DISEÑO DE LA DOCUMENTACIÓN TÉCNICA PARA LA IMPLEMENTACIÓN DE UN EQUIPO DE RESPUESTA ANTE EMERGENCIAS INFORMÁTICAS (CSIRT) PARA LA EMPRESA CASO DE ESTUDIO CIBERSECURITY DE COLOMBIA LTDA.

DUVAN ESTEBAN URREGO FERNANDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA.
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ

2020

DISEÑO DE LA DOCUMENTACIÓN TÉCNICA PARA LA IMPLEMENTACIÓN DE UN EQUIPO DE RESPUESTA ANTE EMERGENCIAS INFORMÁTICAS (CSIRT) PARA LA EMPRESA CASO DE ESTUDIO CIBERSECURITY DE COLOMBIA LTDA.

DUVAN ESTEBAN URREGO FERNANDEZ

PROYECTO

PARA OBTENER EL GRADO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA.

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ

2020

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

Bogotá Colombia,

AGRADECIMIENTOS.

Este trabajo de grado es dedicado a la memoria de mi abuela María del Carmen, quién me animó en cada paso que daba. Sus consejos siempre en busca de una mejora para mi vida espiritual, social amorosa, profesional, familiar y económica.

A mis Padres

Que con gran esfuerzo y dedicación día a día me demuestran su infinito amor y dedicación, gracias a ellos soy la persona y profesional hoy en día orgullosamente y con la cara muy en alto agradezco a Arcadio Urrego y Flor María Fernández, mi mayor motor para seguir avanzando.

A mi Novia

A medida que transcurre el tiempo encuentras personas maravillosas que generan un apoyo incondicional en cada paso que das, con sus consejos, amor y paciencia se convierten en un apoyo incondicional para cumplir tus metas.

CONTENIDO

Pág.

INTRODUCCION 11
1 PLANTEAMIENTO DEL PROBLEMA 12
2 JUSTIFICACIÓN 14
3 OBJETIVOS 15
3.1 OBJETIVO GENERAL 15
3.2 OBJETIVOS ESPECÍFICOS 15
4 MARCO REFERENCIAL 16
4.1 MARCO TEÓRICO 16
4.1.1 Equipo de respuesta ante incidentes de seguridad de la información (CSIRT) 16
4.1.2 Seguridad informática 20
4.1.3 Amenaza de seguridad informática 21
4.1.4 CSIRTs en Colombia 21
4.1.5 Ciberataques en Colombia 23
4.2 MARCO CONCEPTUAL 23
4.2.1 IPS 23
4.2.2 UTM 24
4.2.3 Honeypot 25
4.2.4 Hardening 26
4.2.5 Vulnerabilidad 26
4.2.6 Incidente de seguridad informática 26
4.2.7 Servicio 27
4.2.8 Proceso 28
4.3 MARCO LEGAL 28
4.3.1 Ley 1273 de 2009 (enero 05) 28
4.3.2 Proyecto de ley 241 de 2011 del senado 29
4.3.3 Ley estatutaria 1581 de 2012. 30
4.4 MARCO ESPACIAL 31

4.5 MARCO METODOLÓGICO 31
5 RESULTADOS 32
5.1 HERRAMIENTAS DE SOFTWARE PROPUESTAS PARA ELCSIRT 32
5.1.1 Sitio web 32
5.1.2 Correo electrónico 33
5.1.3 Manejo de incidentes 34
5.1.4 Acceso remoto 35
5.1.5 Sistema SIEM (security incident and event management systems) 36
5.1.6 Software de Copias de seguridad 36
5.1.7 Software de Sandbox 38
5.1.8 Sistema CRM (customer relationship management) 40
5.1.9 Identificación de vulnerabilidades 41
5.2 HERRAMIENTAS DE HARDWARE PROPUESTAS PARA EL CSIRT 42
5.2.1 Servidores 42
5.2.2 Equipos de comunicación (telefonía) 42
5.2.3 Equipos de computación PC. 42
5.2.4 Hadware de Firewall 43
5.2.5 IPS 43
5.2.6 Honeypot: 43
5.2.7 Hardening: 43
5.2.8 FAX 43
5.2.9 Sistema de respaldo de datos 43
5.2.10 Almacenamiento lógico portátil. 44
5.3 DEPENDENCIAS PARA LA CONFORMACIÓN DEL CSIRT 44
5.3.1 Dirección: 44
5.3.2 Operaciones y seguridad de la información: 45
5.3.3 Investigación forense y nuevos desarrollos 45
5.3.4 Telecomunicaciones y TI 45
5.3.5 Relaciones Públicas 46
5.3.6 Jurídico 46
5.4 PERFILES DEL EQUIPO DE TRABAJO PARA LA CONFORMACIÓN DEL CSIRT 46

5.4.1 Rol: director de CSIRT 47
5.4.2 Rol: Analista de operaciones y seguridad de la información 48
5.4.3 Rol: analista de investigación forense y nuevos desarrollos 48
5.4.4 Rol: analista de telecomunicaciones y TI 49
5.4.5 Rol: analista en relaciones públicas. 49
5.4.6 Rol: especialista Jurídico. 50
5.5 Esquema organizativo propuesto para el CISRT 50
Fuente: Elaboración propia. 51
5.5.1 Topología de red 51
5.5.2 Planta física 53
5.6 GUIA TÉCNICA DE INSTALACIÓN DE HERRAMIENTAS DE SOFTWARE 55
5.6.1 Instalación de Bacula 55
5.6.2 Instalación de Cuckoo Sandbox 71
5.7 AlienVault SIEM (OSSIM) 89
5.8 Instalación de NAGIOS. 102
6 CONCLUSIONES 118
7 BIBLIOGRAFÍA 119

LISTA DE TABLAS

Pág.

Tabla 1: Posibles servicios prestados por un CSIRT. 18
Tabla 2: Dimensionamiento de Bacula 55
Tabla 3 Recursos utilizados de hardware instalación de prueba Cuckoo Sandbox 71
Tabla 4 Requisitos mínimos del sistema de hardware 90
Tabla 5: Requerimientos Nagios. 103

LISTA DE FIGURAS

Pág.

Figura 1: Etapas para la implementación de un CSIRT 17
Figura 2: Tipos de CSIRT a nivel mundial 20
Figura 3: Packet processing Flow 24
Figura 4: Amenazas controladas con UTM 25
Figura 5: Redes de honeypots 25
Figura 6: Proceso de la gestión de incidentes 27
Figura 7: Components or Service 38
Figura 8 Organigrama propuesto para la implementación del CISRT 51
Figura 9 Esquema de red CSIRT, Cibersecurity de Colombia 52
Figura 10: Propuesta de planta física CSIRT. 53
Figura 11: Bacula Architecture 57
Figura 12: Actualización de repositorios CentOS. 57
Figura 13. Instalación de módulos de Bacula y BD 58
Figura 14: Creación de base de datos y tablas Bacula 59
Figura 15: Modificación parámetros de seguridad MariaDB 59
Figura 16: Contraseña de usuario Bacula. 60
Figura 17: Habilitar Demonio MariaDB 60
Figura 18:Selección de motor de base de datos 61
Figura 19: Creación directorios Bacula 61
Figura 20:Permisos directorios Bacula 62
Figura 21: Apertura bacula-dir.conf 62
Figura 22: Configuración recurso Director. 63
Figura 23: Trabajo LocalFile 63
Figura 24: Trabajo restauración de archivos 64
Figura *25: Configuración FileSet* 64
Figura 26: Configuración almacenamiento Backup 65
Figura 27: Configuración recurso Catalogo. 65
Figura 28: Configuración recurso Pool para BackUp 66
Figura 29: Verificación archivo bacula-dir.conf 66
Figura 30: Apertura archivo bacula-sd.conf 67
Figura 31: Configuración IP servidor de Backup 67
Figura 32: Configuración dispositivos de almacenamiento. 67
Figura 33: Comprobación archivo bacula-sd.conf 68
Figura 34: Configuración contraseñas bacula-dir 68
Figura 35: Configuracion de contraseñas bacula-sd 69
Figura 36: Configuración de contraseñas bacula-fd 69
Figura 37: Inicio de servicios de Bacula 70
Figura 38: Configuración de demonios Bacula. 70
Figura 39: Arquitectura de red de Cuckoo SandBox. 72

Figura 40: Instalación de software requerido. 73
Figura 41: Creación de usuario Cuckoo. 73
Figura 42: Configuración de permisos usuario Cuckoo. 74
Figura 43: Descarga de imagen ISO. 75
Figura 44: Instalación VirtualBox 75
Figura 45: Configuración grupo vboxusers 76
Figura 46: Instalación de dependencias. 76
Figura 47: Instalación de dependencias zlib y libjpg 76
Figura 48: Instalación de dependencias Python. 77
Figura 49: Acceso usuario cuckoo. 77
Figura 50: Ejecución de instalación Cuckoo 78
Figura 51: Configuración de adaptador vboxnet0 78
Figura 52: Montar imagen de windows7 78
Figura 53: Creación de máquina virtual win7x64. 79
Figura 54: Clonación de maquina win7x64base 79
Figura 55: Lista de paquetes vmcloak 80
Figura 56: Instalación de software en máquina virtual 80
Figura 57: Snapshot de máquina virtual win7x64cuckoo 81
Figura 58: Lista de máquinas virtuales. 81
Figura 59: Creación de directorio userhome/.cuckoo 82
Figura 60: Ruta personalizada cwd. 82
Figura 61: instalación de motor de BD Postgresql. 83
Figura 62: Instalación de psycopg2 83
Figura 63: Creación de base de datos postgres. 84
Figura 64: Configuración de conexión Postgressql 84
Figura 65: Agregar máquinas virtuales a Cuckoo 85
Figura 66: Instalar firmas más recientes de Cuckoo. 85
Figura 67: Permiso de acceso a las interfaces de red 86
Figura 68: Reglas de firewall para Cuckoo 86
Figura 69: Instalación de motor BD MongoDB 87
Figura 70: Habilitar base de datos MongoDB 87
Figura 71: Interfaz WEB Cuckoo. 88
Figura 72: Máquina virtual Windows7 88
Figura 73: System Architecture and Components 90
Figura 74: Ventana de inicio OSSIM 91
Figura 75 Selección de Idioma OSSIM 92
Figura 76 Selección de ubicación 92
Figura 77 Carga de componentes del instalador 93
Figura 78 Configuración de Red 93
Figura 79 Ingreso de máscara de red 93
Figura 80 Configuración IP de la red 94
Figura 81 Configuración de usuario y contraseña 94

Figura 82 Formateando particiones de disco 95
Figura 83 Fin de la instalación 95
Figura 84 Inicio por consola 96
Figura 85 Verificación de inicio 96
Figura 86 Crear cuenta de administrador 97
Figura 87 Iniciar sesión 97
Figura 88 Ventana de inicio 98
Figura 89 Configurar red 99
Figura 90 Agregar activos 99
Figura 91 Configuración de implementar HIDS 100
Figura 92 Implementar host 100
Figura 93 Unirse a OTS 101
Figura 94 Panel principal 101
Figura 95 Arquitectura usada para monitorear con Nagios. 104
Figura 96 Instalación de repositorios 104
Figura 97 Instalación de paquetes de descarga de NAGIOS 105
Figura 98 Archivos para instalación de NAGIOS 105
Figura 99 Descarga de NAGIOS 106
Figura 100 Descompresión de archivo de instalación 106
Figura 101 Cambio de directorio 106
Figura 102 Ejecución de script de verificación 107
Figura 103 Mensaje de verificación 107
Figura 104 Ejecución de comando MAKE 108
Figura 105 Mensaje de validación 108
Figura 106 Creación de nuevo usuario 108
Figura 107 Agregar usuario al grupo 109
Figura 108 Instalación de archivos 109
Figura 109 Crear directorio externo 109
Figura 110 Instalación de archivos de configuración de Nagios 110
Figura 111 Configuración de servidor Apache 110
Figura 112 Verificación de servidor Apache 111
Figura 113 instalación del archivo unidad system 111
Figura 114 Creación del administrador llamado nagiosadmin 112
Figura 115 Reinicio de servicios de apache 112
Figura 116 Apertura de puertos del firewall 112
Figura 117 Descargas de repositorios de GitHub 113
Figura 118 Archivo .tar 113
Figura 119 Compilación de los complementos 113
Figura 120 make 114
Figura 121 instalación del make 114
Figura 122 Iniciar los servicios de Nagios 114
Figura 123 Mensaje de ejecución correcta 115

Figura 124 Acceso a la interfaz web de Nagios 116
Figura 125 Interfaz de inicio de Nagios 116

RESUMEN

Hoy en día la información corresponde a uno de los activos más destacables de las organizaciones, por lo cual es de suma consideración asegurar la entereza, disponibilidad y confiabilidad de la información, con el fin de evadir perjuicios o modificaciones ocasionadas por agentes o componentes internos o externos a la organización, por lo previo y con propósito de proteger la información se han desarrollado los CSIRT, que son los responsables de atender accidentes, errores o algún tipo de ataque informático dentro de las compañías.

Esta tesis se enfoca en el diseño técnico de un CSIRT que permita ofrecer un avance a las ocupaciones propias de un equipo de respuesta frente incidentes de seguridad informáticas, exponiendo los distintos puntos que deben tener los servicios ofrecidos por dicho equipo, por ende, se estableció la recopilación relacionada con herramientas de software que permitan el avance de las ocupaciones relacionadas con el CSIRT, junto con el diseño de la estructura tecnológica teniendo en cuenta las diferentes dependencias con las que se debe contar para la elaboración del mismo.

Palabras Clave: Riesgos, ataques informáticos, CSIRT, CERT, Manejo de incidentes, SIEM, Vulnerabilidades

INTRODUCCION

El tráfico de datos a través del ciberespacio crece a volúmenes vertiginosos, pues con el desarrollo de nuevas redes sociales y tecnologías digitales, así como la aparición de la pandemia del covid 19, obliga a la población mundial a optar por alternativas comunicacionales en esta época de distanciamiento social, por lo tanto, la conectividad nos permite acceder a las actividades sistema educativas en línea, mantenernos informados, trabajar y conservar nuestro bienestar mental e incluso físico.

Sin embargo, una de las máximas en seguridad informática es que empresas, instituciones y ciudadanos; ninguno de estos factores está exento de ser violentados por terceros, más tarde o temprano todos pueden ser susceptibles de un ciberataque

En este sentido la legislación colombiana promulgo La Ley 1273 de 2009 donde creó nuevos tipos penales relacionados con delitos informáticos y así promover la protección de la información y de los datos de la población en general.

A pesar de esto, estamos viendo un incremento de ataques dirigidos por grupos cibercriminales, ataques cada vez más sofisticados, en los que la nueva tendencia son los ataques tipo Ransomware (secuestro de datos) y pedir un rescate. El año 2019 se vio un incremento de ataques a los dispositivos móviles, ataques cada vez más sofisticados, por lo que no valen las soluciones tradicionales.

Es por esto que la empresa Cibersecurity pretende desarrollar una documentación técnica que le permita implementar un equipo de respuesta ante emergencias informáticas. Este equipo da respuesta ante incidentes de seguridad de la información correspondería a una unidad compuesta por personas expertas en los diferentes campos de seguridad de la información, cuyo principal objetivo sería prevenir y dar solución a los diferentes incidentes presentados en las compañías en relación a sus sistemas informáticos donde ocurran o pueden ocurrir eventos anómalos que representa una amenaza y afectan la confidencialidad e integridad de la información e impiden su buen funcionamiento.

Con esto se lograría el objetivo principal de la empresa Cibersecurity que es llevar a cabo su propósito de consolidarse como un Centro de Respuesta a Incidentes Cibernéticos en el ámbito de CSIRT, evitando los incidentes de seguridad informática de sus clientes.

1 PLANTEAMIENTO DEL PROBLEMA

En los últimos tiempos, la cantidad de personas, empresas y distintos tipos de organizaciones que ingresan a Internet, ha tenido un elevado incremento, lo que ha generado una interacción constante de la sociedad con el mundo digital, ya sea para revisar información, trabajar, realizar compras, distraerse, entre otras actividades. La mayoría de estas actividades son ejecutadas de manera automática por las personas y generan beneficios, pero en muchos casos existen riesgos asociados a la interacción digital, en cuanto al manejo de información delicada y susceptible de ser robada.

Es por esto que a la par del desarrollo de nuevas aplicaciones en Internet para usuarios, ha venido creciendo una nueva rama que se encarga de la protección y seguridad de la información tanto de personas como de organizaciones de diversas índoles, cuyo objetivo se centra en ser entidades capaces de prevenir amenazas informáticas y en caso de que no se puedan prevenir, generar mecanismos de respuesta para la protección de los datos de los usuarios afectados.

En virtud de este escenario, las organizaciones se han visto en la necesidad de realizar una serie de estudios y análisis más profundos, acerca de los mecanismos de seguridad que requiere la información que los usuarios ingresan en Internet, y así comprender que la implementación de mecanismos de seguridad (firewalls, herramientas antivirus y anti-spam) son solo una pequeña parte de una arquitectura de seguridad, que debe contener políticas, estándares, normas, modelos de gestión de tecnología y operaciones de seguridad, que permitan minimizar el impacto ante un ataque a las actividades de cualquier organización.

De esta realidad mundial no escapa ningún país, y en el caso de Colombia, donde cada día son más los usuarios con capacidad de conectarse a Internet ya sea desde sus casas u oficinas, es de suma importancia crear mecanismos de seguridad de información que es ingresada a los diferentes portales que hacen vida en Internet.

Los equipos de respuesta ante incidentes informáticos, denominados CERT, CSIRT o CIRT, son entidades que tienen como propósito generar políticas, mecanismos y procedimientos para la protección de la información de los usuarios ante las diversas amenazas existentes, pues tienen un enlace único de contacto en las organizaciones para la recepción de notificaciones de seguridad, manejo de incidentes y análisis de vulnerabilidades tanto en los recursos, así como en los servicios que soportan la información. Un gran número de países a nivel mundial han considerado la implementación de equipos de respuesta ante incidentes informáticos, como enlace de contacto a nivel nacional ante eventos de seguridad informática.

Cibersecurity de Colombia es una empresa dedicada a la prestación de servicios de seguridad para la protección de la Información, y en la actualidad, no cuenta con un equipo de respuesta a emergencias informáticas (CSIRT), por lo que una de las prioridades de la empresa es el diseño y la posterior implementación de un CSIRT (Equipo de Respuesta ante Incidencias de Seguridad Informática), para prestar un servicio proactivo y eficiente a sus clientes, de acuerdo a las necesidades de cada uno de ellos.

¿Como diseñar la documentación técnica que permita implementar las herramientas de software, hardware, esquemas tecnológicos y modelo organizativo para un CSIRT, en la empresa Cibersecurity de Colombia LTDA?

2 JUSTIFICACIÓN

La empresa Cibersecurity de Colombia LDTA, tiene el propósito principal de consolidarse a nivel nacional como un Centro de Respuesta a Incidentes Cibernéticos en el ámbito de CSIRT, por lo tanto, es importante el diseño y compilación de toda la documentación técnica necesaria para poder dar inicio al desarrollo de funciones de respuesta a incidentes cibernéticos y así poder ofrecer servicios a personas y organizaciones que aparte de dar solución, proporcionaran soporte audaz y eficaz a las vulnerabilidades que se puedan presentar en las empresas colombianas.

Adicionalmente, la realización de este trabajo de aplicabilidad generará una serie de herramientas que permitirán tener una estructura y un organigrama, que ayudará a la ejecución del diseño y posterior aplicación de un CSIRT, que dé solución a las falencias de la seguridad informática que posee la mencionada empresa en la actualidad, y así mismo disminuya el impacto que tienen los ataques cibernéticos de hoy día.

La guía técnica que se presenta en el siguiente trabajo para la empresa Cibersecurity de Colombia LTDA, es de suma importancia ya que agrupa toda la documentación técnica, organizacional y los procedimientos mínimos necesarios, para la implementación de un CSIRT que se encargue de la prevención, manejo y respuesta eficaz a los ataques de seguridad informática que se puedan llevar a cabo sobre las personas y las diferentes organizaciones suscritas a la empresa, y que adicionalmente, puede ser tomado como referencia para la creación de otros CSIRT a nivel nacional.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar una guía técnica de implementación que permita desarrollar las actividades propias de un Equipo de Respuesta ante Incidentes de seguridad informática (CSIRT) de Cibersecurity de Colombia.

3.2 OBJETIVOS ESPECÍFICOS

- Seleccionar las herramientas de hardware y software adecuadas para la implementación de un CSIRT en Cibersecurity de Colombia.
- Representar la estructura tecnológica para la implementación de un CSIRT teniendo presente las diferentes dependencias de Cibersecurity de Colombia.
- Elaborar los perfiles profesionales necesarios que permitan el desarrollo de las actividades del CSIRT.
- Crear una guía técnica para la instalación de las herramientas de software utilizadas en el CSIRT.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

Para el desarrollo del proyecto es necesario tener conocimientos claros en el contorno de seguridad de la información en todos sus niveles tanto de hardware, software y estándares que regulan la protección y mitigación de ataques e incidentes presentados en las organizaciones en su infraestructura tecnológica, para esto a continuación se puede observar algunos conceptos a tener presentes.

4.1.1 Equipo de respuesta ante incidentes de seguridad de la información (CSIRT)

Según el Ministerio de Defensa en la guía de creación de un CERT/CRIST. Un equipo de respuesta ante incidentes de seguridad de la información corresponde a una unidad compuesta por personas expertas en los diferentes campos de seguridad de la información, cuyo principal objetivo es prevenir y dar solución a los diferentes incidentes presentados en las compañías en relación a sus sistemas informáticos donde ocurran o pueden ocurrir eventos anómalos a su buen funcionamiento , además, ayuda con la administración de la seguridad de la información como servicio a los diferentes clientes o entorno de trabajo. Los CSIRT pueden efectuar tareas conjuntas entre diferentes CSIRTs y empresas dedicadas a prestar diferentes servicios de seguridad informática"[1].

Uribe Edgar nos presenta que "la composición de comunicación entre CSIRTs como se visualiza hoy en día, es una composición por jerarquías en las que hay CSIRTs que dan solución a usuarios o grupos de usuarios y algunos que solamente son utilizados como centro de sincronización de distintos CSIRTs en ubicaciones geográficas diferentes, frecuentemente esta categoría es informal, la composición informal facilita a los CSIRTs comunicar información de manera ligera así como eficiente con otros CSIRTs, llegando a si a tener una sincronización al instante con el fin de brindar el soporte para resolver los diferentes incidentes de seguridad."[2].

---

[1] MUÑOZ, M. Estado actual de equipos de respuesta a incidentes de seguridad informática. [En línea]. Septiembre 2020. Disponible en: http://www.scielo.mec.pt/scielo.php?pid=S1646-98952015000100002&script=sci_arttext

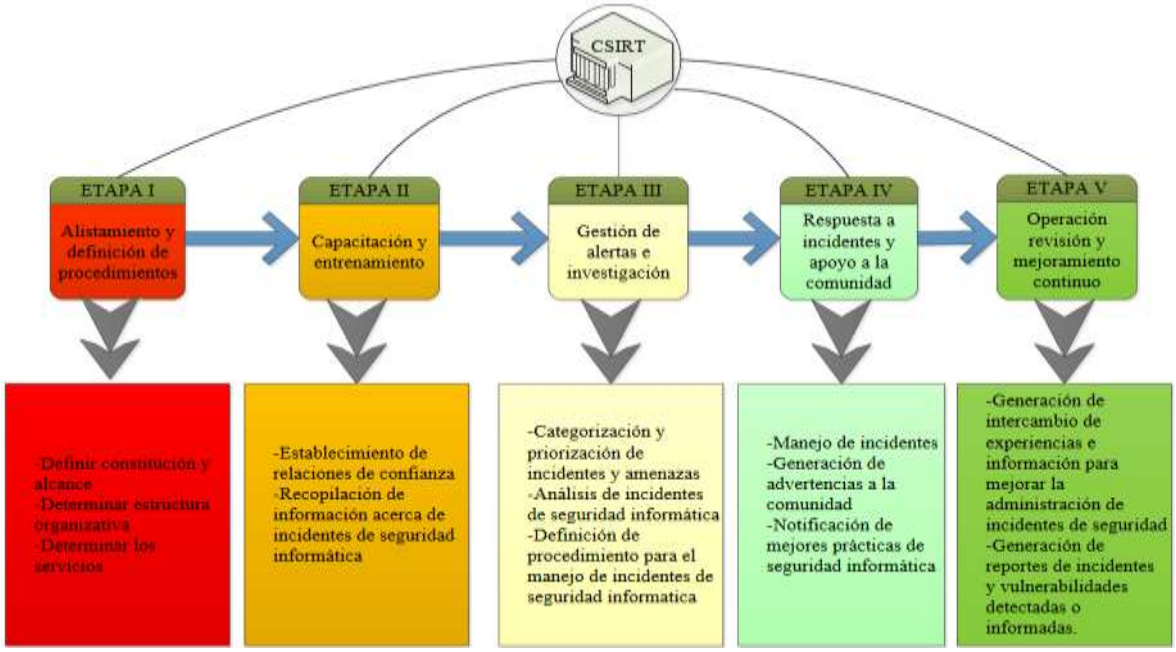
[2] URIBE, Edgar. Proceso para la Definición de Servicios Iniciales en un Equipo de Respuesta ante Incidencias de Seguridad Informática (CSIRT). Zacatecas. 2014. 211 p. Trabajo de grado para Maestro en Ingeniería de Software Centro de Investigación en Matemáticas, A.C.

Los objetivos esenciales de un CSIRT son, por un lado, vigilar los inconvenientes causado por problemas informáticos a cualquier sistema de información de las organizaciones, proporcionando respuesta y sustento para dar solución de estos, y, además, desarrollar ocupaciones que permitan impedir que se repitan accidentes semejantes.

Existen unas etapas de puesta en marcha para los servicios de un CSIRT, las cuales se listan a continuación:

- Etapa 1. Alistamiento y definición de procedimientos.
- Etapa 2. Capacitación y entrenamiento.
- Etapa 3. Gestión de alertas e investigación.
- Etapa 4. Respuesta a incidentes y apoyo a la comunidad.
- Etapa 5. Operación, revisión y mejoramiento continuo.[3]

Figura 1: Etapas para la implementación de un CSIRT



Fuente: DIGETIC, Etapas para la implementación de un CSIRT [imagen]. Dirección General de Tecnologías de la Información y Comunicación FFAA. Parte de la II Revista Digital 2020. p. 21.

[3] ANDRADE, R., & FUERTES, W. Diseño y dimensionamiento de un equipo de respuesta ante incidentes de seguridad informática (CSIRT). Caso de estudio: Escuela Politécnica del Ejército [en línea]. Octubre 2020. Disponible en: http://repositorio.espe.edu.ec/bitstream/21000/6972/1/AC-GRT-ESPE-047091.pdf

Por parte de Ochoa Ovalles se sugieren 5 etapas de nivel alto como lo son: Capacitación, Planificación, Utilización, Operación y Colaboración. Estas etapas brindan guía clara en la caracterización de la actividad implicada en la construcción de un CSIRT desde la idealización de este hasta la construcción y cuidado de la aptitud de administración frente a incidentes.[4]

4.1.1.1 SERVICIOS DE UN CSIRT

En un CSIRT los servicios se ajustan a las pretensiones de los profesionales en seguridad informática (Penedo, 2006). Un equipo de respuestas ante incidentes informáticos puede prestar un amplio portafolio de servicios, pero por la complejidad y la disponibilidad de dichos servicios en la actualidad ningún CSIRT está en la capacidad de prestar todos los servicios posibles. En la siguiente tabla podemos visualizar un resumen de la perspectiva general de los servicios que puede prestar un CSIRT[5].

Tabla 1: Posibles servicios prestados por un CSIRT.

Servicios reactivos	Servicios proactivos	Manejo de solicitudes
Notificación de alertas	Avisos	Análisis de instancias
Resolución de incidentes	Laboratorio de tecnología	Manejo de incidentes sobre solicitud
Estudio de incidentes	Análisis de seguridad informática.	sincronización
Soporte	Administración y sostenimiento de la seguridad informática	Funcionalidad de soporte prestado
Administración	Desarrollo de seguridad	Auditoria de riesgos
Brindar respuestas ante incidentes	IPS	Recuperación de desastres y continuidad del negocio
Soporte en sitio ante incidentes	Divulgación de la seguridad	Consultoría de seguridad
Procesamiento de vulnerabilidades		Sensibilización

[4] OCHOA OVALLES, Sergio. Seguridad informática en Contribuciones a las Ciencias Sociales. [en línea]. Julio 2020. Disponible en: http://www.eumed.net/rev/cccss/21/oocs.html

[5] PENEDO, D. Technical Infrastructure of a CSIRT. [en línea]. Noviembre 2020. Disponible en: https://ieeexplore.ieee.org/abstract/document/1690411

Análisis		Alineación y educación
Respuesta ante un incidente de seguridad		Productos con certificación

Fuente: ENISA. Posibles servicios prestados por un CSIRT**.** CÓMO CREAR UN CSIRT PASÓ A PASO**.** Producto WP2006/5.1 (CERT-D1/D2).

4.1.1.2 TIPOS DE CSIRT

En la actualidad existen diferentes CSIRT según su público objetivo, pertenecientes a distintos sectores de la sociedad y de organizaciones. Para el (De La Torre & Parra, 2018) los diferentes ámbitos en los que se ha implementado equipos CSIRT son[6]:

CSIRT para las Pymes: Por el tamaño que mantienen estas empresas es poco viable que de forma individual estas empresas implementen las funcionen de un CSIRT. Por lo tanto, este tipo de equipos de respuesta buscan agrupar pequeñas organizaciones que mantengan características similares para ofrecerles el servicio.

CSIRT Académico: Estos centros optan por tener su responsabilidad en entidades académicas conformadas por estudiantes y personal de universidades o colegios. La dimensión de la comunidad estipulará los servicios a ofrecer, el modo que lo van a hacer y el grado de intervención directa en el campo.

CSIRT Comercial: Prestan servicios a cambio de una remuneración económica a clientes profesionales del sector comercial, normalmente utilizan acuerdos de servicios específicos con cada cliente de su comunidad.

CSIRT Militar: Proporcionan servicios a instituciones militares con compromisos de infraestructuras de TI para generar un alto grado de defensa contra ataques cibernéticos. Su comunidad está determinada por organizaciones militares y entidades estrechamente relacionadas.

CSIRT Gubernamental: En este tipo de equipos se encuentran aquellos CSIRT cuyo objetivo es proteger la infraestructura de TI de un gobierno u estado y los servicios que son ofrecidos a su población. Generalmente la comunidad a la que se encuentran dirigidos son las administraciones públicas y sus organismos. Estos equipos pueden combinarse con CSIRT Nacionales o funcionar de manera independiente. Estos CSIRT habitualmente están patrocinados por instituciones del estado.

[6] DE LA TORRE, H., & PARRA, M. Estrategia y diseño de un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) académico. Universidad de las Fuerzas Armadas ESPE. 2018. Pág. 46.

CSIRT Nacional: Estos tipos de CSIRT son fundamentales como punto de contacto para todo un país, puesto que tienen coordinación y responsabilidad sobre todos los sectores de este. En muchos casos estos equipos atienden a la comunidad CSIRT de su país y asumen la responsabilidad de coordinación de otros CSIRT en el perímetro local.

CSIRT de Defensa de Infraestructuras Críticas: Pueden ser considerados CSIRT del sector interno, puesto que se centran en el resguardo de las infraestructuras críticas de la información, por ejemplo, Sistemas financieros, Organizaciones de telecomunicaciones, Centrales de energía, Sector sanitario, Instalaciones de investigación, alimentación, agua, transporte, entre otras).

CSIRT de Proveedor: Su objetivo central son los productos o servicios que ofrece un proveedor, eliminando o reduciendo el impacto negativo de las vulnerabilidades de los mencionados, ya sea un producto tecnológico o servicio de TI.

Figura 2: Tipos de CSIRT a nivel mundial

Fuente: Morales, Ronald. Tipos de CSIRT a nivel mundial. TB-Security. Retico.gt/retisecure

4.1.2 Seguridad informática

Para Eunet, se puede determinar cómo un grupo de métodos, gadgets o utilidades encargadas de garantizar la privacidad, integridad y disponibilidad de la información en los diferentes sistemas tecnológicos e intentar disminuir las posibles amenazas que pueden llegar a afectar o corromper los sistemas de una organización[7].

En su tesis de Uribe Edgar[8] titulada Proceso para la Definición de Servicios Iniciales en un Equipo de Respuesta ante Incidencias de Seguridad Informática (CSIRT)en esta se genera la descripción de los tres pilares de la seguridad informática como lo son:

---

[7] OCHOA OVALLES, Sergio. Seguridad informática en Contribuciones a las Ciencias Sociales. [en línea]. Julio 2020. Disponible en: http://www.eumed.net/rev/cccss/21/oocs.html

[8] URIBE, Edgar. Proceso para la Definición de Servicios Iniciales en un Equipo de Respuesta ante Incidencias de Seguridad Informática (CSIRT). Zacatecas. 2014. 211 p. Trabajo de grado para Maestro en Ingeniería de Software Centro de Investigación en Matemáticas, A.C.

Integridad: mantiene la estabilidad, claridad y fiabilidad de los datos a través de todo su ciclo.
Confidencialidad: permite que la información sea evidenciada solo a personas autorizadas.
Disponibilidad: que se puede tener acceso a la información.

4.1.3 Amenaza de seguridad informática

En el descubrimiento de los ordenadores, la evolución de los medios donde se almacena la información ha cambiado, pasando por formatos como la talla en piedra y el papel llegando a un formato electrónico con un sinfín de dispositivos. Inicialmente la preocupación solo era resguardar la información ya que en ese tiempo las ejecuciones de software eran secuenciales y no existía una red para compartir dicha información almacenada, con la llegada de los computadores y la red de redes (internet), se aumentó de forma exponencial el número de personas y de elementos transmitidos y almacenados no solo por empresas sino también por usuarios final, esto conlleva a que la información o los datos cada vez estén expuestos a más amenazas con un grado de sofisticación día a día más avanzado.

4.1.4 CSIRTs en Colombia

Colombia ha estado a la vanguardia en el campo de la seguridad de la información, en los últimos años se ha planeado, implementado, evaluado y exigido el cumplimiento de políticas y/o procedimientos para la prevención de ataques cibernéticos en el país, para que, de esta forma, se proteja a los colombianos y su economía de potenciales amenazas. El gobierno nacional ha adoptado buenas prácticas mediante la expedición del "documento CONPES 3854"[9], del 11 de abril de 2016, el cual comprende de manera detallada la política pública de ciberseguridad, este documento representa un punto de partida para la elaboración de estrategias de prevención y lucha contra los riesgos cibernéticos.

CONPES (El Consejo Nacional de Política Económica y Social), es la máxima autoridad a nivel nacional para la planeación y asesoría del gobierno en los aspectos relacionados con el desarrollo económico y social del país. El CONPES realiza el estudio y da la posterior aprobación de documentos sobre el desarrollo de políticas generales que son presentados en sus sesiones, particularmente en el caso de ciberseguridad, el CONPES presentó un documento de Seguridad Digital que

[9] CONPES 3854, C. N. Departamento Nacional de Planeación. {En línea}. {diciembre de 2020}. Disponible en: https://observatorioplanificacion.cepal.org/es/instituciones/consejo-nacional-de-politica-economica-y-social-conpes-de-colombia

integra seis capítulos; introducción, antecedentes y justificación, marco conceptual, diagnóstico, definición de la política y recomendaciones.

Partiendo de los lineamientos emanados por el CONPES y en virtud de las necesidades y los problemas relacionados con la ciberseguridad en Colombia, el país ha impulsado la gestión de la seguridad en ambientes digitales, con la creación de CSIRTs a nivel nacional.

A continuación, se mencionan algunos de los CSIRTs más importantes en el país:

- GRUPO DE RESPUESTA A EMERGENCIAS CIBERNETICAS DE COLOMBIA– colCERT: Es el organismo coordinador a nivel nacional en aspectos que se refieren a la ciberseguridad y la ciberdefensa de la nación, tiene como misión la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional.
- CSIRT- CCIT Es un centro de coordinación de atención a incidentes de seguridad informática que ocurren en Colombia, el cual está en contacto directo con los centros de seguridad de las empresas afiliadas y tiene la capacidad de coordinar el tratamiento y solución de solicitudes y denuncias sobre problemas de seguridad informática que sean recibidas en la cuenta de correo electrónico. Este Centro también actúa como contacto nacional e internacional para la gestión y atención a incidentes de seguridad informática que involucren redes y/o servicios Colombianos.
- CSIRT-PONAL: Es un equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional, es un grupo creado para atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática, con el fin de proteger la infraestructura tecnológica, los activos de información y mitigar el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones.
- CSIRT FINANCIERO ASOBANCARIA: Es un equipo de apoyo para la respuesta a incidentes cibernéticos, comunidad de intercambio, centro de excelencia en investigación y colaboración para anticipar y mitigar riesgos derivados de amenazas cibernéticas.

