PROPUESTA TÉCNICA PARA LA CREACIÓN DE UN CENTRO DE RESPUESTA A INCIDENTES CIBERNÉTICOS PARA LA EMPRESA CASO DE ESTUDIO CIBERSECURITY DE COLOMBIA LTDA

ALEX AUGUSTO BALLESTEROS CARDENAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA.
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTA
2020

PROPUESTA TÉCNICA PARA LA CREACIÓN DE UN CENTRO DE RESPUESTA A INCIDENTES CIBERNÉTICOS PARA LA EMPRESA CASO DE ESTUDIO CIBERSECURITY DE COLOMBIA LTDA

ALEX AUGUSTO BALLESTEROS CARDENAS

Trabajo de grado como requisito para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director. Ing. EDGAR MAURICIO LOPEZ
Magister en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA.
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTA
2020

NOTA DE ACEPTACIÓN

Firma presidente del jurado

Firma del jurado

Firma del jurado

Bogotá, Cundinamarca, 01 octubre de 2020.

DEDICATORIA

A mi madre Graciela Cárdenas, esposa Alba Padilla e hijos Juan Andrés y David Alejandro, por motivarme a iniciar y culminar este nuevo reto de mejoramiento profesional y personal, por apoyarme y siempre estar en el momento que más los necesito.

A mi Padre Carlos Augusto Ballesteros Bueno, aunque no se encuentre conmigo sin su educación, valores y herramientas que me proporciono para la vida, no hubiera sido posible afrontar y culminar este proyecto de grado.

AGRADECIMIENTOS

Al Ing. Luis Fernando Zambrano, Esp. en Seguridad Informática, quien fue tutor y director del curso proyecto de grado 1 por sus observaciones pertinentes y guía durante el desarrollo del proyecto de grado en su primera fase.

A la Ing. Katerine Márceles tutora del curso proyecto de grado 2 por su apoyo y orientación en el desarrollo de este.

Al Ing. Edgar Mauricio López, Magister en seguridad informática y Director del proyecto de Grado por sus aportes puntuales y relevantes para la construcción del documento proyecto aplicado para la construcción y presentación de un trabajo con calidad.

A mi esposa Alba Libia Padilla Arredondo por su apoyo incondicional y motivación, sin ella no hubiera sido posible tener la constancia y tenacidad para desarrollar este proyecto de grado.

RESUMEN

La empresa CIBERSECURITY DE COLOMBIA LTDA. No cuenta con un CERT (Equipo de respuesta a emergencia de informática) sigla utilizada en estados unidos creador del primer de estos y posteriormente creado en Europa utilizando las siglas CSIRT (Equipo de Respuesta ante Incidencias de Seguridad Informática) , la empresa en mención tiene como objetivo para el 2021 tener un CSIRT para prestar un servicio proactivo de acuerdo a las necesidades de sus clientes, es importante resaltar la relevancia de contar con un CSIRT , como menciona DNP[1] mediante el Conpes 3701 de 2011, se dan los lineamientos incluidos en el plan de desarrollo, para la creación con el nombre de COLCERT perteneciente al ministerio de defensa y con el cual su objetivo principal es estar preparados y contrarrestar un ciberataque, como se menciona en las noticias de la Mc Guinness. D. BBC NEWS[2]. con el ciberataque que ocurrió en 2007 en estonia con (BOTNETS), el cual afecto a toda la nación por varias semanas colapsando bancos, correos electrónicos de las entidades públicas y privadas, generando caos, incertidumbre y confusión entre la población de este país, alertando a los países de la OTAN (organización para el tratado atlántico norte) de que este ataque fue realizado por el gobierno ruso lo cual nunca se pudo comprobar y el ocurrido a nivel mundial con Botnets Mariposa el cual afecto a 190 países siendo Colombia el quinto país.

Durante la construcción de la propuesta en la fase 1, se realizará un levantamiento de información de las herramientas de software con la característica que sean open source que aplique para para los servicios mínimos que prestara en cuanto a incidentes reactivos y proactivos en el CSIRT, se realizara el diseño de la estructura con las áreas mínimas que debe tener, haciendo énfasis en operaciones, también para la fase 2 se relacionara todo el levantamiento del hardware necesario para desarrollar la actividades, se hará la implementación de un laboratorio controlado con los servicios de monitoreo, correlacionador de eventos, copias de seguridad y SandBox, presentando los respectivos informes, evidencias para la sustentación de este proyecto aplicado.

Se elaborará el diseño de la estructura tecnológica en especial del centro de operaciones, con un levantamiento de información de las herramientas a nivel de hardware para el desarrollo de las distintas actividades y servicios como lo es monitoreo, correlacionador de eventos, servidor de copias de seguridad y sanbox.

[1] COLOMBIA. DNP. Conpes 3701 de 2011, p.22. [En linea]. Disponible https://mintic.gov.co/portal/604/articles-3510_documento.pdf

[2] MCGUINNESS. D. BBC NEWS Mundo. Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país. Mayo 6 2017. [En linea] Disponible https://www.bbc.com/mundo/noticias-39800133

Junto a un recuento de los antecedentes a la creación del primer CSIRT, el cual se crea por causa de un ataque informático por el estudiante Robert Tappan Morris de la universidad de Cornell (estados unidos) este gusano fue liberado el 2 de noviembre de 1988, el cual quería pasar el código de computador a computador y nunca imagino el alcance de este virus de tipo gusano, fue capaz de infectar al 10% de los computadores de esa época e incluso afectar a la NASA.

Por medio del Conpes 3701 de 2011, menciona dentro de sus logros específicos la creación de nuevas instancias para ciberseguridad y ciberdefensa del país entre las cuales se encuentra COLCERT del ministerio de defensa, comando conjunto cibernético (CCOC) fuerzas militares de Colombia y el centro cibernético de la policía nacional (CCP).[3]

A demás todo este proyecto se realizará por medio de la investigación documental, utilizando técnicas de recopilación de información de bibliotecas, periódicos, internet, utilizando la lectura crítica, registros de gráficos.

Esta es de tipo cualitativo enfocada desde lo interpretativo y análisis de documentos y otras fuentes de información, realizando un análisis, comparación y críticas constructivas entre el diseño técnico de los diferentes CSIRT.
Para tener como resultado esperado la elaboración y entrega de la estructura tecnológica, junto a las herramientas de hardware y software, con su respectiva documentación técnica para el desarrollo de actividades y la simulación de un laboratorio controlado para los servicios virtualizados y funcionales como (monitoreo, correlacionador de eventos, copias de seguridad y Sandbox) todo lo anterior para el desarrollo de actividades del CSIRT para la empresa CIBERSECURITY DE COLOMBIA LTDA.

Palabras Claves- CSIRT, CERT, Seguridad informática. Incidente, Vulnerabilidad.

[3] MINTIC. Conpes 3701, pág. 20. Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación. Bogotá D.C., 14 de julio de 2011. [En linea]. Disponible https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

ABSTRACT

The company CIBERSECURITY DE COLOMBIA LTDA. It does not have a CERT (Computer Emergency Response Team) acronym used in the United States creator of the first of these and subsequently created in Europe using the acronym CSIRT (Computer Security Incident Response Team), the company in question has as objective for 2021 to have a CSIRT to provide an active, reactive service according to the needs of its customers, it is important to highlight the relevance of having a CSIRT, as DNP mentions through Conpes 3701 of 2011, the guidelines included in the development plan, for the creation with the name of COLCERT belonging to the defense ministry and with which its main objective is to be prepared and counteract a cyber-attack, as mentioned in the McGuinness news. D. BBC NEWS. with the cyber-attack that occurred in 2007 in Estonia with (BOTNETS) which affected the entire nation for several weeks collapsing banks, emails from public and private entities, generating chaos, uncertainty and confusion among the population of this country, alerting NATO countries (organization for the North Atlantic Treaty) that this attack was carried out by the Russian government which could never be verified and that occurred worldwide with Botnets Mariposa which affected 190 countries, with Colombia being the fifth most affected.

During the construction of the proposal in phase 1, an information gathering of the latest open source hardware and software tools will be carried out that applies to the minimum services provided in terms of active and reactive incidents in the CSIRT, will be carried out the design of the structure with the minimum areas that it must have, with emphasis on operations, also for phase 2 all the necessary hardware to develop the activities will be related, the implementation of a controlled laboratory will be made with the monitoring services, correlator of events , backups and Sandbox, presenting the respective reports, evidence for the support of this applied project.

The information collection of tools that allow the development of the activities to respond to the active and proactive incidents will be carried out with the condition that these are with free software, the design of the technological structure in particular of the operations center will be elaborated, with an information gathering of the tools at the hardware level for the development of the different activities and services such as monitoring, event correlator, backup server and sandbox.

Together with a recount of the background to the creation of the first CSIRT because it arises from the need because of a computer attack by the student Robert Tappan Morris of Cornell University (United States) this worm was released on November 2, 1988, which wanted to pass the code from computer to computer and never imagined the extent of this worm-like virus capable of infecting 10% of computers at that time and even affecting NASA.

Through Conpes 3701 of 2011, he mentions within his specific achievements the creation of new instances for cybersecurity and cyber defense of the country, among which is COLCERT of the Ministry of Defense, Joint Cyber Command (CCOC), Colombian military forces and the cyber center of the national police (CCP).
In addition, this entire project will be carried out through documentary research, using information collection techniques from libraries, newspapers, internet, using critical reading, graphic records. This is a qualitative type focused from the interpretive and analysis of documents and other sources of information, making an analysis, comparison and constructive criticism between the technical design of the different CSIRT.
To have as an expected result the development and delivery of the technological structure, together with the hardware and software tools, with their respective technical documentation for the development of activities and the simulation of a controlled laboratory for functional virtualized services (monitoring, correlator of events, backups and Sandbox) all of the above for the development of CSIRT activities for the company CIBERSECURITY DE COLOMBIA LTDA.

Keywords- CSIRT, CERT, Computer Security, Incident, vulnerability.

TABLA DE CONTENIDO Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

INTRODUCCION

Con la evolución de las tecnologías de la información e infraestructura tecnológica en las últimas décadas donde las operaciones de las empresas, organizaciones públicas y privadas se rigen en un entorno digital y directamente relacionado con el internet para así de esta manera ser partícipes en la globalización y no quedándose atrás, también donde el bien más preciado por estas es la información la cual está exequible en todo momento, hace que este expuesta y vulnerable, si no se toman las medidas pertinentes para garantizar el cumplimiento de los tres pilares de la información aplicados en el SGSI (sistema de gestión de seguridad de la información) confidencialidad, integridad y disponibilidad.[4]

Es así como en la actualidad se ha aumentado la ciberdelincuencia forzando a las empresas a tomar medidas de seguridad, es ahí donde surge los CERT (Equipo de respuesta a emergencia de informática) sigla utilizada en estados unidos creador del primer de estos y posteriormente creado en Europa utilizando las siglas CSIRT (Equipo de Respuesta ante Incidencias de Seguridad Informática) encargados de dar respuestas a los incidentes reactivos y proactivos a través de herramientas tecnológicas idóneas para esta labor, además de contar con una infraestructura tecnológica bien definida, segmentada, también con un entorno de pruebas y separadas desde el mismo acceso proporcionado por un ISP de la infraestructura de producción, se resalta que este tipos de CSIRT puede ser una área adicional de una empresa tanto a nivel físico (oficinas, hardware) como lógico (Red, aplicaciones) como también puede ser una Empresa u organización que proporciona y dar respuesta a los incidentes reactivos y proactivos que para este proyecto aplicado como alternativa de grado, se tiene la empresa CIBERSECURITY DE COLOMBIA LTDA caso de estudio , la cual a través de la creación del diseño técnico permita dar desarrollo a las actividades del CSIRT y de acuerdo a los niveles de servicio contratados por sus clientes dar respuesta a los incidentes reactivos y proactivos de una manera eficiente, rápida y eficaz.

Para esto se realizara la recopilación y elaboración de un listado de las herramientas tecnológicas para realizar las actividades propias del CSIRT, teniendo en cuenta el uso de software open source, se realizará el diseño de la infraestructura tecnológica, con el mínimo de áreas requeridas (centro de datos, Investigación y desarrollo, centro de operaciones de seguridad (SOC) en el cual se hará énfasis en su descripción del diseño tecnológico, soporte de TI, logística y en las salas de capacitación y crisis) el área de operaciones de seguridad es una de las más primordiales, no restándole importancia a las otras mencionadas, ya que en esta se realiza la gestión de incidentes proactivos y reactivos, monitoreo, depuración de eventos entre otras, las anteriores actividades corresponden a las que se

[4] ISOTOOLS.ISO 27001.Pilares fundamentales de un SGSI. [En linea]. Enero 13 2015. Disponible https://www.isotools.org/2015/01/13/iso-27001-pilares-fundamentales-sgsi/

desarrollaran en la etapa 1 de este proyecto aplicado, ya para la etapa 2, estará enfocada en el cumplimiento de los objetivos 3 y 4 de este proyecto, donde se realizara la búsqueda de hardware y software para el desarrollo de los servicios que permitirán las actividades del CSIRT (web, correo, intranet, archivos, copias de seguridad, DNS, monitoreo físico y lógico, Sanbox, correlacionador de eventos, registro y seguimiento de incidentes e informática forense) también se realizara diseño lógico y presentación de un laboratorio controlado con los servicios virtualizados de monitoreo, correlacionador de eventos, copias de seguridad y Sanbox, realizando las pruebas; además se realizara la sustentación de la información técnica para la ejecución de las tareas y un video donde se explique de manera concisa esta implementación.

1 PLANTEAMIENTO DEL PROBLEMA

La Empresa CIBERSECURITY DE COLOMBIA LTDA tiene como propósito para el 2021 la implementación de un CSIRT (Equipo de Respuesta ante Incidencias de Seguridad Informática) por lo tanto va a realizar el levantamiento de información , entrega de mapa de la estructura tecnológica, informe de las herramientas de software y hardware que se requieren para proporcionar los servicios de tipo reactivo y proactivo, condicionadas a ser con Software Libre, también se requiere el diseño lógico de un laboratorio controlado con hipervisor con los servicios de monitoreo, correlacionador de eventos, Backups y un servidor de Sandbox, ni tampoco con las dependencias mínimas, como son un centro de datos, desarrollo e investigación, soporte de tecnologías de información, área donde coordina toda la operación, logística, salón de capacitación para el personal interno, salón de crisis y centro de operaciones este último se profundizara en sus detalles en el diseño y descripción de la estructura tecnológica, a continuación, se formulará el motivo por el cual es necesario la implementación de un CSIRT.

¿las empresas de Colombia han contemplado la necesidad de tener la documentación técnica para reaccionar y dar continuidad de una manera rápida y eficaz a su operación tecnológica después de un ataque informático?
Con la investigación y elaboración de la documentación del diseño tecnológico, herramientas de software, hardware, identificación, simulación de un laboratorio controlado para dar respuesta a los incidentes reactivos y proactivos se tiene como meta que la empresa en mención cuente con todo lo necesario para la implementación y puesta en marcha de un CSIRT.

Según una investigación realizada por el periódico portafolio[5] las cifras de la policía nacional que en 2017 los delitos informáticos aumentaron 28,3%, afectaron a 446 empresas del país. La suplantación del correo corporativo tuvo pérdidas por 380 millones de pesos. También mencionan varias empresas han sido víctimas de los ciberataques como es el caso de Indurtex, la cual fue víctima por un virus en uno de sus servidores y la empresa rico pollo bloqueando los computadores a través de un mensaje que pedían dinero a cambio por devolver la información en ambas empresas, solicitaban realizar el pago con Bitcoins, en ambos casos la policía nacional en este mismo artículo menciona que se abstengan de pagar para no fomentar los ciberdelitos. De la misma manera se menciona en la revista Dinero las empresas colombianas destinan un bajo porcentaje en temas de seguridad informática "Lo más grave es que no se invierte lo suficiente. Según indica el estudio, “la mitad de las organizaciones colombianas destinan solo entre 1% y 5% del presupuesto de Tecnología e Información (TI) para fortalecer el sistema de

[5] PORTAFOLIO. Empresas. El secuestro de información desangra a las empresas del país.29 de enero de 2019. [En linea]. Disponible https://www.portafolio.co/negocios/empresas/ciberataques-a-las-empresas-en-colombia-525729

ciberseguridad, lo que corresponde a 13 puntos menos que la región. Solo 10% asigna más de 11% del presupuesto de TI a mejorar la gestión del riesgo"[6].
También como lo menciona Certicamara Colombia y otros países de Latinoamérica son los que más ataques han recibido a través de sitios Web maliciosos.

"Y es que en la encuesta global The Impossible Puzzle of Cybersecurity, de la firma Sophos publicada en julio de este año y donde participaron 3100 gerentes TI de importantes organizaciones del mundo y el que incluyó por primera vez a Colombia junto con otros países de Latinoamérica, concluyó que el país es el que más ciberataque ha recibido a través de sitios web maliciosos con un 42%, seguido por Australia con el 36%y Estados Unidos con un 34%"[7].

[6] Dinero. Tendencias. 4 de cada 10 empresas en América Latina sufrieron ciberataques en los últimos años. 7 de abril 2019. [En linea]. Disponible https://www.dinero.com/tecnologia/articulo/empresas-en-colombia-sufren-de-ataques-ciberneticos-regularmente/273870
[7] Certicamara. Ciberseguridad Corporativa así está el panorama. 13 de septiembre de 2019. [En linea]. Disponible https://web.certicamara.com/sala_de_prensa/noticia/385

2 JUSTIFICACION

La relevancia del desarrollo de este proyecto tiene como finalidad el diseño técnico para la creación de un CSIRT (Equipo de Respuesta ante Incidencias de Seguridad Informática), para dar respuesta a los incidentes de la seguridad informática, con sus dependencias mínimas de hardware y software para el desarrollo de las actividades que lo competen y dar respuesta de manera eficiente, rápida y eficaz a los clientes. Lo anterior con el propósito de cumplir para el 2021 la empresa caso de estudio CIBERSECURITY DE COLOMBIA LTDA se consolide en Colombia como unas de las primeras en proporcionar servicios a incidentes de seguridad informática a través de un CSIRT, el cual tendrá beneficios detectando de manera eficaz un ataque informático, prevención de amenazas, mitigación de vulnerabilidades, capacitación del personal interno y externo en todo lo referente a la seguridad informática, garantizando la confidencialidad, disponibilidad e integridad de la información, sin ser afectada con tiempos de indisponibilidad de los servicios, desprestigio de la empresa, riesgo de daño, hurto o manipulación de sus activos y protegiendo de manera efectiva lo más preciado que es la información.

Se contara con las herramientas de software y hardware para brindar una atención oportuna a los incidentes solicitados por los clientes de acuerdo a las condiciones y restricciones, niveles de servicio definidos en lo contractual, teniendo como apoyo la documentación de las herramientas de software , hardware para realizar las tareas de forma precisa y con calidad aplicadas a su mínimo de servicios virtualizados de monitoreo, correlacionador de eventos, backup y Sandbox para ejecutar las tareas y actividades del CSIRT, de esta manera cumplir con la satisfacción y expectativas de los clientes internos , externos y consolidación de la empresa caso de estudio como una de las primeras en Colombia en brindar servicios de seguridad informática.

Se resalta el caso de éxito al implementar estrategias en materia de ciberseguridad que menciona la ORG. de Argentina ATICMA[8] con la empresa Proyectos Milemium con 15 años de experiencia en ventas, la cual estaba propensa a un ataque informático ya que su infraestructura era muy débil con una carencia de controles y que a través de una auditoria intrusiva realizada por la empresa Talsoft Security previamente autorizada , con las recomendaciones implementadas por esta se mitigo y mejoró la seguridad en esta empresa , permitiendo tener un protocolo de continuidad del negocio y mejorar su imagen a los clientes y proveedores.

Otro caso de éxito al implementar medidas de protección es la empresa Peruana Optical Networks proveedor de servicios de internet de alta Velocidad con enlaces dedicados y un Firewall de última generación el 12 de Noviembre de 2016, recibió

[8] ORG ATIGMA. Caso de éxito: Integración de Ciberseguridad a sistema de ventas multinivel. 31 de octubre de 2017. [En linea] Recuperado https://www.aticma.org.ar/caso-exito-integracion-ciberseguridad-sistema-ventas-multinivel/.

un reconocimiento a nivel internacional de la empresa líder en seguridad informática FORTINET, “La empresa peruana Optical Networks (ON) avanza a paso firme en el mercado de las telecomunicaciones, y esta vez, ha sido elegida como el “mejor canal de servicios administrativos de seguridad” por Fortinet, la compañía especializada en seguridad a nivel mundial que los reconoce por cuarta vez.”[9].

[9] ON OPTICAL NETWORKS. Optical Networks es reconocida por Fortinet como uno de sus socios de negocio más destacados. [En linea]. Disponible https://www.optical.pe/optical-networks-es-reconocida-por-fortinet-como-uno-de-sus-socios-de-negocio-mas-destacados/

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar la propuesta Técnica para la creación de un centro de respuesta a Incidentes cibernéticos para la empresa caso de estudio CIBERSECURITY DE COLOMBIA LTDA.

3.2 OBJETIVOS ESPECÍFICOS

- Entregar listado de herramientas de software y hardware para las actividades del CSIRT, aplicando al mínimo de servicios requeridos que permita dar respuesta a los incidentes proactivos y reactivos de los clientes, de la empresa CIBERSECURITY DE COLOMBIA LTDA.

- Esbozar mapa de la estructura tecnológica del CSIRT donde incluye el mínimo de dependencias para el desarrollo de las actividades.

- Presentar y sustentar laboratorio controlado con servicios virtualizados como son monitoreo, correlacionador de eventos, backup y Sandbox para ejecutar las tareas del CSIRT.

- Elaborar documentación técnica para ejecutar las tareas del CSIRT.

4 MARCO REFERENCIAL

A continuación, se realizará una descripción de los distintos marcos para el proyecto.

4.1 MARCO CONCEPTUAL

Se pretende dar claridad aquellos conceptos para que no presenten ambigüedad:
CERT: Grupo de respuesta a emergencias de informática, el uso de esta sigla está registrada en estados unidos por CERT Coordination Center (CERT/CC) .es un grupo de expertos para prevenir y dar respuesta a incidentes en lo referente a las tecnologías de información, manteniendo la seguridad de redes, computadores, también provee servicios para ayudar a robustecer la seguridad en una empresa u organización, elevando la seguridad en los sistemas para uso confiable de los usuarios, enfocado principalmente a una repuesta rápida ante un colapso informático [10]

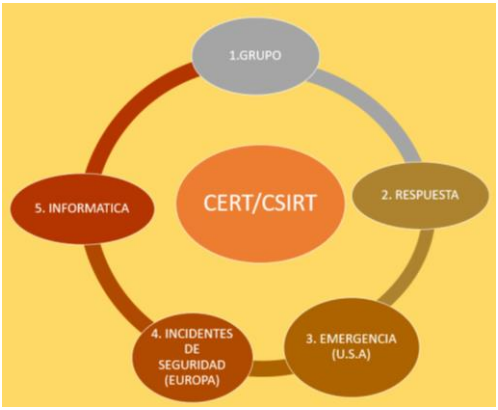
CSIRT: Grupo de respuesta a incidentes de seguridad informática, el uso de esta sigla es para Europa la cual se estableció a final de la década de los 90 convirtiéndose en sinónimo de (CERT) sobresaliendo este porque está más enfocado a la prevención. Es el mismo concepto que un CERT, su finalidad es robustecer la capacidad de prevención, detección y reacción ante un incidente informático dando respuesta oportuna en el menor tiempo posible.[11]

FIRST: Foro de Grupos de seguridad y respuesta a incidentes, es el foro mundial para interacción y colaboración de los CERT y CSIRT.
En la figura 1, se puede observar la relación que hay entre las definiciones para Estados Unidos, los incidentes lo interpretan como una (emergencia) antecedido por (informática) que combinaría emergencia informática o en Europa se cataloga como (incidente de seguridad) antecedido por (informática) que combinaría Incidente de seguridad informática, dejando por ambas partes los demás términos iguales (informática, Respuesta y equipo) lo que la interpretación no cambia el concepto general, que se conforma un equipo para dar respuesta rápida y oportuna a una situación, emergencia e incidente tecnológico.

[10] LUQUE JUÁREZ, J.M. (2019): Programa de doctorado en Ciencias Sociales. Universidad Católica de Murcia, p. 223. [En linea]. Disponible http://repositorio.ucam.edu/bitstream/handle/10952/4239/Tesis.pdf?sequence=1&isAllowed=y

[11] Ibíd., P.223.

Figura 1.CERT y CSIRT.



Fuente: Propia.

4.2 MARCO TEÓRICO

El primer CERT (grupo de respuestas a incidentes informáticos) surge de la necesidad , producto de un gusano informático creado por el estudiante Robert Tappan Morris de la universidad de Cornell (estados unidos) este gusano fue liberado el 2 de noviembre de 1988, fue el primer incidente de internet en ese tiempo se denominaba (ARPANET) se estima que infecto aproximadamente 6.000 computadoras, el 10% aproximadamente de las que existían en todo el mundo, afectando entidades gubernamentales, entre su más relevantes la NASA[12], las perdidas en ese entonces fueron de aproximadamente 1 millón de dólares, por esta razón el Gobierno de los estados unidos tomo la decisión de crear este equipo (CERT) en respuesta al incidente del gusano Morris ya que lo consideró como un ataque a la seguridad nacional aunque más adelante se pudo comprobar lo que manifestó el acusado que fue por error en el código que solo quería pasar el código de computadora en computadora y luego volverse indetectable en la Red.
La motivación principal para la creación del primer CERT fue las pérdidas del gusano Morris por aproximadamente 19 Millones de Dólares, también a futuro prevenir perdidas por ataque de virus, acceso no autorizados a la información, explotación de vulnerabilidades entre otros y proporcionar una respuesta oportuna reduciendo al máximo el tiempo de indisponibilidad de una organización pública y privada[13].

[12] DIARIO DE SEVILLA. Aniversario del gusano Morris. sábado, 21 de septiembre, 2019. [En linea]. Disponible https://www.diariodesevilla.es/efemerides/gusano-Morris-malware-internet_0_1296170714.html

[13] PERIODISTA DIGITAL. El Gusano Morris y los daños que causó en Internet. Julio 2019 [En linea]. Disponible https://www.periodistadigital.com/tecnologia/tec-internet/20190726/gusano-morris-danos-causo-internet-noticia-689404036001/

Ya para 1992 la organización holandesa Surfnet implementó el primero en Europa de nombre Surfnet.Cert, los cuales se han aumentado progresivamente en toda Europa.[14]

El 27 de abril de 2007 Estonia fue víctima de un ciberataque, colapsando en todo el país el correo electrónico, bancos, cajeros automáticos, entidades gubernamentales, medios de prensa, debido a un incremento del tráfico de internet de proporciones nunca antes vistas utilizando Botnets (Redes automatizadas de robots) enviaron spam y pedidos online (produciendo caos y confusión en la nación) aunque el ataque fue evidenciado que se produjo desde IPs rusas no se pudo comprobar que el Gobierno de este país estuvo comprometido, porque también los ciberdelicuentes se sumaron al ataque, durando este varias semanas, actualmente producto de este ataque cibernético estonia se ha consolidado como la meca de la ciberseguridad en Europa.[15]

El 10 de marzo de 2010, la guardia española con el apoyo del FBI y panda security, detuvo a 3 españoles que tenían controlados a 13 millones de computadoras zombi sin que lo dueños de estos lo supieran, solo en España 800.000, obteniendo datos personales y financieros. Su poder de destrucción a nivel de ciberseguridad pudo haber sido mayor que los ocasionados en 2007 en estonia, afectando a 190 países de los cuales entre ellas más de 1000 empresas, Colombia ocupo el quinto país y segundo en Latinoamérica de los más afectados con este ataque.[16]

El Gobierno Colombiano al evidenciar las debilidades con el ciberataque de los Botnets Mariposa y teniendo como fundamento que no tienen la capacidad de hacerle frente a una amenaza en ciberseguridad que involucre la seguridad nacional lo incluyen en el plan nacional de desarrollo del 2010 nombrado “Prosperidad para Todos”, como parte del Plan Vive Digital.[17] De aquí surge la iniciativa y el capital para realizar la implementación de un CERT para Colombia de nombre COLCERT.

4.3 MARCO LEGAL

Conpes 3701 de 2011 Menciona dentro de sus logros específicos la creación de nuevas instancias para ciberseguridad y ciberdefensa del país entre las cuales se encuentra COLCERT del ministerio de defensa, Comando conjunto cibernético

---

[14] LINTI, Laboratorio de Investigación en Nuevas Tecnologías Informáticas, Facultad de Informática, Universidad Nacional de La Plata. Pág. 33. [En linea]. Disponible http://sedici.unlp.edu.ar/bitstream/handle/10915/19431/Documento_completo.pdf?sequence=1&isAllowed=y

[15] BBC. News-Mundo. Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país. Mayo 6 2017. [En linea]. Disponible https://www.bbc.com/mundo/noticias-39800133

[16] DIARIO EL PAÍS. Tecnología. Cae la red cibercriminal 'Mariposa', que controlaba millones de ordenadores 'zombis' en 190 países. Marzo 3 de 2010. [En linea]. Disponible https://elpais.com/tecnologia/2010/03/02/actualidad/1267524068_850215.html

[17] MINTIC. Compes 3701, pág. 6. Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación. Bogotá D.C., 14 de julio de 2011. [En linea]. Disponible https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

(CCOC) fuerzas militares de Colombia y el centro cibernético de la policía nacional (CCP).[18]
MINTIC Decreto 0032 de 2013 creación de la comisión nacional digital y de información estatal para uso de manera efectivo de la información del país.[19]
Conpes 3854 de 2016 Menciona los logros alcanzados en materia de ciberseguridad y ciberdefensa con la creación de COLCERT del ministerio defensa, el CCOC de las fuerzas militares de Colombia y el CSIRT PONAL de la policía nacional.[20]

Ley 1273 de 2009 en la cual contempla un nuevo bien Jurídico el cual su finalidad es proteger la información, preservar su integridad en el ámbito de las TICs mencionando en el:

Artículo 269ª: Acceso abusivo a un sistema informático.

Articulo 269b: Impedir el acceso a un sistema Informático o impedir su correcto uso.

Articulo 269c: Interceptar datos sin la debida autorización de la entidad o Judicial.

Articulo 269d: Destruir, dañar, alterar la información, borrar de forma física o lógica.

Articulo 269e: Uso de software Malicioso.

Articulo 269g: Realizar suplantación de datos personales con fines delincuenciales.

