Switch.

Para la interconexión y acceso de usuarios finales a la red LAN se ha adquirido un equipo Switch de 48 puertos en salidas para RJ 45 y dos para módulos Mini GBic SFP con una capacidad de 1Giga TX BaseT para la interconexión al router.

8.1.2.4 Módulos tranceiver SFP para fibra óptica Multimodo.

Conocidos también como transductores que transforman las señales eléctricas en señales lumínicas, usados en la interconexión de equipos activos de red, esto es routers a switchs, switchs a switchs, router a router con interconexión en fibra óptica únicamente y que se encuentran con características específicas de acuerdo con las necesidades que se presente en cada proyecto.

8.1.2.5 Equipo server

En proceso de consecución para virtualizar maquinas necesarias en la configuración de las herramientas básicas del CSIRT

8.1.2.6 Equipo de cómputo.

Se ha dispuesto de un equipo de cómputo de escritorio con procesador AMD A10 para usar en la oficina, con el objeto de llevar la relación de atención a los usuarios internos y externos por parte de la empresa.

8.1.2.7 Impresora multifuncional.

Se ha dispuesto para el proyecto una impresora Lexmark X5495 series para hacer uso de cualquiera de sus servicios como los son Fax, Escáner e impresión de documentos.

8.1.2.8 Teléfono SIP

Equipo de comunicación de voz que hace uso de los protocolos de internet para transportar y codificar la voz sobre las redes de datos y el servicio de internet.

8.1.3 SOFTWARE HYPERVISORES

Es el software que permite la creación y administración de máquinas virtuales, permite virtualizar, equipos, servicios, aplicaciones y se accede a estos a través de los diferentes tipos de navegadores disponibles en los sistemas operativos.

Algunos de estos hypervisores son propietarios, OpenSource o con licencia de pruebas por 60 días, que permiten la creación de máquinas virtuales, instalación de sistemas operativos; instalación y configuración de aplicaciones y bases de datos, así como también la creación de redes virtuales que permiten la implementación de la conectividad al interior de cualquier empresa.

8.1.3.1 VMware ESXi vSphere

VMware ESXi VSphere sin sistema operativo, usado como base para el equipo servidor físico, en donde se crearán máquinas virtuales para ser usadas en aplicaciones necesarias básicas del CSIRT.
Este software de la casa matriz de VMware Inc., es usado en la infraestructura de data center de las empresas de hoy en día, permite implementar las soluciones de cloud y proveer los modelos servicios y/o por capas, como son:

- SaaS, (Software As A Service).
- PaaS, (Platform As A Service).
- IaaS, (Infraestructure As A Service).

De acuerdo con VMware, *"Una máquina virtual es un equipo con software que, al igual que un equipo físico, ejecuta un sistema operativo y aplicaciones. La máquina virtual está compuesta por un conjunto de archivos de configuración y especificaciones"*. Este tipo de plataforma es el implementado en el desarrollo del

presente proyecto y es la infraestructura en la cual se crea e instala las aplicaciones necesarias[20].

Características de ESXi vSphere

Mediante VMware ESXi vSphere, se puede:

- Consolidar el hardware para mejorar la utilización de la capacidad.
- Aumentar el rendimiento para lograr una ventaja competitiva.
- Optimizar la administración de TI mediante una gestión centralizada.
- Reducir la inversión en capital y los gastos operativos.
- Reducir al mínimo los recursos de hardware necesarios para ejecutar el hipervisor, lo que se traduce en una mayor eficiencia[21] (VMware.Inc, 2020).

Administración de ESXi vSphere

Esta es posible realizarse mediante un plugin o cliente para las versiones anteriores a la ESXi vSphere 6.7 y directamente desde cualquier navegador web para las versiones de ESXi vSphere 6.7 en adelante, accediendo mediante la dirección IP que se le ha configurado; también existe la versión de data center denominada vCenter y mediante el cual es posible realizar toda la administración de la infraestructura basada y creada usando ESXi vSphere[22] (VMware, Inc., 2018).

8.1.3.2 VirtualBox

Hipervisor de Oracle micro systems para virtualización en arquitectura de x86/amd64, software libre y de código abierto y que es posible ser usado para este proyecto en la virtualización de equipos para la instalación y configuración de aplicaciones. VirtualBox no solo es un producto extremadamente rico en funciones y de alto rendimiento para clientes empresariales, sino que también es la única solución profesional que está disponible gratuitamente como software de código

---

[20] VMware Inc., VMware vSphere. Administrar máquinas virtuales de vSphere. Palo Alto, CA 94304.2020. p 9.

[21] Descripción, características de ESXi vSphere. VMware Inc. {en línea}. {15 de marzo 2020}. 3401 Hillview Ave -Palo Alto, CA 94304. Estados Unidos. Disponible en: https://www.vmware.com/latam/products/esxi-and-esx.html. https://www.vmware.com/latam.

[22] Administrar máquinas virtuales de vSphere, VMware vSphere 6.7, VMware ESXi 6.7, vCenter Server 6.7. 2009-2018 VMware, Inc. 3401 Hillview Ave. Palo Alto, CA 94304 EE.UU. abril 04 2018. P 17. Disponible en: https://www.vmware.com/latam. https://docs.vmware.com/es/.

abierto bajo los términos de la GNU General Public License (GPL) versión 2[23] (2004-2020 Oracle Corporation, 2020).

8.1.3.3 Proxmox VE

Proxmox VE es una plataforma completa de código abierto para la virtualización empresarial. Con la interfaz web incorporada, puede administrar fácilmente máquinas virtuales y contenedores, almacenamiento y redes definidos por software, agrupación en clúster de alta disponibilidad y múltiples herramientas listas para usar en una sola solución.

Proxmox VE es una plataforma que está basada en Debian Linux, completamente de código abierto[24] (Proxmox Server Solutions GmbH, 2020).

8.1.4 APLICACIONES

En este caso son los programas seleccionados a usar como herramientas en la creación, implementación y configuración del CSIRT planteado en el presente proyecto, las cuales se enumeran a continuación.

8.1.4.1 Principales aplicaciones y/o Herramientas

A continuación, se listan las principales herramientas debido a su función y que son necesarias en la creación y configuración de un CSIRT para realizar la atención e investigación de incidentes informáticos por parte del equipo.

- ✓ SIEM correlacionador eventos = logs
- ✓ Firewall = IP table = SNORT
- ✓ Antivirus = Sophos-AVG
- ✓ Correo electrónico = Zimbra
- ✓ Sandbox = análisis malware = Cuckoo
- ✓ Bases de Datos
- ✓ Nessus

---

[23] User Manual Versión 6.1.14. Oracle VM VirtualBox., Oracle Corporation 2004-2020. Weinstadt-Alemania. 2020. p 12. Disponible en. http://www.virtualbox.org.

[24] PROXMOX VE ADMINISTRATION GUIDE RELEASE 6.2. Proxmox Server Solutions GmbH. Dietmar y Martin Maurer 2008. Headquatered Viena Austria. Mayo 10 2020. p 2. Disponible en: www.proxmox.com.

- ✓ Nmap
- ✓ Server PHP serverMON, Herramienta de monitoreo web
- ✓ Criptografía

8.1.4.2 AlienVault OSSIM

Cuenta con la confianza de miles de profesionales de la seguridad en 140 países ... y contando.

AlienVault® OSSIM ™, Open Source Security Information and Event Management (SIEM), le proporciona un SIEM de código abierto rico en funciones completo, con recopilación, normalización y correlación de eventos. Lanzado por ingenieros de seguridad debido a la falta de productos de código abierto disponibles, AlienVault OSSIM fue creado específicamente para abordar la realidad que enfrentan muchos profesionales de seguridad: un SIEM, ya sea de código abierto o comercial, es prácticamente inútil sin los controles de seguridad básicos necesarios para la seguridad visibilidad.

Nuestro SIEM de código abierto (AlienVault OSSIM) aborda esta realidad al proporcionar una plataforma unificada con muchas de las capacidades de seguridad esenciales que necesita, como:

- ✓ Descubrimiento de activos
- ✓ Evaluación de vulnerabilidad
- ✓ Detección de intrusiones
- ✓ Monitoreo de comportamiento
- ✓ SIEM correlación de eventos

AlienVault OSSIM aprovecha el poder de AlienVault® Open Threat Exchange® (OTX ™) al permitir que los usuarios contribuyan y reciban información en tiempo real sobre hosts maliciosos. Además, ofrecemos desarrollo continuo para AlienVault OSSIM porque creemos que todos deberían tener acceso a tecnologías de seguridad sofisticadas para mejorar la seguridad de todos. Desde los investigadores que necesitan una plataforma para la experimentación y los héroes anónimos que no pueden convencer a sus empresas de que la seguridad es un problema, AlienVault OSSIM le ofrece la oportunidad de aumentar la visibilidad y el control de seguridad en su red[25]. (Cybersecurity, 2019).

[25] AT&T cybersecurity, AlienVault OSSIM The world's most widely used Open Source SIEM: AlienVault OSSIM {en línea}. {12 de Noviembre 2019}. Disponible en: (https://www.alienvault.com/products/ossim)

8.1.4.3 Firewall (cortafuegos)

Es posible definirse como un equipo o software con la capacidad de permitir o negar el tráfico de datos (comunicaciones) saliente y entrante entre un equipo de cómputo o cualquier dispositivo conectado a una LAN y la red extendida de Internet.

De acuerdo con la necesidad y robustez de la infraestructura tecnológica es posible hacer uso de software instalado en máquinas virtuales sencillas, o realizar la adquisición completa de hardware y software especializado para ser instalado y configurado en exclusividad a actuar como firewall empresarial, tal es el caso de firmas como Fortinet, Paloalto, etc.

Permite realizar filtrado de tráfico desde una red a otra, especialmente aquellas que dan salida a un usuario o grupo de usuarios finales a recursos directos alojados en Internet, este sistema de seguridad existe como hardware de tipo propietario y licenciado por módulos, de igual forma es un software de aplicación que puede ser implementado sobre un sistema operativo, tal es el caso de pfSense OpenSource, el firewall de Windows (Windows Defender), como un módulo integral de un antivirus tal es el caso de AVG o de ambos[26] (hardware y Software) Fortinet.

8.1.4.4 Tipo de firewall mediante software

En la búsqueda de una posible solución de firewall y aplicando que sea del tipo OpenSource para nuestro proyecto se ha encontrado dos opciones las cuales se presenta a continuación:

8.1.4.5 IpTable

Es un sistema de firewall vinculado al kernel de linux que se ha extendido enormemente a partir del kernel 2.4 de este sistema operativo[27]. (Izura, 2019)

[26] PELLO XABIER, Altadill Izura. IPTABLES Manual práctico. Bilbao País Vasco. p 1.
Ibid., p 4

[27] PELLO XABIER, Altadill Izura. IPTABLES Manual práctico. Bilbao País Vasco. p 1.

8.1.4.6 Snort

Snort es un software de sistema de detección de intrusos de red (NIDS) de código abierto, gratuito y liviano para Linux y Windows usado para detectar amenazas emergentes[28]. (snort-cisco, 2019).

Para la instalación y la configuración de reglas del IDS Snort se ha acudido a la literatura hallada y se ha usado el software libre basado en sistemas operativos linux para la configuración de cada una de las maquinas necesarias[29] (Neil Archibald, 2005).

8.1.4.7 Antivirus

Es un software o programa informático diseñado para la detección de virus (malware) y otros programas que destruyen antes o después que ingresan al sistema de un computador, destruyendo o sustrayendo la información en el equipo alojada[30]. (Informática, 2019)

8.1.4.8 Correo electrónico = Zimbra

Es una **suite de colaboración** (en inglés, ***Zimbra Collaboration Suite*** o **ZCS**) es un programa informático colaborativo o Groupware que consta de un servicio de correo electrónico creado por Zimbra Inc. compañía ubicada en San Mateo, California[31]. (es.wikipedia.org/wiki/, 2019)

---

[28] Snort-Cisco. SNORT Users Manual 2.9.16. The Snort Project. Writing Snort Rules by Martin Roesch and further work from Chris Green. The Snort Team. {en línea} {12 April 8, 2020}. p 9. Disponible en: https://www.snort.org/ , https://www.snort.org/documents/1.

[29] Neil Archibald, Gilbert Ramírez, Noam Rathaus. Nessus, Snort, & Ethereal, Power Tools; Customizing Open Source Security Applications. Hingham St, Rockland, Massachusetts United States. Septiembre 2005. p 14.

[30] Tecnología + Informática, Guillermo Venturini. Que es un antivirus {En línea}. {15 noviembre 2019}. Disponible en: https://www.tecnologia-informatica.com/que-es-un-antivirus-como-funciona/

[31] Fundación Wikimedia, Inc. es.wikipedia.org. Zimbra. San francisco California, {en línea}. {Agosto 12 de 2019}. p1. Disponible en:(https://es.wikipedia.org/wiki/Zimbra).

Esta fue Fundada en 2003, Zimbra es un software de mensajería y de colaboración de código abierto. En el año 2010, fue adquirida por el fabricante de software de virtualización más importante del mundo (VMware).
Zimbra es un servidor de mensajería de colaboración (groupware) que permite compartir, almacenar y organizar mensajes de correo electrónico, citas, contactos, tareas, documentos y mucho más. Zimbra está disponible desde un acceso al correo web (web 2.0), además puede trabajar sin estar conectado a la red, usando Zimbra Desktop, Thunderbird, MS Outlook y Mac, o cualquier tipo de PDA[32]. (ultimobyte.es, 1995)

Es una buena opción para realizar la creación y configuración de un sistema y servicio de mensajería (correo electrónico) para una empresa haciendo uso de tecnologías Open Source.

8.1.4.9 Sandbox

En la práctica es un mecanismo de seguridad creado para tener un entorno aislado del resto del sistema operativo, en este entorno se realiza el análisis de malware con el objeto de identificarlo plenamente.

8.1.4.10 Cuckoo

Cuckoo Sandbox es el principal sistema automatizado de análisis de malware de código abierto. Es un software gratuito que automatizó la tarea de analizar cualquier archivo malicioso en Windows, macOS, Linux y Android.
Analiza diferentes archivos maliciosos (ejecutables, documentos de oficina, archivos pdf, correos electrónicos, etc.), así como sitios web maliciosos en entornos virtualizados Windows, Linux, macOS y Android[33] (Georg Wicherski, 2018).
Puede volcar y analizar el tráfico de red, incluso cuando está cifrado con SSL / TLS. Cuenta con soporte de enrutamiento de red nativo para eliminar todo el tráfico o enrutarlo a través de InetSIM, una interfaz de red o una VPN[34]. (Foundation, 2019)

---

[32] ultimobyte, Correo electrónico Zimbra, Av. Aragón 8 - Entlo. E 46021 Valencia. {en línea}. p1. Disponible en: (https://www.ultimobyte.es/productos/zimbra-correo-electronico-y-groupware).

[33] Georg Wicherski, David Watson, Christian Seifert. Cuckoo Sandbox Book, Release 2.0.6. Mountain View California Estados Unidos. 06 octubre 2018. p 27.

[34] Cuckoo Automated malware Analisys. Stichting Cuckoo Foundation, Claudio Guarnieri. {En línea}. {19 junio 2019}. Disponible en: https://cuckoosandbox.org/

8.1.4.11 Bases de Datos

Conjunto de información que hace parte del mismo contexto, ordenada sistemáticamente para ser recuperada posteriormente, su análisis y/o transmisión. En la actualidad existe diversas formas de bases de datos, desde una biblioteca hasta los más avanzados conjuntos de datos de usuarios de una empresa, instituciones y organizaciones en su infraestructura de telecomunicaciones.

8.1.4.12 Nessus

Tenable Nessus es la solución N° 1 para evaluaciones de vulnerabilidades, es el estándar de facto de la industria para la evaluación de vulnerabilidades.
Nessus® Professional, que cuenta con la confianza de más de 24.000 organizaciones en todo el mundo, automatiza las evaluaciones en un momento dado para ayudar a identificar y reparar con rapidez las vulnerabilidades, incluidos parches faltantes, defectos de software, malware y configuraciones erróneas, en diversos sistemas operativos, dispositivos y aplicaciones[35]. (Tenable®, 2019)

8.1.4.13 Características Generales

- ✓ Detección de virus, malware, puertas traseras, botnets, procesos conocidos/desconocidos, enlaces a contenido malicioso.
- ✓ Actualizaciones constantes
- ✓ Escaneo de vulnerabilidades (incluidos IPv4/IPv6/redes híbridas)
- ✓ Integración a su flujo de trabajo existente.
- ✓ Generación flexible de informes[36].

8.1.4.14 Nmap

("Network Mapper") herramienta de software gratuita y de código abierto, usada para descubrir redes y auditar la seguridad de esta y los sistemas operativos. Permite hacer inventario de red, controlar horarios de actualización y supervisar la actividad de un equipo o un servicio determinado. Su particularidad es el escaneo de redes rápidamente sin importar que tan grandes sean estas[37]. (nmap.org, 2019).

---

[35] Nessus Professional. Nessus Professional. Hoja de datos de Nessus Professional. {en línea}. Maryland. p1.

[36]GitHub, Inc. phpservermon {en línea}. San Francisco. p1. © 2019

[37] Nmap Security Scanner. nmap.org, Gordon Lyon. Palo Alto, California, EE. UU. {En línea}. {20 enero 2019}. Disponible en: https://nmap.org/

8.1.4.15 Server PHP serverMON, Herramienta de monitoreo web

PHP Server Monitor es un script que comprueba si sus sitios web y servidores están en funcionamiento. Viene con una interfaz de usuario basada en la web donde puede administrar sus servicios y sitios web, y puede administrar usuarios para cada servidor con un número de teléfono móvil y una dirección de correo electrónico[38]. (GitHub, 2019)

8.1.4.16 Características Generales

- ✓ Supervisar servicios y sitios web.
- ✓ Correo electrónico, SMS, Pushover, notificaciones de Telegram.
- ✓ Ver gráficos de historial de tiempo de actividad y latencia.
- ✓ Autenticación de usuario con 2 niveles (administrador y usuario normal).
- ✓ Registros de errores de conexión, correos electrónicos salientes y mensajes de texto.
- ✓ Implementación fácil de cronjob para verificar automáticamente sus servidores.

8.1.4.17 Criptografía

Criptografía es la **ciencia y arte de escribir mensajes en forma cifrada o en código.** Es parte de un campo de estudios que trata las comunicaciones secretas, usadas, entre otras finalidades, para[39]: (tecnologia+informatica, 2019)

- ✓ Autentificar la identidad de usuarios.
- ✓ Autentificar y proteger el sigilo de comunicaciones personales y de transacciones comerciales y bancarias.
- ✓ Proteger la integridad de transferencias electrónicas de fondos.

8.1.4.18 ¿Qué es el cifrado?

El cifrado es el proceso de convertir la información en un formulario donde una parte no autorizada no puede leerla. Solo una persona confiable y autorizada con la clave secreta o la contraseña puede descifrar los datos y acceder a ellos en su forma original. El cifrado en sí mismo no impide que alguien intercepte los datos. El cifrado

[38] Phpservermon. GitHub, Inc. 2019, Pepijn Over. {En línea}. {25 enero 2019}. Disponible en: https://github.com/. https://github.com/phpservermon/phpservermon

[39] Tecnología + Informática, Guillermo Venturini. Que es la criptografía. {En línea}. {10 febrero 2019}. Disponible en: https://tecnologia-informatica.com/que-es-la-criptografia/

solo puede evitar que una persona no autorizada vea o acceda al contenido[40]. (academy, 2018).

8.1.5 INFRAESTRUCTURA

8.1.5.1 Aspectos importantes de la infraestructura

Su importancia y relevancia en la aplicación e implementación en los sistemas de TI se debe a la alineación que tiene con la norma ISO/IEC 27001 y la relaciona con el control y la política de seguridad descrita a continuación para lograr su cumplimiento

8.1.5.2 Política A.11.2 Equipos

ISO/IEC 27001:2005 presenta: “Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización”[41].

8.1.5.3 (A.11.2.1) Ubicación y protección de los equipos

De acuerdo con la ISO 27001 hace referencia a que se debe contar con un lugar físico en el cual permita asegurar los equipos tecnológicos de los accesos no autorizados, intrusiones de personal ajeno a las instalaciones, de igual forma refiere a que se deben proteger de frente a daños causados por medioambiente, daño físico, inundaciones entre otros.

Control

Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, y las posibilidades de acceso no autorizado[42]. (ISO/IEC 27002:2005, 2005)

---

[40] Academy, Cisco networking. Introduction to Cybersecurity. San Francisco San Francisco, EE.UU. 10 enero 2018. Disponible en: https://static-course-assets.s3.amazonaws.com/CyberEss/es/index.html#4.1.1.1

[41] ISO/IEC 27002:2005. Estándar para la seguridad de la información. Ginebra Suiza. ISO/IEC 270021:2005. 2005. p. Anexo A.

[42] ISO/IEC 27002:2005, op. cit. Anexo A.

8.1.5.4 (A.11.2.3) Seguridad del cableado

De acuerdo con la ISO 27001 hace referencia a que todos los equipos que hacen parte de la infraestructura de telecomunicaciones, comunicación de datos, red cableada y accesorios se deben resguardar con el objeto de evitar fugas, interceptación, perdida y sustracción de información, así como el daño de la infraestructura misma, para lo cual se hace necesario contar con gabinetes, rack y cuartos de comunicaciones con puertas o algún tipo de control de acceso que impida fácilmente el acceso a estos.

Control

"El cableado de potencia y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño".

8.1.5.5 Rack de Comunicaciones

El rack o gabinete para telecomunicaciones es el accesorio principal que permite alojar equipos de comunicaciones y la conexión cruzada de forma ordenada y organizada de los usuarios finales que acceden a la red mediante el uso del cableado estructurado; este elemento debe cumplir con algunas especificaciones básicas y contar con barrajes que permita conectar los equipos a sistemas de protección contra descargas atmosféricas y sobretensiones que afecten los equipos allí alojados.

8.1.5.6 Sistemas y elementos de potencia

Es otro de los componentes con que debe contar cualquier infraestructura que sea dedicada a soportar equipos que hacen parte integral en sistemas tecnológicos que soportan las telecomunicaciones y la información (datos), es el componente que permite que los equipos funciones proveyendo el voltaje correcto que necesita el equipo para funcionar; este componente hace referencia a la alimentación por voltaje regulado que impide las variaciones de voltaje que afectan el normal funcionamiento de estos.

Estos sistemas regulados son sometidos a un filtrado y estabilización a través de dispositivos especiales que mantienen un mismo nivel de tensión de salida sin importar la variación con que ingresa o es entregada por el operador de red eléctrica presente en el lugar.

Para lograr la estabilidad en el suministro de voltaje a los equipos de comunicaciones los ingenieros de TI hacen el uso de equipos tales como:

8.1.5.7 UPS (Uninterruptible Power Supply)

Dispositivos que mantienen el suministro eléctrico a los equipos durante los fallos de energía gracias a los bancos de baterías con los que cuenta y estos siguen funcionando por un determinado tiempo dependiendo la cantidad de equipos de comunicaciones conectados a estos elementos.

8.1.5.8 Fuente redundante

Son los dispositivos que permiten que un dispositivo electrónico, en este caso los routers, switchs y servidores se conecten a dos fuentes de suministro de energía distintitos; esto con el fin de que cuando un circuito sea des-energizado el otro quede activo y por tanto el equipo en funcionamiento, evitando indisponibilidades y perdida de información.

8.1.5.9 Sistemas de Cableado Estructurado

El cableado estructurado es la infraestructura de comunicaciones que permite que los equipos de cómputo de cada usuario final sean conectados a los equipos switchs y/o red LAN a través del cable UTP y accesorios, este sistema debe cumplir con una normalización y estándar propios emitidos para este sistema por organismos internacionales y locales.

8.1.5.10 Bandeja de Fibra óptica

Caja o dispositivo mecánico que permite alojar magazines o caseteras en las cuales se realiza la conectorización y terminado de la fibra en un conector específico de acuerdo con la salida (puerto) que tenga el dispositivo activo de red, estos pueden ser salidas en conector LC-LC, ST, SC, etc.

8.1.5.11 Fibra óptica

Elemento que actúa como medio de transmisión en el cual la información viaja como ondas lumínicas en un rango de frecuencias específicas, esta información es procesadas por dispositivos transductores que realizan el proceso de recuperar la información cuando la transforman en señales eléctricas.

8.1.5.12 Patch Panel

Herraje preensamblado o modular con salidas del tipo RJ45 hembra con 8 conexiones, 8 posiciones que son la cantidad de conductores de cobre que contiene el cable UTP de par trenzado.

8.1.5.13 Cable UTP (*Unshielded Twisted Pair*) Categoría 6A y accesorios

Unshielded Twisted Pair (UTP) o cable de par trenzado sin blindaje: cable de par trenzado formado por cuatro grupos de dos hilos de cobre cada grupo, usado como medio de transmisión en las redes locales de datos. De bajo costo y fácil uso, pero produce más errores que otros tipos de cable, su limitación de transmisión está dada hasta 100 metros lineales. Su impedancia característica es de 100 ohmios.
La categoría va definida en función de la capacidad de respuesta en frecuencia y ancho de canal para trasmitir un paquete de información a través de un canal de comunicación de datos, en este caso la categoría 6A tiene la capacidad de soportar 10 Gigabytes de información.

8.1.5.14 Organizadores de cables de 2UR

Elemento que permite la organización de cable sobrante o Patch cords con los cuales se realiza la conexión cruzada, entre el equipo de cómputo y equipo activo de red, estos organizadores existen de dos tipos, organizadores horizontales y organizadores verticales o escalerillas.

8.1.5.15 Organizadores laterales tipo escalerilla

Es un elemento que permite organizar el cableado al interior del rack en forma vertical y por lo general se ubica en los costados.

8.2 ANÁLISIS DE PROCEDIMIENTOS, PRÁCTICAS Y NECESIDADES TÉCNICAS

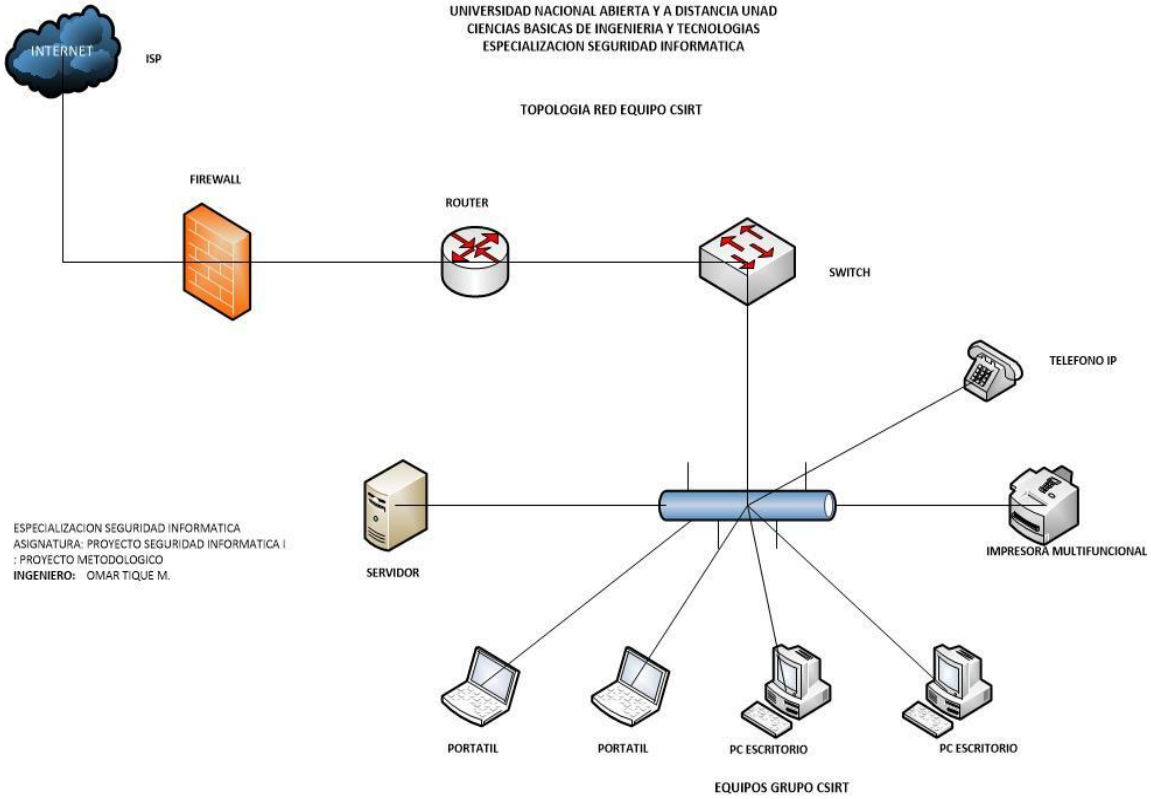
8.2.1 Aspectos técnicos

Referente a este componente y con el firme propósito de lograr alcanzar el objetivo propuesto se hace necesario la adquisición, instalación, configuración y puesta en funcionamiento de la siguiente infraestructura tecnológica a nivel físico y lógico (Hardware-software) así como la configuración e integración de aplicaciones que

permitan el funcionamiento y la disponibilidad de las herramientas tecnológicas con las cuales se dará respuesta, se realizara investigación y se entregaran resultados a los afectados por ataques de tipo informático o cuando se presenten los eventos; con el objeto de cumplir con la tarea se hace necesaria la creación de una red LAN que permita la comunicación interna del equipo de respuesta a los incidentes informáticos y el uso de las herramientas necesarias para ello, de tal forma se usará el siguiente diagrama de red general para validar su jerarquía.

8.2.1 Topología de Red en el CSIRT Propuesto

Figura 4. Topología en la Red del CSIRT propuesto para el proyecto a presentar.



Fuente: Software diseño gráfico diagrama de red, Omar Tique M., mayo de 2020.

De acuerdo con la topología propuesta y en función de salvaguardar la información tanto a nivel físico y lógico se ha tenido en cuenta las consideraciones emitidas por el estándar de seguridad de la información la ISO/IEC 27000, ISO/IEC 27001 para garantizar disponibilidad, seguridad y confidencialidad de la información (datos).

En tal sentido los siguientes son los ítems para cumplir en la infraestructura, equipos y resguardo de estos, estas consideraciones han sido relacionadas en el marco conceptual como parte integral en la creación de un grupo que dé respuesta en

investigaciones de ataques informáticos y/o materialización de amenazas y riesgos en las empresas de clientes atendidos.

8.2.2 A.13 Seguridad de las comunicaciones

8.2.3 A.13.1.1 Controles de redes

Control

“Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones”.

8.2.4 (A.13.1.2) Seguridad de los servicios de red

Control

“Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente”.

8.2.5 (A.13.1.3) Separación en las redes

Control

“Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes”.

8.2.6 HARDWARE

8.2.6.1 Equipos activos de red

Se han adquirido para el proyecto los siguientes equipos activos de red necesarios para brindar conectividad, administración y acceso a internet, tales como router, Switch, conversores de medios como conectores de fibra óptica o tranceiver para la interconexión de equipos mediante fibra óptica. A continuación, se indica mediante fotografía cuales son estos equipos adquiridos e integrados al proyecto dentro de red LAN configurada.

Router

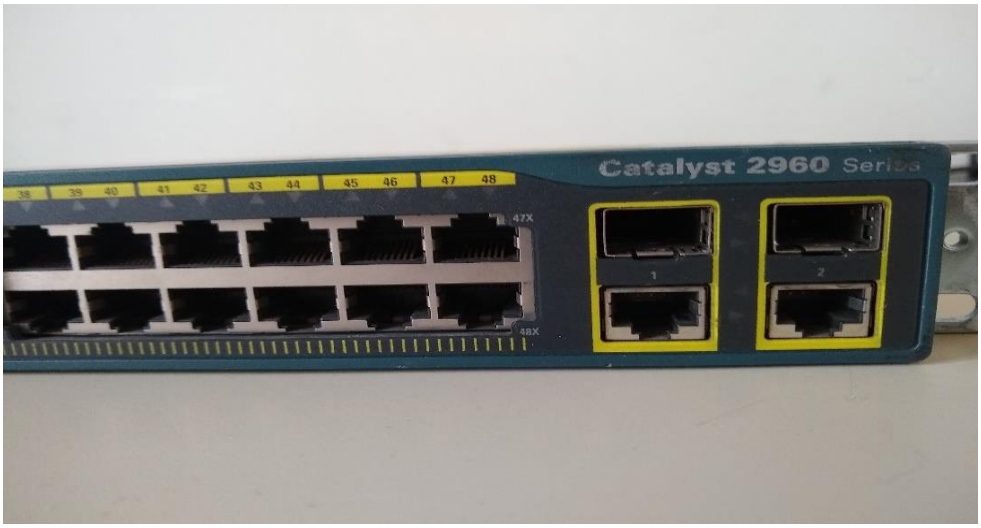
Figura 5. Router Cisco 3800 Series usado como salida a Internet y la red interna.

Fuente: Fotografía equipos infraestructura TI., Omar Tique M., mayo de 2020.

Se ha dispuesto de la utilización en el proyecto del equipo router cisco 3860 relacionado en las figuras anteriores como enrutador de nuestra red LAN, ha sido necesaria su adquisición para poder realizar el enrutamiento del tráfico de datos que se genere en nuestra red.

Switch

Figura 6. Switch Cisco Catalyst 2960 Series.

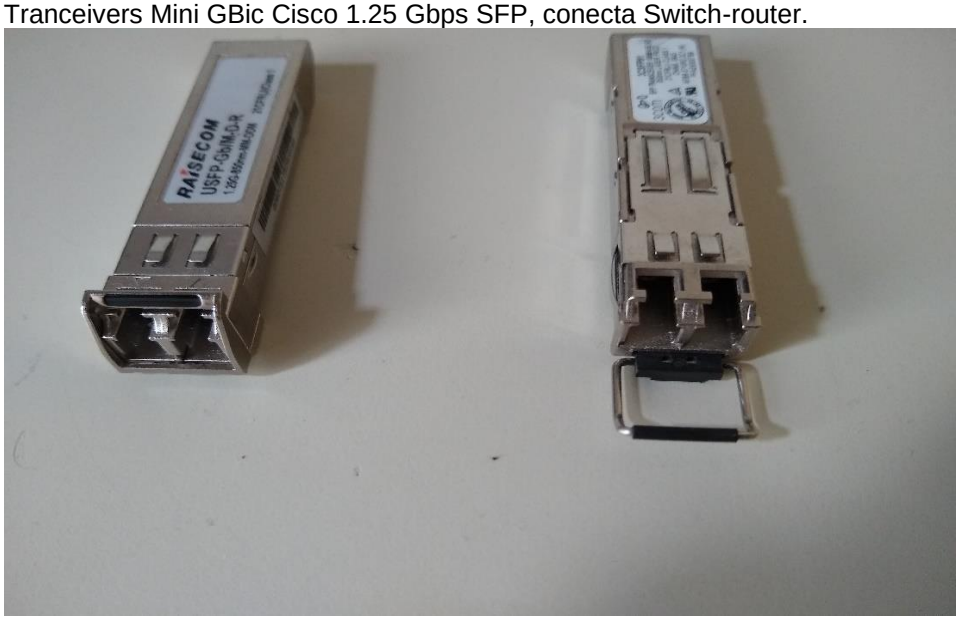


Fuente: Fotografía equipos infraestructura TI., Omar Tique M., mayo de 2020.

Para la interconexión y acceso de usuarios finales a la red LAN se ha adquirido un equipo Switch de 48 puertos en salidas para RJ 45 y dos para módulos Mini GBic SFP con una capacidad de 1Giga TX BaseT para la interconexión al router y cada uno de los usuarios que hacen parte del equipo de respuesta e investigación de incidentes informáticos CSIRT.