4.1.5 Ciberataques en Colombia

Según lo señalado por Pérez, Yuly en el artículo La Importancia de la Ciberseguridad en Colombia[10], en muchos medios de comunicación, tales como periódicos nacionales, entre ellos: Semana, El Tiempo, El Heraldo, se ha dado a conocer información sobre los ciberataques ocurridos a diario de forma pasiva y activa en Colombia, ya sea en las entidades financieras, instituciones del gobierno, organizaciones privadas, universidades y ciudadanos. Los ciberataques han generado impactos de millones de pesos porque en su mayoría no cuentan con planes de prevención y respuesta ante este tipo de incidentes.

Es importante mencionar los casos más relevantes ocurridos a nivel nacional, estos son:

- En el año 2011, el conocido grupo Anonymous atacó los sitios web del Ministerio de educación, Senado, Ministerio de Defensa, Presidencia de la República y el sitio de Juan Manuel Santos. En el año 2012, nuevamente este grupo se atribuye el ataque al sitio web de la policía.
- En el año 2016, días antes del plebiscito, página de la Registraduría Nacional del Estado Civil sufre ataque.
- El periódico El Tiempo, el 13 Julio de 2016, publico que en América Latina, Colombia es después de Brasil y México el tercer país con más ataques cibernéticos. La página web del Centro Cibernético de la Policía Nacional de Colombia - CCPN, ofrece una plataforma llena de servicios, informes, boletines, reportes de incidentes y guías sobre la temática tratada, además que allí se encontrara con los casos más relevantes registrados por este centro.

4.2 MARCO CONCEPTUAL

4.2.1 IPS

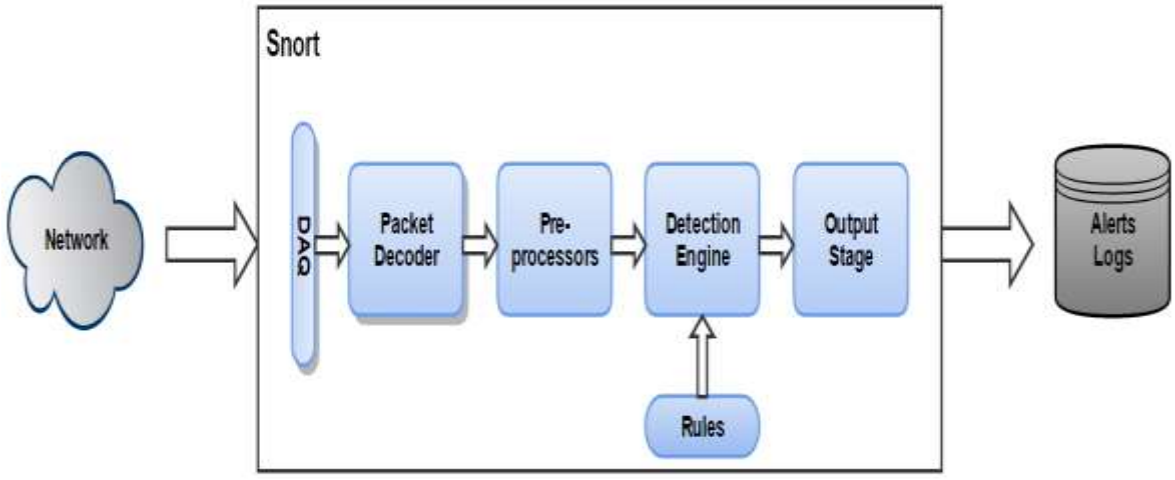
El IPS (sistema de prevención de intrusión) es un programa o appliance que asegura el correcto funcionamiento y evitan amenazas conocidas y de día 0 en la red de una organización, bloqueando amenazas (ITECO CERT, 2009)[11]. Este tipo de programas se encargan de analizar los paquetes en la red con el objetivo de buscar y bloquear intentos de intrusión en los diferentes dispositivos que conforman una

[10] PEREZ PEREZ, Yuly. La importancia de la Ciberseguridad en Colombia. [En Línea]. 18 de diciembre de 2020. Disponible en: http://polux.unipiloto.edu.co:8080/00003620.pdf

[11] ITECO CERT. (2009). Instituto Nacional de Tecnologías de la Comunicación. [En línea] Septiembre 2020. Disponible en: www.inteco.es/extfrontinteco/icd/pdf/Cortafuegos_VPN_IDS_IPS.pdf

red. Este tipo de herramientas de seguridad tienes acciones establecidas que pueden ser configuradas manualmente o generar acciones automáticas descartando paquetes que presenten algún tipo de anomalías o amenaza para la red. Los IPS se clasifican como programas proactivos, ya que toman decisiones de forma automática si se observa un incidente de seguridad dentro de la red.

Figura 3: Packet processing Flow



Fuente: Asher Gruber. Packet processing Flow. The Interdisciplinary Center, Herzliya E_ Arazi School of Computer Science. Disponible en: deepness-lab.org/pubs/project_snort_dpisrv.pdf

4.2.2 UTM

Los UTM son soluciones unificadas contra amenazas para organizaciones que quieren asegurar numerosos sistemas apoyándose en un solo dispositivo (ITECO CERT, 2009)[12]. Disponen de funcionalidades de administración de red, así como bloqueo de tráfico, también pueden ser utilizados como utilidad de análisis de accionar de sistema y la red. Muchos de los dispositivos que se encuentran en el mercado proporcionan utilidades de análisis forense, defensa contra virus, gusanos, controles de aplicación o web, IPS, entre otros.

[11] ITECO CERT. (2009). Instituto Nacional de Tecnologías de la Comunicación. [en línea]. Septiembre 2020. Disponible en: www.inteco.es/extfrontinteco/icd/pdf/Cortafuegos_VPN_IDS_IPS.pdf

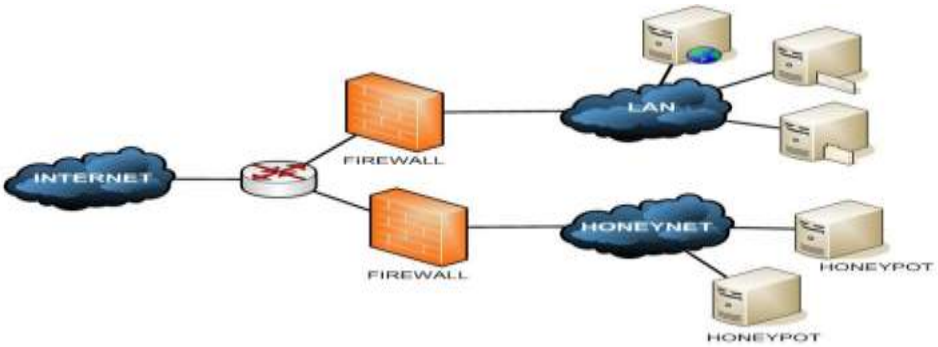
Figura 4: Amenazas controladas con UTM

Fuente: Amenazas controladas con UTM (Infosecurity Bureau, 2007)

4.2.3 Honeypot

Es un recurso de computacional, el cual tiene como funcionalidad ser analizado, vulnerado, puesto en compromiso, utilizado o accedido de manera no autorizada por usuarios internos o externos, con el fin de conseguir información acerca del atacante, métodos utilizado en el ataque, determinar nuevo software malicioso en las compañías o estudiar el accionar de Ciberdelincuentes, entre otros. Estos elementos por recomendación tienen que estar aislados del ámbito de producción o de cualquier sistema que le represente un potencial peligro. Según un trabajo de investigación hecho por la Agencia Europea de Seguridad de las Redes y de la Información (ENISA)[13].

Figura 5: Redes de honeypots



Fuente: Fernando Cócaro. Redes de honeypots. InCo – Facultad de Ingeniería - Universidad de la República. Disponible en: https://docplayer.es/3907747-Diseno-e-implantacion-de-un-honeypot.html

[12] ENISA (2016). CSIRT Setting up Guide in Spanish. [En línea] Agosto 2020. Disponible en: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullRepor

4.2.4 Hardening

El proceso de fortalecimiento (Hardening) tiene relación al desarrollo de métodos que permitan garantizar la seguridad de un sistema por medio de la disminución de inseguridades, esto se consigue bloqueando programa, procesos, controlando usuario y revisando los puertos del sistema con el fin de realizar filtros sobre los puertos que sea requerido, también varios otros procedimientos y métodos que pueden llegar a ser implementadas en los sistemas de una organización[14].

Es sustancial nombrar que los parámetros de seguridad implementados no puedes proteger ante incidentes donde el tráfico no esté redirigido y pasando por dichos sistemas, de copias o extracción ilegal de información en medios de alojamiento físico como memorias USB o unidades ópticas, errores de capa 8, de malwares en ficheros o programa y de posibles errores de configuración en los sistemas de seguridad y protocolos de seguridad[15].

4.2.5 Vulnerabilidad

Los bugs o segmentos de código mal escrito presentes en los diferentes sistemas informáticos representan la primera causa de amenazas e incidentes de seguridad informática tanto para un usuario final como para una compañía. Estas vulnerabilidades abarcan un creciente número de inseguridades que conllevan a enormes agujeros de seguridad en los sistemas tecnológicos por ejemplo las redes, SO, bases de datos, entre otros. Los inconvenientes emergen cuando las inseguridades expuestas no son parchadas o depuradas a tiempo, los piratas informáticos conocen que así los proveedores de software liberen actualizaciones de seguridad, esto no significa que los administradores del sistema o el usuario lo implementen en su sistema.

4.2.6 Incidente de seguridad informática

Los incidentes de seguridad informática son aquellos que representa una amenaza o afectan los tres pilares fundamentales de la seguridad de la información como lo son la confidencialidad, disponibilidad e integridad de la información. Impidiendo el buen funcionamiento o la operación correcta de las redes o cualquier sistema

---

[13] DUAN, Qi; AL-SHAER, Ehab; JAFARIAN, Haadi. Efficient random route mutation considering flow and network constraints. En 2013 IEEE Conference on Communications and Network Security (CNS). IEEE, 2013. p. 260-268.

[14] ITECO CERT. (2009). Instituto Nacional de Tecnologías de la Comunicación. [En línea] septiembre 2020. Disponible en: www.inteco.es/extfrontinteco/icd/pdf/Cortafuegos_VPN_IDS_IPS.pdf

informático; entre los que podemos encontrar accesos no autorizados, robo de contraseñas, robo de información confidencial, ingeniería social, entre otras.

Figura 6: Proceso de la gestión de incidentes

Fuente: Loayza Alberto. Proceso de la gestión de incidentes. Modelo de gestión de incidentes para una entidad estatal. 2016. Disponible en: https://dialnet.unirioja.es/descarga/articulo/6043083.pdf

4.2.7 Servicio

Los servicios son procesos o actividades que pueden llegar a realizar una organización con el fin cumplir con determinado proceso o generar la elaboración de un bien en específico. Los servicios tienen la posibilidad de ser dirigidos externamente, al cliente o tienen la posibilidad de ser dirigidos desde adentro de la compañía hacia trabajadores, clientes o un actor que interactúe con la labor de la organización.

4.2.8 Proceso

CERT-RMM precisa los procesos a modo de: “Un grupo de ocupaciones interrelacionadas que convierten entradas en salidas, con un objetivo o propositivo definido”[16] Los procesos en los CSIRT organizan y generan la constitución y base de la prestación de servicios, permitiendo organizar y estandarizar cada uno de los elementos del CSIRT.

4.3 MARCO LEGAL

4.3.1 Ley 1273 de 2009 (enero 05)

Con el auge que ha tenido las nuevas tecnologías, internet y el rápido crecimiento de los sistemas informáticos, ha llevado a la masificación del uso de dispositivos tecnológicos en las compañías y por consiguiente el aumento de los delitos informáticos, llevando a que el Congreso de Colombia sancionará la Ley 1273 el 5 de enero de 2009, mediante el cual se modifica el Código Penal, se crea un nuevo activo legal protegido custodia de información y datos personales y los sistemas que utilizan tecnologías de información y comunicaciones se conservan por completo, incluidas las disposiciones[17] con el fin de establecer normatividad para combatir el cibercrimen. Con la creación de esta Ley se da un valor jurídico a la información, estableciendo las conductas criminales que tienen que ver con sistemas de cómputo y las nuevas tecnologías. En esta ley se encuentran establecidos artículos para los diferentes ciberdelitos, los cuales son aplicables al presente trabajo:

- Artículo 269A: Acceso abusivo a un sistema informático: ocurre cuando el ciberdelincuente vulnera y genera acceso a un sistema por medio de una falla de este y genera extracción de información personal o lucros económicos en sus actos.
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación: ocurre cuando el ciberdelincuente bloquea de forma ilegal el uso de un sistema hasta cuando obtiene un beneficio económico.
- Artículo 269C: Interceptación de datos informáticos: cuando valiéndose de los recursos tecnológicos, sin autorización legal obstruye datos.

---

[15] URIBE, Edgar. Proceso para la Definición de Servicios Iniciales en un Equipo de Respuesta ante Incidencias de Seguridad Informática (CSIRT). Zacatecas. 2014. 211 p. Trabajo de grado para Maestro en Ingeniería de Software Centro de Investigación en Matemáticas, A.C.

[17] SENADO DE LA REPUBLICA. Ley 1273 de 2009. [en línea]. Noviembre 2020. Disponible en: https://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.h

- Artículo 269D: Inconveniente Informático. cuando un individuo que, sin estar autorizada, modifica, altera, daña, borra y elimina datos del programa o de documentos electrónicos.
- Artículo 269E: Uso de programa malicioso: cuando se generan, consiguen, venden, distribuyen, envían, introducen o extraen del país programa que produce perjuicios en los elementos informáticos.
- Artículo 269F: Violación de datos personales: cuando un sujeto sin estar facultado sustrae, vende, envía, adquisición, divulga o emplea datos personales almacenados con el fin de lograr utilidad personal o para otros[18].

4.3.2 Proyecto de ley 241 de 2011 del senado

Por la cual se rige el compromiso por los delitos de derecho de creador y los derechos en relación con internet.

El Congreso Decreta:

CAPÍTULO I

Juicios de Compromiso Artículo 1°. Prestamistas de productos de internet. A lo que genera esta ley se entiende por la gente que presten uno o numerosos de los próximos servicios:

a) Comunicar, guiar o proveer enlaces para materiales sin llevar a cabo ediciones en su contenido.

b) Guardar datos por un tiempo por medio de un desarrollo automático.

c) Guardar a petición de un usuario la información que se alberga en un sistema o red operado por el prestador de servicios.

d) Vincular a los individuos a un sitio online por medio de la utilización de utilidades de búsqueda de información, introduciendo hipervínculos y directorios"[19].

---

[18] SENADO DE LA REPUBLICA. Ley 1273 de 2009. [En línea]. Noviembre 2020 Disponible en: https://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.h

[19] SENADO DE LA REPUBLICA. Ley 241 de 2011. [en línea]. Noviembre 2020. Disponible en: http://www.senado.gov.co/index.php/documentos/az-legislativo-categoria/conciliaciones/217-texto-conciliado-plan-nacional-de-desarrollo/file

4.3.3 Ley estatutaria 1581 de 2012.

Empezó a regir la Ley 1581, Esta brinda los lineamientos para la protección de los datos personales donde está regida por lo establecido por el Congreso de la república y la Sentencia de la Corte Constitucional C-748 de 2011.

Debido a la ordenanza, tiene seis meses toda entidad pública o privada para hacer sus reglas internas para administrar los datos íntimos, detallar métodos correctos para la vigilancia de necesidades, quejas y reclamos, de esta forma cambiar los métodos, tratados y permisiones contenidos dentro de la norma.

Puntos importantes:

1. Toda persona tiene la oportunidad de acceder o consultar datos sobre su información personal y solicitar la eliminación o rectificación ante cualquier entidad que almacene su información.

2. Dice que los elementos primarios tienen que ser de suma obligatoriedad por los entes que hagan uso de la información, del régimen o contengan un banco de información personal, cualquier persona que sea su fin.

3. Distingue varios tipos de información personal creando lineamientos con el fin de generar la instauración de los distintos niveles de custodia que tienen que enseñar si son públicos o privados, de esta forma como las finalidades permitidas para su utilización"[20].

4. Crea una custodia a los datos de las personas de edades inferiores.

5. Dispone los lineamientos para la cesión de datos entre entidades y los procesos de importación y exportación de información personal que se hagan en adelante.

6. Da las responsabilidades de las compañías de servicios tercerizados, así como Call y Contact Center, entidades de cobranza y, generalmente, todos esos que manejen datos personales por cuenta de un tercero, tienen que cumplir en adelante.

7. Fija la supervisión y control de las bases de datos personales a la ya construida Superintendencia para la Custodia de Datos Personales, de la Superintendencia de Industria y Comercio.

8. Crea el Registro Nacional de Bases de Datos.

9. Establece una serie de sanciones de carácter personal e institucional dirigidas a entidades y funcionarios responsables del cumplimiento de sus lineamientos"[21].

---

[20] MinTIC. (2012). Ley 1581. [En línea]. Octubre 2020. Disponible en: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

[21] MinTIC. (2012). Ley 1581. [En línea]. Octubre 2020. Disponible en: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

4.4 MARCO ESPACIAL

El diseño e implementación de este proyecto, se va a ejecutar para la empresa Cibersecurity de Colombia LTDA, la cual tiene su planta física ubicada en la ciudad de Bogotá, Colombia.

4.5 MARCO METODOLÓGICO

Basado en el libro “El proyecto de Investigación” de la autora, Jacqueline Hurtado de Barrera, [22]El tipo de estudio es investigativo, descriptivo y proyectivo ya que se estudia y analiza las diferentes variables y situaciones, para ello tendremos en cuenta los siguientes pasos:

Paso 1: Recopilación de información de los procesos y servicios que un CSIRT sugiere para su correcta implementación.

Paso 2: Sustracción de datos global de los CSIRT con el fin de recopilar herramientas de software utilizadas en la prestación de servicios.

Paso 3: Sustracción de información global requerida para la implementación de los servicios que se van prestan en un CSIRT.

Paso 4: Elaboración de lista categorizada de tratamiento de incidentes en los servicios prestados por el CSIRT.

Paso 5: Creación de métodos o procesos que nos ayuden a identificar y definir los servicios de un CSIRT.

Paso 6: Selección de los perfiles profesionales del personal necesario para la prestación de los servicios del CSIRT.

Paso 7: Elaboración de una guía técnica que permita la instalación de las herramientas de software utilizadas en el CSIRT.

[22] HURTADO DE BARRERA, Jacqueline. El Proyecto de Investigación. Comprensión holística de la metodología y la investigación. Ediciones Quirón. 8va edición. 2015

5 RESULTADOS

La fase inicial de este proyecto consiste en el diseño de la documentación técnica para el nuevo CSIRT que se pretende implementar en la empresa Cybersecurity de Colombia LTDA, se propone organizar un CSIRT interno, que preste servicios a la mencionada empresa, es importante que el departamento de TI (tecnología de información) local y su personal, apoye y coordine el tratamiento de los incidentes relacionados con la seguridad de las TI.

Para definir las herramientas de hardware y software necesarias en el diseño e implementación del CSIRT, se hizo un análisis e investigación de la documentación obtenida de diversas fuentes de información, y se procedió a realizar la selección de las herramientas, es importante mencionar que se usó lo propuesto en la guía de ENISA (European Union Agency for Cybersecurity) “cómo crear un CSIRT paso a paso” y el “Handbook for Computer Security Incident Response Teams (CSIRTs)”. Las herramientas seleccionadas se mencionan a continuación.

5.1 HERRAMIENTAS DE SOFTWARE PROPUESTAS PARA ELCSIRT

Las siguientes herramientas de software son recomendaciones realizadas a partir del análisis de la documentación obtenida, así como de los requerimientos de la empresa. Como se mencionó anteriormente se tomó como base principalmente, lo consultado en la guía de ENISA (European Union Agency for Cybersecurity) y del Handbook for Computer Security Incident Response Teams (CSIRTs), también es importante destacar, que las herramientas seleccionadas pertenecen al grupo de herramientas Open Source.

5.1.1 Sitio web

Según Penedo en el trabajo “Technical Infrastructure of a CSIRT “ [23] relata que, para los clientes o potenciales clientes, el primer contacto que se tiene en la prestación de servicios para un CSIRT se lleva a cabo por medio de la página web de este. En ella deberíamos encontrar información como objetivos, servicios, perspectiva, personal de contacto e información sobre noticias de seguridad informática, también secciones de cursos para la concientización y educación del usuario final con respecto a la seguridad informática. De hecho, posibilita el proceso de creación de

[23] PENEDO, D. Technical Infrastructure of a CSIRT. [en línea]. Noviembre de 2020. Disponible en: https://ieeexplore.ieee.org/abstract/document/1690411

casos de incidentes de seguridad informática en la misma por medio de formularios web o redireccionando a un service desk, en los cuales se puede llevar la trazabilidad del evento ocurrido de esta forma facilita la categorización y asignación del incidente a personal encargado de dar respuesta en el CSIRT.

Para Cibersecurity de Colombia será el principal medio de contacto con los clientes ya que a través del sitio web se proporcionará la información de servicios prestados, contactos de soporte y comercial, intranet e información relacionada a temas de seguridad relevante para los clientes.

5.1.1.1 Herramienta de software Joomla

Hasta el momento no se ha definido algún estándar sobre en qué lenguaje de programación se recomienda codificar la página web de un CSIRT, por ende, se general algunas recomendaciones de gestores que facilitan el desarrollo y correcto funcionamiento de la página WEB, entre los que se encuentra JOOMLA.

Se escogió Joomla Como administrador de contenidos dada la facilidad de manejo y por su alto nivel de aceptabilidad, las ventajas de utilizar el Gestor de Contenidos CMS Joomla (Content Management System) para crear un sitio web profesional y llamativo. CMS Joomla permite crear desde la página Web más sencilla hasta crear la página WEB más compleja, Utilizando plantillas programadas y ampliándolas con muchas funcionalidades. Se trata de un sistema auto gestionable y totalmente actualizable en tiempo real con lo cual permite realizar los cambios necesarios a una página Web al instante y alimentarla de contenido.

5.1.2 Correo electrónico

Se recomienda usar el estilo corporativo en el diseño del correo electrónico estándar y del boletín de aviso estándar. Es muy importante que el correo electrónico soporte PGP / GPG / S/MIME. El correo debe ffuncionar para recibir notificaciones con respecto a incidentes de seguridad presentados del grupo de clientes atendidos, también para sincronizarse con otros grupos o realizar aportes y prestar apoyo a los diferentes incidentes de seguridad que se presenten[24]. Es recomendable que el correo electrónico lleve una firma digital con PGP y que los mensajes sobre incidentes siempre se deben enviar encriptados.

[24] SEYMOUR, Michael. Global Initiatives to Secure Cyberspace - An Emerging Landscape. Disponible en: http://dx.doi.org/10.1007/ 978-0-387-09764-0.

5.1.2.1 Herramienta de software Zimbra

Para el correo electrónico tampoco se ha definido un servidor especifico estandarizado para dar cumplimiento a las necesidades de un CSIRT, por lo anterior se generan sugerencias de implementación de un servidor de correo electrónico base open source como lo es Zimbra, ya que este cumple con los requerimientos técnicos y funcionales que debe tener el correo electrónico según la guía de Enisa[25].

Zimbra incluye un servicio completo de correo electrónico, contactos, calendario, uso compartido de archivos, tareas y chat al se puede acceder desde el cliente web de Zimbra a través de cualquier dispositivo o cualquier otro servicio de correo electrónico. Puedes implementar Zimbra como una instalación local tradicional o a través de un proveedor de alojamiento Zimbra, ofreciendo diferentes clases de servicios necesarios para la comunicación de los empleados y clientes dentro del CSIRT.

5.1.2.2 Herramienta de software Asterisk

Se selecciona un servidor Asterisk puesto que tiene funcionalidades similares a centrales de uso propietario como lo son Cisco, Avaya, Alcatel, Siemens, entre otras. Desde las más sencillas funcionalidades que poseen desvíos, capturas, transacciones, multi-conferencias, etc, hasta las más importantes en las que se encuentran Buzones de voz, IVR, CTI y ACD, por lo previo tenemos la posibilidad de decir que una de las primordiales virtudes en la utilización de Asterisk es el ahorro de gastos en relación con contratar los sistemas habituales de telefonía., puesto que obtendremos unas prestaciones máximas con una inversión mínima.

Asterisk se ajusta a las pretensiones de cualquier clase CSIRT, desde CSIRT chicos que necesiten una centralita virtual simple, hasta CSIRT nacionales con un centro de atención telefónica con centenares de operadores recibiendo cientos de llamada cotidianas.

5.1.3 Manejo de incidentes

El equipo debe guardar el historial de cada evidencia, así como todas las comunicaciones, archivos de log, evidencias, acciones tomadas, etc. Es por ello por lo que es indispensable contar con una herramienta que se encargue de llevar el

[25] ENISA. (2006). Cómo crear un CSIRT paso a paso. (CERT-D1/D2). [en línea]. Septiembre de 2020. Disponible en: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

seguimiento del incidente y que contenga una base de conocimientos para saber cómo actuar ante un incidente dado[26].

5.1.3.1 Herramienta de software RTIR (request tracker for incident response)

RTIR Request Tracker for Incident Response corresponde a un sistema gratuito y de open source para la administración de incidentes de seguridad informática. El diseño de esta herramienta corresponde a las diferentes necesidades planteadas por CERT entre otros equipos de respuesta ante incidentes a nivel mundial.

La selección de esta herramienta se basa en su desarrollo, amplia utilización de los equipos CERT/CSIRT y la financiación conjunta de nueve Equipos de Respuesta a Incidentes de Seguridad (CSIRT) europeos, tanto de ámbito académico, como gubernamental.[27]

5.1.4 Acceso remoto

El acceso remoto a los servicios del CSIRT para labores de administración y/o soporte a clientes o teletrabajo es una recomendación que realiza el CCN[28]. Es posible hacer uso de tecnologías como telnet, steltet y el ssh para la administración remota

5.1.4.1 Herramienta de software open ssh

Como se dijo previamente, SSH se utiliza para entrar a máquinas remotas por medio de una red. Facilita conducir completamente la PC por medio de un intérprete de comandos y además puede redirigir el tráfico de una computadora, un programa para conseguir plataforma de trabajo gráfica en sistemas UNIX, para lograr realizar programas gráficos si poseemos utilizable un Servidor.

OpenSSH es la primordial utilidad de conectividad para el inicio de sesiones remotas por medio del protocolo SSH. Cifra todo el tráfico para remover las escuchas, el

---

[26] SEYMOUR Michael (2009). Global Initiatives to Secure Cyberspace - An Emerging Landscape. Disponible en: http://dx.doi.org/10.1007/ 978-0-387-09764-0. Volumen 42.

[27] CCN-CERT LUCIA. Centro Criptológico Nacional España. Versión 2.02. [En línea]. Ubicación: https://www.ccn-cert.cni.es/documentos-publicos/877-lucia-presentacion/file.html. Octubre 2020.

[28] WARNING, ADVICE AND REPORTING POINTS. (2014). [En línea]. Octubre de 2020. Disponible en: http://www.warp.gov.uk.

secuestro de conexiones y otros tipos de ataques. Además, OpenSSH brinda un extenso grupo de habilidades de túnel seguro, numerosos procedimientos de autenticación y configuraciones de configuración sofisticadas para un CSIRT.

5.1.5 Sistema SIEM (security incident and event management systems)

Una de las tareas de un CSIRT es monitorear los eventos de seguridad relacionados con los activos de TI de su organización y de sus clientes, esta tarea es responsable de una herramienta SIEM, la cual recolecta, normaliza y analiza los eventos de seguridad de diferentes fuentes[29].

5.1.5.1 Herramienta de software OSSIM

La versión de código abierto de la oferta de Gestión de Seguridad Unificada (USM) de AlienVault, OSSIM es probablemente una de las plataformas SIEM de código abierto más populares. OSSIM incluye componentes clave de SIEM, a saber, recopilación de eventos, procesamiento y normalización, y lo más importante: correlación de eventos.

Ossim puede proporcionar a un CSIRT procesos de abstracción en el que millones de eventos incompresibles se convierten en alarmas comprensibles de manera gráfica, este desarrollo se transporta a cabo primordialmente en el motor de correlación que brinda OSSIN , donde el gestor crea ordenes de correlación para juntar diferentes eventos de bajo nivel en una exclusiva alarma de prominente nivel, cuyo propósito es incrementar la sensibilidad y la fiabilidad de la red, brindándonos una perspectiva general y detalla de los eventos que este provocando las distintas utilidades de un CSIRT.

5.1.6 Software de Copias de seguridad

El respaldo de los datos es esencial en la infraestructura de un CSIRT, realizar copias de seguridad con frecuencia de los archivos confidenciales e importantes depende la continuidad del CSIRT. Cuando un desastre ocurre y los datos se ven comprometidos supone una pérdida de horas de trabajo y de proyectos que tendría graves consecuencias para la continuidad del negocio y el cumplimiento de los SLAS, Hay que tener en cuenta que los soportes donde recogemos dicha información suelen tener una vida útil limitada (averías, desgastes…) y están sujetos a diversos riesgos y/o amenazas (accidentes, ataques...). Por estos motivos

[29] SOFTWARE ENGINEERING INSTITUTE. CREATE A CSIRT TECHNICAL REPORT. [en línea]. Octubre 2020. Disponible en: http://www.cert.org/incident-management/products-services/creating-a-csirt.cfm.

tenemos que implementar las medidas para proteger el mayor activo que almacenamos en dichos soportes, la información.

Según el Proyecto AMPARO en el trabajo “Manual básico de: Gestión de incidentes de seguridad informática”. Este servidor tiene la tarea de realizar copia de seguridad de la información de todos los sistemas del CSIRT y estaciones de trabajo. Se generan copias de seguridad en bóveda fuera del sitio desde este equipo.

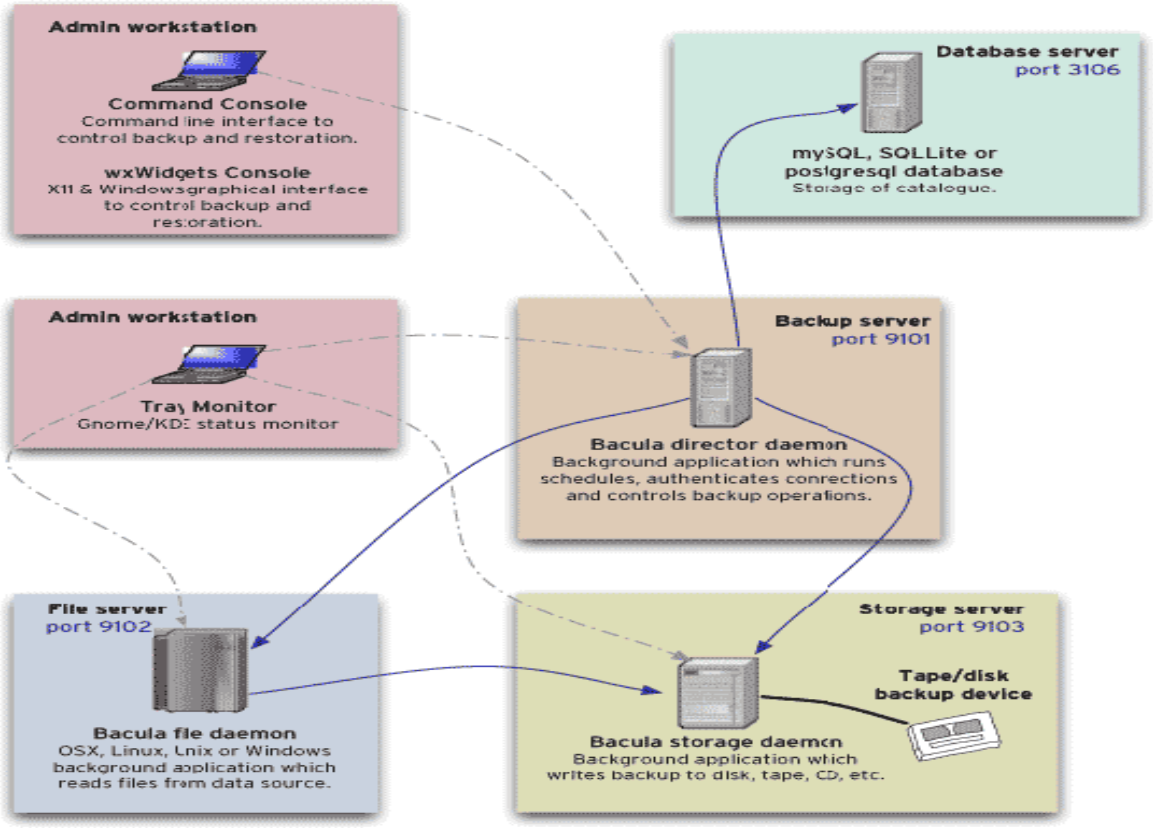
5.1.6.1 Herramienta de software Bacula

En la actualidad no se ha definido o estandarizado un software para realizar copias de seguridad en los CSIRT, por ende, la selección de la herramienta Bacula se genera con base al estudio realizado por Alberto Pozuelo en su trabajo “Implantación de sistemas de BackUp Empresarial”[30]. Allí podemos observar las comparativas realizadas entre los diferentes softwares de copias de seguridad tanto de código abierto como privativas, con sus principales características, ventajas y desventajas, a partir de dicha información se seleccionó la herramienta Bacula como la mejor opción para el manejo de copias de seguridad en el CSIRT en Cibersecurity de Colombia.

Bacula es una herramienta de software de código abierto que permite a un administrador de TI gestione las copias de seguridad, la restauración de la información y la verificación de los datos a través de una red de servidores de diferentes tipos. Su infraestructura se basa en cliente/servidor. Esta herramienta es fácil de utilizar y eficiente la misma ofrece funcionalidades avanzadas en la administración del almacenamiento que facilita la búsqueda y restauración de datos que se vieron comprometidos en un incidente de seguridad, esta herramienta proporciona compatibilidad para sistemas operativos Windows, MacOS y GNU/Linux.

[30] POZUELO, Alberto. Implantación de sistemas de BackUp Empresarial. 2017. Universitat Oberta de Catalunya. [En línea]. Septiembre 2020. Disponible en: http://hdl.handle.net/10609/63285

Figura 7: Components or Service



Fuente: Wiki.bacula.org (2020). Bacula Components or Service. [En línea] Disponible en: http://wiki.bacula.org/lib/exe/detail.php?id=bacula_manual:what_is_bacula&media=bacula_manual:bacula-applications.png

5.1.7 Software de Sandbox

Un SANDBOX (caja de arena), como lo explica el CSIRT-PONAL[31] de la Policía Nacional, es un entorno completamente aislado donde se pueden detonar archivos o URLs con el fin de generar un análisis de los diferentes comportamientos que se generan en un dispositivo, para así poder clasificar si dicho archivo es potencialmente peligroso para el sistema.

Los análisis de malware en un Sandbox permiten recolectar información de análisis estáticos y dinámicos de forma totalmente automática. En un CSIRT se implementa para generar análisis de forma masiva de diferentes tipos de muestras de malware, la ejecución del SandBox debe realizarse en entornos controlados dentro de un

[31] MINISTERIO DE DEFENSA. Sandbox CSIRT – PONAL. [en línea]. Febrero de 2020. Disponible en: https://cc-csirt.policia.gov.co/noticias/2020/1er-trimestre/sandbox-ponal

laboratorio de CSIRT, normalmente basados en máquinas virtuales, se debe prohibir dentro del CSIRT la ejecución o pruebas en cualquier sistema de producción tanto estaciones de trabajo como servidores.

5.1.7.1 Herramienta de software CUCKOO

Una solución de Sandbox debe ayudar a un CSIRT a mejorar la situación de la organización frente a los ataques sofisticados o selectivos mediante un una detección avanzada y su capacidad de generación de informes sobre amenazas evasivas y persistentes que puede llegar a penetrar la red de la organización o uno de los clientes[32].