Articulo 269I: Robo a través de medios informáticos suplantando sistemas de autenticación según lo menciona el artículo 239.

Los anteriores delitos que se mencionan en la Ley 1273 de 2009, están relacionados con los ataques informáticos que pueden realizar los ciberdelicuentes y su vez están expuestas las empresas del ámbito privado y gubernamental por esta razón es sumamente relevante para las funciones que realiza el CSIRT ya que una de sus funciones principales es prevenir, mitigar y dar respuestas a los incidentes ya sean reactivos reportados por los usuarios o proactivos detectados por el departamento del CSIRT. [21]

---

[18] MINTIC. Op. cit. p. 20.

[19] MINTIC. Decreto 0032 de 2013. "Por la cual se crea la Comisión Nacional Digital y de Información Estatal". [En linea]. Disponible https://www.mintic.gov.co/portal/604/articles-3602_documento.pdf

[20] REPÚBLICA DE COLOMBIA DEPARTAMENTO NACIONAL DE PLANEACIÓN. Bogotá D.C., 11 de abril de 2016 Mintic. Compes 3854, pág. 13. Consejo Nacional de Política Económica y Social. [En linea]. Disponible https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

[21] COLOMBIA. MINISTERIO DEL INTERIOR Y DE JUSTICIA. Ley 1273 de 2009 (5, enero, 2009). Diario oficial Bogotá D.C., 2009 No 47.223 {En línea} {22 de abril de 2016} [En linea]. Disponible

4.4 MARCO TECNOLÓGICO

Se utilizará software open source para gestionar los incidentes proactivos y reactivos manteniendo los principios, se expresa claramente el significado de software libre, es la libertad en que los usuarios tienen para la ejecución, el copiado, la distribución, el estudio, la edición, las mejoras del software. Con las siguientes libertades:

Libertad 0: Ejecución del programa sin importar el objetivo.
Libertad 1: Acceso al código fuente para estudiarlo y de esta manera acoplarlo a las necesidades.
Libertad 2: Libre distribución de copias para ayuda común.
Libertad 3: Acceso al código fuente para realizar mejoras y ayudar a la comunidad haciendo estas públicas.[22]

A continuación, se realizó un listado de las herramientas de software libre para cubrir los servicios que brindará el CSIRT, relacionados en la tabla 1.

Tabla 1. Herramientas de software libre para un CSIRT.

Nombre del servicio	software libre	Descripción	Sitio web descarga e instalación
Web	Apache, php y msql	Sitio Web	http://httpd.apache.org/docs/2.4/es/install.html[23]
Correo Institucional	Zimbra	Servidor de correo.	https://www.zimbra.com/downloads/[24]
Intranet	Joomla	Sitio web privado para una empresa.	https://downloads.joomla.org/co/[25]
Archivos	Samba	Servicios de gestión de archivos.	https://unmtrabajos.blogspot.com/2019/01/servidor-samba-ubuntu-1804-lts-tutorial.h[26]

http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[22] STALLMAN, R. M. (2004). Software libre para una sociedad libre. Introducción de Lawrence Lessig (P.45). [En linea]. Disponible https://biblioweb.sindominio.net/pensamiento/softlibre/softlibre.pdf

[23] APACHE. HTTP SERVER PROJECT. Compilar e instalar. [En linea]. Disponible http://httpd.apache.org/docs/2.4/es/install.html

[24] ZIMBRA A SYNACOR PORDUCT. Zimbra Downloads. [En linea]. Disponible https://www.zimbra.com/downloads/

[25] JOOMLA. Joomla Downloads. [En linea]. Disponible https://downloads.joomla.org/co/

[26] UNM TRABAJOS. Administración de Sistemas operativos. Servidor Samba Ubuntu 18.04 LTS, Tutorial. [En linea]. Disponible https://unmtrabajos.blogspot.com/2019/01/servidor-samba-ubuntu-1804-lts-tutorial.html

Copias de Seguridad	Veeam Backup & Replication C.E.	Copias de seguridad automatizado.	https://www.veeam.com/es-lat/downloads.html[27]
DNS	DNS	Resolución de nombres.	https://unmtrabajos.blogspot.com/2019/01/servidor-dns-ubuntu-1804-lts-tutorial.html[28]
Monitoreo	Pandora FMS	monitoreo de dispositivos en una red.	https://pandorafms.org/features/free-download-monitoring-software/[29]
Sandbox	Firejail	Iniciar software en ambiente controlado	https://geekland.eu/firejail-sandbox-para-linux/[30]
Correlacionador de Eventos	Alien Vault OSSIM	Correlacionador de eventos	https://www.alienvault.com/products/ossim[31]
Registro y seguimiento de Incidentes	Mantis BT	Registro y seguimiento de Incidentes	https://www.mantisbt.org/download.php[32]
Dispositivos Conectividad	Pandora FMS	monitoreo de Red.	https://pandorafms.org/features/free-download-monitoring-software/[33]
Informática forense	Sans Dfir	Análisis forense	https://digital-forensics.sans.org/[34]

Fuente: Propia.

4.5 MARCO METODOLÓGICO

Esta se realizó por medio de la investigación documental, utilizando técnicas de recopilación de información de bibliotecas, periódicos, internet, utilizando la lectura crítica, registros de gráficos.

Esta es una investigación de tipo cualitativa enfocada desde lo interpretativo y análisis de documentos y otras fuentes de información.

---

[27] VEEAM. Descargar productos de Veeam. [En linea]. Disponible https://www.veeam.com/es-lat/downloads.html

[28] UNM TRABAJOS. Administración de Sistemas operativos. Servidor Samba Ubuntu 18.04 LTS, Tutorial. [En linea]. Disponible https://unmtrabajos.blogspot.com/2019/01/servidor-dns-ubuntu-1804-lts-tutorial.html

[29] PANDORA FMS.Pandora FMS Community Downloads. [En linea]. Disponible https://pandorafms.org/features/free-download-monitoring-software/

[30] GEEKLAND. Blog de Tecnología. Firejail, un sandbox para Linux para ejecutar programas de forma segura. [En linea]. Disponible https://geekland.eu/firejail-sandbox-para-linux/

[31] AT&T .Alienvault is now AT&T cybersecurity. [En linea]. Disponible https://www.alienvault.com/products/ossim

[32]Mantis Bug tracker. MantisBT 2.22.1. [En linea]. Disponible https://www.mantisbt.org/download.php

[33] PANDORA FMS.Pandora FMS Community Downloads. [En linea]. Disponible https://pandorafms.org/features/free-download-monitoring-software/

[34] SANS DFIR. Digital Forensics and Incident Response. [En linea]. Disponible https://digital-forensics.sans.org/

Por medio de esta metodología se hizo un análisis, comparación y críticas constructivas entre el diseño técnico de los diferentes CSIRT.

Se tuvo como referencia principal las fuentes de información como son los materiales electrónicos y gráficos, aplicando el uso de fuentes primarias y secundarias.

Garantizando su autenticidad, confiabilidad del autor o entidad origen de esta fuente y relevancia en cuanto al diseño de un CSIR, también que la documentación no fuese alterada.

De igual manera se realizó un análisis de la credibilidad de las fuentes para comprobar su veracidad y exactitud, así mismo que la información que provee el autor sea objetiva, la relevancia del documento aplicado a este diseño, su significado con la claridad de la información contenida.

Durante el desarrollo de la investigación documental en donde a las fuentes no se pudieron aplicar los elementos de **autenticidad, credibilidad, representatividad y significado**, se aplicará lo inverso llamado método de confianza donde se

comprueba que esta fuente no es auténtica, no es creíble y no es representativa. [35] Además, se realizó el análisis e interpretación de la información, una vez se depuro, selecciono y clasifico, se inició la construcción del proyecto de manera jerárquica como el cuerpo, tema, subtemas y de esta manera se pasó al parte final para la construcción de las conclusiones, recomendaciones y finalizar del proyecto.

4.5.1 Técnica de recolección de información. La técnica que se utilizó para la recolección de información en este proyecto aplicado es el análisis documental realizando su estudio de dos formas[36]:

4.5.1.1 Análisis formal. Permite su identificación de forma única ya sea física o digital, es la descripción de la bibliografía del documento para saber su fuente principal.

[35] INVESTIGACIÓN CIENTÍFICA. ¿Qué es la investigación documental? Definición y objetivos. Investigación Documental. [En linea]. Disponible https://investigacioncientifica.org/que-es-la-investigacion-documental-definicion-y-objetivos/

[36] PROFESORA ASOCIADA CASTILLO. L. Universidad de Valencia. Biblioteconomía. Segundo cuatrimestre. Curso 2004-2005. Tema 5. Análisis documental.pp. 5-9. [En linea]. Disponible https://www.uv.es/macas/T5.pdf

4.5.1.2 Análisis interno. Aplica sobre el análisis del documento, representa la información ya depurada, entre esta se tienen:

- La indexación:

Selecciona términos para representar el contenido de un documento, se puede indizar de dos maneras utilizando palabras claves para designar diferentes aspectos de los temas ya sea por extracción o derivación, en la primera tenemos los términos y en la segunda utilizando términos que no están en el texto para estos se utiliza diccionarios de sinónimos y especializados.
Otra manera es por resumen, que es la representación del contenido de forma abreviada sin realizarla de forma crítica, entre los más importantes tenemos:

- Descriptivo:

Es el resumen que hace referencia al tipo de escrito y los temas que se abordan.

- Analítico:

Dedicados a un solo tema ya que facilita extraer la mayor cantidad de información cualitativa y cuantitativa.

- Selectivo:

Solo toma partes que son esenciales en un tema determinado.

- Clasificación

Se organiza por clases según el contenido del escrito, texto, documento, revista entre otros.

Su principal objetivo es agrupamiento en materia específicas, que facilita el organizar, almacenar y recuperación de estos clasificados en temas más globales, su característica principal es su estructura en jerarquías de los más global a lo más específico.

5 DESARROLLO DE ACTIVIDADES EN UN CSIRT

Entre las diferentes actividades se encuentran la respuesta a incidentes de tipo:

5.1 REACTIVOS

Estos surgen de un evento inesperado, generado por algún colaborador de la empresa al detectar algo inusual o anomalía relacionada con la infraestructura tecnológica, como por ejemplo cuando el ciberdelincuente ha explotado una vulnerabilidad, infección de los ordenadores por un código malicioso o virus, detección de intrusos en los sistemas y en la red entre otros.

A continuación, se relacionan estos tipos de Incidentes:

- Alertas detectadas o reportadas.
- Análisis, soporte y respuesta en sitio a incidentes.
- Coordinación de incidente.
- Análisis y respuesta a vulnerabilidades.
- Coordinación de vulnerabilidades.

5.2 PROACTIVOS

Su finalidad es bridar información a los colaboradores de la empresa para proteger los recursos tecnológicos, haciendo énfasis en las recomendaciones y buenas prácticas, también para mejorar la seguridad y prevenir ataques que pueden suceder por una acción de un empleado al desconocer la manera correcta de hacerlo, como por ejemplo: un empleado por falta de capacitación abre un correo de un contacto desconocido y por curiosidad abre también el adjunto de éste ejecutando de forma involuntaria un virus, el cual puede permitir un ciberataque a toda la organización.

Como complemento incluir auditorias, estándares de las correctas configuraciones con la creación de manuales, evaluaciones y mantenimiento de las herramientas utilizadas entorno a la seguridad informática.

5.3 HERRAMIENTAS DE SOFTWARE OPEN SOURCE

Se utilizará software open source para gestionar los incidentes proactivos y reactivos manteniendo los principios, que expresa claramente el significado de

software libre, es la libertad en que los usuarios tienen para la ejecución, el copiado, la distribución, el estudio, la edición, las mejoras de mejorar el software. Con la libertades que este contiene al ejecutar un programa independiente del uso, ya que permite acceder al código original haciendo mejoras, poder analizarlo y amoldarlo a las necesidades, distribuir las copias y realizar su publicación todo esto en beneficio de la comunidad.[37]

Como se puede observar en el listado de las herramientas de software libre para cubrir los servicios que brindara el CSIRT, relacionados en la tabla 1, que se mencionan en el marco tecnológico, a continuación, se realizará una descripción de cada uno de estos servicios y la función que cumplen y el tipo de software para este:

5.3.1 Servicio Web. Tiene la funcionalidad de permitir la publicación de todo lo referente a las alertas semanales por medio de su boletín en lo referente a la seguridad informática, tomando como modelo a seguir el sitio web de COLCERT, por medio de su boletín semanal realiza un resumen en cuanto brechas de seguridad publicadas en el (NIST) en su base de datos (NVD) aplicando una puntuación y un nivel de severidad en categorías alta, media y baja.[38]

- Contendrá un servidor en Apache última versión Apache httpd 2.4.41 Released. [39]

- Un lenguaje de programación del sitio web en PHP última versión 7.3.11 Released[40]

- Para la base de datos se utilizará Mysql última versión 8.0. [41]

En la siguiente imagen se puede observar desde el año 2010 hasta el 21 de mayo de 2019, en cuanto a servidores web el competidor de apache es Nginx, mostrando una curva ascendente, pero lo que hace sobresalir a apache es que está incluido como un rol en la mayoría de las distribuciones de Linux como es el caso de Ubuntu, CentOS, Debian entre otros.

---

[37] STALLMAN, R. M. (2004). Software libre para una sociedad libre. Introducción de Lawrence Lessig (P.19). [En linea]. Disponible https://biblioweb.sindominio.net/pensamiento/softlibre/softlibre.pdf

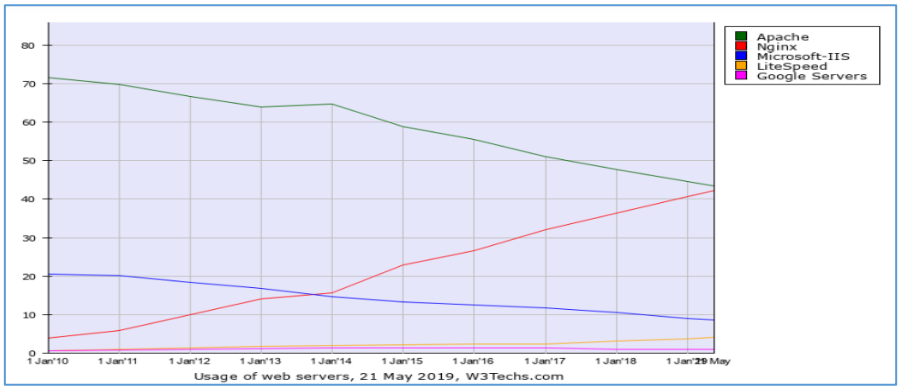
[38] CISA CYBER INFRAESTRUCTURE. (2019, Noviembre 25). US CERT GOV. Official website of the Department of Homeland Security: [En linea]. Disponible https://www.us-cert.gov/ncas/bulletins/sb19-336

[39] APACHE. HTTP Server Project. Apache httpd 2.4.41 Released 2019-08-14. [En linea]. Disponible https://httpd.apache.org/

[40] PHP. News Archive – 2019. PHP 7.3.11 Released. [En linea]. Disponible https://www.php.net/archive/2019.php#2019-10-24-2

[41] MYSQL. Documentation. Changes in MySQL 8.0.18 (2019-10-14, General Availability). [En linea]. Disponible https://dev.mysql.com/doc/relnotes/mysql/8.0/en/news-8-0-18.html

Figura 2. Comparativo Web server apache vs Nginx.



Fuente: JANKOV, Tonino. Kinsta. Nginx vs Apache: Lucha entre Servidores Web. [En linea]. Disponible https://kinsta.com/es/blog/nginx-vs-apache/

5.3.2 Servicio de Correo. Este será el encargado de la administración de las todas las cuentas, grupos de correo, buzones, y mensajes electrónicos de la empresa para esta labor se utilizará Zimbra en su última versión 8.8. Open source Edition.

5.3.3 Servicio de intranet. Es el gestor de contenidos dinámicos e interactivos Joomlaa última versión 3.9.12. donde se publicará toda la información relevante para todo lo relacionado con el CSIRT.[42]

Se eligió a Zimbra como la herramienta para proveer el servicio del CSIRT por sus conectores de clientes de correo más completo, según se describe en el siguiente cuadro comparativo.

Figura 3. Cuadro comparativo de conectores para los clientes de correo.

Conectores para clientes de correo	Zimbra	OX open-xchange	SCALIX a xandros company
Outlook 2003 / 2007	Completa	Sólo PIM	Completa
iSync Mac	Completa	Completa	No disponible
Thunderbird	IMAP (PIM con Funambol)	IMAP (PIM con Funambol)	IMAP
KDE Kontact / Kmail	Sólo IMAP	Completa	Sólo IMAP
Novell Evolution	Completa	IMAP + Calendario	Completa

Fuente: QUERYSYSTEM. Comparativa de soluciones Open Source Groupware. Comparativa de las soluciones. [En linea]. Disponible https://quersystem.com/docs/Comparativa%20soluciones%20Groupware%20(Zimbra,%20Open-Xchange,%20Scalix).pdf

[42] JOOMLA. Downloads. [En linea]. Disponible https://downloads.joomla.org/co/

5.3.4 Servicio de archivos. Se utilizará Samba como protocolo para la administración de archivos, incorporado en la capa de aplicación del modelo OSI. Esta permite la comunicación entre host de varios sistemas operativos como por ejemplo: Windows y Linux, de manera que para el usuario final su conexión es trasparente una de sus características es poder unirse a un directorio activo por medio del protocolo LDAP y autenticación por kerberos.[43]

5.3.5 Servicio de Copias de Seguridad. Teniendo en cuenta que ante un ciberataque la información está expuesta a ser alterada, dañada, indescifrable, hurtada, las copias de seguridad tienen una función muy relevante a la hora de restablecer los servicios y plan de continuidad del negocio es por eso que se eligió teniendo en cuenta el cuadrante mágico de Gardner para el 2020, donde la solución de Veeam Backup se sitúa como líder, como se muestra en la figura 4.

Figura 4. Magic Quadrant for data center backup and recovery solutions.

Fuente: VEEAM. Cuadrante mágico de Gartner 2020. [En linea] Disponible https://www.veeam.com/es-lat/2020-gartner-magic-quadrant.html

[43] RED HAT ENTERPRISE. Linux 4: Manual de Referencia. (n.d). Capítulo 14. Samba. Web.mit.edu. [En linea]. Disponible https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-samba.html

En el siguiente cuadro comparativo se puede apreciar las características más relevantes entre la Herramienta Veeam Backup frente a Comvault y veritas technology líderes a nivel mundial según Figura 4. “Magic Quadrant for data center backup and recovery solutions”. Aunque las 2 últimas no cuentan con una versión sin costo o Community Edition que cuente con características de automatización, Cifrado, Deduplicacion, laboratorios de pruebas que garantice las restauraciones de los backups a nivel corporativo.

Tabla 2. Comparativo herramientas de Backup.

Características	Veem Backup C.E.[44]	Coomvault Backup[45]	Veritas Technology Backup Exec [46]
Implementación	Practica e intuitiva	Compleja se requiere capacitación ..	Implementación sencilla.
Administración	Interfaz web fácil de usar al programar backup y configuraciones por medio de asistentes. Compatible con Hypervisores Vmware y Hyper-V.	Intuitiva por interfaz web. Plataforma única local y en la nube.	Única consola Web y configuración con asistentes.
Detección de Rasomware	Backup cifrados Libres de Malware	Cifrado en reposo y en caliente.	Función que impide modificaciones por procesos sin autorización.
Plataformas soportadas	Windows y Linux	Unix, Linux, Windows y macintosh.	Windows, Unix y Linux.
Backup y Restauración .	Automatizada	Automatizada	Automatizada

[44] VEEAM. Veeam Availability Suite. Comparación de productos. [en linea] Disponible https://www.veeam.com/es-lat/products-edition-comparison.html

[45] COMMVAULT. Commvault Backup & Recovery. [En linea] Disponible https://www.commvault.com/complete-data-protection/backup-and-recovery

[46] VERITAS. Backup Exec. [En linea] Disponible https://www.veritas.com/content/dam/Veritas/docs/data-sheets/V1001_GA_ENT_DS_Backup-Exec.pdf

Opciones de almacenamiento	Discos, Biblioteca de cintas físicas y Virtuales.	Discos o RAID, cintas, en la nube y Red NAS.	Nube, disco y cintas.
Backup y restauración en la nube	Amazon EC2 y Office 365.	Principales proveedores de la Nube.	Nube privada y pública.
Restauración Granular y confiable.	Vms, Vms Disk y archivos. Testeada en los laboratorios de Veeam.	Vms, Vms Disk y archivos, Testeo sin información disponible.	Nube, disco y cinta. Testeo sin información disponible.
Deduplicacion	Incluida	Incluida	Incluida.

Fuente: Propia.

Se utilizará la versión Veeam Backup & Replication C.E. 9.5, que permite realizar copias de seguridad hasta 10 máquinas virtual sin costo.[47]

5.3.6 Servicio de DNS. En toda organización es necesario tener activo el servidor de Dns (Domain Name System) para poder validar continuamente las comunicaciones a través de red interna con la externa y viceversa, para el caso de los dns internos estos validan continuamente cada servicio a que dns corresponde y de manera externa cuál de estos son consultados en internet, entonces este hace de intermediario en los servicios existentes y el internet, haciendo la traducción entre las direcciones IPS y los nombres de dominio.

Como este es un servicio y no una aplicación estará contenida dentro de una distribución de Linux Ubuntu Server 18.4 LTS. La cual cuenta con soporte hasta abril 2023.[48]

5.3.7 Servicio de monitoreo. Uno de los servicios más importantes en un CSIRT, es este servicio ya que se tiene las evidencias e información de primera mano y en tiempo real de un incidente ya sea proactivo o reactivo, permite tener una respuesta rápida y oportuna por este motivo lo importante de tener esta herramienta optimizada y parametrizada de forma correcta, con la aplicación PANDORA FMS[49]

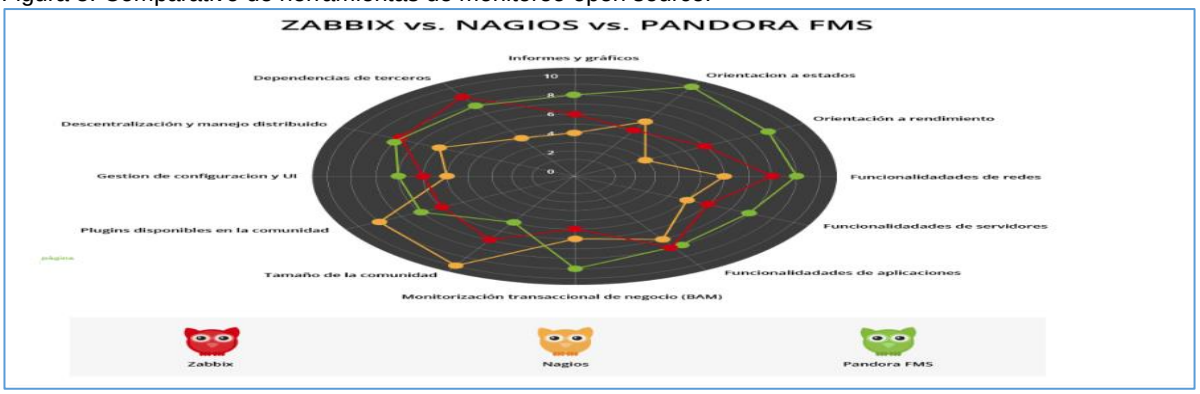
En la siguiente figura se puede observar como la herramienta de monitoreo Pandora FMS, sobresale en una escala de 0 a 10, en orientacion a estados, rendimiento, funcionalidades de redes y servidores de sus compentidores Nagios y Zabbix.

[47] VEEAM. (2019). Veeam Backup & Replication Community Edition 9.5. [En linea]. Disponible https://www.veeam.com/es-lat/virtual-machine-backup-solution-free.html

[48] CANONICAL. Ubuntu. Ubuntu Server 18.04.3 LTS. [En linea]. Disponible https://ubuntu.com/download/server

[49] PANDORA FMS. Monitoring Pandora: Documentation. Parte 2 Instalación y configuración. [En linea]. Disponible https://pandorafms.com/docs/index.php?title=Pandora:Documentation

Figura 5. Comparativo de herramientas de monitoreo open source.



Fuente: PANDORA FMS. Zabbix vs Nagios vs Pandora FMS: una comparativa en profundidad. [En linea]. 17 de junio 2016. Disponible https://pandorafms.com/blog/es/zabbix-vs-nagios-vs-pandorafms-una-comparativa-en-profundidad/

En el siguiente cuadro comparativo tomando como referencia la figura anterior en el cual se avalúa características relevantes en una escala de 0 a 10 siendo el anterior el valor más alto, se evidencia que Pandora FMS promedia un valor más alto en comparación a Nagios y Zabbix.

Tabla 3. Cuadro comparativo cuantitativo herramientas de Monitoreo.

Característica	**Pandora FMS**	**Nagios**	**Zabbix**
Informe y gráficos	8	4	6
Orientación a estados	10	6	5
Orientación a rendimiento	9	3	6
Funcionalidades de redes	9	6	8
Funcionalidades de servidores	8	5	6
Funcionalidades de aplicaciones	8	7	8
Monitorización transaccional del negocio (BAM)	9	6	5
Tamaño de la comunidad	5	10	7
Plugins disponibles en la comunidad	7	9	6
Gestión de configuración y UI	7	5	6

Descentralización y manejo distribuido	8	6	8
Dependencias de terceros	8	4	9
Promedio	8	6	7

Fuente. PANDORA FMS. Zabbix vs Nagios vs Pandora FMS: una comparativa en profundidad. [En linea]. 17 de junio 2016. Disponible https://pandorafms.com/blog/es/zabbix-vs-nagios-vs-pandorafms-una-comparativa-en-profundidad/

A continuación, otras características para realizar la comparación de la herramienta Pandora FMS vs Nagios y Zabbix ratificando la elección de Pandora FMS como herramienta de monitoreo para el CSIRT.

Tabla 4. Características de comparación herramientas de Monitoreo.

CARACTERÍSTICA	**PANDORA FMS**	**NAGIOS**	**ZABBIX**
Lanzamiento	14 octubre de 2004	14 marzo de1999	2001
Última versión estable	5 mayo 2020	19 agosto 2015	2020
Lenguaje de programación	Perl,PHP,C++,Javascript	Perl y C	C,PHP y JAVA
S.O. Compatibles	Linux, Windows y FrreBSD	Linux y Windows	Multiplataforma
Licencia	GNU GPL	GPL v2	GNU GPL
Ventajas	• Arquitectura Modular. • Tiene gran variedad de plugins y módulos para utilizarlos de forma intuitiva. • Configuración y administración por medio de Interfaz web y Wizards. • Generación de informes intuitivos y se puede visualizar más información rápida y en tiempo real.	• La aplicación es más liviana ya que la mayoría de su código es escrito en C. • Su comunidad es la más grande que Pandora y Zabbix.	• Sistema definido por plantillas. • Plugin para informes viene incluido con la aplicación.

Desventajas	• Tiene menos plugins que Nagios. • No es muy conocido en el mundo de TI como es el caso de Nagios.	• Para la configuración del usuario depende de scripts y procesos manuales y desarrollos a la medida. • Se requiere personal con experticia para la administración de la herramienta. • Uso de add-on de terceros para compensar funcionalidades. • Para los informes se debe realizar con plugins de terceros la personalización de estos es reducida .	• Necesita la instalación del múltiples plugins para tener todo el conjunto de funcionalidades. • No es compatible con Oracle, Exchange, Active directory entre otras.

Fuente. PANDORA FMS. Zabbix vs Nagios vs Pandora FMS: una comparativa en profundidad. [En linea] Disponible: https://pandorafms.com/blog/es/zabbix-vs-nagios-vs-pandorafms-una-comparativa-en-profundidad/

5.3.9 Servicio de Sanbox. Permite ejecutar programas de forma segura en un entorno aislado de la red de producción, esto sucede cuando se tienen programas de terceros o desarrollo de software que se necesita validar el impacto que se tendrá en el entorno de producción, los ambientes de virtualización sirven como un ejemplo .[50]En la tabla 1, se encuentra relacionada la herramienta de software para esta labor de nombre Firejail.

En el siguiente cuadro comparativo se identifican las características, ventajas y desventajas de Firejail con otros Sandbox.

Tabla 5. Comparación Sanbox Firejail vs JS-Interpreter.

Características	FIREJAIL[51]	JS-Interpreter[52]	Cuckoo[53]
Ventajas	Usa espacios de nombres seccomp-bpf. Permite y restringe aplicaciones por medio de listas blancas y negras. Restringe la interacción entre 2 aplicaciones, aunque estén en el mismo contenedor. Basado en el kernel de linux por lo cual no depende de la distribución para su instalación.	Mundialmente conocido este lenguaje de programación. Lenguaje de bajo nivel para su instalación y configuración se necesita un nivel avanzado en Java. Ejecución aislada del entorno principal. No utiliza listas negras en vez de estas crea su propia MV sin APIs Externas. Compatibilidad con múltiples	Analiza en busca de malware archivos de dudosa procedencia a través de los exploradores o en entornos virtuales. Multiplataforma (Windows, linux, Mac y Android). Analiza el tráfico de Red SSL/TLS. Analiza la memora RAM de los Vms. Se puede personalizar su entorno e informes debido a las

[50] NORMAL POPAYÁN. Recursos Normal Popayán. Retrieved from Aislamiento de procesos (informática). [En linea]. Disponible http://recursos.normalpopayan.edu.co:8983/wikipedia_es_all_2017-08/A/Aislamiento_de_procesos_(inform%C3%A1tica).html

[51] FIREJAIL. Features. Firejail Security Sandbox. [En linea] Disponible https://firejail.wordpress.com/features-3/

[52] GITHUB. FRASER. N. Documentation. [En linea] Disponible https://github.com/NeilFraser/JS-Interpreter

[53]CUCKOO. Automated Malware Analisys. [En linea] Disponible https://cuckoosandbox.org/

	Cuenta con documentación y manuales en su paginas oficiales.	navegadores Web.	bondades del Open Source.
Desventajas	Su configuración es de bajo nivel por lo cual se necesita un mínimo de conocimientos en la herramienta y sistema operativo linux.	La implementación, administración y uso de la herramienta requiere conocimientos del lenguaje de programación JAVA.	