8.2.6.2 Módulos para fibra óptica Multimodo Tranceiver SFP

Figura 7. Tranceivers Mini GBic Cisco 1.25 Gbps SFP, conecta Switch-router.



Fuente: Fotografía componentes infraestructura TI, Omar Tique M., mayo de 2020.

8.2.6.3 Equipo server.

En proceso de consecución para virtualizar maquinas necesarias en la configuración de las herramientas básicas del CSIRT

8.2.6.4 Equipo de cómputo.

Se ha dispuesto de un equipo de cómputo de escritorio con procesador AMD A10 para usar en la oficina, con el objeto de llevar la relación de atención a los usuarios internos y externos por parte de la empresa.

8.2.6.5 Impresora multifuncional.

Se ha dispuesto para el proyecto una impresora Lexmark X5495 series para hacer uso de cualquiera de sus servicios como los son Fax, Escáner e impresión de documentos.

8.2.6.6 Teléfono SIP

Se ha adquirido un teléfono SIP que permita realizar una conexión directa desde internet y permita habilitar el servicio de telefonía desde cualquier parte sin

necesidad de estar directamente en la oficina, sino que mediante una conexión a internet y con los parámetros de configuración se pueda obtener una línea telefónica funcional.

Figura 8. Teléfono protocolo SIP Yealink a ser usado en red de datos.

Fuente: Fotografía equipos de infraestructura TI, Omar Tique M., mayo de 2020.

8.2.7 INFRAESTRUCTURA

Referente a la infraestructura necesaria y dando alcance a lo emitido en la norma ISO/IEC 27001 referida a continuación se ha tenido la necesidad de realizar la adquisición de un rack de comunicaciones para salvaguardar los equipos que hacen parte de la solución y tienen una participación importante en el diseño del CSIRT propuesto.

De igual forma ante la implementación de cualquier sistema de cableado estructurado para infraestructura de TI y atendiendo las mejores prácticas, se debe atender las recomendaciones de los estándares internacionales y que son la base para el buen funcionamiento y desempeño de cualquier organización y/o empresa.

8.2.7.1 Estándares aplicables al area de TI

• ANSI/TIA-942 B Infraestructura de Telecomunicaciones para Centros de Datos. Provee las guías y los requerimientos para el diseño e instalación de un Centro de Datos o cuarto de cómputo.

• ANSI/TIA 568-D conjunto de normas para instalaciones de cableado y premisas del cliente.

• ANSI/TIA 568-0-D Generic Telecommunications Cabling for Customer Premises. (TIA STANDAR, 2015)

• ANSI/TIA 568-1-D Commercial Building Telecommunications Infrastructure Standard. (TIA STANDAR, 2015)

• ANSI/TIA 568-2-D Balanced Twisted-Pair Telecommunications Cabling and Components.

• ANSI/TIA 568-3-D Optical Fiber Cabling and Components Standard. (TIA STANDAR, 2016)

• ANSI/TIA 568-4-D Broadband Coaxial Cabling and Components Standard. (TIA STANDAR, 2017)

• ANSI/TIA-569-D Commercial Building Standard for Telecomunications Pathways and Spaces, que estandariza prácticas de diseño y construcción dentro y entre edificios, que son hechas en soporte de medios y/o equipos de telecomunicaciones tales como canaletas y guías, facilidades de entrada al edificio, armarios y/o closet de comunicaciones y cuarto de equipos.

• ANSI/TIA-606 C Administration Standard for the Telecomunications Commercial Building of Comercial Buildings, que da las guías para marcar y administrar los componentes de un sistema de Cableado Estructurado.

• ANSI/TIA-607 C Commercial Building Grounding and Bonding Requeriments for Telecomunications, que describe los métodos estándares para distribuir las señales de tierra a través de un edificio.

• NTC 6064 Tecnología de la Información Cableado Genérico para Instalaciones de Clientes.

Deberá considerarse un sistema completo de energía regulada por UPS en donde estará conectados la totalidad de equipos de cómputo, y cuando esto sucede se debe realizar la Instalación y puesta en funcionamiento del sistema atendiendo las recomendaciones de la NTC 2050, NEC y RETIE.

Observaciones: para el caso específico del proyecto propuesto se obviara el temas de sistemas de respaldo de energía (UPS) en razón a los costos y que será un proyecto de aplicación de conocimientos a nivel técnico y de implementación básico y no para la prestación de servicios definitivos, sino con el firme propósito de optar por el título de Seguridad informática; sin embargo al momento de realizar un diseño

nuevo en el que se incluya este tipo de infraestructura se deben considerar los estándares a nivel internacional aplicables, la nacional, mejores prácticas y la certificación de canal y elementos que hacen parte de este tipo de tecnología.

No se hará relación de cada uno de los aspectos y puntos que contiene el estándar de la ANSI/TIA 568-D en cada uno de los ítems en razón a lo siguiente:

1. Cada ítem es bastante extenso y cuenta con un total de 65 páginas aproximadamente.

2. Se debe adquirir el documento completo de la ANSI/TIA y está prohibida su reproducción total o parcial salvo autorización expresa del autor, lo cual genera costos adicionales.

8.2.7.2 Política de seguridad aplicables al area de TI

- (A.11.2) Equipos

Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.

- (A.11.2.1) Ubicación y protección de los equipos

Control

"Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, y las posibilidades de acceso no autorizado".

- (A.11.2.3) Seguridad del cableado

Control

"*El cableado de potencia y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño*".

8.2.8 Elementos de cableado estructurado y equipos

Una vez alcanzada y superada esta fase de ejecución del proyecto, se ha procedido a la consecución de los elementos y accesorios para los puntos de red, tales como, cable UTP, Patch Panel, conector RJ 45 de ocho conexiones y ocho posiciones tipo IDC (Jacks), Place Plate, Patch Cords, Cajas plásticas porta tomacorrientes y porta

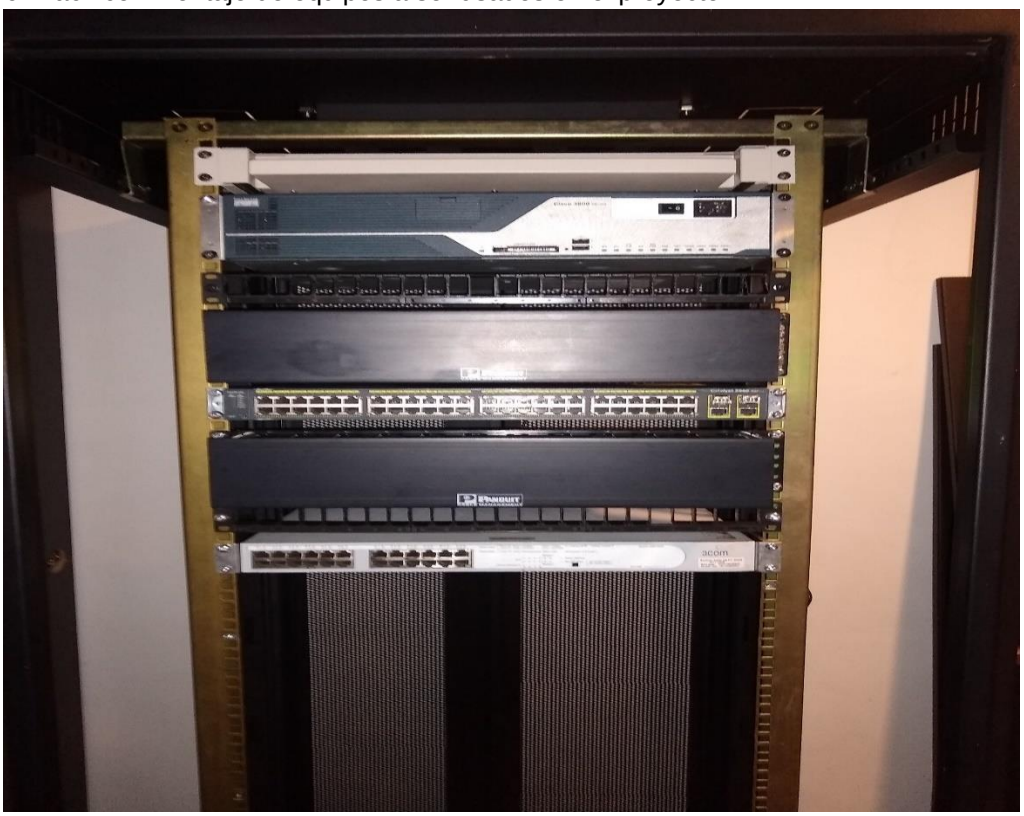
place plate, cinta velcro, tomacorrientes y la herramienta para el ponchado de cada punto de red; los cuales se muestran y describen a continuación.

8.2.8.1 Rack de Comunicaciones

Se ha adquirido un rack de comunicaciones para alojar los equipos activos de red, los puntos de red para la conexión de los equipos de cómputo de los usuarios finales y personal de soporte e ingenieros del **CSIRT**.

Este elemento que hace parte de la solución se encuentra ya instalado en el cuarto de comunicaciones y se continuara realizando las actividades necesarias para lograr la implementación completa de la solución; la siguiente tarea es realizar el montaje de los puntos de red mediante cable UTP.

Figura 9. Rack con montaje de equipos a ser usados en el proyecto.



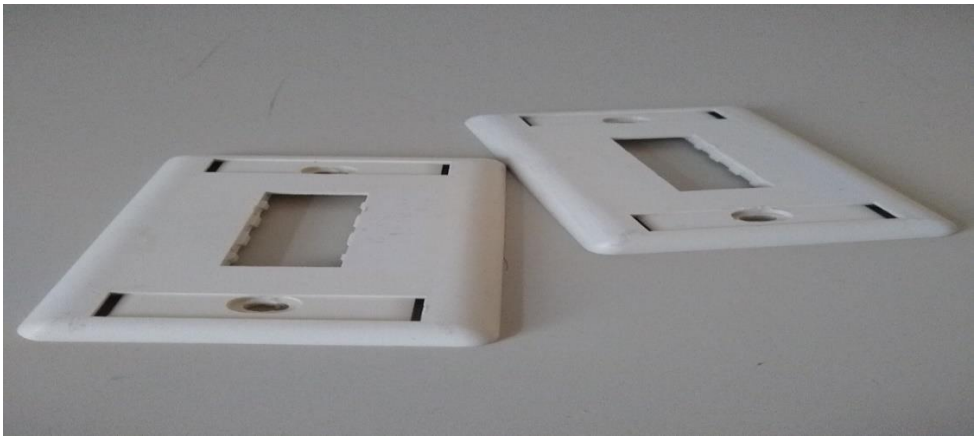
Fuente: Fotografía elementos infraestructura, Omar Tique M., mayo de 2020.

En la figura 9; se puede observar en el proceso, que hasta este punto se ha alcanzado en la fase del proyecto la consecución del rack o gabinete, el armado de este, su localización, así como también la consecución de algunos equipos y la organización de estos equipos al interior de este, tal y como se puede observar.

8.2.8.2 Place plate

De acuerdo con el estándar de la ANSI/TIA 568 D, para cableado estructura y fibra óptica que soporta la infraestructura de TI.

Figura 10. Place Plate dos salidas a usuarios finales.



Fuente: Fotografía elementos infraestructura, Omar Tique M., mayo de 2020.

En la figura 10 se puede observar que se ha realizado la adquisición de los place plate o herrajes para fijar los jacks tipo RJ45 para las salidas a los puestos de trabajo para los usuarios finales.

8.2.8.3 Patch panel

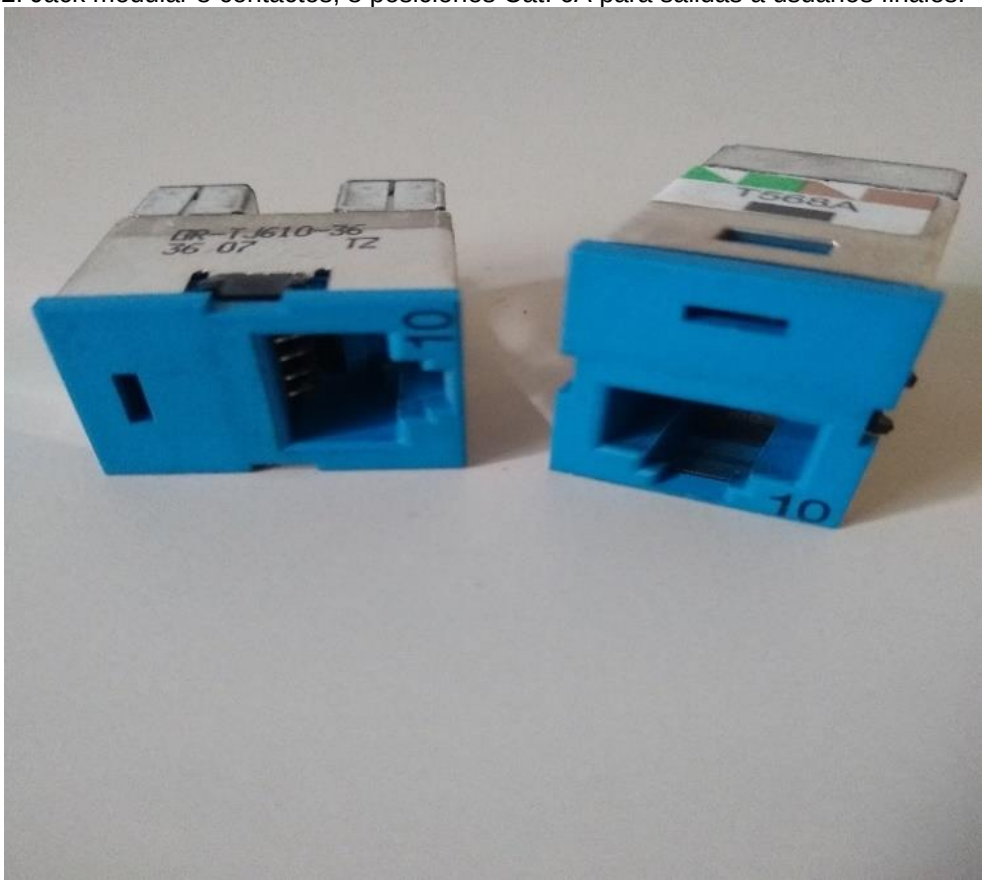
Figura 11. Patch Panel 24 puertos Cat. 6A. interconexión de equipos a la red interna.

Fuente: Fotografía elementos infraestructura, Omar Tique M., mayo de 2020.

En la figura 11 se puede observar que se ha realizado la adquisición del herraje o Patch panel modular de 24 puertos, en este accesorio se fijan los jacks con salida RJ45 para la conexión cruzada con los puertos de los equipos activos de red que serán ubicados en el rack.

8.2.8.4 Jacks tipo RJ45

Figura 12. Jack modular 8 contactos, 8 posiciones Cat. 6A para salidas a usuarios finales.



Fuente: Fotografía elementos infraestructura, Omar Tique M., mayo de 2020.

En la figura 12 se puede observar que se ha realizado la adquisición de los conectores RJ 45 de ocho contactos y ocho posiciones tipo IDC (Jacks), los cuales han sido adquiridos para las terminaciones y/o salidas en el montaje de los puntos de red necesarios para la conexión de los equipos de cada uno de los ingenieros de soporte, estos jacks han sido adquiridos en categoría 6A, de acuerdo con el estándar para cableado estructurado ANSI/TIA 568.D, para un canal con capacidad de 10 Gbps y una distancia de hasta 90 metros de canal fijo.

8.2.8.5 Accesorios para los place plate

En la figura 13 se puede observar que se ha realizado la adquisición de los accesorios usados para los place plate que sirven para acondicionar adecuadamente la llegada del cable UTP a las cajas de salida a los usuarios finales o puestos de trabajo, de igual forma las tapas que se usan para cubrir los orificios de place plate cuando se usa una única salida al puesto de trabajo.

Figura 13. Tapa ciegas para Jack y herrajes de montajes Cat. 6ª.

Fuente: Fotografía elementos infraestructura, Omar Tique M., mayo de 2020.

8.2.8.6 Cajas plásticas

Figura 14. Caja plástica porta place plate y tomacorrientes; (datos) y regulada.

Fuente: Fotografía elementos infraestructura, Omar Tique M., mayo de 2020.

En la figura 14 se puede observar que se ha realizado la adquisición de las cajas plásticas que se usara para soportar las salidas a puestos de trabajo, como porta place plate y como porta tomacorriente del sistema regulado de potencia.

8.2.8.7 Herramienta de ponchado

Figura 15. Ponchadora de impacto para terminación en jacks

Fuente: Fotografía elementos infraestructura, Omar Tique M., mayo de 2020.

En la figura 15 se puede observar que se ha realizado la adquisición de la herramienta de impacto que será usada para realizar el ponchado de cable UTP a los Jack ubicados en el Patch panel del lado del Rack y las salidas a los puestos de trabajo, es importante aclarar que la totalidad del canal ha de ser en una sola marca (Monomarca), quiere decir que todos los elementos que constituyen el canal de transmisión ha de ser de un mismo fabricante, esto con el objeto de garantizar las condiciones de desempeño y los parámetros de transmisión correspondiente a la categoría que será instalada.

8.2.8.8 Cable UTP categoría 6A.

Figura. 16. Cable UTP categoría 6A.

Fuente: Fotografía elementos infraestructura, Omar Tique M., mayo de 2020.

En la figura 16 se puede observar que se ha realizado la adquisición del cable UTP en categoría 6A, de acuerdo con el estándar para cableado estructurado ANSI/TIA 568.D, para un canal con capacidad de 10 Gbps y una distancia de hasta 90 metros de canal fijo; para realizar el cableado desde el Rack hasta los puestos de trabajo y así habilitar el servicio de la red LAN para la interconexión de los usuarios y el acceso a los servicios de red y aplicaciones del CSIRT correspondiente.

8.2.8.9 Patch Cord categoría 6A

Figura 17. Patch cords azul y rojo Cat. 6ª. para conexión cruzada en rack y conexión PC´s.

Fuente: Fotografía elementos infraestructura, Omar Tique M., mayo de 2020.

En la figura 17 se puede observar que se ha realizado la adquisición de los Patch Cords en categoría 6ª de acuerdo con el estándar para cableado estructurado ANSI/TIA 568.D, para un canal con capacidad de 10 Gbps y una distancia de hasta 90 metros de canal fijo, usados para realizar las conexiones de los puestos de trabajo, conexión cruzada en el rack y puertos del Switch y habilitar el servicio de red LAN para el acceso de los usuarios a los servicios de red y aplicaciones del CSIRT correspondiente.

8.2.8.10 Cinta tipo velcro

Figura. 18. Cinta velcro de amarre cable UTP.

Fuente: Fotografía elementos infraestructura, Omar Tique M., mayo de 2020.

En la figura 18 se puede observar que se ha realizado la adquisición de la cinta tipo velcro con el objeto de asegurar los cables UTP a los organizadores verticales del Rack tipo escalerilla para evitar que sufra daño la chaqueta del cable y se pierda su desempeño.

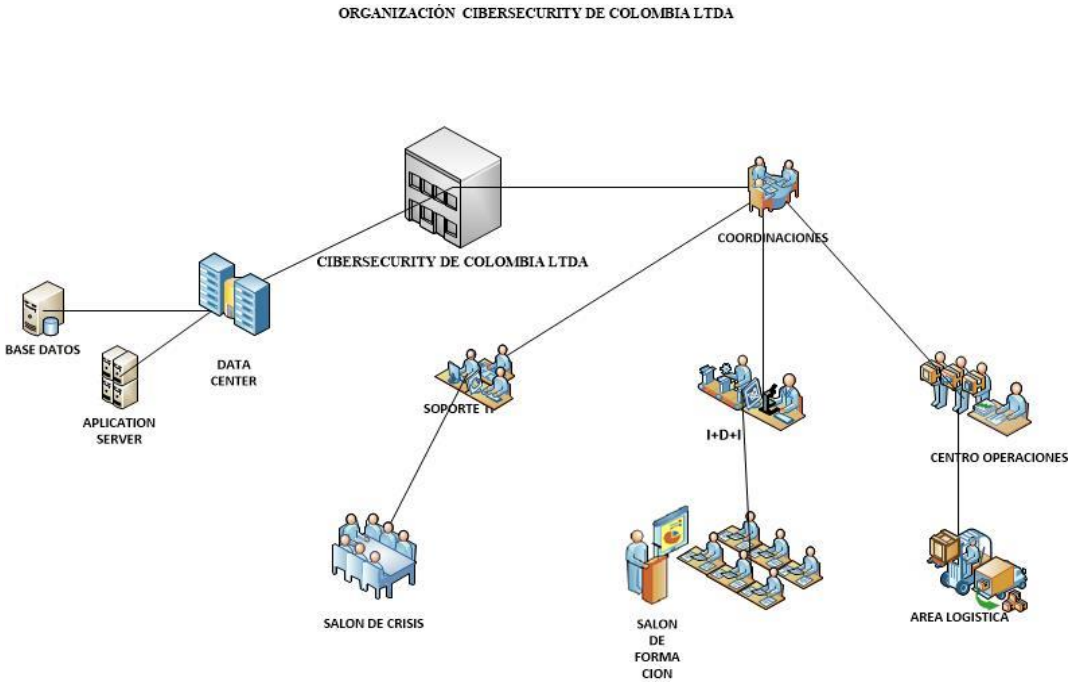
8.3 PROCEDIMIENTO, MEJORES PRÁCTICAS Y CONFIGURACIONES

8.3.1 Organigrama del CSIRT propuesto

De acuerdo con el procedimiento, se realiza la estructuración y diagrama que tendrá el equipo de respuesta proyectado en el presente proyecto y el cual es el siguiente y mediante el cual se pretende alcanzar los objetivos propuestos.

Es de vital importancia realizar esta definición y estructuración con el fin de evitar errores en la proyección, evitando así vacíos y falta de infraestructura y equipos al momento de su materialización.

Figura 19. Organización Organigrama funcional del CSIRT propuesto.



Fuente: Software de diseño Visio demo 30 días, Omar Tique M., mayo de 2020

8.3.1.1 Centro de Datos (Data Center)

Se define como el lugar físico donde se aloja la infraestructura de tecnología de la información, tales como equipos servidores, equipos activos de red (routers, switchs, firewalls, planta telefónica, etc.), es el centro de operaciones del componente tecnológico en cualquier organización o empresa.

8.3.1.2 I+D+i.

Hace referencia al componente dentro de una organización, específicamente a la **Investigación, desarrollo e innovación**, siendo este un nuevo concepto adaptado a los estudios relacionados con el avance tecnológico e investigativo centrados en el avance de la sociedad, siendo una de las partes más importantes dentro de las tecnologías informativas[43]. (http://www.plannacionalidi.es/que-es-idi/) (Innovación, 2013)

[43] Plan Estatal de Investigación Científica y Técnica y de Innovación 2013-2016. {en línea}. España. Disponible en: http://www.plannacionalidi.es/. Fecha de consulta 23 de septiembre de 2019.

8.3.1.3 Centro de Operaciones Seguridad (SOC)

Es el conjunto de soluciones complementarias, modulares y escalables diseñadas para brindar a los clientes la capacidad de anticipar, detectar y responder a amenazas avanzadas, junto con soluciones robustas para mitigar los riesgos y una administración eficiente de sus clientes con vulnerabilidades TIC[44]. (Killcrece, Kossakowski, Ruefle, & Zajicek , December 2003)

Las siguientes son las herramientas de plataforma con las que debe contar un centro de operaciones de seguridad:

Router. Equipo activo de red usado a nivel de infraestructura física y que permite la interconexión de redes lógicas a través de sus interfaces, actuando estas como Gateway a través de una dirección IP única que identifica el segmento de red de esta.

Switchs. Equipo activo de red usado a nivel de infraestructura física y que permite la interconexión de equipos a nivel físico y lógico en una red interna (LAN), también es posible separar los segmentos de red configurando Vlans en este tipo de equipos cuando son 100% administrados.

Firewall. Sistema que puede ser implementado mediante el uso de hardware o software, la combinación de ambos y que permite realizar la configuración de reglas con el objeto de que se pueda acceder o no a un sitio we o aplicación específica y usado en la prevención de ataques informáticos e intrusiones a la red.

Sistemas IDS/IPS. Soluciones de aplicaciones y herramientas configuradas orientadas a la prevención de intrusiones desde la red pública (Internet) a una red interna (Intranet) en una infraestructura tecnológica que soporta una empresa o institución. Funciona como detección y prevención de instrucciones, de acuerdo con su configuración y las necesidades específicas de cada usuario (David Tejada Rentería, 2016).

Sistema de UTM. Sistema implementado al interior de una empresa para protección de su infraestructura, formado por la combinación de hardware y software, orientada la administración unificada de amenazas de la red; esto es formado por firewall, IDS/IPS, antivirus, etc.

---

[44] Organizational Models for Computer Security Incident Response Teams (CSIRTs). Killcrece, Georgia; Kossakowski, Klaus-Peter; Ruefle, Robin; Zajicek, Mark. Copyright 2004. Carnegie Mellon University. Pittsburgh. 2003 December. p.

Sistemas Final (Usuarios). Aquellos orientados a la satisfacción de una necesidad especifica de clientes, que bien puede consumir servicios o productos, y mediante estos interactúa con la empresa o compañía, bien puede ser un sitio web, una VPN, o cualquiera otra tipa se servicio.

Servidores de Aplicaciones. Equipos que permiten ser configurados como servidores y en los cuales se instala y configura sistemas que permiten la interacción de forma externa y a través de internet tanto de empleados como clientes con la empresa o institución.

8.3.1.4 Soporte TI

Para lograr tener la definición del tipo de soporte que se va a proveer a los clientes se hace necesario tener en cuenta la cantidad de clientes y la forma que realizan los aportes y si es proporcional con el tipo de soporte y las horas por semana; inicialmente es posible realizar una clasificación a este servicio el cual puede contener determinados servicios del portafolio completo, dada esta circunstancia pueden existir tres opciones como tal.

Servicios de Nivel Básico

Los servicios que pueden ser prestados (soporte técnico) han de ser los que se relacionan a continuación o se acuerde con el cliente en el respectivo contrato y estar con toda la disposición para hacerlo, contando con el personal capacitado e idóneo y hacer frente a los eventos de seguridad.

Monitoreo y Alerta 24×7
Registros de Recolección y Correlación SIEM
Reglas de Casos de Uso
Portal Web SOC
Inteligencia de Amenazas

Servicios de Nivel Estándar

Solo aquellos que son prestados en primera línea como respuesta a una instrucción, preventivos y de contención en un momento dado, se monitorea y realiza una evaluación en el momento en que ocurre el evento.

Monitoreo y Alerta 24×7
Registros de Recolección y Correlación SIEM
Reglas de Casos de Uso
Portal Web SOC
Inteligencia de Amenazas
Eventos Críticos

Anti-Phishing
Protección eBanking
Servicio de Respuesta a Incidentes Cibernéticos
Pruebas de Penetración / Servicios de Intrusión
Ingenieros Nocturnos
Evaluación de Vulnerabilidad Automática
Gestión de Dispositivos de Seguridad

Servicios de Nivel Superior

En este tipo de servicios además de lo anterior suelen incluir la investigación, los servicios de informática forense, desplazamiento de personal especializado que realice la investigación y llego el caso la recolección, preservación de evidencia, su análisis y la presentación ante un estrado judicial.

Monitoreo y Alerta 24×7
Registros de Recolección y Correlación SIEM
Reglas de Casos de Uso
Portal Web SOC
Inteligencia de Amenazas
Eventos Críticos
Anti-Phishing
Protección eBanking
Servicio de Respuesta a Incidentes Cibernéticos
Pruebas de Penetración / Servicios de Intrusión
Evento de Seguridad Forense
Equipo Dedicado en el Sitio
Ingenieros Nocturnos
Evaluación de Vulnerabilidad Automática
Gestión de Dispositivos de Seguridad
Gestión Proactiva del Cambio
Servidor de Aplicaciones Web y Servicios Anti-DDoS

8.3.1.5 Coordinaciones

Este servicio es provisto principalmente por el personal centralizado del CSIRT. Como punto focal para el análisis y la respuesta a incidentes, coordinan las actividades de los miembros del equipo distribuido para responder a los eventos y actividades de toda la empresa. Los miembros del equipo distribuido, a su vez, confirman que los administradores locales han implementado las acciones apropiadas y transmiten esta información al equipo centralizado.

El personal centralizado también actúa como enlace con otros CSIRT externos, expertos en seguridad y sitios con los que el CSIRT podría necesitar contactar o

colaborar. El CSIRT es el principal punto de contacto para todo trabajo de incidentes y vulnerabilidades. También son el enlace con el asesor legal, los recursos humanos, la alta dirección y cualquier otro grupo organizativo que se ocupe de los problemas de seguridad[45]. (West-Brown, y otros, First release: December 1998, 2nd Edition: April 2003).

8.3.1.6 Área Logística

En razón a que se hace necesario realizar el acompañamiento y apoyo al equipo del CSIRT, se incorpora un grupo logístico que se encargue de las necesidades frente a la realización de sus actividades y cumplimiento de los objetivos, esto especialmente referido a lo que tiene que ver con lo siguiente:

La logística está referida a la satisfacción de las necesidades del personal de ingenieros de soporte y especialistas, que permiten el cumplimiento de funciones y la ejecución de actividades propias de acuerdo con su cargo y perfil, tanto dentro de la oficina como fuera de ella, entonces es absolutamente necesario contar con un lugar en donde funcionar (instalaciones físicas), dotada con los equipos y accesorios de oficina, equipos de cómputo de escritorio y portátiles, así como también un lugar específico en donde permita ser resguardados los equipos que soportan la aplicaciones y herramientas de monitoreo, contención, investigación, recolección de evidencia y equipos que permitan soportar la conectividad de los usuarios y acceso a herramientas y bases de datos.

Además, debe contar con infraestructura que permita realizar pruebas de concepto o laboratorio de los desarrollos o herramientas nuevas antes de ser puestas en producción y como tal también los medios de comunicaciones que ´permitirán al personal interactuar entre ellos y sus clientes en la toma de decisiones y atención cuando sea requerido.
Los miembros distribuidos y segregados del equipo utilizan equipos informáticos, teléfonos, buscapersonas, etc. Que puedan hacer parte de la infraestructura de la organización o que se adquieran para el uso exclusivo en del CSIRT. El área de apoyo logístico debe en cualquier caso satisfacer estas necesidades, las de acceso a teléfonos seguros, correo electrónico e intranet/extranet para poder comunicarse de manera efectiva y segura con el equipo centralizado.

8.3.1.7 Salón de Formación

[45] Handbook for Computer Security Incident Response Teams (CSIRTs) First release: December 1998, 2nd Edition. West-Brown, Moira J.; Stikvoort, Don; Kossakowski, Klaus-Peter; Killcrece, Georgia; Ruefle, Robin; Zajicek, Mark. The Software Engineering Institute. Pittsburgh, U.S. 2003 April. p.

Grupo encargado de la formación y de la sensibilización de su propio personal a nivel interno, de igual forma de la educación o capacitación para sus suscriptores. Esto implica el desarrollo de clases de capacitación sobre seguridad informática y respuesta a incidentes, creación de tutoriales sobre los tipos de ataque y estrategias de mediación, realizar investigaciones sobre las tendencias de incidentes y vulnerabilidades que presentan los sistemas.

8.3.1.8 Salón de crísis

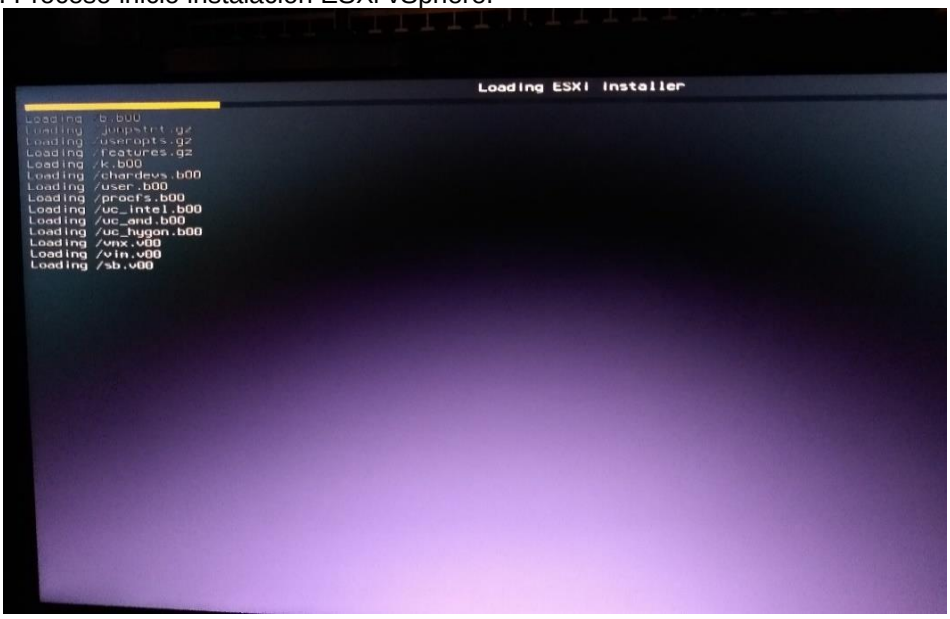
Conformado por el grupo de especialistas del CSIRT quienes tienen la responsabilidad de analizar y decretar autónomamente el estado de un incidente de seguridad de cualquier evento presentado, allí ponen en ejecución el procedimiento al proceso de respuesta a incidentes de seguridad informática, colaboran en el procedimiento al proceso de manejo de incidentes de seguridad, teniendo claridad sobre los niveles de servicio comprometidos y ofrecidos a sus clientes, siendo proactivos en la identificación y notificación de actividades sospechosas en la infraestructura tecnología de sus usuarios, se valida, analiza y toman decisiones coyunturales frente a eventos o incidentes de seguridad informática que se presente en la plataforma tecnológica de sus usuarios.

8.3.1.9 PROCESO INSTALACIÓN ESXi VSPHERE

Finalizada la instalación de los puntos de red y la salida a los puestos de trabajo de los usuarios finales, realizada la organización de los equipos y el cableado en el rak, se procede a la preparación del equipo de cómputo para realizar la creación de máquinas virtuales y la configuración de las aplicaciones respectivas; como sistema operativo base, se ha acudido al uso del hipervisor vSphere 6.7 de VMware para poder acceder al equipo y realizar la creación de cada una de las máquinas virtuales.

Se ha elegido un equipo de cómputo como servidor dadas las circunstancias actuales que se presentan a nivel país y con alcance global sobre la pandemia que se está presentando, no fue posible la consecución de un equipo servidor de mejores características, robustez y gran desempeño, esto ha de repercutir en el normal desarrollo del presente proyecto, por la deficiencia de equipos y los altos costos de hoy día en razón a la emergencia sanitaria que se vive, sin embargo estoy haciendo uso del hypervisor de VMware ESXi vSphere versión 6.7, en Demo de 60 días de prueba, esto para alojar las máquinas virtuales que se hacen necesarias para instalar y configurar las herramientas de monitoreo y atención a los incidentes informáticos que se puedan presentar. proceso instalación en hardware de VMware ESXi vSphere versión 6.7

Figura 20. Proceso inicio instalación ESXi vSphere.