La herramienta seleccionada para prestar los servicios de SandBox en un CSIRT debe integrarse en la arquitectura de seguridad existente o combinarse con diferentes capas de seguridad, además debe ser una herramienta escalable y adaptarse a la evolución de la infraestructura tecnológica. Por lo anterior y tomando como referencias diferentes CSIRT nacionales e internacionales como lo son el CSIRT-PONAL[33], el proyecto MARTA[34] de CCN-CERT de España, AfricaCERT (Resources of CSIRT (Tools and Services of CIRT/CSIRT)[35], se seleccionó la herramienta de software Cuckoo

Cuckoo es un sistema de análisis de malware automatizado de código abierto. Se utiliza para ejecutar y analizar automáticamente archivos y recopilar resultados de análisis completos que describen lo que hace el malware mientras se ejecuta dentro de un sistema operativo aislado[36].

Puede recuperar el siguiente tipo de resultados:

---

[32] RAMÍREZ, L. Desarrollo de un Marco de Trabajo para la Protección de un Equipo de Respuesta ante Incidencias de Seguridad Informática (CSIRT). [en línea]. Octubre de 2020. Disponible en: http://cimat.repositorioinstitucional.mx/jspui/handle/1008/442

[33] MINISTERIO DE DEFENSA. Sandbox CSIRT – PONAL. [en línea]. Febrero de 2020. Disponible en: https://cc-csirt.policia.gov.co/noticias/2020/1er-trimestre/sandbox-ponal

[34] BEN, M. How to Build a CIRT based on Open source tools. [en línea]. Septiembre de 2020. Disponible en: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Africa_Cyberdrill_18/Presentations/5-Services.pdf

[35] INTERNATIONAL TELECOMMUNICATION UNION. RESOURCES OF CSIRT (Tools and Services of CIRT/CSIRT). [en línea]. Noviembre 2020. Disponible en: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Services.pdf

[36] CUCKOO SANDBOX BOOK. [en línea]. Septiembre de 2020. Disponible en: https://cuckoo.readthedocs.io/en/latest/

- Rastros de llamadas realizadas por todos los procesos generados por el malware.
- Archivos que se crean, eliminan y descargan por el malware durante su ejecución.
- Volcados de memoria de los procesos de malware.
- Rastreo de tráfico de red en formato PCAP.
- Capturas de pantalla tomadas durante la ejecución del malware.
- Volcados de memoria completa de las máquinas.

5.1.8 Sistema CRM (customer relationship management)

Si el grupo de cliente que atiende un CSIRT por lo general es muy amplio y tiene necesidades de localizar y tener a la mano todos los detalles y almacenarlos para luego generar consultas y agruparlo en funcionalidades, en un repositorio con el cual el CRM será de mucha utilidad. Con respecto al CRM existen diversos tipos de herramientas de pago o gratuitas dependiendo de la necesidad del cliente.[37]

En determinante, un CRM nos irá a proveer una forma de desarrollar nuestro CSIRT desde el conocimiento de los usuarios, admitiendo diferenciarlos y segmentarlos según sus opciones para proporcionarles la vivencia que ellos esperan en la administración de accidentes y no la que CSIRT cree favorable para ellos. Estas siglas, entendidas en hondura, son sinónimo de reafirmación de usuarios, comprensión de nichos de mercado y avance del CSIRT.

5.1.8.1 Herramienta se software SugarCRM

Uno de los CRM más populares y usados a nivel mundial gracias a su cantidad considerable de funciones. Está dirigido a compañías que quieren sostener una interacción enormemente personalizada con sus usuarios y desean tener un exclusivo sistema para todos los departamentos, de manera que todos dispongan de la misma información y tengan una perspectiva unificada del mismo.

SugarCRM ayuda a los CSIRT a crear la base para entablar una secuencia de procesos internos comerciales que incrementan la efectividad de su acercamiento al mercado, empuja los resultados de ventas, optimizando el agrado del cliente y brinda una perspectiva completa de los resultados de la compañía. En sintetizadas cuentas, SugarCRM es una interfaz escalable, 100 % personalizable, fácil de administrar y gratuita que ayudará a los CSIRT con los objetivos de aumentar ingresos y fidelizar clientes con un coste en licencias nulo. SugarCRM se puede

[37] ENISA. (2006). Cómo crear un CSIRT paso a paso. (CERT-D1/D2). [en línea]. Septiembre de 2020. Disponible en: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

alojar tanto on-site en los servidores de la empresa, como on-demand a través de SugarCRM.

5.1.9 Identificación de vulnerabilidades

Es de suma importancia la gestión de vulnerabilidades en las compañías, esto debido al crecimiento y sofisticados de los ambientes tecnológicos de las organizaciones y la lista exponencial de posibles problemas de seguridad en los diferentes sistemas informáticos como lo son sistemas operáticos, redes, IoT entre otros. Los departamentos de tecnología de la información cuentan con múltiples funciones en su día a día con tiempos limitados donde no se pueden hacer cargo de manejar un ambiente de reconocimiento de vulnerabilidades. Por el alto número de sistemas y la cantidad periódica de actualizaciones distribuidas y las dificultad de analizar el valor de las reparaciones de seguridad para los gerentes de la organización, la reducción de debilidad con las que se cuenta tanto en la red como en aplicaciones críticas es un reto constante para el personal de sistemas[38], es por esto que una de las funcionalidades de un CSIRT es tener control sobre la gestión de vulnerabilidades que tienes los clientes, proporcionando información y análisis y corrección de vulnerabilidades.

5.1.9.1 Herramienta de software OpenVas

El Sistema de Evaluación de Vulnerabilidad Abierta, conocido más comúnmente como OpenVAS, es un conjunto de herramientas que trabajan juntas para ejecutar pruebas en las computadoras de los clientes utilizando una base de datos de vulnerabilidades y vulnerabilidades conocidas. El objetivo es aprender sobre qué tan bien están protegidos los equipos contra los vectores de ataque conocidos.

OpenVAS nos proporciona herramientas robustas que ayudaran a nuestro CSIRT a tener una correcta gestión de vulnerabilidades en los clientes, identificando fallas de configuración y actualizaciones de seguridad que el equipo de TI no se haya percatado, brindándonos una visión estadística de las vulnerabilidades que tiene una compañía. Y dándonos la información necesaria para el análisis del CSIRT.

[38] ORGANIZACIÓN DE ESTADOS AMERICANOS. Buenas prácticas para establecer una CSIRT nacional. [en línea]. Octubre de 2020. Disponible en: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

5.2 HERRAMIENTAS DE HARDWARE PROPUESTAS PARA EL CSIRT

Basado en la guía de ENISA, sobre cómo crear un CSIRT paso a paso, se seleccionaron las herramientas de hardware para la empresa Cybersecurity de Colombia LTDA, las herramientas propuestas son las siguientes: servidores, equipos de comunicaciones, dispositivos de seguridad lógica y repositorios de datos, es de suma importancia que estos equipos permanezcan en un centro de datos o en las instalaciones del CSIRT y que el acceso físico y lógico a estos equipos cumpla con un estricto control que garantice que se respeten las políticas de acceso a la información, además de asegurar la información electrónica, se propone que el CSIRT mantenga un depósito de seguridad para almacenar información sensible no digital, fichas, discos duros y servidores, entre otros.

5.2.1 Servidores

Se propone contar con servidores de intranet, servidor de archivos, servidor de copias de seguridad, servidor DNS, servidor de monitoreo, servidor sandbox.

5.2.2 Equipos de comunicación (telefonía)

Para un CSIRT es fundamental la comunicación, es por esto que se recomienda que el CSIRT tenga acceso directo a los servicios de telefonía, telefonía fija, telefonía IP y los teléfonos móviles, que le permiten hacer llamadas locales e internacionales según sea necesario para operar. entre su equipo, hacia los clientes, con otros CSIRT, con proveedores, entre otros. Es común que un reporte de algún incidente se realice vía telefónica, cuando esto sucede, es necesario generar documentación de todos y cada uno de los detalles del incidente. Se recomienda tener un teléfono central que funcione como principal contacto para el equipo, siendo disponible para ser contestado por cualquier miembro del equipo, para esto es de suma importancia tener un servidor de VoIP robusto que nos ayude a proporcionar las herramientas de comunicación necesarias en el CSIRT

5.2.3 Equipos de computación PC.

Se recomienda que el personal del CSIRT tenga equipos de computación portátiles que se utilicen exclusivamente para funciones de trabajo.

5.2.4 Hadware de Firewall

Es recomendable usar este tipo de hardware especializado, tomando en cuenta que este dispositivo contiene un software preinstalado, el firewall debe ser el primer elemento de seguridad, el objetivo de este dispositivo es bloquear posibles intromisiones a la red de la organización.

5.2.5 IPS

Es aconsejable que el CSIRT disponga de este tipo de hardware ya que el mismo protege a las redes de amenazas conocidas o no bloqueando ataques (ITECO CERT, 2009). Estos dispositivos son encargados de revisar el tráfico de red con el propósito de detectar y responder a posibles ataques o intrusiones.

5.2.6 Honeypot:

Este dispositivo debe estar aislado del ambiente de producción. Según un estudio realizado por ENISA, el mejor honeypot de propósitos generales es Dionaea (Grudziecki, Jacewicz, Juszczyk, Kijewski, & Pawlinski, 2012)

5.2.7 Hardening:

Estos dispositivos son recomendables para el fortalecimiento de todo el proceso ya que asegura al sistema mediante la reducción de vulnerabilidades, eliminado softwares, servicios, usuarios y cerrando puertos que no estén en uso.

5.2.8 FAX

Es recomendable que el CSIRT disponga de fax que sea de uso exclusivo dentro de sus instalaciones, esto con el fin de evitar que cualquier fax con información sensible sea visto por personal no autorizado.

5.2.9 Sistema de respaldo de datos

Es importante contar con un sistema de Discos RAID (Redundant Array of Independent Disks) los cuales hacen copias o espejos de información en tiempo real.

5.2.10 Almacenamiento lógico portátil.

Se hace necesario el uso de unidades externas o unidades flash para el almacenamiento de información. Se sugiere que el CSIRT debe tener como mínimo cuatro unidades externas de 2 TB y cinco unidades de memoria flash de 32 GB.

5.3 DEPENDENCIAS PARA LA CONFORMACIÓN DEL CSIRT

Para definir la estructura bajo la cual estará implementado el CSIRT, primero es importante realizar la definición de las dependencias que lo van a soportar ya que, en base a esto, se definirá el personal necesario para la implementación del CSIRT en la empresa Cibersecurity de Colombia LTDA.

Tomando como referencia lo expresado por la OEA[39], el CSIRT de la empresa Cibersecurity de Colombia LTDA tendrá las siguientes dependencias:

5.3.1 Dirección:

Es la dependencia encargada de establecer la supervisión de toda la estructura de trabajo y del personal que la integra, establece las estrategias de trabajo de la organización, asigna responsabilidades, realiza el reclutamiento de personal, presenta los reportes de los incidentes y amenazas, establece acuerdos de cooperación con otras organizaciones, así como también, debe velar por el recurso administrativo disponible, está conformada por el líder del equipo de respuesta o gerente del CSIRT.

Para la formación de CSIRT se requiere 1 persona en esta dependencia que va a asumir el rol de Director/Coordinador del CSIRT.

[39] ORGANIZACIÓN DE ESTADOS AMERICANOS. Buenas prácticas para establecer una CSIRT nacional. [en línea]. Octubre de 2020. Disponible en: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

5.3.2 Operaciones y seguridad de la información:

Es la dependencia encargada de velar por el monitoreo de las operaciones que realiza el CSIRT y el control de los dispositivos que son supervisados por la organización, realizar análisis de software malicioso, realizar los análisis de vulnerabilidad, definir estrategias de seguridad, dirigir las acciones de respuesta ante incidentes, notificar los incidentes de seguridad de la información ocurridos y elaborar los informes para la notificación a los clientes. Esta dependencia debe estar conformada por especialistas en el área de seguridad informática con alta experiencia.

Para la formación de CSIRT se requieren 2 personas en esta dependencia, un especialista en operaciones y un especialista en seguridad de la información.

5.3.3 Investigación forense y nuevos desarrollos

Es la dependencia encargada de realizar investigaciones especiales para en análisis de incidentes y eventos ocurridos, también debe velar por el desarrollo de nuevas tecnologías que permitan la resolución de los incidentes de forma rápida y oportuna, diseño y ejecución de planes de capacitación al personal de otras dependencias y llevar las estadísticas de los incidentes. Esta dependencia debe estar conformada por especialistas en el área.

Para la formación de CSIRT se requiere 1 persona en esta dependencia para realizar las actividades indicadas.

5.3.4 Telecomunicaciones y TI

Es la dependencia encargada de hacer seguimiento a los incidentes y al tráfico de información de red en la organización, determinar la posible existencia de amenazas, contener los incidentes de peligro en el perímetro de la red evitando su ingreso, mantener el sitio web del CSIRT, gestionar el servicio de correo electrónico y velar por su seguridad e integridad, adicionalmente se encarga de administrar la red interna de la organización y establecer protecciones ante ataques externos. En el caso de los incidentes relacionados con redes debe ayudar en la respuesta a estos casos. Esta dependencia debe estar conformada por especialistas en el área de seguridad informática con alta experiencia.

Para la formación de CSIRT se requieren 2 personas en esta dependencia, un especialista en redes y telecomunicaciones y un especialista en tecnologías de información y gestión de servicios a través de la Web.

5.3.5 Relaciones Públicas

Es la dependencia encargada de gestionar la información y transmitir información a los usuarios que hacer un del servicio proporcionado por la organización, la información emitida debe ser clara y evitar la confusión de usuarios que no son expertos en el lenguaje que maneja la organización, también debe representar al CSIRT en los eventos que sean organizados para los usuarios. La dependencia puede estar conformada por una persona profesional en el área.

Para la formación de CSIRT se requiere 1 persona en esta dependencia para realizar las actividades indicadas.

5.3.6 Jurídico

Es la dependencia encargada de realizar seguimiento jurídico a todos los incidentes por delitos informáticos e iniciar los procedimientos administrativos que así se requieran para la defensa y protección de los usuarios. También es la dependencia encargada de revisar la evolución del marco legal y las adecuaciones del marco normativo de la organización.

Para la formación de CSIRT se requiere 1 abogado.

5.4 PERFILES DEL EQUIPO DE TRABAJO PARA LA CONFORMACIÓN DEL CSIRT

Para definir y representar formalmente la estructura organizativa adecuada para la implementación del CSIRT en la empresa Cibersecurity de Colombia LTDA, es importante tener conocimiento de la estructura de la organización y del grupo de clientes atendido, así como de la posibilidad de contratar expertos para cubrir las necesidades específicas.

El modelo organizativo, propuesto para la empresa Cibersecurity de Colombia LTDA es el modelo incrustado, este modelo se puede usar ya que se va a crear un CSIRT dentro de una organización existente como lo es la mencionada empresa, partiendo

de que la empresa tiene un departamento de TI ya existente, El CSIRT está dirigido por un jefe de equipo responsable de las actividades. El jefe de equipo reúne a los técnicos necesarios cuando resuelve incidentes o trabaja en actividades del CSIRT. Puede pedir asistencia especializada a la organización existente. Lo útil del modelo incrustado es que se puede adaptar a situaciones concretas que vayan surgiendo.

Es casi imposible presentar cifras reales sobre el número de técnicos para la implementación del CSIRT, pero los valores siguientes, fueron tomados de la guía ENISA, ellos proponen usar la siguiente aproximación:

- ✓ Para los servicios básicos de distribución de boletines de seguridad y tratamiento de incidentes: un mínimo de 4 trabajadores a tiempo completo o equivalentes.
- ✓ Para un servicio completo en horario de oficina y servicios de mantenimiento: un mínimo de entre 6 y 8 trabajadores a tiempo completo o equivalentes.
- ✓ Para un turno dotado de todo el personal necesario 24 horas al día, 7 días a la semana (2 turnos fuera del horario de oficina), el mínimo es de unos 12 trabajadores a tiempo completo o equivalentes.

A continuación, se propone un equipo CSIRT típico, con las funciones definidas y se presenta una breve visión general de los perfiles y competencias del personal para ser encargado del CSIRT en la empresa Cibersecurity de Colombia LTDA:

5.4.1 Rol: director de CSIRT

Experiencia requerida: 10 años como analista o líder de equipos de informática.

Titulación requerida: Ingeniero en computación, de sistemas, informática, electrónica, ciber seguridad o a fines, con especialización o maestría en seguridad informática.

Certificaciones: CISSP, ISO27001 Lead Auditor o Implementer, gerencia de proyectos

Conocimientos técnicos: administrador de sistemas operativos (Windows, Linux), conocimientos en seguridad informática y encriptación de datos, programación avanzada, análisis forense de datos, elaboración y gestión de proyectos, gestión de personal, diseño de herramientas de TIC, marco legal inherente al área, gerencia.

Funciones: elaboración de planes de seguridad informáticos, elaboración de planes operativos anuales, diseño de marcos normativos en seguridad electrónica,

evaluación de arquitecturas de seguridad, ejecución de auditorías en seguridad de la información, gestión de equipos de trabajo, gestión de TI, liderar los equipos de trabajo, reclutamiento de personal, elaboración de informes, seguimiento de resolución de conflictos informáticos, evaluación de software, diseño de planes de mejoramiento, punto de contacto con los representantes de comunidades y organizaciones a las que se da servicio y enlace con el resto de CERTs aliados.

5.4.2 Rol: Analista de operaciones y seguridad de la información

Experiencia requerida: 5 años

Titulación requerida: Ingeniero en computación, de sistemas, informática, electrónica, ciber seguridad o a fines, con especialización o maestría en seguridad informática.

Certificación: CISSP o CISA ISO27001 Lead Auditor o ISO27001 Implementer.

Conocimientos técnicos: administrador de sistemas operativos (Windows, Linux), conocimientos en seguridad informática y encriptación de datos, programación avanzada, análisis forense de datos, gestión de personal, diseño de herramientas de TIC.

Funciones: ejecución de planes de seguridad informáticos, elaboración de planes de trabajo semanales, implantación de sistemas de gestión de seguridad de la información, evaluación e implantación de arquitecturas de seguridad, gestión de TIC, resolución de conflictos informáticos, evaluación de software, liderar los equipos de trabajo, elaboración de informes de resultados, elaboración de planes de mejoramiento.

5.4.3 Rol: analista de investigación forense y nuevos desarrollos

Experiencia requerida: 5 años en áreas afines.

Titulación requerida: Ingeniero de sistemas, informático o técnico en informática.

Certificación: OSCP o CEH o OSCE

Conocimientos técnicos: sistemas operativos (Windows, Linux, UNIX) a nivel de administrador, protocolos de seguridad informáticos (IPSec, VPN, SSL, TLS), uso de herramientas de seguridad (scanners, firewalls, IDS, UTM, antimalware),

programación de sockets (RAW, TCP, UDP), criptografías, mecanismos de seguridad (firmas digitales, certificados), informática forense.

Funciones: gestión, análisis y respuesta ante las amenazas que involucran la infraestructura de TI, análisis de eventos y software, evaluación de incidentes, elaboración de reportes de fallas, gestión de bases de datos, análisis de incidentes, mejoramiento en la resolución de eventos.

5.4.4 Rol: analista de telecomunicaciones y TI

Experiencia requerida: 3 años en áreas afines.

Titulación requerida: Ingeniero de sistemas, informático o afín.

Certificación: CCNA, redes, TI.

Conocimientos técnicos: sistemas operativos (Windows, Linux, UNIX) a nivel de administrador, protocolos de red, direccionamiento, trafico web, gestión de correo electrónico, uso de herramientas de seguridad (scanners, firewalls, IDS, UTM, antimalware), programación de sockets (RAW, TCP, UDP), conocimiento de bases de datos.

Funciones: gestión, análisis y respuesta ante las amenazas que involucran la infraestructura de TI, análisis de eventos y software, evaluación de incidentes, gestión de bases de datos.

5.4.5 Rol: analista en relaciones públicas.

Experiencia requerida: 2 años.

Titulación requerida: formación en relaciones públicas, marketing digital, o afines.

Certificación: certificado de marketing digital.

Conocimientos técnicos: desarrollo de imágenes y anuncios para publicidad e identidad corporativa, diseño de logos y propagandas, identificación de tendencias sociales, económicas y políticas, elaboración de planes de trabajo, conocimientos en logística de eventos,

Funciones: desarrollar la imagen corporativa del CSIRT, dirigir y supervisar la estrategia de redes sociales de la empresa, informar a los usuarios de las ventajas de la empresa de forma clara y efectiva, mantener una actividad de comunicación y

promoción con los usuarios, promocionar los servicios que presta y para divulgar conocimiento específico sobre seguridad del CSIRT, llevar a cabo la planificación y ejecución de inauguraciones, eventos, lanzamientos, recopilación de informes y presentaciones de nuevos productos a la prensa.

5.4.6 Rol: especialista Jurídico.

Experiencia requerida: 3 años

Titulación requerida: Título profesional en Abogacía o derecho administrativo.

Certificación: Delitos informáticos

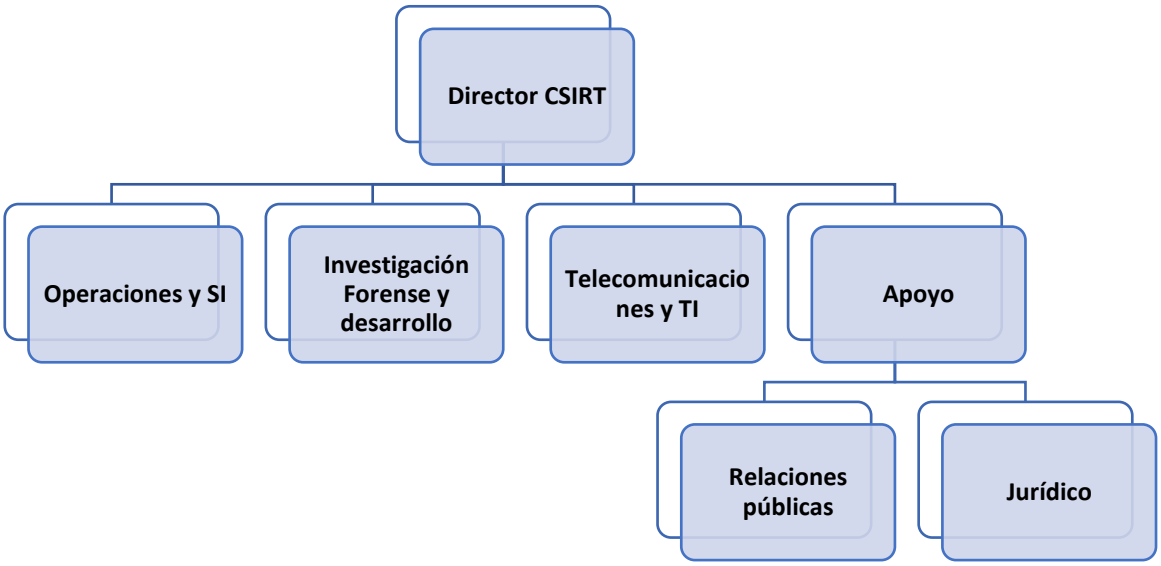
Conocimientos técnicos: auditoría legal en aspectos tecnológicos, delitos informáticos, gerencia de proyectos de archivos bajo el enfoque de PMI, asesoría y recopilación de pruebas electrónicas, leyes nacionales e internacionales en materia de tecnología.

Funciones: análisis de los delitos informáticos, elaboración de informes con implicaciones legales, asesorías a usuarios que han sufrido robo de información, elaboración de procedimientos administrativos y legales contra los responsables de los delitos cometidos.

5.5 Esquema organizativo propuesto para el CISRT

El siguiente diagrama muestra el organigrama propuesto para la implementación de del CSIRT teniendo presente las diferentes áreas establecidas con base a las necesidades y realidades de CIBERSECURITY DE COLOMBIA LTDA.

Figura 8 Organigrama propuesto para la implementación del CISRT

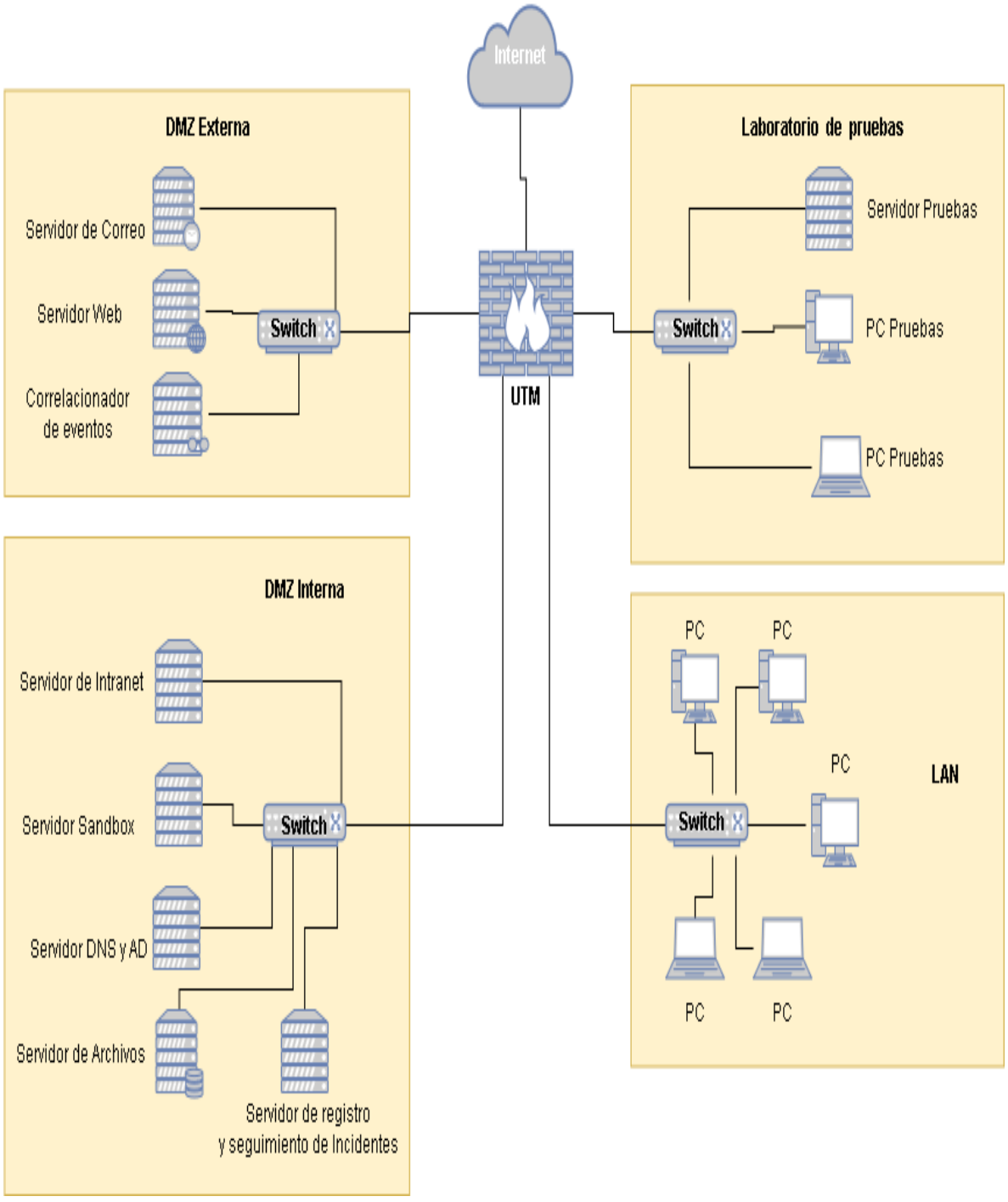


Fuente: Elaboración propia.

5.5.1 Topología de red

La siguiente imagen plantea la topología de red para el CSIRT con sus diferentes elementos de red teniendo en cuenta algunos aspectos generales como lo son: Aire acondicionado y piso falso (principalmente para el centro de datos), Sistemas de detección y extintores en las salas comunes y en el centro de datos, Sistemas redundantes (fuente de Sistema de Alimentación Ininterrumpida (UPS), aire acondicionado, etcétera), Gabinetes de papelería bajo llave.

Figura 9 Esquema de red CSIRT, Cibersecurity de Colombia

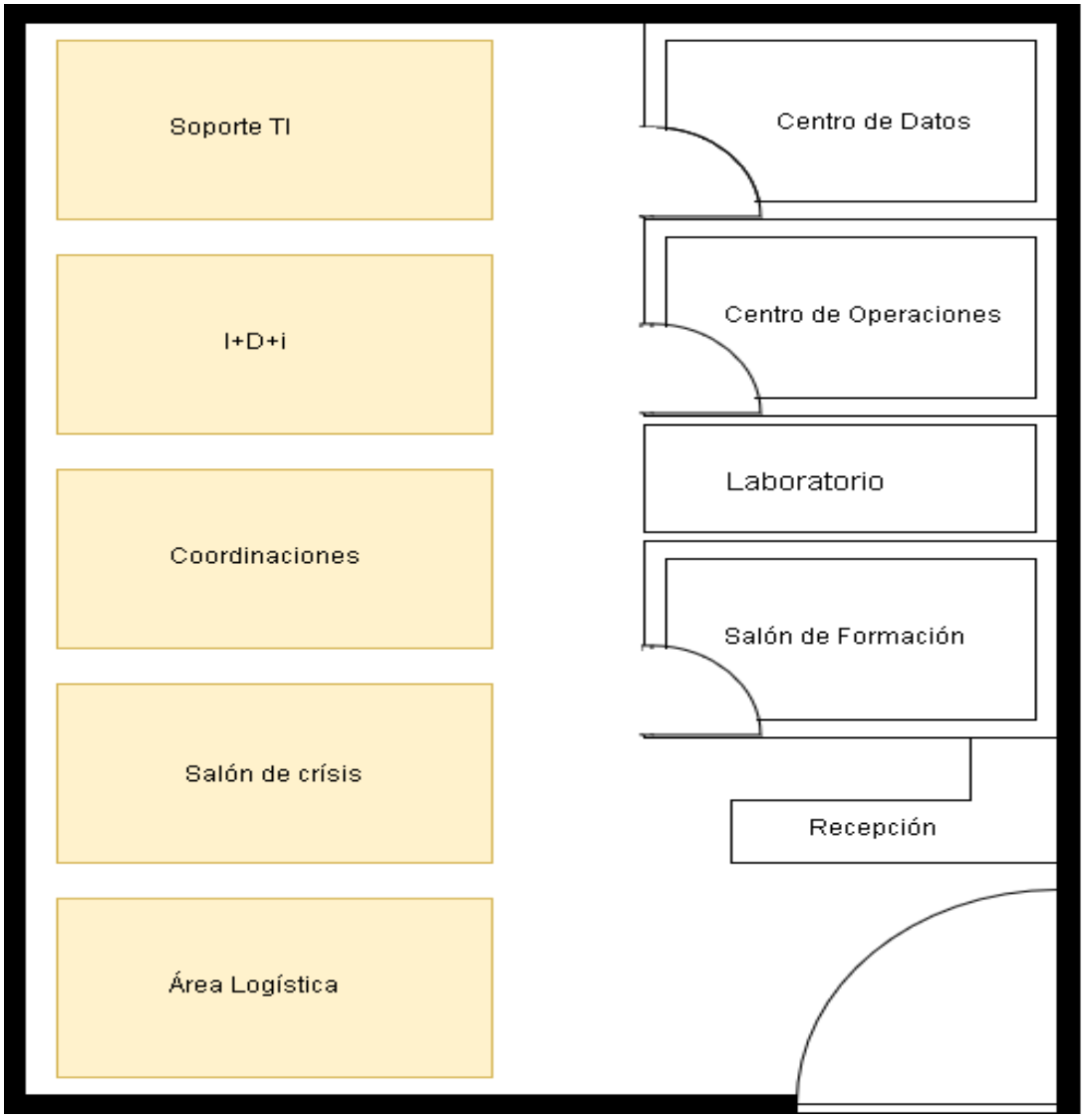


Fuente: Elaboración Propia

5.5.2 Planta física

A continuación, se describe la plata física del CSIRT donde se generan acceso controlado a: El edificio (puertas y ventanas), El piso, Zonas comunes (Operaciones, Soporte Informático, I+D) Centro de datos. Área de Logística, laboratorio, sala de monitoreo, entre otros. El siguiente esquema se realiza con base a la guía “Buenas prácticas para establecer un CSIRT nacional” propuesta por La Organización de los Estados Americanos (OEA).

Figura 10: Propuesta de planta física CSIRT.



Fuente: Elaboración Propia

5.5.2.1 Centro de Datos: es el espacio físico donde están ubicados los servidores de CSIRT y se almacena la información en una base de datos. Este espacio físico debe ser atendido por un especialista y tener óptimas condiciones de temperatura para los equipos que allí se encuentran.

5.5.2.2 Centro de Operaciones: es el espacio físico donde está ubicado el equipo de atención de respuesta rápida a emergencias y eventos que ocurran a los clientes del CSIRT. Los casos que allí se atienden son usualmente de emergencia y estos son asignados directamente por el director o coordinador del CSIRT. En esta locación puede haber hasta cuatro estaciones de trabajo de personal altamente especializado.

5.5.2.3 Laboratorio: es el lugar donde está ubicado el equipo que realiza las pruebas a los softwares maliciosos que han sido detectados por el CSIRT y se realizan las investigaciones para dar solución a estas amenazas. El laboratorio contiene hasta dos estaciones de trabajo de personal especializado.

5.5.2.4 Salón de formación: es un espacio de uso común generalmente utilizado para dar capacitación sobre temas específicos al personal que presta servicios en el CSIRT. Este salón contiene una serie de equipos audiovisuales especiales para dar capacitaciones y podrá recibir hasta 15 personas al mismo tiempo.

5.5.2.5 Área de logística: es el área donde está ubicado el equipo que planifica las actividades a corto plazo del CSIRT y coordina todos los elementos que requieren esas actividades. También cuenta con un depósito donde se tiene un stock de equipos de repuesto en caso de que se requiera reemplazos de urgencia.

5.5.2.6 Salón de crisis: es el espacio donde se encuentra el equipo de atención a los usuarios que han sido atacados y que requieren una atención rápida y personalizada. Este salón tiene dos estaciones de trabajo y el personal que labora en el mismo ha tenido una capacitación especializada en el tema para lograr que la atención de estas personas que están en estado de alteración sea la mejor posible.

5.5.2.7 Coordinaciones: es el espacio donde está ubicada la oficina del director o coordinador del CSIRT que es la persona que dirige el funcionamiento de la oficina. Cuenta con espacio para instalar hasta dos estaciones de trabajo en caso de que se requiera un coordinador o asistente.

5.5.2.8 I+D+I: el espacio donde se realiza la investigación y desarrollo del CSIRT es un área física con espacio hasta para cuatro estaciones de trabajo de personal especializado, donde se realizan investigaciones avanzadas sobre los incidentes y amenazas de software nuevos que tienen como objetivo el robo de información digital a los usuarios. Investigación y Desarrollo es una dependencia física de suma importancia ya que apunta hacia donde se va a inclinar el uso de los CSIRT a futuro.

5.5.2.9 Soporte TI: En este espacio físico se ubican los operadores que dan soporte técnico a los usuarios de los CSIRT vía telefónica o a través del correo electrónico, el área tiene capacidad hasta para cuatro estaciones de trabajo.

5.6 GUIA TÉCNICA DE INSTALACIÓN DE HERRAMIENTAS DE SOFTWARE

A continuación, se realiza la guía de instalación de las principales herramientas de software propuestas para la implementación del CSIRT en Cybersecurity de Colombia.

5.6.1 Instalación de Bacula

Bacula al ser un sistema distribuido, se pueden generar varios arreglos para el deploy de la instalación del sistema de Backup. Para entornos pequeños, una sola máquina probablemente puede alojar todos los componentes del Bacula: el Director, el Almacenamiento Daemon, el File Daemon (cliente de backup), la base de datos del Catálogo y las interfaces web, como bweb (Enterprise) y Baculum (Community)**.** Para entornos más grandes, los Storage Daemons se pueden instalar en diferentes máquinas, proporcionando equilibrio de carga para la carga de trabajo de copia de seguridad.

La siguiente tabla muestra los recursos sugeridos de RAM y CPU para una máquina que aloja el Director y la base de datos

Tabla 2: Dimensionamiento de Bacula

# Clientes de Backup	25	50	200	500	2000	5000
RAM	8	8	16	32	64	128
CPUs	2	2	4	4	8	8

Fuente: Bacula. Dimensionamiento de Bacula [en línea]. Dimensionamiento de Bacula y Distribución de Componentes. 2 de septiembre de 2018. Disponible en: http://www.bacula.lat/dimensionamiento-de-bacula/?lang=es.