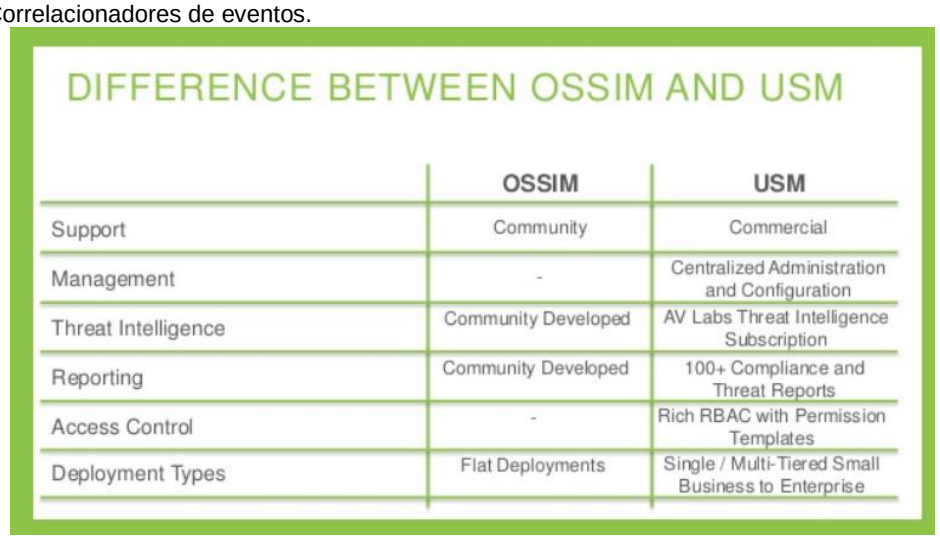
Fuente. Propia.

5.3.10 Correlacionador de Eventos. Es un servicio fundamental para la seguridad de la información donde su función principal es la administración y análisis de eventos de todos los dispositivos de la red para buscar patrones, similitudes, para la detección de vulnerabilidades y ataques, también descarta los falsos positivos para ir optimizando el análisis de estos. Se realizará por medio de la herramienta de software Alien Vault OSSIM [54]

En el siguiente cuadro comparativo que se muestra en la figura 6, resalta que está respaldada por una comunidad de desarrolladores y no genera costo comercial ya que está cubierta bajo GNU/GPL en comparación con la herramienta USM.

[54] AT&T. Alienvault is now AT&T cybersecurity. [En linea]. Disponible https://www.alienvault.com/products/ossim

Figura 6. Correlacionadores de eventos.



Fuente: SLIDESHARE. Difference between Ossim and Usm. [En linea] p.16. Disponible https://pt.slideshare.net/alienvault/ossim-user-training-get-improved-security-visibility-with-ossim?related=1

En el siguiente cuadro comparativo se relaciona las diferentes características, ventajas y desventajas con otras herramientas para analizar y correlacionar los eventos por su implementación práctica, configuración y administración intuitiva se seleccionó la herramienta AlienVault Ossim.

Tabla 6. Cuadro comparativo herramienta correlacionador de eventos.

Características	AlienVault Ossim	Wazuh	Preludio	Sagan
Licencia	GNU Gpl	GNU Gpl v.2.	GNU Gpl v.2. y software propietario	GNU Gpl v.2.
Sistema Operativo	Linux	Multiple plataforma	Linux	Unix
Ventajas	Administración y configuración intuitiva. Su base está desarrollada sobre productos probados de código abierto (Snort, Nagios, OSSEC, Openvas) Tiene una comunidad grande	Admite infraestructura de Docker. Integración con splunk.	Continuo desarrollo desde 1998. Admite diferentes formatos de registro.	Arquitectura multiproceso.

	de usuarios y desarrolladores.			
Desventajas	No cuenta con administración de infraestructura en la Nube.	Arquitectura compleja requiere de la implementación completa de elastic stack.	Limitado en rendimiento ,características y seguridad.	Comunidad pequeña. Instalación compleja lo cual requiere la construcción de este desde la fuente.

Fuente. LOGDNA. Open Source SIEM Solutions. [En linea] Disponible https://logdna.com/open-source-siem-tools/

5.3.11 Servicio Registro y seguimiento de Incidentes. Una de sus funciones más importantes para el CSIRT es dar una respuesta rápida y oportuna a sus incidentes reactivos y proactivos para llevar a cabo de una manera eficiente la gestión de casos, tener trazabilidad y seguimiento de estos se utilizará Mantis Bug Tracker[55]

A través del siguiente cuadro comparativo de la figura 7, se destaca que las herramientas para esta labor son de licencia open source es Bugzilla y Mantis sin embargo esta última está desarrollada en lenguaje php permitiendo más fácil la integración con la base de datos msql y HTML, además que existe mayor documentación para la solución de errores que el lenguaje de programación Perl con el cual está desarrollada Bugzilla.

Figura 7. Comparativo herramientas registro y seguimiento de incidentes.

Fuente: COMMON NINJA. Jira vs Mantis vs Bugzilla. [En linea] Disponible https://tables.commoninja.com/tables/single/124149

[55] Mantis. Bug tracker. MantisBT 2.22.1. [En linea]. Disponible https://www.mantisbt.org/download.php

5.3.12 Servicio Dispositivos de Conectividad. Para estar al tanto de la disponibilidad, alarmas y errores de los dispositivos de la red se utilizará PANDORA FMS, ya que este permite un monitoreo constante.[56]

En la figura 5. Se puede apreciar la gráfica comparativa con otras herramientas open source similares donde se destaca esta.

5.3.13 Informática forense. Es un servicio exclusivo que presta el CSIRT, el cual permite a través de análisis de los diferentes dispositivos electrónicos utilizados o que estén relacionados o involucrados en un ciberataque extraer evidencias contundentes para resolver estos para que sea la ruta hacia la verdad, para presentarlos como pruebas ante un juez y de esta manera por la parte judicial se tomen las medidas y castigos a los ciberdelicuentes, se utilizara para esto la herramienta de software Sans Dfir.[57]

6 MAPA DE LA ESTRUCTURA TECNOLÓGICA

6.1 INSTALACIONES DE UN CSIRT

La información que este va a gestionar es bastante sensible, por lo cual implica tomar medidas para tener restricciones de acceso en cuanto a la parte de sus instalaciones, fisco y lógico en este último no puede estar visible para otras redes abiertas sin que se tomen las diferentes medias de prevención.

Con esto se minimiza el acceso a los recursos y a la información de igual manera debe contar con servicio de vigilancia (24x7x365) esto quiere decir las 24 horas del día, 7 días a la semana, los 365 días del mes, también garantizara las condiciones de seguridad necesarias para salvaguardar el hardware, software e información física que esté relacionado con este.

6.1.1 Espacio físico. Para el Datacenter debe tener piso falso y aire acondicionado, Sistema detección de incendios y extintores en especial en el centro de datos y en las áreas comunes.

Redundancia a nivel de energía en el centro de datos, lo anterior quiere decir que se debe contar en los racks donde estarán alojados los servidores con dobles PDUs y cada una conectada a un circuito independiente, pasando primeramente por la UPS, así para la conexión del aire acondicionado.

---

[56] PANDORA FMS. Monitoring Pandora: Documentation. Parte 2 Instalación y configuración. [En linea]. Disponible https://pandorafms.com/docs/index.php?title=Pandora:Documentation

[57] SANS DFIR. Digital Forensics and Incident Response. [En linea]. Disponible https://digital-forensics.sans.org/

Para la información que no es digital se debe tener un gabinete con la respectiva seguridad ya sea por medio de apertura con llave o clave.

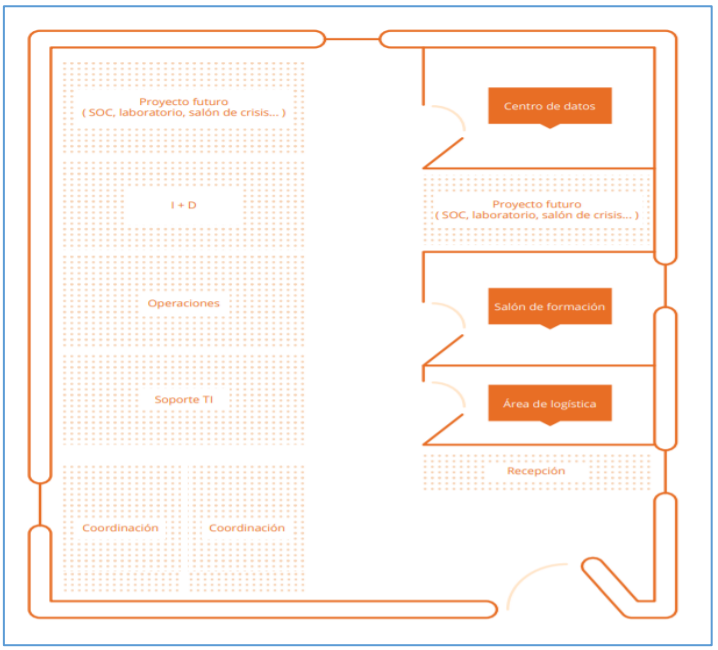
6.1.2 Restricción física. Se debe realizar de una manera controlada para acceder a las instalaciones, puertas, ventanas en lo posible con verificaciones biométricas (huella, escaneo del iris) Zonas compartidas (operaciones, soporte informático, I+D+I, entre otros, también para el Centro de datos, logística, laboratorio y monitoreo)

6.1.3 Visitas de proveedores y personal externo. Se debe establecer un protocolo previo y con la autorización pertinente para el ingreso, deben estar con acompañamiento todo el tiempo de la visita o actividad por el personal del CSIRT, todas las instalaciones del CSIRT deben tener un circuito cerrado de televisión.

6.2 DISEÑO DEL CSIRT

6.2.1 Plano de las Instalaciones. En la siguiente imagen se puede observar la distribución de las instalaciones.

Figura 8. Instalaciones mínimas del CSIRT.



Fuente: ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Buenas prácticas para establecer un CSIRT nacional. Diseño básico de la red CSIRT. [En linea]. p.76. Disponible https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

6.2.2 Descripción de cada área. El centro de datos es el área que tiene los dispositivos de Red (switches, routers, Firewalls, IDS, planta telefónica) y servidores (correo, dns, web, intranet, correlacionador de eventos, archivos, copias de seguridad, registro de incidentes, sandbox, monitoreo, análisis forense entre otros) , también a nivel eléctrico debe contar con doble fase eléctrica independiente (redundante), ups, planta eléctrica, aire acondicionado, piso falso con polo a tierra (para prevenir descargas eléctricas), sistema detector de incendios, extintor de gran capacidad.

6.2.2.1 I+D+I. Entre sus funciones principales es la investigación, desarrollo, innovaciones, realizar análisis estadístico de los incidentes, tendencias, desarrollo de herramientas que permiten mejorar la manera de hacer las cosas en el CSIRT, también realizar capacitaciones al personal, apoyo a las operaciones y realizar investigaciones.

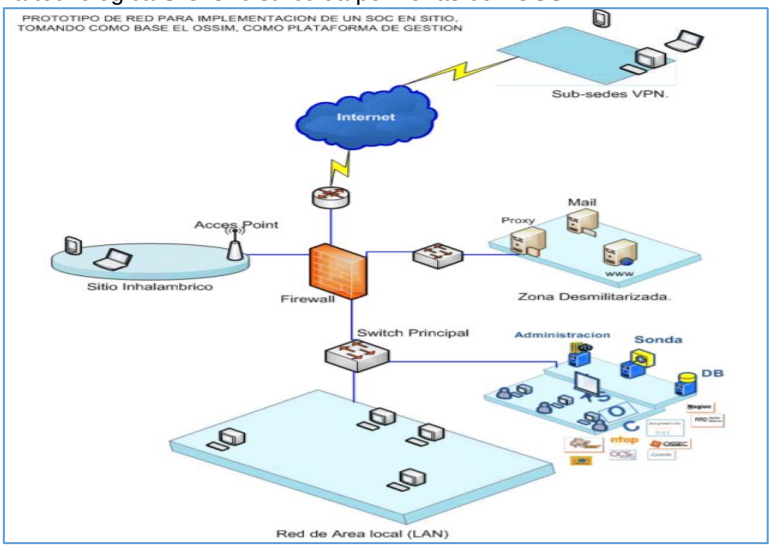
6.2.2.2 SOC (Centro de operaciones de seguridad). Esta es una de las áreas más críticas, debido a que sus roles principales son el monitoreo y la gestión de incidentes es el punto de medición si se están haciendo las cosas bien, la gestión adecuada a los incidentes reactivos y proactivos, el monitoreo de toda la plataforma y el protocolo a seguir en caso de detectar o que se reporte un incidente.

Este se debe apoyar de una herramienta de software la cual se encargará de la administración de eventos de seguridad en la red, prevención y detección de intrusos, para este caso se cuenta con una herramienta open source OSSIM (Open Source Security Information Management), la cual tiene una colección de aplicaciones en todo lo relacionado a la seguridad de la infraestructura tecnológica.[58]

En la siguiente figura se puede visualizar la arquitectura del centro de operaciones con la herramienta antes mencionada para el S.O.C.

[58] SOC COLOMBIA. Security Operation Center. [En linea]. 12 noviembre 2019. Recuperado http://www.soccolombia.com/documentos.php

Figura 9. Arquitectura tecnológica S.O.C. distribuida por zonas con OSSIM.



Fuente: SOC COLOMBIA. Modelo de monitorización del S.O.C. [En linea]. Disponible http://www.soccolombia.com/documentos/documento2.pdf

6.2.2.3 Soporte de TI. Es la encargada de la implementación y administración de todos los sistemas de control e infraestructura, además de la implementación (al inicio del CSIRT), administración, gestión y mantenimiento de los diferentes servicios como el correo, sitio web, archivos, gestión de tiques, monitoreo a nivel físico y lógico como los servidores y dispositivos de la red y los dispositivos de seguridad del CSIRT (biométricos, tarjetas, tokens entre otros).

6.2.2.4 Coordinaciones. Sus funciones son coordinar las respuestas a los incidentes reactivos y proactivos de manera eficaz, oportuna y eficiente, además con la interacción, gestión y colaboración, proporcionando un análisis de incidentes, vulnerabilidades, informando al personal que corresponda a través de boletines de noticias, estadísticas y documentación de las mejores prácticas que se deben tener en un CSIRT.

6.2.2.5 Logística. Para la operación diaria es necesario también en un CSIRT un área que gestione y administre los bienes tangibles e intangibles y mantenga un inventario y acorde a este un stock, ya sea algo tan irrelevante como es un esfero o una hoja de papel disponible como la disponibilidad de una cinta magnética para realizar backup, en este caso los responsables de estas labores dependiendo el tamaño del CSIRT puede ser responsable una persona o personas y no necesariamente es obligatorio la formación técnica de esta en el ámbito de la seguridad informática.

6.2.2.6 Salón de formación. Es donde se capacita y se entrena a colaboradores con el objetivo de adquirir experticia la cual será aplicada al enfrentar un incidente de seguridad , estas no deben enfocarse solamente en lo técnico, también son enriquecedoras para destinar espacios para retroalimentarse de otros centros y resolver inquietudes , también el encargado o los encargados de estas capacitación y entrenamientos tiene el compromiso de identificar temas de interés para los colaboradores , se puede apoyar en otros CSIRT, seminarios, conferencias entre otras.

6.2.2.7 Salón de crisis. Es el área reservada donde se reúne el personan designado e idóneo, con la experticia suficiente para la gestionar de una manera, eficiente y rápida ante una crisis de seguridad informática producto de un incidente activo o reactivo sea a el CSIRT o a la red productiva de la organización o a sus clientes, teniendo en cuenta el alcance de este proyecto para la empresa caso de estudio CIBERSECURITY DE COLOMBIA LTDA.

6.2.3 Características de la red. Internet se define con la red de redes por la cual una red de acceso privado es visible y tiene comunicación con las demás redes que están en internet para poder acceder a este servicio se debe realizar de forma legal con un proveedor de internet (ISP)[59]

6.2.4 Firewall o cortafuegos. Este cumple la función de segmentar las diferentes zonas creadas subdivididas de redes virtuales (Vlans) las cuales a través de reglas en el firewall permite los accesos y restricciones a los servicios de la red en donde se aplican estas a partir de una política en general, ya sea permitir todo o denegar todo , en adelante se habilitan o restringir los permisos, por ningún motivo se debe dejar estas reglas con la característica de (ANY) que significado permitir todo, porque se estaría dejando una brecha de seguridad muy alta.

Según el documento publicado por la organización de estados americanos para las buenas prácticas en un CSIRT, se deben tener mínimo 5 zonas separadas (Internet, Dmz externa, Dmz interna, LAN y pruebas) a continuación se realiza la descripción de estas.[60]

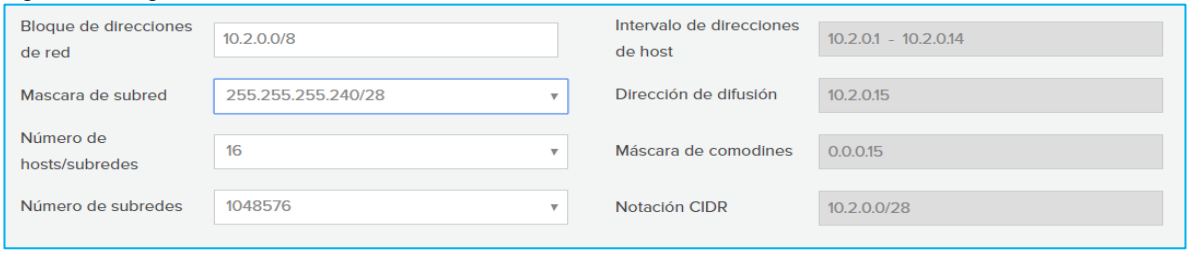
[59] TELEFONICA EQUIPO EDITORIAL. (17 de diciembre de 2018). reportedigital.com. [En linea]. Disponible https://reportedigital.com/cloud/internet-service-provider-isp/

[60] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Buenas Prácticas para establecer un CSIRT nacional. [En linea] 2016. Pág. 77. [Citada: 04 abr. 2020] Disponible https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

6.2.5 DMZ Externa. Esta se utiliza para albergar los servicios que se encuentren en la instalación del CSIRT y que se requiere publicarlos en internet como es el caso (servidor web y correo) con las respectivas reglas en el firewall de entrada y salida, se recomienda que en esta únicamente se deje la aplicación y que la base de datos este alojado en la DMZ Interna, con visibilidad desde y hacia esta por medio del Firewall.

Esta Subred estará definida por una máscara de red (28) de la clase C, permitiendo un máximo de 16 host configurada de la siguiente manera, utilizando una calculadora de subredes IPV4, ver figura.

Figura 10. Segmentación de red DMZ Externa.

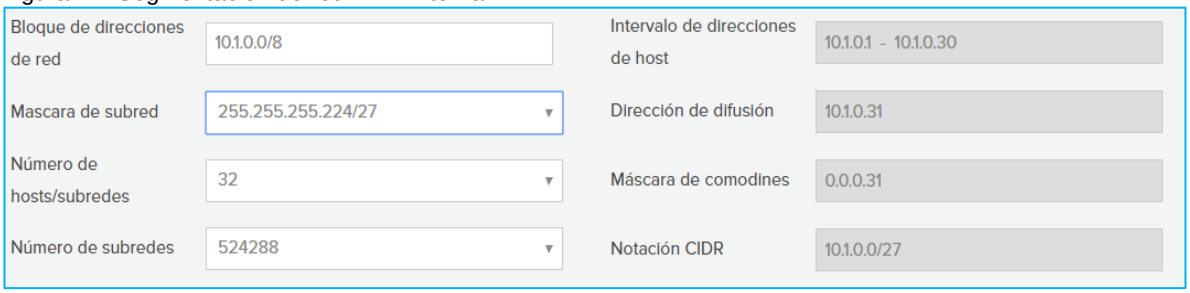


Fuente: SITE24X7. Calculadora de subredes IPv4. [En linea]. Disponible https://www.site24x7.com/es/tools/ipv4-subredes-calculadora.html

6.2.5.1 DMZ Interna. Esta albergara el mínimo de servicios requeridos para ejecutar las tareas el CSIRT (Monitoreo, correlacionador), con la característica de no publicar servicios a internet solamente para servicios exclusivos dentro del CSIRT.

Esta Subred estará definida por una máscara de red (27) de la clase C, permitiendo un máximo de 32 host configurada de la siguiente manera, utilizando una calculadora de subredes IPV4, ver figura.

Figura 11. Segmentación de red DMZ Interna.



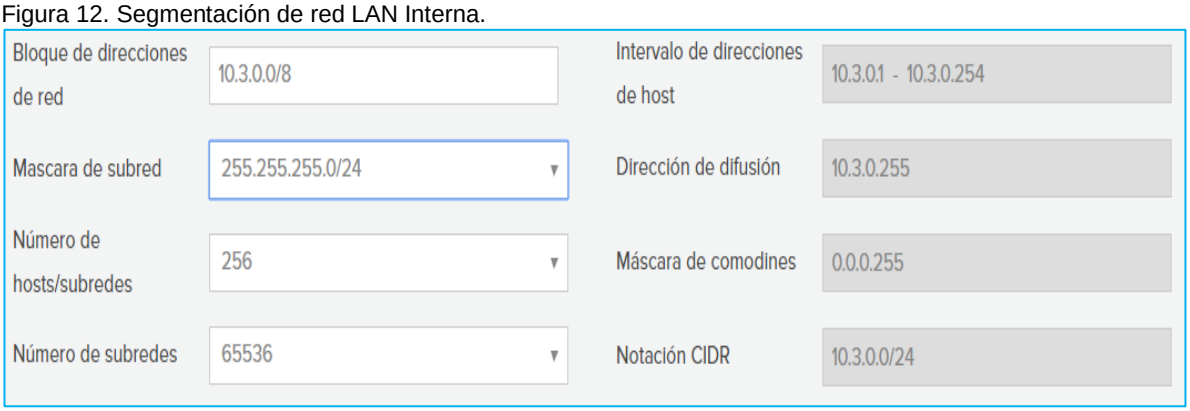
Fuente: SITE24X7. Calculadora de subredes IPv4. [En linea]. Disponible https://www.site24x7.com/es/tools/ipv4-subredes-calculadora.html

6.2.5.2 LAN CSIRT

Esta red almacenara los dispositivos de trabajo para las tareas cotidianas los cuales son (computadores de escritorio, portátiles, tabletas, impresoras entre otros).

Esta Subred estará definida por una máscara de red (24) de la clase C, permitiendo un máximo de 256 host configurada de la siguiente manera, utilizando una calculadora de subredes IPV4, ver figura.

Figura 12. Segmentación de red LAN Interna.

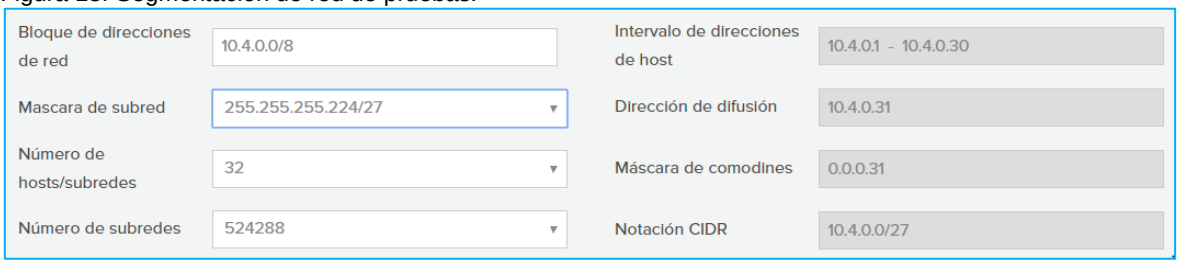


Fuente: SITE24X7. Calculadora de subredes IPv4. [En linea]. Disponible https://www.site24x7.com/es/tools/ipv4-subredes-calculadora.html

6.2.5.3 Red de pruebas. Está destinada para realizar todo lo referente a laboratorios, pruebas de software, es sumamente importante que esta red este aislada lógicamente de las otras redes desde el proveedor de internet (ISP) para prevenir que no se creen puertas traseras para un ciber atacante y de esta manera no comprometer la red principal del CSIRT también esta se utilizara para el servicio de SANBOX Firejail.

Esta Subred estará definida por una máscara de red (27) de la clase C, permitiendo un máximo de 32 host configurada de la siguiente manera, utilizando una calculadora de subredes IPV4, ver figura.

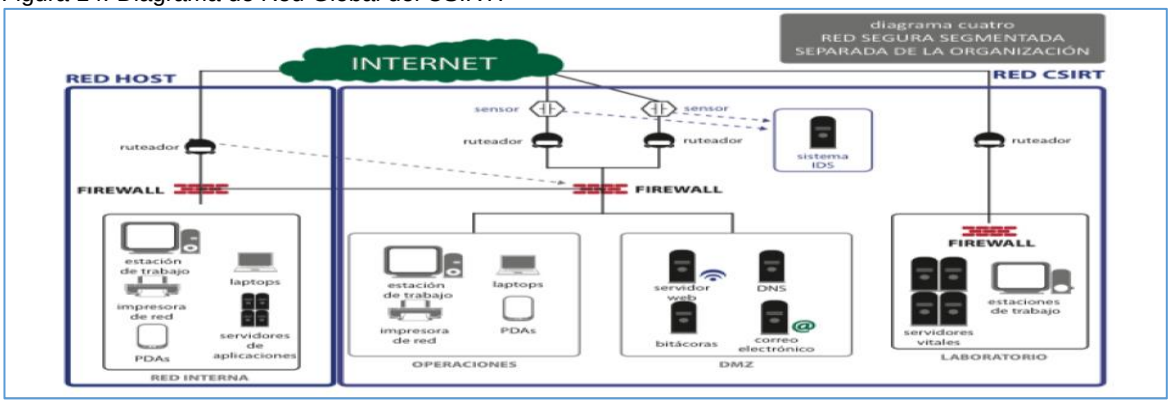
Figura 13. Segmentación de red de pruebas.



Fuente: SITE24X7. Calculadora de subredes IPv4. [En linea]. Disponible https://www.site24x7.com/es/tools/ipv4-subredes-calculadora.html

6.2.5.4 Arquitectura red CSIRT. En la siguiente grafica se puede observar la distribución de los dispositivos de red, aplicando a través del firewall la segmentación para que las redes sean independientes para su entrada y salida a internet, también para que la red de pruebas quede completamente aislada de la red del CSIRT y Red local de producción, además la Red del CSIRT cuenta con unos sensores IDS para interceptar y monitorear todos los paquetes que llegan desde internet, lo cual permite tener un primer anillo de seguridad.

Figura 14: Diagrama de Red Global del CSIRT.



Fuente: LACNIC. Proyecto: AMPARO. Manual básico de:
Gestión de Incidentes de Seguridad Informática. [En linea]. Rambla República de México 6125. Montevideo C.P. 11400 Uruguay. Ed. 201. ISBN: 978 - 9974 - 98 - 741 – 8. p. 77. Disponible https://warp.lacnic.net/wp-content/themes/warpnew/docs/manual_basico_sp.pdf

6.2.5.5 Mínimo de Equipos recomendados para el CSIRT. La O.E.A. en 2016 determino que los servicios mínimos exclusivos que debería contar un CSIRT para su operación. [61]

- Servidor Correo

  Tiene el rol de comunicaciones para el correo electrónico y buzones del CSIRT.

- Servidor web e Intranet

  Para el primero su función es donde se publica la información que no es sensible, contactos, boletines y formularios para notificar los incidentes, para el ultimo es facilitar el intercambiar la información como procedimientos y técnicas para dar respuesta a los incidentes activos y proactivos, también para alojar manuales de operación, buenas practicas entre otros.

[61] Ibíd. P.78.

Para tener mayor seguridad en estas dos aplicaciones se crearán reglas a través de firewall para que solamente sean accesibles por los puertos necesario desde y hacia las Vlans e Ips requeridas.

- Servidor Archivos

  Encargado de alojar los documentos y archivos digitales, disponibles en línea y publicados dentro de las instalaciones del CSIRT.

- Servidor de Copias de seguridad

  Realiza copias de seguridad de todos los servicios y estaciones de trabajo asignadas a los empleados del CSIRT, también se realizan copias de seguridad para enviarlas a custodia fuera de sitio con una empresa especializada en esto.

- Servidor de DNS

  Cumple con el rol de la resolución de nombres de dominio para toda la infraestructura del CSIT.

- Servidor de monitoreo

  Realiza el monitoreo (7x24x365 días) sin interrupción a los todos los sitios web que considere críticos y relevantes en función de la empresa, clientes y entes gubernamentales, es importante que se ubique pantallas de monitoreo sean visibles por todos los colaboradores del CSIRT.

- Servidor para recolectar y correlacionar eventos

  Recolecta todos las transacción, eventos, alertas e información enviada por los sensores de red con la finalidad de hallar factores en común y similitudes que puedan dar evidencias de comportamientos inusuales en los dispositivos del CSIRT.

- Servidor para registrar y hacer seguimiento de incidentes
  Este es el servicio más relevante, es el que tiene el rol de llevar la trazabilidad de los registros de incidentes activos y proactivos, además de una base de conocimiento para el personal, generador de informes mensuales de gestión, cabe resaltar que por cada incidente se debe generar un ticket el cual es un numero único, si el incidente llega por correo este al recibirse la aplicación a utilizar debe estar en la capacidad de crear el ticket y aplicar el escalamiento correspondiente en los mejores escenarios de forma automática.

- Computadores

Deben ser exclusivos para las funciones realizadas por los empleados del CSIRT.

- Teléfonos

  Exclusivos para el CSIRT con la capacidad de realizar llamadas, locales e internacionales con salida directa al proveedor de telefonía.

- Máquina trituradora

  Para destruir la información sensible esta labor exclusivamente la debe realizar personal del CSIRT.

- Almacenamiento portátil

  Cuando se da respuesta a incidentes es necesario contar con un dispositivo para recopilar información como evidencias, se debe contar mínimo con 4 unidades de almacenamiento externo de 2 T.B. y 5 unidades de memoria flash de 32 G.B. para uso exclusivo del personal del CSIRT.