Fuente: Software VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

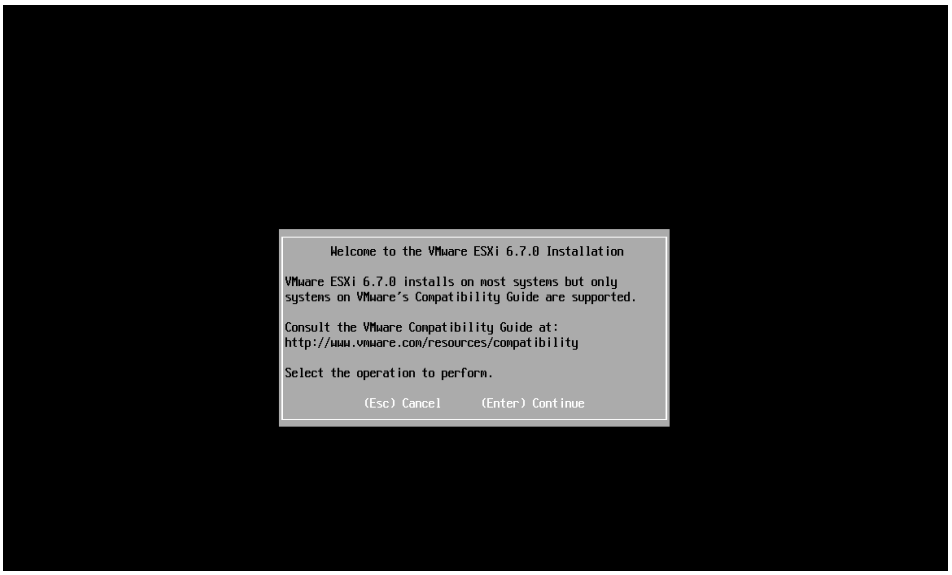
En la figura 20 se puede observar el proceso inicio de la instalación del sistema operativo base para el equipo físico el cual es VMware ESXi vSphere versión 6.7, se realiza el paso a paso guiado para la instalación y configuración del sistema operativo y poder acceder al mismo desde cualquier navegador al equipo y realizar la creación y configuración de las demás máquinas virtuales necesarias a usar en el proyecto.

Figura 21. Proceso carga normal del VMKernel.

Fuente: Software VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 21 se puede observar el proceso de cargado Exitoso del VMKernel 1, reconociendo el respectivo hardware del equipo de cómputo.

Figura 22. Proceso de bienvenida a la instalación.



Fuente: Software VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

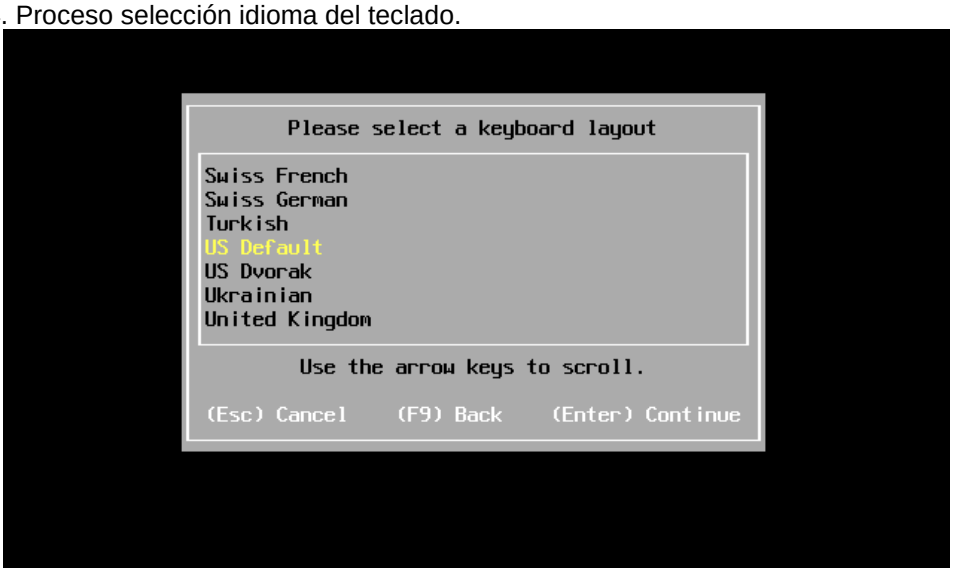
En la figura 22 se puede observar en el proceso, la interfaz de bienvenida a la instalación de vSphere en el equipo de cómputo, además la advertencia sobre la compatibilidad de la instalación y el hardware que se está usando para realizar la instalación y configuración.

Figura 23. Proceso detección almacenamiento.

Fuente: Software VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 23 se puede observar en el proceso, la detección de disco duro de nuestro equipo de cómputo (contenedor), tipo de disco, serial, modelo y la capacidad de este.

Figura 24. Proceso selección idioma del teclado.



Fuente: software VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

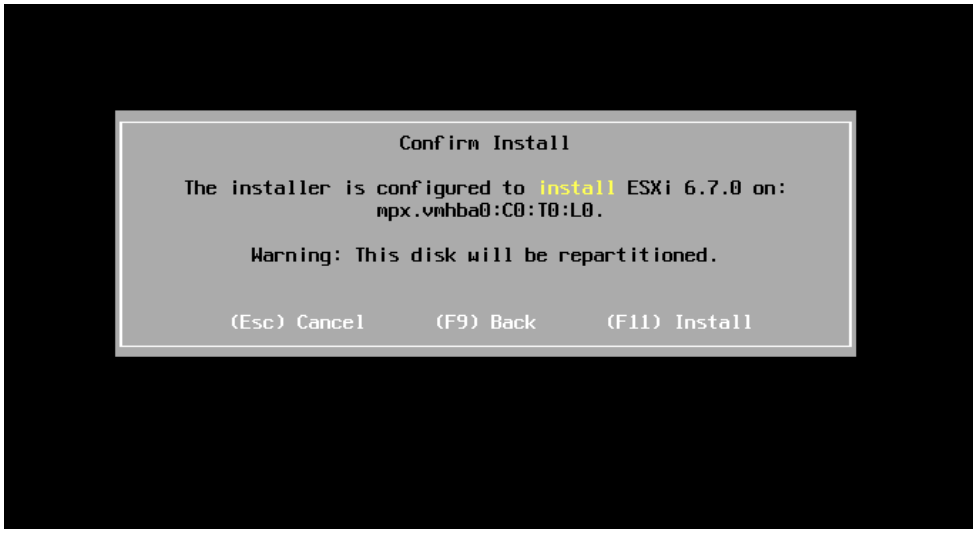
En la figura 24 se puede observar el proceso de instalación y configuración, la interfaz de selección del lenguaje que tendrá nuestro teclado, en este caso seleccionamos la opción de teclado de EE. UU.

Figura 25. Proceso de configuración password root.

Fuente: Software VMware ESXi vSphere versión 6.7, ingreso de contraseña de root, Omar Tique M., mayo de 2020.

En la figura 25 se puede observar en el proceso, la opción de configurar el Password (contraseña) de acceso al equipo que tendrá la cuenta de usuario administrador (root) y con el cual se realizará el loggin para conectarse remotamente usando cualquier navegador.

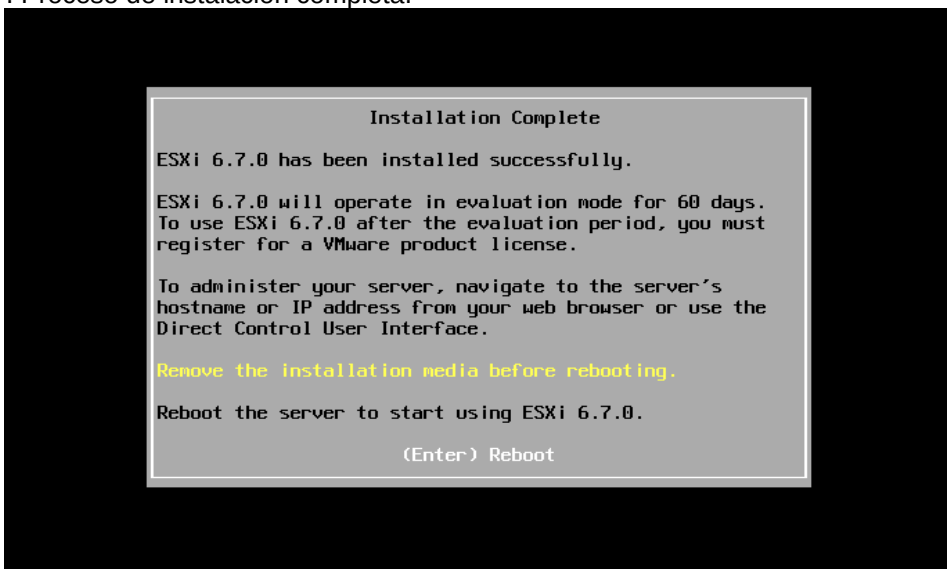
Figura 26. Proceso de advertencia de la instalación



Fuente: Software VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 26 se puede observar en el proceso, la advertencia de particionado de la unidad de almacenamiento, mostrando los identificadores del contenedor en la que se realizara la respectiva instalación del sistema operativo base, en este caso vSphere ESXi 6.7.0.

Figura. 27. Proceso de instalación completa.



Fuente: Software VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

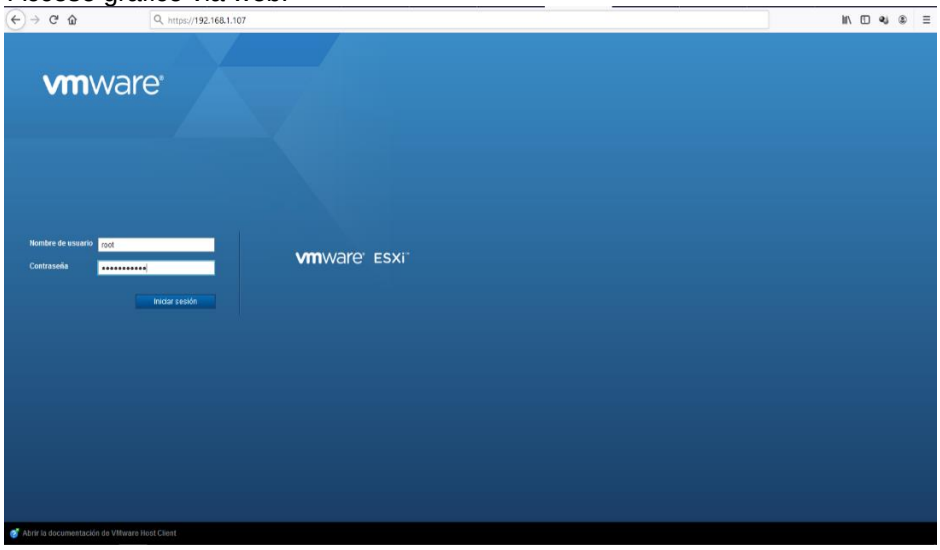
En la figura 27 se puede observar en el proceso, la instalación finalizada, la solicitud de remover los medios de instalación y la solicitud de reinicio del equipo, para completar los parámetros de configuración.

Figura 28. Proceso de carga correcta en vmkfbft.

Fuente: Software VMware ESXi vSphere versión 6.7, vmkfbft, Omar Tique M., mayo de 2020.

En la figura 28 se puede observar en el proceso, la Interfaz de vmkfbft de carga correcta, sin errores e identifica las características de hardware que tiene el equipo de cómputo en el cual se realiza el laboratorio de **CSIRT**.

Figura 29. Acceso grafico via web.

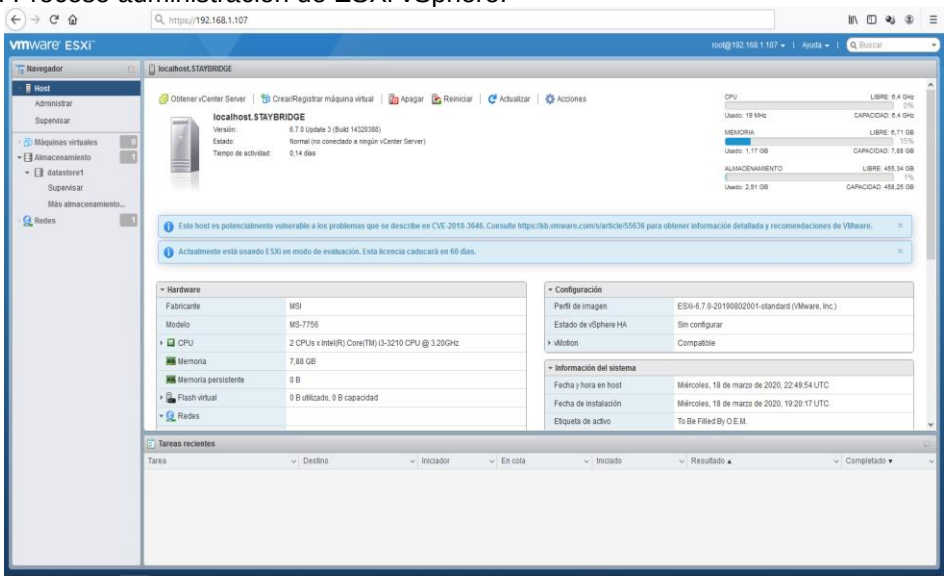


Fuente: Sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 29 se puede observar en el proceso de acceso gráfico a través del navegador web, es independiente el que se seleccione, en este caso se realiza a

través de la dirección IP que se le ha asignado a la maquina física mediante la interfaz gráfica de vSphere y las credenciales de acceso configuradas durante la instalación de forma local.

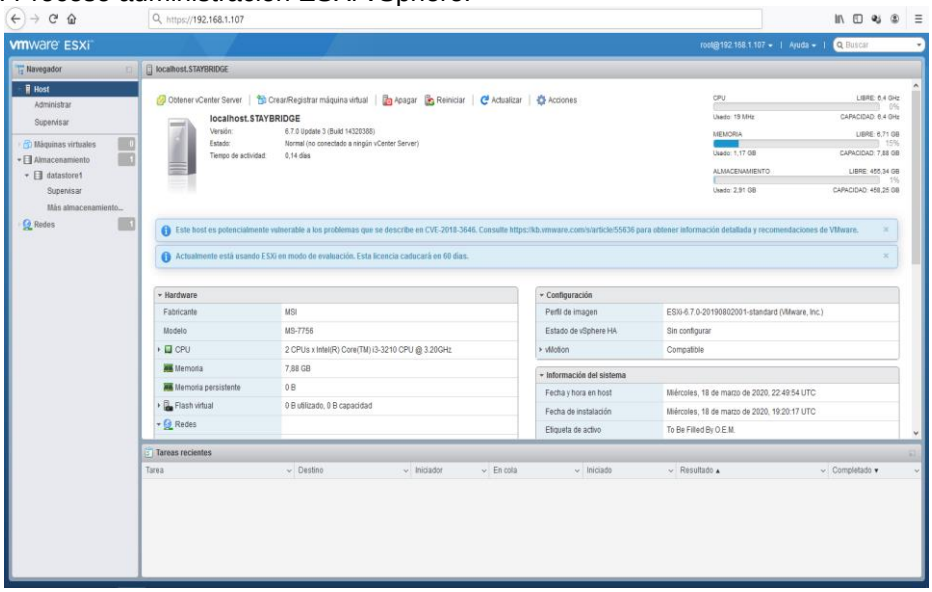
Figura 30. Proceso administración de ESXi vSphere.



Fuente: Sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 30 se puede observar en el proceso, la interfaz gráfica de bienvenida de vSphere desde donde es posible realizar las diferentes acciones de acceso a las herramientas administrativas del sistema operativo, las diferentes configuraciones solo es posible realizarlas desde esta interfaz gráfica.

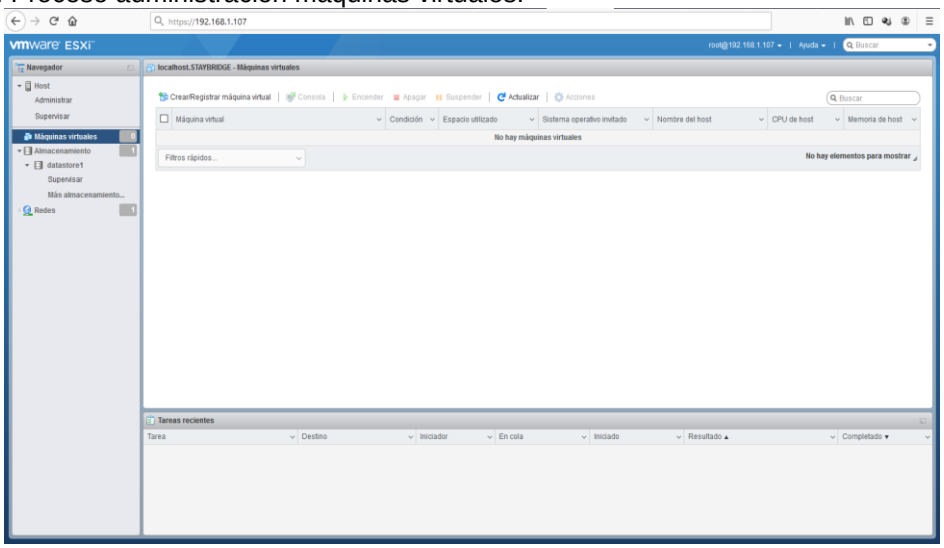
Figura 31. Proceso administración ESXi vSphere.



Fuente: Sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 31 se puede observar en el proceso, la interfaz de host en donde visualiza las características de hardware del equipo usado como servidor para el montaje de las aplicaciones más básicas que generalmente se usa al interior de un CSIRT, esto es como procesador, memoria RAM, almacenamiento y la interfaz de administración.

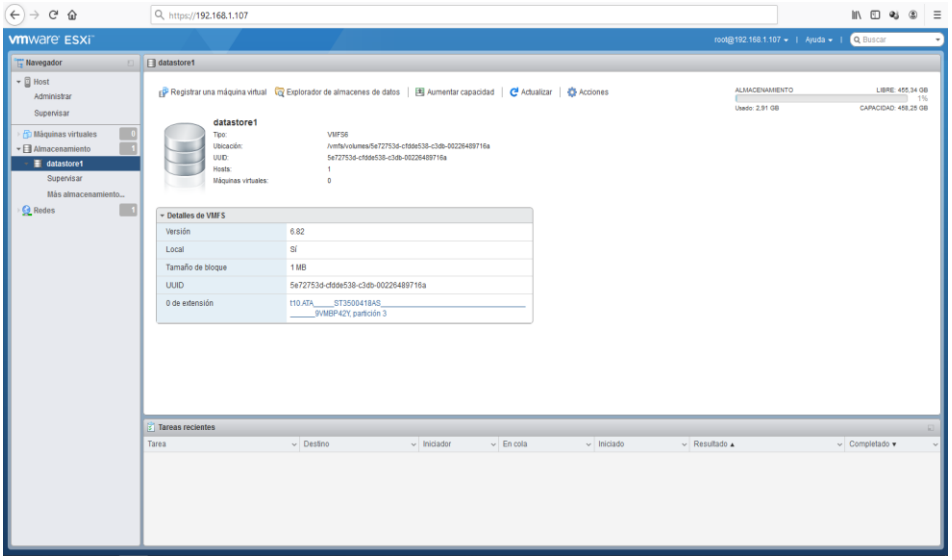
Figura 32. Proceso administración máquinas virtuales.



Fuente: Sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 32 se puede observar en el proceso, la interfaz de administración y las configuraciones de la máquina, el panel de acceso a la administración de estas, el almacenamiento y la tarjeta de red, desde este panel se realiza la administración completa de virtualización.

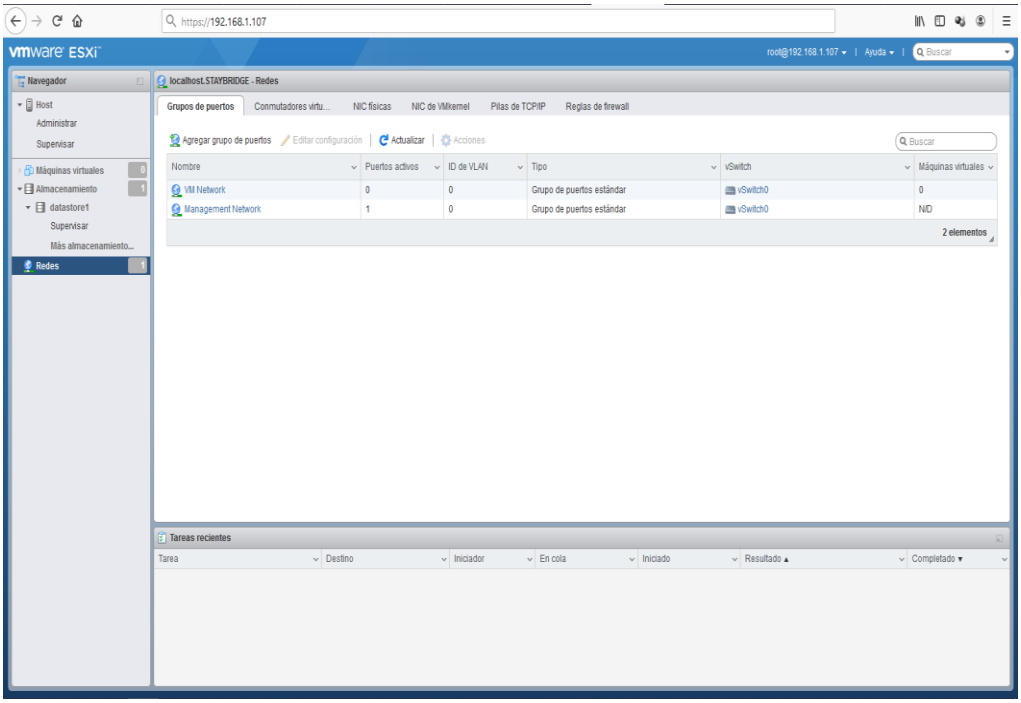
Figura 33. Proceso administración de almacenamiento en la Interfaz.



Fuente: Sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 33 se puede observar en el proceso, la interfaz de acceso a la administración de almacenamiento, especialmente la opción del explorador de almacenamiento, desde donde se puede acceder a las carpetas de archivos de máquinas virtuales y el contenido de cada una de estas.

Figura 34. Proceso administración de Red en la Interfaz.



Fuente: Sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

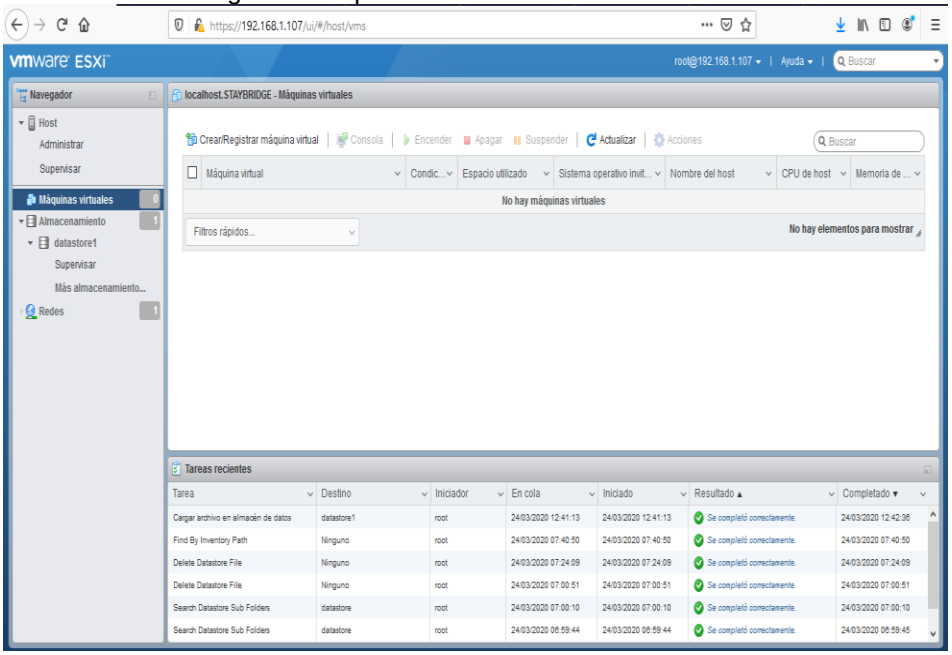
En la figura 34 se puede observar en el proceso, la interfaz de la administración y configuración de las tarjetas de red del equipo físico en el hypervisor de ESXi vSphere versión 6.7.

8.3.1.10 Proceso de creación y configuración máquinas virtuales

A continuación, se realiza la creación de la primera máquina virtual en la cual se instalará y configurará Snort, con un sistema operativo basado en Linux, en nuestro caso se hará uso de Ubuntu server 14.4 LTS.

Se ingresa a la interfaz de control de las máquinas virtuales y se busca la opción de Crear/Registrar Máquina virtual y se procede a dar click a lo cual se inicia el cuadro de dialogo asistido de la aplicación para la creación de máquinas virtuales como se sigue a continuación; del cuadro de dialogo asistido se elige “crea una nueva máquina virtual” como se puede apreciar en la figura derecha en donde se encuentra el panel de opciones.

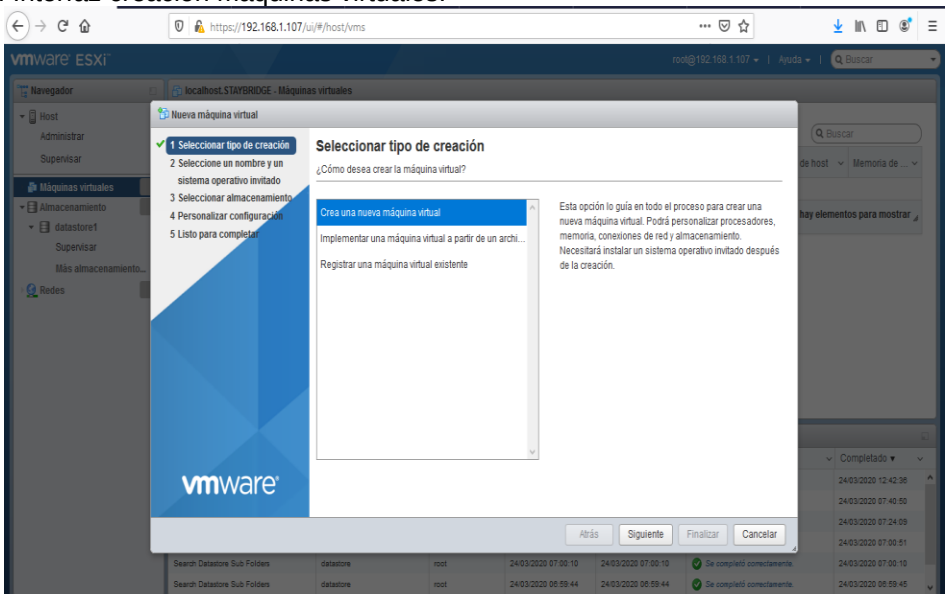
Figura 35. Proceso Crear/Registrar Máquina virtual.



Fuente: Sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 35 se puede observar en el proceso, la interfaz de vSphere desde donde se accede para realizar la creación de máquinas virtuales, configuración e instalación de sistema operativo de acuerdo con el requerimiento de cada aplicación, en este caso se ha ingresado y documenta el procedimiento realizado.

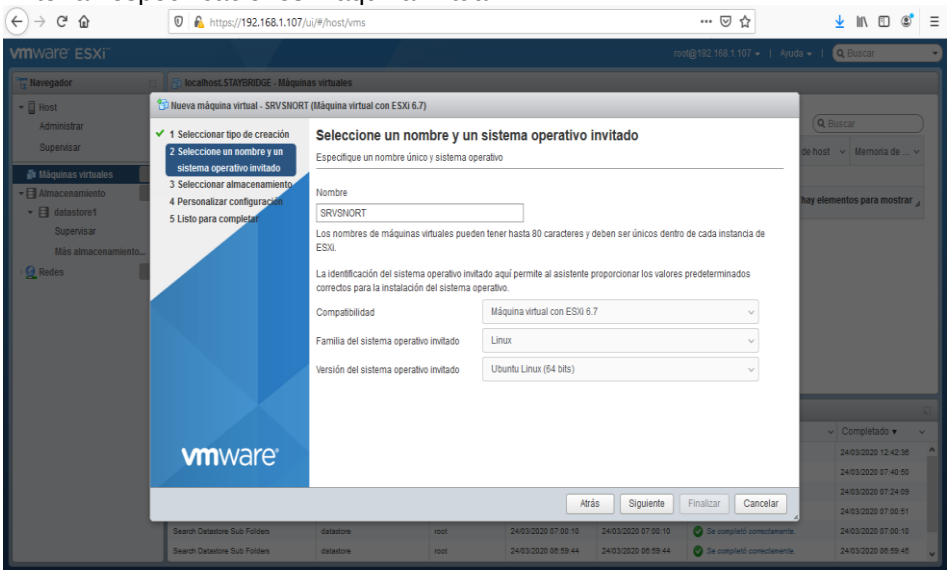
Figura 36. Interfaz creación máquinas virtuales.



Fuente: Sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 36 se puede observar en el proceso, la interfaz asistida de vSphere el inicio de la creación de máquinas virtuales de forma gráfica, se selecciona Crear una nueva máquina virtual y se selecciona la opción de **siguiente**.

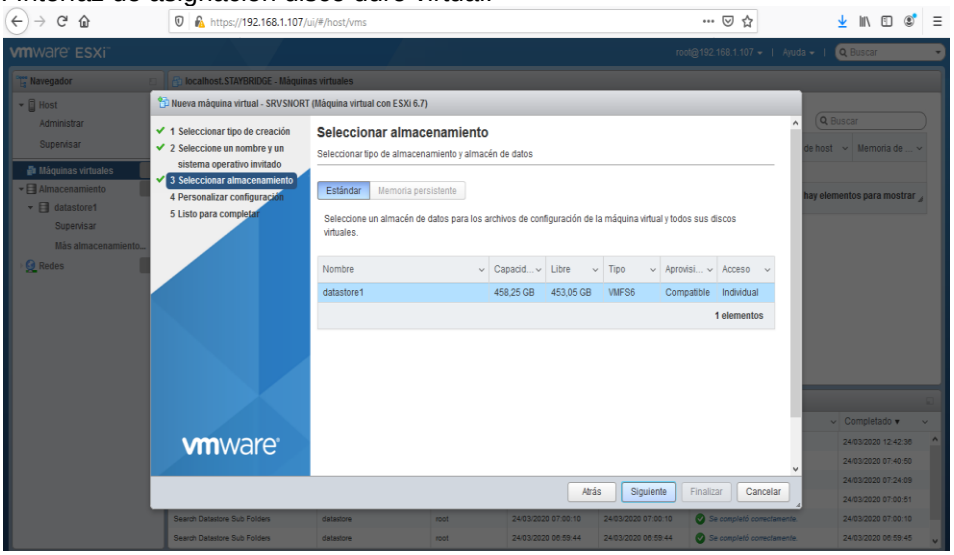
Figura 37. Interfaz especificaciones máquina virtual.



Fuente: Sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 37 se puede observar en el proceso, la interfaz asistida de vSphere que a través de esta se nombra la máquina virtual, usando la nemotecnia de **SRVSNORT**, máquina virtual para ESXi 6.7, con sistema operativo distribución de Linux y en la cuarta casilla se ha seleccionado para Ubuntu de 64 bits, entonces se selecciona la opción de **siguiente**.

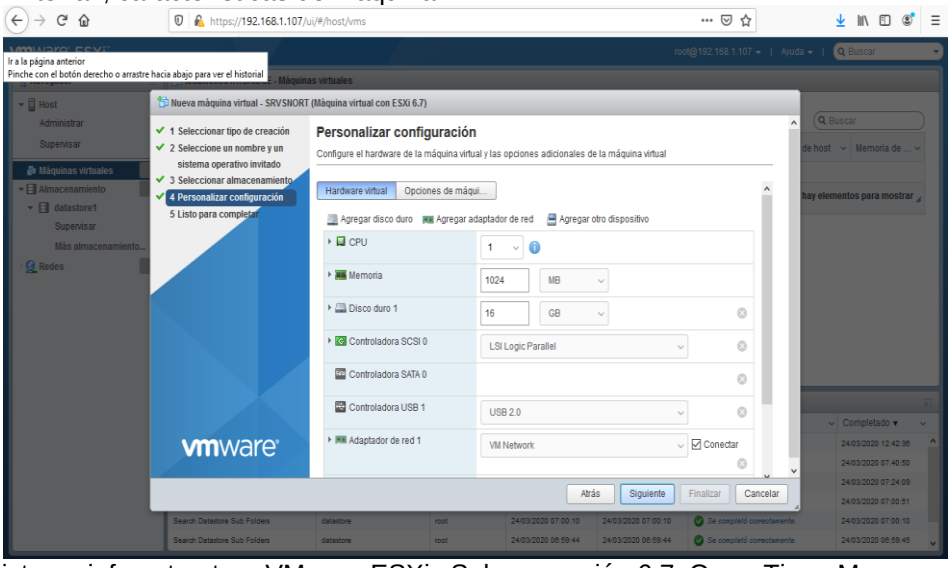
Figura 38. Interfaz de asignación disco duro virtual.



Fuente: Sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 38 se puede observar en el proceso, la opción de almacenamiento donde será alojada nuestra máquina virtual y se continua con las configuraciones previas.

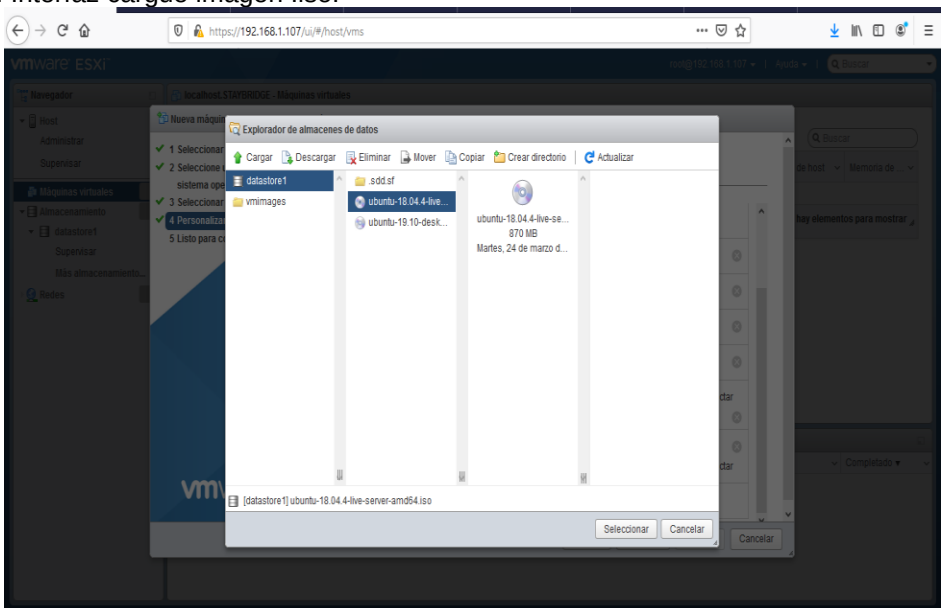
Figura 39. Interfaz, características de máquina.



Fuente: Sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 39 se puede observar en el proceso, las opciones de configuración que de la máquina virtual tales como: capacidad de almacenamiento, disco duro presentado, memoria RAM, procesador, conexión de red.

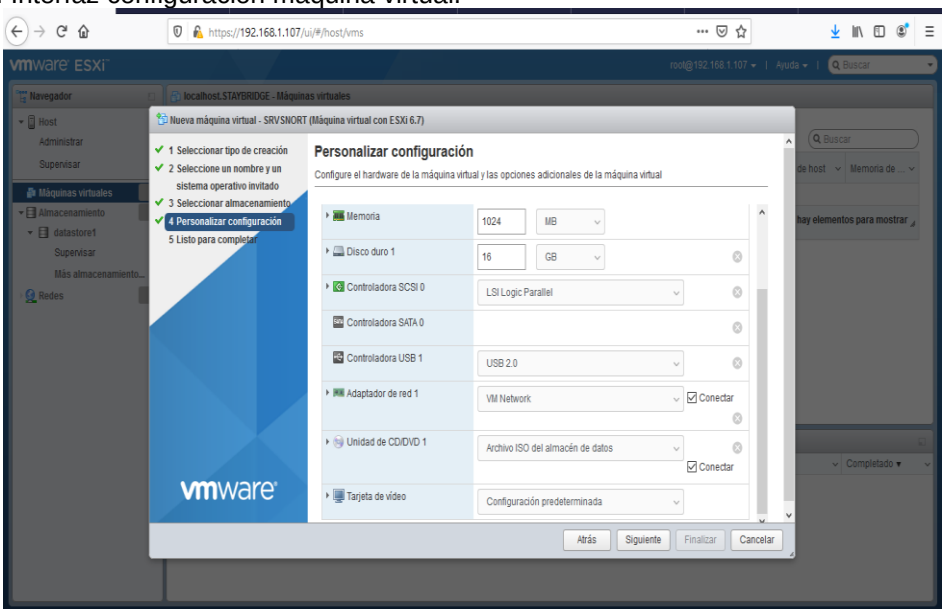
Figura 40. Interfaz cargue imagen .iso.