Sistemas Operativos soportados:

- GNU/Linux 32/64 bits:
  - Gentoo
  - Red Hat
  - Fedora
  - Mandriva
  - Debian
  - OpenSUSE
  - Ubuntu
  - Kubuntu
  - Versiones de kernel 2.6 de Linux
- MS Windows, disponibles como un programa binario de instalación
- MacOSX

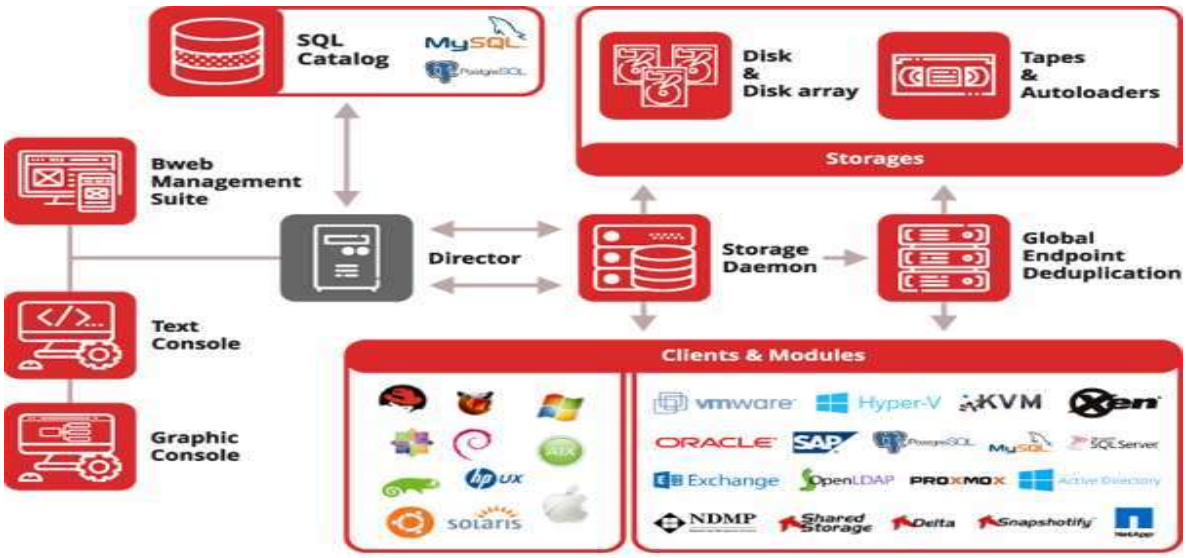
Requerimientos de software adicional.

- Requiere GNU C++, en la versión 2.95 o superior para compilar.
- MySQL 4.1
- PostgreSQL 7.4
- SQLite 2.8.16 o SQLite 3

Los componentes principales del servidor Bacula son:

- ***Bacula Director***: el software que controla las operaciones de copia de seguridad y restauración, controladas por los daemons de archivos y de almacenamiento.
- ***Storage Daemon (SD)***: el software que realiza las operaciones de lectura y escritura de los archivos sobre los dispositivos de almacenamiento usados en las backups.
- ***Catalog***: servicios que mantienen una base de datos de los archivos salvaguardado en las copias de seguridad. La base de datos es MySQL o PostgreSQL.
- ***Bacula console***: una interfaz de línea de comandos que nos permite interactuar y controlar el bacula director.

Figura 11: Bacula Architecture



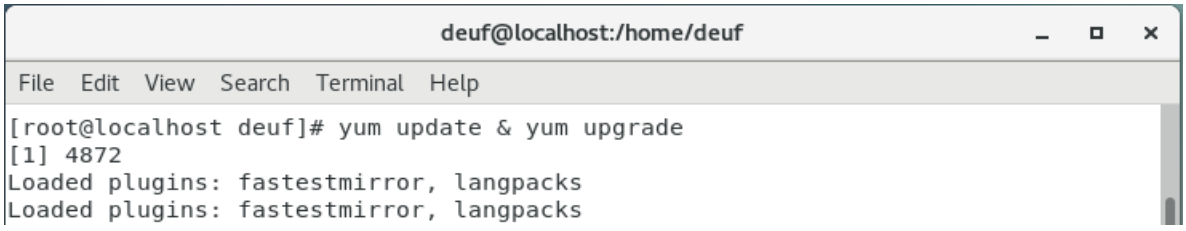
Fuente: Bacula Latinoamérica. Bacula Architecture [En línea] Disponible en: http://www.bacula.lat/bacula-enterprise-edition-10-2-con-copia-de-seguridad-y-recuperacion-integradas-de-los-entornos-de-virtualizacion-de-red-hat/?lang=es

Para la instalación se utilizó una maquina virtualizada en VMware con Centos7, una base de datos Maria DB y Bacula con los módulos (Storage, Console, director y client). Para dicha instalación se tomó como base el documento proporcionado por Bacula A short guide to installing Bacula[40].

Antes de comenzar la instalación de Baculo es necesario actualizar los repositorios y software del sistema operativo para ello ejecutamos los comandos

 # yum update & yum upgrade.

Figura 12: Actualización de repositorios CentOS.



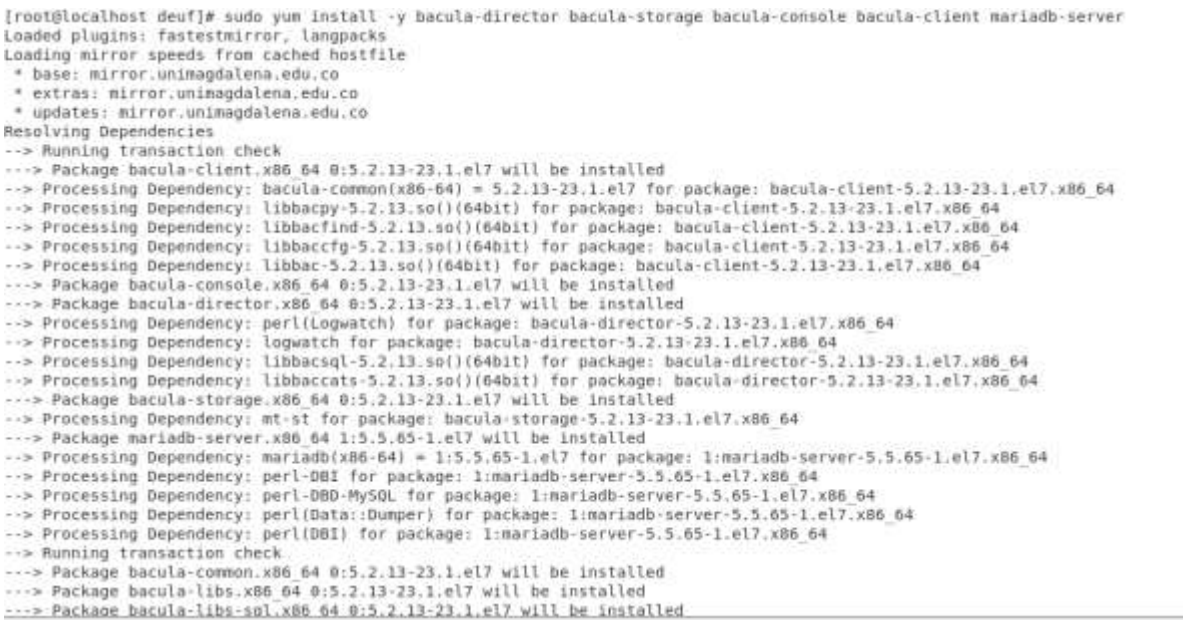
Fuente: Elaboración Propia

[40] Anónimo. Bacula Community Installation Guide A short guide to installing Bacula [En linea]. 20 de Septiembre 2020. Disponible en: https://blog.bacula.org/whitepapers/CommunityInstallationGuide.pdf

Luego de que el sistema operativo este actualizado procedemos con la instalación del software necesario para la instalación del servidor de BackUp para ello se ejecuta el comando

 # yum install -y bacula-director bacula-storage bacula-console bacula-client mariadb-server.

Figura 13. Instalación de módulos de Bacula y BD

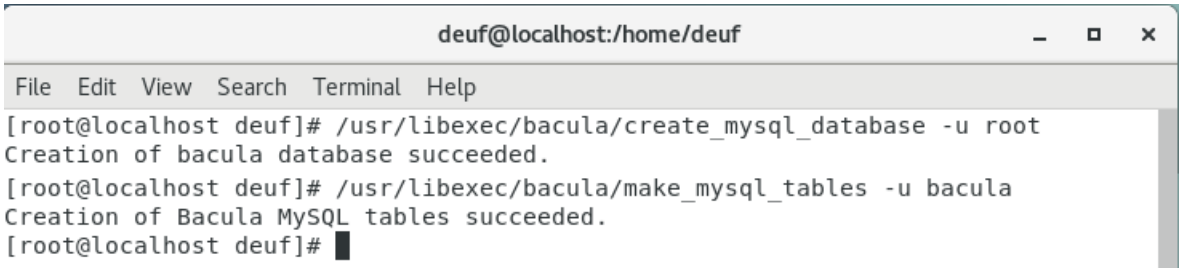


Fuente: Elaboración propia

Con los módulos de Bacula y la base de datos instalada y ejecutándose, se genera la creación de la base de datos Bacula junto con las tablas, para ellos se deben ejecutar los siguientes comandos

 # /usr/libexec/bacula/grant_mysql_privilege
 # /usr/libexec/bacula/create_mysql_database -u root
#/usr/libexec/bacula/make_mysql_tables -u bacula

Figura 14: Creación de base de datos y tablas Bacula

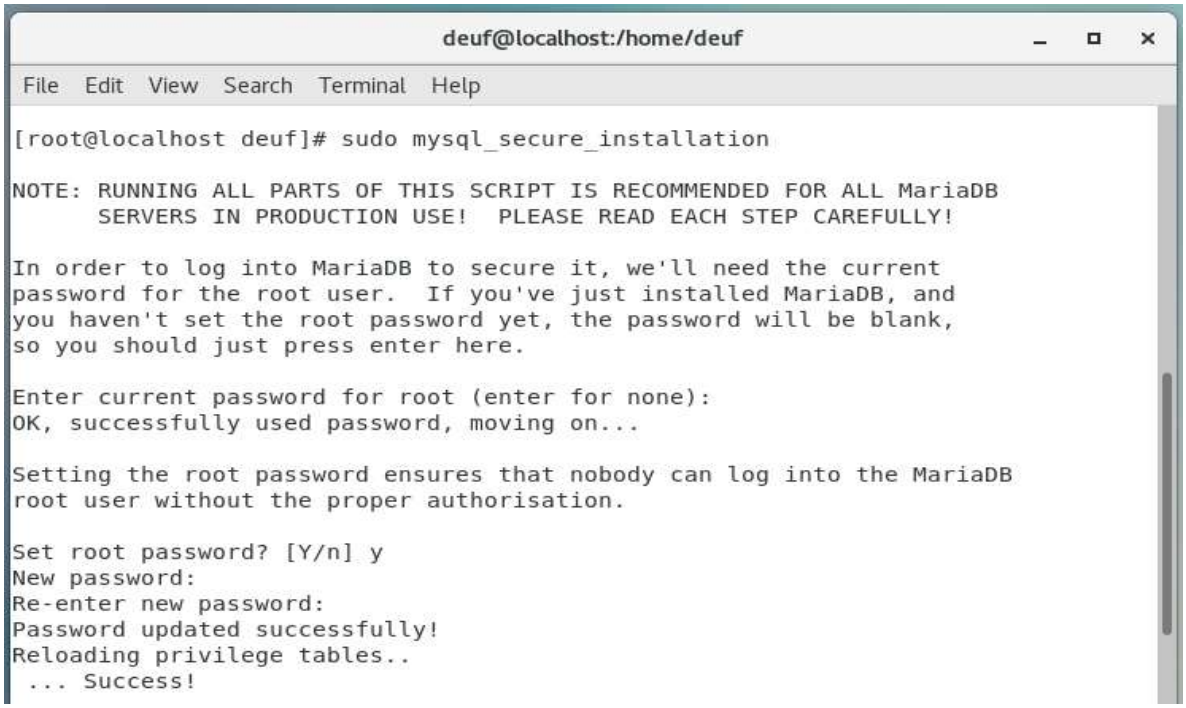


Fuente: Elaboración propia

Ahora para cumplir con los parámetros de seguridad mínimo es necesario ejecutar el script de seguridad para eliminar algunos valores predeterminados peligrosos y agregar contraseña para usuario root de la base de datos, para esto se ejecuta el comando.

mysql_secure_installation

Figura 15: Modificación parámetros de seguridad MariaDB

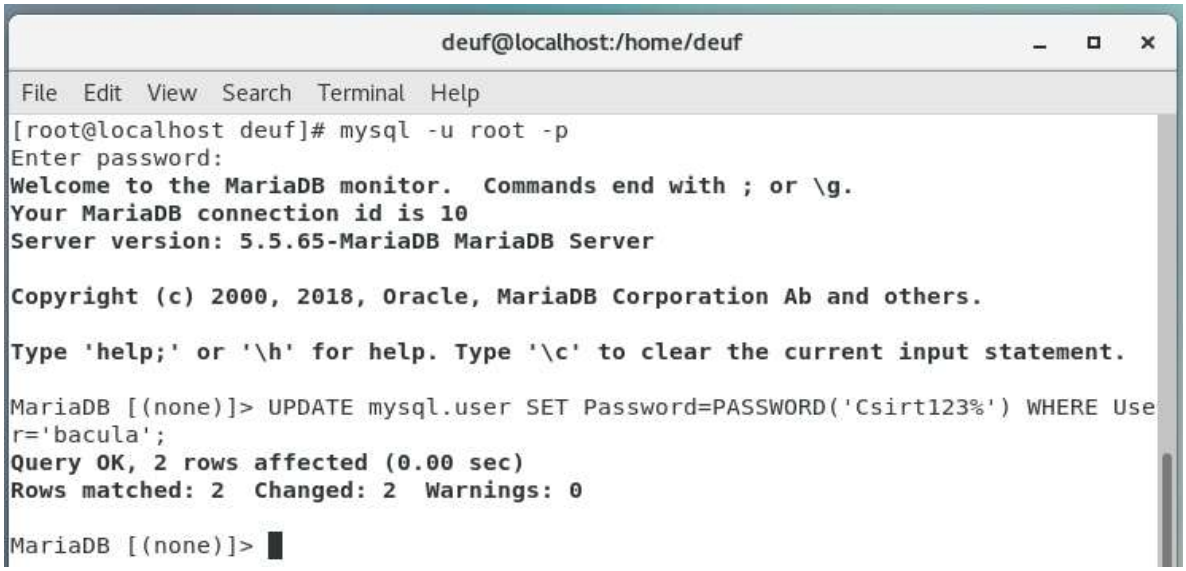


Fuente: Elaboración propia

El siguiente paso fue establecer una contraseña para el usuario Bacula en MariaDB.

 # mysql -u root -p
mysql -u root -pMariaDB [(none)]> UPDATE mysql.user SET Password=PASSWORD('bacula_db_password') WHERE User='bacula';
MariaDB [(none)]> FLUSH PRIVILEGES;
MariaDB [(none)]> exit

Figura 16: Contraseña de usuario Bacula.

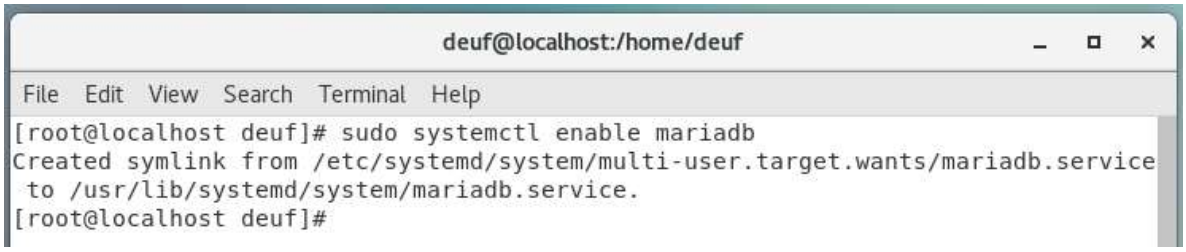


Fuente: Elaboración propia

Se debe habilitar que MariaDB se ejecute automáticamente en el inicio, esto se realiza ejecutando el comando.

 # systemctl enable mariadb

Figura 17: Habilitar Demonio MariaDB

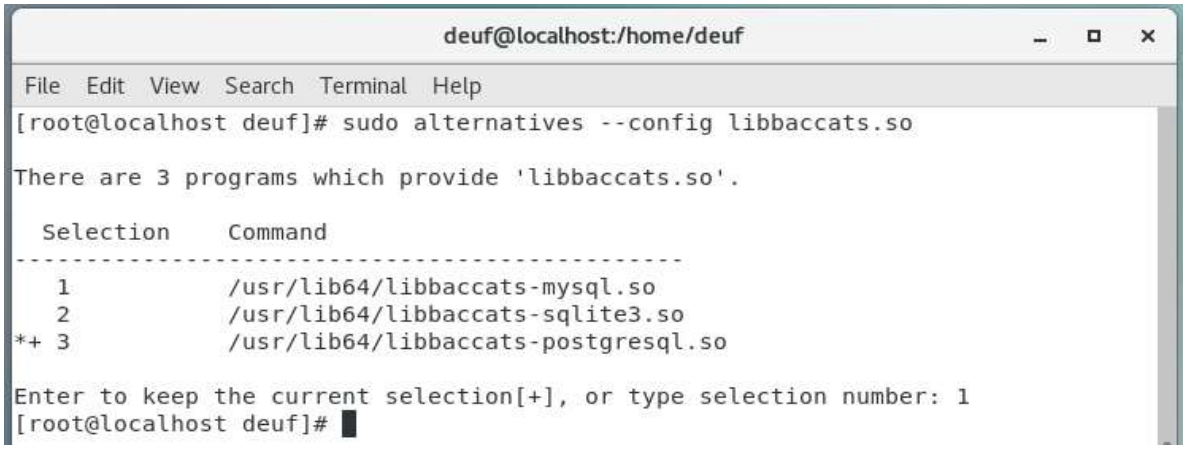


Fuente: Elaboración propia

Para la instalación de Bacula se seleccionó el motor de base de datos MariaDB. Por defecto Bacula viene configurado para trabajar con el motor de base de datos PosgresSQL, por esto es necesario cambiar para usar la biblioteca de MySQL, esto se realiza ejecutando el comando:

 # alternatives --config libbaccats.so

Figura 18:Selección de motor de base de datos

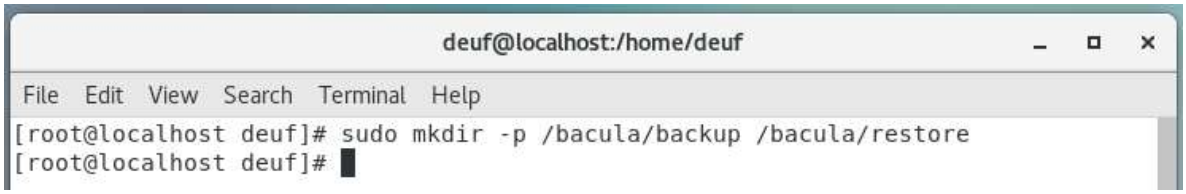


Fuente: Elaboración propia

Con lo anterior ya se tienen correctamente instalados los componentes del servidor Bacula y del cliente Bacula, ahora es necesario crear los directorios de BackUp y restauración. Para que Bacula funcione correctamente es necesario un director para almacenar las copias de seguridad y otro directorio para ubicar los archivos restaurados. A continuación, se muestran los comandos para crear dichos directorios.

 # mkdir -p /bacula/backup /bacula/restore

Figura 19: Creación directorios Bacula



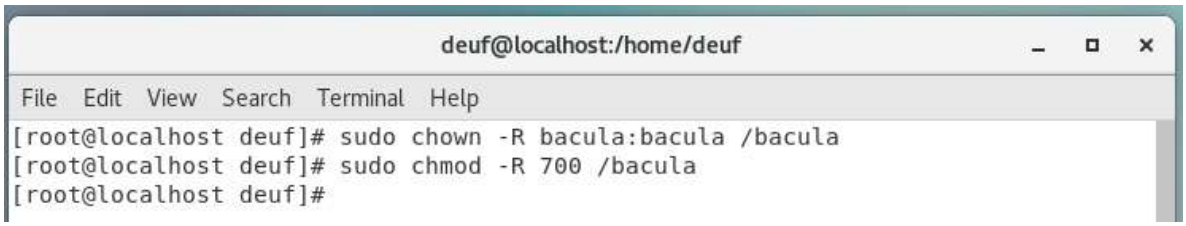
Fuente: Elaboración propia

Ahora se deben modificar los permisos para que solo el usuario bacula y un superusuario puedan acceder a dichos directorios.

 # chown -R bacula:bacula /bacula

 # chmod -R 700 /bacula

Figura 20:Permisos directorios Bacula

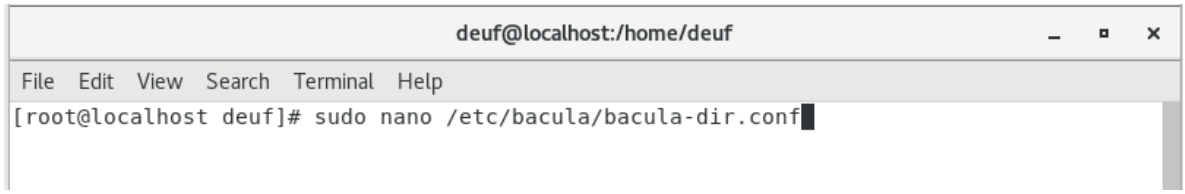


Fuente: Elaboración Propia

A continuación, se debe modificar el archivo de configuración de Bacula con el editor preferido, para este caso se utilizó nano.

 # nano /etc/bacula/bacula-dir.conf

Figura 21: Apertura bacula-dir.conf

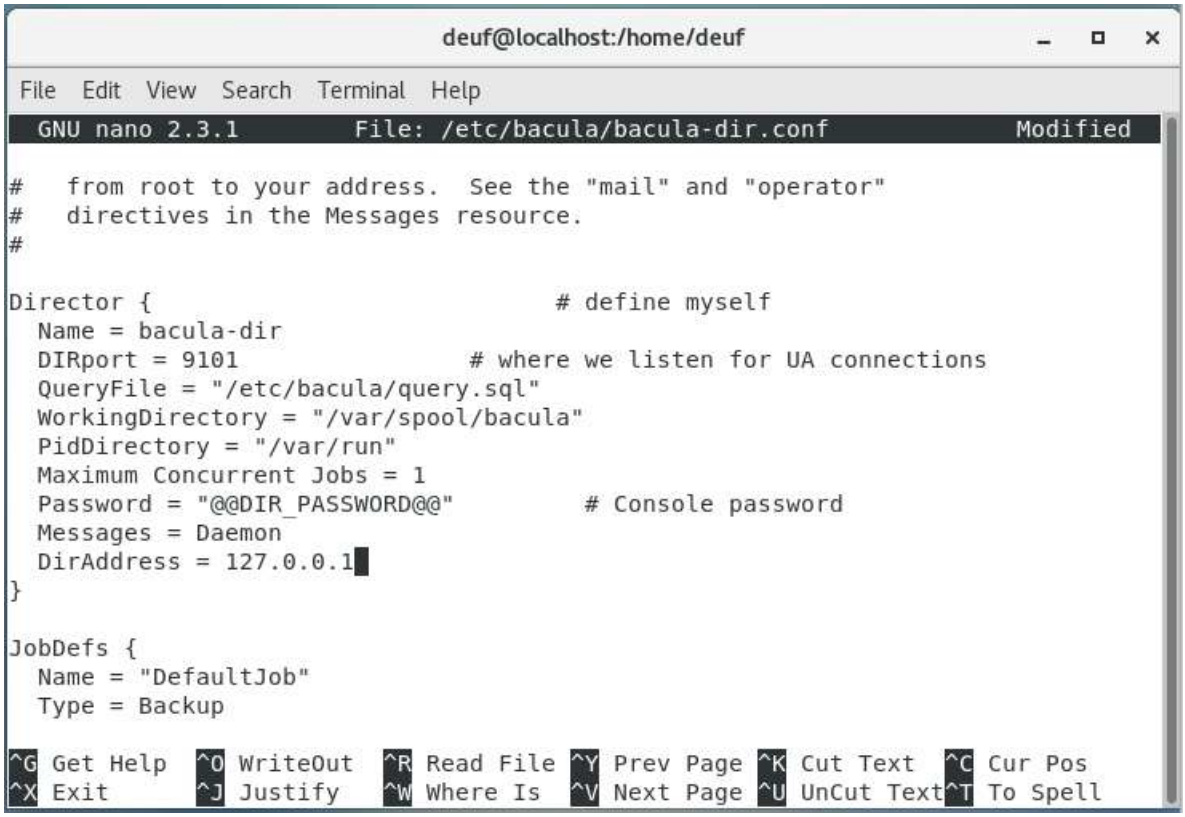


Fuente: Elaboración Propia

Con el archivo abierto se configura el recurso Director para escuchar sobre localhost, añadiendo la línea “DirAddress”:

DirAddress = 127.0.0.1

Figura 22: Configuración recurso Director.



Fuente: Elaboración Propia

Ahora se deben configurar los Jobs locales, Un job en Bacula se utiliza para definir trabajos de copia de seguridad y restauración de archivos, para este caso definimos los trabajos que se usaran para realizar BackUp de ficheros locales. Se genera la búsqueda del recurso “Job” con el nombre de “BackupClient1“, y cambiamos el valor.

Figura 23: Trabajo LocalFile

```
Job {
  Name = "BackupLocalFile"
  JobDefs = "DefaultJob"
}
```

Fuente: Elaboración Propia

Ahora configuramos el recurso “Job” que se llama “RestoreFiles“, y se cambian los valores de “Name” y “Where“:

Figura 24: Trabajo restauración de archivos

```
Job {
  Name = "RestoreLocalFiles"
  Type = Restore
  Client=bacula-fd
  FileSet="Full Set"
  Storage = File
  Pool = Default
  Messages = Standard
  Where = /bacula/restore
}
```

Fuente: Elaboración Propia

Con esto ya tenemos configurado el job "*RestoreLocalFiles*" para restaurar ficheros en /bacula/restore, el directorio que creamos previamente. A partir de dichos trabajos según los requerimientos del CSIR si irán creando los Jobs necesarios tanto a nivel de BackUp como de restauración.

El siguiente paso es configurar los FileSet, en este parámetro se define un conjunto de directorios que deseamos incluir o excluir de la copia de seguridad. Dentro del archivo bacula-dir.conf el parámetro se encuentra inicialmente con el nombre de Full Set, allí se pueden agregar opciones como gzip para comprimir los BackUp.

Para el BackUp de prueba del equipo GNU/Linux se agregó la carpeta raíz y algunas rutas excluidas como se observa en la siguiente imagen.

Figura *25: Configuración FileSet*

```
# List of files to be backed up
FileSet {
  Name = "Full Set"
  Include {
    Options {
      signature = MD5
      compression = GZIP
    }
    File = /
  }
  Exclude {
    File = /var/lib/bacula
    File = /tmp
    File = /proc
    File = /tmp
    File = /.journal
    File = /.fsck
  }
}
```

Fuente: Elaboración Propia

El siguiente paso es definir el Daemon de almacenamiento al que Bacula Director se conectará. Para esto reemplazamos el valor de “Address“, localhost, por la IP del servidor de BackUp, o un nombre FQDN.

Figura 26: Configuración almacenamiento Backup

```
# Definition of file storage device
Storage {
  Name = File
# Do not use "localhost" here
  Address = 192.168.233.130
  SDPort = 9103
  Password = YTExNzJkMGE3YWUzOGZhODUyMTJiMjZhM
  Device = FileStorage
  Media Type = File
  Maximum Concurrent Jobs = 10
}
```

Fuente: Elaboración Propia

También se debe realizar la comunicación con la base de datos para esto localizamos el recurso de Catálogo, llamado MyCatalog y actualizamos el valor de “dbpassword” con el valor de la password que tenga el usuario Bacula de la base de datos.

Figura 27: Configuración recurso Catalogo.

```
Catalog {
  Name = MyCatalog
# Uncomment the following line if you want the dbi driver
# dbdriver = "dbi:postgresql"; dbaddress = 127.0.0.1; dbport =
  dbname = "bacula"; dbuser = "bacula"; dbpassword = "Csirt123%"
}
```

Fuente: Elaboración Propia

Configurar el Pool para el BackUp, un Pool delimita el conjunto de almacenamiento utilizado por Bacula para generar copias de seguridad. Se puede modificar el valor label para identificar correctamente los backups del CSIRT.

Figura 28: Configuración recurso Pool para BackUp

```
# File Pool definition
Pool {
  Name = File
  Pool Type = Backup
  Label Format = Local-
  Recycle = yes                       # Bacula can automatically recycle Volumes
  AutoPrune = yes                     # Prune expired volumes
  Volume Retention = 365 days         # one year
  Maximum Volume Bytes = 50G          # Limit Volume size to something reasonable
  Maximum Volumes = 100               # Limit number of Volumes in Pool
}
```

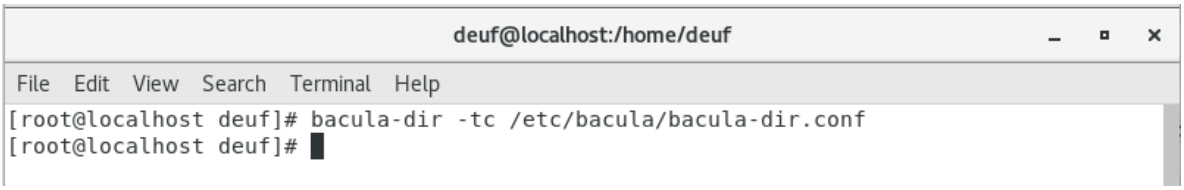
Fuente: Elaboración Propia

Para validar que todas las configuraciones realizadas están correctamente se puede ejecutar el siguiente comando.

 # bacula-dir -tc /etc/bacula/bacula-dir.conf

Si no hay errores no muestra ningún mensaje. Si encuentra errores de configuración, muestra1 un mensaje de advertencia con los errores a corregir.

Figura 29: Verificación archivo bacula-dir.conf

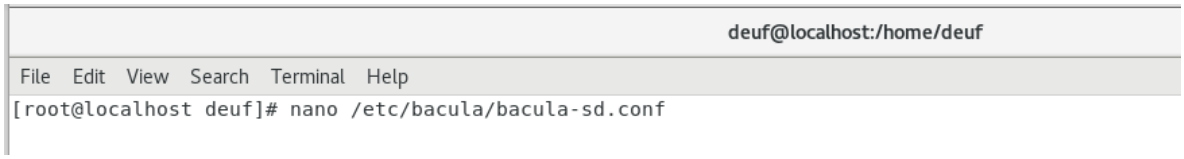


Fuente: Elaboración Propia

Si todo hasta esta sección esta correctamente pasamos a la configuración del servidor de almacenamiento, necesario para indicar a Bacula donde se almacenen las copias de seguridad creadas. Para este procedimiento es necesario abrir y editar el archivo de configuración del Daemon de almacenamiento.

 # nano /etc/bacula/bacula-sd.conf

Figura 30: Apertura archivo bacula-sd.conf



Fuente: Elaboración Propia

Se debe establecer las conexiones donde escuchara el proceso SD (Storage Daemon), para esto añadimos el parámetro "*SDAddress*" , y lo asignamos a la IP del servidor de BackUp o el nombre FQDN.

Figura 31: Configuración IP servidor de Backup

```
Storage {                             # definition of myself
  Name = BackupServer-sd
  SDPort = 9103                  # Director's port
  WorkingDirectory = "/var/lib/bacula"
  Pid Directory = "/var/run"
  Maximum Concurrent Jobs = 20
  SDAddress = 192.168.233.130
}
```

Fuente: Elaboración Propia

También es necesario definir el dispositivo de almacenamiento, lo siguiente es localizar el recurso llamado "*FileStorage*", y actualizar el valor de "*Archive Device*" para que coincida con el directorio de BackUp:

Figura 32: Configuración dispositivos de almacenamiento.

```
Device {
  Name = FileStorage
  Media Type = File
  Archive Device = /bacula/backup
  LabelMedia = yes;                   # lets Bacula label unlabeled media
  Random Access = Yes;
  AutomaticMount = yes;               # when device opened, read it
  RemovableMedia = no;
  AlwaysOpen = no;
}
```

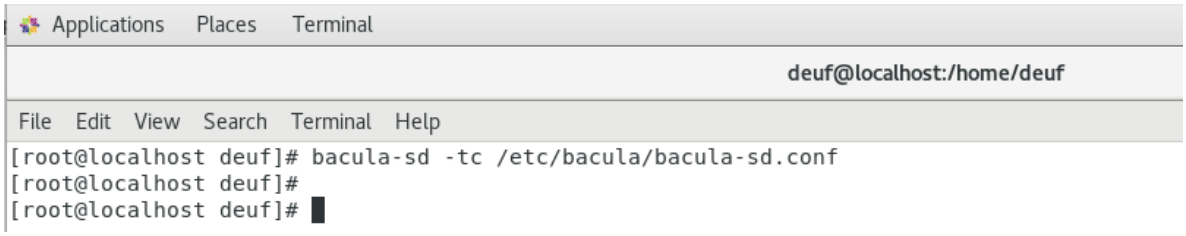
Fuente: Elaboración Propia

Para evidenciar que la configuración realizada esta correcta, se puede comprobar el archivo con la siguiente línea de código.

 # bacula-sd -tc /etc/bacula/bacula-sd.conf

Si todo está bien, no debe mostrar ningún mensaje como la siguiente imagen.

Figura 33: Comprobación archivo bacula-sd.conf

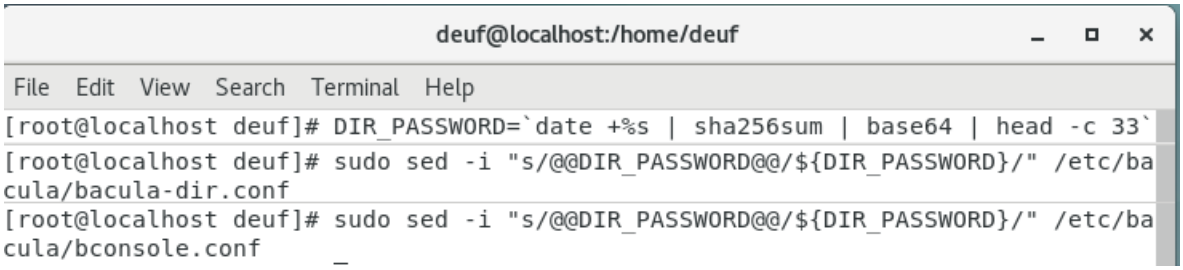


Fuente: Elaboración Propia

Todos los módulos de Bacula, como el Director, FD y SD, usan contraseñas para comunicarse. Es por esto que es necesario configurar dichas contraseñas, este proceso se puede realizar de forma manualmente o generarlos aleatoriamente (estos passwords no necesitamos conocerlos, y no tendremos que introducirlos). Este proceso se ejecuta con los siguientes comandos.

 # DIR_PASSWORD=`date +%s | sha256sum | base64 | head -c 33`
 # sed -i "s/@@DIR_PASSWORD@@/${DIR_PASSWORD}/" /etc/bacula/bacula-dir.conf
 # sed -i "s/@@DIR_PASSWORD@@/${DIR_PASSWORD}/" /etc/bacula/bconsole.conf

Figura 34: Configuración contraseñas bacula-dir



Fuente: Elaboración Propia

También Generar y establecer la contraseña de SD (StorageDaemon / daemon de almacenamiento)

 # SD_PASSWORD=`date +%s | sha256sum | base64 | head -c 33`
 # sed -i "s/@@SD_PASSWORD@@/${SD_PASSWORD}/" /etc/bacula/bacula-sd.conf
 # sed -i "s/@@SD_PASSWORD@@/${SD_PASSWORD}/" /etc/bacula/bacula-dir.conf

Figura 35: Configuracion de contraseñas bacula-sd

Fuente: Elaboración Propia

Ahora se deben establecer las contraseñas para el cliente de Bacula que instalamos en el mismo equipo como prueba, para esto ejecutamos los comandos.