7 DISEÑO LÓGICO DE LABORATORIO CONTROLADO

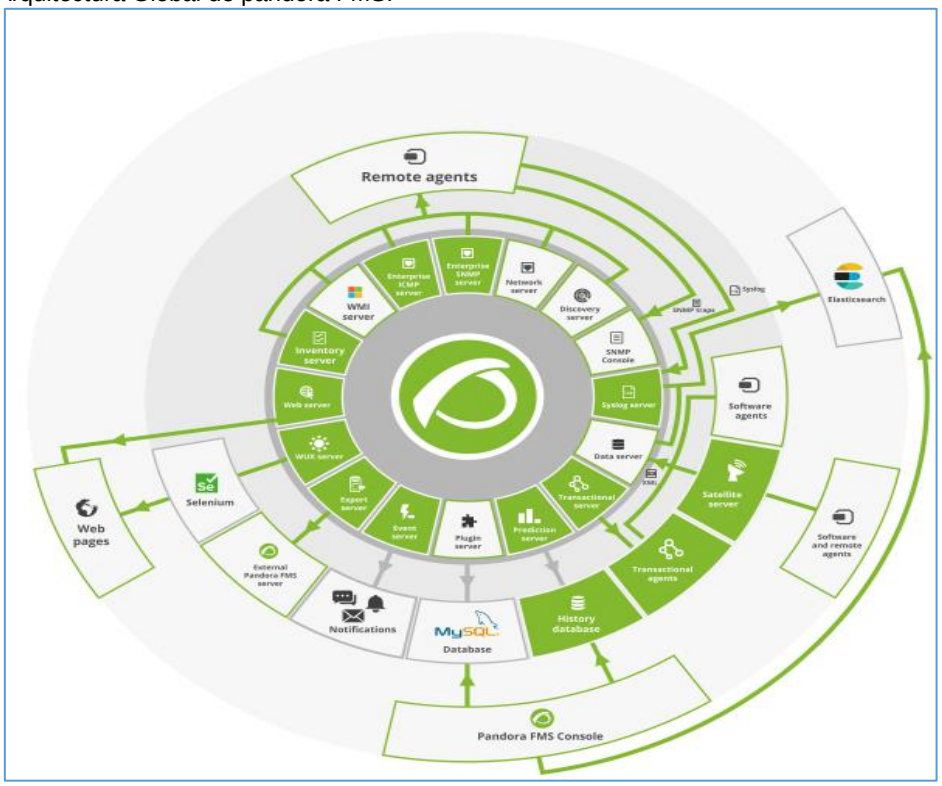
A continuación, se realiza la descripción de la arquitectura de las herramientas para prestar los servicios del CSIRT.

7.1 PANDORA FMS

Para el almacenamiento de la información contiene una base de datos en Mysql , sus componentes tienen replicación y se comportan en un entorno de alta disponibilidad (activo, pasivo) o formando un clúster (activo, activo), también se resalta que unos de sus elementos más importantes son los servidores ya que tienen la función de recibir y hacer procesamiento de la información, esta a su vez es enviada a la base de datos, por otro lado tenemos los agentes que esta previamente instalado en los dispositivos también envían información a la base de datos, después de esto al acceder a la consola de administración se puede ver reflejada lo almacenado en la base de datos y realizar la interacción con el usuario.

En la siguiente imagen se puede observar a nivel general la arquitectura de la aplicación Pandora FMS.

Figura 15. Arquitectura Global de pandora FMS.



Fuente: PANDORAFMS. Documentation es: Arquitectura. [En linea]. Disponible https://pandorafms.com/docs/index.php?title=Pandora:Documentation_es:Arquitectura.

7.1.1 Licenciamiento de Mysql. Pandora FMS Edición Community (E.C.) está bajo la licencia GPL v.2. De igual manera la base de datos de Mysql tiene licenciamiento dual por el cual se pueda optar por utilizar el licenciamiento GPL o comercial para esta aplicación se opta por el primer licenciamiento de esta manera se garantizará que mientras la aplicación en mención no se salga de los parámetros permitidos en cuando al licenciamiento GPL no será necesario adquirir licenciamiento comercial, ya que esta cuenta con las características estándar para el óptimo funcionamiento y soporte[62]

7.1.2 Tamaño máximo en la tablas y ficheros de MYSQL. El tamaño máximo de las bases de datos en Mysql es determinado por el tamaño límite del Sistema Operativo mas no por los limites internos de esta para el caso de almacenamiento con MyISAM para el tipo de almacenamiento en cuanto INNODB se puede crear varios archivos para las tablas de esta manera se puede distribuir en varias particiones de disco permitiendo tablas muy grandes con un tamaño máximo de 64 TB.

El tamaño máximo de ficheros haciendo la referencia del sistema operativo para el caso de pandora FMS la base de datos de MYSQL está instalada en Linux y utiliza un sistema de archivos EXT3 con lo cual el tamaño máximo por fichero es de 4 T.B. Debido a que MYSQL utiliza un licenciamiento dual (GPL y Comercial) estos no tienen restricciones en cuanto al tamaño del fichero de la base de datos solamente aclara que no exceda los parámetros de el licenciamiento de libre distribución GPL en el momento que no se cumpla con estas condiciones se debe adquirir una licencia comercial, en la siguiente tabla se muestra el comparativo del sistema operativo vs tamaño máximo de fichero.

Tabla 7. Tamaño base de datos en MYSQL.

Sistema operativo	Tamaño máximo de fichero
Linux 2.2-Intel 32-bit	2GB (LFS: 4GB)
Linux 2.4	(usando sistema de ficheros ext3) 4TB
Solaris 9/10	16TB
Sistema de ficheros NetWare w/NSS	8TB
win32 w/ FAT/FAT32	2GB/4GB
win32 w/ NTFS	2TB (posiblemente mayor)
MacOS X w/ HFS+	2TB

Fuente: ORACLE CORPORATION. MySQL 5.0 Reference Manual. Dimensiones máximas de las tablas MySQL. [En linea]. p.10,11. Disponible https://downloads.mysql.com/docs/refman-5.0-es.pdf

[62] MYSQL COMMUNITY EDITION. The MySQL Community Edition includes. [En linea] [Citada: 04 abr. 2020] Disponible https://www.mysql.com/products/community/

7.1.3 Servidores. Aproximadamente 10 servicios están contenidos en la Aplicación de Pandora Server la cual es multi-hilo para tener concurrencia de las distintas instancias, una de las funciones principales de estos es enviar alertas para tener control de la situación de la información. Para manejar grandes cargas de datos pueden operar con balanceo de cargas y distribuida en diferentes zonas geográfica, al detectar estos algunos acontecimientos que pueda causar algún problema genera una alerta y realizar una acción de tipo SMS, email o script, aunque los servidores tienen diferentes roles siempre hay uno principal y los otros son secundarios entonces en la caída o falla de unos de estos el principal se encarga de procesar la información.

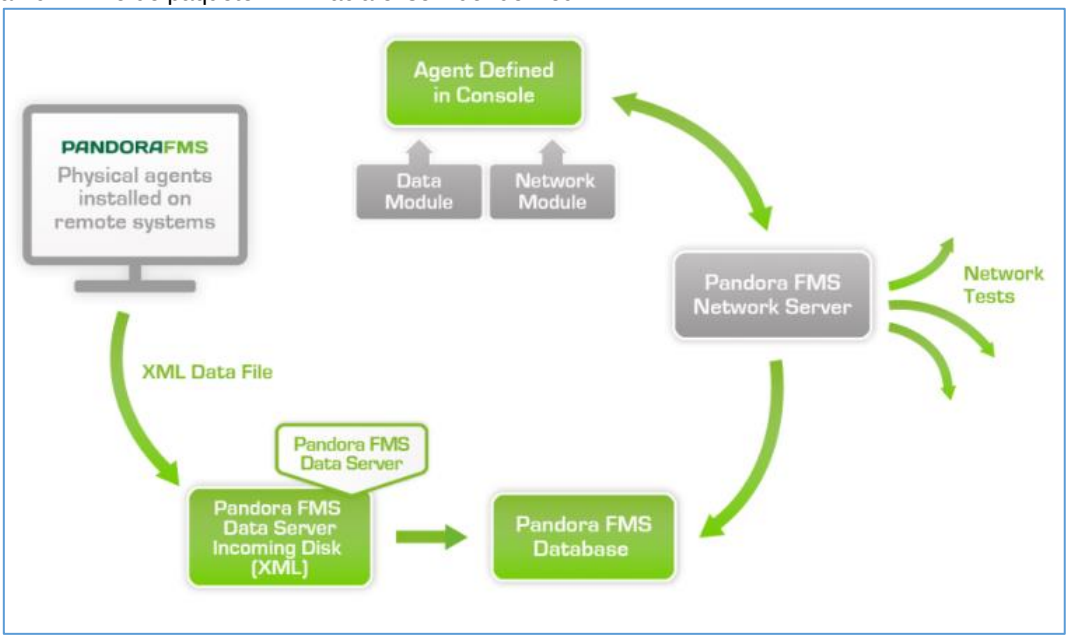
Adicionalmente la aplicación se encarga del estado de cada servidor la carga y los demás parámetros relevantes para su funcionamiento, por medio de la consola web un usuario puede realizar un monitoreo de los servidores por el modulo (estado de los servidores) los siguientes son los tipos de servidores que contiene la aplicación de Pandora FMS.

7.1.3.1 Datos. Es el que realiza el procesamiento de los paquetes en formato XML que envían los dispositivos que tienen los agentes instalados estos son alojados en un directorio especifico y se almacenas en la base de datos, puede haber uno o varios servidores específicos que pueden ser virtuales y así aprovechar el hardware cuando es para infraestructuras robustas, convirtiéndose este en unos de los servidores más relevantes de este sistema, sus funciones es recopilar y depurar la información enviada por los agentes en cuanto alertas y eventos , este servidor no realiza ninguna validación remota.

7.1.3.2 Red. Realiza monitoreo por medio de la red utilizando el protocolo ICMP, hace peticiones TCP y SNMP, al apuntar un agente a este servidor queda ligado a este para realizar para realizar los chequeos por este motivo es relevante que estos servidores sean visibles en toda la red afectada para realizar el monitoreo y que respondan a un ping desde el dispositivo que tiene el agente instalado, en la siguiente figura se puede observar la ruta que realiza el envío de un paquete XML desde el agente hasta el servidor de red.[63]

[63]PANDORA FMS, Arquitectura de Pandora FMS. Servidores [En linea]. Disponible https://pandorafms.com/docs/index.php?title=Pandora:Documentation_es:Arquitectura

Figura 16. Envió de paquete XML hacia el servidor de Red.



Fuente: PANDORAFMS. Documentation es: Arquitectura. [En linea]. Disponible https://pandorafms.com/docs/index.php?title=Pandora:Documentation_es:Arquitectura.

7.1.3.3 SNMP. Realiza la recolección de traps por medio del (demonio, servicio en segundo plano) este los recolecta y la consola y la consola de SNMP los procesa y almacena, este servidor tiene como rol que los agentes SNMP envían alarmas a los diferentes dispositivos como switches, routers, servidores entre otros en eventos como, por ejemplo:

I. Caída de un punto de conexión.
II. Daño de una fuente o ventilador en un switches o servidor.
III. Exceder la carga al realizar un proceso puede ser de un alto consumo de CPU o alto porcentaje de escritura en disco en una base de datos.
IV. Desborde de almacenamiento en un servidor o storage.
V. cambio de los umbrales del estado de una UPS.

Es importante que cuando se parametrizan estos valores se deben ajustar las métricas de los diferentes dispositivos a monitorear para evitar que se envíe un falso positivo al administrador de la infraestructura, un ejemplo de esto es cuando se ajusta la métrica para que envié un trap o alarma cuando se llena un disco o almacenamiento configurando el umbral al 40% cuando en la realidad estas alarmas se deben notificar a partir del 30% que es realmente cuando se debe prestar atención y tomar medidas preventivas y correctivas en caso de ser necesarios, las últimas medidas no es solamente realizar un cambio físico al presentar fallas si no que cuando está a punto de llenarse un disco, discos, volúmenes virtual, se debe pensar en realizar una expansión de estos ya sea si lo permite un servidor o un storage. Cuando se tienen las alarmas o traps, se envían estos logs al servidor

SYSLOG el cual centraliza estos, también se notifica con prontitud al NOC y se generan reportes diarios.[64]

7.1.3.4 SNMP Versión 3. Pandora FMS es compatible con este protocolo al lanzar consultas activas o por demanda (polling) o cuando envía mensajes de eventos asincrónicos la aplicación de este protocolo es parametrizado al realizar la configuración y parametrización de esta herramienta de monitoreo también permitiendo una mayor seguridad por su modularidad, dejando de forma independiente el mecanismo para el control de acceso de autenticar y privacidad, permitiendo que una entidad pueda tener simultáneamente modelos de seguridad y control de acceso mejorando la flexibilidad y la interoperación, define la seguridad de los usuarios por medio del modelo (USM) y controla el acceso por medio de vistas (VACM), también utilizando de las versiones anteriores los mejores conceptos.[65]

7.1.3.5 WMI. Es se encarga a través del protocolo WMI de realizar el monitoreo del APP y S.O. remotamente.

7.1.3.6 Servidor de reconocimiento. Es el encargado de realizar la detección de dispositivos a la red y por medio de una plantilla le aplica los módulos de forma automática de esta manera quedan incluidos al monitoreo, por esta razón que todos los servidores y dispositivos entre si no tengan ninguna restricción para poder ser accesibles entre ellos a nivel de red.

Este servidor también puede enviar tareas programadas y realizar un monitoreo especifico en ambientes de virtualización, servicios en la nube, bases de datos entre otros.

7.1.3.7 Servicio de complementos. Este servidor permite a usuarios avanzados hacer uso de scripts para realizar tareas complejas y ejecutarlos desde un punto central de forma general o específica a los dispositivos.

7.1.3.8 Predicción. Utiliza la estadística y la I.A. para predecir los eventos del último mes de esta manera detectar si hay un comportamiento inusual en un dispositivo.

---

[64] VICENTE.C. Universidad de Oregon. Gestión de Traps SNMP. [En linea]. Disponible https://nsrc.org/workshops/2008/walc/presentaciones/gestion_traps.pdf

[65] RED IRIS. La seguridad en la familia de protocolos SNMP. La seguridad en la versión 3 del protocolo. [En linea] [Citada: 04 abr. 2020] Disponible https://www.rediris.es/difusion/publicaciones/boletin/50-51/ponencia16.html

7.1.3.9 Chequeos web. Este servidor recibe como nombre GOLIAT, es el encargado de realizar pruebas de carga en un sitio web, también permite tener los tiempos de latencia y la experiencia en la navegación y sus contenidos de las páginas web (imágenes, texto, videos, formularios entre otros).[66]

Otros servicios de exportación, inventario, correlacionador de eventos, servidor de red con ICMP, satélite entre otros están disponible en la versión Enterprise.

7.1.4 Interface Web. Permite a través de asignación de roles a usuarios tener diferentes privilegios para la administración y operación, entre sus funciones esta:

I. Controlar los agentes.
II. Información estadística.
III. Poder generar tablas y gráficos.
IV. Gestionar incidentes.
V. Crear informes.
VI. Creación de perfiles y usuarios.

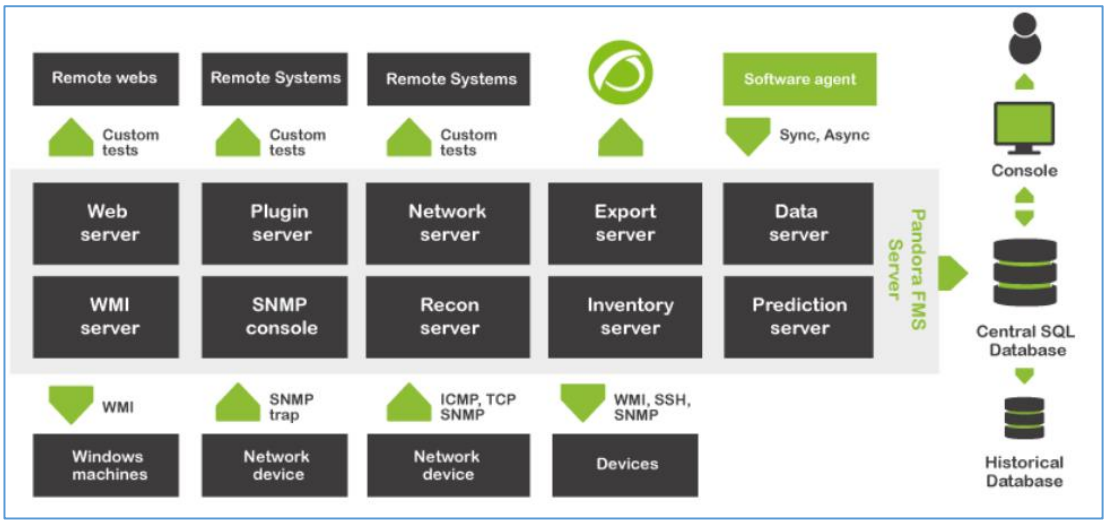
Su interfaz web está desarrollada en PHP no siendo necesario ningún complemento, plugin adicional para acceder a este solo se ingresa por un browser con HTML y CSS como es el caso de Firefox y Chrome cabe resaltar que en la navegación con internet Explorer se pierden funciones relevantes, además permite acceder simultáneamente.

7.1.5 Base de datos. Esta es la parte más importante de la aplicación Pandora FMS, está en Mysql donde realiza sus transacciones y guarda la información en tiempo real, también contiene todo el historial y configuraciones, también soporta otro tipo de base de datos como MariaDB y Percona.

En la siguiente figura se puede observar su diseño.

[66] PANDORA FMS, Arquitectura de Pandora FMS. Redes [En linea]. Disponible https://pandorafms.com/docs/index.php?title=Pandora:Documentation_es:Arquitectura

Figura 17. Diseño Base de datos Pandora FMS.



Fuente: PANDORAFMS. Documentation es: Arquitectura. [En linea]. Disponible https://pandorafms.com/docs/index.php?title=Pandora:Documentation_es:Arquitectura.

7.1.5.1 Mantenimiento de la base de datos. Lo realiza periódicamente y automático en una fecha indicada, liberando de esta tarea al operador y administrador de la aplicación.

7.1.6 Agentes. Aunque este permita realizar el monitoreo de múltiples dispositivos como servidores y dispositivos en la red, la aplicación Pandora FMS para este proyecto realizara la función de monitorear el mínimo de servicios (Correlacionador de eventos, servidor de copias de seguridad y SandBox) requeridos en el CSIRT de la empresa caso de estudio.

Pandora FMS utiliza 2 diferentes agentes para realizar labores en la aplicación.

7.1.6.1 Contenedor. Es creado en la consola web estando asociado a varios elementos a monitorizar, también puede estar relacionado con una o un rango de direcciones IP, también puede tener módulos remotos como:

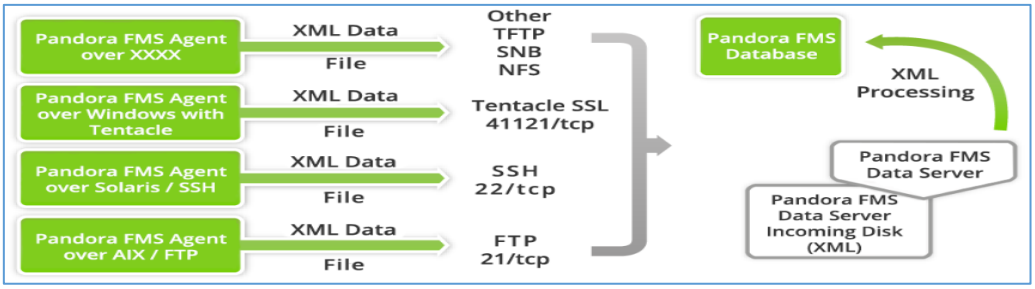
I. Verificar ping.
II. Revisar el estado de un puerto (abierto o cerrado).
III. Revisa si un objeto en la red responde correctamente.
IV. Monitoriza el hardware por SNMP.
V. Verifica la latencia entre el dispositivo origen y destino.

Tenemos los agentes de tipo remoto como servidores de red y los de tipo local que se encargan de procesar y recolectar por el servidor de datos.[67]

7.1.6.2 Software. Se utilizan principalmente en servidores para realizar el monitoreo del Hardware (disco, memoria, procesadores, fuentes, ventiladores entre otros) y a nivel de software según las aplicaciones instaladas (base de datos, servicios, sistema operativo entre otros) cabe resaltar que en cuento a dispositivos de red estos se realizan de forma remota sin la necesidad de este tipo de agente.

En la siguiente figura se puede observar cómo se recolectan los datos de manera local, en donde cada agente realiza varias revisiones de cada parámetro especifico en un dispositivo como es el uso del procesador y todo esto queda en un solo archivo XML que lo envía al servidor de Pandora. Este es copiado periódicamente con intervalos de cada 6 minutos, la aplicación pandora no funciona en tiempo real pero su tiempo de respuesta está entre 3 a 5 segundos.

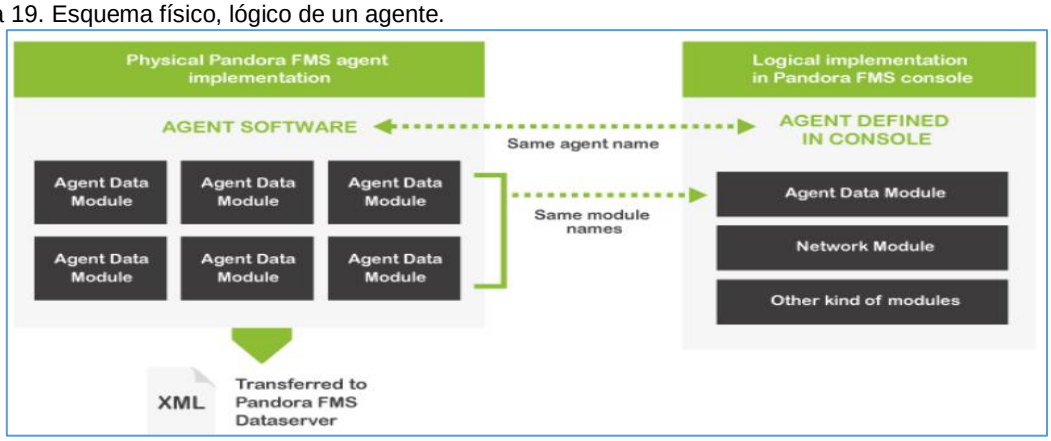
Figura 18. Recolección de datos local.



Fuente: PANDORAFMS. Documentation es: Arquitectura. [En linea]. Disponible https://pandorafms.com/docs/index.php?title=Pandora:Documentation_es:Arquitectura.

En la siguiente figura se observa el esquema físico, lógico de un agente.

Figura 19. Esquema físico, lógico de un agente.



Fuente: PANDORAFMS. Documentation es: Arquitectura. [En linea]. Disponible https://pandorafms.com/docs/index.php?title=Pandora:Documentation_es:Arquitectura.

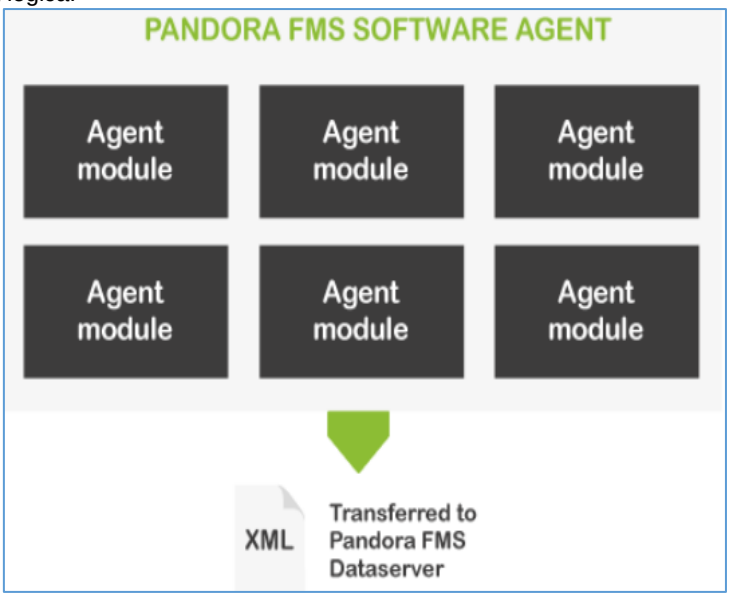
[67]PANDORA FMS, Arquitectura de Pandora FMS. Base de Datos. [En linea]. Disponible https://pandorafms.com/docs/index.php?title=Pandora:Documentation_es:Arquitectura

El transporte de paquetes XML se puede realizar por medio de los protocolos tentacle, ssh o ftp, haciendo este seguro ya que no se envían contraseñas por la red y los paquetes están todos cifrados aplicando la integridad, confidencialidad y autenticidad de la conexión entre el servidor y el agente, el más recomendado es tentacle ya que utiliza el protocolo criptográfico SSL. [68]

7.1.6.3 Archivo XML. Su estructura y nombre son la combinación del host donde está instalado el agente y la extensión (.data) asignado un serial diferente para cada uno de los paquetes, también genera un archivo de verificación (checksum) el cual tiene un Hash MD5 el cual verifica que no se hayan alterado antes de ser procesados.

A continuación, en la figura se observa su estructura lógica.

Figura 20. Estructura lógica.



Fuente: PANDORAFMS. Documentation es: Arquitectura. [En linea]. Disponible https://pandorafms.com/docs/index.php?title=Pandora:Documentation_es:Arquitectura.

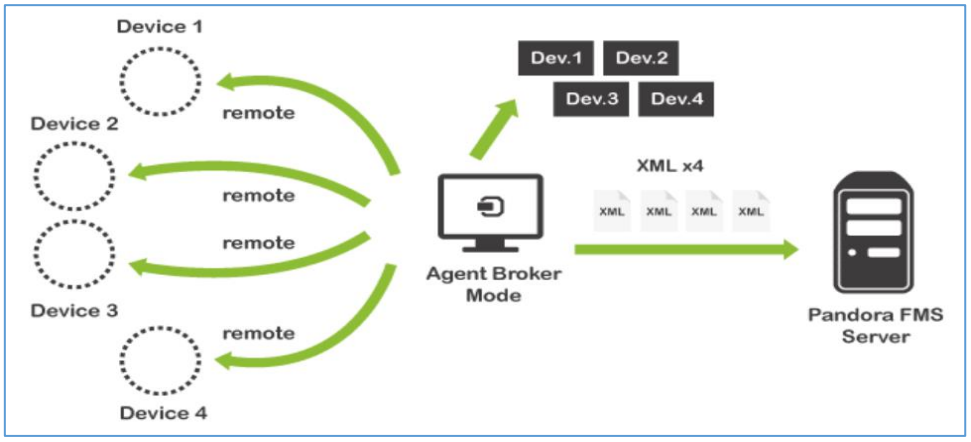
7.1.7 Topologías de red para monitorizar. A continuación, se describen las diferentes metodologías de forma local y remota.

[68] PANDORA FMS, Arquitectura de Pandora FMS. Agente de software. [En linea]. Disponible https://pandorafms.com/docs/index.php?title=Pandora:Documentation_es:Arquitectura

7.1.7.1 Red con accesibilidad. Fácil implementación, es del tipo centralizada organizada y de tamaño mínimo, esta red es accesible remota centralizada desde el servidor de Pandora se accede a todos los dispositivos a monitorear, también está de la forma que en cada dispositivo instalamos un agente y este envía loa paquetes XML al servidor de Pandora.

7.1.7.2 Red con difícil acceso. Se puede usar un agente para realizar las verificaciones remotas con un agente Broker o por satélite server el cual permite las verificaciones remotas con funciones avanzadas como se observa en la siguiente figura.

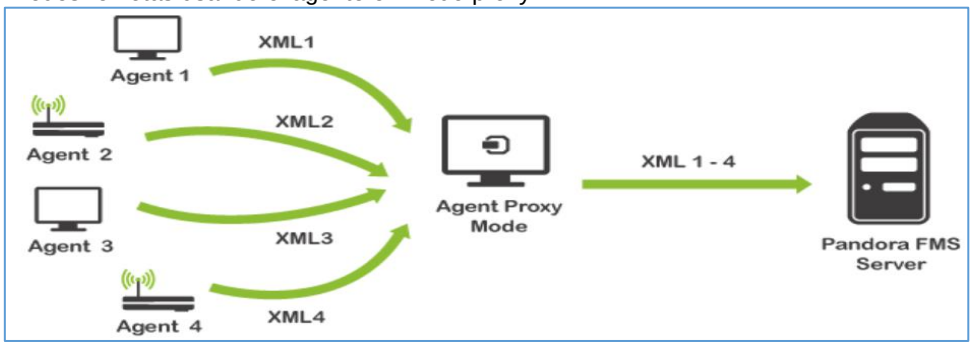
Figura 21. Modo Broker en redes remotas con difícil acceso.



Fuente: PANDORAFMS. Documentation es: Arquitectura. [En linea]. Disponible https://pandorafms.com/docs/index.php?title=Pandora:Documentation_es:Arquitectura.

Cuando no se tiene acceso al servidor por parte de los agentes de software se hace necesario colocar un proxy para utilizar un agente intermedio que si tiene acceso al servidor de Pandora el cual es reenviar todos los archivos XML de los dispositivos incluyendo el propio de este proxy de nombre (agent Proxy Mod) como se muestra en la siguiente figura.

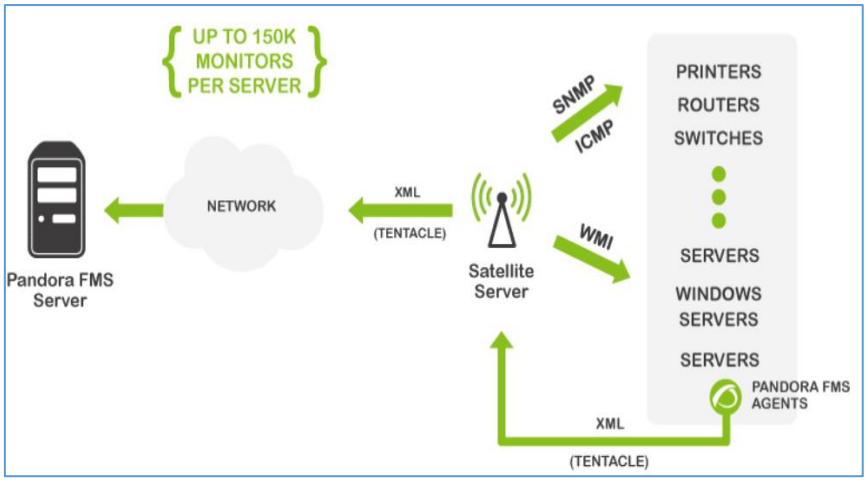
Figura 22. Redes remotas usando el agente en modo proxy.



Fuente: PANDORAFMS. Documentation es: Arquitectura. [En linea]. Disponible https://pandorafms.com/docs/index.php?title=Pandora:Documentation_es:Arquitectura.