Fuente: Sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 40 se puede observar en el proceso, la selección realizada de la imagen .iso de sistema operativo invitado con el cual se va a iniciar la máquina virtual, para este caso Ubuntu 14.04 a 64 bits, esta se encuentra alojada en el Datastore1 del equipo de cómputo seleccionado para virtualización.

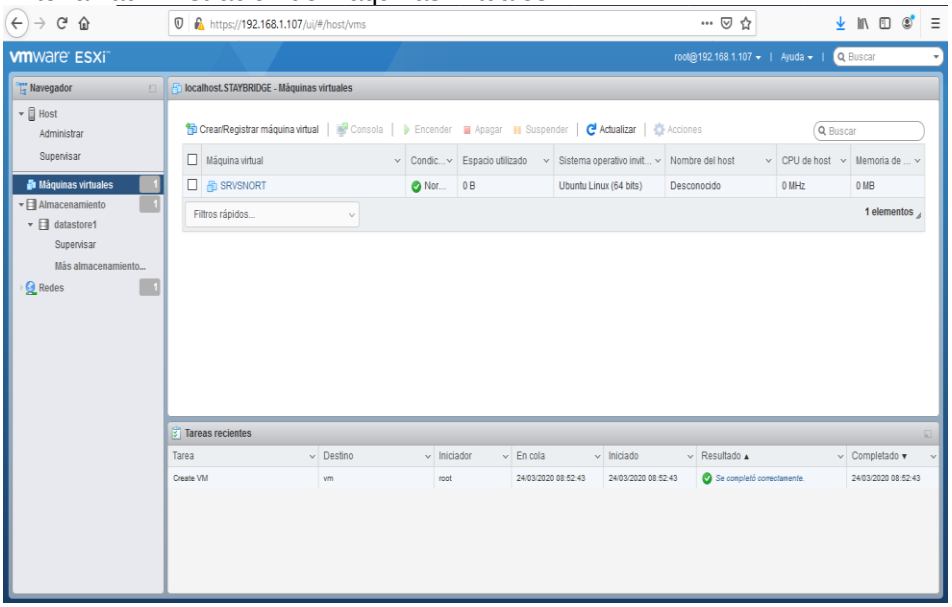
Figura 41. Interfaz configuración máquina virtual.



Fuente: Sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 41 se puede observar en el proceso, que se ha configurado la imagen .iso para iniciar la máquina e instalar el sistema operativo invitado.

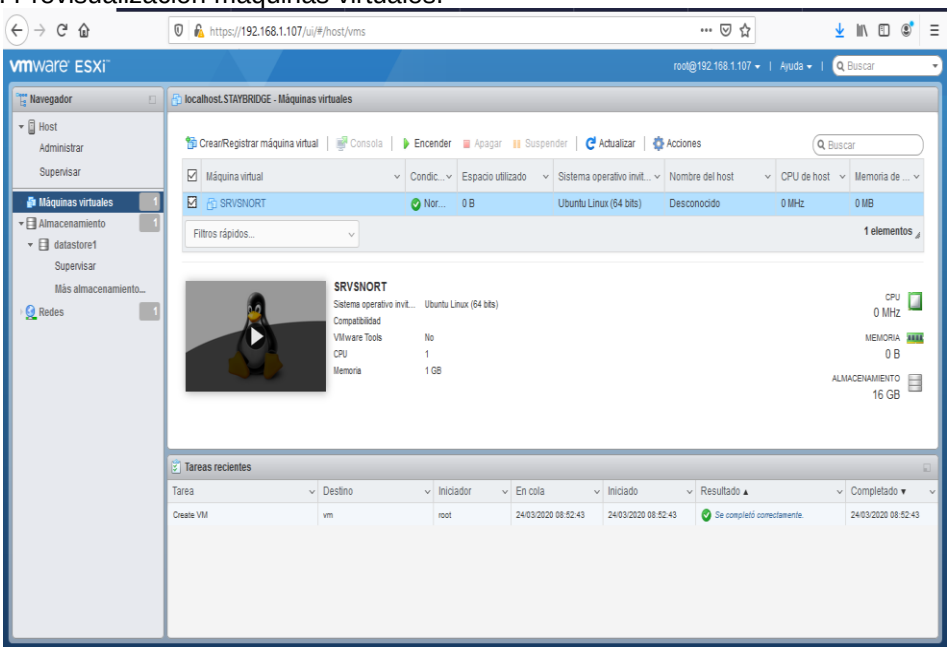
Figura 42. Interfaz administración de máquinas virtuales.



Fuente: Sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 42 se puede observar en el proceso, que se ha creado la primera máquina virtual, siendo visible en el inventario de máquinas en la interfaz de la columna derecha del hypervisor.

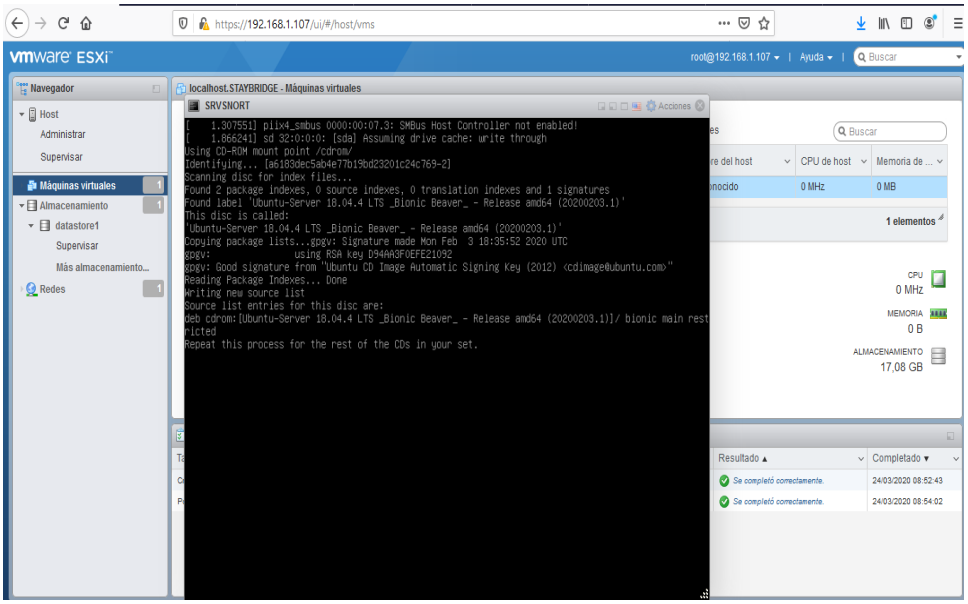
Figura 43. Previsualización máquinas virtuales.



Fuente: Sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 43 se puede observar en el proceso, la creación de la máquina, siendo visible el logo de Linux que la identifica, se procede al encendido e inicio de esta.

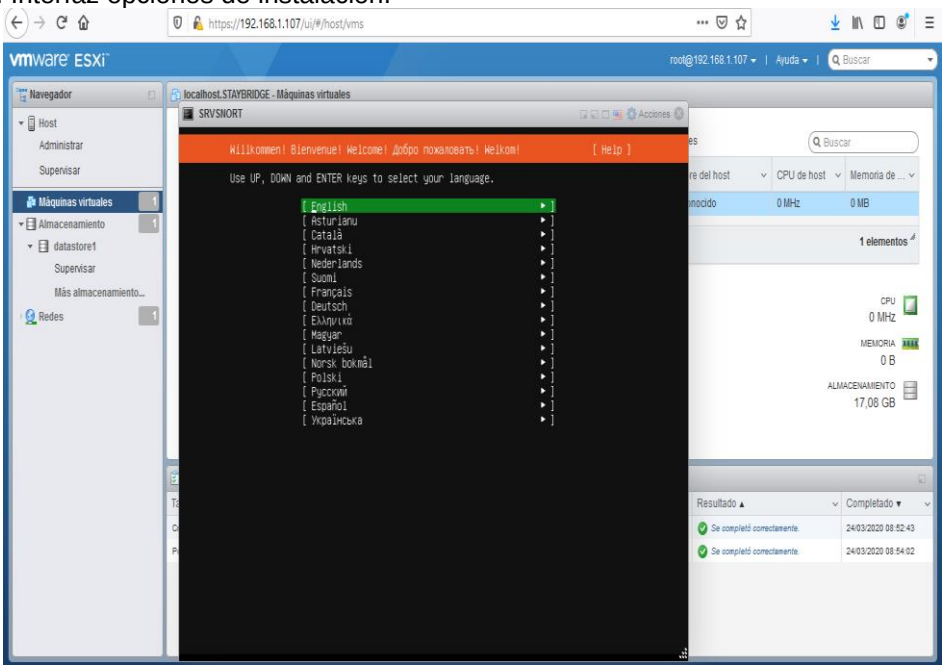
Figura 44. Interfaz instalación SO invitado.



Fuente: Sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 44 se puede observar el proceso, de inicio de la instalación del sistema operativo de Ubuntu en la cual se realizará la instalación y configuración de la herramienta de Snort.

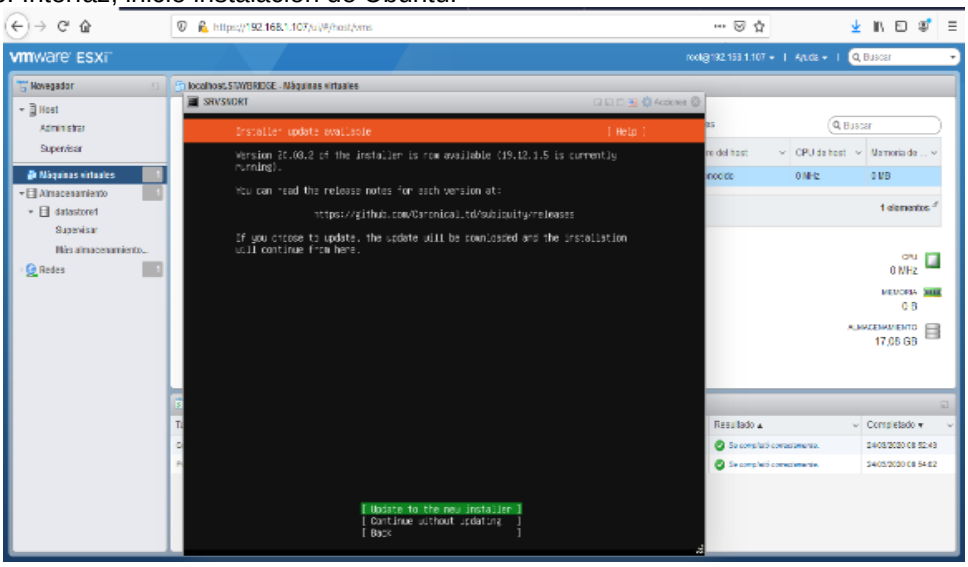
Figura 45. Interfaz opciones de instalación.



Fuente: Sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 45 se puede observar en el proceso, que se procede a realizar la selección de opciones de lenguaje que tendrá el teclado que se usará para el ingreso de información y configuraciones del sistema operativo.

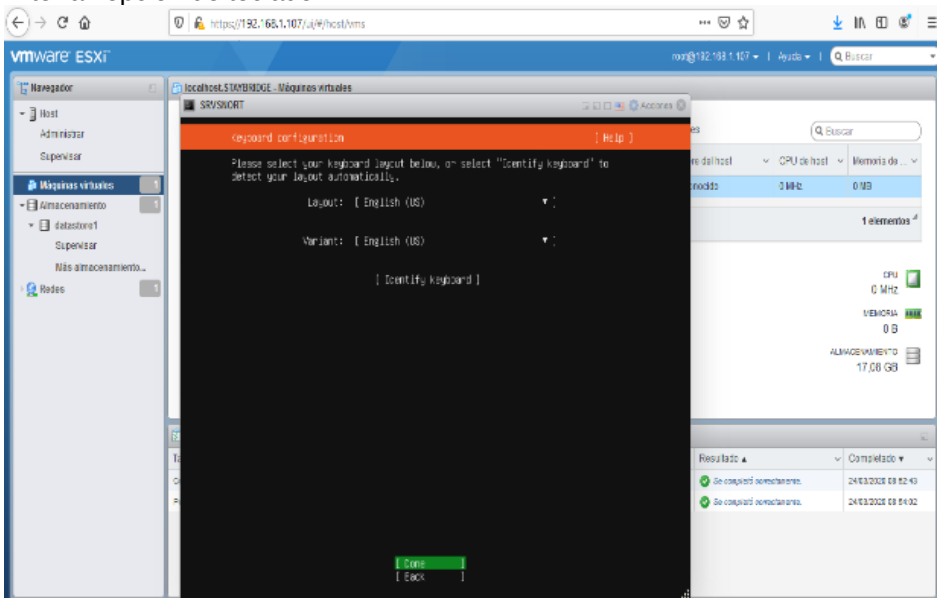
Figura 46. Interfaz, inicio instalación de Ubuntu.



Fuente: sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 46 se puede observar en el proceso, que se ha seleccionado la opción de instalar Ubuntu y se continua con las siguientes fases del proceso de instalación del sistema operativo invitado.

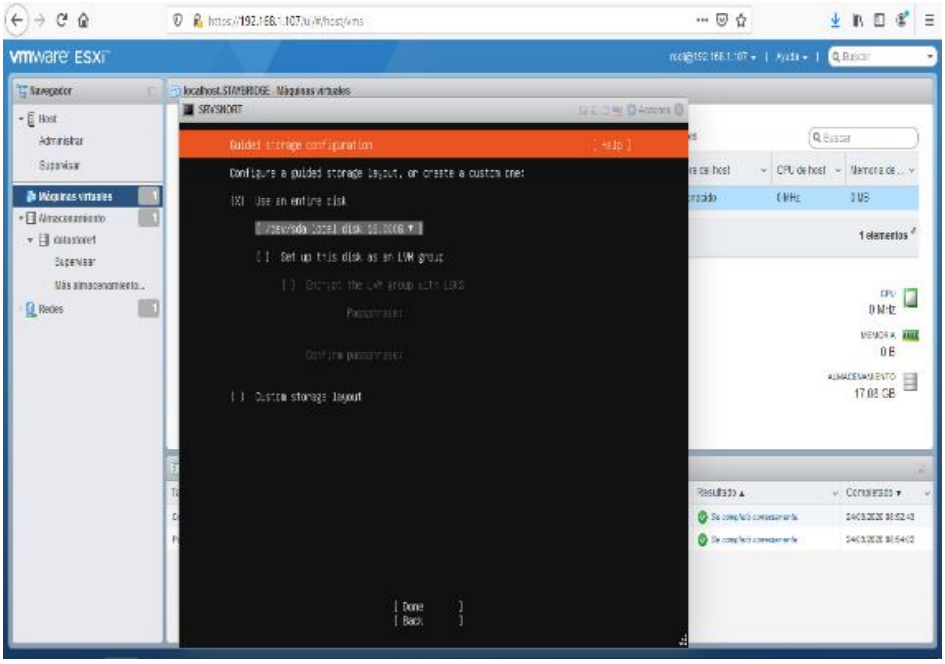
Figura 47. Interfaz opción de teclado.



Fuente: Sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 47 se puede observar en el proceso, la selección de opciones de lenguaje de disposición en el teclado y se elegido el de ingles americano.

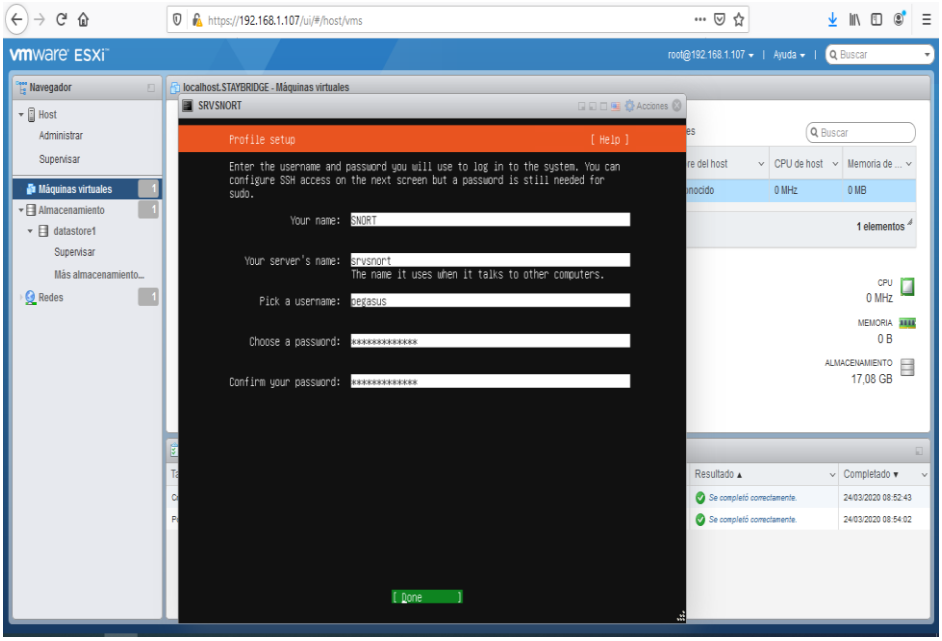
Figura 48. Interfaz selección disco duro.



Fuente: sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 48 se puede observar en el proceso, la selección de opciones de disco de almacenamiento virtual, configuración y formato, se acepta y continua con el proceso de configuración.

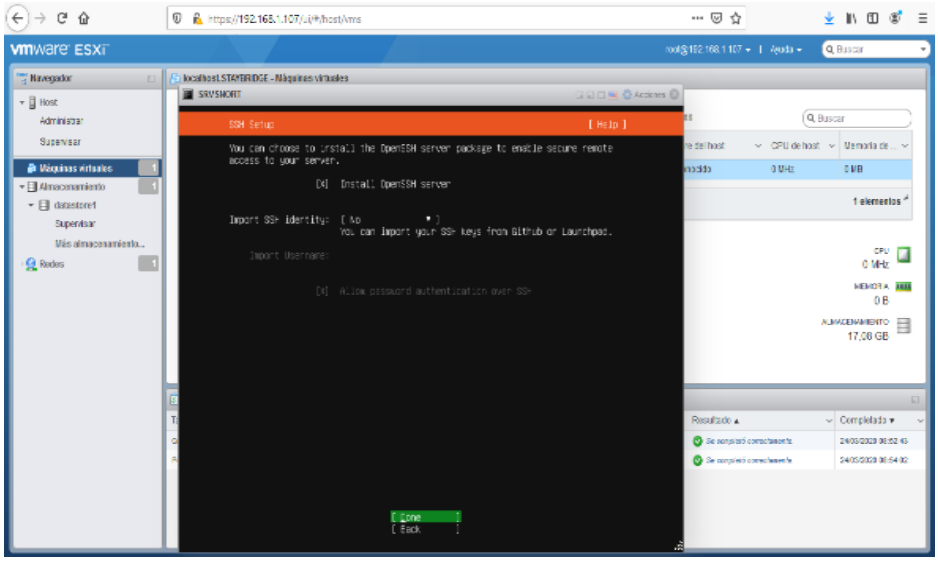
Figura 49. Interfaz de credenciales de acceso.



Fuente: sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 49 se puede observar en el proceso, la configuración de credenciales de acceso a la máquina virtual, se ingresa la información, se selecciona la opción de instalar “SSH server”, se acepta y continua con el proceso de configuración.

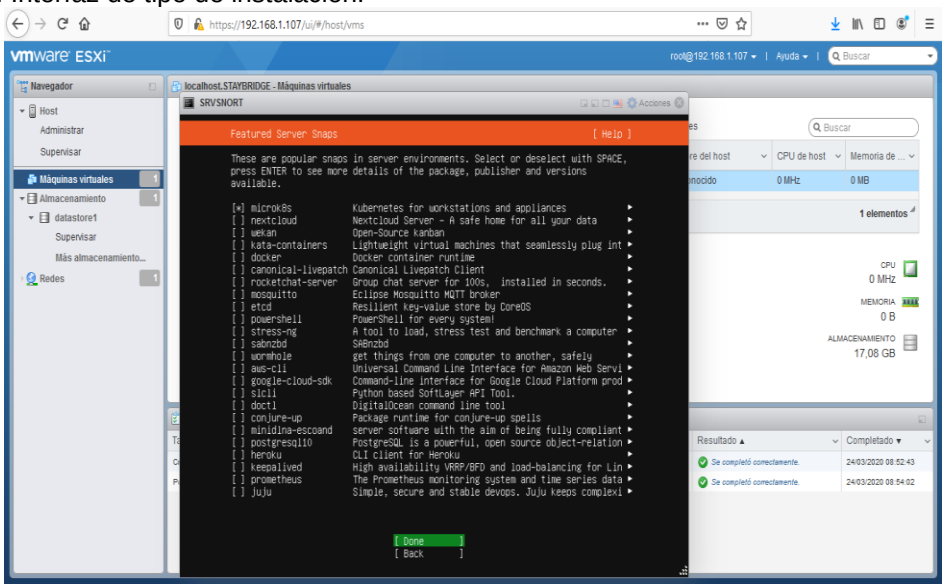
Figura 50. Interfaz instalación SSH server.



Fuente: sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 50 se puede observar en el proceso, la opción de instalar “SSH server”, se da continuar a la instalación, se acepta y continua con el proceso de configuración.

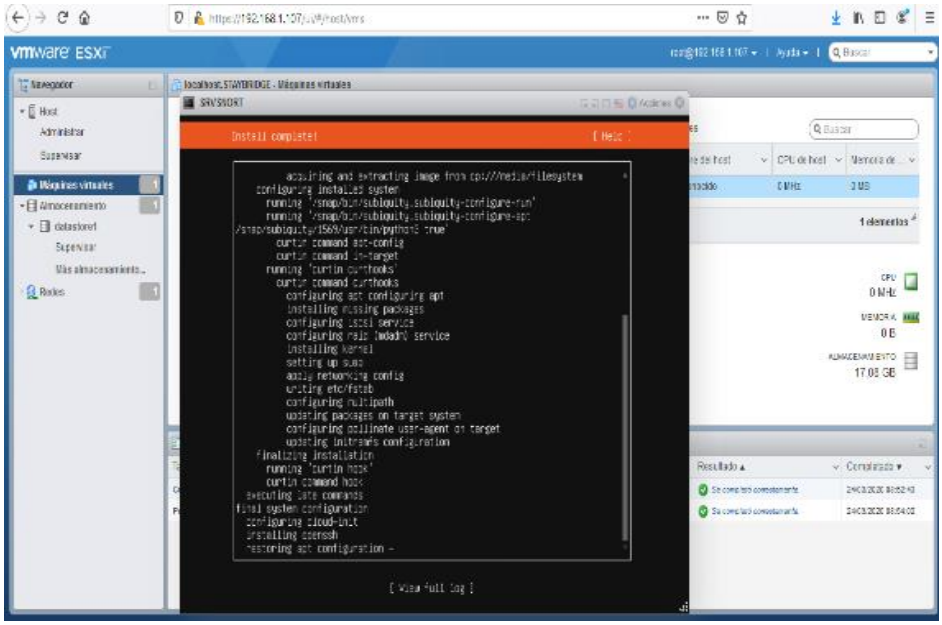
Figura 51. Interfaz de tipo de instalación.



Fuente: sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 51 se puede observar en el proceso, que se realiza la selección de la instalación que se hará, en este caso es del tipo servidor marcándose como tal, posteriormente se continua con la instalación del sistema operativo invitado.

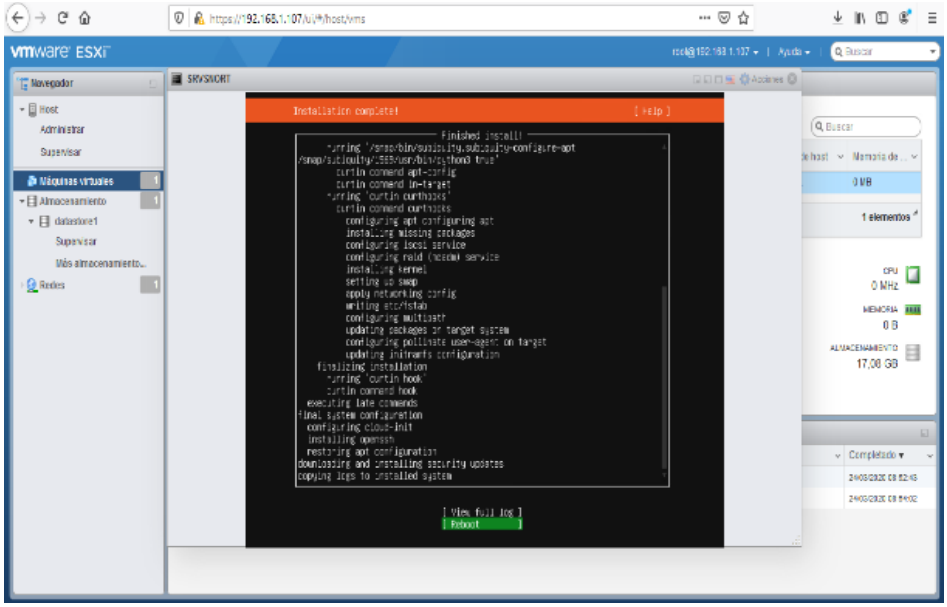
Figura 52. Interfaz de inicio instalación.



Fuente: sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 52 se puede observar en el proceso, que se ha iniciado la instalación propia del sistema operativo invitado y demás herramientas específicas de este.

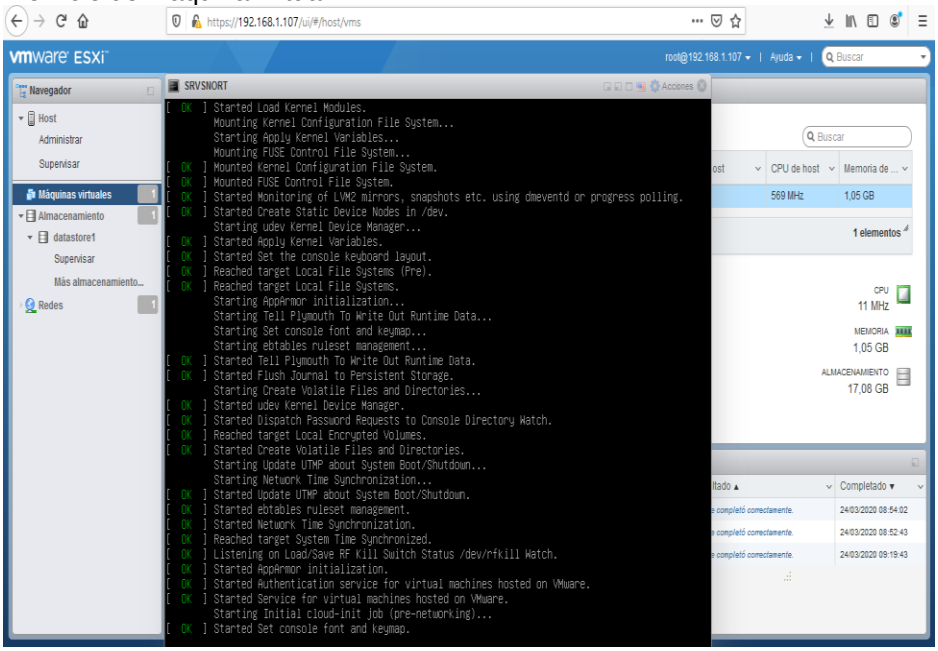
Figura 53. Interfaz de finalización instalación.



Fuente: sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 53 se puede observar en el proceso, que se ha finalizado la instalación propia del sistema operativo invitado y demás herramientas específicas de este, de igual forma se procederá al reinicio para finalizar instalación.

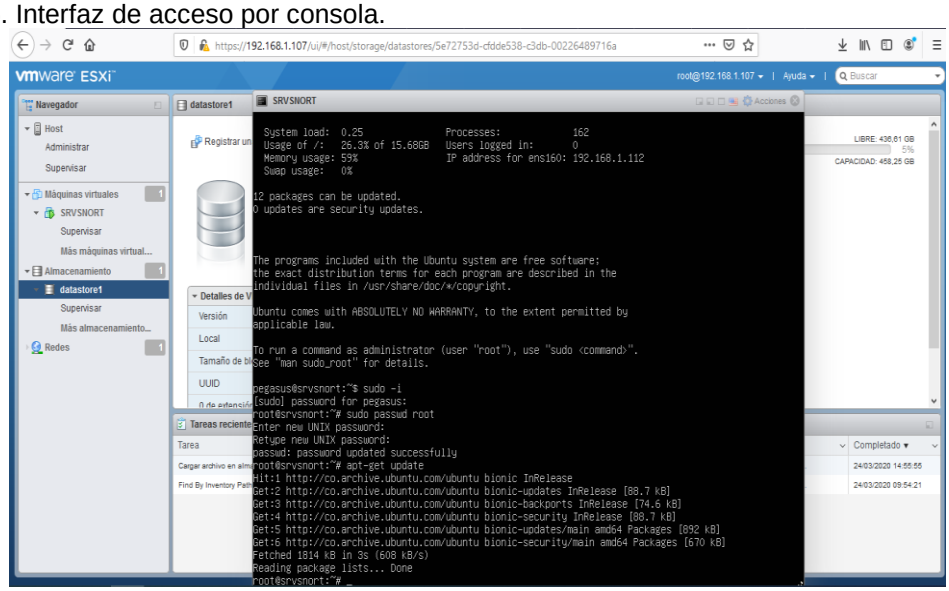
Figura 54. Reinicio de máquina virtual.



Fuente: Infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020

En la figura 54 se puede observar en el proceso, que se iniciado el reinicio y arranque de la máquina virtual creada y en la cual se instaló el sistema operativo Ubuntu server 14.04 LTS.

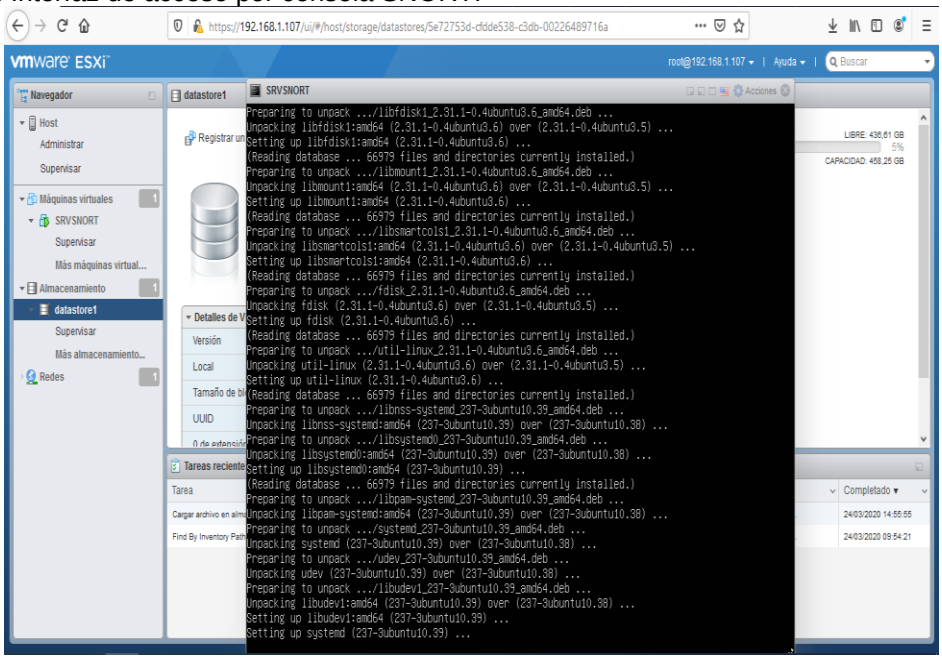
Figura 55. Interfaz de acceso por consola.



Fuente: sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 55 se puede observar en el proceso, que se ingresa mediante consola con las credenciales de acceso y se realiza la actualización del sistema operativo invitado.

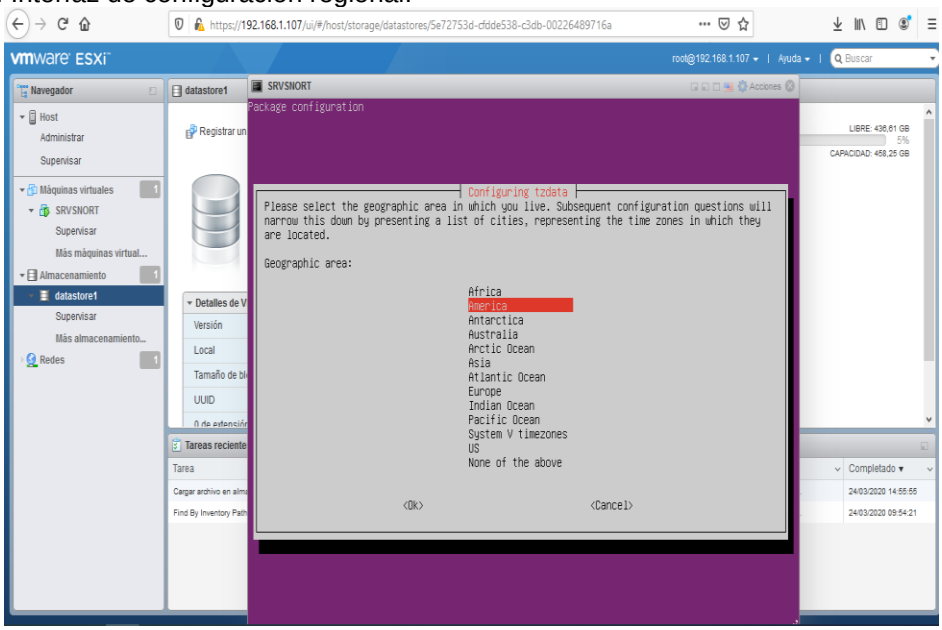
Figura 56. Interfaz de acceso por consola SNORT.



Fuente: sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 56 se puede observar en el proceso, que se ingresa mediante consola con las credenciales de acceso y se realiza la actualización del sistema operativo invitado.

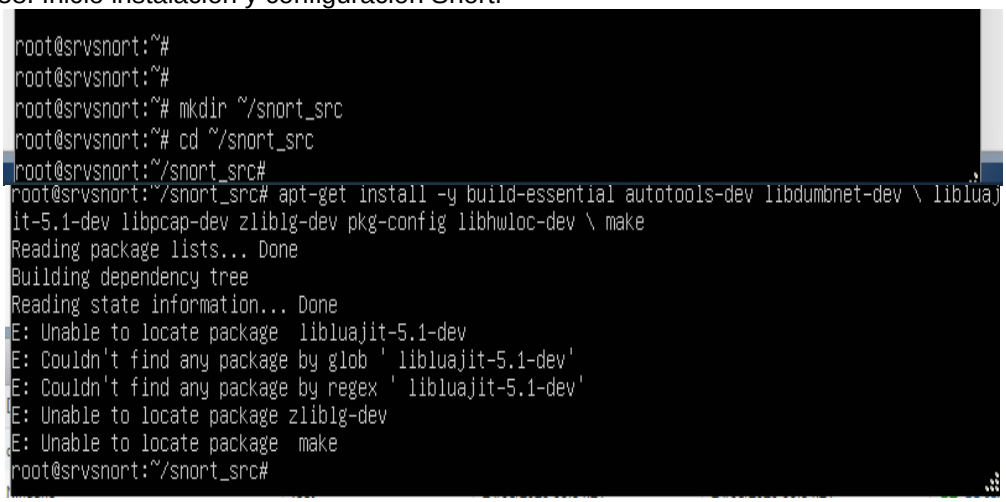
Figura 57. Interfaz de configuración regional.