 # FD_PASSWORD=`date +%s | sha256sum | base64 | head -c 33`
 # sed -i "s/@@FD_PASSWORD@@/${FD_PASSWORD}/" /etc/bacula/bacula-dir.conf
 # sed -i "s/@@FD_PASSWORD@@/${FD_PASSWORD}/" /etc/bacula/bacula-fd.conf

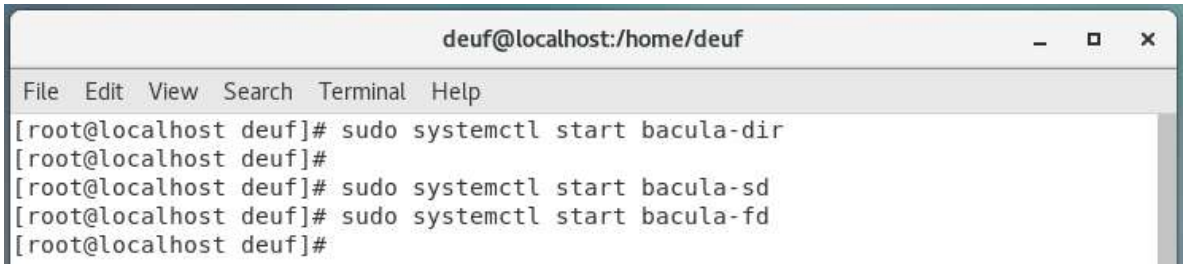
Figura 36: Configuración de contraseñas bacula-fd

Fuente: Elaboración Propia.

Ya con esto se puede iniciar Bacula Director, el Daemon de Almacenamiento (SD), y el daemon de archivos locales (FD).

 # systemctl start bacula-dir
 # systemctl start bacula-sd
 # systemctl start bacula-fd

Figura 37: Inicio de servicios de Bacula

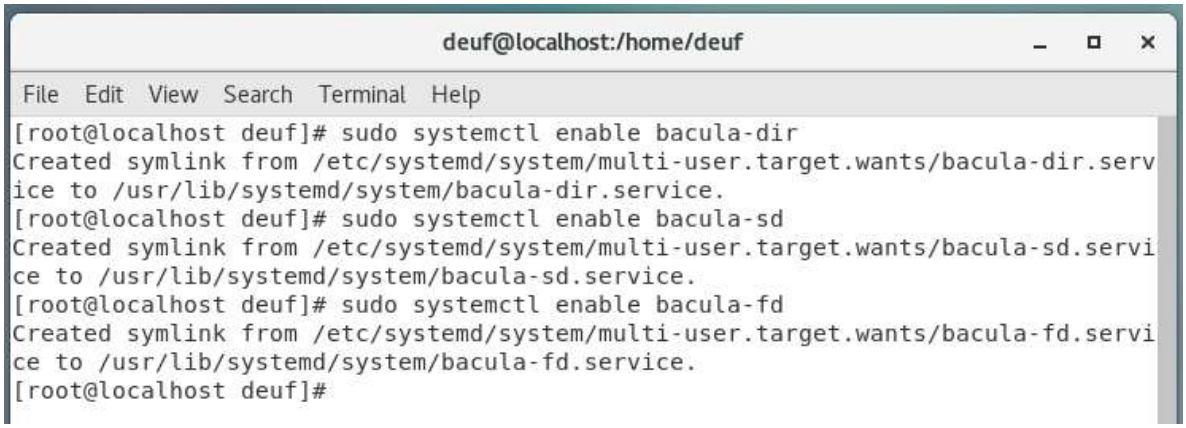


Fuente: Elaboración Propia

Lo recomendable es que estos servicios inicien junto al sistema operativo, para esto se deben ejecutar los siguientes comandos.

 # systemctl enable bacula-dir
 # systemctl enable bacula-sd
 # systemctl enable bacula-fd

Figura 38: Configuración de demonios Bacula.



Fuente: Elaboración Propia

Con esta parametrización el servidor de BackUp estaría funcional para empezar con la configuración de los BackUp

5.6.2 Instalación de Cuckoo Sandbox

Cuckoo es un software de gestión central que se encarga de la ejecución y análisis de muestras de posible malware. Cada análisis se pone es ejecutado en una máquina virtual nueva y aislada del sistema central. La Infraestructura de Cuckoo está compuesto por una máquina host (software de gestión) y un número de máquinas de clientes (máquinas virtuales para el análisis).

Desde su inicio Cuckoo se ha diseñado de forma modular, por ende, es altamente personalizable a la hora de generar integración con diferentes herramientas con el fin de extender sus funcionalidades. Entre los módulos más útiles encontramos Volatility y YARA, que llevan a cabo intensivos y avanzados análisis sobre la memoria del sistema operativo en la máquina virtual. A continuación, se enumeran las características de la conducta de la muestra cargada de malware que Cuckoo Sandbox extrae y genera el análisis:

• Llamadas realizadas a la API del sistema por todos los procesos generados por el malware.
• Volcados de memoria de los procesos generados por el malware.
• Volcados de la memoria completa de las máquinas virtuales.
• Archivos PCAP con el tráfico de red.
• Archivos descargados, creados y/o eliminados por los procesos generados por el malware.
• Capturas de pantalla realizadas durante el análisis.

A continuación, se listan los recursos utilizados a nivel de Hardware en la instalación de prueba de Cuckoo Sandbox, la cantidad de hardware puede varía dependiendo la cantidad de máquinas Guest que utilicemos.

Tabla 3 Recursos utilizados de hardware instalación de prueba Cuckoo Sandbox

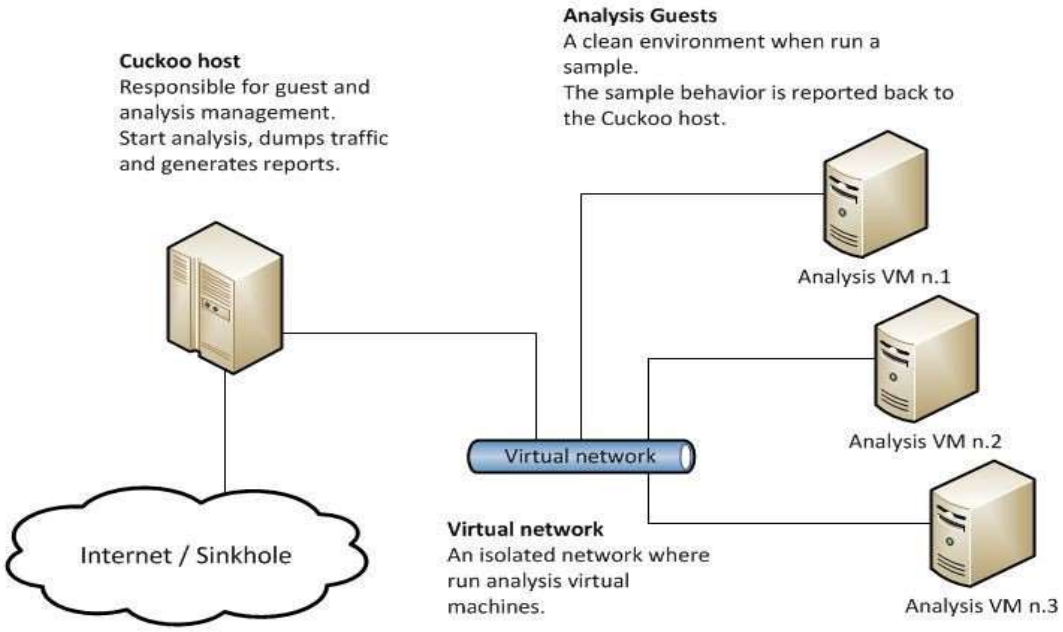
Equipo	Equipo Principal	Equipo Guest
Procesador	4	2
Memoria	6GB	2GB
Disco duro	100 GB	25GB

Fuente: QUEZADA HARO. ONATHAN. Referencia de los equipos virtuales [en linea]. Ecuador. 2017. Disponible en: http://dspace.espoch.edu.ec/bitstream/123456789/6848/1/98T00139.pdf

- **Sistemas operativos de host compatibles:** GNU / Linux (se prefiere Debian / Ubuntu), Mac OS X
- **Software de host requerido:** Python-2.7, Virtualización (VirtualBox, QEMU-KVM, etc.)

- **Sistemas operativos virtualizados compatibles**: Windows XP Service Pack 3, Windows Vista, Windows 7

Figura 39: Arquitectura de red de Cuckoo SandBox.



Fuente: Barcenas G., Alejandro. Análisis de Malware con Cuckoo SandBox [imagen]. Arquitectura de red de Cuckoo SandBox. Disponible en: http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/11118/Tesis%20Alejandro%20B%C3%A1rcenas.pdf?sequence=1

Para la instalación se utilizó una maquina virtualizada en VMware con Ubuntu 16.4 una base de datos postgres, para la virtualización de máquinas Guest se utilizó virtualbox con sistema operativo Windows 7. Como base para el proceso de instalación se utilizó la información suministrada directamente por Cuckoo.[41]

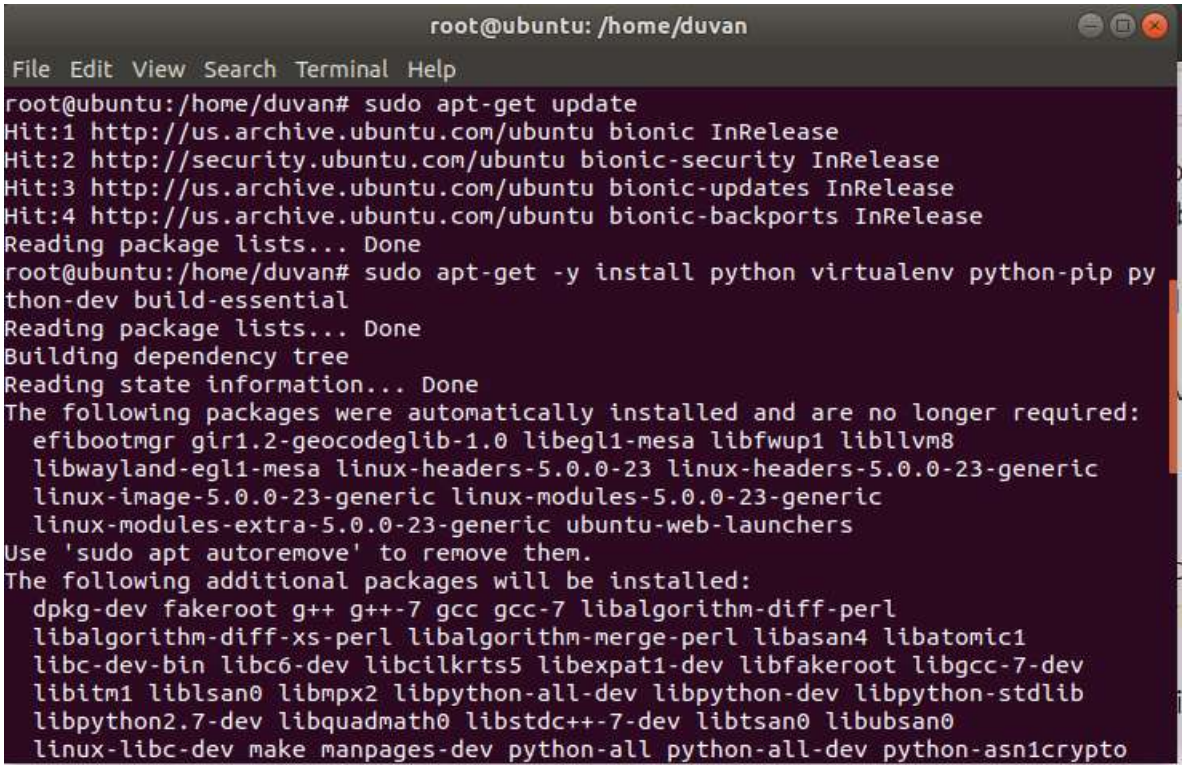
Lo primero a realizar es colocar al día el repositorio de paquetes, instalar virtualenv y garantizar que tenemos instaladas las herramientas principales adecuadas, para esto ejecutamos los siguientes comandos:

 # apt-get update

 # apt-get -y install python virtualenv python-pip python-dev build-essential.

[41] Cuckoo Installation. [en línea]. Septiembre de 2020. Disponible en: https://cuckoo.sh/docs/installation/index.html

Figura 40: Instalación de software requerido.

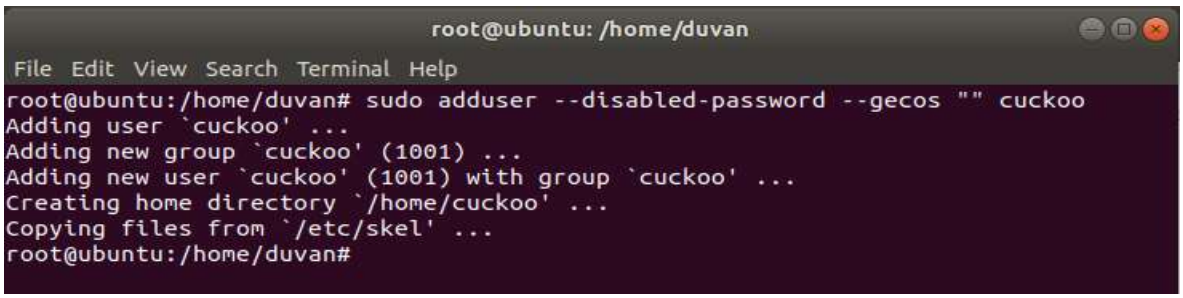


Fuente: Elaboración Propia.

El siguiente paso se debe crear un nuevo usuario para ejecutar Cuckoo. Es necesario ejecutar Cuckoo bajo un usuario separado con el fin de tener una configuración segura, se va a analizar malware; si se encuentra y explota una vulnerabilidad será más difícil comprometer toda la máquina de un usuario que se cree con pocos privilegios:

 # adduser --disabled-password --gecos "" cuckoo

Figura 41: Creación de usuario Cuckoo.



Fuente: Elaboración Propia.

El usuario que se creo debe tener autorización de crear volcados de red durante los análisis de Cuckoo, por lo que le damos permiso para hacerlo:

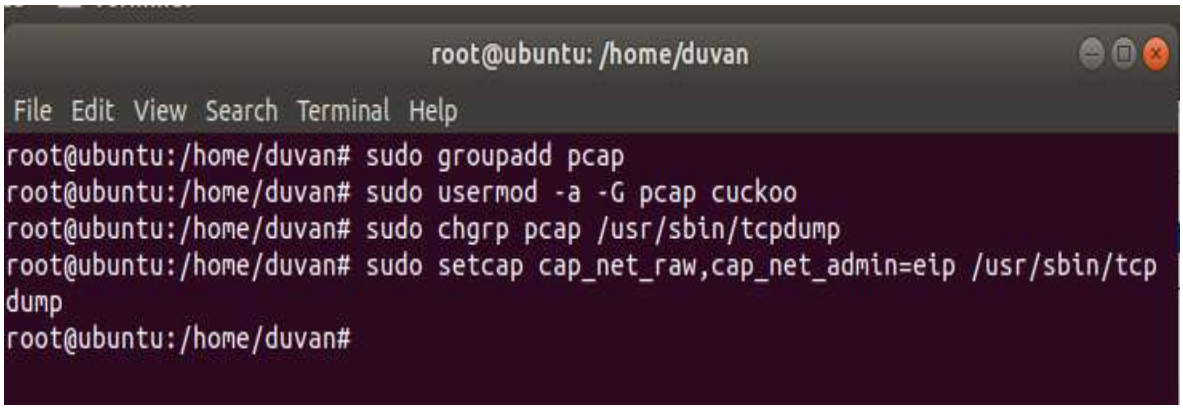
 # groupadd pcap

 # usermod -a -G pcap cuckoo

 # chgrp pcap /usr/sbin/tcpdump

 # setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump

Figura 42: Configuración de permisos usuario Cuckoo.



Fuente: Elaboración Propia.

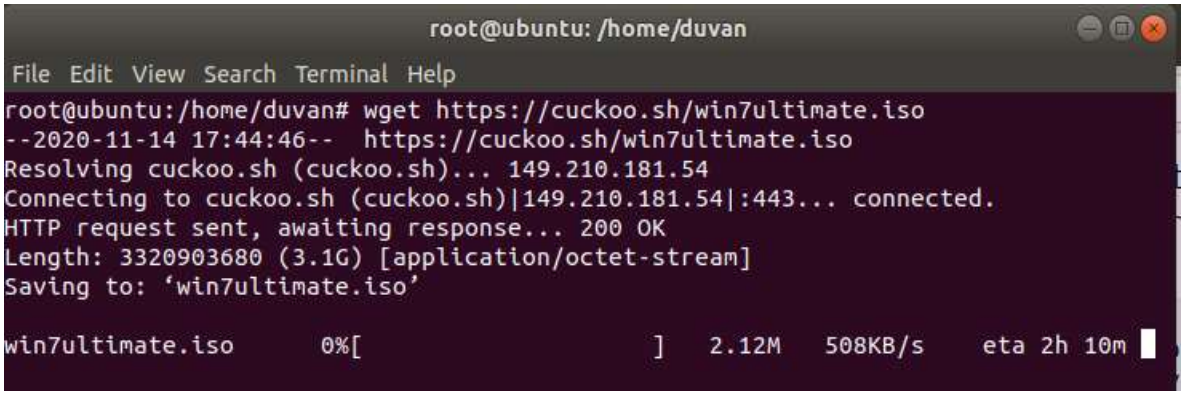
Antes de empezar con la instalación de Cuckoo, es requerido una ISO; para este caso se utilizó Windows 7. Se realiza la descarga del repositorio de Cuckoo.sh. Después de la descarga, tenemos que montar la ISO para utilizarla más adelante:

 # wget https://cuckoo.sh/win7ultimate.iso

 # mkdir /mnt/win7

 # mount -o ro,loop win7ultimate.iso /mnt/win7

Figura 43: Descarga de imagen ISO.

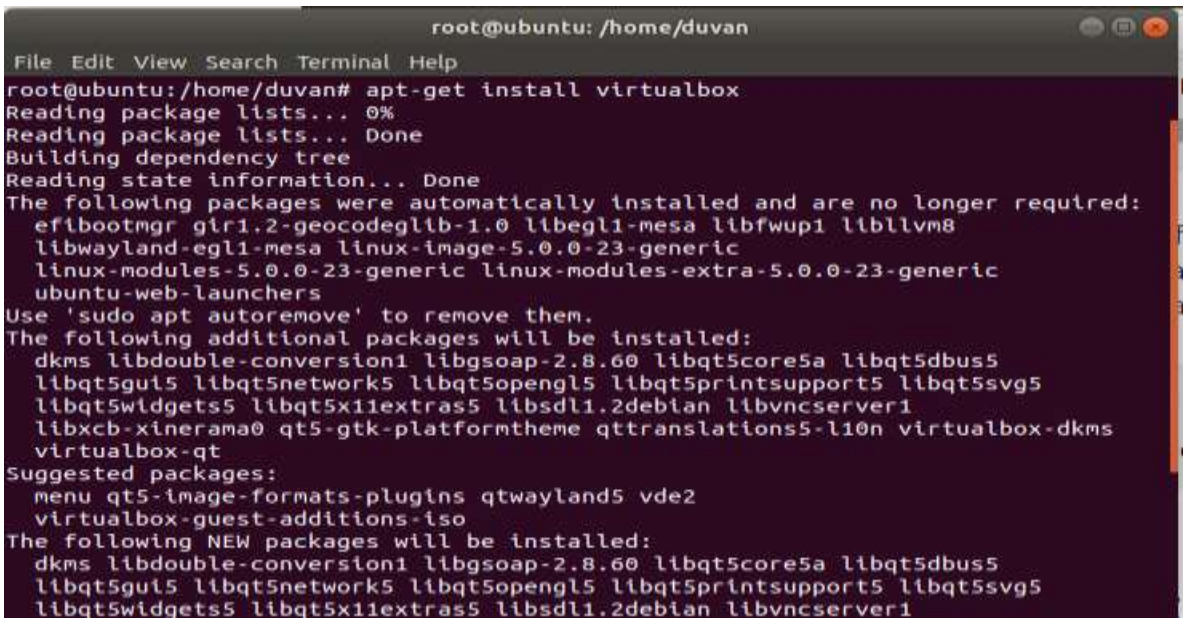


Fuente: Elaboración Propia.

El siguiente paso es instalar un hipervisor, como se explicó anteriormente se utilizará VirtualBox esta descarga se realiza desde el repositorio de VirtualBox, ya que esto nos garantiza una actualización más fácil a versiones recientes. Es de suma importancia instalar actualizaciones para la capa de virtualización, ya que pueden incluir actualizaciones de seguridad. Principalmente para VirtualBox, que ha visto numerosas vulnerabilidades de 0 Day en los últimos años, es importante ejecutar la última versión de VirtualBox 5 o VirtualBox 6 (para este caso se utilizó la versión 5.2).

 # apt-get install virtualbox

Figura 44: Instalación VirtualBox

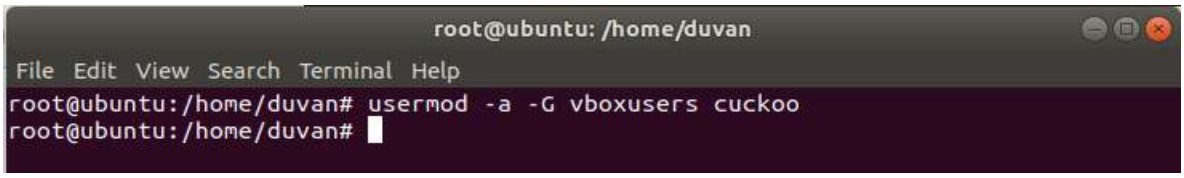


Fuente: Elaboración Propia.

Ahora agregamos el usuario cuco al grupo vboxusers, esto se realiza con el siguiente comando:

 # usermod -a -G vboxusers Cuckoo

Figura 45: Configuración grupo vboxusers

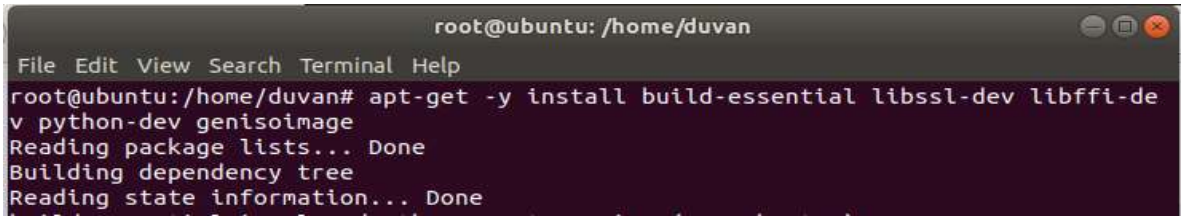


Fuente: Elaboración Propia.

Antes de instalar Cuckoo y VMCloak, es necesario la instalación de varios paquetes. Estas dependencias son requeridas para que VMCloak y Cuckoo funcione correctamente.

 # apt-get -y install build-essential libssl-dev libffi-dev python-dev genisoimage

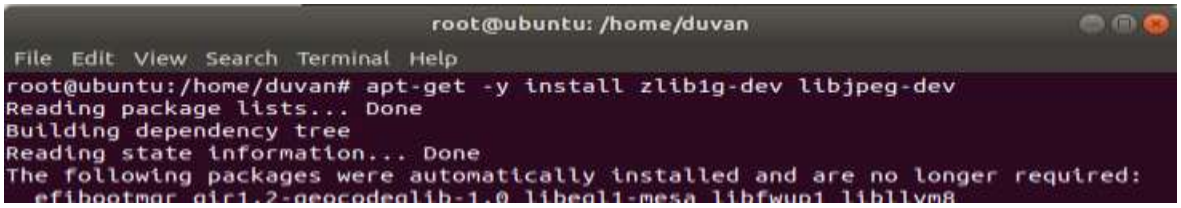
Figura 46: Instalación de dependencias.



Fuente: Elaboración Propia.

 # apt-get -y install zlib1g-dev libjpeg-dev

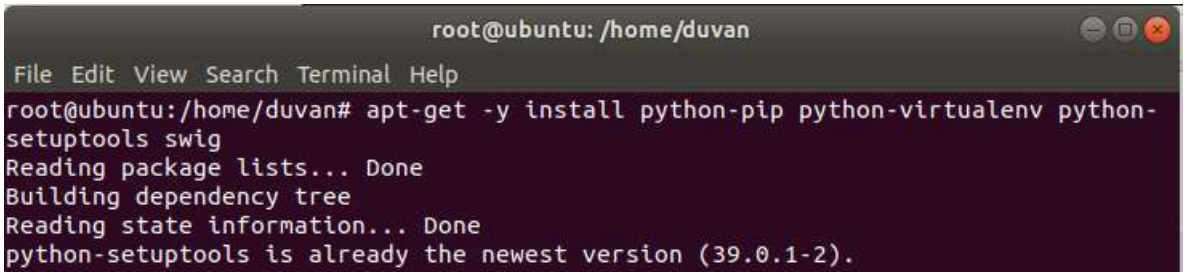
Figura 47: Instalación de dependencias zlib y libjpg



Fuente: Elaboración Propia.

 # apt-get -y install python-pip python-virtualenv python-setuptools swig

Figura 48: Instalación de dependencias Python.



Fuente: Elaboración Propia.

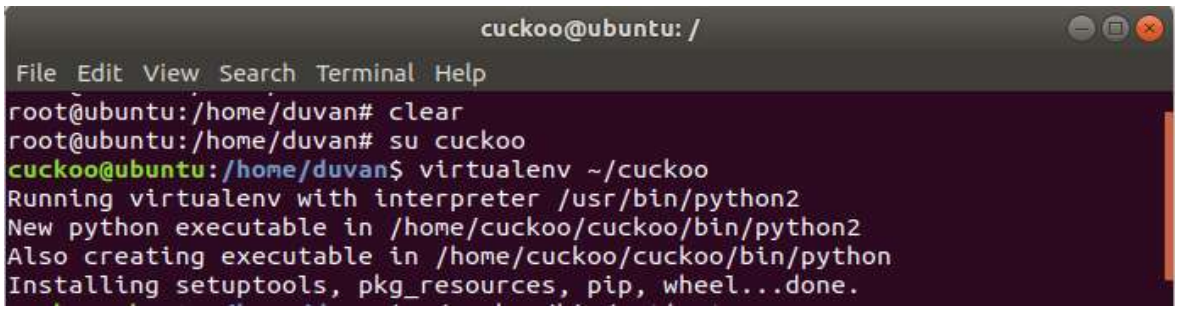
Con las dependencias instaladas, se puede ejecutar la instalación de Cuckoo y VMCloak. Para esto lo primero a realizar es cambiar al usuario cuco y se crea un nuevo virtualenv:

 # su cuckoo

 # virtualenv ~/cuckoo

 # ~/cuckoo/bin/actívate

Figura 49: Acceso usuario cuckoo.



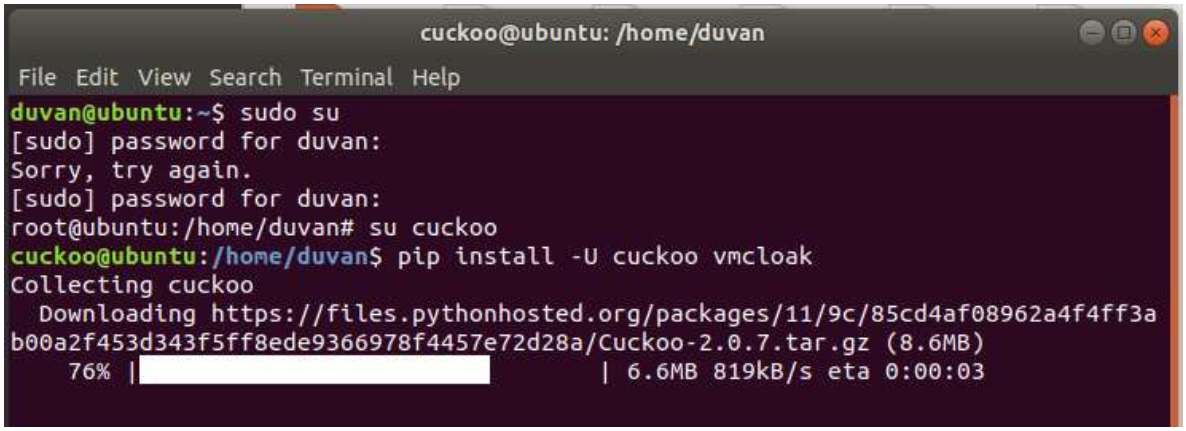
Fuente: Elaboración Propia.

Para poder instalar dependencias dentro del directorio raíz y así evitar interferencias con otros paquetes python instalados globalmente debemos utilizar Virtualenv.

Ahora se genera la instalación de VMCloak y Cuckoo Sandbox en el mismo virtualenv:

 # pip install -U cuckoo vmcloak

Figura 50: Ejecución de instalación Cuckoo



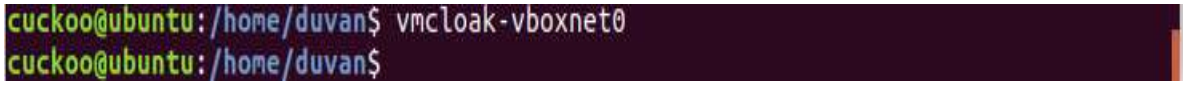
Fuente: Elaboración Propia.

Ahora generaremos la instalación de la imagen ISO que descargamos en el paso anterior para esto vamos a utilizar VMCloak

Lo primero a realizar es definir y crear una instancia de un adaptador de red en VirtualBox Host-Only para que las máquinas virtuales lo utilicen:

 # vmcloak-vboxnet0

Figura 51: Configuración de adaptador vboxnet0

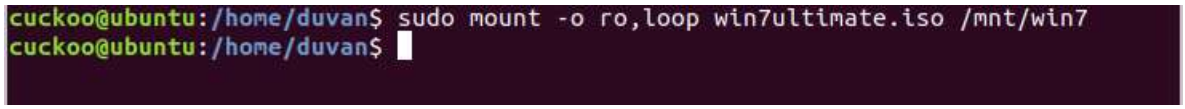


Fuente: Elaboración Propia.

El siguiente paso es montar la imagen ISO en el equipo.

 # mount -o ro,loop win7ultimate.iso /mnt/win7

Figura 52: Montar imagen de windows7

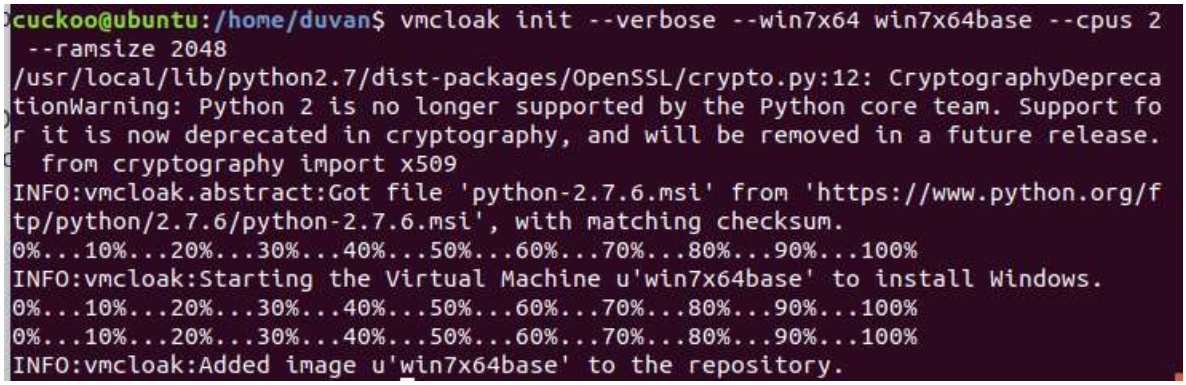


Fuente: Elaboración Propia.

A continuación, se creará la máquina virtual e instalará automáticamente Windows. Este paso tomará aproximadamente de 15 a 20 minutos. Una máquina virtual de análisis Cuckoo debe tener al menos 2 GB de memoria y preferiblemente dos o más núcleos de CPU.

 # vmcloak init --verbose --win7x64 win7x64base --cpus 2 --ramsize 2048

Figura 53: Creación de máquina virtual win7x64.

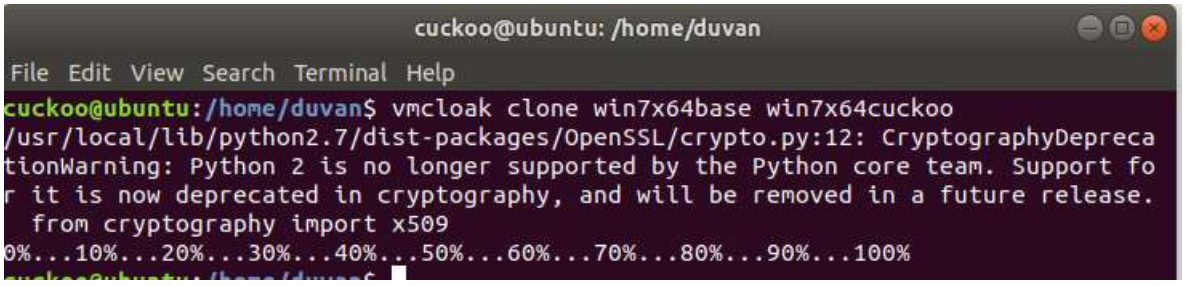


Fuente: Elaboración Propia.

Cuando el VMCloak finalice, se puede empezar a instalar software que debería estar presente en las instantáneas de máquina virtual. Es necesario tenr presente que cuando hemos creado instantáneas de una imagen, ya no se puede cambiar, por lo tanto es necesario clonar la imagen base instalada limpiamente para que se pueda instalar software.

 # vmcloak clone win7x64base win7x64cuckoo

Figura 54: Clonación de maquina win7x64base



Fuente: Elaboración Propia.

VMCloak admite la instalación de diferentes paquetes de software. Se puede enumerar una lista completa de paquetes y versiones compatibles con el siguiente comando.

 # vmcloak list deps

Figura 55: Lista de paquetes vmcloak

```
cuckoo@ubuntu:/home/duvan$ vmcloak list deps
/usr/local/lib/python2.7/dist-packages/OpenSSL/crypto.py:12: CryptographyDepreca
tionWarning: Python 2 is no longer supported by the Python core team. Support fo
r it is now deprecated in cryptography, and will be removed in a future release.
  from cryptography import x509
Name version target sha1 arch
adobe9
  * 9.0.0   None 8faabd08289b9a88023f71136f13fc4bd3290ef0
    9.1.0   None 1e0db06c84d89c8f58b543a41ec35b133de7ea19
    9.2.0   None 4b6207b018cf2be2f49d1f045ff369eb3bee88da
    9.3.0   None 98cacd6069e78a0dd1ef87ce24e59716fecf8aa0
    9.3.3   None b1ed1d350db97ddd562606449804e705d4ffe1c7
    9.3.4   None e3bb8eff9d199ab1f4b5f7a10e514a74e0384ca0
    9.4.0   None 4652a454056b2323097a6357292db3af239bb610
    9.5.0   None e46000691a6dbcd7892078b46c8ee13613683545
    10.1.4  None fe6808d5d11e94dc5581f33ed386ce552f0c84d6
    11.0.0  None e7dd04e037c40b160a2f01db438dba9ea0b12c52
    11.0.2  None e1d9e57f08e169fb1c925f8ded93e5f5efe5cda3
    11.0.3  None 9c2b6903b000ecf2869e1555bc6e1b287e6176bf
    11.0.4  None 9c295c16d374735bf292ef6c630c9ab392c22500
    11.0.6  None 6a3d5b494b4ed6e11fc7d917afc03eaf05d4a6aa
    11.0.7  None 3e08c3f6daad59f463227590cc438b3906648f5e
    11.0.8  None 3e889258ea2000337bbe180d81317d44f617a292
    11.0.9  None 53b367bff07a63ee07cf1cd090360b75d3fc6bfb
    11.0.10 None 98b2b838e6c4663fefdfd341dfdc596b1eff355c
```

Fuente: Elaboración Propia.

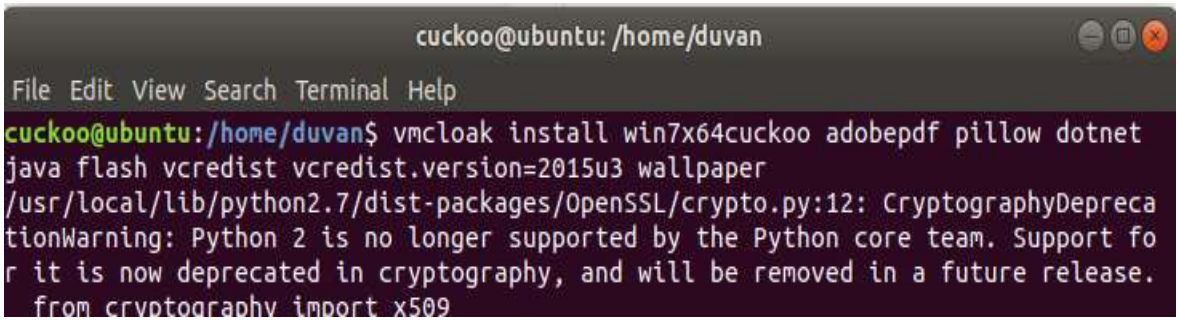
Se realizar la instalación de un paquete de software con la siguiente sintaxis:

vmcloak install <image name> <package>package.version=Xpackage.serialkey=X

Tambien se puede proporcionar una versión específica o una clave de serie añadiendo: o . Si no se selecciona ninguna versión, se seleccionará la versión predeterminada. Vamos a instalar algunos paquetes de software básicos:

 # vmcloak install win7x64cuckoo adobepdf pillow dotnet java flash vcredist vcredist.version=2015u3 wallpaper

Figura 56: Instalación de software en máquina virtual



Fuente: Elaboración Propia.