Cuando son redes diferentes con conexión remota al servidor se puede utilizar el Satellite Server o varios servidores con la salvedad de que deben estar conectados a la misma base de datos, cada componente realiza el monitoreo de su red con una consola de administración y gestión para todas las redes como se observa en la siguiente figura.

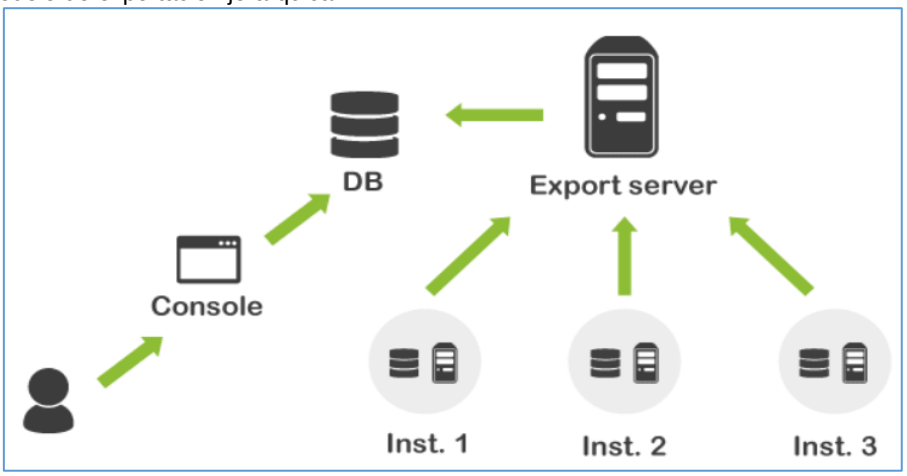
Figura 23. Sedes remotas con Satellite Server.



Fuente: PANDORAFMS. Documentation es: Arquitectura. [En linea]. Disponible https://pandorafms.com/docs/index.php?title=Pandora:Documentation_es:Arquitectura.

En el caso de que se requiera varias sedes realizar el monitoreo con diferentes configuraciones se debe contar con un servidor de nombre export server para que desde cada instancia envié los XML y sean reenviados a la Base de datos principal, también la administración seria fragmentada ajustada a través de permisos sobre políticas como se observa en la siguiente figura.

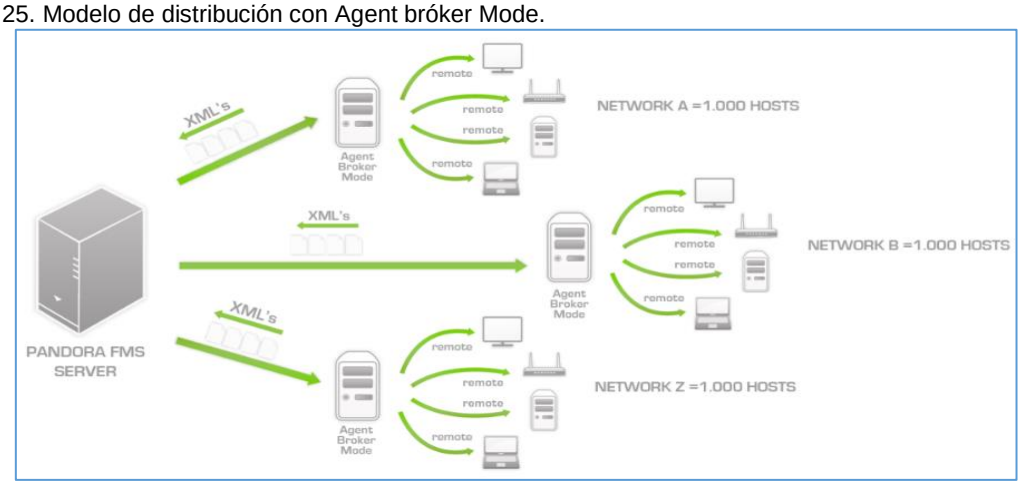
Figura 24. Modelo de exportación jerárquica



Fuente: PANDORAFMS. Documentation es: Arquitectura. [En linea]. Disponible https://pandorafms.com/docs/index.php?title=Pandora:Documentation_es:Arquitectura.

7.1.7.3 Red robusta. Tiene las características de tener aproximadamente 50 chequeos lo cual se debe implementar de forma descentralizada para distribuir las peticiones en varios
servidores con el rol de (Agent Broker mode) a continuación en la siguiente figura se observa el modelo.

Figura 25. Modelo de distribución con Agent bróker Mode.



Fuente: PANDORAFMS. Documentation es: Arquitectura. [En linea]. Disponible https://pandorafms.com/docs/index.php?title=Pandora:Documentation_es:Arquitectura.

7.1.8 Instalación y Configuración Pandora FMS. Se debe cumplir con los requisitos mínimos de hardware como se observa en la siguiente figura.

Figura 26. Requerimientos mínimos de hardware.

Hardware	PEQUEÑO: Hasta 500 agentes o 5000 módulos	MEDIANA: Hasta 2000 agentes o 10000 módulos	GRANDE: Para más de 4000 agentes*
CPU	1 núcleo a 2 GHz	2 núcleos a 2,5 GHz	4 núcleos a 3 GHz
RAM	4 GB	8 GB	16 GB
Disco Duro	7200 rpm	15K rpm o SSD	SSD
Espacio en disco	20GB mínimo 40GB recomendado	60GB mínimo 120GB recomendado	120GB mínimo 250GB recomendado

Fuente: Fuente: PANDORAFMS. Documentation es: Instalación. [En linea]. Disponible https://pandorafms.com/docs/index.php?title=Pandora:Documentation_es:Instalacion

Seguidamente se puede observar la compatibilidad de sistemas operativos.

Figura 27. Compatibilidad de sistemas operativos.

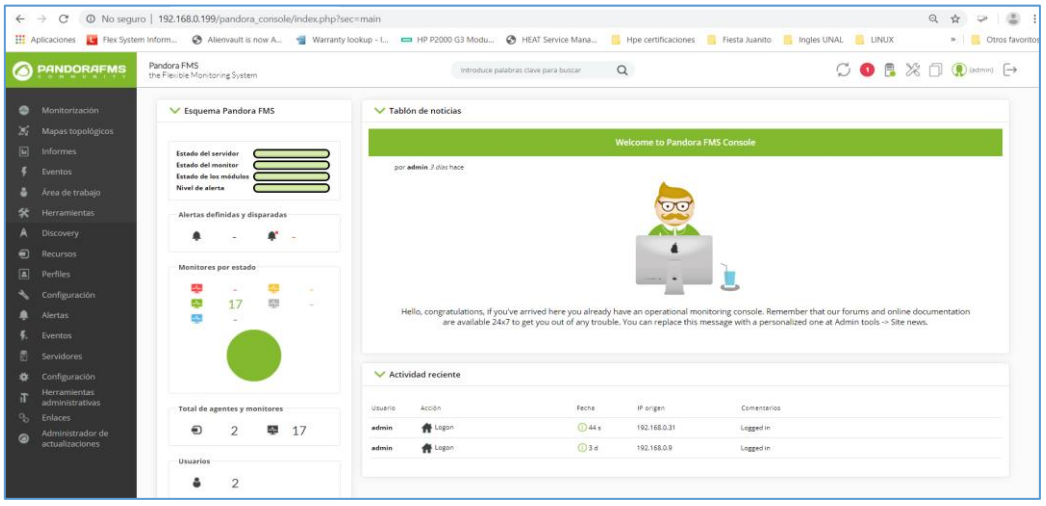
Software	Requisitos	
Sistema Operativo	Windows Server (2003 o superior) RedHat Enterprise (RHEL) 7.X CentOS 7.X (Recomendado) SLES 11 SP1 o superior OpenSUSE 11.X o superior Debian 5, 6, 7 o superior Ubuntu 11 o superior	
	FreeBSD 9.X y 10.X Solaris 10/OpenSolaris	Pandora FMS no da soporte oficial en estas plataformas

Fuente: Fuente: PANDORAFMS. Documentation es: Instalación. [En linea]. Disponible https://pandorafms.com/docs/index.php?title=Pandora:Documentation_es:Instalacion

Se realiza la descarga la imagen ISO desde la página Oficial de Pandora FMS esta contiene la máquina virtual preconfigurada (Appliance) con la aplicación y distribución Linux.

Después de realizar el despliegue del (Appliance) a través del Hypervisor se procede ingresar por la interfaz web, donde se solicita para el ingreso por primera vez el usuario de administración por defecto (admin) y su respectiva contraseña (pandora) como se observa en la figura.

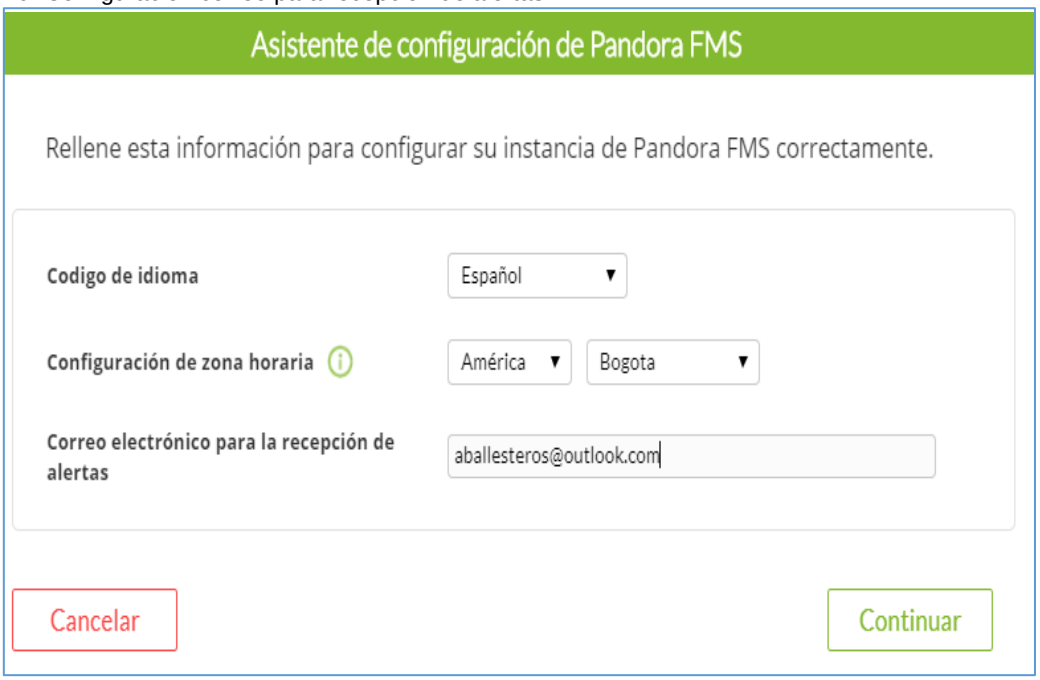
Figura 28.Ingreso a la consola de administración Pandora FMS.



Fuente: Propia.

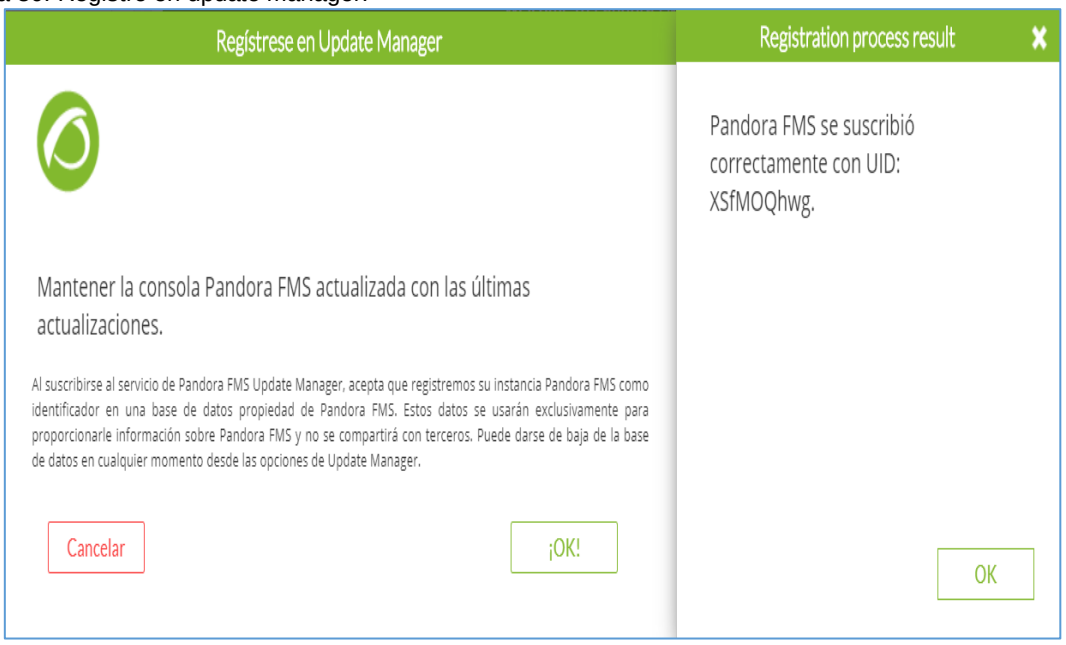
Una vez se ingresa se configura el correo para recibir alertas como se puede observar en la siguiente figura.

Figura 29. Configuración correo para recepción de alertas.



Fuente: Propia.

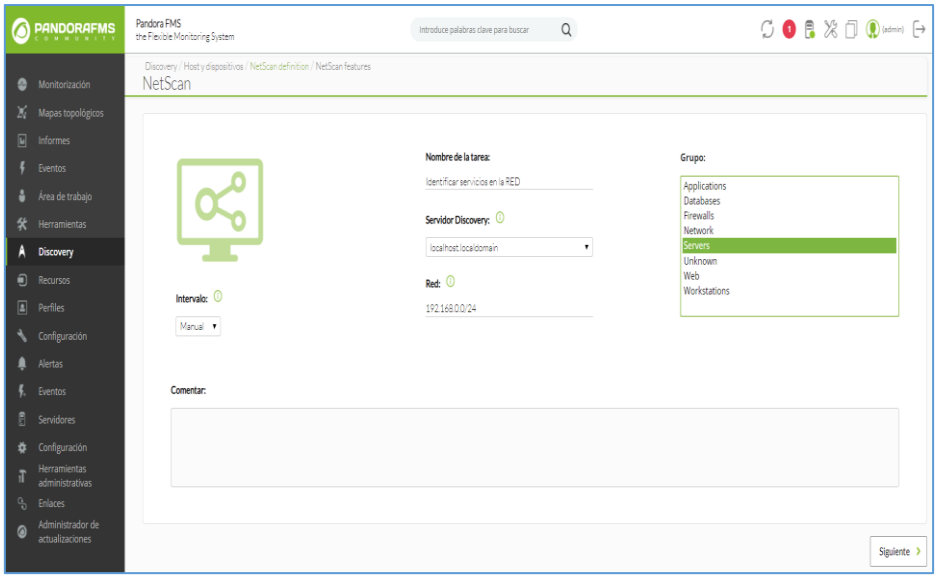
Figura 30. Registro en update manager.



Fuente: Propia.

7.1.9 Pruebas uso de la aplicación. Se procede a crear una tarea para identificar los servidores de la Red, ver figura.

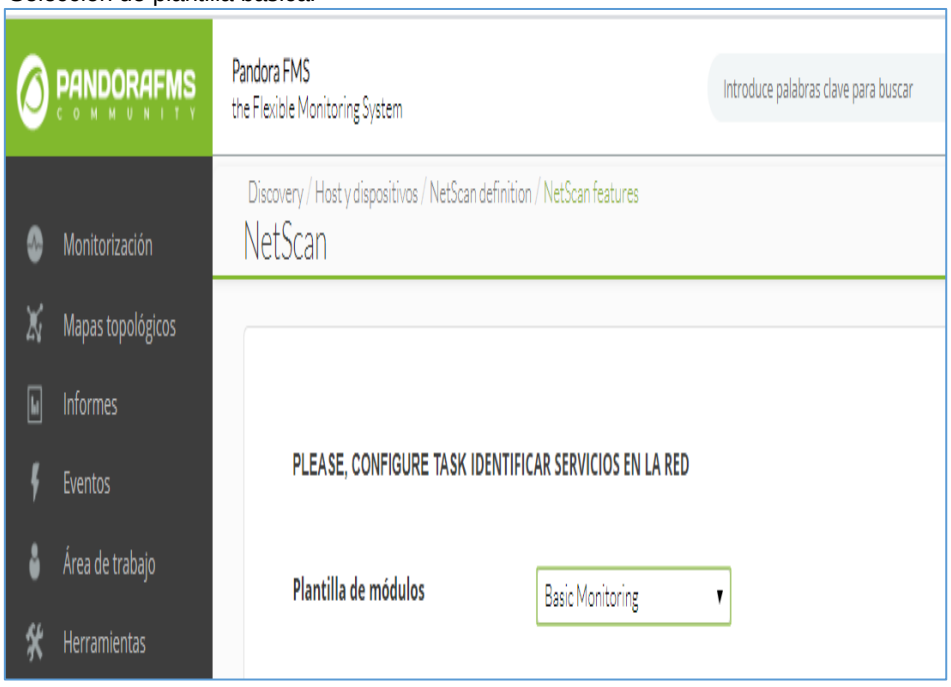
Figura 31. Descubrir servidores en la red local.



Fuente: Propia.

A continuación, se utiliza una plantilla básica para la tarea como se observa en la siguiente figura.

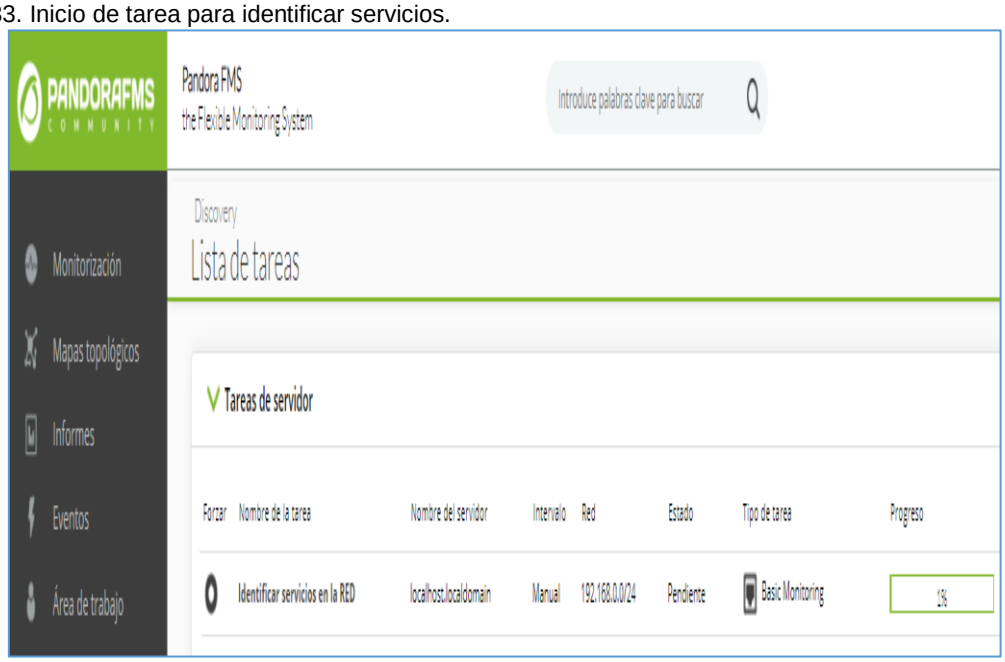
Figura 32. Selección de plantilla básica.



Fuente: Propia.

Después se ejecuta la tarea para descubrir los servicios.

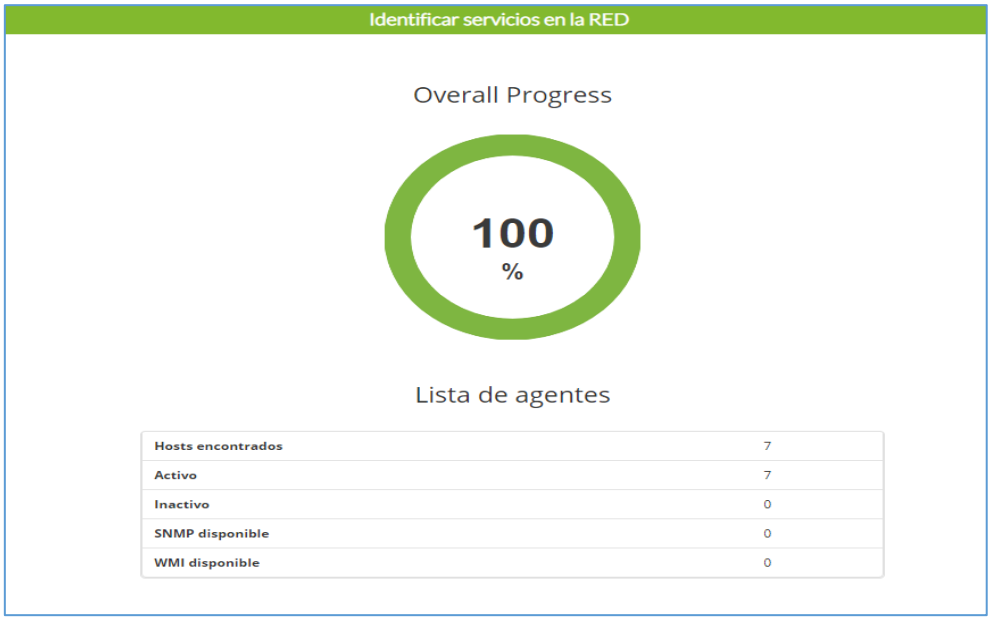
Figura 33. Inicio de tarea para identificar servicios.



Fuente: Propia.

Se evidencia que se han encontrado 7 host en la red. Ver la siguiente figura.

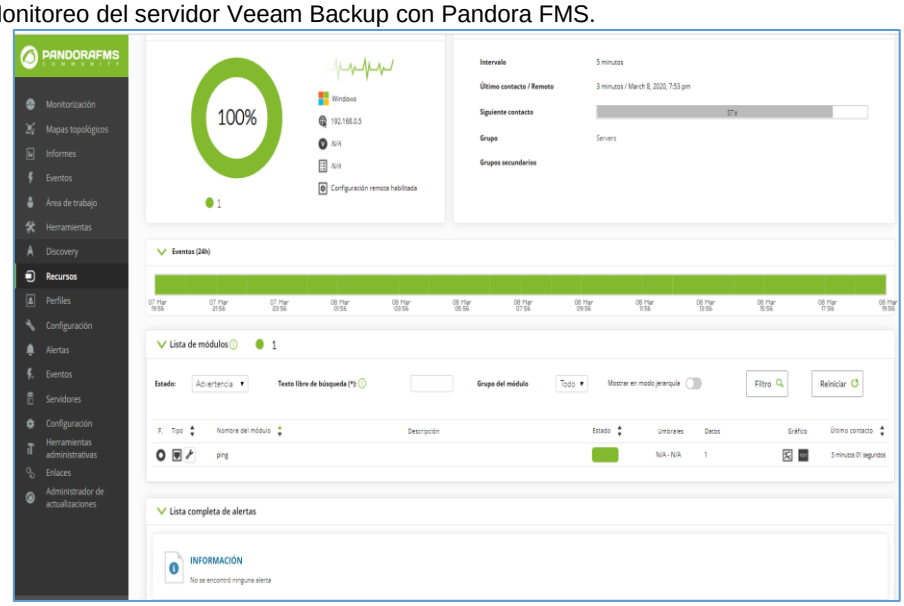
Figura 34. 7 host detectados.



Fuente: Propia.

A continuación, se observa que el servidor de Veeam Backup queda incluido al monitoreo con Pandora FMS, como se puede observar en la figura no tiene ninguna alerta.

Figura 35. Monitoreo del servidor Veeam Backup con Pandora FMS.



Fuente: Propia.

Seguidamente aparece los dispositivos a nivel de la Red LAN descubiertos.

La Subred que proveerá el mínimo de servicios para las tareas del CSIRT pertenece a la DMZ Interna estará definida por una máscara de red (27) de la clase C, permitiendo un máximo de 30 host configurada de la siguiente manera, haciendo uso de una calculadora para IPV4, ver figura.

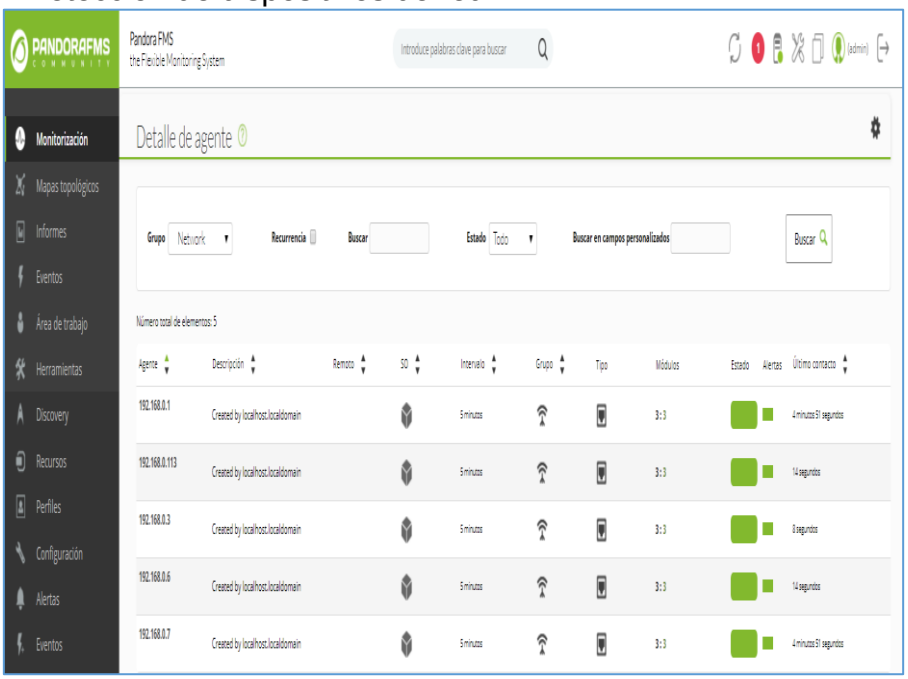
Figura 36. Calculo Subred de servidores IPV 4.

Fuente: SITE24X7. Calculadora de subredes IPv4. [En linea]. Disponible https://www.site24x7.com/es/tools/ipv4-subredes-calculadora.html

Lo anterior se evitará un cuello de botella, se reducirá el broadcast y aplicar está de acuerdo a la importancia de un CSIRT.

A continuación, se puede observar la detección de algunos dispositivos de red para realizar el monitoreo.

Figura 37. Detección de dispositivos de red.



Fuente: Propia.

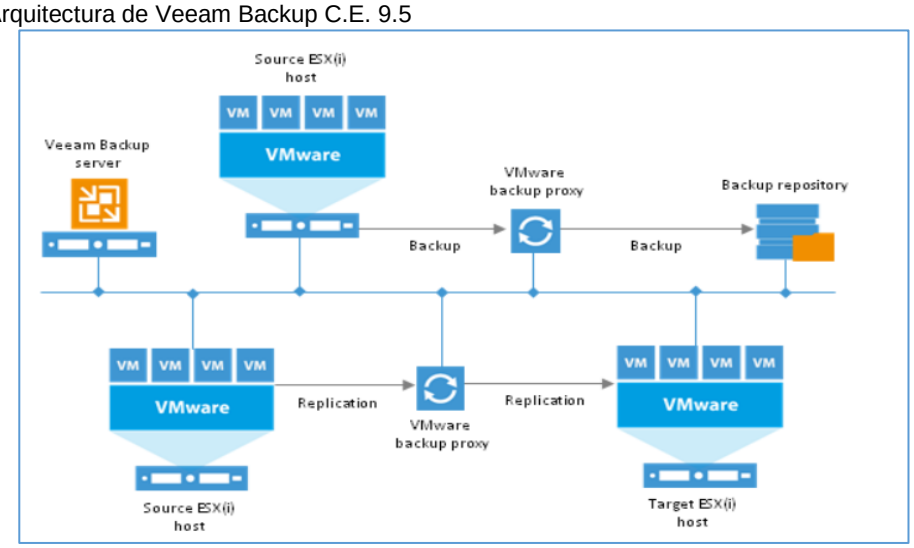
7.2 VEEAM BACKUP COMMUNITY EDITION

Para esta labor se utilizó la aplicación Veeam Backup & Replication 9.5 U4, la cual permite hasta 10 cargas de trabajo sin costo en licenciamiento, es decir cada carga de trabajo se crea un Job (tarea) y se podrían crear hasta 10 Jobs uno por servidor virtual para realizar el Backup.[69]

Para realizar el Backup de las aplicaciónes en el CSIRT se utilizara la version 9.5 Update 4, en la siguiente figura se puede observar su arquitectura.

[69] VEEAM. Veeam Backup & Replication Community Edition. El backup GRATUITO imprescindible para VMWare y Hyper-V. [En linea]. Disponible https://www.veeam.com/es-lat/virtual-machine-backup-solution-free.html

Figura 38. Arquitectura de Veeam Backup C.E. 9.5



Fuente: PAGGI, Hernan.Rhpware. Enterprise cloud computing blog. Veeam Backup & Replication: Parte 1 – Componentes. [En linea] Disponible https://www.rhpware.com/2014/02/veeam-backup-replication-parte-1.html

7.2.1 Instalación de Veeam Backup C.E. Se realizará en un servidor físico con Windows server 2016 a 64 bits, dedicado para esta aplicación.

Como dice Microsoft[70], se requiere una licencia de Windows server 2016 en su versión standard la cual permite hasta 2 MV con sistema operativo Windows server sin costo adicional o al tener una o varios sistemas operativo Linux aplica el licenciamiento de libre distribución que aplica para cada sistema operativo, siendo el ultimo aplicable al caso de estudio ya que los servicios de monitoreo, correlacionador de eventos y Sanbox están instalados sobre distribuciones de linux.

Aunque es posible instalar sobre este mismo servidor físico los servicios restantes virtualizados del CSIRT ya que al estar con sistema operativo Linux no se excedería el licenciamiento antes mencionado sin embargo no es una buena práctica tener todos en un solo servidor físico entonces los servicios restantes (Monitoreo Pandora FMS, Correlacionador de eventos Alient Vault OSSIM y SANBOX Firejail) se instalaran en un segundo servidor físico con sistema operativo Hyper-V server, según Microsoft[71] , si es exclusivamente para Virtualizar y cumpliendo esta condición no es necesario adquirir licenciamiento adicional de sistemas operativos, entonces Hyper-V server es un producto free.