Fuente: Sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 57 se puede observar en el proceso, que se reconfigura la zona horaria del sistema operativo invitado, se selecciona Bogotá.

Figura 58. Inicio instalación y configuración Snort.

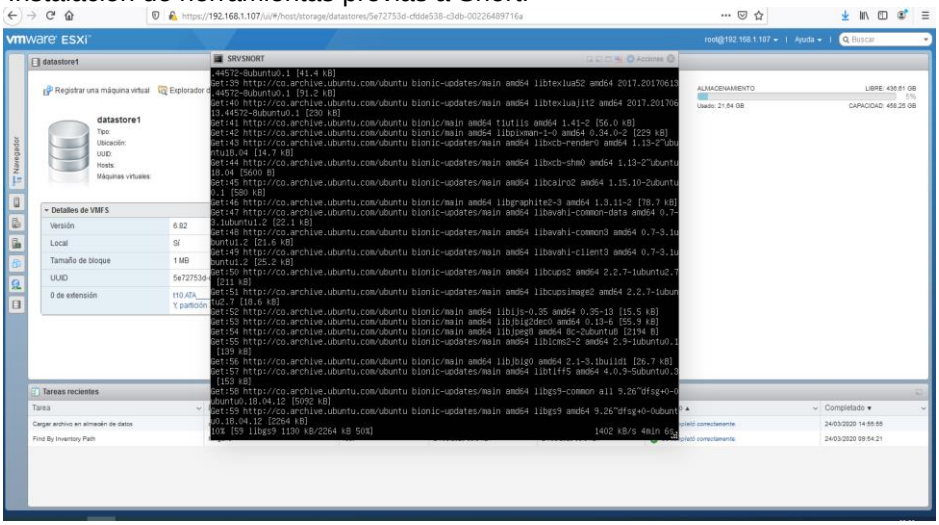


Fuente: Linux Ubuntu, creación del directorio en Snort, Omar Tique M., mayo de 2020.

En la figura 58 se puede observar en el proceso, que se inicia la instalación y configuración de la herramienta de Snort en la maquina invitada, mediante comando

de línea: creándose el directorio en donde se alojará los archivos esto es ***~# mkdir*** y posteriormente se ingresa al directorio ***~# cd ~/Snort_scr***

Figura 59. Instalación de herramientas previas a Snort.



Fuente: Linux Ubuntu, paquetes de Snort, Omar Tique M., mayo de 2020.

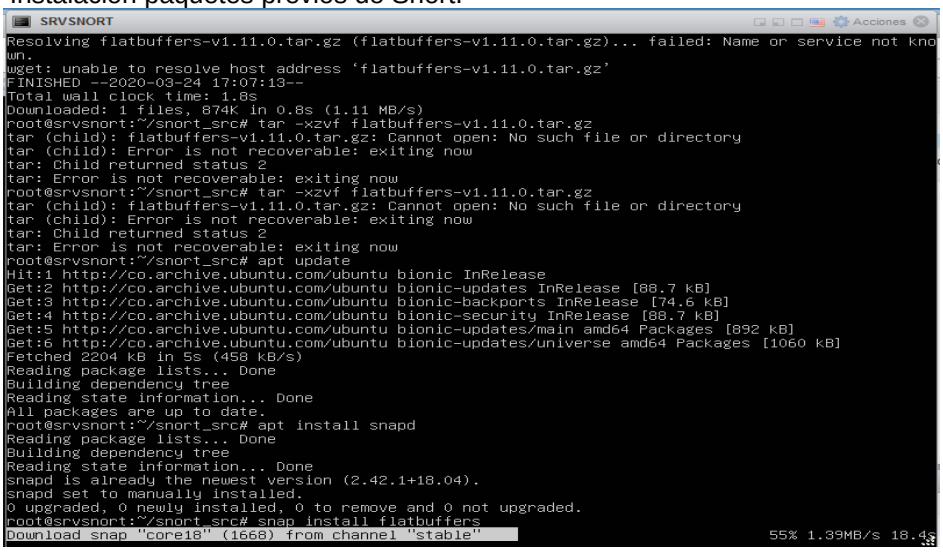
En la figura 59 se puede observar en el proceso, que se ingresa al directorio se procede con el siguiente comando para la obtención de paquetes y herramientas previas necesarias para la instalación, configuración y puesta a punto de nuestro equipo servidor; Continuando con la instalación de paquetes a través del siguiente comando, se espera obtener las librerías para Openssl que se necesita dentro de las funcionalidades de nuestro sistema IDS el cual es: ~# sudo apt-get install -y liblzma-dev Openssl libssl-dev cpputest libsqlite3-dev uuid-dev

Figura 60. Barra estado de Instalación de herramientas previas a Snort.

Fuente: Linux Ubuntu, aplicación de Snort, Omar Tique M., mayo de 2020.

En la figura 60 se puede observar en el proceso que, se realiza la instalación de Hyperscan, librerias, cmake y se puede apreciar en la barra de estado el porcentaje de instalación y finalización de descargas de paquetes.

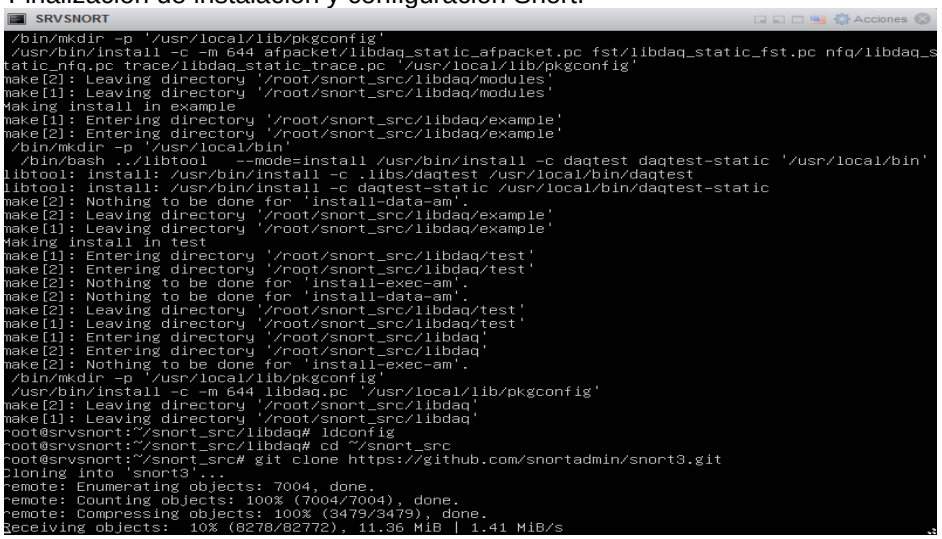
Figura 61. Instalación paquetes previos de Snort.



Fuente: Linux Ubuntu, aplicación de Snort, Omar Tique M., mayo de 2020.

En la figura 61 se puede observar en el proceso, la obtención e instalación de los paquetes de snap, estas son herramientas previas necesarias para la instalación, configuración y puesta en funcionamiento de la herramienta de Snort en el equipo servidor.

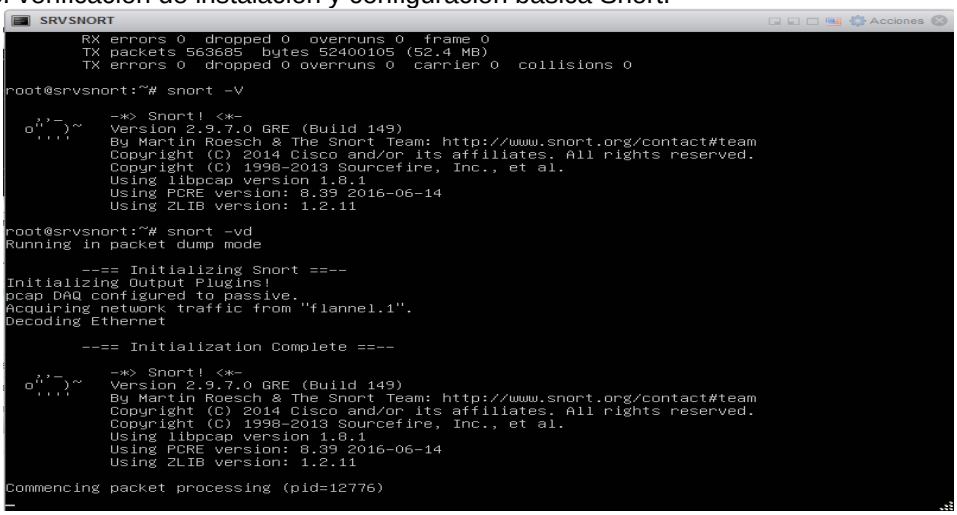
Figura 62. Finalización de instalación y configuración Snort.



Fuente: Linux Ubuntu, aplicación de Snort, Omar Tique M., mayo de 2020.

En la figura 62 se puede observar en el proceso, la finalización de instalación de paquetes y la herramienta de Snort en el servidor que ha sido designado para realizar su configuración final y puesta en funcionamiento.

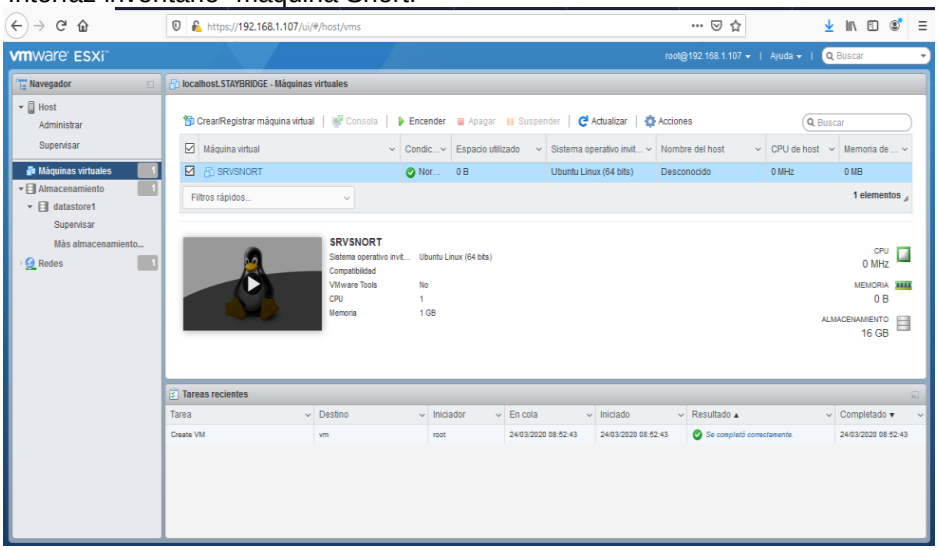
Figura 63. verificación de instalación y configuración básica Snort.



Fuente: Linux Ubuntu, aplicación de Snort, Omar Tique M., mayo de 2020.

En la figura 63 se puede observar en el proceso, que ha sido instalado el paquete de la aplicación Snort de acuerdo con los parámetros arrojados al realizar la consulta respectiva ~# Snort -V, no indicando.

Figura 64. Interfaz inventario- maquina Snort.



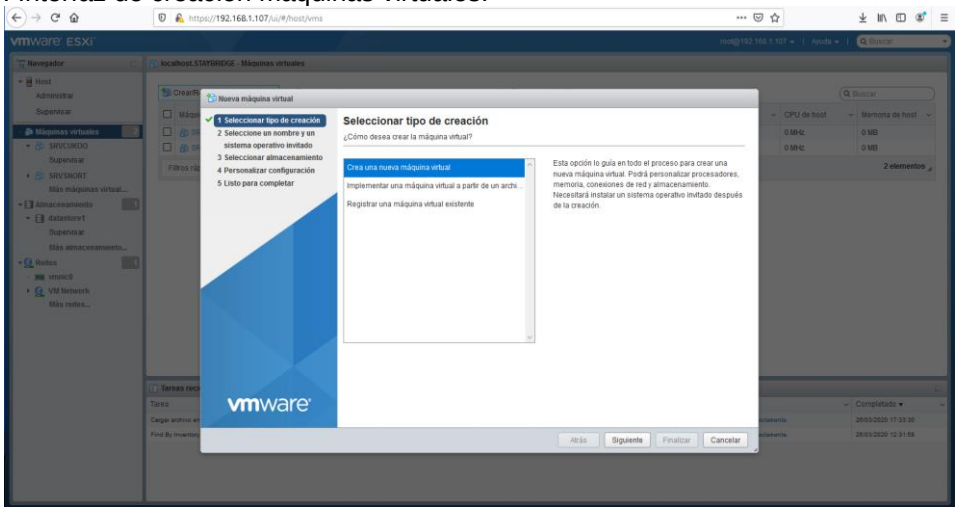
Fuente: Sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 64 se puede observar en el proceso, que ha sido instalado el paquete de la aplicación Snort, esta máquina virtual se encuentra en el inventario de ESXi vSphere y con el sistema operativo invitado funcionando.

8.3.1.11 Proceso creación máquina virtual de Alíen Vault Ossim

Para las demás máquinas virtuales residentes en nuestro equipo de cómputo se usa linux Ubuntu server 18 LTS a 64 bits, sin embargo, para la creación, instalación y configuración, así como la instalación de la herramienta de Alíen Vault OSSIM el procedimiento es distinto en función que la aplicación es embebida en el sistema operativo, se encuentra customizado, por lo tanto, se documenta la creación de la máquina virtual y la instalación de la aplicación **Alíen Vault Ossim**.

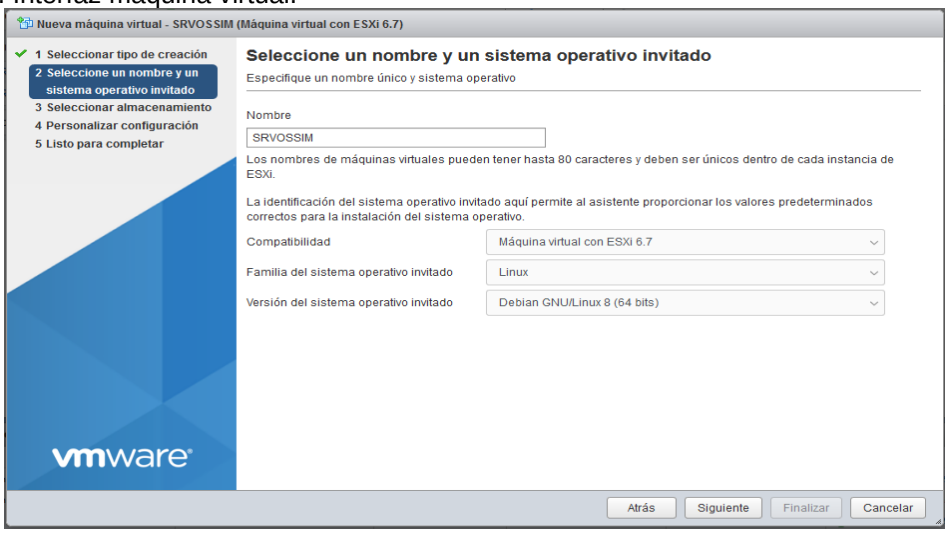
Figura 65. Interfaz de creación máquinas virtuales.



Fuente: Sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 65 se puede observar en el proceso, la interfaz asistida de vSphere el inicio de la creación de máquinas virtuales de forma gráfica, se selecciona Crear una nueva máquina virtual y se hace click en la opción de **siguiente**.

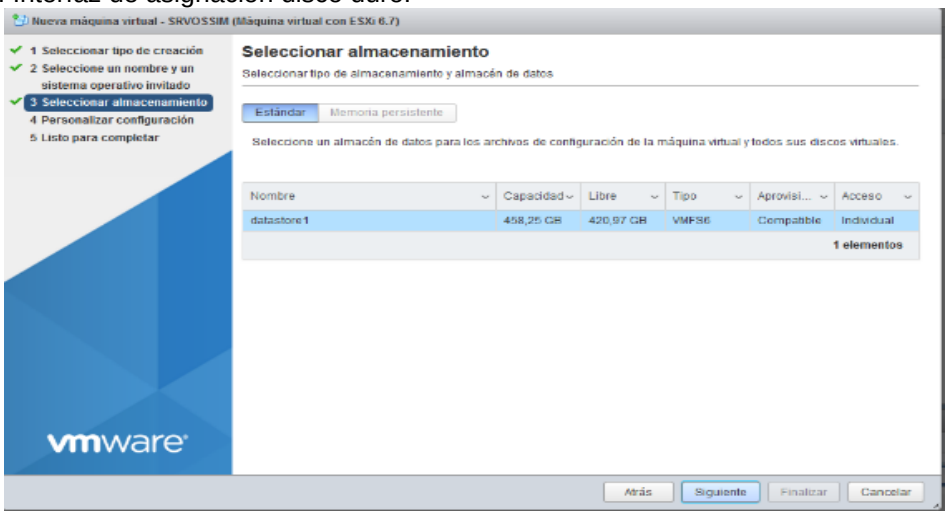
Figura 66. Interfaz máquina virtual.



Fuente: sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 66 se puede observar en el proceso, la interfaz asistida de vSphere que a través de esta se nombra la máquina virtual, usando la nemotecnia de **SRVOSSIM**, máquina virtual para ESXi 6.7, con sistema operativo distribución de Linux y en la cuarta casilla se ha seleccionado para Debian 8 de 64 bits, entonces se selecciona la opción de **siguiente**.

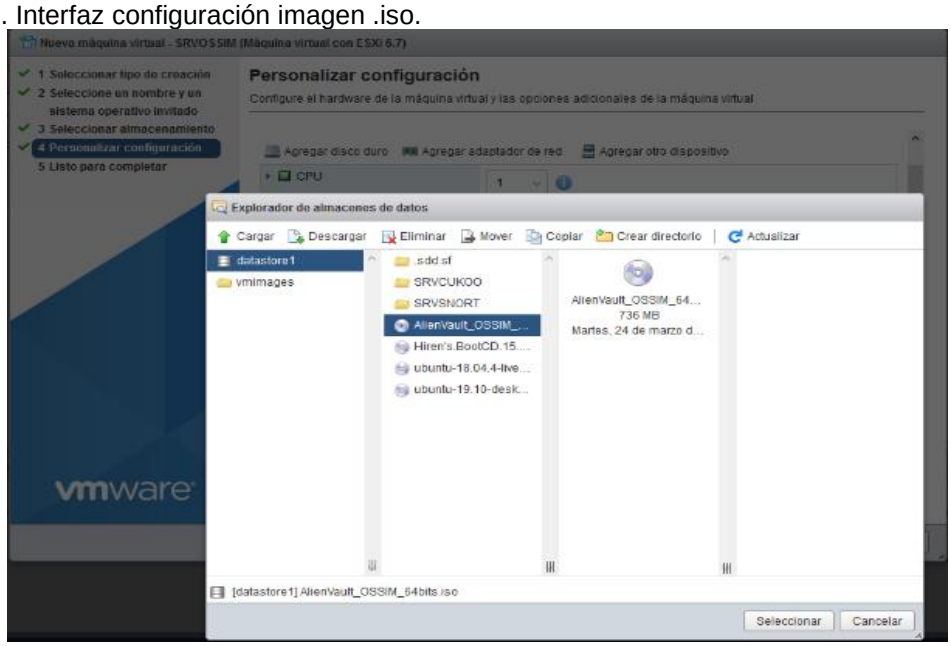
Figura 67. Interfaz de asignación disco duro.



Fuente: sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 67 se puede observar en el proceso, la opción de almacenamiento (**Datastore1**) donde será alojada la máquina virtual y se continua con las configuraciones previas.

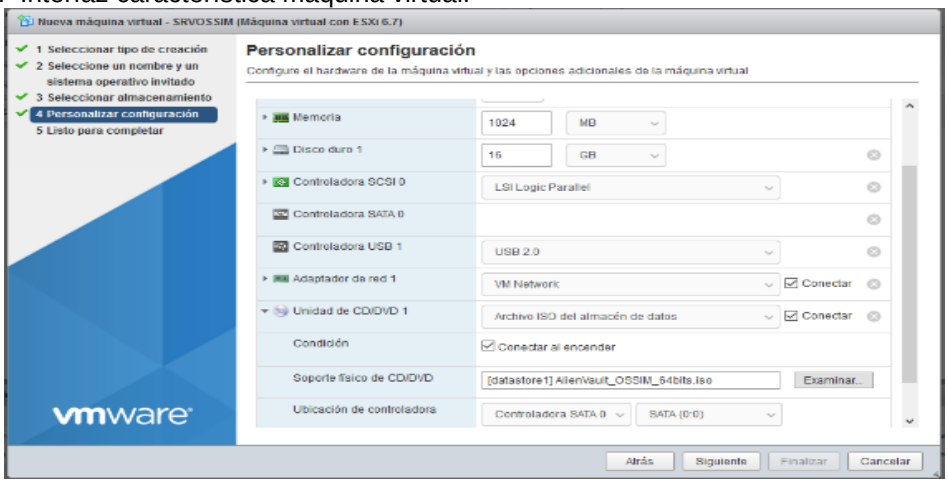
Figura 68. Interfaz configuración imagen .iso.



Fuente: sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 68 se puede observar en el proceso, la selección realizada de la imagen .iso en la cual se encuentra el sistema operativo invitado con el cual se va a iniciar la máquina virtual, para este caso Debian 8 a 64 bits, junto con la aplicación de Alíen Vault OSSIM; esta se encuentra alojada en el Datastore1 del equipo de cómputo seleccionado para virtualización.

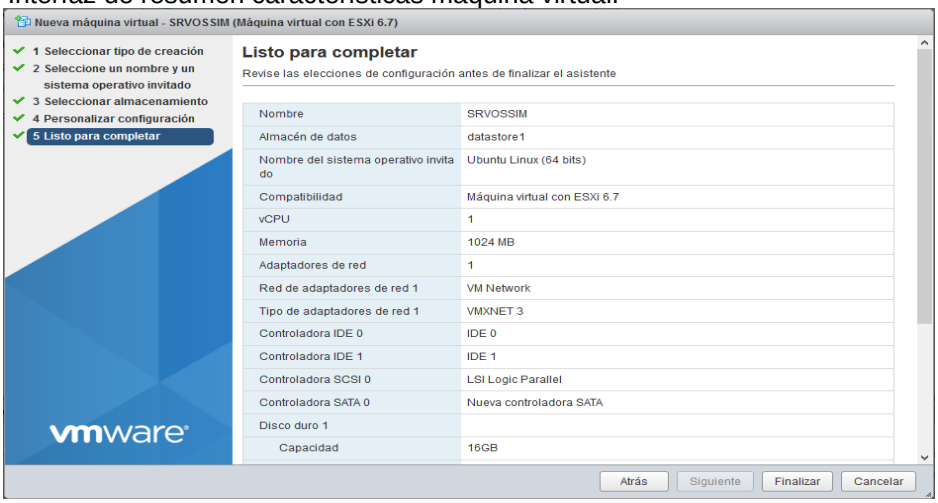
Figura 69. Interfaz característica máquina virtual.



Fuente: sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 69 se puede observar en el proceso, que se ha configurado la imagen .iso para iniciar la máquina e instalar el sistema operativo invitado, de igual forma capacidad de almacenamiento disco duro presentado, memoria RAM, procesador y tarjeta de red.

Figura 70. Interfaz de resumen características máquina virtual.

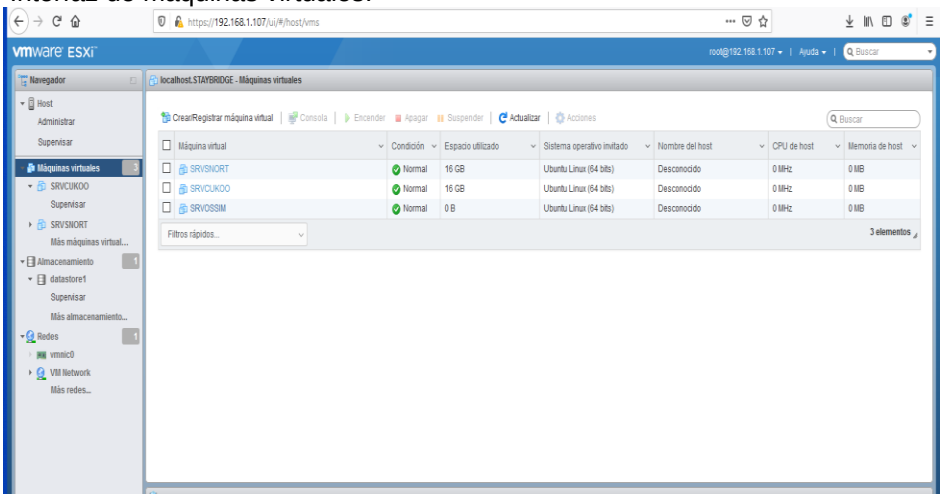


Fuente: sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura. 70. Se muestra, que se ha creado la máquina virtual y las características con las cuales se ha configurado, esto de acuerdo con la necesidad, el

almacenamiento se ha realizado como aprovisionamiento fino, que permita crecer en función de la cantidad de disco que se va ocupando por la herramienta y de sus complementos tales como bases de datos y demás paquetes necesarios de los cuales hace uso la herramienta de Alíen Vault OSSIM.

Figura 71. Interfaz de máquinas virtuales.



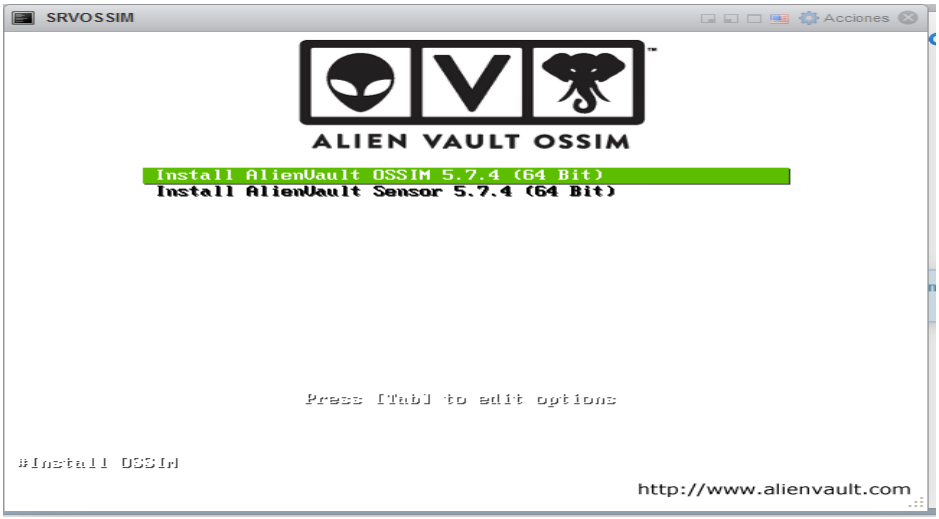
Fuente: sistema infraestructura VMware ESXi vSphere versión 6.7, Omar Tique M., mayo de 2020.

En la figura 71 se puede observar en el proceso, que se ha creado la máquina virtual, esta se visualiza en el inventario en la columna derecha del hypervisor.

8.3.1.12 Instalación y configuración de Alíen Vault Ossim

A continuación, se inicia el proceso instalación y configuración de la herramienta de Alíen Vault Ossim.

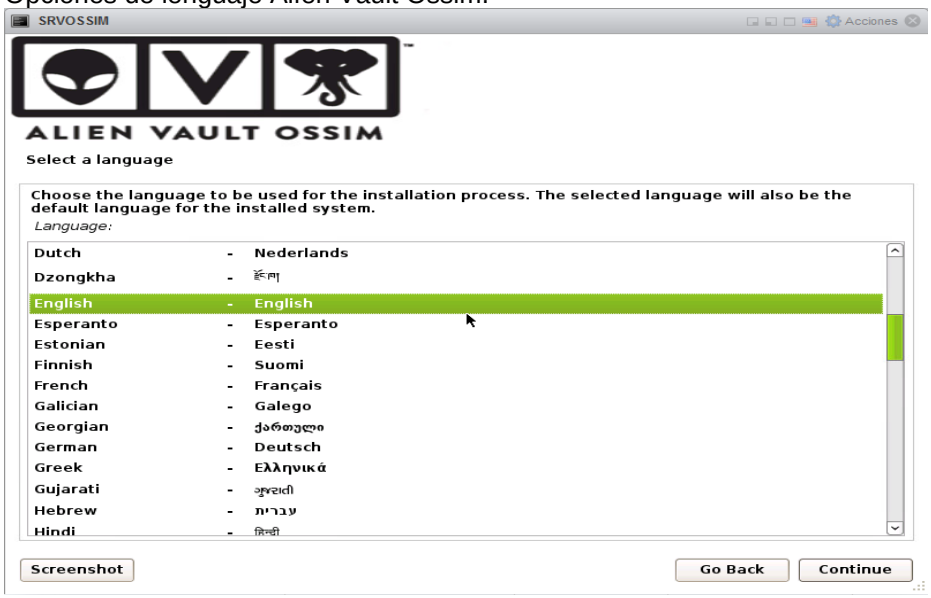
Figura 72. Interfaz instalación Alíen Vault Ossim.



Fuente: software instalación Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 72 se puede observar en el proceso, que se ha iniciado la instalación de la herramienta de Alíen Vault Ossim, se marca la opción que se instala, se da continuar con el proceso.

Figura 73. Opciones de lenguaje Alíen Vault Ossim.



Fuente: software instalación Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

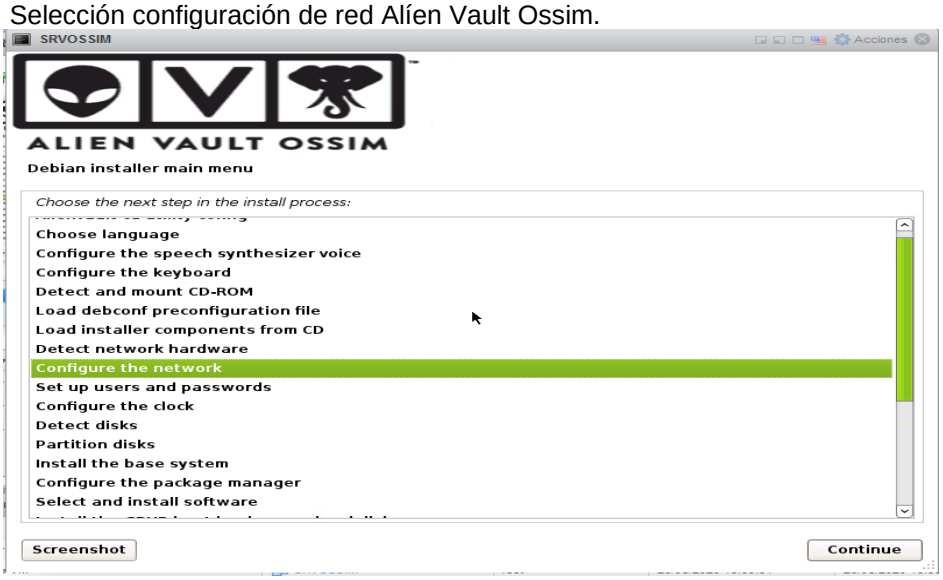
En la figura 73 se puede observar en el proceso, que se ha seleccionado el lenguaje para la instalación y funcionamiento de la herramienta Alíen Vault Ossim, es posible seleccionar cualquier otro lenguaje.

Figura 74. Carga de componentes adicionales Alíen Vault Ossim.

Fuente: software instalación Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 74 se puede observar en el proceso, que se ha iniciado la carga de componentes adicionales de la herramienta Alíen Vault Ossim.

Figura 75. Selección configuración de red Alíen Vault Ossim.



Fuente: software instalación Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

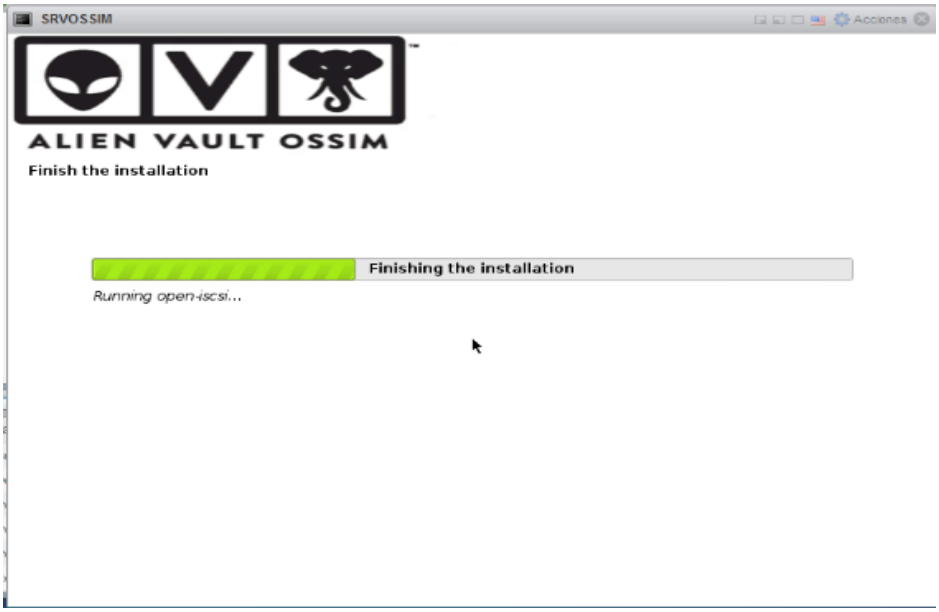
En la figura 75 se puede observar en el proceso, que se ha seleccionado la opción de configuración de red; se hace necesario instalar una tarjeta de red adicional y presentarla a la máquina virtual para realizar el monitoreo de puertos, se usa una tarjeta para la administración de la herramienta y la otra para realizar la escucha de puertos de la infraestructura.

Figura 76. Particionado y formateo de discos Alíen Vault Ossim.

Fuente: software instalación Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 76 se puede observar en el proceso, el inicio de particionado y formateo de la unidad de disco duro que se ha presentado para la instalación del sistema operativo y componentes de la herramienta Alíen Vault Ossim.

Figura. 77. Finalización instalación Alíen Vault Ossim.



Fuente: software instalación Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

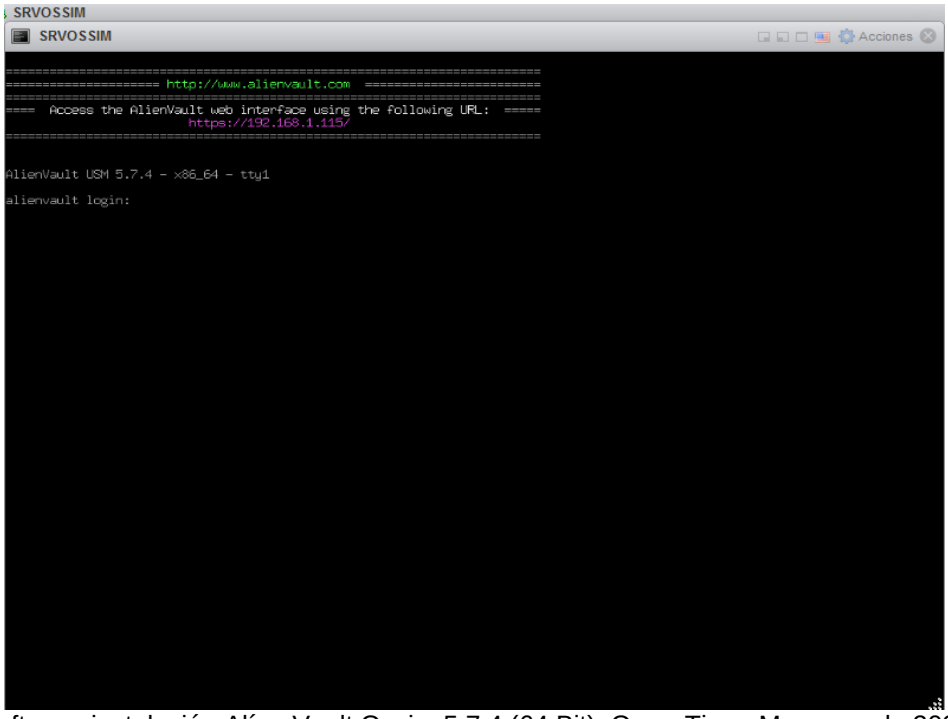
En la figura 77 se puede observar en el proceso, la finalización de la instalación del sistema operativo y componentes de la herramienta Alíen Vault Ossim que se usara en el CSIRT propuesto.