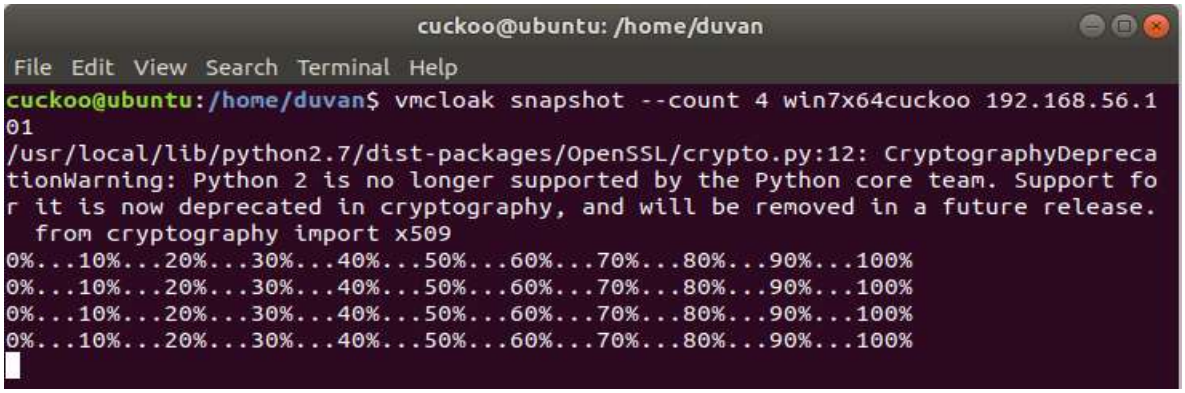
Luego de terminar con la instalación de los paquetes de software, se pueden crear las instantáneas de máquina virtual. VMCloak registrará una máquina virtual VirtualBox para cada instantánea creada. Después de la creación de instantáneas, ya no es posible cambiar la imagen. La sintaxis del comando snapshot es:

vmcloak snapshot <options> <image name> <vmname> <ip to use>

Utilizando el parámetro --count podemos crear varias instantáneas a la vez.

 # vmcloak snapshot --count 4 win7x64cuckoo 192.168.56.101

Figura 57: Snapshot de máquina virtual win7x64cuckoo



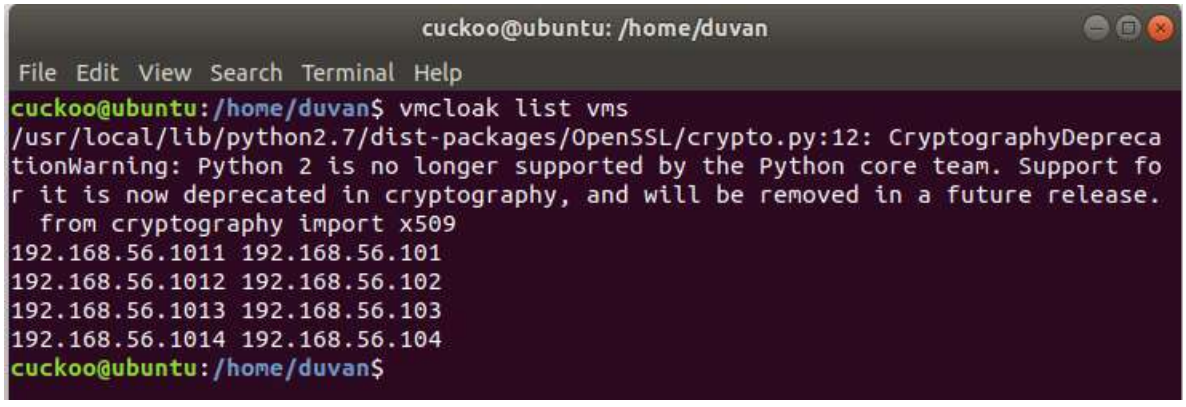
Fuente: Elaboración Propia.

El comando anterior creará máquinas virtuales con direcciones IP. win7x64cuckoo1-4192.168.56.101-104

Una vez finalizada la clonación, es posible listar las máquinas virtuales.

 # vmcloak list vms

Figura 58: Lista de máquinas virtuales.

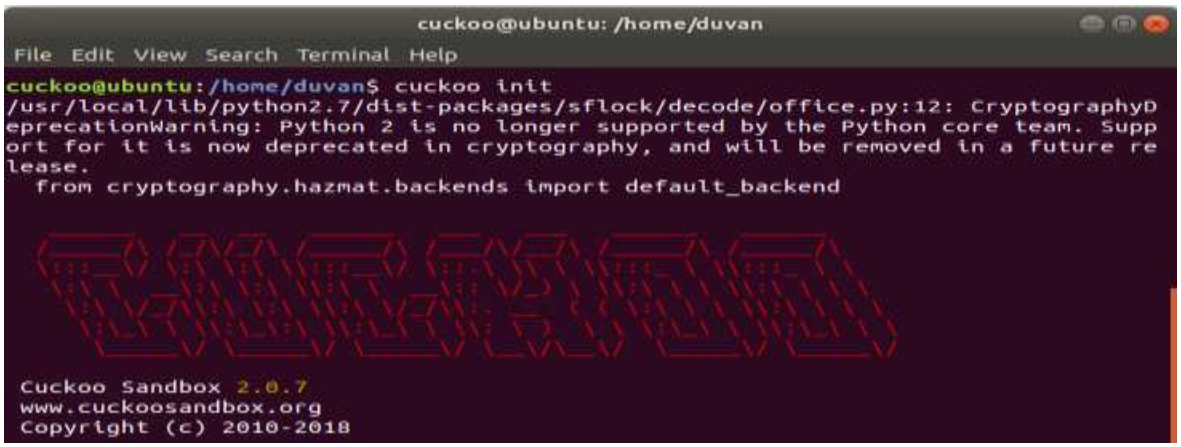


Fuente: Elaboración Propia.

Cuckoo sube los archivos de configuración, firmas y otros archivos que pueden ser cambiados por el usuario desde su directorio de trabajo de Cuckoo (CWD). Antes de que se empiece a utilizar Cuckoo, primero es necesario crear el directorio: USERHOME/.cuckoo , para esto ejecutamos los siguientes comandos

 # cuckoo init

Figura 59: Creación de directorio userhome/.cuckoo

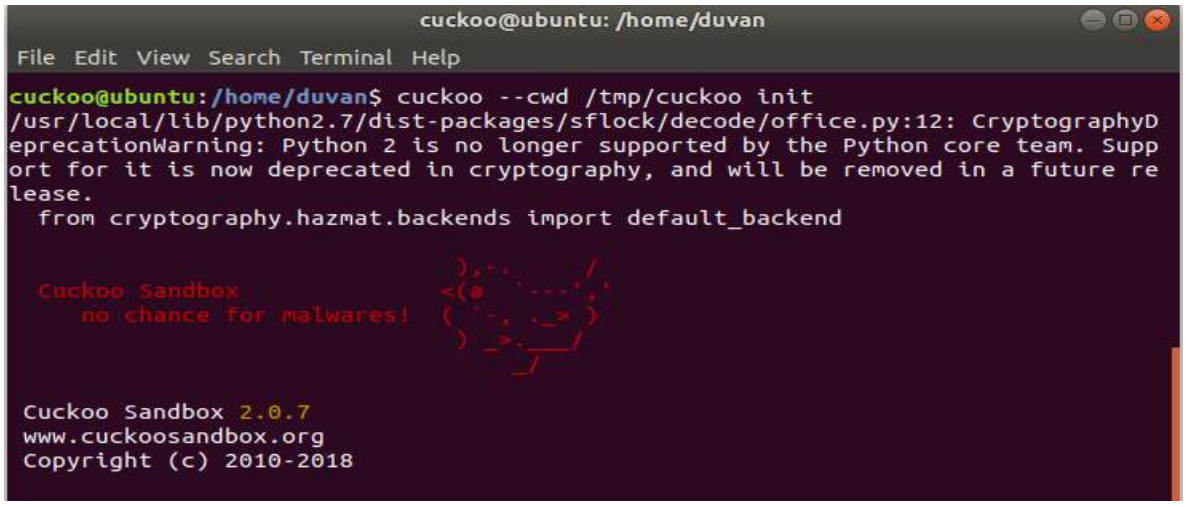


Fuente: Elaboración Propia.

Se puede generar el CWD personalizado, la ruta debe utilizarse al crearlo y debe proporcionarse con el comando Cuckoo, por ejemplo: --cwd <path>

 # cuckoo --cwd /tmp/cuckoo init

Figura 60: Ruta personalizada cwd.



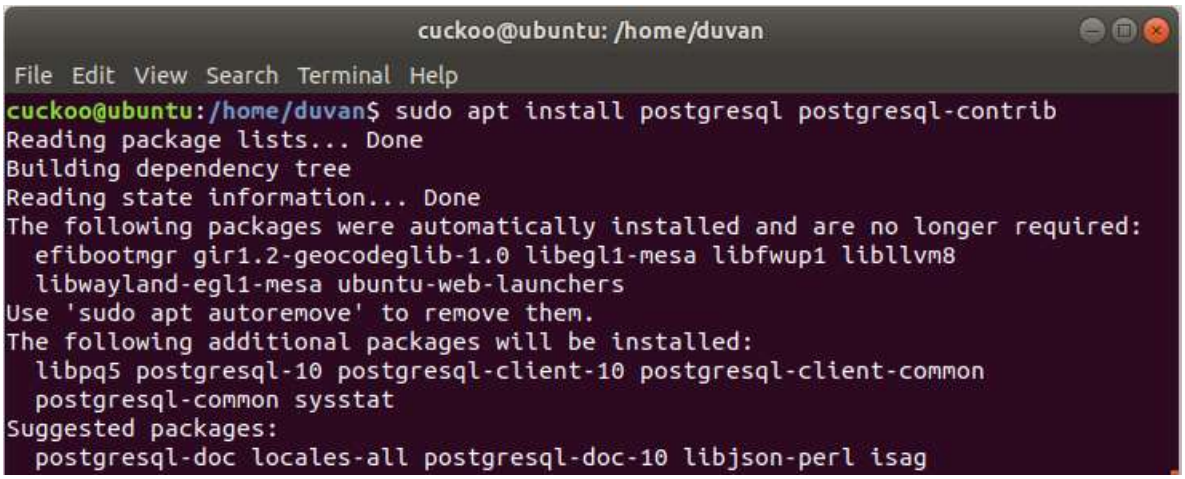
Fuente: Elaboración Propia.

Ahora se utilizará Postgres como DBMS. Este paso se puede omitir si no está utilizando más de un par de máquinas virtuales de análisis y no usará instancias de procesamiento de Cuckoo.

Lo primero es instalar Postgres. Para esto se debe ejecutar el siguiente comando:

 # apt install postgresql postgresql-contrib

Figura 61: instalación de motor de BD Postgresql.

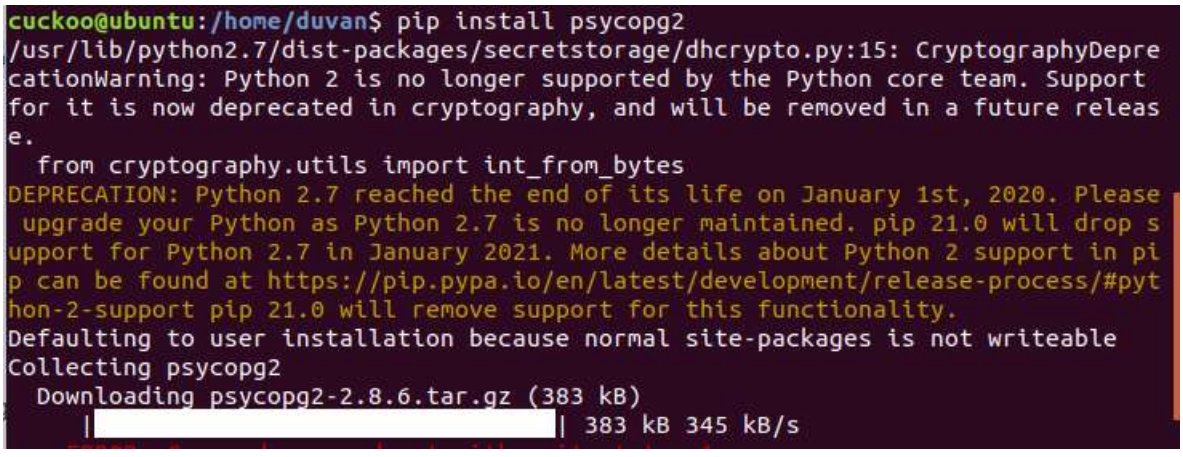


Fuente: Elaboración Propia.

Ahora se genera la instalación del controlador de base de datos Postgres para Cuckoo:

 # pip install psycopg2

Figura 62: Instalación de psycopg2.



Fuente: Elaboración Propia.

El siguiente paso es crear un usuario y una base de datos para que Cuckoo utilice:

 # -u postgres psql

>CREATE DATABASE cuckoo;

>CREATE USER cuckoo WITH ENCRYPTED PASSWORD 'password';

>GRANT ALL PRIVILEGES ON DATABASE cuckoo TO cuckoo;

>\q

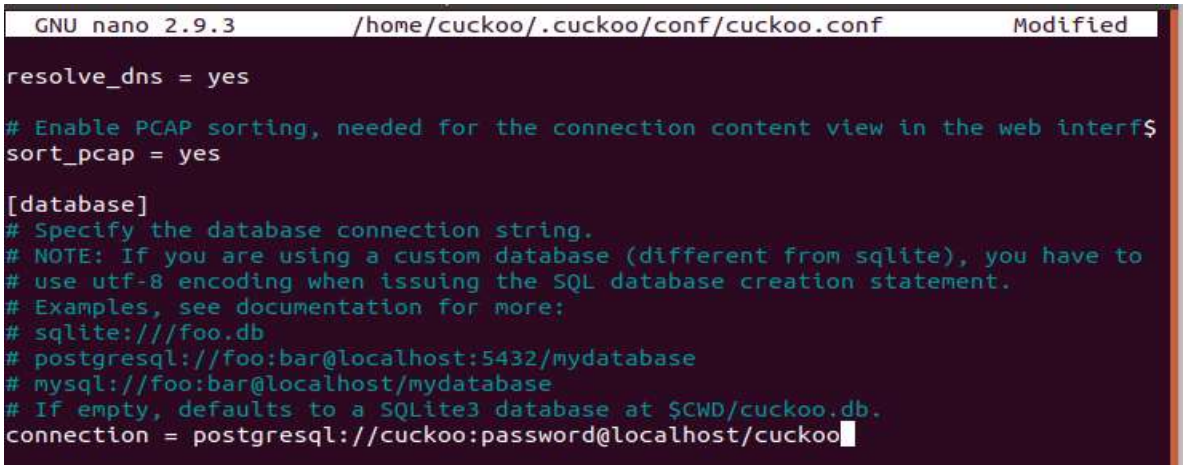
Figura 63: Creación de base de datos postgres.

Fuente: Elaboración Propia.

Después de eso, es necesario decirle a Cuckoo que utilice Postgres en lugar de SQLite. Abra el archivo CWD/conf/cuckoo.conf y busque la sección [database]connection =

connection = postgresql://cuckoo:password@localhost/cuckoo

Figura 64: Configuración de conexión Postgressql



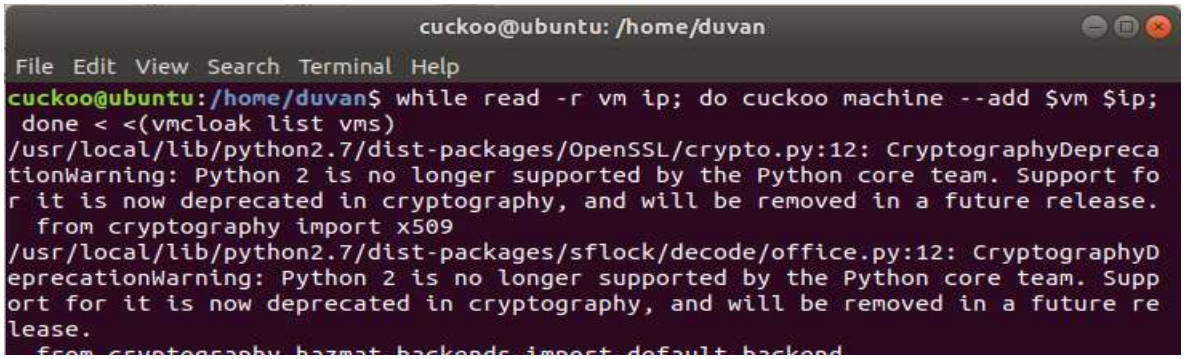
Fuente: Elaboración Propia.

Continuando con el proceso, se deben agregar las máquinas virtuales creadas a Cuckoo. Para ello es necesario decirle a Cuckoo que agregue la máquina a su configuración. Esto tiene que hacerse para cada máquina, para facilitar este proceso podemos ejecutar el siguiente formato de comando:

cuckoo machine --add <vm name> <ip>vmcloak list vms

 # while read -r vm ip; do cuckoo machine --add $vm $ip; done < <(vmcloak list vms)

Figura 65: Agregar máquinas virtuales a Cuckoo

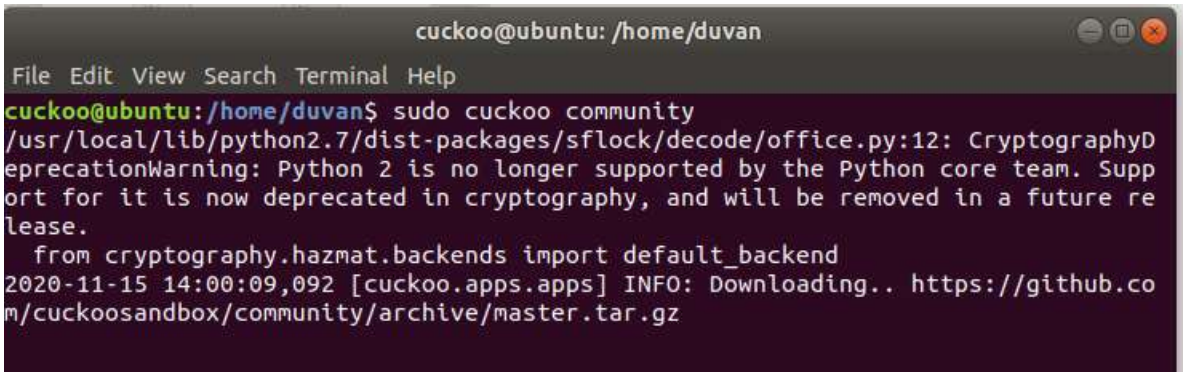


Fuente: Elaboración Propia.

Para instalar las firmas Cuckoo más reciente, ejecutamos el siguiente comando:

 # cuckoo community

Figura 66: Instalar firmas más recientes de Cuckoo.



Fuente: Elaboración Propia.

A continuación, se debe proporcionar a las máquinas virtuales conexión a Internet.

El acceso a internet en las máquinas virtuales no es del todo necesario, sin embargo, no tener una conexión a Internet restringe el análisis de malware y recuperar datos tales cargas útiles e instrucciones. Esto puede afectar a la precisión de los resultados del análisis.

Lo primero que se tiene que realizar es cambiar a una cuenta que tenga privilegios de root y habilite el reenvío. Haga esto para la interfaz de entrada y salida.

 # sysctl -w net.ipv4.conf.vboxnet0.forwarding=1

 # sysctl -w net.ipv4.conf.ens33.forwarding=1

Figura 67: Permiso de acceso a las interfaces de red

Fuente: Elaboración Propia.

El siguiente paso es habilitar el enrutamiento global para las máquinas virtuales conectadas a la *interfaz* vboxnet0, este proceso se realiza con el siguiente comando:

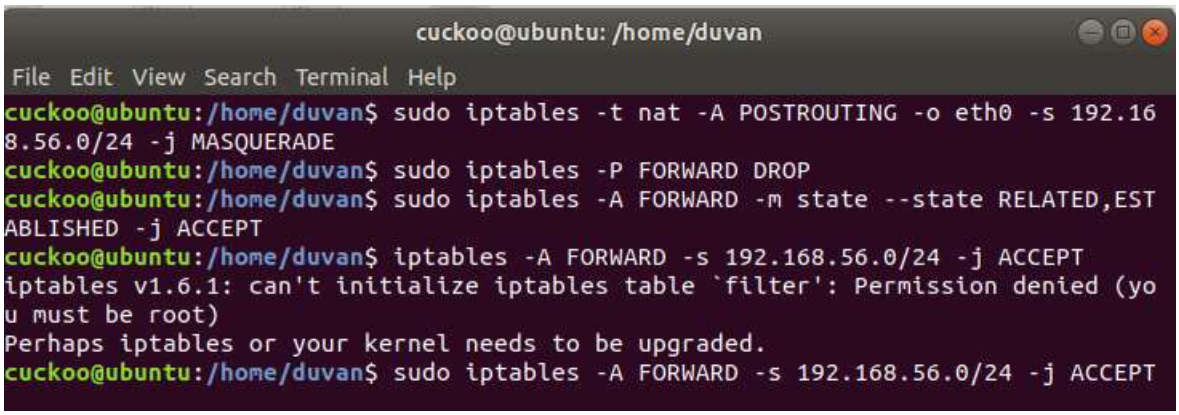
 # iptables -t nat -A POSTROUTING -o eth0 -s 192.168.56.0/24 -j MASQUERADE

 # iptables -P FORWARD DROP

 # iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT

 # iptables -A FORWARD -s 192.168.56.0/24 -j ACCEPT

Figura 68: Reglas de firewall para Cuckoo



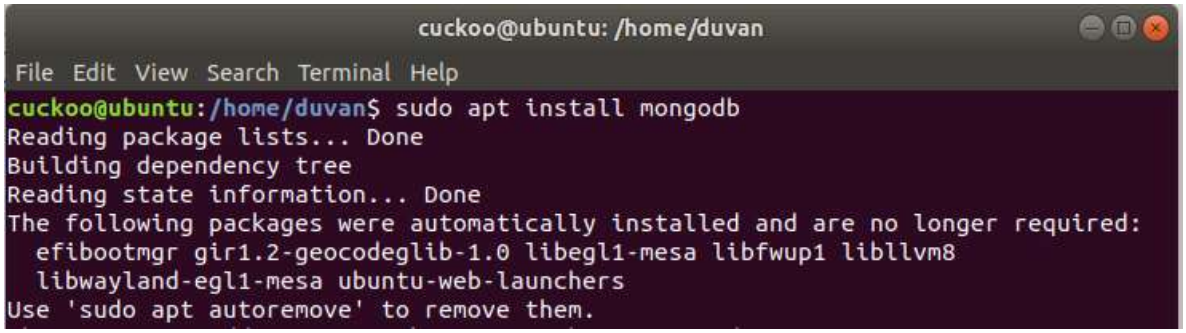
Fuente: Elaboración Propia.

Con los pasos anteriores si todo salió correctamente se tiene Cuckoo instalado y configurado, Ahora se generará la instalación de la interfaz web de Cuckoo, esta se puede utilizar para enviar nuevas tareas y ver los resultados del análisis. Para esto se requiere que MongoDB esté instalado y habilitado en el archivo .reporting.conf

Para la instalación de MongoDb se debe ejecutar el siguiente comando:

 # apt install mongodb

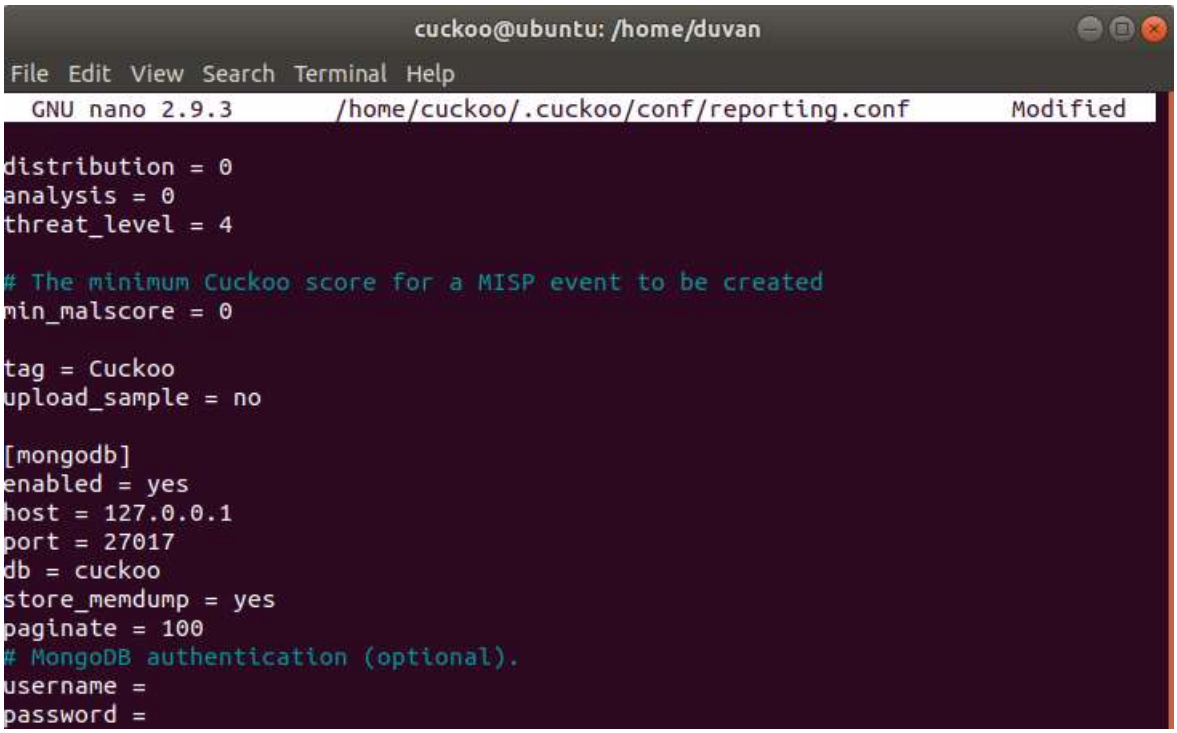
Figura 69: Instalación de motor BD MongoDB



Fuente: Elaboración Propia.

Ahora se debe generar la activación en el archivo reporting.conf de Mongo debe para esto se debe abrir dicho archivo y buscar la sesión de [MongoDB]enabled = noenabled y cambiarla por [MongoDB]enabled = yes

Figura 70: Habilitar base de datos MongoDB

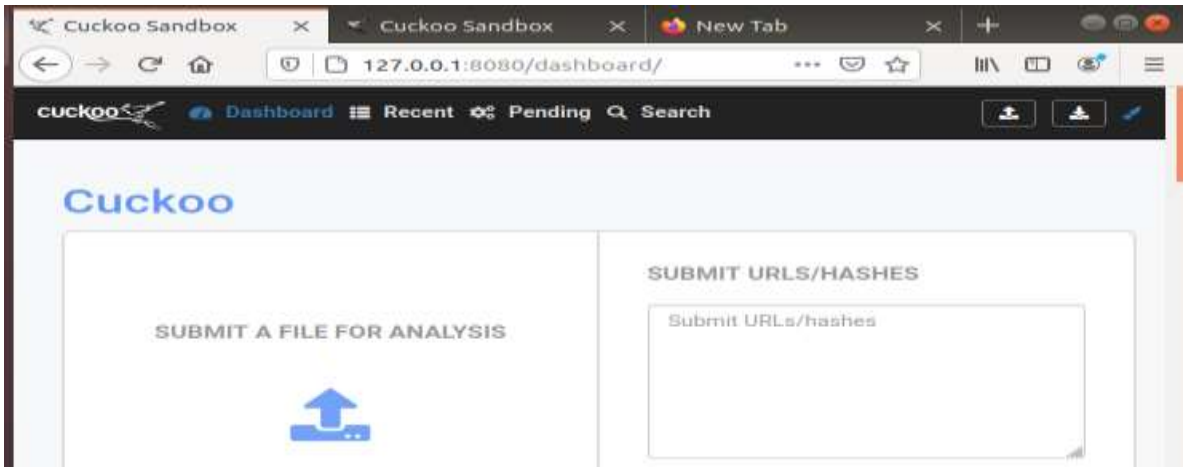


Fuente: Elaboración Propia.

Para la instancia Web se puede ejecutar por medio del el servidor web integrado. Este servidor se puede iniciar ejecutando:

 # cuckoo web --host 127.0.0.1 --port 8080

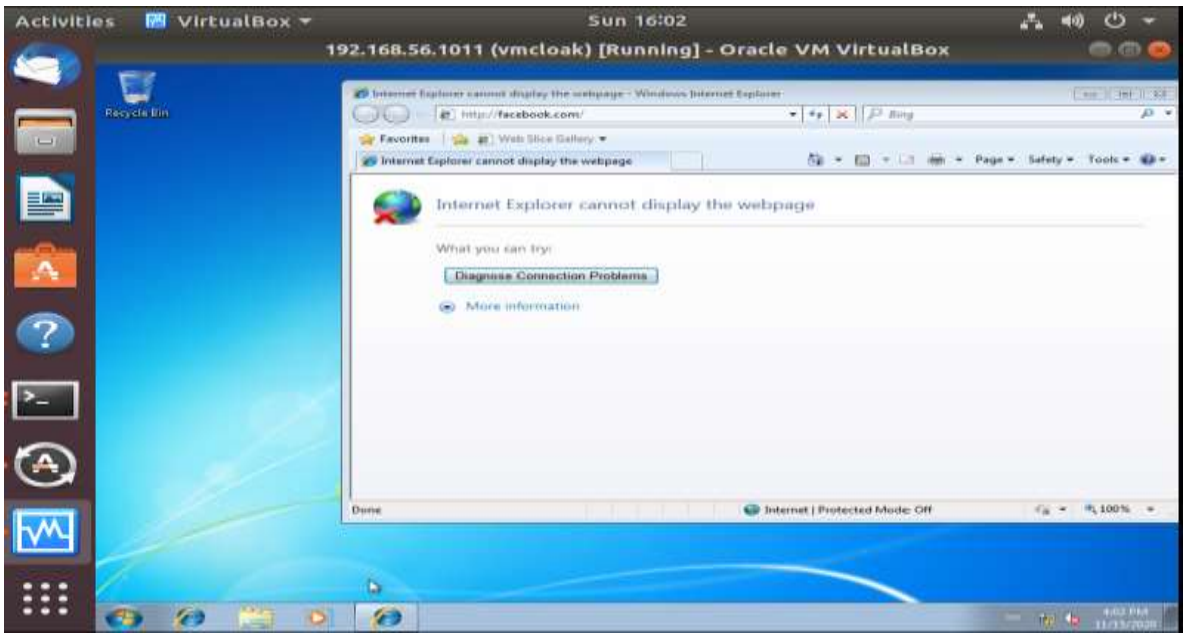
Figura 71: Interfaz WEB Cuckoo.



Fuente: Elaboración Propia.

Ahora podemos enviar tareas y ver los resultados en la interfaz web. Cuckoo debe estar funcionando para que los análisis comiencen, de lo contrario las tareas permanecerán en el estado pendiente.

Figura 72: Máquina virtual Windows7



Fuente: Elaboración Propia.

5.7 AlienVault SIEM (OSSIM)

OSSIM es una plataforma unificada que provee las capacidades de seguridad esenciales. Muchos softwares de seguridad de código abierto probados están integrados en la plataforma OSSIM. Sigue siendo la forma más rápida de dar los primeros pasos hacia la visibilidad de seguridad unificada de los sistemas en una organización[42].

La plataforma OSSIM admite los siguientes softwares/plugins de código abierto como lo son:

Snort: es el más importante IDS Open Source disponible en la actualidad. OSSIM contiene una versión personalizada de esta herramienta y es quien alerta sobre intentos de ataques a la red.

OpenVAS: es la versión GPL (General Public License) de Nessus, una popular herramienta de escaneo de vulnerabilidades Open Source. Esta herramienta se utiliza para proporcionar búsqueda de vulnerabilidades de los recursos de red y añade esta valiosa información a la base de datos de OSSIM.

Ntop: es una popular herramienta Open Source para la monitorización del tráfico de la red. Esta herramienta proporciona información muy valiosa sobre el tráfico en la red, que puede ser utilizada para detectar de una manera proactiva el tráfico anormal o malicioso

Nagios: es una popular herramienta Open Source de monitoreo de dispositivos de red. Es una de las herramientas más complejas, pero le permite al administrador tener una única visión del estado de los hosts de la red. A través del monitoreo de hosts, Nagios puede enviar alertas en caso de fallas y posee una interface web desde donde se puede observar el estado de la red.

PADS: El Sistema de Detección Pasiva de Activos (PADS por sus siglas en inglés) es una herramienta única. La herramienta supervisa silenciosamente el tráfico de red, los registros del host y las actividades de servicio, con el objetivo de detectar anomalías sin generar tráfico de red, realizando un inventario de activos y revisando los servicios que cada cual ejecuta.

P0f: La herramienta P0f toma pasivamente las huellas dactilares del sistema operativo (el descubrimiento del tipo de sistema operativo y su versión). Esta herramienta escucha silenciosamente el tráfico de red e identifica los sistemas

[42] AT&T CYBERSECURITY. USM Appliance. Deployment Guide. [en línea]. Octubre de 2020. Disponible en: https://cybersecurity.att.com/documentation/resources/pdf/usm-appliance-deployment-guide.pdf

operativos que se comunican en la red. Esta información resulta útil en el proceso de correlación.

OCS-NG: La OCS-NG (Open Computer and Software Inventory Next Generation) ofrece la capacidad multi-plataforma de gestión de recursos. Esta herramienta permite mantener un inventario actualizado en tiempo real de los dispositivos existentes en la red.

Para una instalación de AlienVault OSSIM, los requisitos de hardware dependen de la cantidad de sensores y la cantidad de registros que se quieren procesar. Los requisitos mínimos del sistema son los siguientes

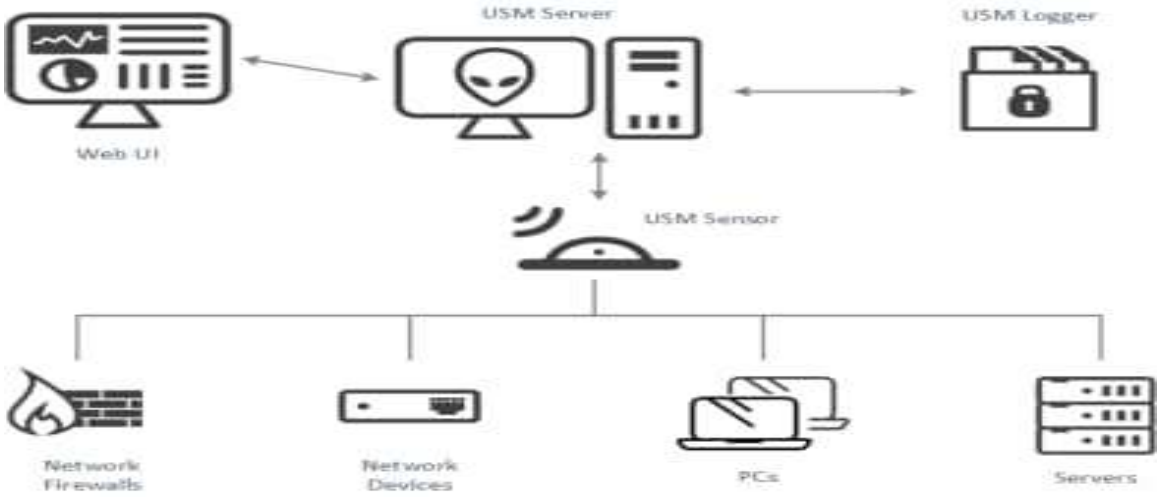
Tabla 4 Requisitos mínimos del sistema de hardware

RAM	4-8 GB
Procesadores	2 núcleos
Disco Duro	250 GB

Fuente: TORRES MANRIQUE, Marcofi. Requerimientos de Hardware OSSIM [en linea]. INTEGRACIÓN DE OSSIM Y UNTANGLE. Colombia. 2010. Disponible en: https://repository.icesi.edu.co/biblioteca_digital/bitstream/10906/76599/1/torres_integracion_ossim_2011.pdf.