[70] MICROSOFT. Commercial Licensing reference Guide. Server licensing overview. [En linea] 2007, p. 6 [Citada: 30 abril, 2020] Disponible http://download.microsoft.com/download/E/6/4/E64F72BF-55E9-4D85-9EFE-39605D7CE272/WindowsServer2016-Licensing-Guide.pdf

[71] MICROSOFT. Microsoft Hyper-V Server. Description. Microsoft Hyper-V Server is a free product. [en linea] Disponible https://www.microsoft.com/en-us/evalcenter/evaluate-hyper-v-server-2016

7.2.1.1 Requisitos para la instalación. Se recomienda un Core ya sea físico o virtual, 4 GB por cada 10 Jobs esto significa que al programar el backup para 10 VM se crea 1 Jobs para cada una, en este orden de ideas por buenas practicas se debe tener como requisitos mínimo 2 CPU o cores y 8 GB de ram, todas las configuraciones de las sesiones quedan almacenadas en la base de datos SQL Server la cual se instala con Imagen ISO que se descarga desde la página oficial de Veeam. [72]

El espacio en disco se necesitan aproximadamente 30 GB (10 GB para la instalación de los productos, 10 GB por cada 100 VM, 10 GB para el recovery) adicional a las 50 GB que se necesitan como mínimo para la instalación de Windows Server en total serian 80 GB.

A continuación, en la siguiente tabla se puede observar un resumen de los requerimientos de hardware y software para su instalación.

Tabla 8. Requisitos para la instalación.

Especificación	Requisitos	Observaciones
Hardware	4 cores, 8 GB Ram, 80 HDD o SSD	
OS	Windows server 2012 o 2016 .	
Software	• Microsoft .NET Framework 4.5.2 • Microsoft Windows Installer 4.5 • Microsoft SQL Server Management Objects • Microsoft SQL Server System CLR Types • Microsoft Visual C++ 2010 Service Pack 1 redistributable package	Estos paquetes los realiza durante la instalación, los cuales están contenidos en la imagen ISO de la instalación, se recomienda en el momento de la instalación tener conexión a internet para recibir las actualización de estos.
Base de datos SQL	• Microsoft SQL Server 2017	

[72] VEEAM. Veeam Backup & Replication Best Practices. Compute requirements. [En linea]. Disponible https://www.veeambp.com/backup_server_introduction/backup_server_sizing

	• Microsoft SQL Server 2016 • Microsoft SQL Server 2014 • Microsoft SQL Server 2012 (Microsoft SQL Server 2012 SP3 Express Edition is included in the setup)	

Fuente: VEEAM. Help Center. Veeam Backup & Replication 9.5 Archived. System Requirements. [En linea] Disponible https://helpcenter.veeam.com/archive/backup/95/vsphere/system_requirements.html#backup_server

El servidor físico tendrá el primer arreglo de discos en RAID 1 (contenido en 2 discos físicos conexión sata de tipo SSD 300 G.B. Para el sistema Operativo e instalación de Veeam Backup) un segundo arreglo e discos con RAID 6 (contenido en 4 discos físicos conexión sata de tipo SAS, tamaño 4 T.B. quedando 8 T.B. efectivas para el almacenamiento de backups).

La solución de copias de seguridad queda con un Datastore de 8. T.B creado en Veeam Backup con una proyección anual de aproximadamente 2.5 T.B. a 3 años, realizando backup full inicial de las máquinas virtuales con incrementales diarios, full semanal, Full mensual y Full anual, estimando un incremento del 10% semanal de la data en cada uno de los backup según se relaciona en siguiente tabla.

También en función de las buenas prácticas y garantizar la disponibilidad de los backups se realizará también un backup full semanal, mensual, anual y se guardará en cinta enviándolo en custodia a una empresa especializada.

Tabla 9. Relación de espacio de almacenamiento para copias de seguridad.

Servicio	Tipo	S.O.	Volumen	Tamaño G.B. backup full inicial	Tamaño G.B. backup full semanal	Tamaño G.B. backup full mensual	Tamaño G.B. backup full anual
Pandora FMS	Virtual	Linux	1	20	22	28	336
Alien Vault OSSIM	Virtual	Linux	1	40	44	56	672
Firejail	Virtual	Linux Ubuntu	1	10	11	14	168
Veeam Backup	Físico	Window server	1	80	88	112	1344

		2016 Std.					
Backup en Cinta (G.B)				**150**	**165**	**210**	**2520**
Total Backup Datastore (G.B)							**2520**

Fuente: Propia.

7.2.2 Bases de datos. SQL Server almacena todo el historial, sesiones y configuraciones en una instancia, esta base de datos puede estar en el mismo servidor de la aplicación, en otro servidor físico o virtual o remoto por lo cual antes de realizar la instalación se debe planificar su ubicación según lo robusta de la infraestructura.

Por defecto Veeam Backup CE 9.5 U4, por defecto se instala con SQL server 2016 Express por lo tanto el tamaño de esta no puede pasar exceder los 10 GB.

7.2.2.1 Rendimiento. Al ejecutar los Jobs (tareas) de manera automática por el SQL server se aumenta el consumo de recursos en cuanto a procesador y memoria, en la siguiente figura se observa los recursos que se necesitan de estos en cuanto la concurrencia de Jobs.

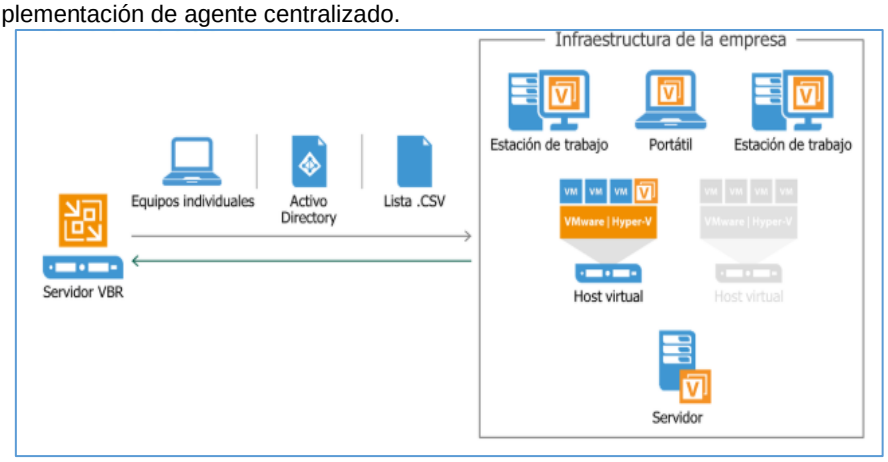
Figura 39. Requerimientos de CPU y Memoria versus concurrencia de Jobs.

Number of concurrently running jobs	CPU	RAM
Up to 25	2	4 GB
Up to 50	4	8 GB
Up to 100	8	16 GB

Fuente: VEEAM. Veeam Backup & Replication Database. Sizing. [En linea]. Disponible https://www.veeambp.com/backup_server_introduction/backup_server_database

7.2.3 Agente de Veeam Backup. Por Medio un Job desde la consola principal de Veeam Backup se puede desplegar el agente centralizado para realizar el backup ya sea el servidor físico o virtual esto está habilitado para Sistemas operativos Windows y Linux, se realiza el proceso para detectar los servidores mediante grupos dinámicos dentro de un directorio activo o red local, en la siguiente figura se puede observar la arquitectura para la implementación del Agente.

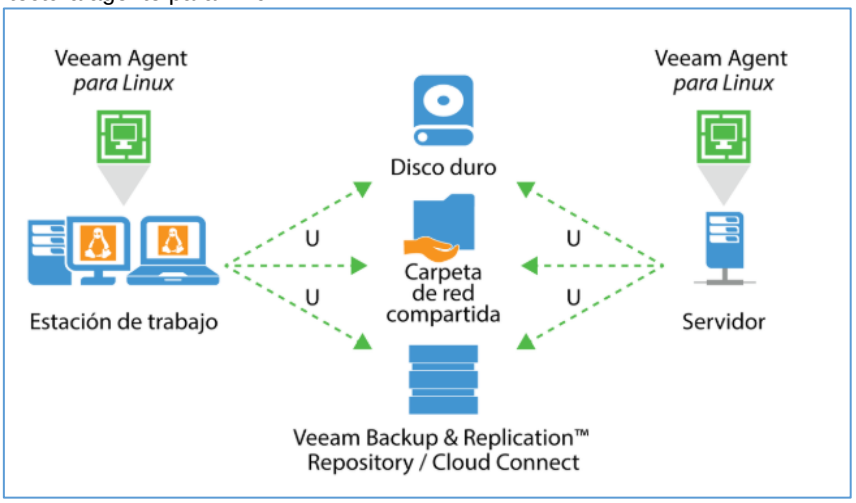
Figura 40. Implementación de agente centralizado.



Fuente: VEEAM. Implementación y administración de backup centralizadas para Veeam Agents. [En linea]. Disponible https://www.veeam.com/es-lat/backup-management-tool-vm-physical-cloud.html

7.2.3.1 Agente para Linux. Garantiza tener disponibles las instancias de servidores para el sistema operativo Linux ya sea que estos servicios estén alojados en la Nube o en sitio y acceso a los repositorios de Backup como se puede observar en la figura.

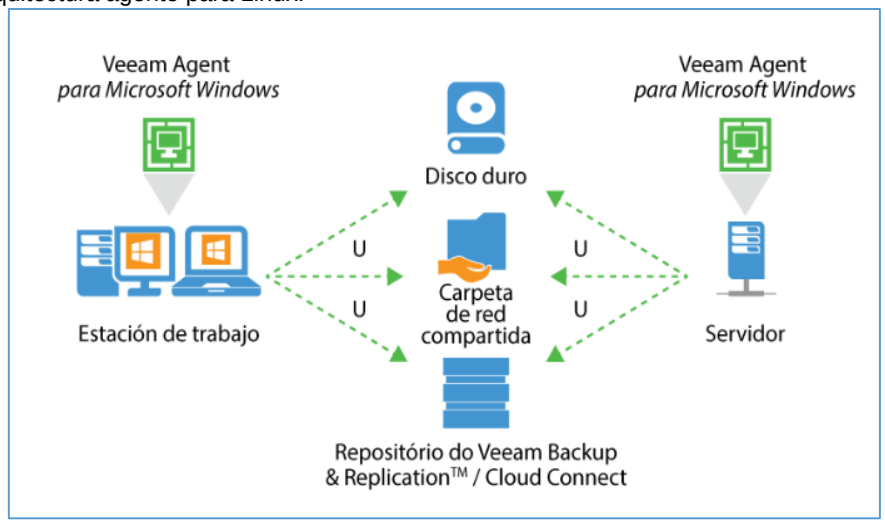
Figura 41. Arquitectura agente para Linux.



Fuente: VEEAM. Implementación y administración de backup centralizadas para Veeam Agents. [En linea]. Disponible https://www.veeam.com/es-lat/backup-management-tool-vm-physical-cloud.html

7.2.3.2 Agente para Microsoft Windows. Permite tener la disponibilidad de las cargas de trabajo para servidores físicos, virtuales, host en la nube y remotos de igual manera se realiza por medio de un Job el despliegue del agente desde la consola de administración, se puede observar su arquitectura en la siguiente figura.

Figura 42. Arquitectura agente para Linux.

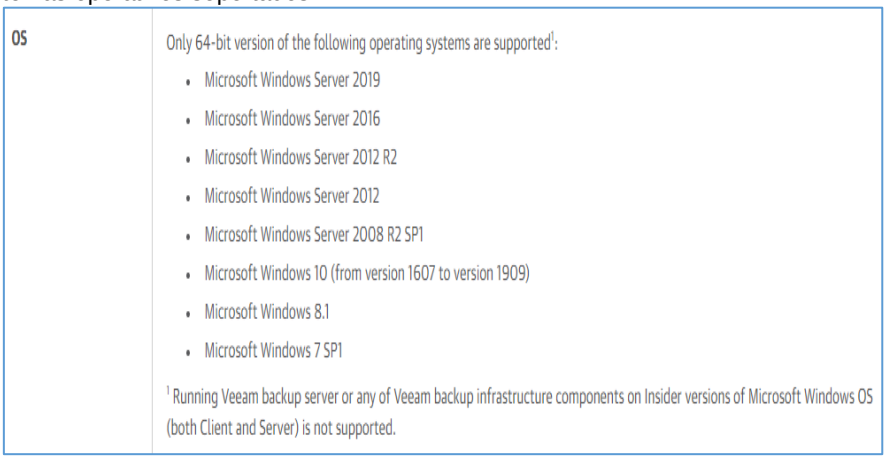


Fuente: VEEAM. Implementación y administración de backup centralizadas para Veeam Agents. [En linea]. Disponible https://www.veeam.com/es-lat/backup-management-tool-vm-physical-cloud.html

7.2.4 Instalación y configuración Veeam Backup C.E.

Antes de iniciar la instalación se debe tener en cuenta la compatibilidad de la aplicación vs el sistema operativo soportado como se puede observar en la siguiente figura.

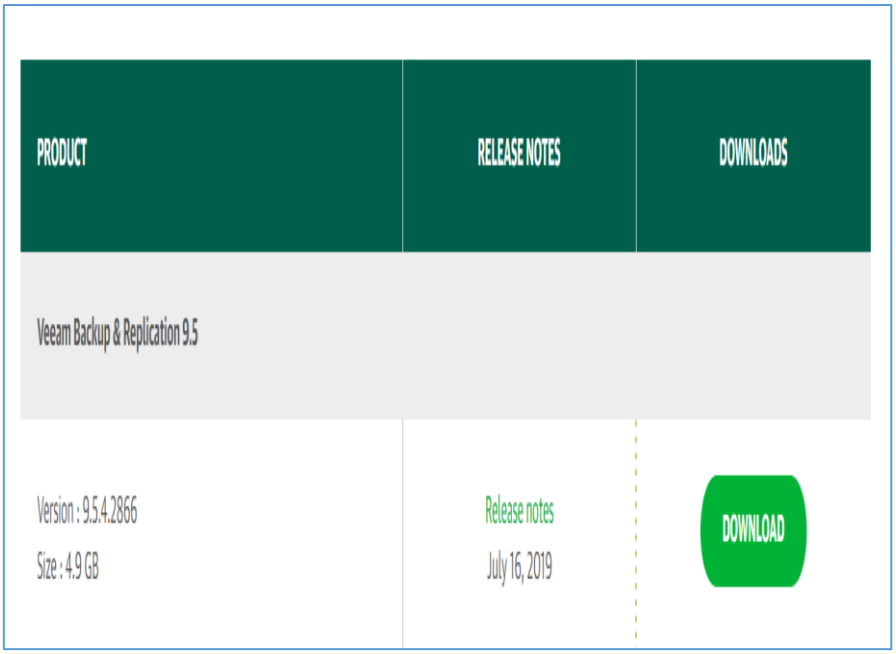
Figura 43. Sistemas operativos soportados.



Fuente: VEEAM. Veeam Backup & Replication 10. System Requirements. Backup Server. [En linea]. Disponible https://helpcenter.veeam.com/docs/backup/vsphere/system_requirements.html?ver=100#backup_server

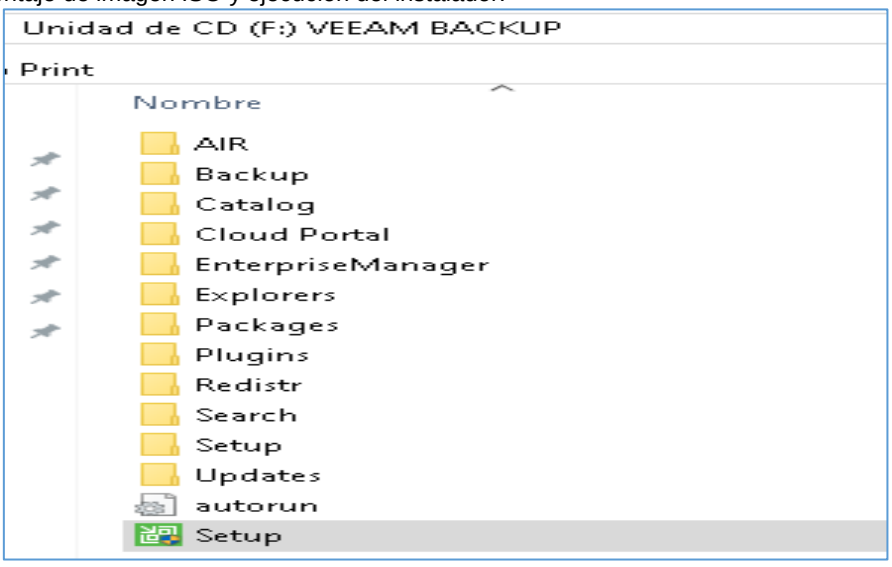
También se puede hacer referencia en la tabla 4, que menciona los requisitos para la instalación del hardware, software y base de datos, después de la anterior verificación se inicia con la descarga de la imagen ISO que contiene el instalador de la aplicación desde la página oficial de Veeam, ver figura.

Figura 44. Descarga de Imagen ISO.



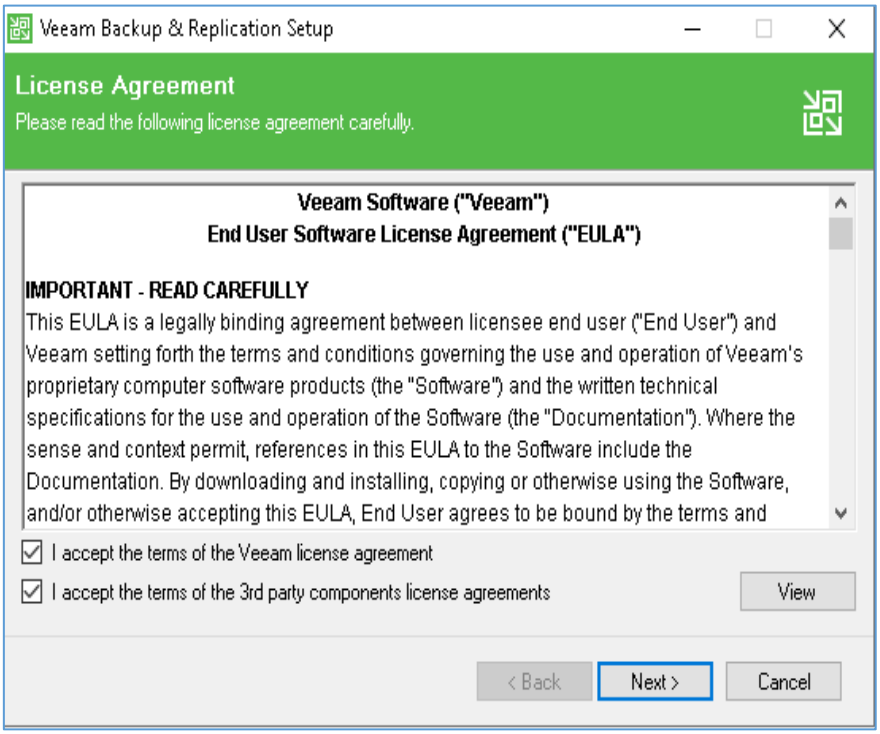
Fuente: VEEAM. Veeam Backup & Replication Community Edition. Descargue gratis. [En linea]. Disponible https://www.veeam.com/es-lat/virtual-machine-backup-solution-free.html

Figura 45. Montaje de imagen ISO y ejecución del instalador.



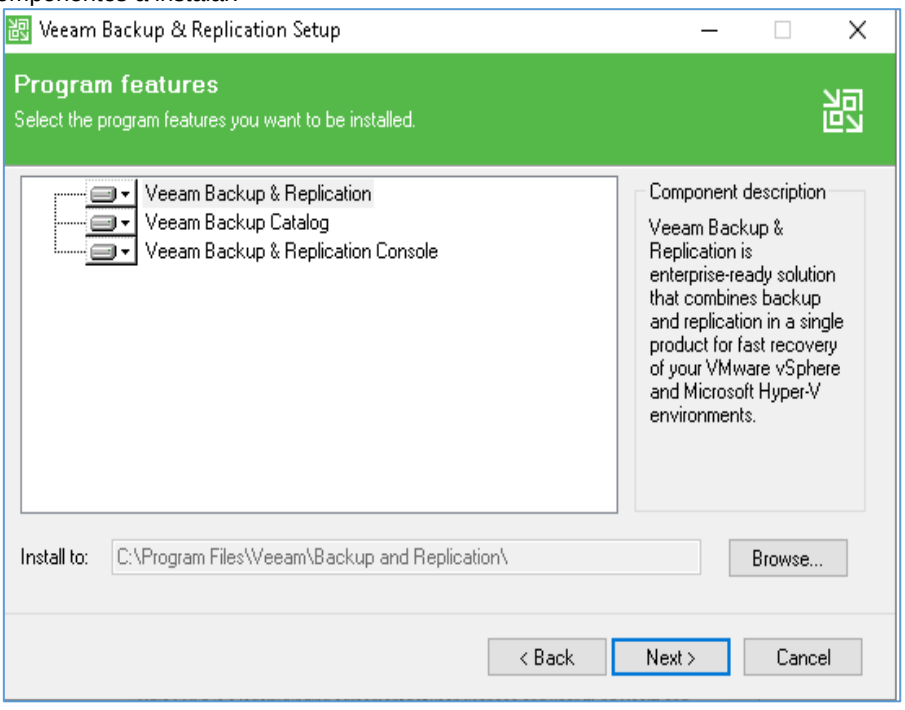
Fuente: Propia.

Figura 46. Aceptación de términos de la licencia.



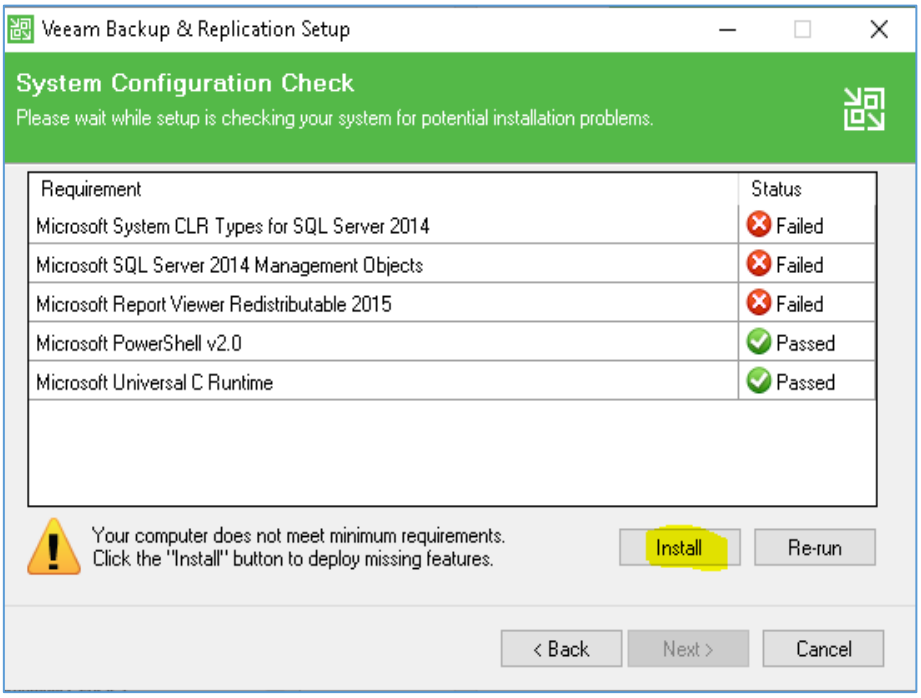
Fuente: Propia.

Figura 47. Componentes a instalar.



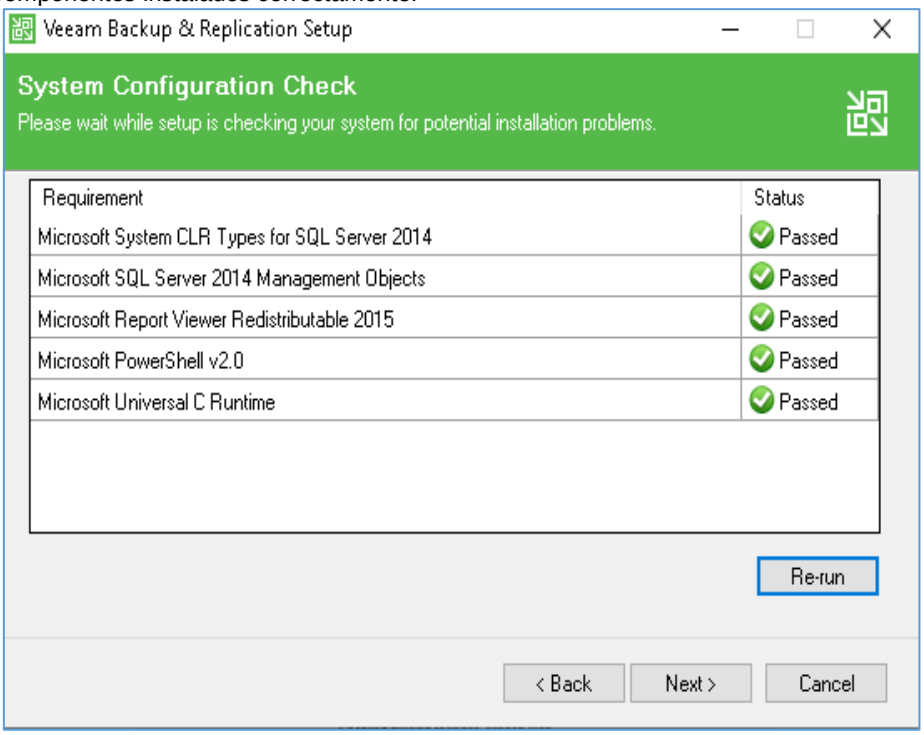
Fuente: Propia.

Figura 48. Verificación de componentes e instalación de los restantes.



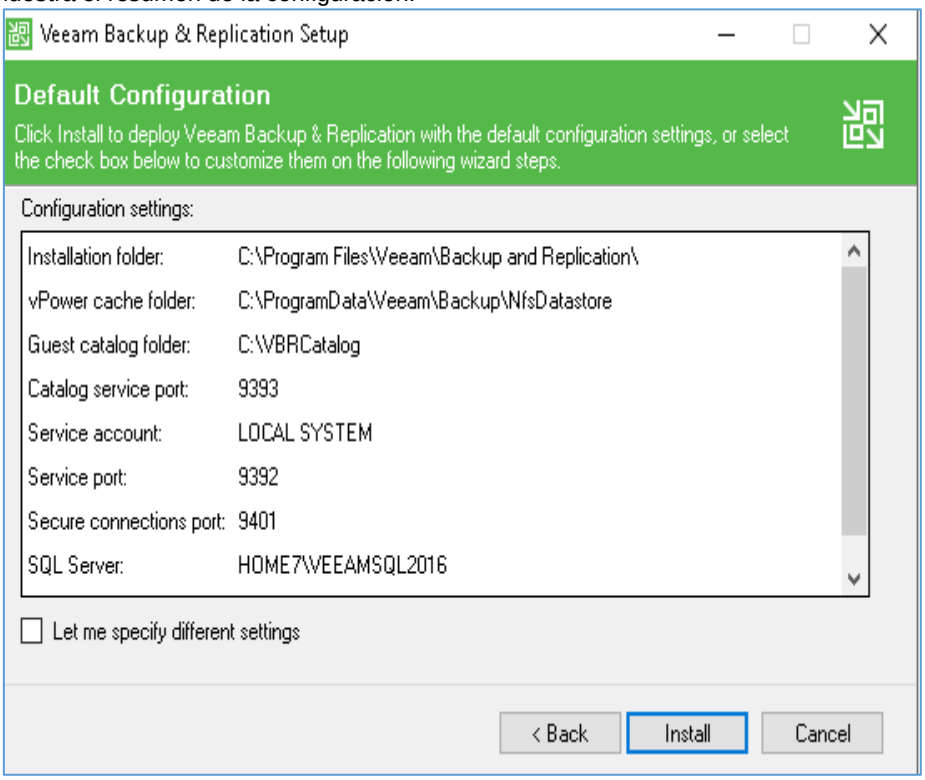
Fuente: Propia.

Figura 49. Componentes instalados correctamente.



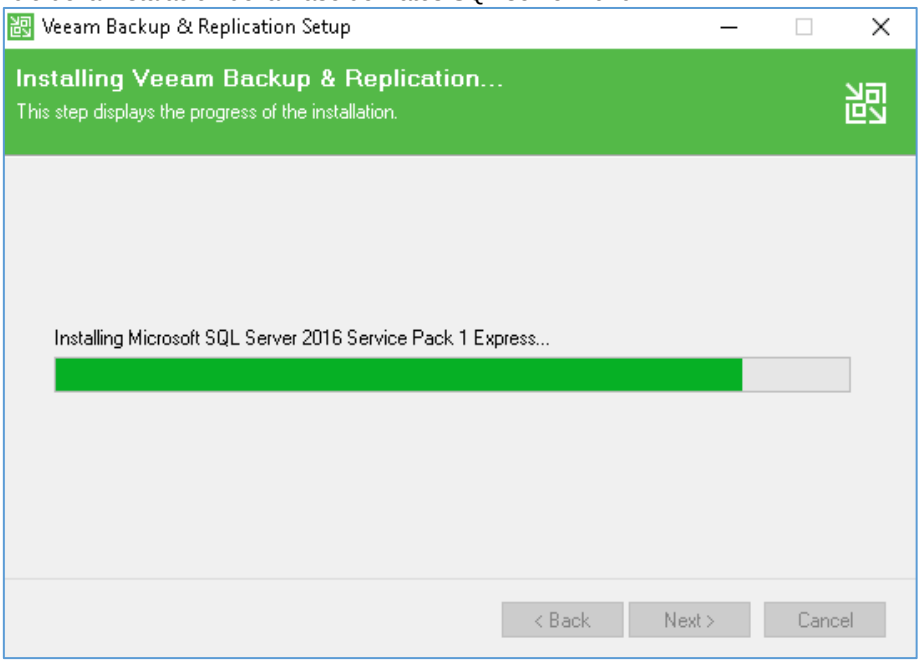
Fuente: Propia.

Figura 50. Muestra el resumen de la configuración.