Figura 78. Interfaz logo Alíen Vault Ossim.

Fuente: software instalación Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 78 se puede observar en el proceso, la finalización de la instalación del sistema operativo y aplicación, presentando el logo de Alíen Vault OSSIM en la máquina virtual, su acceso se realiza mediante navegadores.

Figura 79. Interfaz de consola Alíen Vault Ossim.



Fuente: software instalación Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 79 se puede observar en el proceso, la interfaz de finalización de instalación del sistema operativo y la aplicación se muestra el url o dirección **IP** a la cual se debe conectar desde un navegador para ingresar a la interfaz y realizar las configuraciones necesarias propias de la herramienta, acceso a la interfaz administrativa y funcional de la Alíen Vault Ossim.

Se ha finalizado la creación de las máquinas virtuales, instalación y configuración de sistema operativo y también la instalación de algunas de las herramientas que serán usadas al interior del CSIRT propuesto, se dará continuidad con la configuración y puesta en funcionamiento de las herramientas necesarias en un CSIRT básico a nivel técnico.

A continuación, se procederá a realizar la configuración de la aplicación Alíen Vault OSSIM a usar como SIEM, de acuerdo con la información hallada se hace necesario seleccionar el tipo de monitoreo a realizar y las sondas que deben ser habilitadas previamente con el objetivo de poder escuchar los puertos a través de las interfaces de la tarjeta de red habilitada en el hardware (servidor).

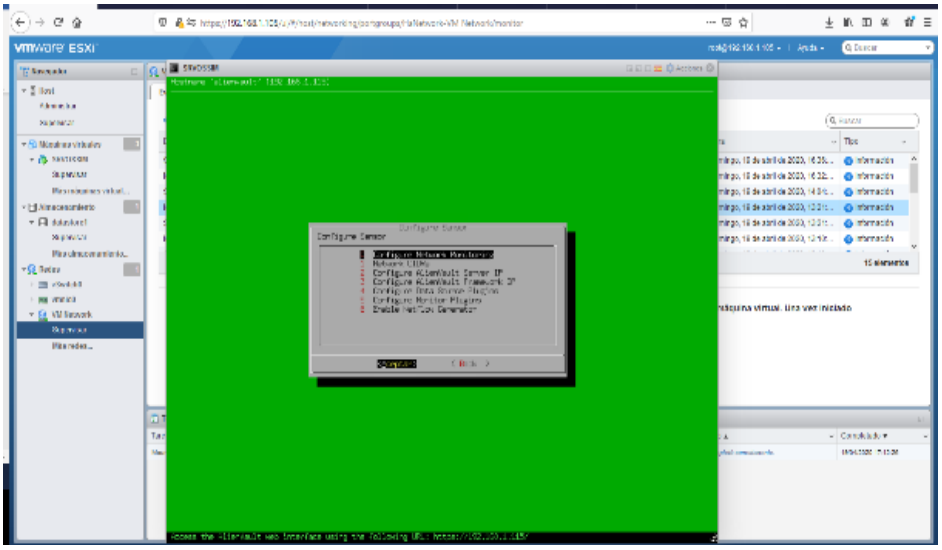
Antes de acceder a la aplicación a través de la interfaz web ha sido necesario realizar algunas configuraciones previamente como realizar aumento en la capacidad de almacenamiento en disco de hasta 60 Gigas Bytes como mínimo para poder guardar información, de igual forma aumentar la capacidad de memoria RAM de 4 Gigas Bytes para poder que se ejecute la aplicación de forma básica.

Por otra parte se pasó de usar un VCPU a dos (02) procesadores para las capacidades de cómputo en la máquina virtual creada, configurada y puesta en funcionamiento, adicionalmente se realizó la instalación de otra tarjeta de red a nivel físico en el equipo de cómputo que se ha seleccionado para la instalación de las máquinas virtuales en donde funcionaran las aplicaciones básicas; la tarjeta se configura y se presenta a la máquina virtual que será dedicada al monitoreo y en donde se ha instalado la aplicación Alíen Vault OSSIM, denominada como SRVOSSIM.

Realizar la configuración de red a través de la interfaz directa en la aplicación en el servidor, en donde se ha configurado la dirección IP. **192.168.1.115** para la administración propia de la aplicación a través del navegador web; y la tarjeta adicionada se ha configurado con la dirección IP. **192.168.1.120** para usarla como escucha o monitoreo de la red por donde es posible realizar el uso como IDS, IPS y el uso propio de las herramientas del SIEM a configurar.

Antes de poder acceder mediante cualquier navegador se hace necesario realizar las configuraciones que a continuación son descriptas, estas consisten en activar las sondas necesarias como escuchas, de igual forma se realiza de acuerdo con el equipo que ha sido seleccionado para trabajar como un SIEM; las configuraciones realizadas se pueden observar en las figuras subsiguientes así:

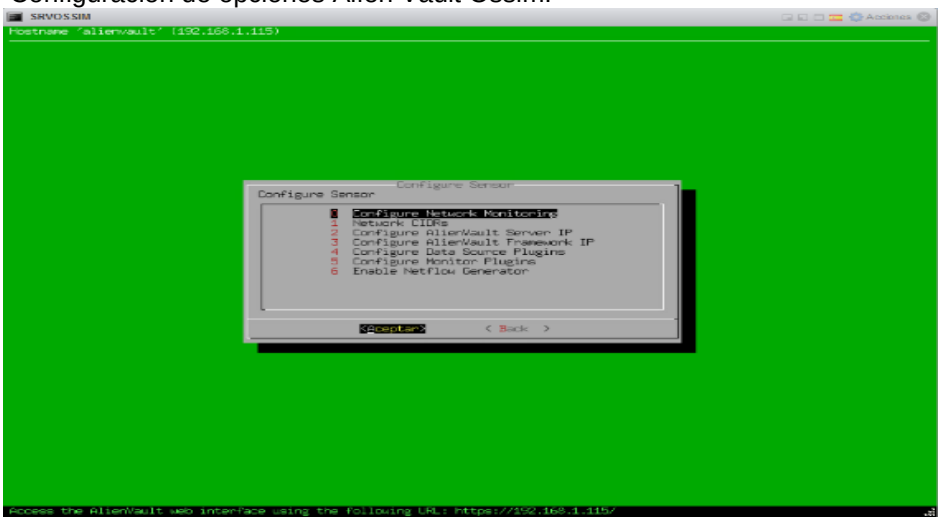
Figura 80. Interfaz de consola Alíen Vault Ossim.



Fuente: configuración Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 80 se puede observar en el proceso, la interfaz de administración y configuración por medio de la consola directamente en el servidor, esto se realiza una vez se autentica con las credenciales habilitadas durante la instalación del sistema operativo y la aplicación, estas configuraciones son previas al acceso desde la interfaz administrativa y funcional de Alíen Vault Ossim.

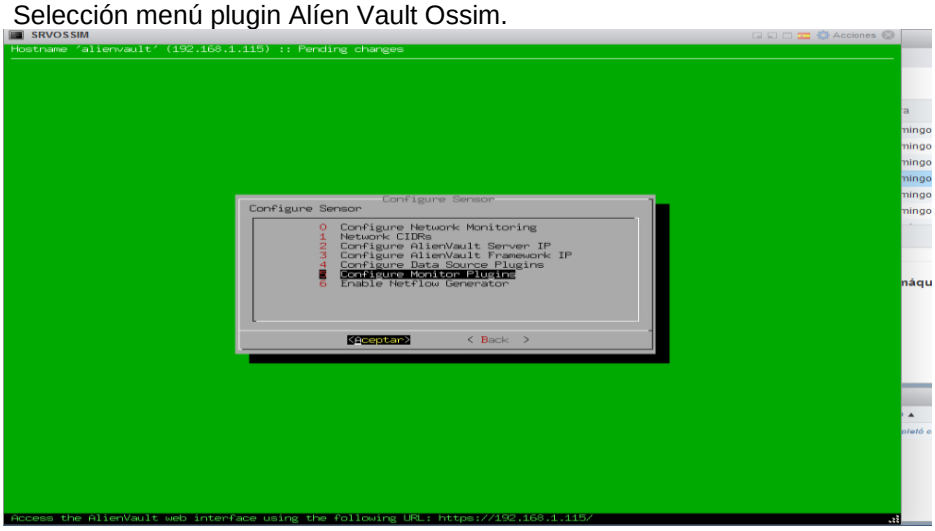
Figura 81. Configuración de opciones Alíen Vault Ossim.



Fuente: software instalación Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 81 se puede observar en el proceso, la interfaz gráfica de opciones desde la consola de Alíen Vault Ossim directamente en el equipo, se hace necesario el ingreso, configuración de sonda, tarjeta de red y direccionamiento IP, esto con el objeto de poder ingresar desde los navegadores.

Figura 82. Selección menú plugin Alíen Vault Ossim.

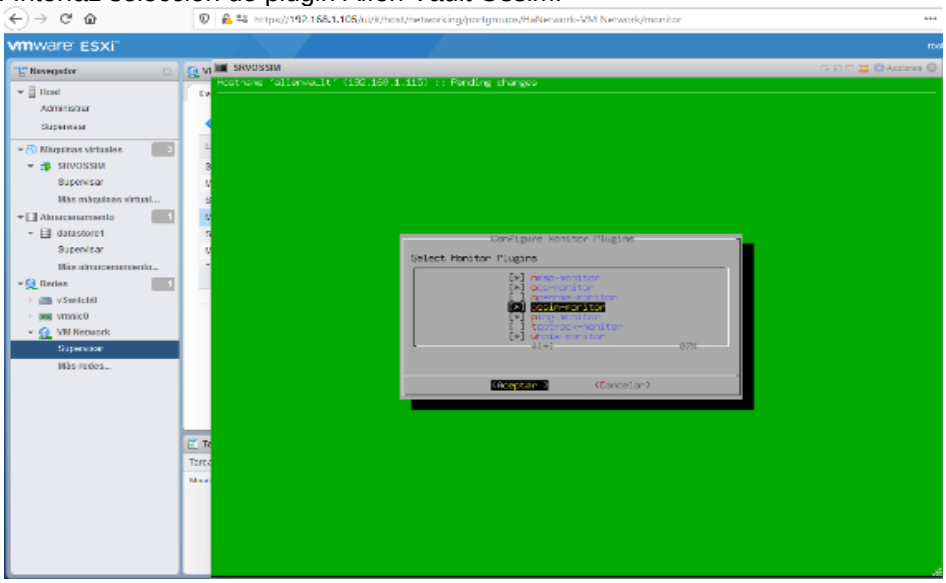


Fuente: software instalación Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 82 se puede observar en el proceso, la interfaz gráfica de opciones desde la consola de Alíen Vault Ossim, seleccionando el plugin de monitoreo de la

herramienta, se habilita para poder desde la interfaz gráfica de los navegadores hallarla y configurarla correctamente.

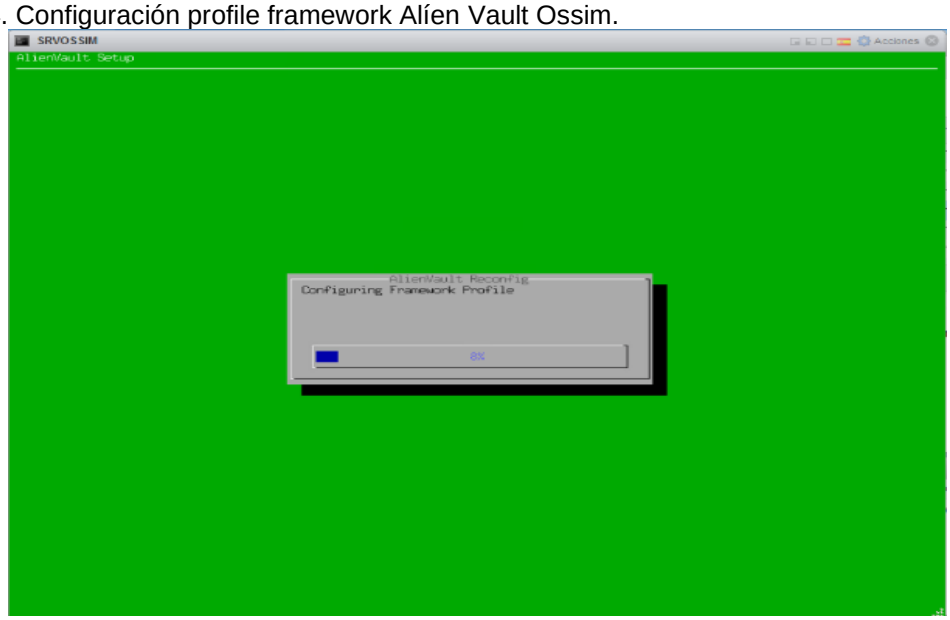
Figura 83. Interfaz selección de plugin Alíen Vault Ossim.



Fuente: software instalación Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 83 se puede observar en el proceso, la interfaz gráfica de opciones desde la consola de Alíen Vault Ossim, se ha seleccionado la sonda que se hace necesario habilitar, se acepta y continua con el proceso de configuraciones.

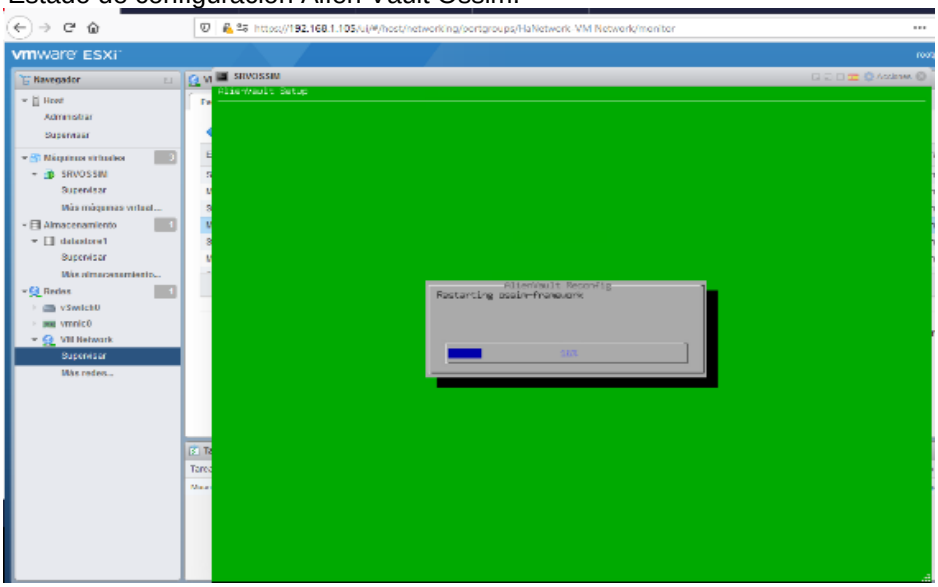
Figura 84. Configuración profile framework Alíen Vault Ossim.



Fuente: software instalación Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 84 se puede observar en el proceso, la interfaz gráfica de opciones desde la consola de Alíen Vault Ossim, seleccionando la opción “configurar el perfil de Framework”, en el cual se ha procedido a realizar la respectiva configuración.

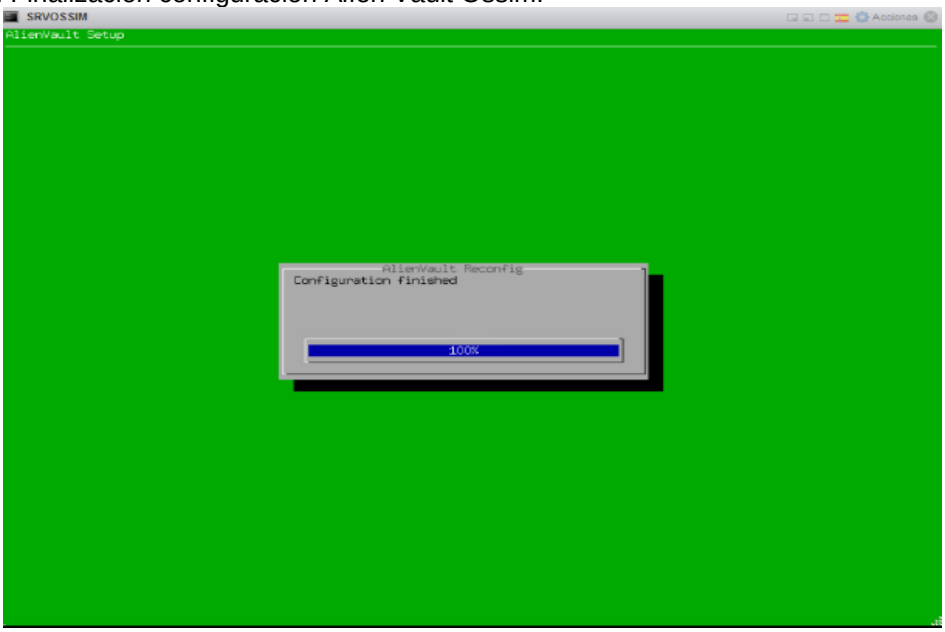
Figura 85. Estado de configuración Alíen Vault Ossim.



Fuente: software instalación Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 85 se puede observar en el proceso, la interfaz gráfica de opciones desde la consola de Alíen Vault Ossim, seleccionando la de configurar el perfil de Framework, en el cual se ha procedido a realizar la respectiva configuración.

Figura 86. Finalización configuración Alíen Vault Ossim.

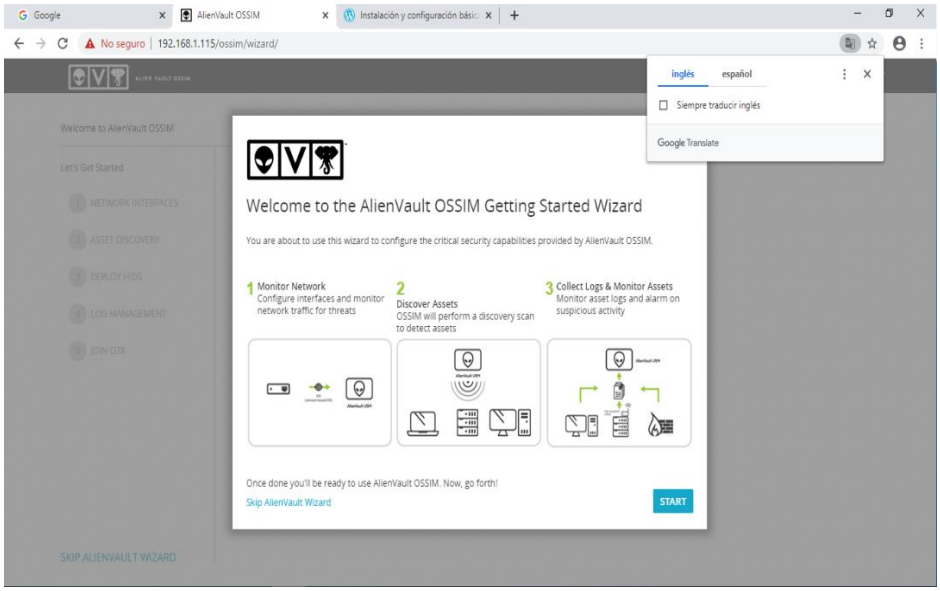


Fuente: software instalación Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 86 se puede observar en el proceso, la interfaz gráfica de opciones desde la consola de Alíen Vault Ossim, la finalización de configuraciones realizadas.

8.3.1.14 Acceso web a la herramienta de Alíen Vault Ossim

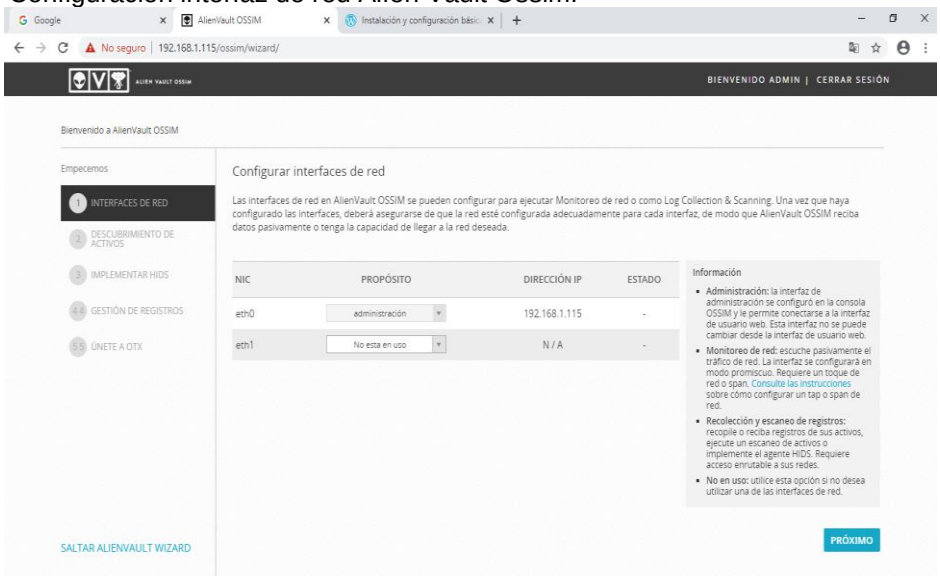
Figura 87. Interfaz Web bienvenida Alíen Vault Ossim.



Fuente: Configuración gráfica Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 87 se puede observar en el proceso, la interfaz gráfica de bienvenida web de Alíen Vault Ossim una vez finalizada las configuraciones y que se ha validado mediante el acceso web a la aplicación.

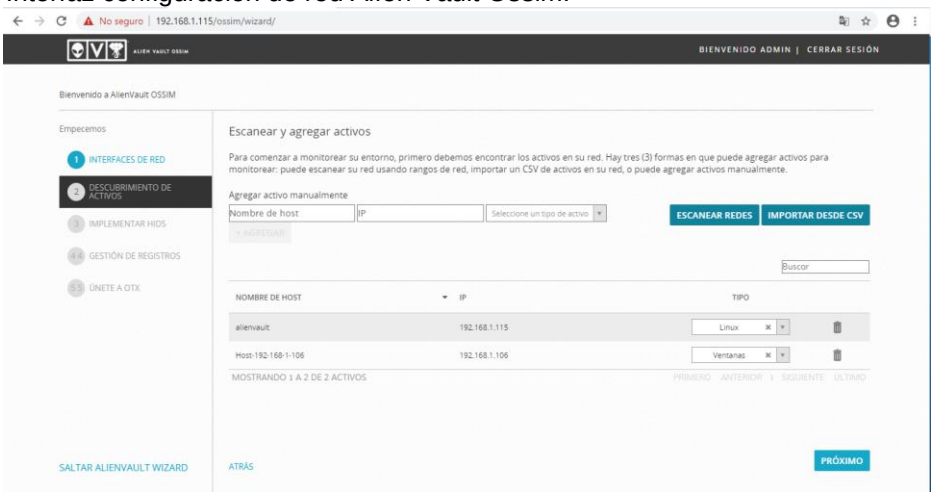
Figura 88. Configuración interfaz de red Alíen Vault Ossim.



Fuente: configuración gráfica Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 88 se puede observar en el proceso, la interfaz gráfica inicial web de Alíen Vault Ossim en este punto permite realizar las configuraciones de las tarjetas de red que se encuentren instaladas y presentadas a la herramienta durante la instalación, o se pueden adicionar desde este panel de opciones.

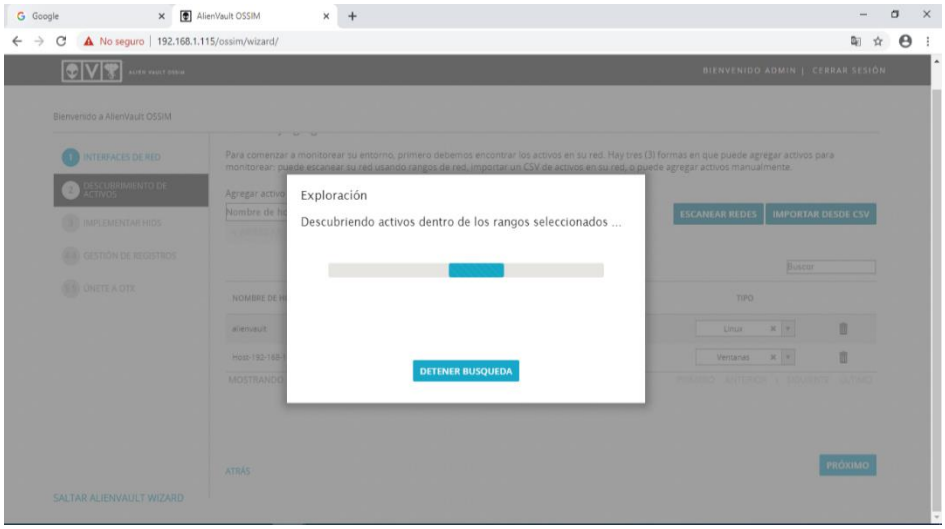
Figura 89. Interfaz configuración de red Alíen Vault Ossim.



Fuente: Configuración gráfica Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 89 se puede observar en el proceso, la interfaz gráfica inicial web de Alíen Vault Ossim, se ha realizado la adicción de la tarjeta de red y se configura direccionamiento adicional con el objeto de que la herramienta pueda realizar el monitoreo de puertos.

Figura 90. Escaneo de activos Alíen Vault Ossim.

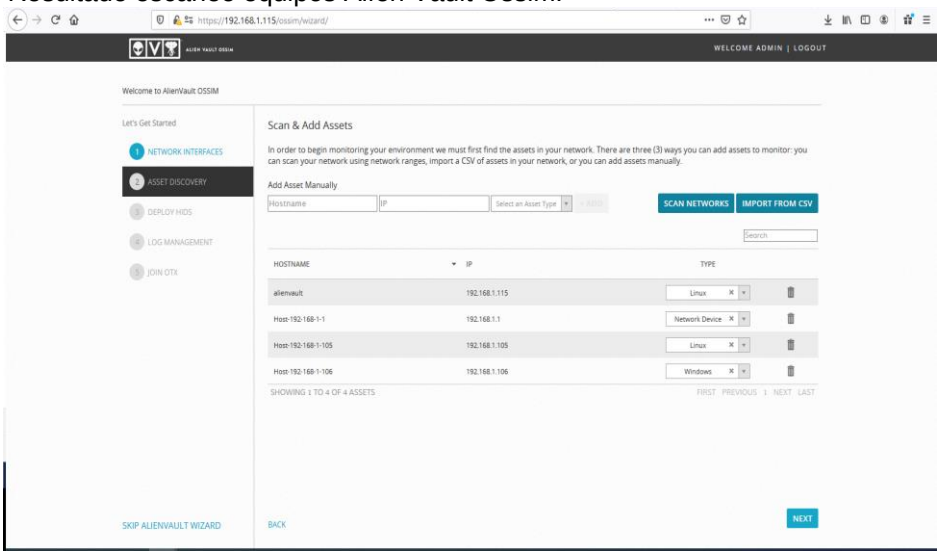


Fuente: Configuración gráfica Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 90 se puede observar en el proceso, la interfaz gráfica web de Alíen Vault Ossim, se ha enviado un descubrimiento de equipos activos que estén

conectados a la red LAN, estos pueden ser equipos switchs y router, como también servidores y equipos de escritorio.

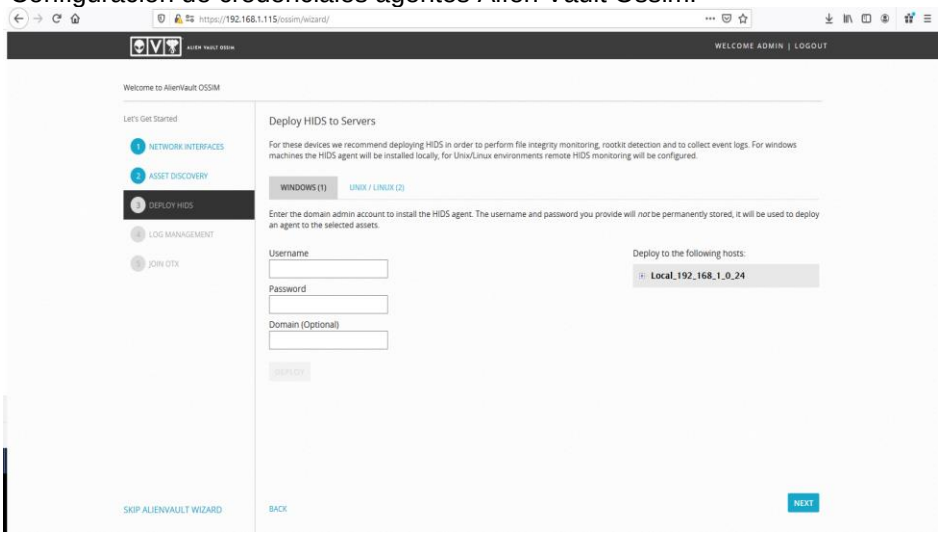
Figura 91. Resultado escaneo equipos Alíen Vault Ossim.



Fuente: Configuración gráfica Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

En la figura. 91. Se muestra, la interfaz gráfica inicial web de Alíen Vault Ossim, se puede observar que ha realizado el escaneo de equipos conectados a la red LAN y arroja el resultado, mostrando los equipos hallados al momento de realizar el escaneo.

Figura 92. Configuración de credenciales agentes Alíen Vault Ossim.

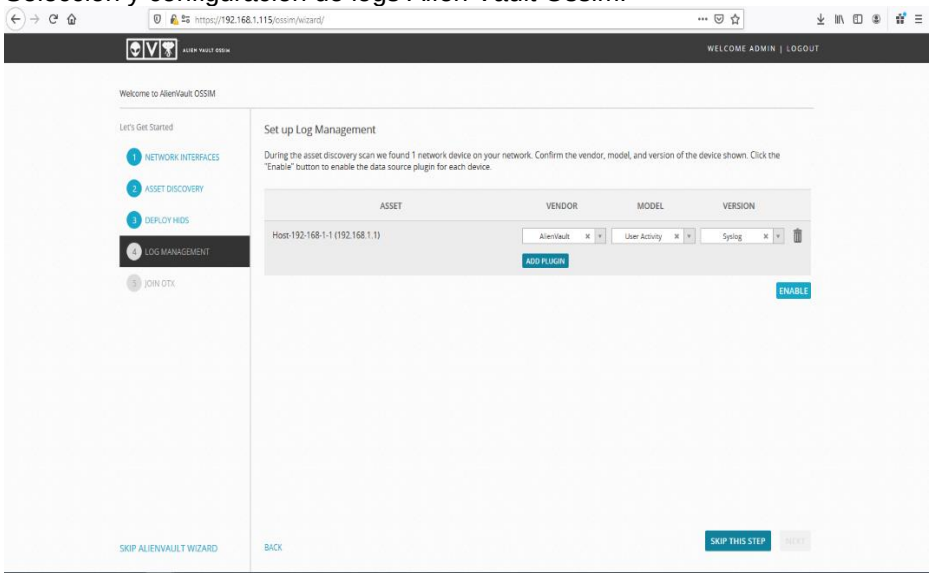


Fuente: Configuración gráfica Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 92 se puede observar en el proceso, en la interfaz gráfica inicial web de Alíen Vault Ossim, se encuentra la opción de configuración de credenciales para

desplegar los agentes que realizan el monitoreo en los equipos al interior de una red LAN, pueden ser para sistemas operativos Windows o linux.

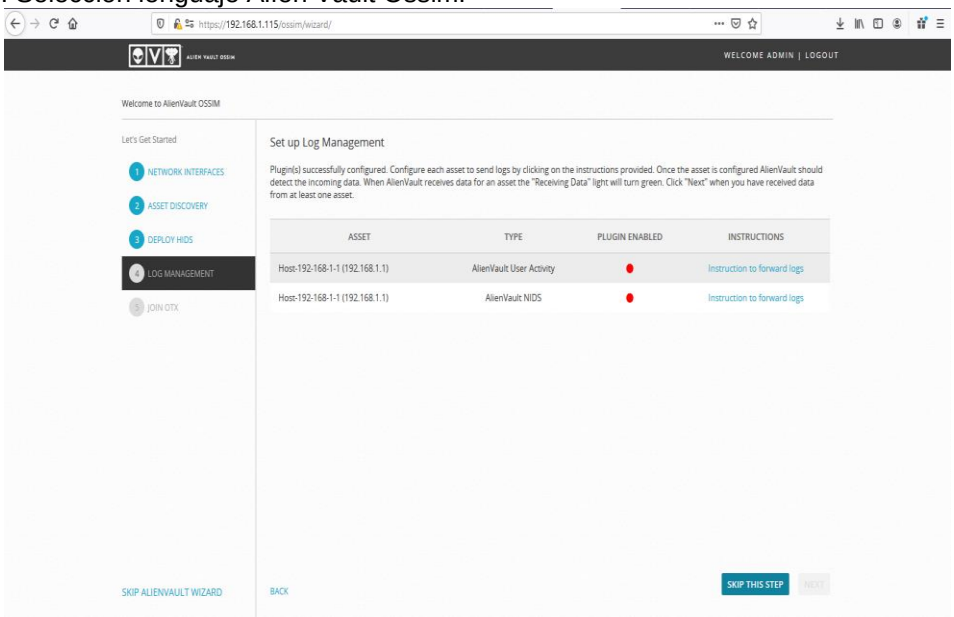
Figura 93. Selección y configuración de logs Alíen Vault Ossim.



Fuente: Configuración gráfica Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 93 se puede observar en el proceso, la interfaz gráfica inicial web de Alíen Vault Ossim, se encuentra la opción de configuración de administración de logs de la herramienta de monitoreo, eventos, esto referido al equipo de red que se ha descubierto en el escaneo de red que se realizara con anterioridad.

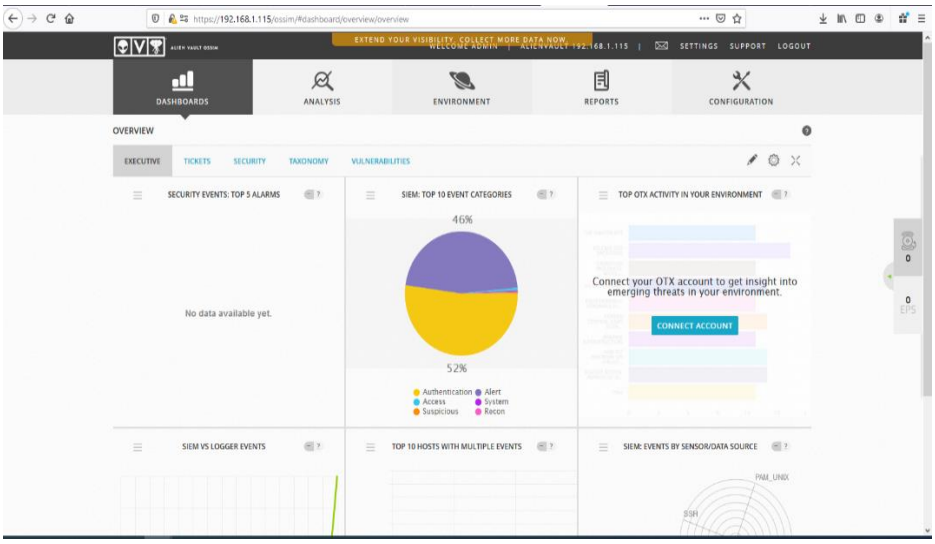
Figura 94. Selección lenguaje Alíen Vault Ossim.