A continuación, se muestra la arquitectura con la que trabaja OSSIM, esta arquitectura es muy similar a las arquitecturas de un SIEM tradicional.

Figura 73: System Architecture and Components



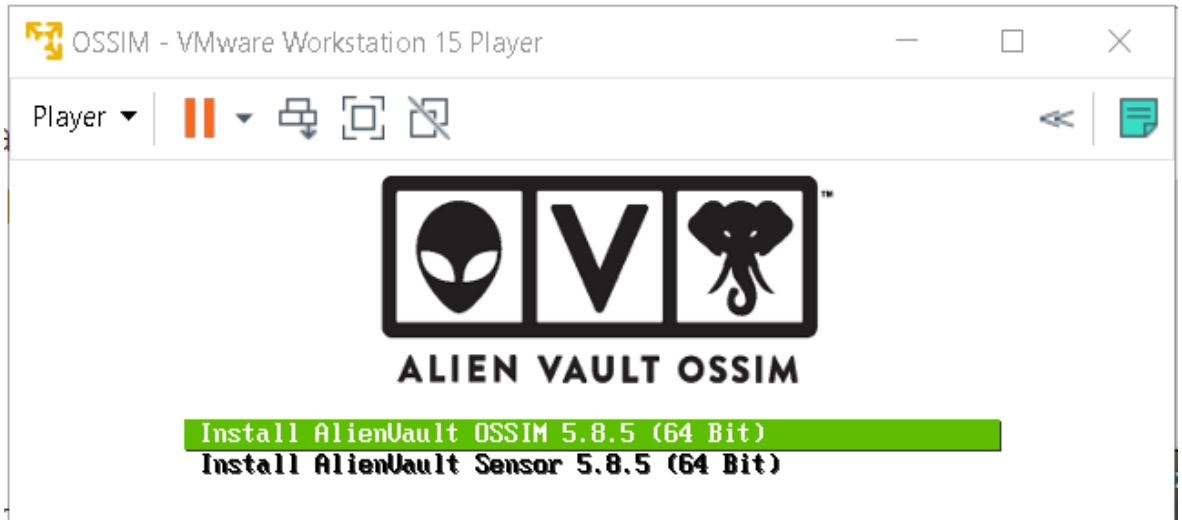
Fuente: AlienVault OSSIM. About USM Appliance System Architecture and Components. System Architecture and Components. Disponible en: https://cybersecurity.att.com/documentation/usm-appliance/system-overview/about-usm-architecture-components.htm

Lo primero que se debe realizar para las instalación de OSSIM es descargar la iso para esto se debe ir a la pagina https://dlcdn.alienvault.com/AlienVault_OSSIM_64bits.iso. Para este caso instalamos OSSIM en la máquina virtual de VMwarew en lugar de un servidor físico con las siguientes especificaciones:

Procesador: 2 VCPU, RAM: 4 GB , Tamaño del disco duro: 80GB , IP de Gestión : 192.168.233.10/24 y Red de Activos : 192.168.0.0/24

Cuando OSSIM arranque con la imagen iso, se muestran dos opciones en el asistente de instalación como se observa en la siguiente imagen:

Figura 74: Ventana de inicio OSSIM

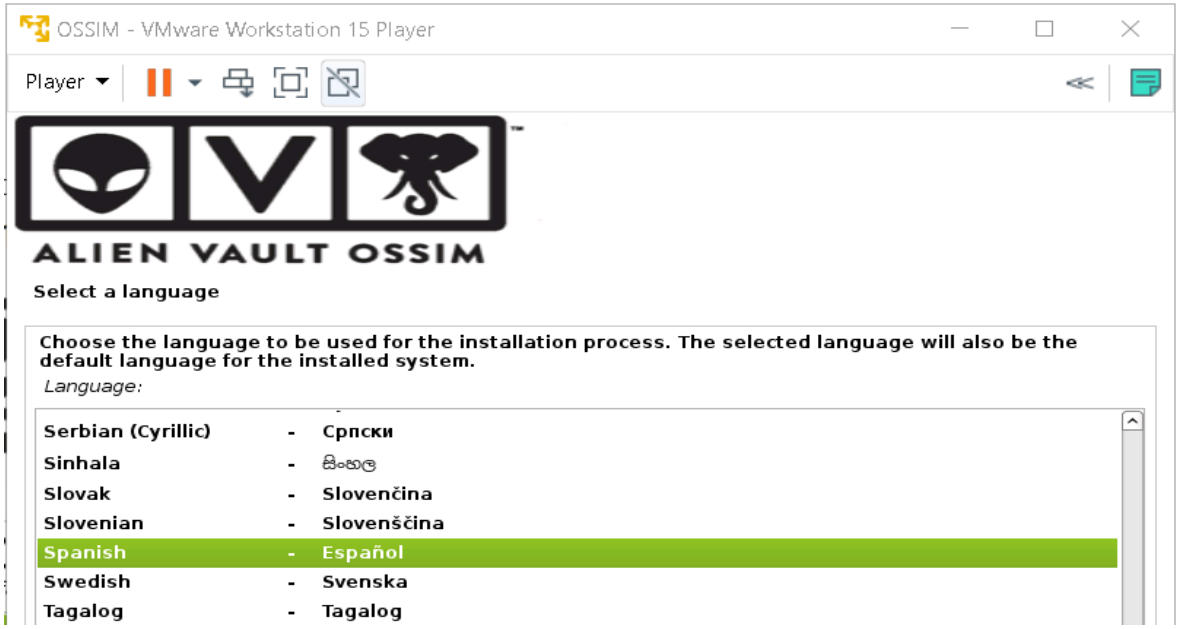


Fuente: Elaboración Propia.

Se debe seleccionar la opción resaltada en verde como se observa en la figura anterior, esta opción instalará OSSIM en la máquina virtual, al pulsar enter se inicia el proceso de instalación.

El siguiente paso es seleccione el idioma con el que queremos que se instale OSSIM

Figura 75 Selección de Idioma OSSIM



Fuente: Elaboración Propia.

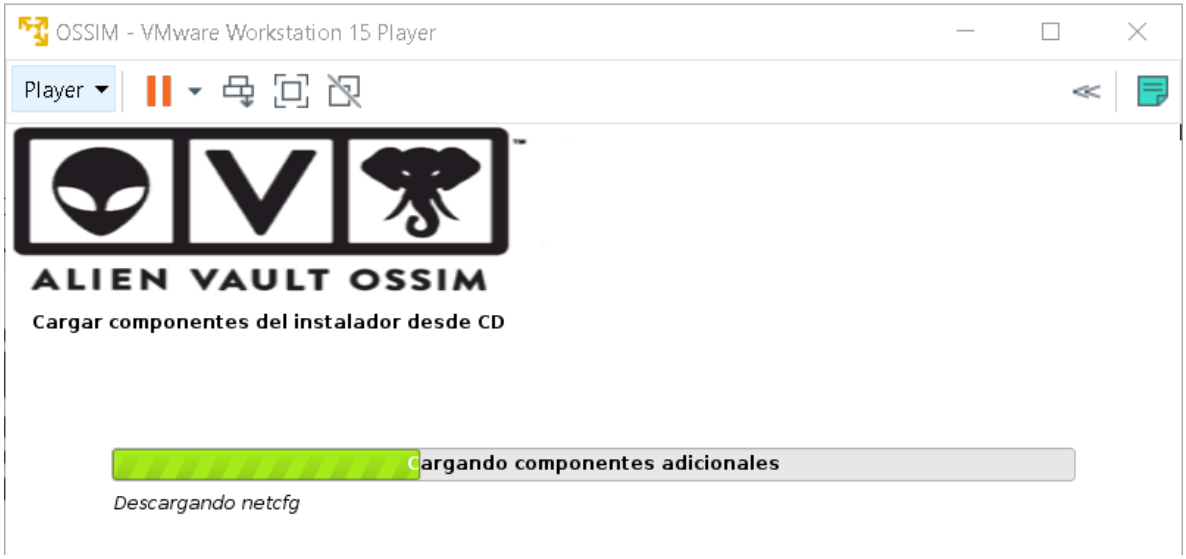
También es necesario seleccionar la ubicación y la configuración del teclado.

Figura 76 Selección de ubicación

Fuente: Elaboración Propia

Luego de esto se empezarán a cargar los componentes necesarios para dar inicio a la instalación.

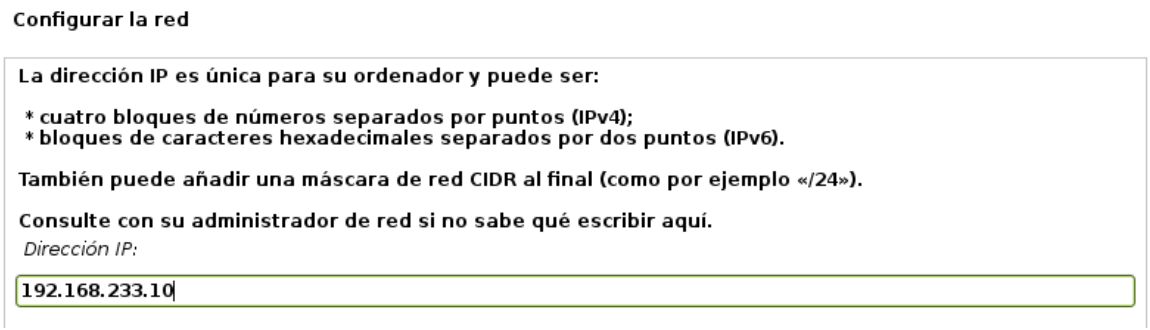
Figura 77 Carga de componentes del instalador



Fuente: Elaboración Propia

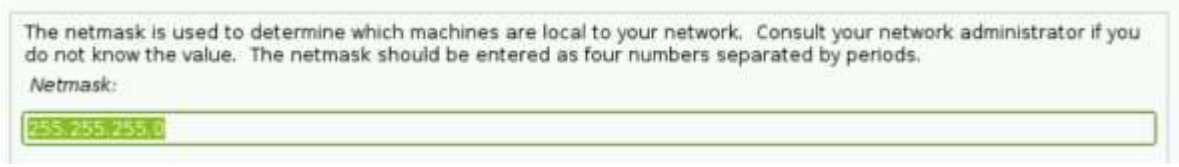
En este paso, se genera la configuración de la red para la máquina virtual OSSIM. Lo primero es agregar es la ip junto con la máscara de red y el gatway a la máquina de OSSIM.

Figura 78 Configuración de Red



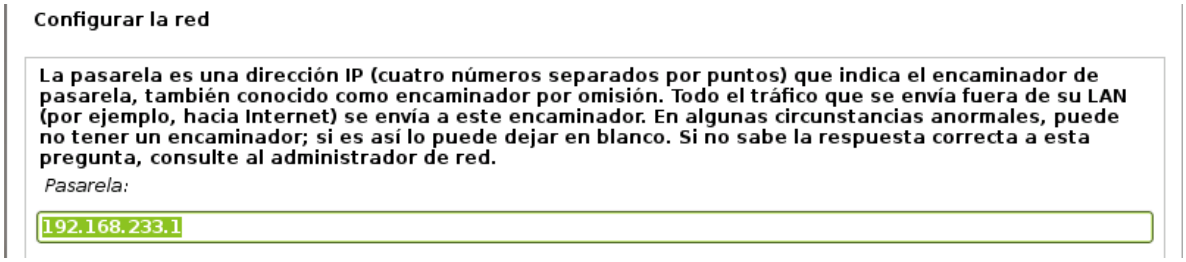
Fuente: Elaboración Propia

Figura 79 Ingreso de máscara de red



Fuente: Elaboración Propia

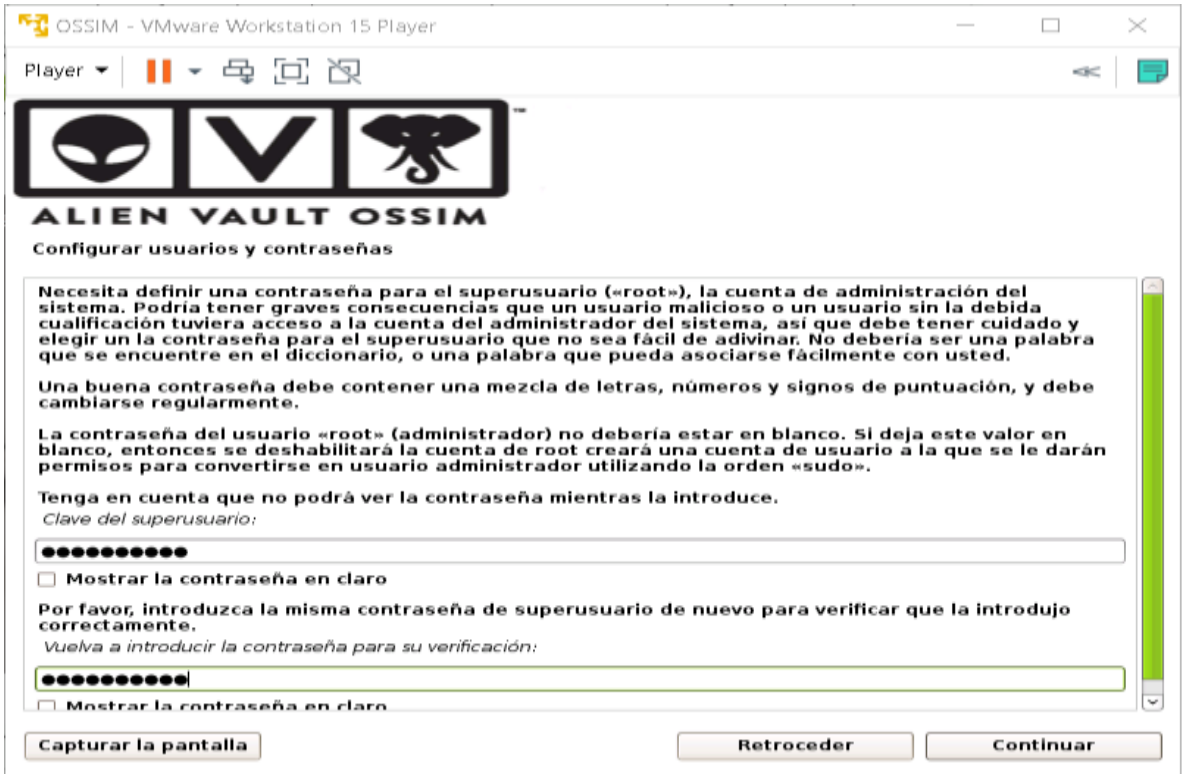
Figura 80 Configuración IP de la red



Fuente: Elaboración Propia

Después de la configuración de red, la siguiente ventana de configuración solicita la contraseña del usuario root que puede acceder a la CLI del servidor OSSIM. La contraseña del usuario raíz debe ser robusta.

Figura 81 Configuración de usuario y contraseña



Fuente: Elaboración Propia

Después de configurar los datos de red y la contraseña, el asistente realiza automáticamente el paso de partición de disco y comienza a instalar el sistema base. Este paso tomará casi 10-30 minutos.

Figura 82 Formateando particiones de disco

Fuente: Elaboración Propia.

Luego de esto, se muestra la etapa final de la instalación como se observa en la siguiente figura.

Figura 83 Fin de la instalación

Finalizado este proceso se genera un reinicio de la maquina y nos mostrara el login para el inicio por CLI de OSSIM, el usuario es root y la contraseña es la que configuramos en el paso anterior.

Figura 84 Inicio por consola

Fuente: Elaboración Propia

Con esto ingresamos al navegador y escribimos la dirección IP de OSIMM pare este caso es https://192.168.233.10, se solicita autorización para continuar a la página esto debido a que el certificado no es de confianza porque OSSIM utiliza el certificado autofirmado.

Figura 85 Verificación de inicio

Fuente: Elaboración Propia.

Luego de esto se solicita la información necesaria para el administrador del servidor OSSIM. Se deben agregar los datos que se solicitan como se visualiza en la siguiente figura.

Figura 86 Crear cuenta de administrador

Fuente: Elaboración Propia.

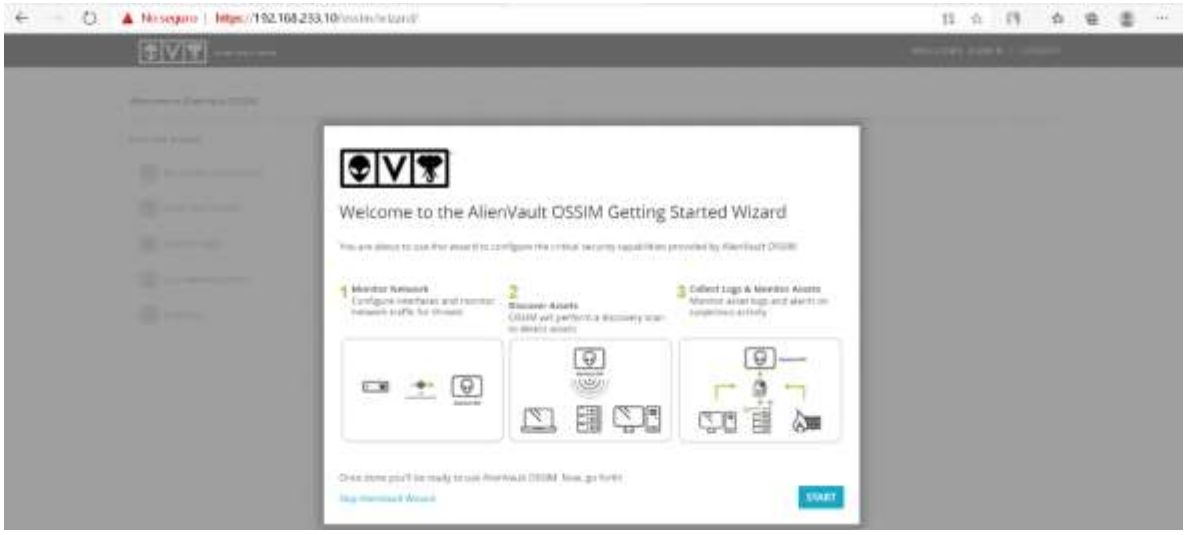
Ya con esto nos redirecciona a la página de inicio de sesión, allí se debe colocar el usuario y la contraseña que se agregaron en el paso anterior.

Figura 87 Iniciar sesión

Fuente: Elaboración Propia.

Luego de iniciar sesión correctamente en la interfaz web, aparece el asistente para la configuración adicional del servidor OSSIM.

Figura 88 Ventana de inicio



Fuente: Elaboración Propia.

Muestra las siguientes tres opciones

- Supervisar red (Configurar red que está siendo supervisada por el servidor OSSIM)
- Detección de activos (detección automática de dispositivos de red en la organización)
- Recopilación de registros y supervisión de nodos de red

Le damos clic al botón inicio para comenzar con el proceso de configuración.

Después de hacer clic en la primera opción, solicitará la configuración de red que se muestra en la figura siguiente. Para este caso se configura eth0 para el recopilador de registros y la interfaz de supervisión del servidor OSSIM.

Figura 89 Configurar red

Fuente: Elaboración Propia.

En la segunda opción, OSSIM realizará la detección automática de los activos de red. En OSSIM tenemos tres opciones de agregar los activos esta son: de forma manual, por medio de un escaneo de red o importado un archivo CSV. Los tipos de activos en el servidor OSSIM son Windows, Linux y Dispositivo de red.

Figura 90 Agregar activos

Fuente: Elaboración Propia.

Después de la configuración de red y la detección de activos, el siguiente paso es la implementación de los agentes HIDS en dispositivos Windows/Linux para realizar la integridad de los archivos, la supervisión, la detección de rootkits y la recopilación de registros de eventos. Para este caso se debe Introduzca el nombre de usuario/la contraseña del recurso para la implementación de HIDS.

Figura 91 Configuración de implementar HIDS

Fuente: Elaboración Propia.

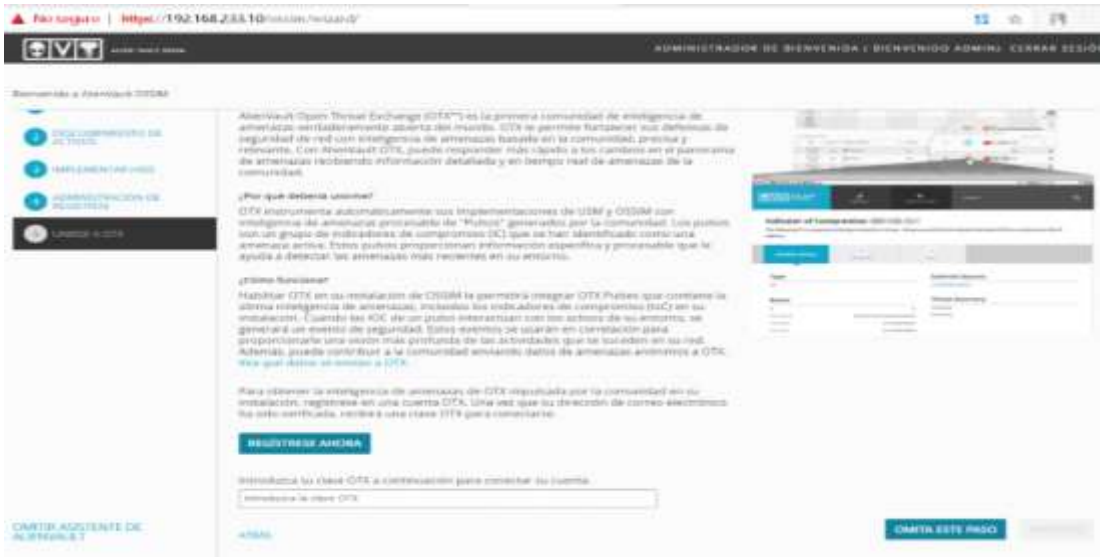
Se selecciona el equipo deseado de la lista y se da clic en el botón Implementar para la implementación de HIDS. Se realiza nuevamente clic en el botón Continuar para iniciar el proceso de implementación como se muestra en la figura. Este proceso tardará algunos minutos para la implementar el agente en el host seleccionado.

Figura 92 Implementar host

Fuente: Elaboración Propia.

La última opción del asistente de configuración es unirse a OTX (Programa de intercambio de amenazas de AlienVault). Para este caso no se configura esta opción. Lo siguiente es dar clic en el botón de finalización.

Figura 93 Unirse a OTS



Fuente: Elaboración Propia.

Ya con estos pasos se tiene OSSIM correctamente instalado y configurado. Se muestra el panel principal del servidor con la información de la recolección de datos, desde aquí también se pueden agregar nuevos activos según el requerimiento del CSIRT.

Figura 94 Panel principal

Fuente: Elaboración Propia.

5.8 Instalación de NAGIOS.

Nagios Core es una herramienta de código abierto muy poderosa que contiene una serie de complementos llamados "complementos" estos pueden ayudar a verificar el estado del hardware o software de un servidor. Una de sus ventajas más importantes es que permite personalizar las alarmas y complementos que se utilizarán.

Nagios proporciona una interfaz WEB desde la cual puede ver el estado de los servidores monitoreados por él. Dependiendo de la configuración realizada durante la instalación, es posible acceder a dicha interfaz WEB a través del puerto 80 o 443.

Además de los plugins con los que cuenta Nagios, brinda la posibilidad de desarrollar complementos ajustados a las necesidades de la organización, esto con el fin de verificar el estado de los componentes que aún no están completados.

A continuación, se listan las características más relevantes de Nagios.

- Permite el control de servicios (SNMP, POP3, HTTP, PING, etc. de forma ya implementada en la herramienta.)
- Permite monitorizar recursos de los equipos tales como carga de CPU, llenado de discos, etc.
- Permite la implementación de scripts adaptados para chequeo de servicios pasivos generados por aplicaciones o comandos externos.
- Permite la monitorización de factores ambientales con la infraestructura que posee la empresa actualmente (sensores de temperatura, humedad, aire acondicionado, etc.…)
- Permite el Balanceo tanto por ubicación física como por criticidad de los servicios para identificar rápidamente los servicios prioritarios.
- Implementación de notificaciones automáticas por mail, Twitter y otros métodos no incluidos en este proyecto como por ejemplo SMS.
- Inclusión de enlaces en la propia interfaz Web a BBDD que contengan los procedimientos a seguir en caso de detectar una alarma.
- Implementación de Plugins como Thruk que permiten facilitar las tareas del técnico. Lo que también permite una visión sencilla de los elementos gestionados a través de una interfaz Web sin sobrecarga de recursos. Programación de poll con o sin notificaciones, para evitar molestias a horas en que la disponibilidad del servicio no es crítica. Posibilidad de incluir

usuarios de sólo lectura y usuarios administradores de la interfaz Web.[43]

La siguiente tabla proporciona recomendaciones de hardware basadas en una relación de nodo (host) a servicio de 1: 5[44]

Tabla 5: Requerimientos Nagios.

Monitored Nodes / Hosts	Monitored Services	Hard Drive Space	CPU Cores	RAM
50	250	40 GB	1 – 2	1 – 4 GB
100	500	80 GB	2 – 4	4 – 8 GB
> 500	> 2500	> 120 GB	> 4	> 8 GB

Fuente: MARTÍNEZ RAMÍREZ, Sergio. Requerimientos Nagios [en línea]. Implementación de un Servidor Nagios para el control y monitoreo de la Red del GDF. México. 2016. Disponible en: http://www.ptolomeo.unam.mx:8080/jspui/bitstream/132.248.52.100/10527/1/Tesina.pdf

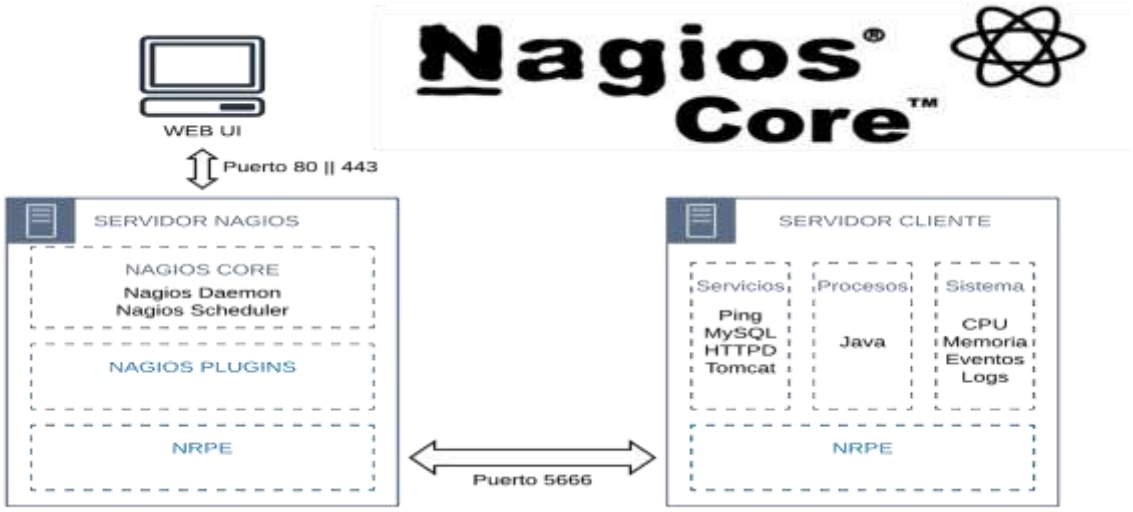
El proceso interno con el que trabaja Nagios se divide en una estructura de ficheros, esto con el fin que todo quede ordenado. Para poder trabajar de manera correcta con Nagios es preciso conocer la base de cómo está estructurado y los diferentes ficheros que es posible modificar para suplir las necesidades que se tenga dentro de la organización.

A continuación, podemos observar la estructura de Nagios con la que se trabaja normalmente.

[43] MARCH, M. Memoria TFC: Integración Sistema de Monitorización Nagios con Twitter. [en línea]. Noviembre de 2020. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/40561/3/dperverTFC0115memoria.pdf

[44] NAGIOS XI. Hardware Requirements. [en línea]. Noviembre de 2020. Disponible en: https://assets.nagios.com/downloads/nagiosxi/docs/Nagios-XI-Hardware-Requirements.pdf

Figura 95 Arquitectura usada para monitorear con Nagios.



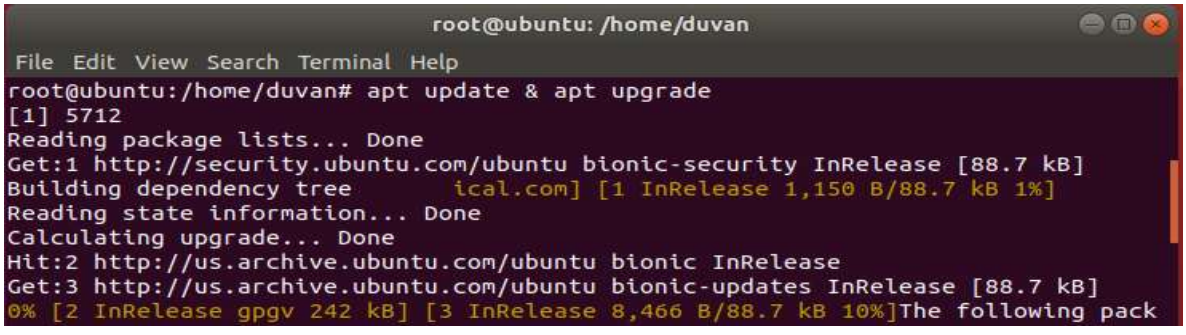
Fuente: ORELLANA, Sebastian. Arquitectura usada para monitorear con Nagios. NAGIOS WITHOUT PAIN. 2019. Disponible en: https://medium.com/@siorellana/nagios-without-pain-b938276b058e.

Para la instalación de Nagios utilizamos un sistema operativo Ubuntu 20.04 virtualizado en VMware, Antes de comenzar con la instalación, es necesario haber iniciado sesión como usuario con privilegios de sudo.

Lo primero que se debe realizar es actualizar el sistema Ubuntu, tanto repositorios como paquetes instalados.

 # apt update & apt update

Figura 96 Instalación de repositorios

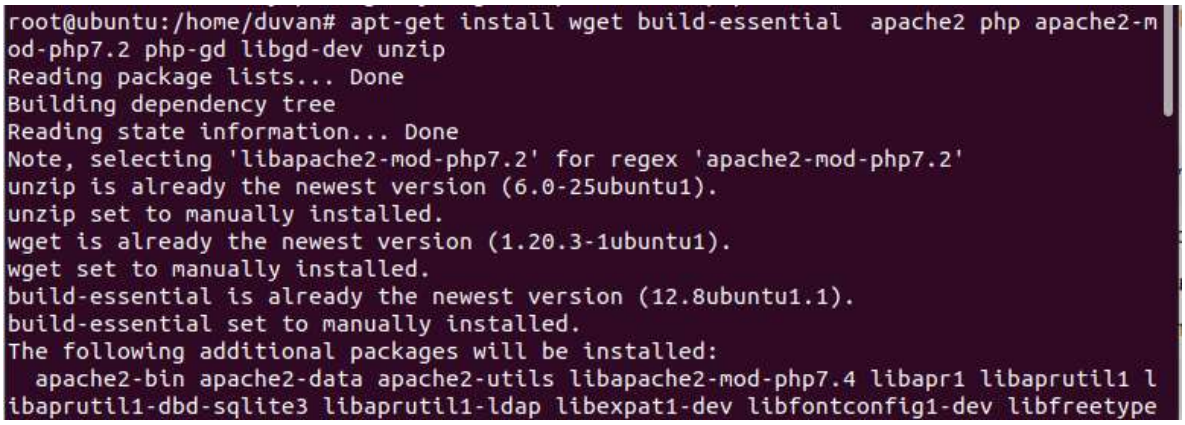


Fuente: Elaboración Propia.

El siguiente paso es instalar los paquetes y dependencias necesarias para llevar a cabo la descarga y compilación del aplicativo principal de Nagios y los plugin de Nagios:

 # apt-get install wget build-essential apache2 php apache2-mod-php7.0 php-gd libgd-dev unzip

Figura 97 Instalación de paquetes de descarga de NAGIOS

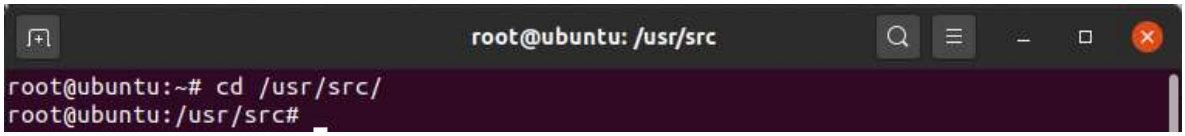


Fuente: Elaboración Propia.

Ahora se genera la descarga de los archivos necesarios para la instalación de Nagios, estos se guardarán en el directorio /usr/src, esta es la ubicación común para colocar los archivos fuente. Se accede a la ruta:

cd /usr/src/

Figura 98 Archivos para instalación de NAGIOS

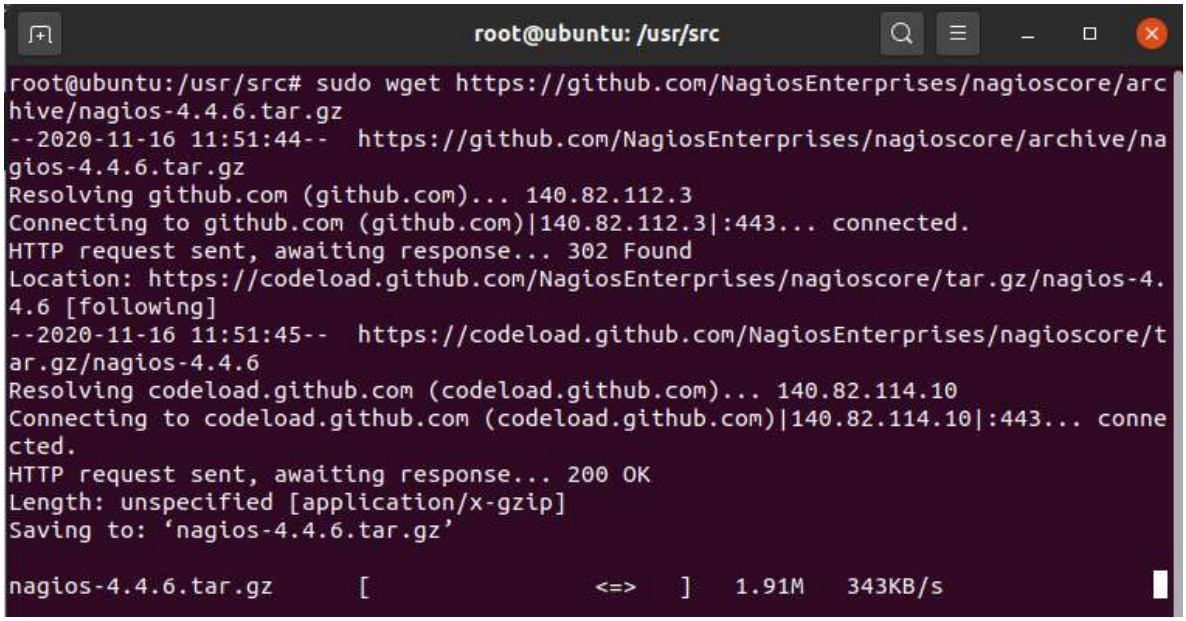


Fuente: Elaboración Propia.

A continuación, realizamos la descarga de la última versión (4.4.6) de Nagios del repositorio de Github del proyecto, para ello utilizando el siguiente comando wget:

 # wget https://github.com/NagiosEnterprises/nagioscore/archive/nagios-4.4.6.tar.gz

Figura 99 Descarga de NAGIOS



Fuente: Elaboración Propia.

Luego de terminar la descarga es necesario descomprimir el archivo .tar:

 # tar zxf nagios-.tar.gz*

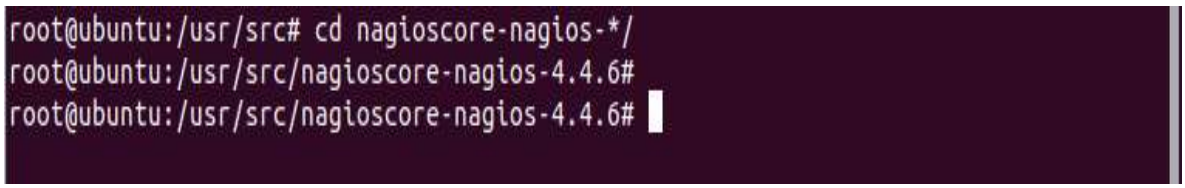
Figura 100 Descompresión de archivo de instalación

Fuente: Elaboración Propia.