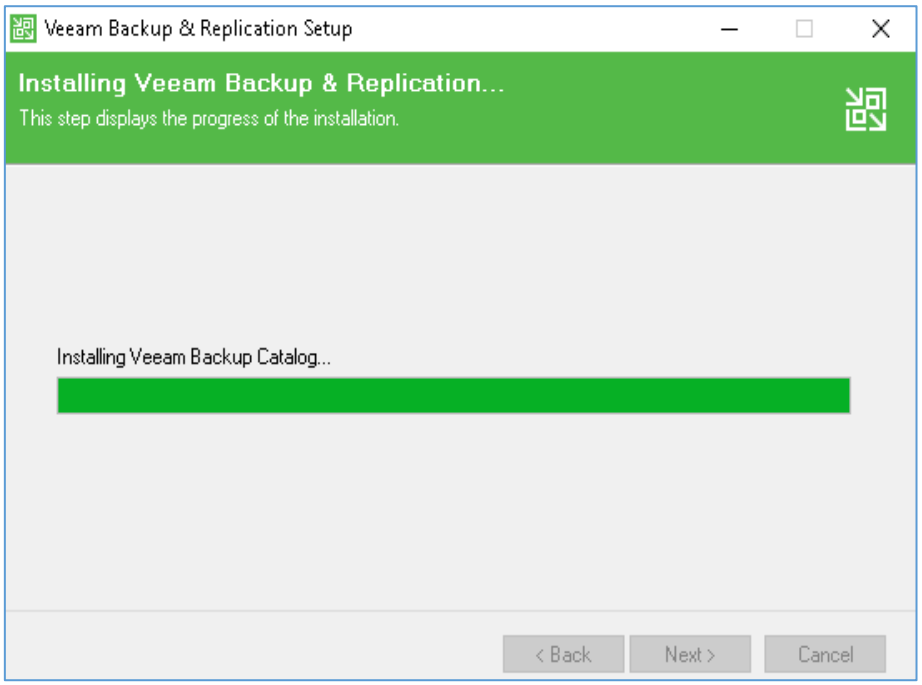
Fuente: Propia.

Figura 51. Inicio de la instalación de la Base de Datos SQL server 2016.



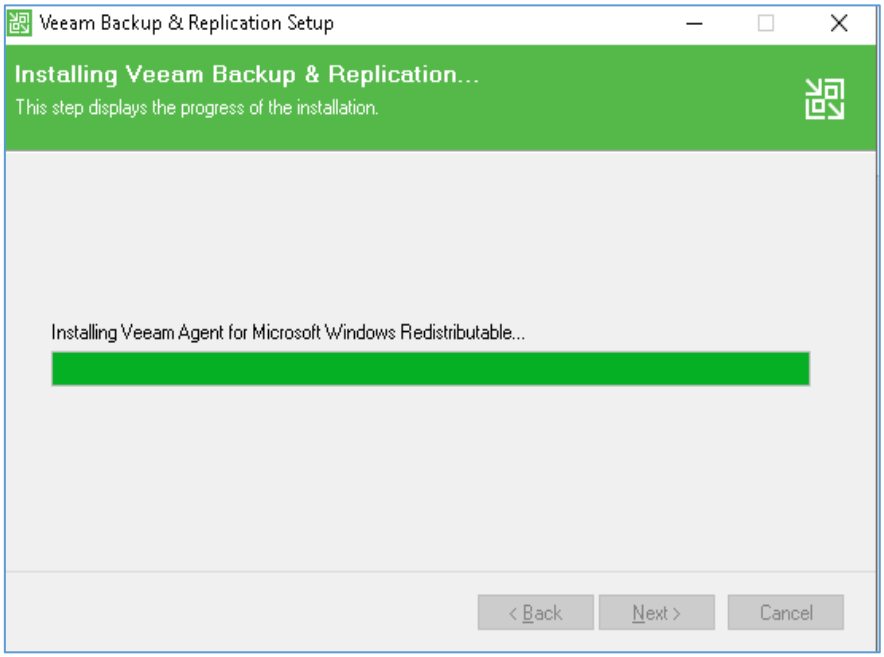
Fuente: Propia.

Figura 52. Continua con la instalación de los catálogos.



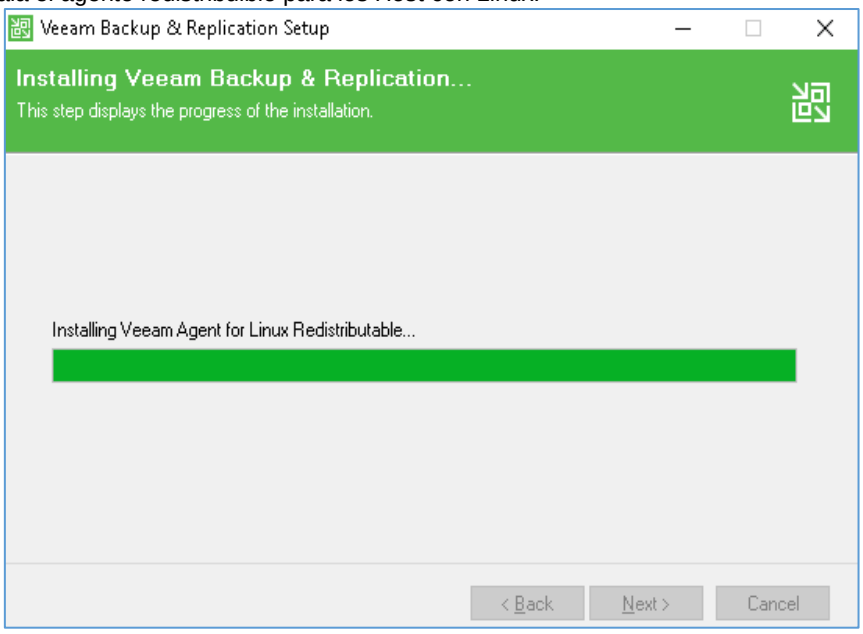
Fuente: Propia.

Figura 53. Instala el agente redistribuible para los Host con Windows.



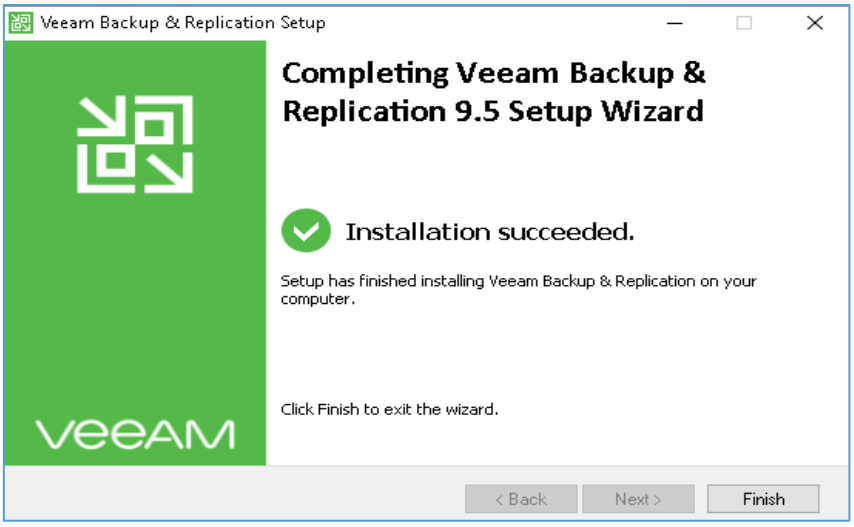
Fuente: Propia.

Figura 54. Instala el agente redistribuible para los Host con Linux.



Fuente: Propia.

Figura 55. Finaliza la instalación.

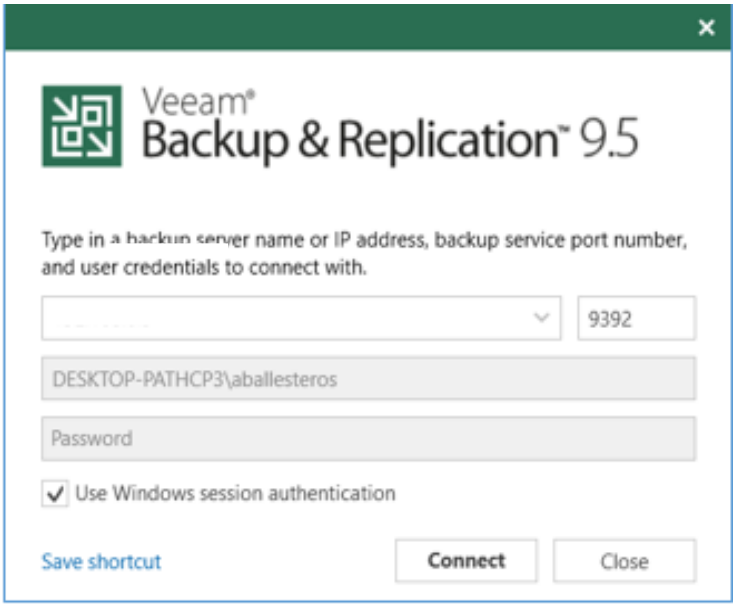


Fuente: Propia.

Una vez terminada la instalación y reiniciado el ordenador se procede a ingresar a la consola de administración para este caso se autenticará con el mismo de inicio de sesión de Windows:

Usuario: aballesteros
Contraseña: 1234.abcd
IP: 204.17.5.5
Puerto: 9392

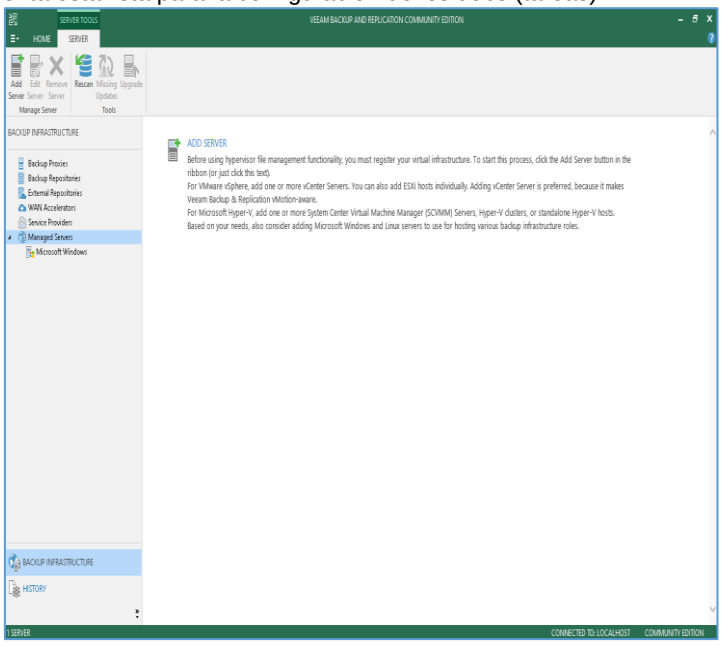
Figura 56. Inicio de sesión a la consola de administración de Veeam Backup C.E.



Fuente: Propia.

Después de haber ingresado a la sesión de la consola de administración de forma correcta, donde se valida a nivel de red el hosname, IP y puerto 9392, está disponible la aplicación para su configuración de los Jobs (tareas) como se puede observar en la siguiente figura.

Figura 57. La herramienta esta lista para la configuración de los Jobs (tareas)



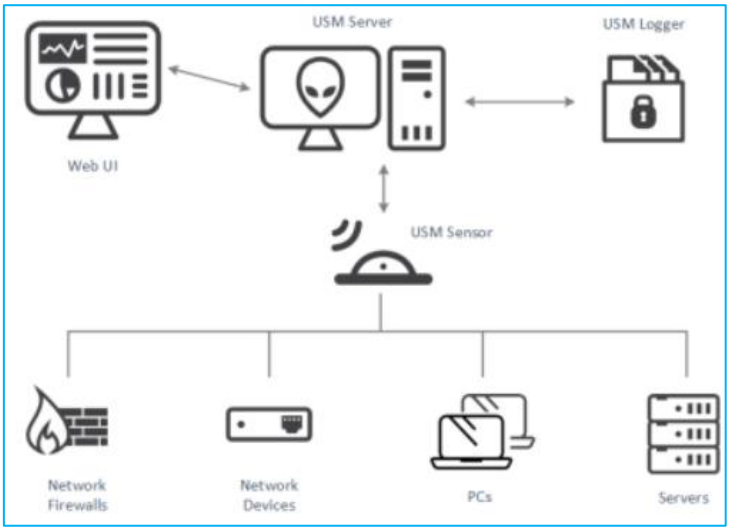
Fuente: Propia.

7.3 CORRELACIONADOR DE EVENTOS ALIENT VAULT OSSIM

La aplicación OSSIM (Open Source Security Information Management) es una herramienta a nivel de red para prevenir y detectar intrusos permitiendo realizar una recolección de todos los eventos de seguridad que este contenido en la infraestructura informática de esta manera puede hallar patrones significativos que puedan prevenir un inminente ataque informático.

7.3.1 Arquitectura. Esta consta de un servidor con todos los componentes de la aplicación o varios servidores físico o virtual, en la siguiente figura se puede observar los requisitos mínimos para la aplicación.

Figura 58. Arquitectura OSSIM



Fuente: AT&T. Cybersecurity. About USM Appliance System Architecture and Components. [En line]. Disponible https://cybersecurity.att.com/documentation/usm-appliance/system-overview/about-usm-architecture-components.htm

Sus componentes principales del USM (**Unified Security Management)** son los siguientes:

- Sensor USM:

Recopila toda la información de cualquier dispositivo de la red que se quiera administrar a través de un Plugin (complemento) realiza el procesamiento de logs como por ejemplo Firewall, routers, servidores entre otros.

- Servidor USM:

Correlación la información que proveen los sensores, tiene un panel de administración, se pueden genera informes y gestión de la herramienta.

- USM Logger:

Almacena de forma segura los eventos recolectados sin ser procesados esto es muy útil y valioso para una investigación de informática forense.

- Web UI:

Es la interfaz que permite administrar la aplicación de un entorno gráfico y de forma dinámica a través de un navegador web compatible Firefox, Chrome, Internet Explorer en sus versiones más recientes.[73]

7.3.2 Instalación y configuración de OSSIM. Para la instalación se debe cumplir con un mínimo de características de hardware ya sea que sea físico o virtualizado:

Procesamiento: 4 Cores.
Memoria Ram: 8 G.B.
Almacenamiento: 32 G.B.

Tarjeta de Red: de 2 puertos ethernet o embebidos en el servidor.

Una vez se cumpla con el mínimo de requerimientos de hardware se realiza la descarga de la imagen ISO desde la página Oficial de Alient Vault OSSIM esta contiene la máquina virtual preconfigurada (Appliance) con la aplicación y distribución Linux Debian 9 Stretch, de esta manera se identifica que la distribución de linux y compatibilidad de la aplicación es definida previamente por el proveedor no disponiendo para realizar una instalación por separado aplicación vs sistema operativo.[74]

Después de realizar el despliegue del (Appliance) a través del Hypervisor se procede ingresar por la interfaz web, donde se solicita para el ingreso por primera vez crear una cuenta de administración como se observa en la figura.

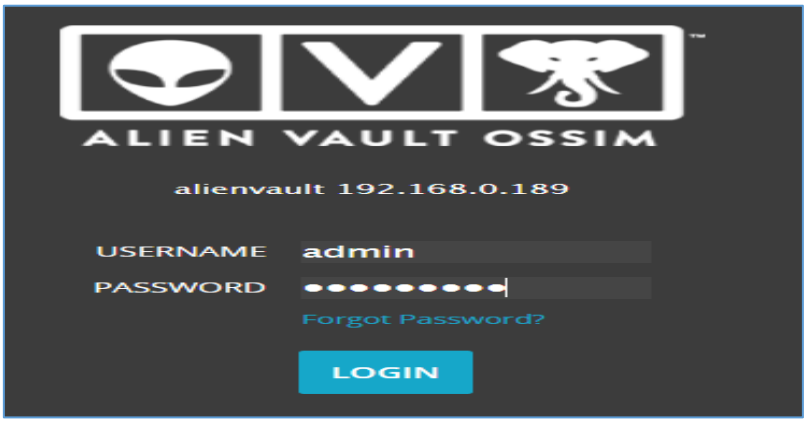
[73] ALIENVAULT. AlienVault Unified Security Management (USM) for Security Engineers. LAN Guide. AlienVault USM for Security Engineers v5.3.4 Rev A. [En linea] 2017.Pag. 1. [Citado: 5 abril. 2020] [En linea].Disponible https://www.dbi-services.com/wp-insides/uploads/2017/09/AlienVault-USM-5.3.4-Rev-A-for-Security-Engineers-Lab-Guide.pdf

[74] AT&T CYBERSECURITY. USM Appliance Deployment Types. AlienVault USM Appliance deployment solutions. [En linea] Disponible https://cybersecurity.att.com/documentation/usm-appliance/deployment-plan/about-usm-deployment-types.htm?tocpath=Documentation%7CAlienVault%C2%AE%20USM%20Appliance%E2%84%A2%7CDeployment%20Guide%7CUSM%C2%A0Appliance%20Deployments%7C_____1

Figura 59. Se ingresa por la interfaz web con la IP asignada.

Fuente: Propia.

Figura 60. Se realiza el proceso de autenticación con el usuario creado admin, password (1234.abcd)



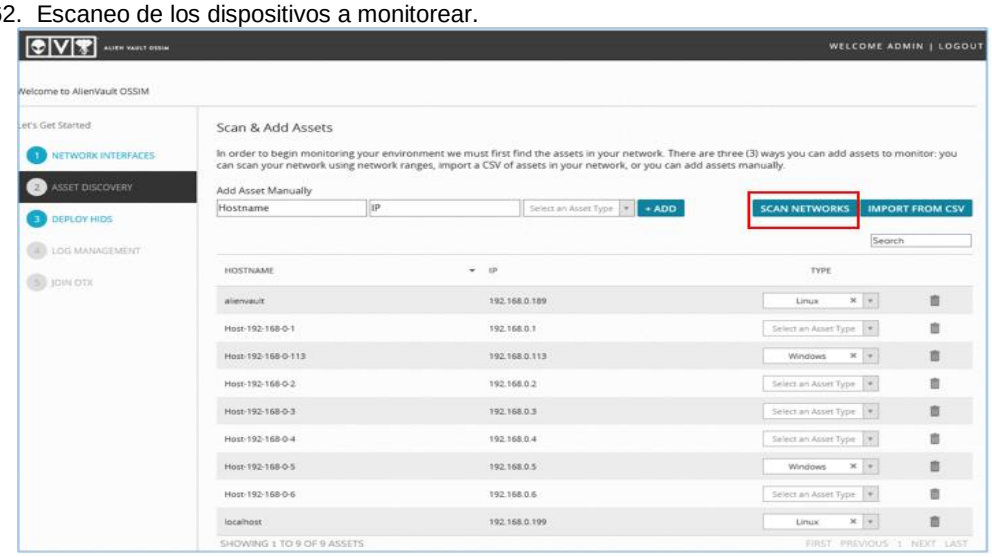
Fuente: Propia.

Figura 61. Aparece la pantalla con el asistente de configuración.

Fuente: Propia.

7.3.3 Prueba uso de la aplicación. Hay 3 maneras de incluir los dispositivos al monitoreo de seguridad por medio manual, escaneado la red o importando un archivo CSV, la manera más práctica es realizarla por scan networks como se observa en la siguiente figura.

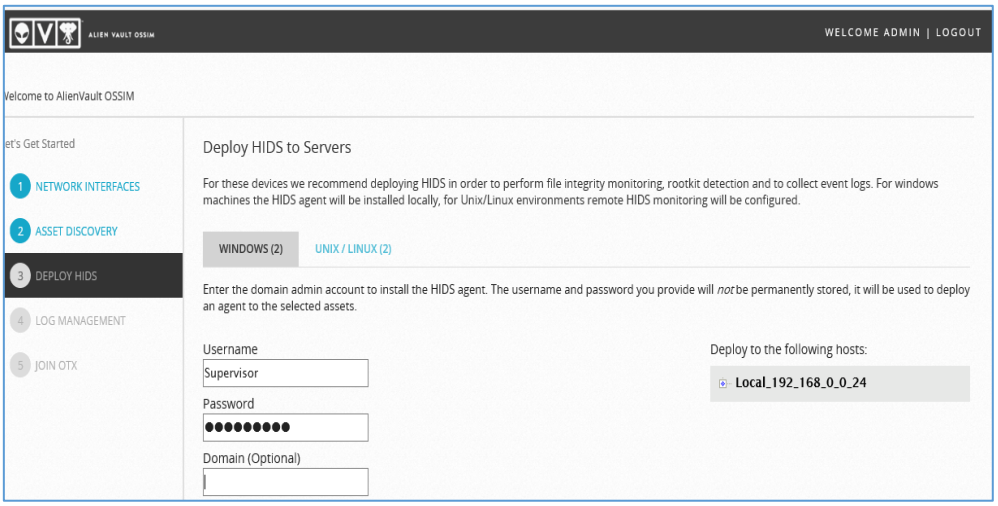
Figura 62. Escaneo de los dispositivos a monitorear.



Fuente: Propia.

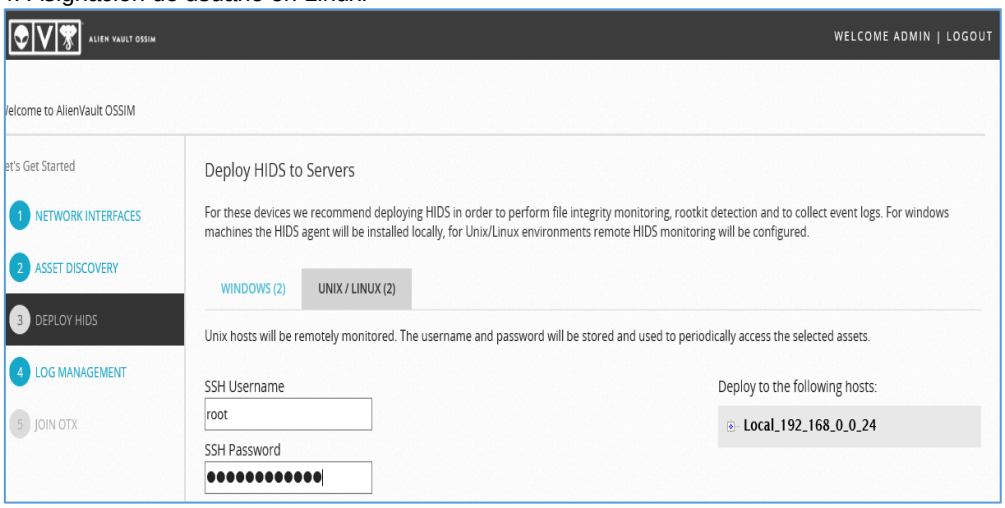
Seguidamente se debe asignar un usuario y contraseña para Windows y otra para linux para la instalación del agente HIDS, hay que tener en cuenta que para el primer sistema operativo se debe estar creado el usuario en todos los Servidores y equipos de cómputo para linux es el mismo usuario que permite conectarse por SSH por lo cual se debe verificar que esté instalado y activo este servicio.

Figura 63. Asignación de usuario en Windows.



Fuente: Propia.

Figura 64. Asignación de usuario en Linux.

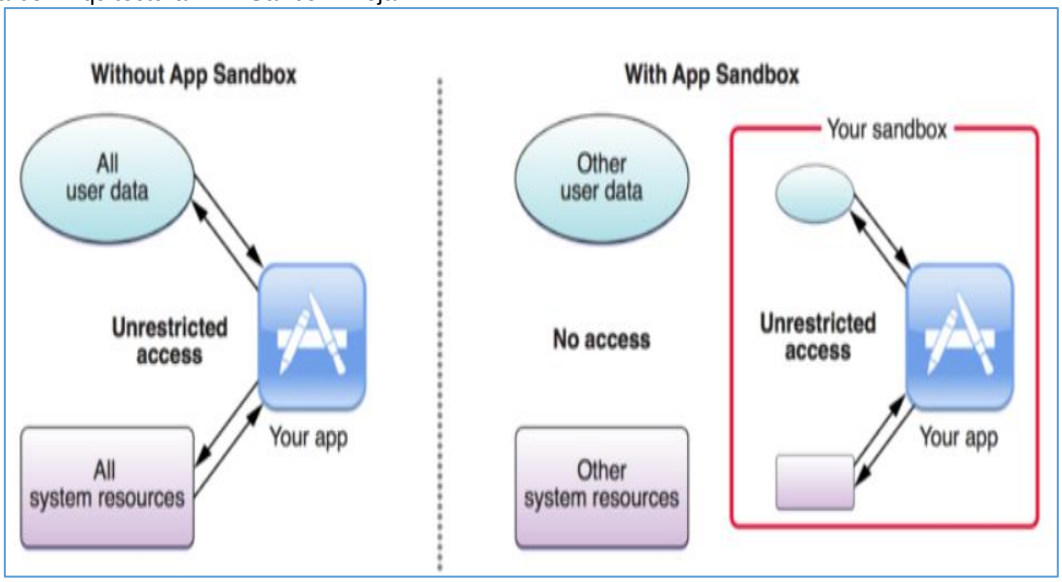


Fuente: Propia.

7.4 SANDBOX FIREJAIL

7.4.1 Arquitectura de la aplicación. Permite ejecutar y probar programas, herramientas y servicios en un segmento de red aislado de producción, usando linux namespaces que se encuentran en el kernel de linux de esta manera se realiza la ejecución de manera controlada en un entorno aislado, en la siguiente figura se puede observar el escenario de la izquierda sin un Sanbox y el de la derecha con Sanbox.

Figura 65. Arquitectura APP Sanbox Firejail.

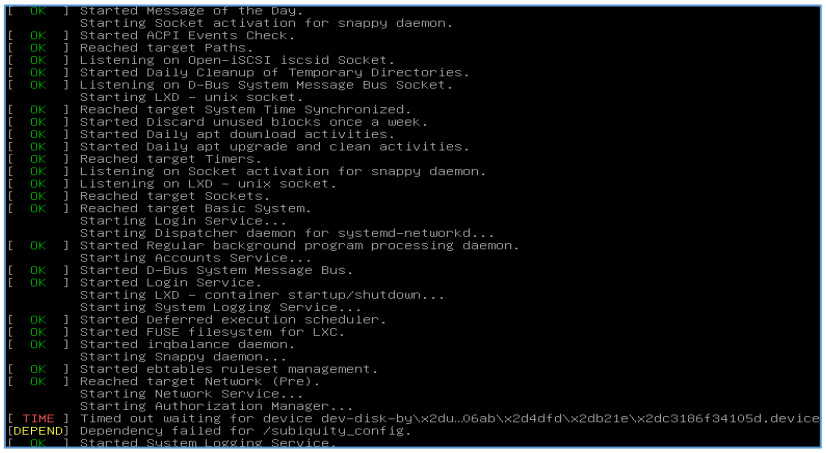


Fuente: TUNNELIX. Operation Prison Break by cyberstorm.mu – Sandboxing and Firejail. [En linea] Disponible https://tunnelix.com/operation-prison-break-by-hackers-mu-sandboxing-and-firejail/

7.4.2 Instalación y Configuración. Este Sanbox Firejail su compatibilidad es enfocada a las distribuciones de Linux, según la comunidad de Firejail[75],está desarrollado haciendo uso del kernel de Linux en el cual se debe habilitar la característica de user-namespaces , se realizara la simulación de la herramienta en la distribución Ubuntu 18.4 LTS la cual tiene soporte por 10 años.[76]

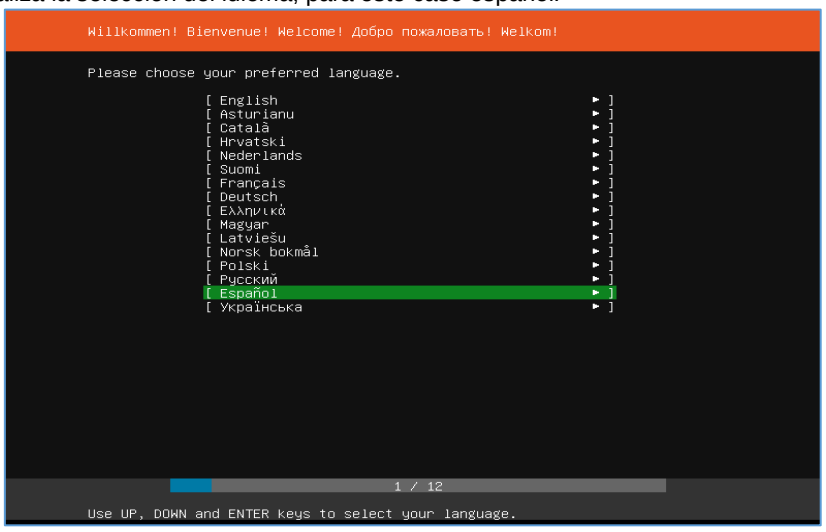
Después de realizar la descarga de la imagen ISO que contiene el instalador de Ubuntu server se inicia el cargue de esta en el Hypervisor e inicia el proceso de como se observa en la siguiente figura.

Figura 66. Inicio de instalación.



Fuente: propia.

Figura 67. Se realiza la selección del idioma, para este caso español.

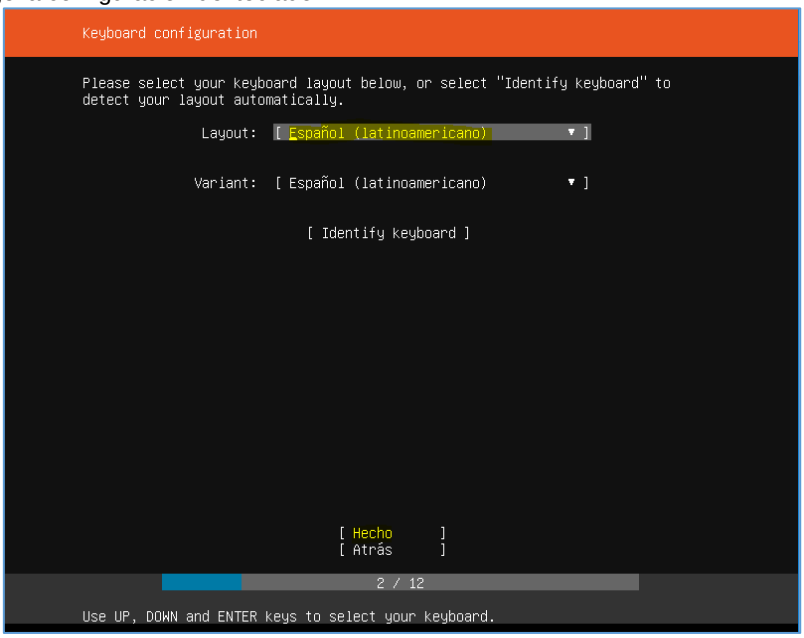


Fuente: propia.