Fuente: Configuración gráfica Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 94 se puede observar en el proceso, en la interfaz gráfica inicial web de Alíen Vault Ossim, se encuentra la opción de configuración de administración de logs de la herramienta de monitoreo, eventos, esto referido al equipo de red que se ha descubierto en el escaneo de red LAN.

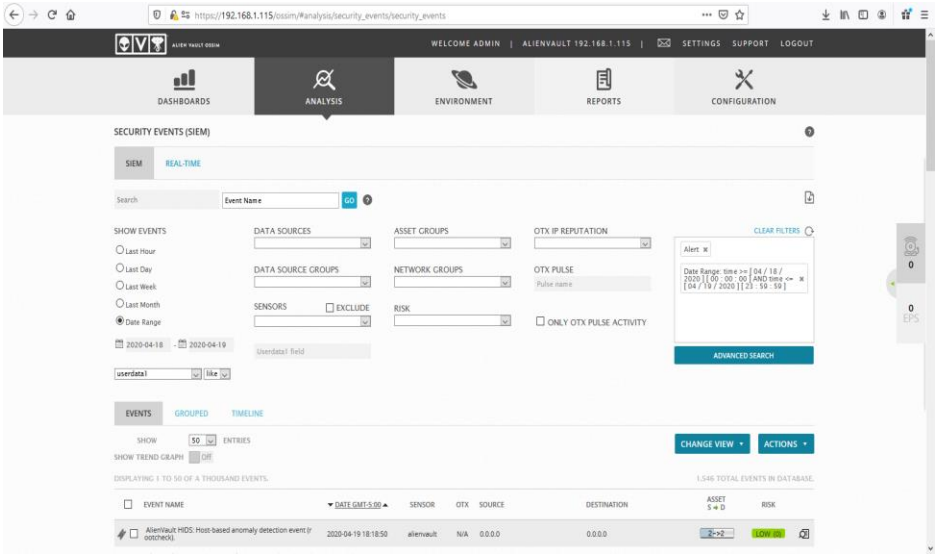
Figura 95. Dashboards Interfaz Administración web Alíen Vault Ossim.



Fuente: Configuración gráfica Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 95 se puede observar en el proceso, la interfaz gráfica de administración web de Alíen Vault Ossim, desde donde se accede a cada una de las funcionalidades del SIEM, se realiza habilitación y configuración de cada uno de los ítems monitorear, ver estadísticas gráficamente, comportamientos de la infraestructura tecnológica, equipos de red, servidores y equipos de cómputo.

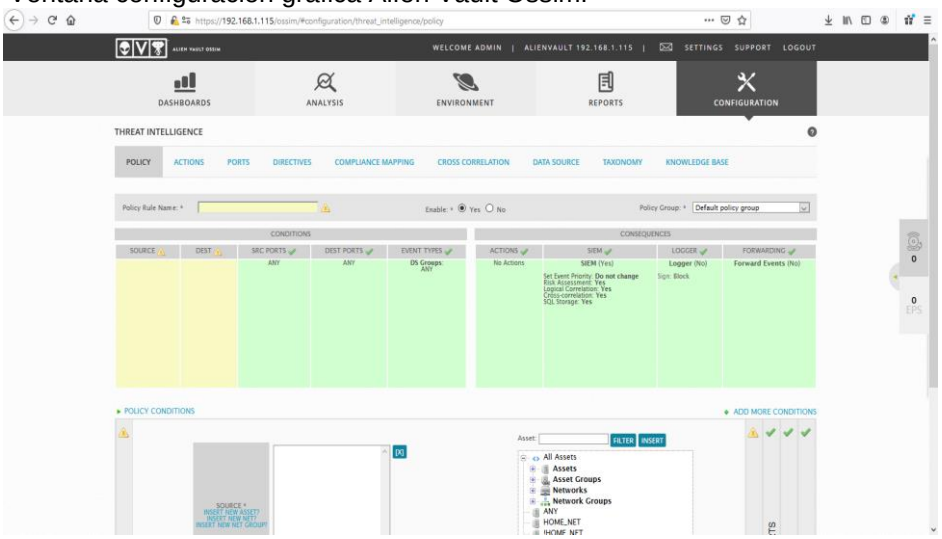
Figura. 96. Administración web ¨análisis¨ Alíen Vault Ossim.



Fuente: Configuración gráfica Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 96 se puede observar en el proceso, la interfaz gráfica de administración web de Alíen Vault Ossim, desde donde se accede a cada una de las funcionalidades del SIEM, se realiza acceso al módulo de análisis en el cual se verifica las opciones disponibles que podemos configurar de acuerdo con la infraestructura.

Figura 97. Ventana configuración gráfica Alíen Vault Ossim.



Fuente: Configuración gráfica Alíen Vault Ossim 5.7.4 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 97 se puede observar en el proceso, la interfaz gráfica de administración web de Alíen Vault Ossim, se accede a la funcionalidad inteligencia de amenazas del SIEM, se realiza acceso al módulo de configuraciones en el cual se verifica las opciones disponibles a configurar

Hasta este punto se ha realizado la creación de la máquina virtual, instalación del sistema operativo de la misma, basada en distribuciones linux y se ha procedido a la instalación y configuración de la herramienta Alíen Vault Ossim que funciona como un SIEM al interior de cualquier empresa en el componente de infraestructura tecnológica, y que puede ser usad el área de seguridad informática.

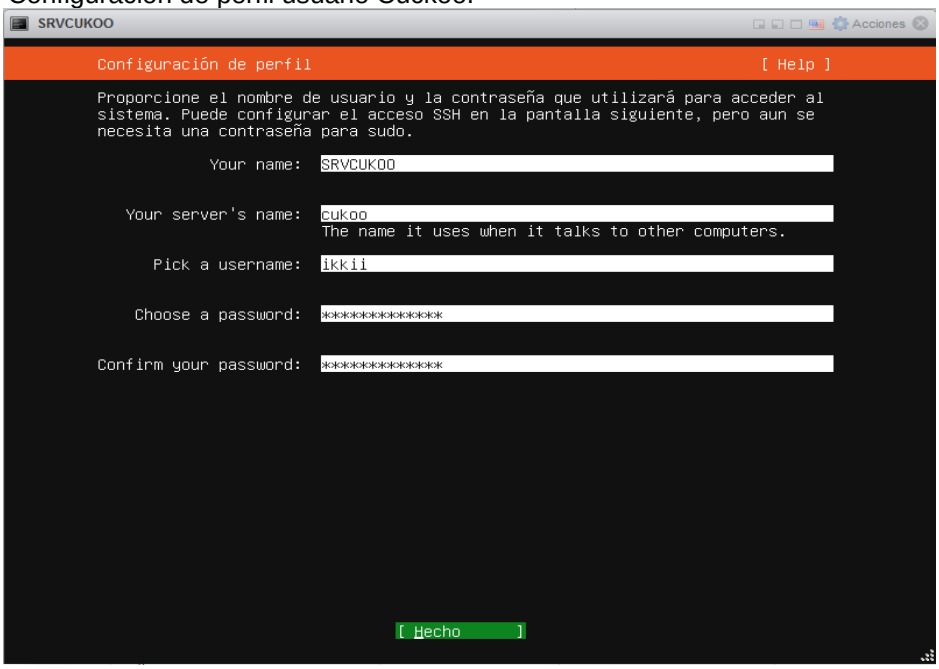
Se ha finalizado la creación de las máquinas virtuales, instalación y configuración de sistema operativo y también la instalación de algunas de las herramientas que serán usadas al interior del CSIRT propuesto, se da continuidad con la configuración y puesta en funcionamiento de las herramientas necesarias en un CSIRT básico a nivel técnico.

8.3.1.15 Root Creación e instalación de la sandbox Cuckoo

Siendo reiterativo a continuación se muestra en la gráfica la configuración que tendrá la máquina virtual basada en la distribución de Ubuntu 18, como lo es: el

nombre de la máquina, el usuario, de igual forma se configura el password y se da inicio primero a la instalación del sistema operativo y posteriormente a la aplicación de la herramienta de sandbox Cuckoo.

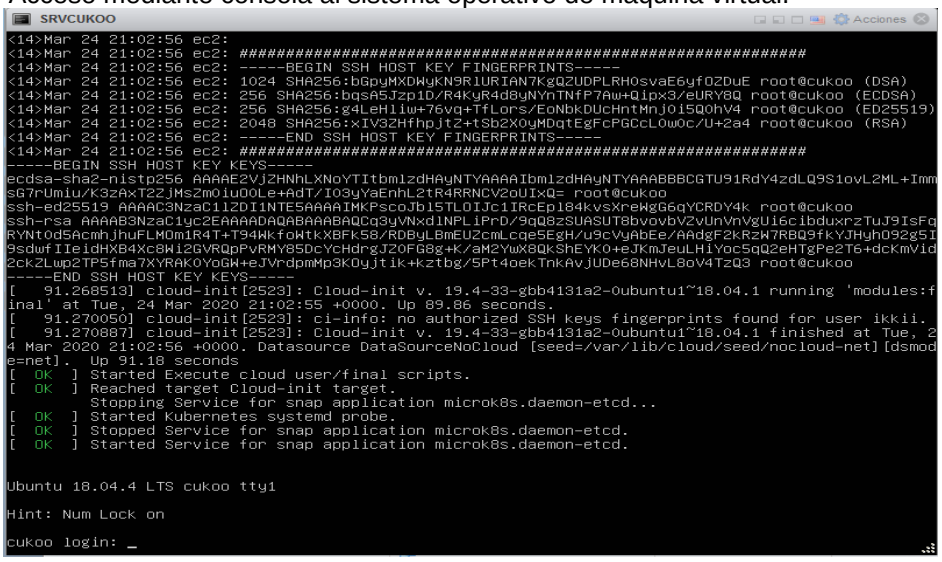
Figura 98. Configuración de perfil usuario Cuckoo.



Fuente: Instalación sistema operativo Ubuntu 18 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 98 se puede observar en el proceso, la interfaz gráfica de configuración de perfil, se asigna nombre a la máquina virtual, credenciales de usuario, nombre de servidor y credenciales de acceso a la aplicación.

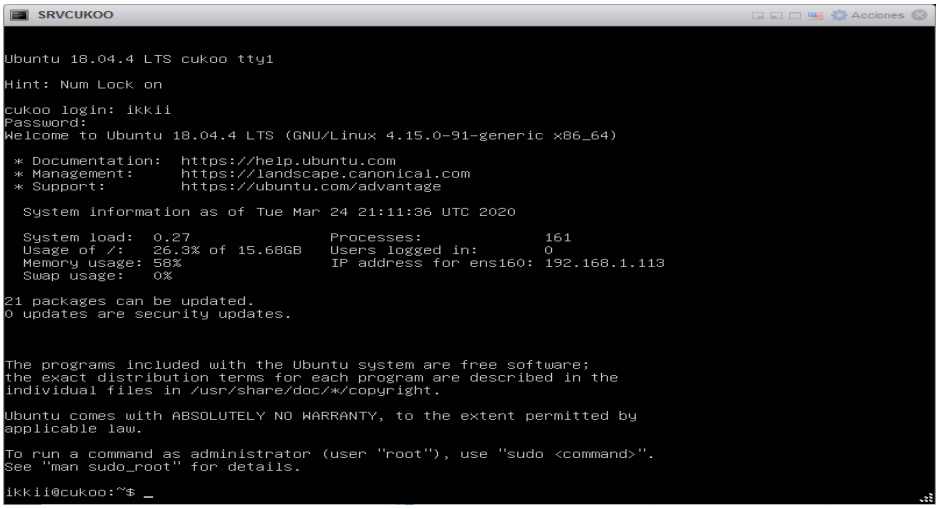
Figura 99. Acceso mediante consola al sistema operativo de máquina virtual.



Fuente: Instalación sistema operativo Ubuntu 18 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 99 se puede observar en el proceso, la interfaz la finalización de instalación del sistema operativo invitado en el equipo para la máquina virtual, en la interfaz de consola solicita credenciales de acceso para el usuario Cuckoo al acceder al sistema y configuraciones. Al finalizar la instalación del sistema operativo se accede mediante consola, se actualiza el sistema operativo tal y como se aprecia, se corren las actualizaciones de Linux.

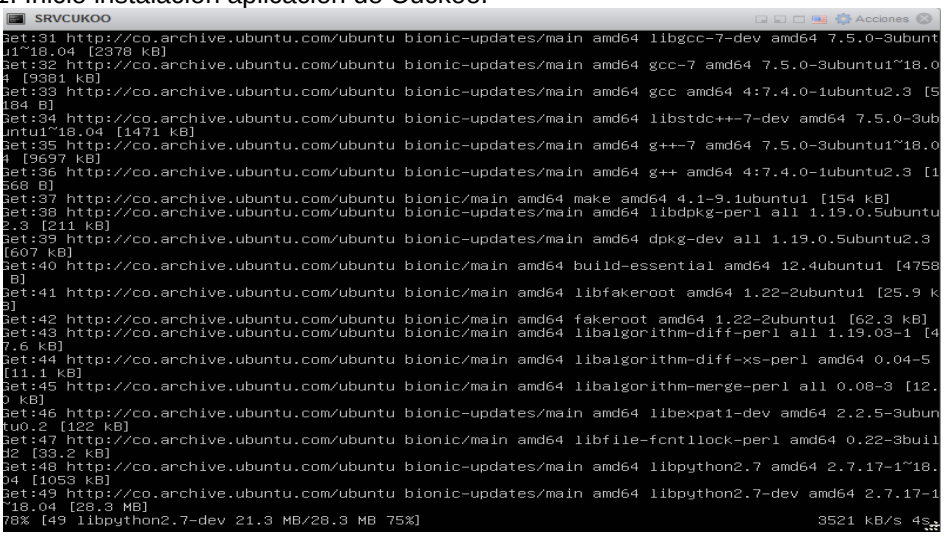
Figura 100. Acceso mediante Consola de usuario creado



Fuente: Instalación sistema operativo Ubuntu 18 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 100 se puede observar en el proceso, la interfaz de consola del sistema operativo para la administración de este, crear el usuario para realizar el ingreso a la máquina virtual, realizar la instalación y configuración de la herramienta que se usara como sandbox en el proyecto aplicado y que está orientado a la creación del CSIRT.

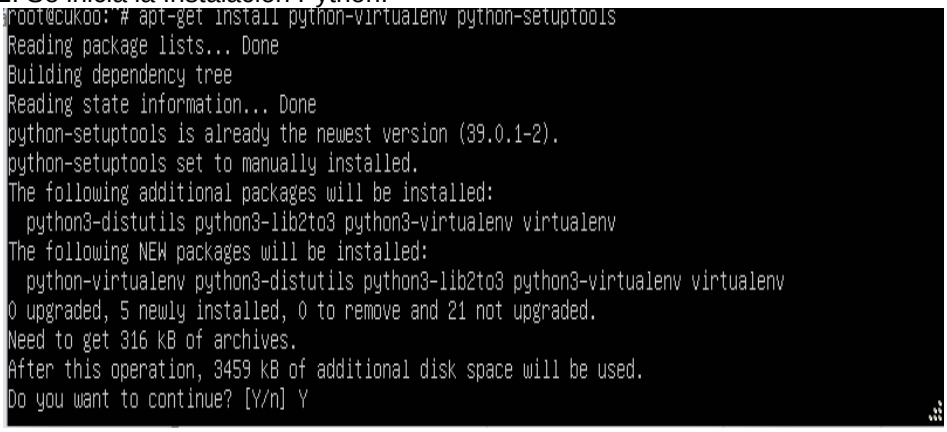
Figura 101. Inicio instalación aplicación de Cuckoo.



Fuente: Actualización sistema operativo Ubuntu 18 (64 Bit), Omar Tique M., mayo de 2020.

En la figura 101 se puede observar el proceso de instalación de los paquetes necesarios para la configuración y puesta en funcionamiento de la herramienta Cuckoo en la máquina virtual. Se ha iniciado la instalación de la aplicación para la sandbox, antes de la instalación definitiva, se debe descargar e instalar algunos paquetes que son fundamentales para el normal funcionamiento como lo es Python y sus dependencias, DBmongo, crear directorios y subdirectorios.

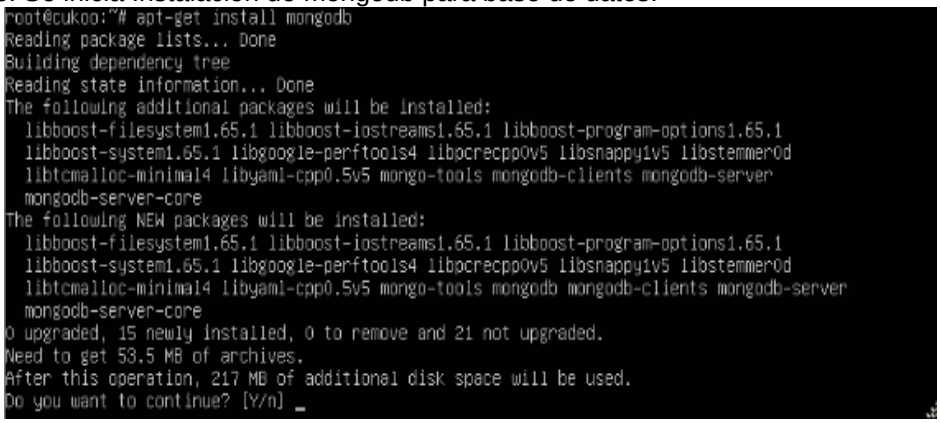
Figura 102. Se inicia la Instalación Python.



Fuente: Instalación de Python y herramientas (64 Bit), Omar Tique M., mayo de 2020.

En la figura 102 se puede observar en el proceso, el inicio de descarga de paquetes y la instalación de Python con las dependencias necesarias para el funcionamiento de la sandbox que se ha decidido instalar y configurar en el presente proyecto como trabajo final para la especialización.

Figura 103. Se inicia Instalación de mongodb para base de datos.

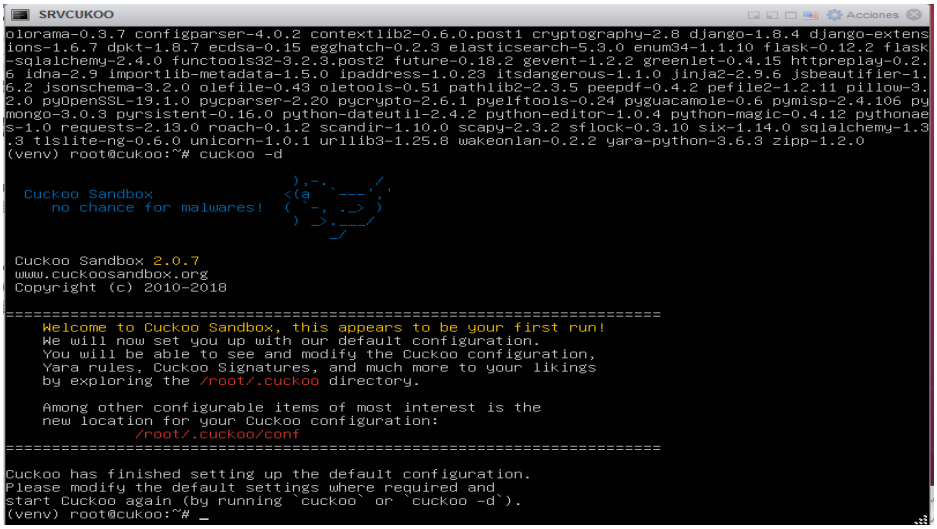


Fuente: Instalación de mongodb (64 Bit), Omar Tique M., mayo de 2020.

En la figura 103 se puede observar en el proceso, el inicio de descarga de paquetes y la instalación de mongodb con las dependencias necesarias en el funcionamiento de la sandbox, usado por esta como base de datos y soportar la aplicación y servir de contenedor para los paquetes y archivos que se analicen.

Una vez finalizada la instalación y configuración de máquinas virtuales, sistemas operativos invitados, se procedió con la instalación y configuración de las aplicaciones y herramientas a ser usadas, posteriormente se realiza la configuración de las herramientas en función de lo que debe hacer cada una de estas al interior de la infraestructura.

Figura 104. verificación instalación de Cuckoo.



Fuente: Software aplicación Cuckoo Sandbox 2.0.7 (64 Bit), Omar Tique M., mayo de 2020.

En la figura. 104. Se indica, en la interfaz de consola que se ha realizado la verificación de la instalación de la herramienta de Cuckoo a ser usada como sandbox en el CSIRT como herramienta de apoyo al soporte de infraestructura a nivel de software y aplicación para validar posibles vulnerabilidades de archivos que son enviados.

8.4 CREACIÓN DEL CSIRT CIBERSECURITY DE COLOMBIA LTDA

8.4.1 Instalación centro de cableado, puntos de red y equipos

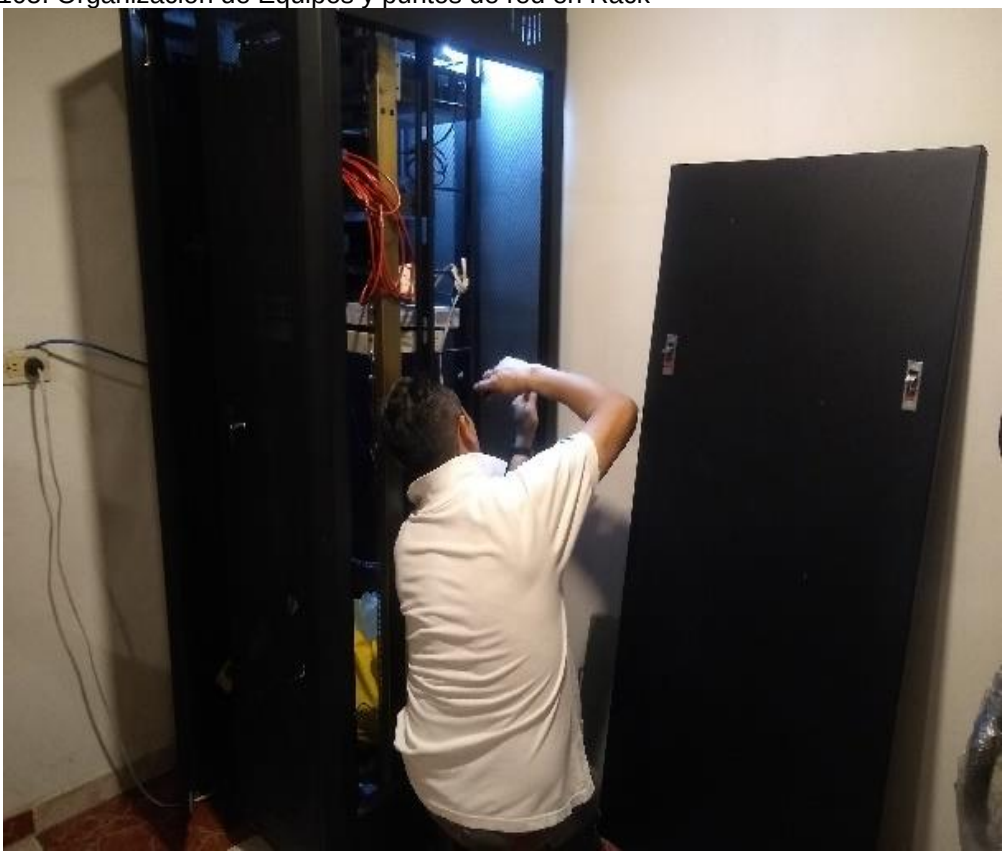
En la siguientes figuras se puede observar la actividad concerniente a el armado del rack de comunicaciones, la instalación de regleta de tomacorrientes para la conexión de equipos de red, los equipos de red, equipo servidor usado para virtualizar las maquinas en las cuales se realizara la instalación y configuración de las herramientas básicas para la configuración del CSIRT; se ha realizado la instalación de los puntos de red que darán servicio a los puestos de trabajo, para interconexión de equipos usados en los escritorios por los ingenieros que brindan soporte frente a los incidentes informáticos que se presenten.

Se ha usado cable UTP en categoría 6A con el objeto de contar con un canal de hasta 10 Gigas con capacidad de transferencia rápida de archivos; se ha usado un canal en Monomarca para eliminar cuellos de botellas que se generan por acoples con valores distintos de impedancia, por variedad de marcas en un mismo canal o enlace.

Se realizo la instalación de diez puntos de red para lograr la interconexión de los equipos de cómputo a la red LAN, se ha dispuesto de cuatro puestos de trabajo con equipos de cómputo portátiles y de escritorios, en este caso.

A continuación, se está finalizando la actividad con la instalación de la regleta multitoma en el rack y el peinado de los Patch Cord que interconectan las salidas a los puestos de trabajo.

Figura 105. Organización de Equipos y puntos de red en Rack

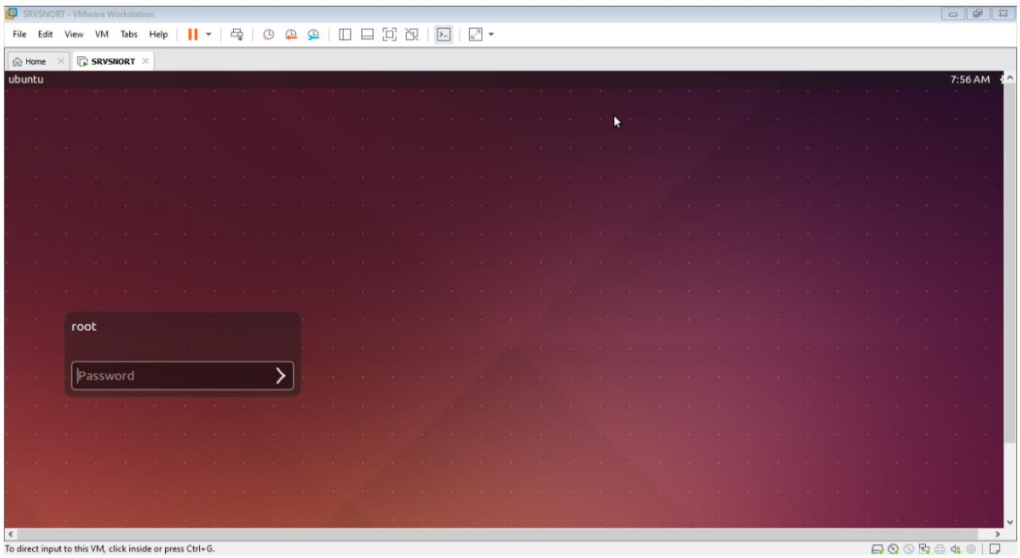


Fuente: Fotografía acondicionamiento de Rack, Omar Tique M., mayo de 2020.

A continuación, en la siguiente figura se puede observar la salida de datos a los puestos de trabajo (usuario final), en categoría 6 A, debidamente identificados.

8.4.2 Acceso Máquina Virtual de SNORT virtualizado

Figura 106. Acceso grafico a la máquina virtual de Snort.

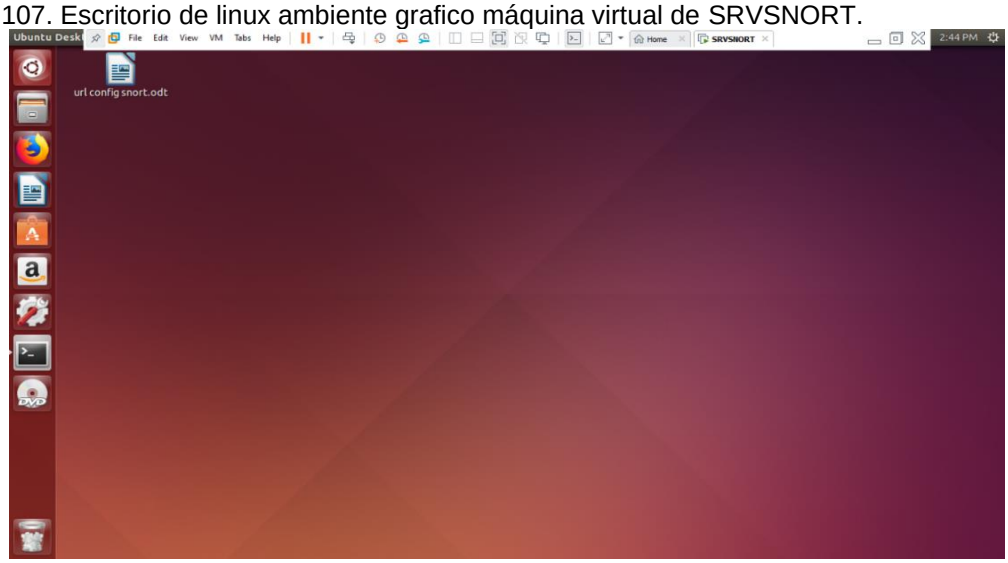


Fuente: Sistema operativo Ubuntu Desktop (64 Bit), Omar Tique M., mayo de 2020.

En la figura. 106. Se indica, la interfaz de acceso a la máquina virtual y el sistema operativo en Ubuntu para acceder a la herramienta de Snort mediante el uso de las credenciales configuradas durante la instalación del sistema operativo invitado el cual se encuentra virtualizado mediante VMware.

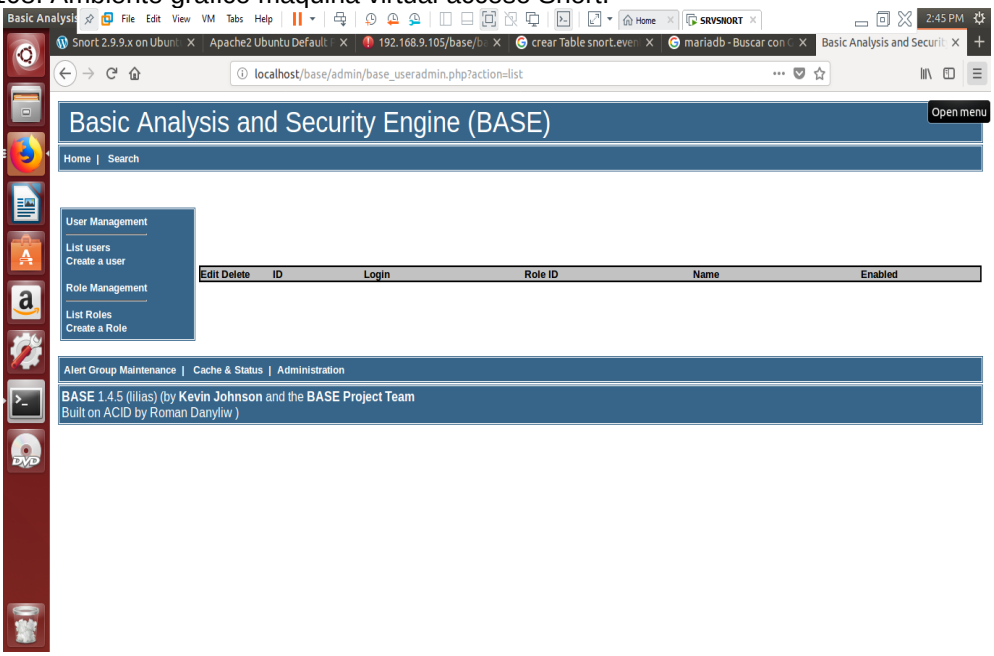
En la figura. 107. Se indica, la interfaz de administración en la máquina virtual y el sistema operativo en Ubuntu para acceder a la herramienta de Snort, esta se encuentra virtualizado mediante VMware, se ha hecho necesario recurrir a software en demo o trial para lograr la virtualización de cada una de las maquinas necesarias en el desarrollo del proyecto aquí presente.

Figura 107. Escritorio de linux ambiente grafico máquina virtual de SRVSNORT.



Fuente: Sistema operativo Ubuntu Desktop (64 Bit), Omar Tique M., mayo de 2020.

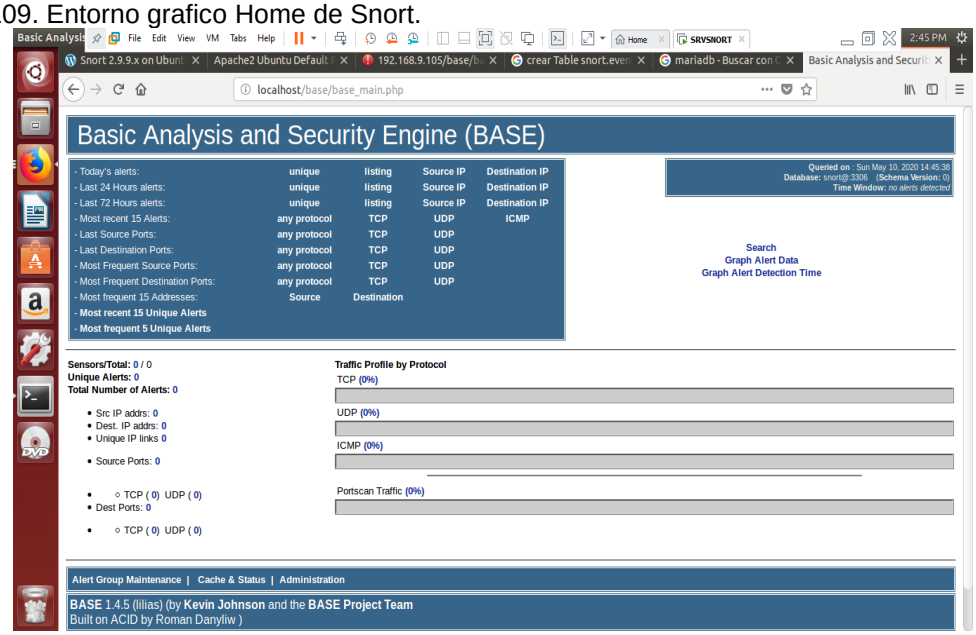
Figura 108. Ambiente gráfico máquina virtual acceso Snort.



Fuente: Sistema IDS Snort en Sistema operativo Ubuntu Desktop (64 Bit), Omar Tique M., mayo de 2020.

En la figura. 108. Se indica, la interfaz de acceso a la herramienta Snort base, se encuentra configurado en modo básico y permite realizar las configuraciones iniciales de acuerdo con la necesidad particular en la administración de infraestructura tecnológica.

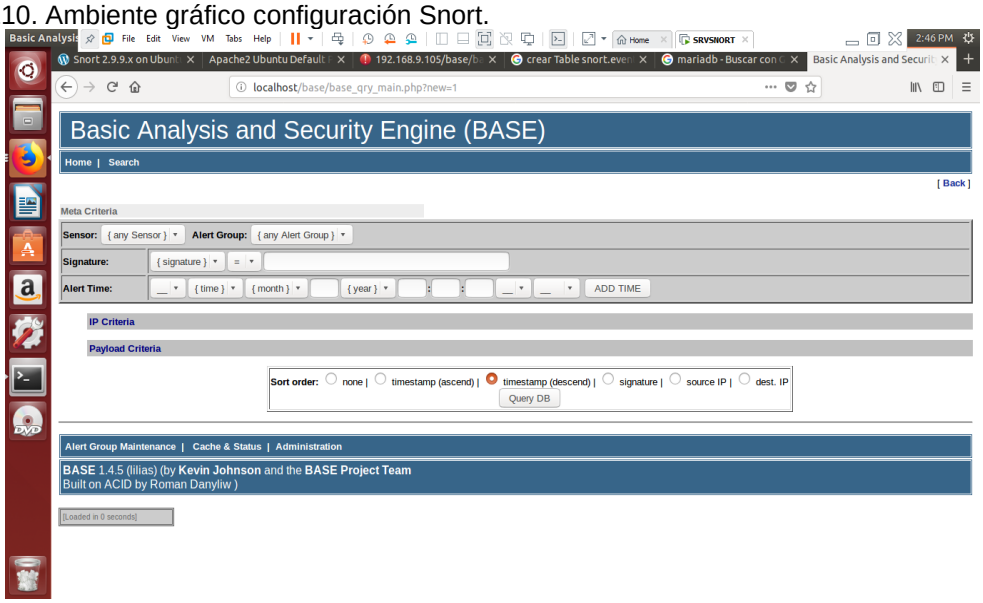
Figura 109. Entorno grafico Home de Snort.