Para poder ejecutar las sentencias de compilación es necesario cambiar al directorio de origen de Nagios para esto escribimos:

 # cd nagioscore-nagios-/*

Figura 101 Cambio de directorio

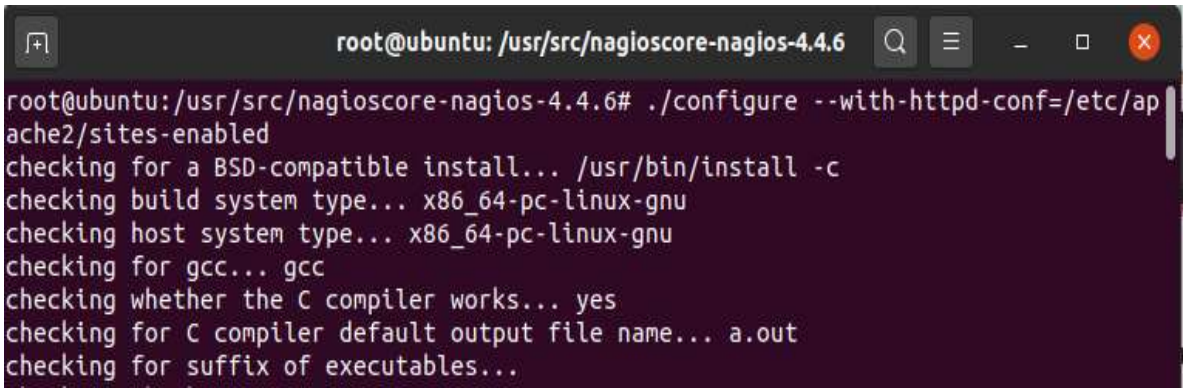


Fuente: Elaboración Propia.

El siguiente paso es ejecutar el proceso de compilación de Nagios, para esto se ejecuta el script de configuración, este script realizará una serie de verificaciones para asegurarse de que todas las dependencias de su sistema estén presentes:

#. /configure --with-httpd-conf=/etc/apache2/sites-enabled

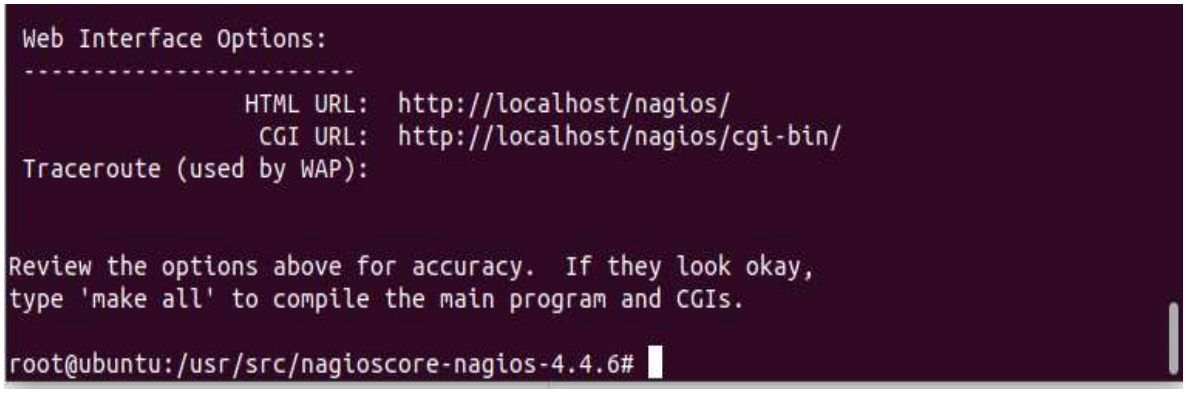
Figura 102 Ejecución de script de verificación



Fuente: Elaboración Propia.

Si todo está correcto se mostrará un mensaje como el siguiente:

Figura 103 Mensaje de verificación

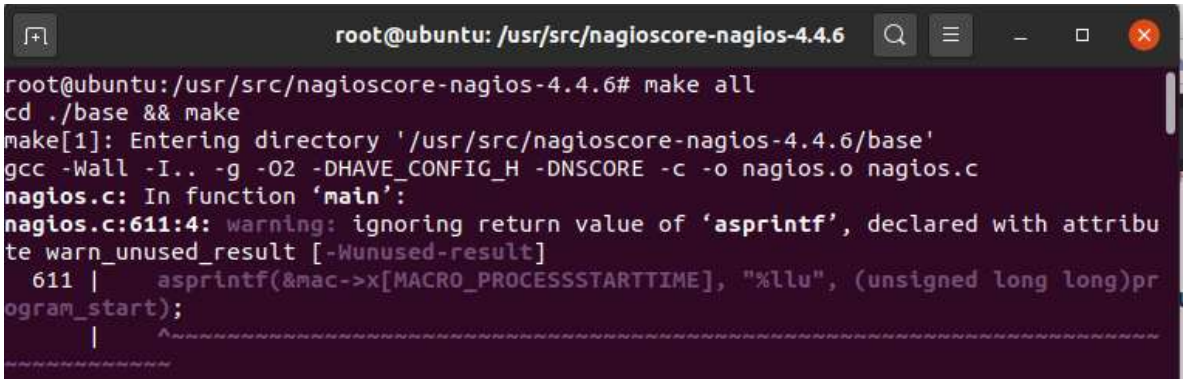


Fuente: Elaboración Propia.

Ahora ya es posible comenzar el proceso de compilación, para esto ejecutamos comando make como se muestra a continuación:

 # make all

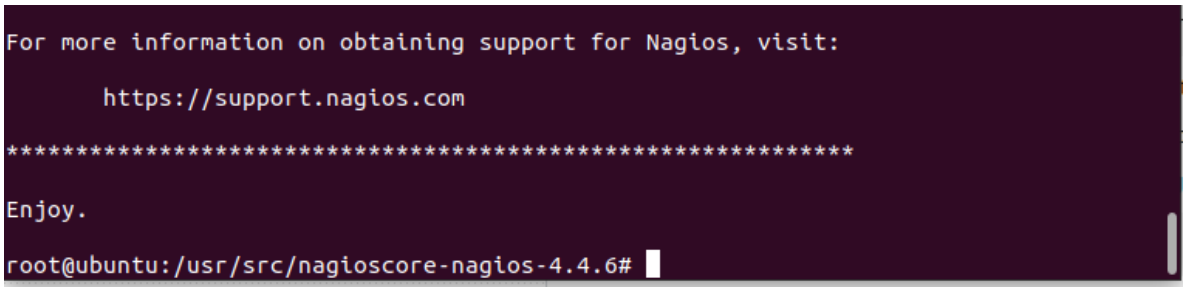
Figura 104 Ejecución de comando MAKE



Fuente: Elaboración Propia.

Esta compilación puede tardar algún tiempo, dependiendo de los recursos asignados al sistema donde se instala Nagios. Una vez que se complete el proceso de compilación, se mostrará el siguiente mensaje:

Figura 105 Mensaje de validación

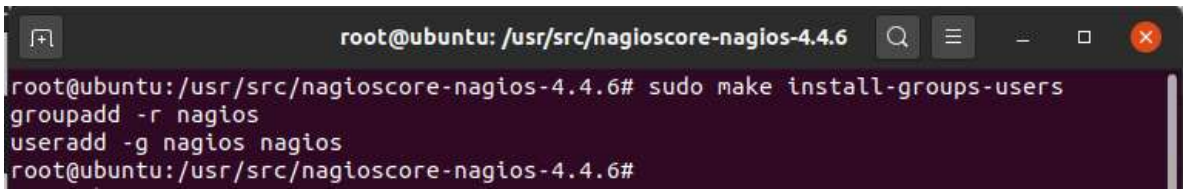


Fuente: Elaboración Propia.

El siguiente paso es crear un nuevo usuario y grupo de nagios en el sistema:

 # make install-groups-users

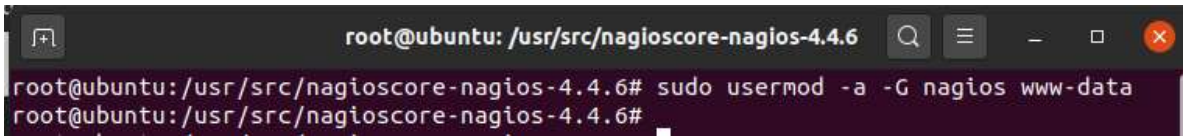
Figura 106 Creación de nuevo usuario



Fuente: Elaboración Propia.

Ahora se debe agregar el usuario de www-data Apache www-data al grupo que creamos:

Figura 107 Agregar usuario al grupo

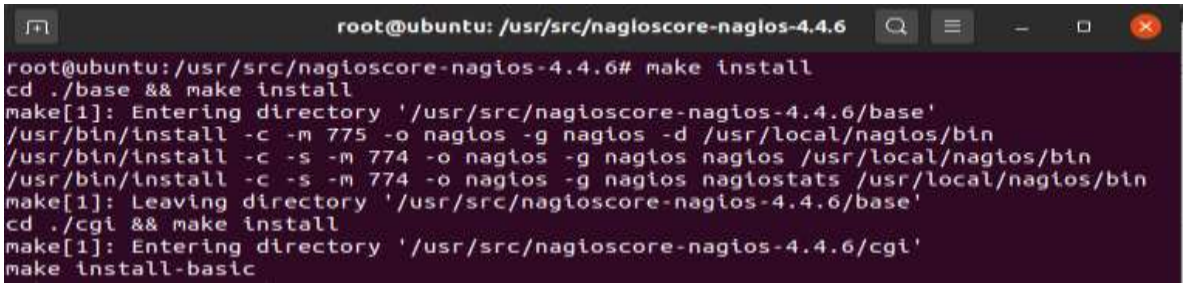


Fuente: Elaboración Propia.

Después de agregar los usuarios, seguimos con la instalación de los archivos binarios de Nagios, CGI y archivos HTML para esto se ejecuta el siguiente comando:

 # sudo make install

Figura 108 Instalación de archivos

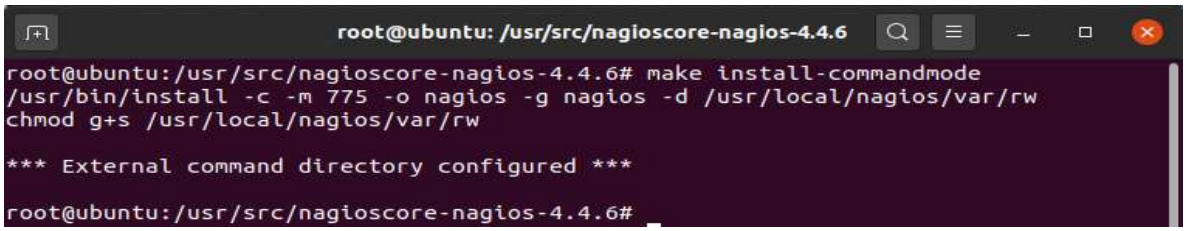


Fuente: Elaboración Propia.

Nagios tiene la capacidad de procesar comandos desde aplicaciones externas. Para habilitar esta opción se debe crear el directorio de comandos externo y darle los permisos necesarios:

 # make install-commandmode

Figura 109 Crear directorio externo

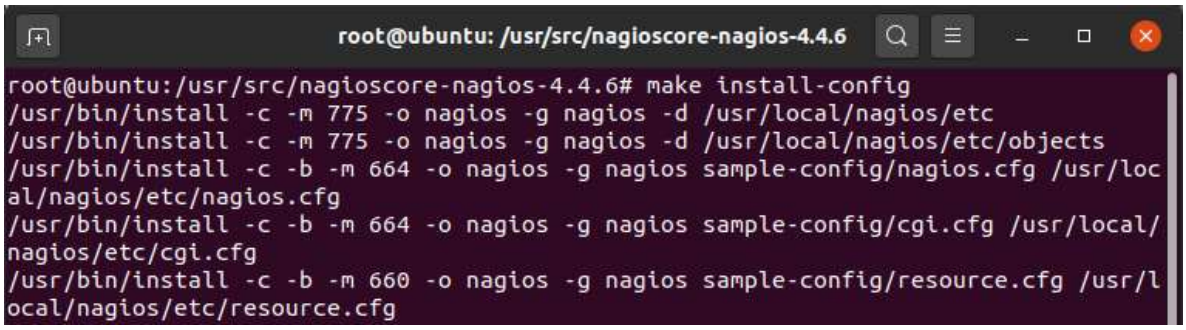


Fuente: Elaboración Propia.

También es posible Instalar los archivos de configuración de Nagios de muestra para ello se ejecuta el comando:

 # make install-config

Figura 110 Instalación de archivos de configuración de Nagios

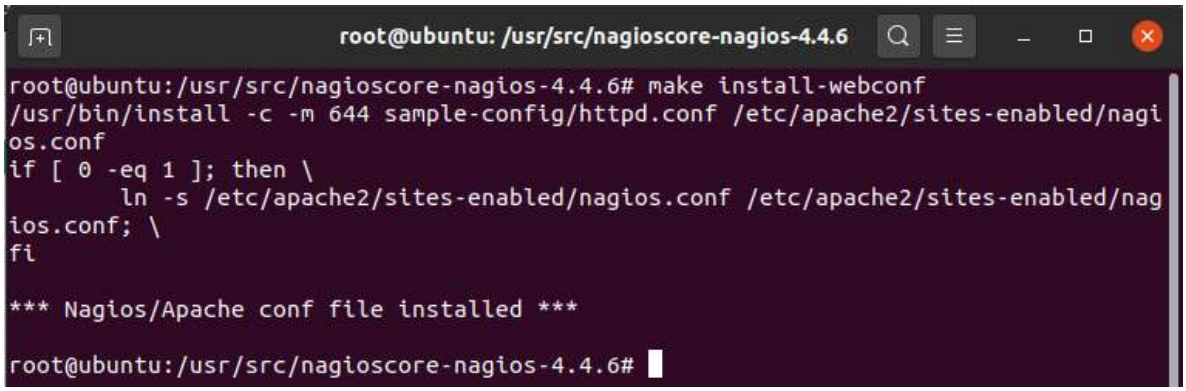


Fuente: Elaboración Propia.

Es necesario configurar el servidor web apache. Con el siguiente comando instalara los archivos necesarios:

 # make install-webconf

Figura 111 Configuración de servidor Apache

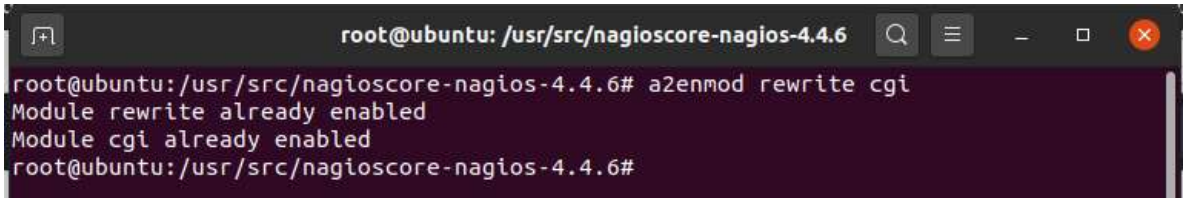


Fuente: Elaboración Propia.

Ahora es necesario comprobar que Apache rewrite y los módulos cgi estén habilitados:

 # a2enmod rewrite cgi

Figura 112 Verificación de servidor Apache

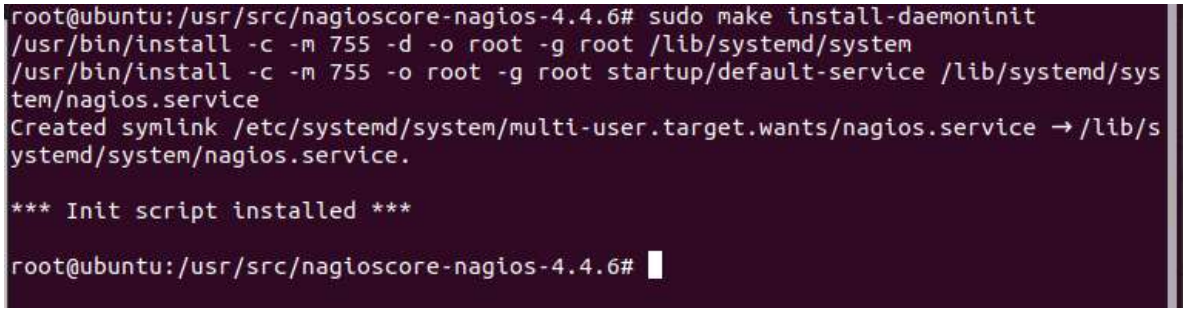


Fuente: Elaboración Propia.

A continuación, se genera la configuración para que Nagios se ejecute como demonio en el arranque de sistema operativo. Con el siguiente comando se instala el archivo de unidad systemd y configura el demonio:

 # make install-daemoninit

Figura 113 instalación del archivo unidad system

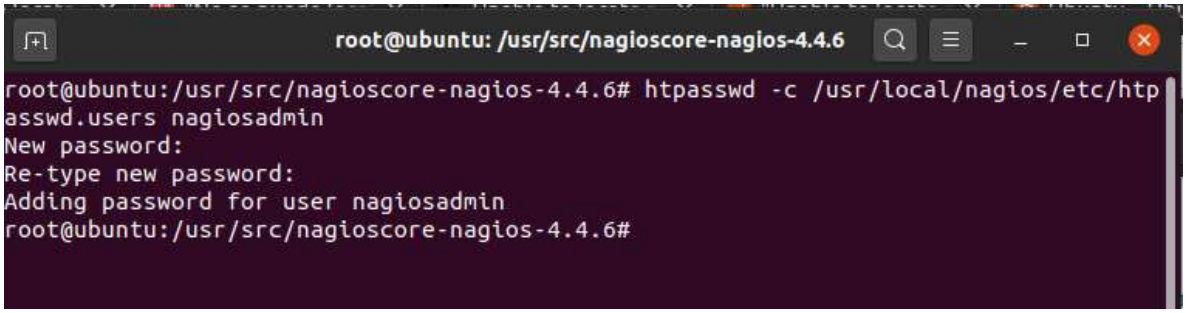


Fuente: Elaboración Propia.

Ya con anteriores pasos tenemos instalado y correctamente configurado el servidor Nagios, antes de iniciar y para poder acceder a la interfaz web de Nagios, es necesario crear un administrador llamado nagiosadmin, para crear un usuario se debe ejecutar el comando htpasswd como se observa a continuación:

 # htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin

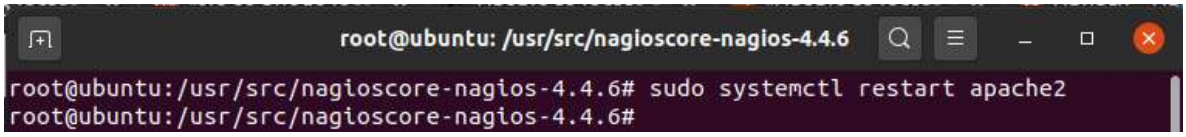
Figura 114 Creación del administrador llamado nagiosadmin



Fuente: Elaboración Propia.

Para que los cambios surjan efecto es necesario reiniciar los servicios de apache

Figura 115 Reinicio de servicios de apache

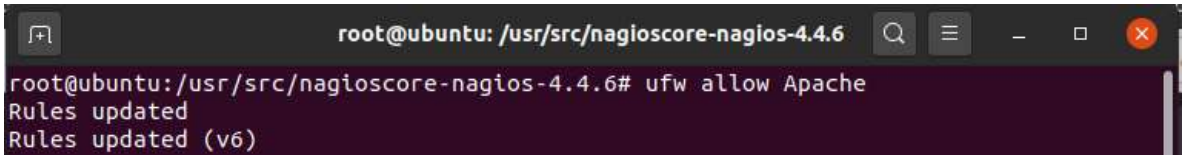


Fuente: Elaboración Propia.

Es necesario abrir los puertos del firewall para impedir que se genere algún bloqueo sobre el servicio de Nagios.

ufw allow Apache

Figura 116 Apertura de puertos del firewall



Fuente: Elaboración Propia.

El siguiente paso es instalar los complementos de Nagios, para esto descargamos los archivos necesarios desde los repositorios de GitHub

 # wget -O nagios-plugins.tar.gz https://github.com/nagios-plugins/nagios-plugins/archive/release-2.2.1.tar.gz

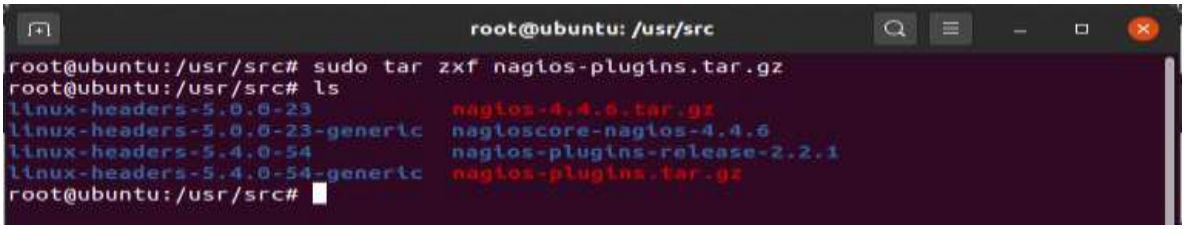
Figura 117 Descargas de repositorios de GitHub

Fuente: Elaboración Propia.

Terminada la descarga es necesario descomprimir el archivo .tar.

 # tar zxf nagios-plugins.tar.gz

Figura 118 Archivo .tar

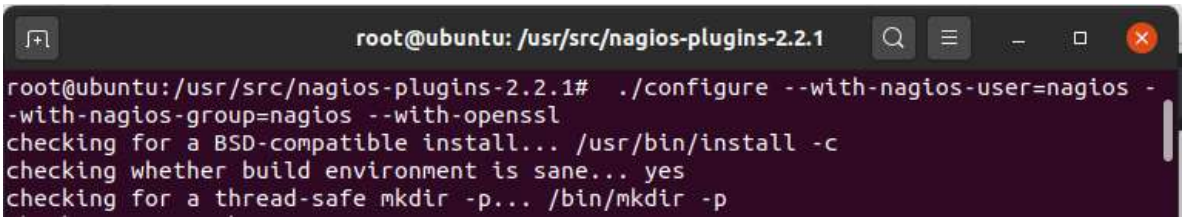


Fuente: Elaboración Propia.

Ingresamos al directorio de nagios-plugins y compilamos los complementos.

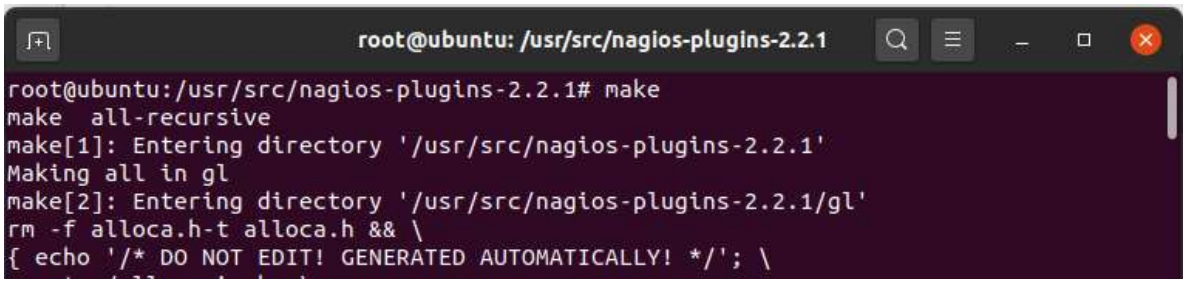
 # ./configure --with-nagios-user=nagios --with-nagios-group=nagios --with-openssl

Figura 119 Compilación de los complementos



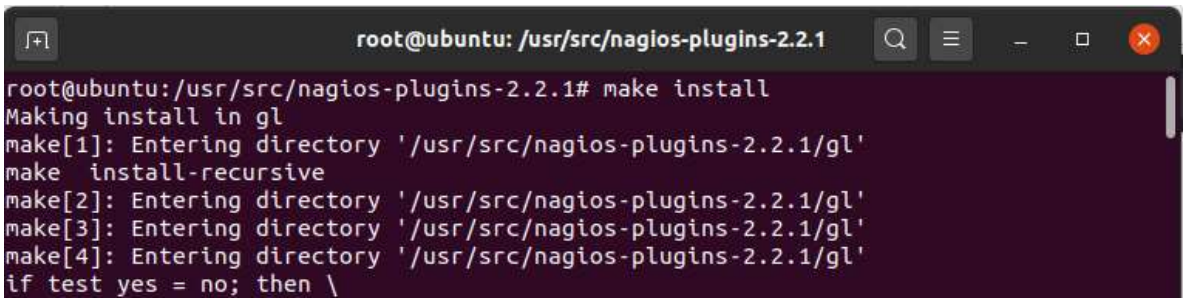
Fuente: Elaboración Propia.

Figura 120 make



Fuente: Elaboración Propia.

Figura 121 instalación del make

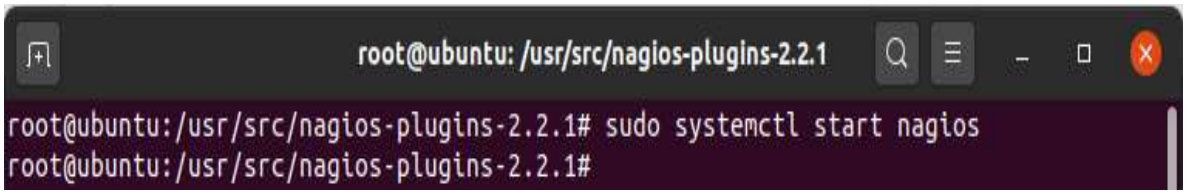


Fuente: Elaboración Propia.

Ya con esto yanto Nagios como los complementos se encuentran instalados y correctamente funcionales. Debemos iniciar los servicios de Nagios, esto se realiza con el siguiente comando.

 # systemctl start nagios

Figura 122 Iniciar los servicios de Nagios

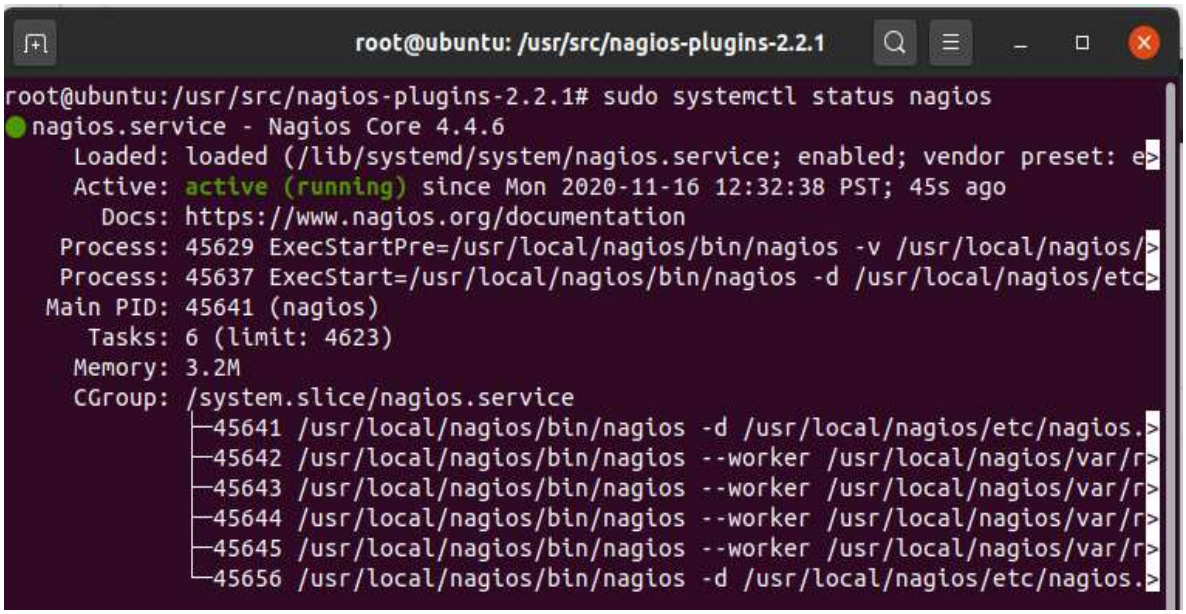


Fuente: Elaboración Propia.

Si es necesario se puede comprobar que Nagios se está ejecutando correctamente, si todo está correctamente debe aparecer un mensaje como el siguiente.

 # systemctl status nagios

Figura 123 Mensaje de ejecución correcta



Fuente: Elaboración Propia.

Para acceder a la interfaz web de Nagios, en un navegador se escribe la dirección IP des servidor seguido de /nagios, para este caso la ruta es http://192.168.266.143/nagios

Figura 124 Acceso a la interfaz web de Nagios

Fuente: Elaboración Propia.

Ingresamos con el usuario nagiosadmin y la contraseña que se configuro en el paso anterior y ya tendremos la interfaz de inicio de Nagios, donde se puede empezar a agregar los servidores que se van a monitorear.

Figura 125 Interfaz de inicio de Nagios

Fuente: Elaboración Propia.

Finalmente, el análisis de las herramientas presentadas para la implementación del CSIRT en Cibersecurity de Colombia LTDA, permitió contribuir con la evaluación de componentes de hardware, software, estructura tecnológica, modelo organizativo y perfiles profesionales necesarios, para el correcto funcionamiento del CSIRT de la mencionada empresa.

6 CONCLUSIONES

Con base al primer objetivo específico, se seleccionaron las herramientas de hardware y software necesarias para la creación e implementación de un CSIRT en la empresa Cibersecurity de Colombia LTDA, basándose en el criterio de que el CSIRT debe dar respuesta a los incidentes de seguridad de la información de forma rápida y oportuna.

Con respecto a la estructura tecnológica necesaria para la implementación del CSIRT, se definió un modelo organizativo, basado en una estructura básica que permitirá a futuro el crecimiento del CSIRT, en caso de ser necesario, esta estructura que fue definida funcionará con la menor cantidad de personal requerida para realizar todas las actividades necesarias y de esta forma proteger la información de los usuarios.

Adicionalmente, se elaboraron los perfiles profesionales para el reclutamiento del personal que va a trabajar en el CSIRT, velando por que el mismo este conformado por personal con conocimientos avanzados en cada especialidad requerida, lo que permitirá a futuro, expandir la estructura de CSIRT y crear roles de líderes de unidad de forma rápida.

Finalmente, se creó una guía técnica de referencia para la instalación e implementación de las herramientas de software necesarias para el funcionamiento del CSIRT de la empresa Cibersecurity de Colombia LTDA, la guía detalla paso a paso, cual es el software que se requiere para el funcionamiento de CSIRT, el procedimiento para la instalación y por último el uso que se le debería dar.

7 BIBLIOGRAFÍA

ANÓNIMO. Bacula Community Installation Guide A short guide to installing Bacula [en linea]. 20 de Septiembre 2020. Disponible en: https://blog.bacula.org/whitepapers/CommunityInstallationGuide.pdf

ANDRADE, R., & FUERTES, W. Diseño y dimensionamiento de un equipo de respuesta ante incidentes de seguridad informática (CSIRT). Caso de estudio: Escuela Politécnica del Ejército [en línea]. Octubre 2020. Disponible en: http://repositorio.espe.edu.ec/bitstream/21000/6972/1/AC-GRT-ESPE-047091.pdf

AT&T CYBERSECURITY. USM Appliance. Deployment Guide. [En línea]. Octubre de 2020. Disponible en: https://cybersecurity.att.com/documentation/resources/pdf/usmappliancedeployment-guide.pdf

BEN, M. (2018). How to Build a CIRT based on Open source tools. [En línea]. Septiembre de 2020. Disponible en: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Africa_Cyberdrill_18/Presentations/5-Services.pdf

CUCKOO SANDBOX Book. [En línea]. Septiembre de 2020. Disponible en: https://cuckoo.readthedocs.io/en/latest/

CUCKOO INSTALLATION. [En línea]. Septiembre de 2020. Disponible en: https://cuckoo.sh/docs/installation/index.html

CCN-CERT LUCIA. Centro Criptológico Nacional España. Versión 2.02. [En línea]. Diciembre de 2020. Ubicación: https://www.ccn-cert.cni.es/documentos-publicos/877-lucia-presentacion/file.html. Octubre 2020.

CONPES 3854, C. N. Departamento Nacional de Planeación. [En línea]. Diciembre de 2020. Disponible en: https://observatorioplanificacion.cepal.org/es/instituciones/consejo-nacional-de-politica-economica-y-social-conpes-de-colombia

DE LA TORRE, H., & PARRA, M. (2018). Estrategia y diseño de un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) académico. Universidad de las Fuerzas Armadas ESPE. Pag 46.

ENISA. (2006). Cómo crear un CSIRT paso a paso. (CERT-D1/D2). [En línea]. Septiembre de 2020. Disponible en: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

ENISA. (2016). CSIRT Setting up Guide in Spanish. [En línea] Agosto 2020. Disponible en: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullRepor

ITECO CERT. (2009). Instituto Nacional de Tecnologías de la Comunicación. [En línea] Septiembre 2020. Disponible en: www.inteco.es/extfrontinteco/icd/pdf/Cortafuegos_VPN_IDS_IPS.pdf

INTERNATIONAL TELECOMMUNICATION UNION. Resources of CSIRT (Tools and Services of CIRT/CSIRT). [En línea]. Noviembre 2020. Disponible en: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Services.pdf

MUÑOZ, M. Estado actual de equipos de respuesta a incidentes de seguridad informática. [En línea]. Septiembre 2020. Disponible en: http://www.scielo.mec.pt/scielo.php?pid=S1646-98952015000100002&script=sci_arttext

MICHAEL, P. SEYMOUR, E. Global Initiatives to Secure Cyberspace - An Emerging Landscape. Disponible en: http://dx.doi.org/10.1007/ 978-0-387-09764-0. Volumen 42.

MinTIC. (2012). Ley 1581. [En línea]. Octubre 2020. Disponible en: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

MINISTERIO DE DEFENSA. Sandbox CSIRT – PONAL. [En línea]. Febrero de 2020. Disponible en: https://cc-csirt.policia.gov.co/noticias/2020/1er-trimestre/sandbox-ponal

ORGANIZACIÓN DE ESTADOS AMERICANOS. Buenas prácticas para establecer una CSIRT nacional. [En línea]. Octubre de 2020. Disponible en: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

OCHOA, Ovalles**.** Seguridad informática en Contribuciones a las Ciencias Sociales. [En línea]. Julio 2020. Disponible en: http://www.eumed.net/rev/cccss/21/oocs.html

PEREZ PEREZ, Yuly. La importancia de la Ciberseguridad en Colombia. [En Línea]. 18 de diciembre de 2020. Disponible en: http://polux.unipiloto.edu.co:8080/00003620.pdf

PENEDO, D. Technical Infrastructure of a CSIRT. [En línea]. Noviembre 2020. Disponible en: https://ieeexplore.ieee.org/abstract/document/1690411

POZUELO, Alberto. Implantación de sistemas de BackUp Empresarial. 2017. Universitat Oberta de Catalunya. [En línea]. Septiembre 2020. Disponible en: http://hdl.handle.net/10609/63285

RAMIREZ, L. Desarrollo de un Marco de Trabajo para la Protección de un Equipo de Respuesta ante Incidencias de Seguridad Informática (CSIRT). [en línea]. Octubre de 2020. Disponible en: http://cimat.repositorioinstitucional.mx/jspui/handle/1008/442

SENADO DE LA REPUBLICA. Ley 1273 de 2009. [En línea]. Noviembre 2020. Disponible en: https://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.h

SENADO DE LA REPUBLICA. Ley 241 de 2011. [En línea]. Noviembre 2020. Disponible en: http://www.senado.gov.co/index.php/documentos/az-legislativo-categoria/conciliaciones/217-texto-conciliado-plan-nacional-de-desarrollo/file

SOFTWARE ENGINEERING INSTITUTE. Create a CSIRT Technical Report. [En línea]. Disponible en: http://www.cert.org/incident-management/products-services/creating-a-csirt.cfm. Octubre 2020.

URIBE, Edgar. Proceso para la Definición de Servicios Iniciales en un Equipo de Respuesta ante Incidencias de Seguridad Informática (CSIRT). Zacatecas. 2014. 211 p. Trabajo de grado para Maestro en Ingeniería de Software Centro de Investigación en Matemáticas, A.C.

WARNING, ADVICE AND REPORTING POINTS. [En línea]. Octubre de 2020. Disponible en: http://www.warp.gov.uk.