Fuente: Sistema IDS Snort, entorno gráfico de home, Omar Tique M., mayo de 2020.

En la figura. 109. Se indica, la interfaz de acceso a Snort y se visualiza la interfaz en Home, desde donde se puede acceder a las diferentes opciones de la herramienta.

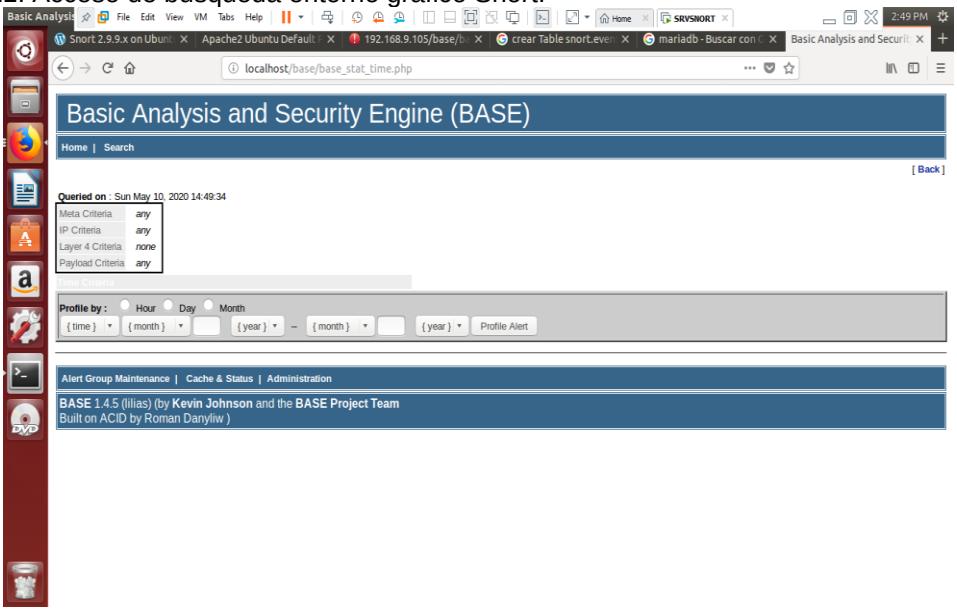
Figura 110. Ambiente gráfico configuración Snort.



Fuente: Sistema IDS Snort, entorno gráfico de (BASE), Omar Tique M., mayo de 2020.

En la figura. 110. Se indica, la interfaz de búsqueda y configuración de sensores que permiten el monitoreo y aplicación de regles de acuerdo con la necesidad que se presente.

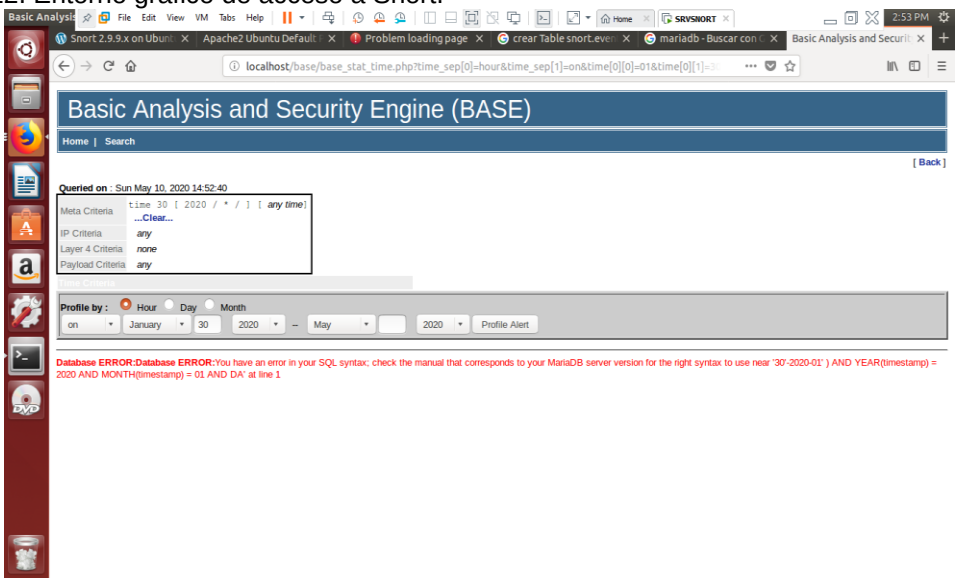
Figura 111. Acceso de búsqueda entorno gráfico Snort.



Fuente: Sistema IDS Snort, entorno gráfico de (BASE), Omar Tique M., mayo de 2020.

En la figura. 111. Se indica, la interfaz de acceso a la configuración de criterios de búsqueda y reglas aplicadas en función de tiempo.

Figura 112. Entorno gráfico de acceso a Snort.

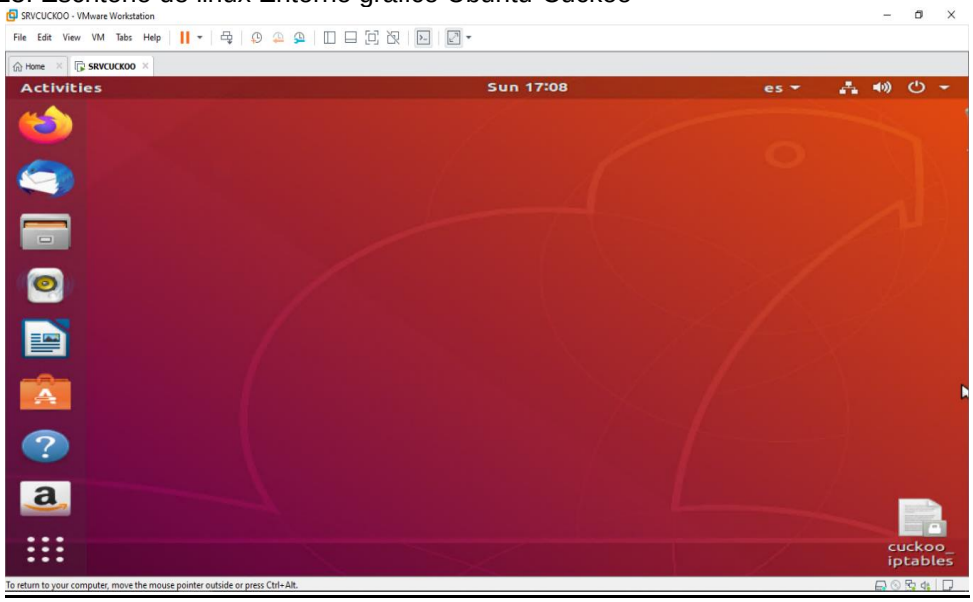


Fuente: Sistema IDS Snort, entorno gráfico de (BASE), Omar Tique M., mayo de 2020.

En la figura. 112. Se indica, la interfaz que se ha realizado una búsqueda en función de tiempo y valores, pero arroja un error en la base de datos, esto se debe a que hasta el momento esta no se configurado correctamente.

8.4.3 Acceso a máquina virtual sandbox Cuckoo

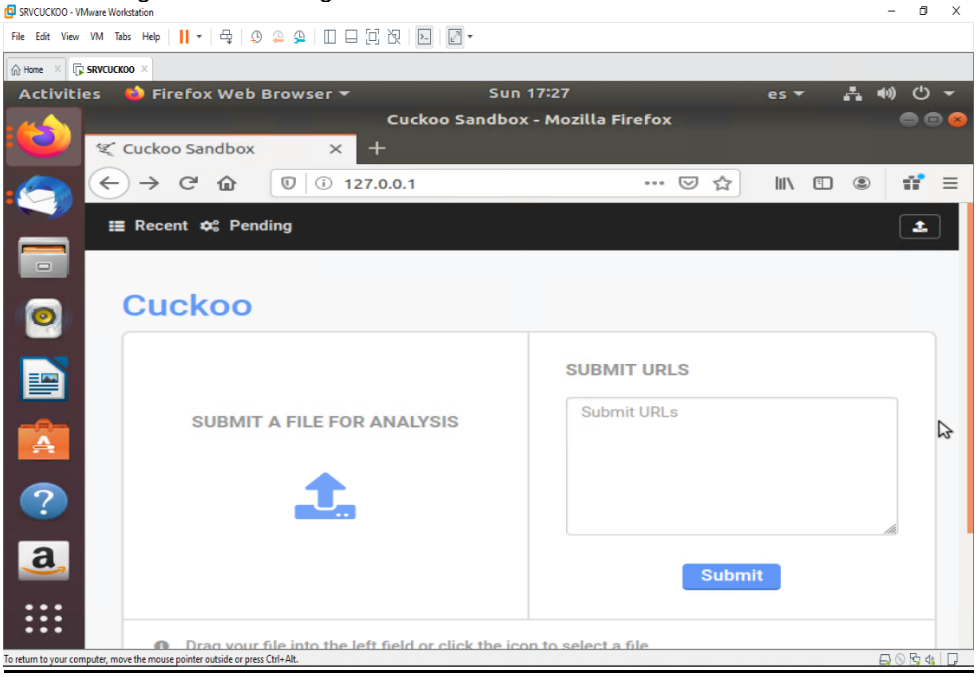
Figura 113. Escritorio de linux Entorno grafico Ubuntu-Cuckoo



Fuente: Sistema operativo Ubuntu (64 Bits), Omar Tique M., mayo de 2020.

En la figura. 113. Se indica, la interfaz del escritorio de la máquina de Ubuntu virtualizada en la cual se creado, montado y configurado nuestra sandbox (Cuckoo).

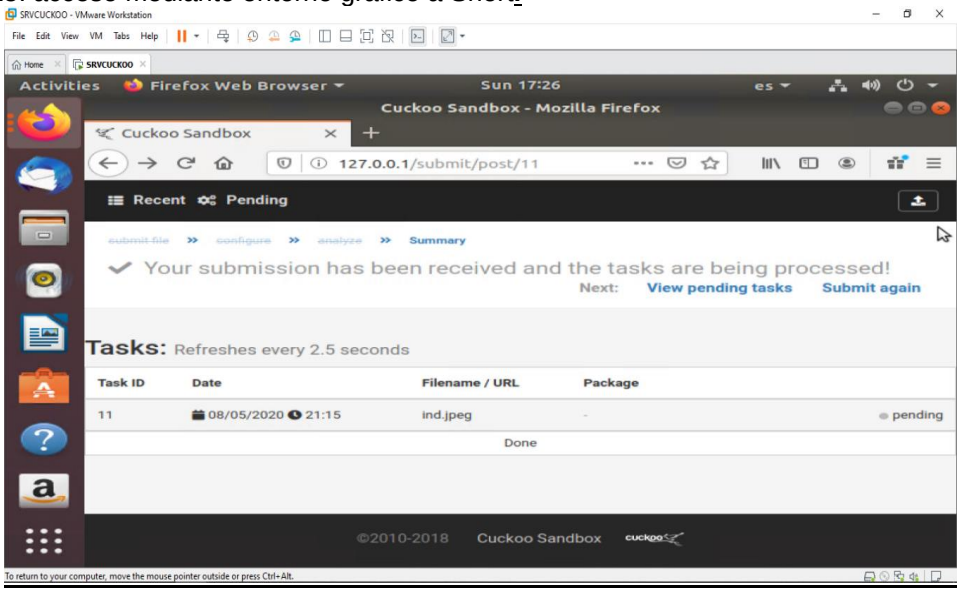
Figura 114. Acceso gráfico a Testing Sandbox.



Fuente: Sandbox Cuckoo en Sistema operativo Ubuntu (64 Bit), Omar Tique M., mayo de 2020.

En la figura. 114. Se indica, la interfaz de prueba de funcionamiento de la sandbox, en esta se puede evidenciar de las dos opciones básicas de revisión, una para la validación de archivos maliciosos y la otra para realizar el test de sitios web.

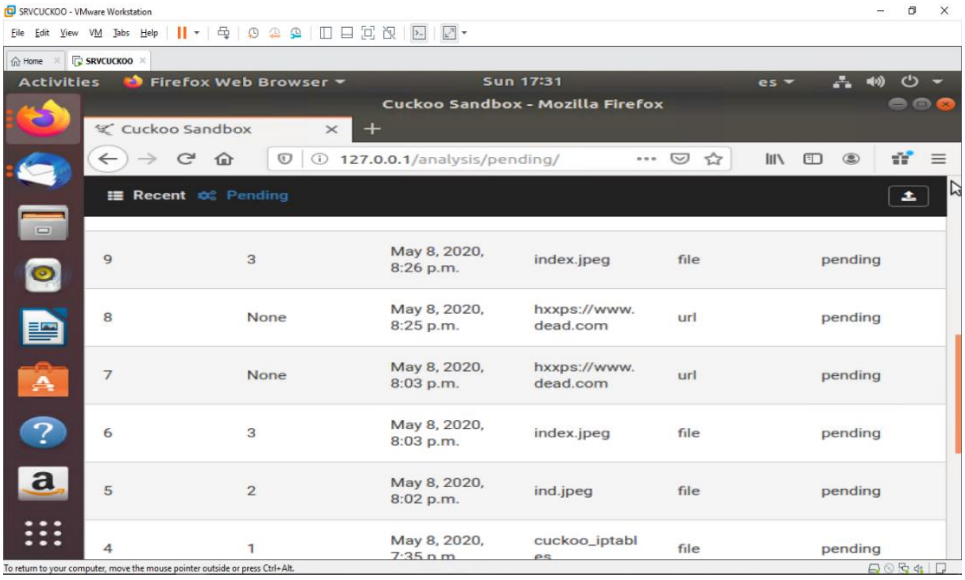
Figura 115. acceso mediante entorno gráfico a Snort.



Fuente: Sandbox Cuckoo en Sistema operativo Ubuntu (64 Bit), Omar Tique M., mayo de 2020.

En la figura. 115. Se indica, la interfaz de prueba de funcionamiento con un archivo la cual fue realizada durante la creación del video a presentar en la tarea, esta no se visualiza en el video en razón a que se accedió de forma remota a la maquina y no tomo esta descripción realizada.

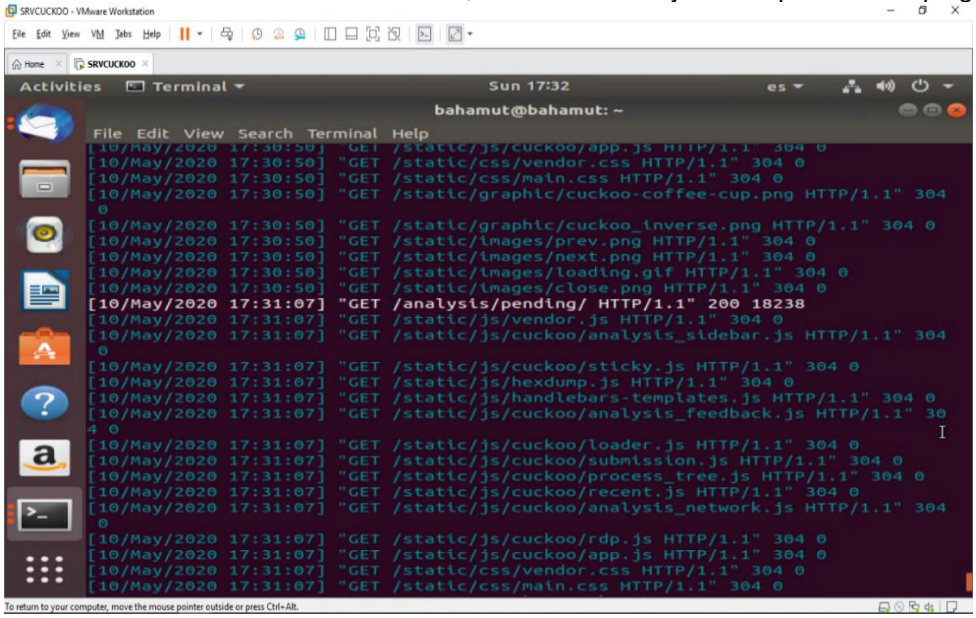
Figura 116. Archivos testeados en la sandbox.



Fuente: Sandbox Cuckoo en Sistema operativo Ubuntu (64 Bit), Omar Tique M., mayo de 2020.

En la figura. 116. Se indica, en la interfaz las pruebas de funcionamiento realizadas en el video demostrativo de funcionamiento, este arroja los resultados de acuerdo con la criticidad de los archivos y las amenazas que tenga embebidas.

Figura 117. Acceso a Cuckoo mediante consola, verificación de ejecución proceso desplegado.



Fuente: Sandbox Cuckoo en Sistema operativo Ubuntu (64 Bit), Omar Tique M., mayo de 2020.

En la figura. 117. Se indica, en la interfaz que se ha validado el funcionamiento del servidor durante las pruebas realizadas, se puede observar que realmente realiza un Testing sobre la información, archivo y url ingresadas a través de la interfaz gráfica de la aplicación.

8.4.3 Diseño técnico y creación del CSIRT

En este caso es el entregable del proyecto aplicado propuesto como una transferencia de conocimiento, consiste en el **DISEÑO TÉCNICO, CONFIGURACIÓN BÁSICA Y CREACION DEL CSIRT EN CIBERSECURITY DE COLOMBIA LTDA**., que finalmente se ha logrado realizar e implementar para la prevención y la investigación de incidentes de seguridad de tipo informático.

En este caso se han instalado y configurado las siguientes herramientas y aplicaciones informáticas (básicas) con el objeto de ser puestas en funcionamiento al interior de la empresa, administradas y monitoreadas por el personal que conforma el equipo de respuesta e investigación a incidentes informáticos, esto es:

Puestos de trabajo
Centro de cableado
Rack de comunicaciones
Alíen Vault OSSIM
Sandbox Cuckoo
IDS/IPS Snort

Esta es la infraestructura, los equipos y las herramientas mínimas con las cuales debe contar cualquier CSIRT que se dedique a las actividades de monitoreo, respuesta e investigación de incidentes informáticos; como se ha podido observar existe los servicios de Informática Forense que también pueden ser prestados por un equipo de estos, pero que de acuerdo al alcance del proyecto y la infraestructura disponible en su momento del desarrollo, las circunstancias particulares de cuarentena decretadas por la pandemia y la emergencia sanitaria, los recurso han sido muy limitados; además se debe tener en cuenta los costos de las herramientas informáticas y equipos necesarios empleados en el análisis forense.

8.4. Tabla presupuestal diseño técnico y creación del CSIRT

En la tabla siguiente se ha realizado la proyección del presupuesto que se necesita en función de lograr la adquisición mínima de elementos y equipos, así como software y soporte para lograr la realización de pruebas funcionales de concepto previo a la implementación de un CSIRT, con los componentes esenciales que permitan la realización de atención de incidentes de seguridad informática.

Tabla. 2. Cuadro de presupuesto

Recurso	Descripción	Presupuesto			
		Valor unitario	**Cantidad**	**Financia Estudiante**	**Total**
Recurso Humano	Instalación equipo	$150000	01	X	$150000
	Instalación OS	$150000	01	X	$150000
	Instalación y configuración aplicaciones	$1200000	01	X	$1200000
	Implementación	$1´000.000	01	X	$1´000.000
	Integración herramientas	$1200000	01	X	$1200000
Equipos / Software	Server	$5000000	01	X	$5000000
	Router	$1200000	01	X	$1200000
	Switchs	$1000000	01	X	$1000000
	Distribución Linux como OS	$2000000	01	X	$2000000
	ESXi vSphere	$1500000	01	X	$1500000
	VirtualBox	$500000	01	X	$500000

Fuente: Elaboración de presupuesto de proyecto, Omar Tique M., mayo de 2020.

Tabla. 2. (Continuación)

Recurso	Descripción	Presupuesto			
		Valor unitario	**Cantidad**	**Financia Estudiante**	**Total**
Equipos / Software	Proxmox	$500000	01	X	$500000
	VCSA 6.7	$1500000	01	X	$1500000
Viajes/Salidas	N/A	N/A	N/A	N/A	N/A
Materiales y suministros	USB	$ 25.000	02	X	$ 50.000
	Videograbadora	$ 550.000	01	X	$ 550.000
	Cámara Fotográfica	$ 250.000	01	X	$ 250.000
	Bolígrafos	$ 1500	02	X	$ 3000
	DVD	$ 2.500	02	X	$ 5.000
	CD	$ 1.500	02	X	$ 3000
Bibliografía	Papel (Resma)	$ 15000	01	X	$ 15000
	Internet	$ 500	300	X	$ 150.000
	Fotocopia	$ 100	90	X	$ 9.000

Fuente: Elaboración de presupuesto de proyecto, Omar Tique M., mayo de 2020.

Tabla 2. (Continuación)

Recurso	Descripción	Presupuesto			
		Valor unitario	**Cantidad**	**Financia Estudiante**	**Total**
Análisis y manejo	Equipo de computo	$2000.000	01	X	$ 2000.000
	Celular	$ 650.000	01	X	$ 650.000
	Plan de minutos	$ 58.000	12	X	$ 696.000
Total				**$**	**15,922,005.00**

Fuente: Elaboración de presupuesto de proyecto, Omar Tique M., mayo de 2020.

8.4.5 Cumplimiento del Desarrollo de los Objetivos

Los objetivos propuestos en el presente trabajo de investigación se han logrado en razón a lo siguiente:

Se ha logrado definir con claridad que es un CSIRT, los servicios que presta, sus orígenes y la razón de su existencia.

Se ha realizado un análisis sobre principios, su estandarización, el marco legal que aplica en nuestro país.

Se logra tener claridad sobre su importancia y la necesidad que reviste la adquisición de este conocimiento por parte del personal de ingenieros administradores de infraestructura de TIC´s para poder mantener la Disponibilidad, confidencialidad e integridad de los datos a través de actividades preventivas y la investigación de incidentes informáticos.

Se ha desarrollado el laboratorio a nivel físico de montaje y creación de una red LAN en la cual es posible realizar pruebas de funcionamiento de este tipo de herramientas y que se orientan al aseguramiento de infraestructura tecnológica y las aplicaciones que determinan y soportan los servicios y la administración de una empresa.

Se logra la configuración de equipos, instalación de sistemas operativos, la instalación y configuración de las herramientas básicas que están orientadas a ser usadas al interior de un equipo de respuestas; estas han sido el SIEM de Alíen Vault OSSIM, la herramienta Sandbox de Cuckoo y el HIDS de Snort, analizador y detección de vulnerabilidades y amenazas Nessus.

Resultados del proyecto

Tabla 3. Cuadro de resultados/indicadores

Resultado/Producto Esperado	Indicador	Beneficiario
Conocer que es y cómo funciona un CSIRT	100%	Administrador de TI
Identificar las herramientas técnicas de un CSIRT	100%	Administrador de TI
Realizar la configuración de las herramientas técnicas y tecnológicas en un CSIRT.	100%	Administrador de TI
Saber cuáles son los procesos, procedimientos y servicios que presta un CSIRT.	100%	Administrador de TI

Fuente: Elaboración de cuadro de resultados, Omar Tique M., mayo de 2020.

9 CONCLUSIONES

Se concluye que mediante la presente investigación se evidencia que la documentación existente aplica a seguir como un referente de los implementados en otros países y que debe tenerse en cuenta su creación en función de sus objetivos y tipos de CSIRT o equipos de respuesta a incidentes informáticos.

Es evidente que debe realizarse una definición del tipo de CSIRT que se implementara, esto de acuerdo con los servicios que prestará y así mismo definirá las herramientas tecnológicas necesarias y serán estas las que determinen su configuración final.

Se evidenció que validando información de sitios web existen parámetros que hay que seguir y definir y lograr contar con procesos y procedimientos definidos que eviten malos procedimientos y la investigación que se realice no sea efectiva.

Se concluye que las configuraciones de las herramientas tecnológicas, sistemas operativos, tipo de servidores son propias de cada equipo de respuesta a incidentes CSIRT en donde influyen sus conocimientos y experiencia; además del nivel complejidad que cada uno quiera imprimirle y sus capacidades de respuesta con se cuenten, por tanto, esta parte no se encuentra documentada, se documentara en el desarrollo del proyecto cuando se implementen las herramientas tecnológicas.

Se ha concluido con que debe existir total sinergia entre dos aspectos fundamentales al interior de la infraestructura tecnológica, esto es la infraestructura de red y la infraestructura de servidores, aplicaciones, aplicaciones y herramientas administrativas, las de monitoreo y búsqueda de vulnerabilidades y detección de amenazas; ha sido lo evidenciado en la instalación, configuración y puesta en pruebas de funcionamiento las herramientas del presente proyecto, por tanto es recomendable la inclusión de una herramienta automatizada para la gestión de incidentes de seguridad, que permita ser orientada a su vez a la auditoria.

10 RECOMENDACIONES

1. Es necesario documentar la normatividad y los estándares aplicados a la seguridad informática, especialmente los procedimientos a seguirse en la atención e investigación de los casos que sean atendidos frente a las vulnerabilidades materializadas y de conocimiento directo por el equipo de repuesta al interior de la infraestructura tecnológica.

2. Incluir ciberseguridad y ciberdefensa, capacitación para integrar el CSIRT con otras organizaciones, empresas e instituciones del sector público y privado, con el objeto de lograr la contención de amenazas y explotación de vulnerabilidades mediante la actualización constante, mediante la base de conocimientos que conservan los equipos creados mediante el mismo objetivo.

3. Desarrollar estrategias aplicables a la seguridad informática, proyectar y realizar un plan de capacitación que cubra el área de acción frente a la atención, prevención, investigación de incidentes presentados en la infraestructura tecnológica, de igual forma si se incorpora servicios de Informática Forense, se debe capacitar en Derecho Informático, así como también en el manejo de la evidencia digital a los profesionales que integren el equipo de respuesta.

4. Capacitar constantemente al personal de ingenieros que formen parte del equipo de respuesta a incidentes informáticos y su investigación, este personal se encuentran en primera línea ante cualquier evento, tanto externo como interno, de igual forma interactuaran directamente con evidencias localizadas y que deberán focalizar en aras de lograr cumplir con los objetivos del CSIRT y la contención de ataques informáticos, y salvaguardar el activo de la empresa.

5. Implementar este tipo de herramientas para el monitoreo de infraestructura, la búsqueda de vulnerabilidades y la detección de amenazas de tipo informático en los sistemas de información y comunicaciones, así como en la preservación de los datos es sus variantes definidas como lo es su producción, transformación y transmisión de estos.

11. REFERENCIAS BIBLIOGRÁFICAS

Academy, Cisco networking. Introduction to Cybersecurity. San Francisco San Francisco, EE.UU. 10 enero 2018. Disponible en: https://static-course-assets.s3.amazonaws.com/CyberEss/es/index.html#4.1.1.1

Administrar máquinas virtuales de vSphere, VMware vSphere 6.7, VMware ESXi 6.7, vCenter Server 6.7. 2009-2018 VMware, Inc. 3401 Hillview Ave. Palo Alto, CA 94304 EE.UU. abril 04 2018. P 17. Disponible en: https://www.vmware.com/latam. https://docs.vmware.com/es/.

Agencia Europea de Seguridad de las Redes y de la Información. Como Crear un CSIRT paso a paso. Producto WP2006/5.1 (CERT-D1/D2). Heraklion, C reta: ENISA, 2006. p. 7.

ANSI/TIA. ANSI/TIA-568.0-D-2015, Generic Telecommunications Cabling for Customer Premises. Courthouse Road, Suite 200 Arlington, VA 22201 U.S.A.. 14 septiembre 2015. p 13.

ANSI/TIA. ANSI/TIA-568.1-D Commercial Building Telecommunications Infrastructure Standard. Courthouse Road, Suite 200 Arlington, VA 22201 U.S.A.. 09 SEPTEMBER 2015.

ANSI/TIA. NSI/TIA-568.3-D-2016, Optical Fiber Cabling and Components Standard. Courthouse Road, Suite 200 Arlington, VA 22201 U.S.A. 25 octubre 2016. p.

Asamblea Nacional Constituyente. Constitución Política de Colombia. Bogotá D.C. Colombia: Constituyente. 1991. p.3.

Asamblea Nacional Constituyente. Constitución Política de Colombia. Bogotá D.C. Colombia: Constituyente. 1991. p.11.

AT&T cybersecurity, AlienVault OSSIM The world's most widely used Open Source SIEM: AlienVault OSSIM {en línea}. {12 de Noviembre 2019}. Disponible en: (https://www.alienvault.com/products/ossim)

Buenas Prácticas CCN-CERT BP-01/16, Principios y recomendaciones básicas en Ciberseguridad. Centro Criptológico Nacional. España. Octubre de 2017. p. 25.

CENTRO CRIPTOLOGICO NACIONAL. Guía de seguridad (CCN-STIC-810). Guía de creación de un CERT / CSIRT. Madrid España: ENS, 2011. p.9.

Certified Information Systems Security Professional Study Guide, Seventh Edition, CISSP 7°, James Michael Stewart, Mike Chapple, Darril Gibson. Indianápolis, Indiana New York United States. Septiembre 10 2015. p. 742.

Certified Information Systems Security Professional Study Guide, Seventh Edition., James Michael Stewart, Mike Chapple, Darril Gibson., Indianápolis, Indiana, EE. UU., 2015. p 744.

Descripción, características de ESXi vSphere. VMware Inc. {en línea}. {15 de marzo 2020}. 3401 Hillview Ave -Palo Alto, CA 94304. Estados Unidos. Disponible en: https://www.vmware.com/latam/products/esxi-and-esx.html, https://www.vmware.com/latam

INCIDENT RESPONSE & COMPUTER FORENSICS. Second Edition. Introduction to the Incident Response Process. CHRIS PROSISE, KEVIN MANDIA, Matt Pepe. McGraw-Hill Companies, Inc. San Francisco, New York Chicago United States of América. Enero 20 2003. p 11.

Plan Estatal de Investigación Científica y Técnica y de Innovación 2013-2016. {en línea}. España. Disponible en: http://www.plannacionalidi.es/. Fecha de consulta 23 de septiembre de 2019.

Organizational Models for Computer Security Incident Response Teams (CSIRTs). Killcrece, Georgia; Kossakowski, Klaus-Peter; Ruefle, Robin; Zajicek, Mark. Copyright 2004. Carnegie Mellon University. Pittsburgh. 2003 December. p.

Handbook for Computer Security Incident Response Teams (CSIRTs) First release: December 1998, 2nd Edition. West-Brown, Moira J.; Stikvoort, Don; Kossakowski, Klaus-Peter; Killcrece, Georgia; Ruefle, Robin; Zajicek, Mark. The Software Engineering Institute. Pittsburgh, U.S. 2003 April. p.

VMware Inc., VMware vSphere. Administrar máquinas virtuales de vSphere. Palo Alto, CA 94304.2020. p 9.

User Manual Versión 6.1.14. Oracle VM VirtualBox., Oracle Corporation 2004-2020. Weinstadt-Alemania. 2020. p 12. Disponible en. http://www.virtualbox.org.

PROXMOX VE ADMINISTRATION GUIDE RELEASE 6.2. Proxmox Server Solutions GmbH. Dietmar y Martin Maurer 2008. Headquatered Viena Austria. Mayo 10 2020. p 2. Disponible en: www.proxmox.com.

PELLO XABIER, Altadill Izura. IPTABLES Manual práctico. Bilbao País Vasco. p 1.
1. Ibid., p 4

PELLO XABIER, Altadill Izura. IPTABLES Manual práctico. Bilbao País Vasco. p 1.

Snort-Cisco. SNORT Users Manual 2.9.16. The Snort Project. Writing Snort Rules by Martin Roesch and further work from Chris Green. The Snort Team. {en línea} {12 April 8, 2020}. p 9. Disponible en: https://www.snort.org/ , https://www.snort.org/documents/1.

Neil Archibald, Gilbert Ramírez, Noam Rathaus. Nessus, Snort, & Ethereal, Power Tools; Customizing Open Source Security Applications. Hingham St, Rockland, Massachusetts United States. Septiembre 2005. p 14.

Tecnología + Informática, Guillermo Venturini. Que es un antivirus {En línea}. {15 noviembre 2019}. Disponible en: https://www.tecnologia-informatica.com/que-es-un-antivirus-como-funciona/

Fundación Wikimedia, Inc. es.wikipedia.org. Zimbra. San francisco California, {en línea}. {agosto 12 de 2019}. p1. Disponible en:(https://es.wikipedia.org/wiki/Zimbra).

VMware Inc., VMware vSphere. Administrar máquinas virtuales de vSphere. Palo Alto, CA 94304. p 9. Disponible en: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiysJzyvqPsAhWirVkKHWnJAlwQFjAAegQIBxAC&url=https%3A%2F%2Fdocs.vmware.com%2Fes%2FVMware-vSphere%2F6.7%2Fvsphere-esxi-vcenter-server-67-virtual-machine-admin-guide.pdf&usg=AOvVaw1a_O6OTxw9FRdkPEf2MczI

ultimobyte, Correo electrónico Zimbra, Av. Aragón 8 - Entlo. E 46021 Valencia. {en línea}. p1. Disponible en: (https://www.ultimobyte.es/productos/zimbra-correo-electronico-y-groupware).

Georg Wicherski, David Watson, Christian Seifert. Cuckoo Sandbox Book, Release 2.0.6. Mountain View California Estados Unidos. 06 octubre 2018. p 27.

Nessus Professional. Nessus Professional. Hoja de datos de Nessus Professional. {en línea}. Maryland. p1. Disponible en. https://es-la.tenable.com/data-sheets/nessus-professional

GitHub, Inc. phpservermon {en línea}. San Francisco. p1. © 2019. Disponible en: GitHub - phpservermon/phpservermon: PHP Server Monitor

Nmap Security Scanner. nmap.org, Gordon Lyon. Palo Alto, California, EE. UU. {En línea}. {20 enero 2019}. Disponible en: https://nmap.org/

Phpservermon. GitHub, Inc. 2019, Pepijn Over. {En línea}. {25 enero 2019}. Disponible en: https://github.com/. https://github.com/phpservermon/phpservermon

Tecnología + Informática, Guillermo Venturini. Que es la criptografía. {En línea}. {10 febrero 2019}. Disponible en: https://tecnologia-informatica.com/que-es-la-criptografia/

ISO/IEC 27002:2005. Estándar para la seguridad de la información. Ginebra Suiza.

ISO/IEC 270021:2005. 2005. p.

ISO/IEC 27002:2005, op. cit.

ISO/IEC 27035-1:2016. Information Technology — Security techniques — Information Security Incident Management — Part 1: Principles of Incident Management. Ginebra Suiza: 2016.

INTERNATIONAL STANDARD ISO/IEC 27000:2018, Fifth Edition 2018-02. Information Technology — Security techniques — Information security management systems — Overview and vocabulary. Vernier, Geneva, Switzerland. 10 febrero 2018. P 11. Disponible en: https://www.iso.org/standard/73906.html

ISO/IEC_INCONTEC INTERNACIONAL. GUÍA TÉCNICA COLOMBIANA GTC ISO/IEC 27002 TECNOLOGÍA DE LA INFORMACIÓN. Bogotá D.C Cundinamarca Colombia, 22 Julio 2015.

Zajicek, Moira J. West-Brown Don Stikvoort Klaus-Peter Kossakowski Georgia Killcrece Robin Ruefle Mark. Handbook for Computer Security Incident Response Teams (CSIRTs), First release: December 1998 2^{nd} Edition: April 2003. 10 abril 2003. P 27. Disponible en: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305

Organización de los Estados Americanos OEA, Buenas prácticas para establecer un CSIRT nacional. 1889 F Street, N.W., Washington, D.C., 2006, U.S.A. 25 Abril 2016. p. www.oas.org/cyber/