[75] COMUNIDAD FIREJAIL. Firejail Security Sandbox. Firejail Usage. [En linea] Disponible https://firejail.wordpress.com/documentation-2/basic-usage/

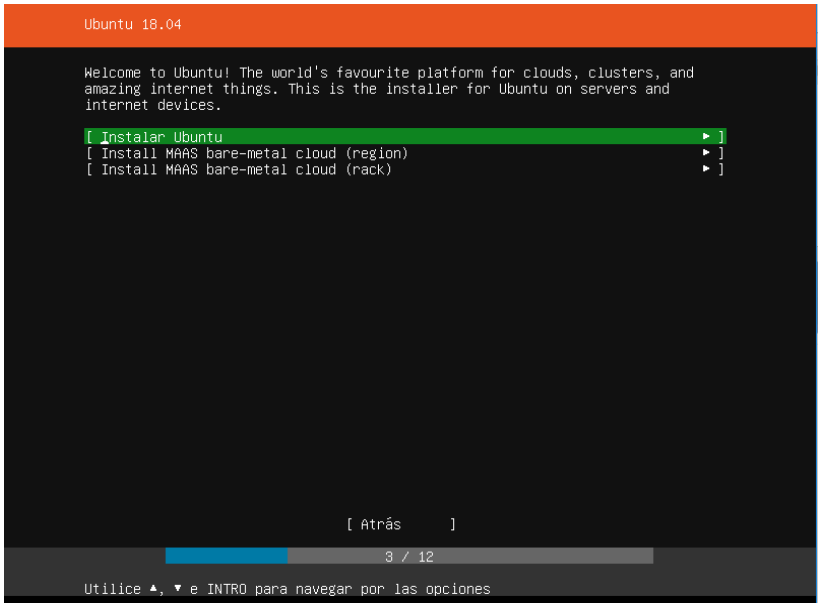
[76] MA-NO.ORG. Ubuntu 18.04 LTS Tendrá 10 Años de Soporte! [En línea] Disponible https://www.ma-no.org/es/redes/servers/ubuntu-18-04-lts-tendra-10-anos-de-soporte

Figura 68. Se elige la configuración del teclado.



Fuente: propia.

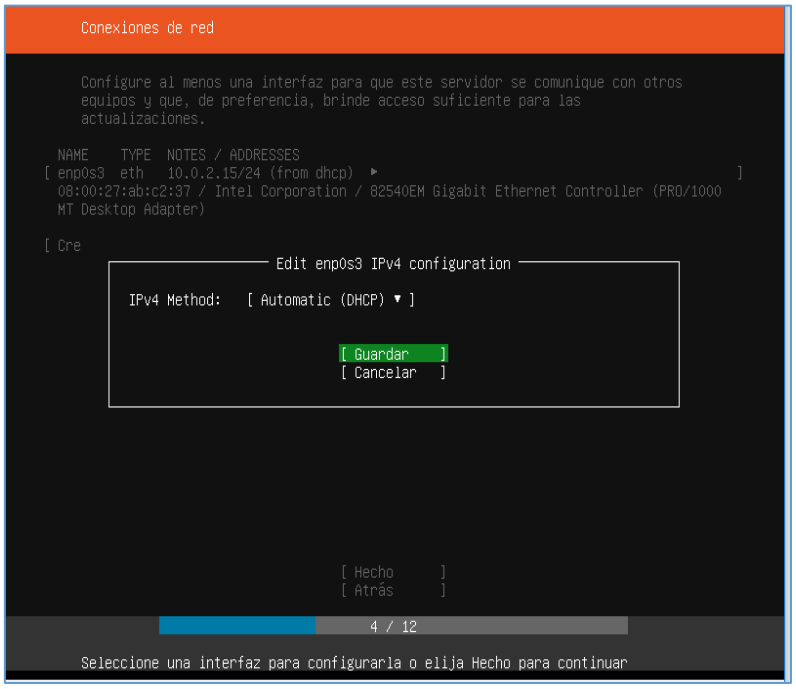
Figura 69. Se continua con la instalación de Ubuntu.



Fuente: propia.

En este paso se puede configurar el direccionamiento IP o realizarlo al finalizar la instalación para esta ocasión se deja por DHCP.

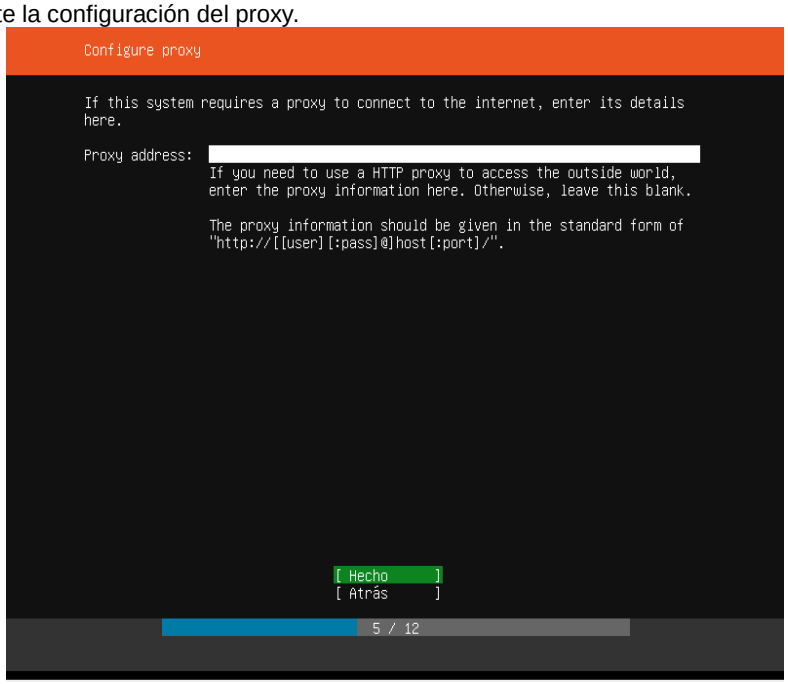
Figura 70. Configuración de direccionamiento IPV 4.



Fuente: propia.

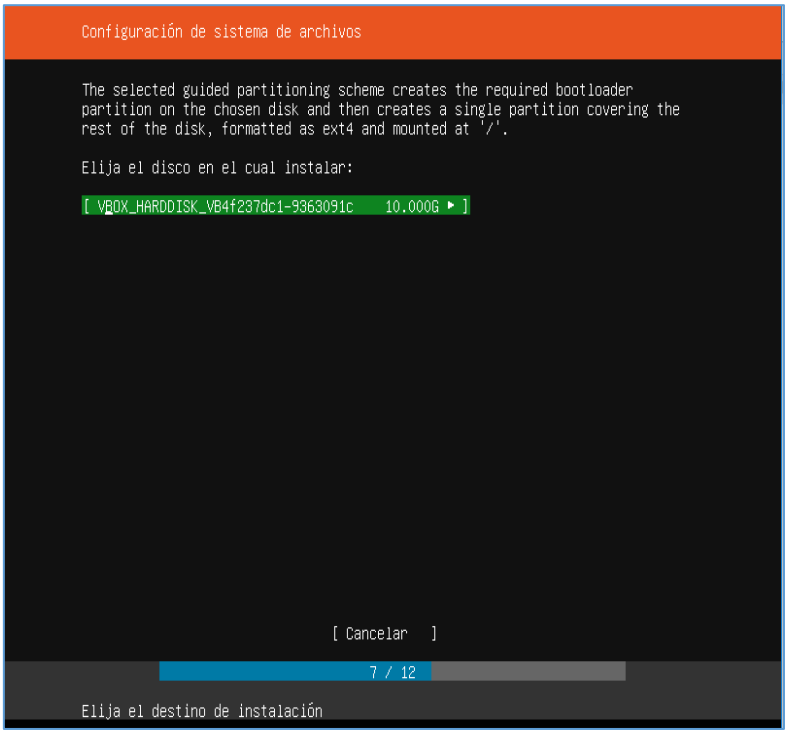
Omitimos los detalles del proxy ya que no se utilizará este servicio para salir a internet.

Figura 71. Se omite la configuración del proxy.



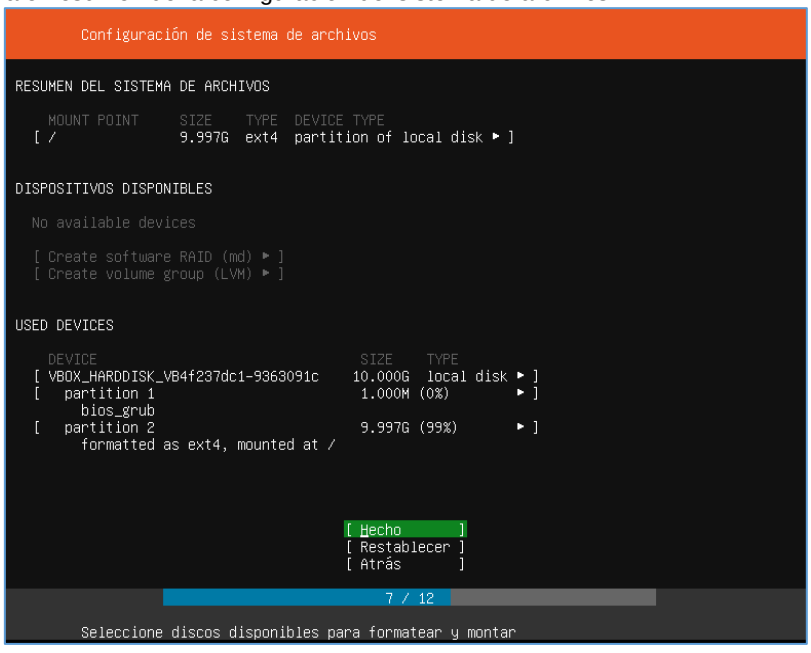
Fuente: propia.

Figura 72. Se confirma el disco donde se instalará Ubuntu.



Fuente: propia.

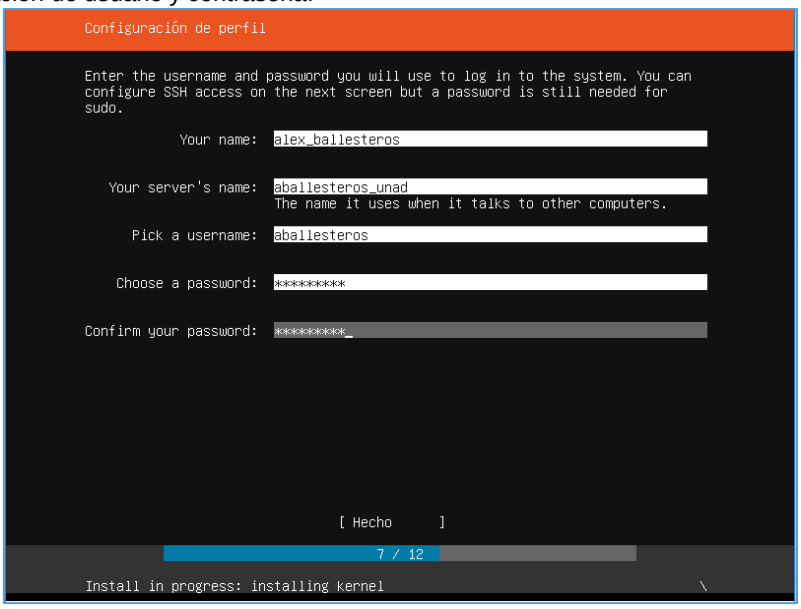
Figura 73. Muestra el resumen de la configuración del sistema de archivos.



Fuente: propia.

Colocamos los datos del perfil como se observa en la siguiente imagen.
Usuario: aballesteros
Password: 1234.ABCD

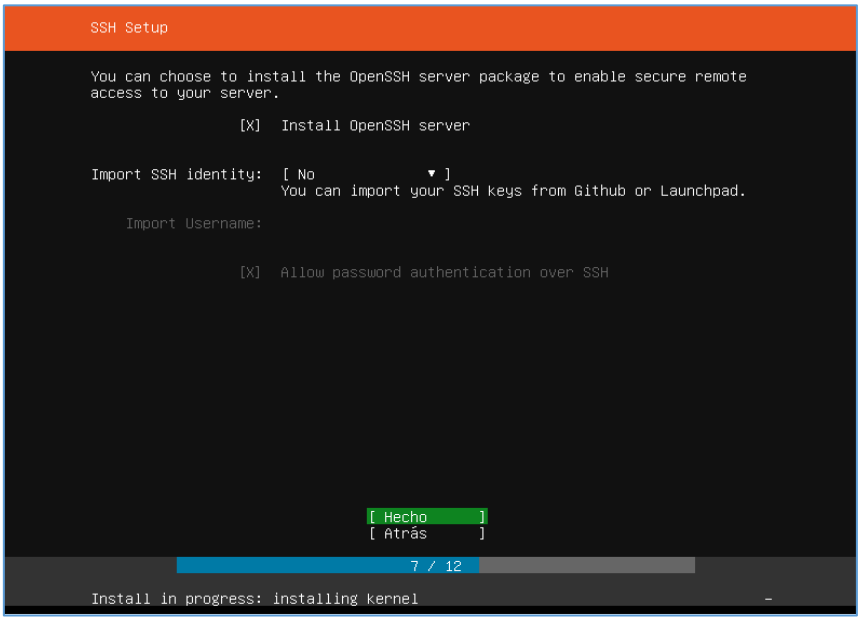
Figura 74. Asignación de usuario y contraseña.



Fuente: propia.

Se habilita para que durante la instalación de Ubuntu se cargue el paquete OpenSSH para acceder a este servidor remotamente.

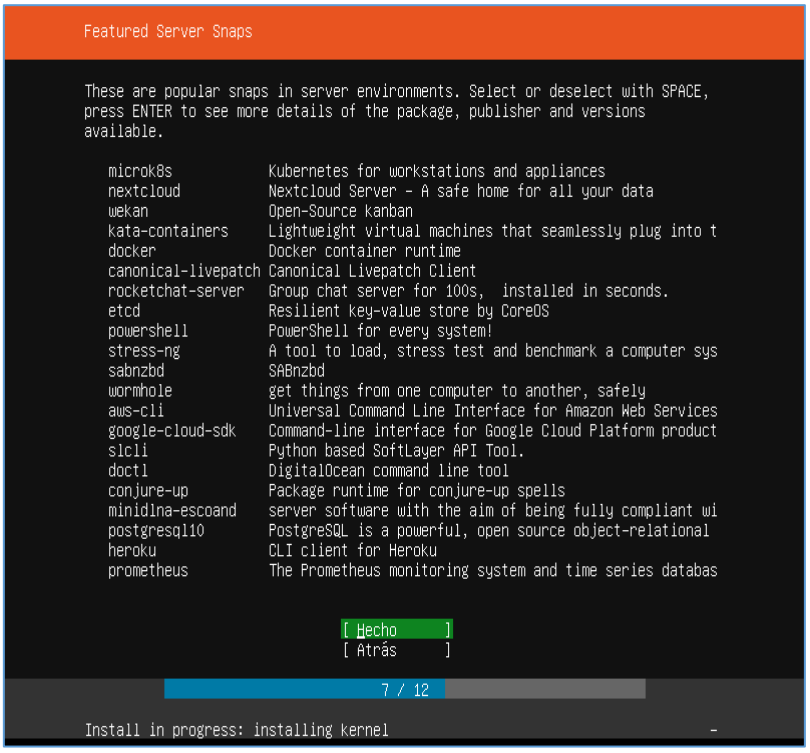
Figura 75. Instalación de Open SSH para administración remota.



Fuente: propia.

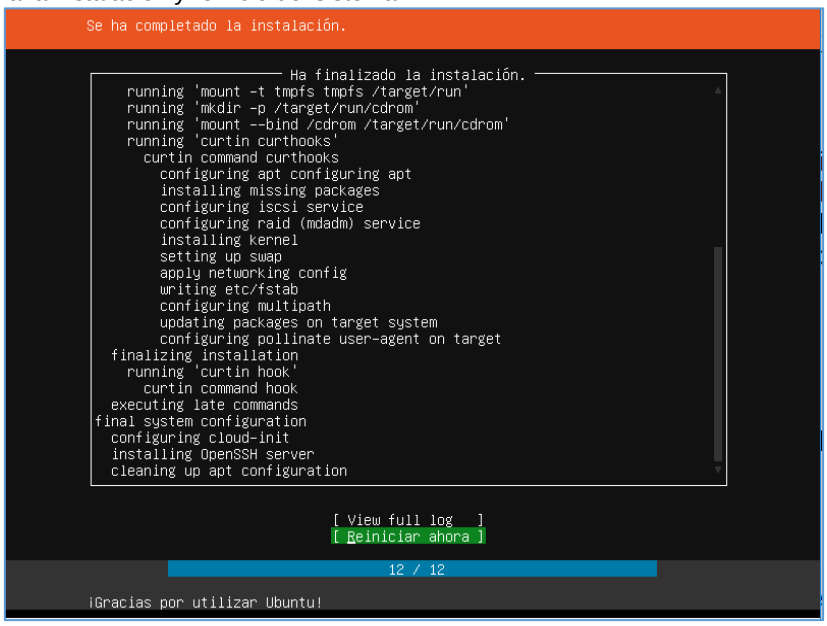
Al continuar con la instalación se puede observar en la siguiente figura los paquetes a instalar.

Figura 76. Paquetes a instalar.



Fuente: propia.

Figura 77. Finaliza la instalación y reinicio del sistema.



Fuente: propia.

Para finalizar la instalación se realiza la configuración acuerdo al apartado (6.2.5.3 Red Pruebas) donde se define el direccionamiento Ip para esta Red la cual está aislada de la red Corporativo y utiliza diferente proveedor ISP.

7.4.3 Video Laboratorio Controlado. Una vez realizada la instalación y configuración del mínimo de servicios virtualizados como son monitoreo (Pandora FMS), correlacionador de eventos (Open Vault OSSIM), backup (Veeam Backup C.E.) y Sandbox (Firejail) para ejecutar las tareas del CSIRT, se realizó un video donde se describe ingreso a la consola de administración y características generales ya que para un nivel intermedio y avanzado del manejo de estas es necesario la consulta de manuales, videos y cursos los cuales se encuentran en sus páginas oficiales, comunidades asociadas a estos proyectos entre otros.

A continuación, se encuentra el link de acceso al video publicado en la plataforma YouTube con la socialización del Proyecto de Grado fase 1.

Se sugiere reproducir este desde el navegador Google Chrome o Mozilla Firefox en sus últimas versiones.

https://www.youtube.com/watch?v=ftr_zQWbU8g&feature=youtu.be

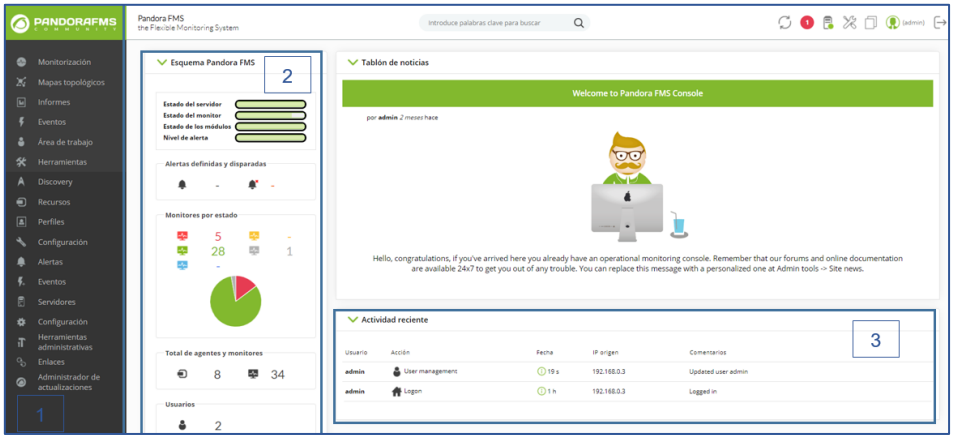
8 DOCUMENTACIÓN TÉCNICA PARA EJECUTAR LAS TAREAS DEL CSIRT

Para realizar las tareas en el CSIRT es necesario contar con el mínimo de servicios los cuales son Monitoreo (Pandora FMS), Copias de Seguridad (Veeam Backup C.E.) Correlacionador de eventos (Alient Vault OSSIM) y Sandbox (Firejail), a continuación, se describen las tareas cotidianas realizadas en cada uno de los servicios mencionados.

8.1 PANDORA FMS COMMUNITY EDITION

Esta herramienta de monitoreo es interactiva y cuenta con amplia documentación en su portal oficial lo cual permite adquirir experticia de forma gradual realizando las tareas diarias de monitoreo, en la siguiente figura se observa el ingreso al panel de instrumentos, identificado con el (1) se encuentra el menú principal que permite navegar hacia los deferentes características de la aplicación, con el (2) muestra el esquema que permite visualizar el monitoreo por estado, total de agentes, monitores y usuarios conectados, en el (3) permite ver las actividades recientes.

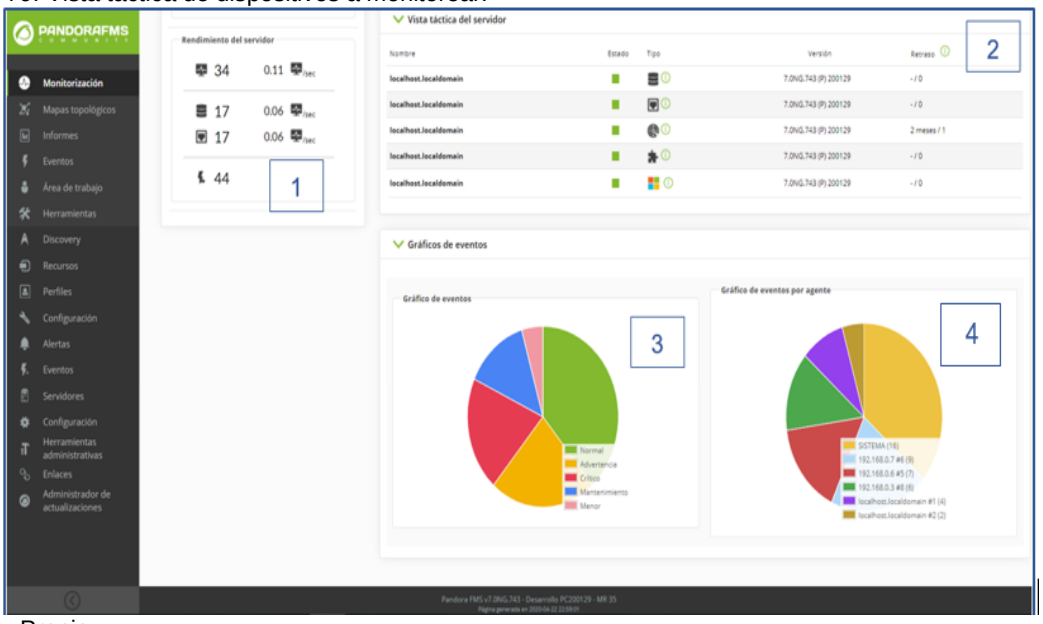
Figura 78. Panel de instrumentos.



Fuente: Propia.

Al ingresar por la opción de monitoreo, vista táctica, como se puede observar en la siguiente figura permite al operador de monitoreo del CSIRT tener información de primera mano cómo es el rendimiento de los servidores en el numeral (1), en el numeral (2) la vista táctica de los servidores (nombre, tipo de sistema operativo, versión del agente instalado entre otra información) en el gráfico de eventos identificado con el (3) permite ver el grafico identificando los eventos por colores verde para un estado normal y rojo para un estado crítico entre otros, para el numeral(4) muestra el gráfico de eventos por agente de los diferentes dispositivos que realiza monitoreo la herramienta, lo anterior permite identificar rápidamente en color rojo advierte que hay 7 eventos que requieren atención.

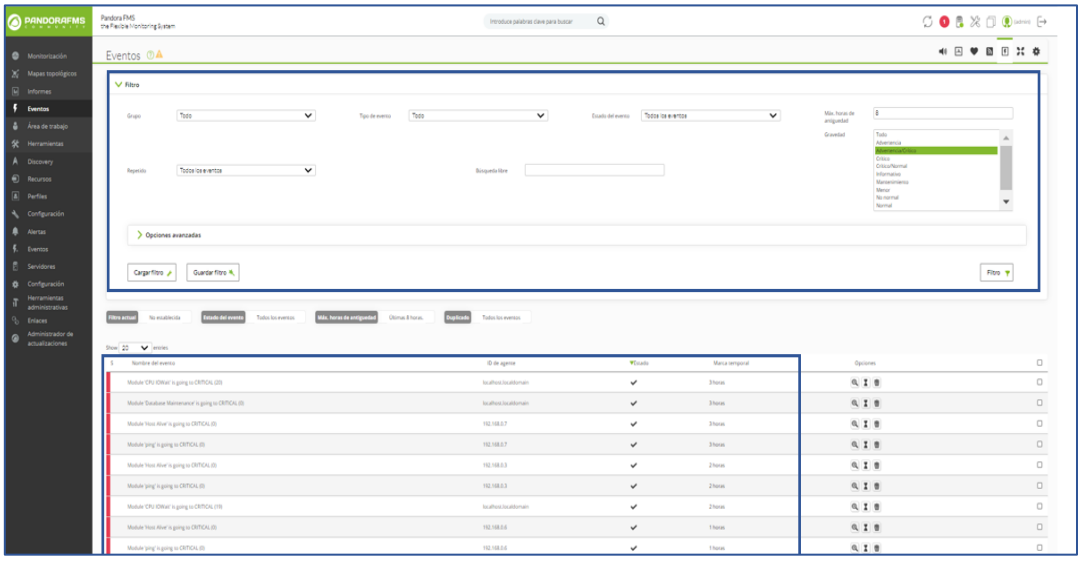
Figura 79. Vista táctica de dispositivos a monitorear.



Fuente: Propia.

El menú eventos permite realizar un filtro por grupo, por tipo, por estado, si es repetitivo y por su gravedad, al aplicar esta muestra los resultados permitiendo identificar el nombre, dispositivo entre otros valores para realizar una acción más efectiva y asertiva, ver figura.

Figura 80. Filtrado de eventos.

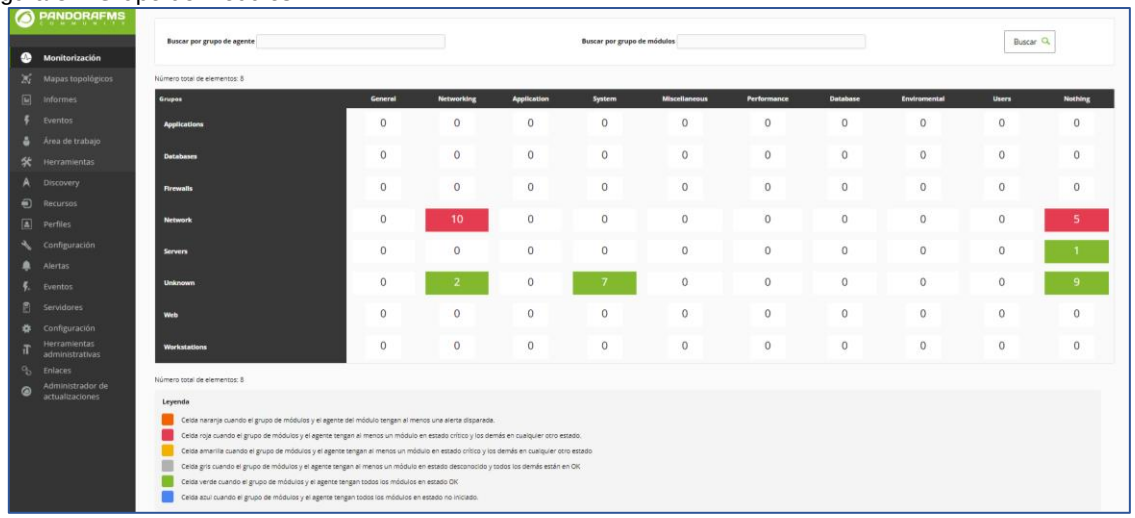


Fuente: Propia.

Al ingresar por el menú monitoreo, submenú grupo de módulos, permite tener una visión global de las alertas de los dispositivos los cuales se relacionan por grupos y aplicaciones, facilitando identificar los diferentes

estados y alertas desde normal en color verde hasta un estado crítico en color rojo, al final de la figura se pueden observar las convenciones según el tipo de estado.

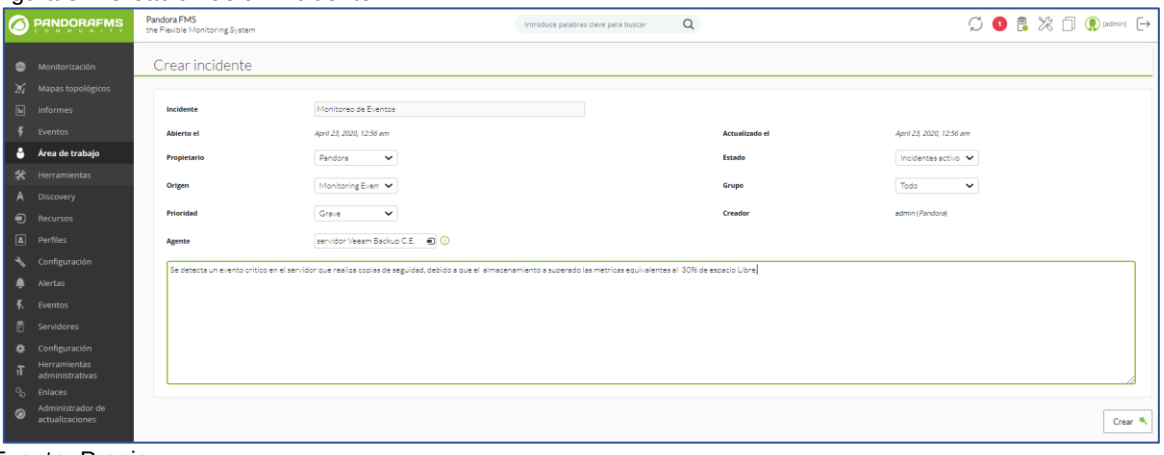
Figura 81. Grupo de módulos.



Fuente: Propia.

En el menú de área de trabajo, submenú incidente, como se observa en la siguiente figura se puede crear un incidente colocando la prioridad, el grupo, el origen del evento para este caso es de monitoreo y un breve comentario, lo cual permite llevar la trazabilidad de todos los incidentes reportados y encontrados convirtiéndose esta herramienta en el primero filtro para dar respuesta a los incidentes activos y reactivos en el CSIRT.

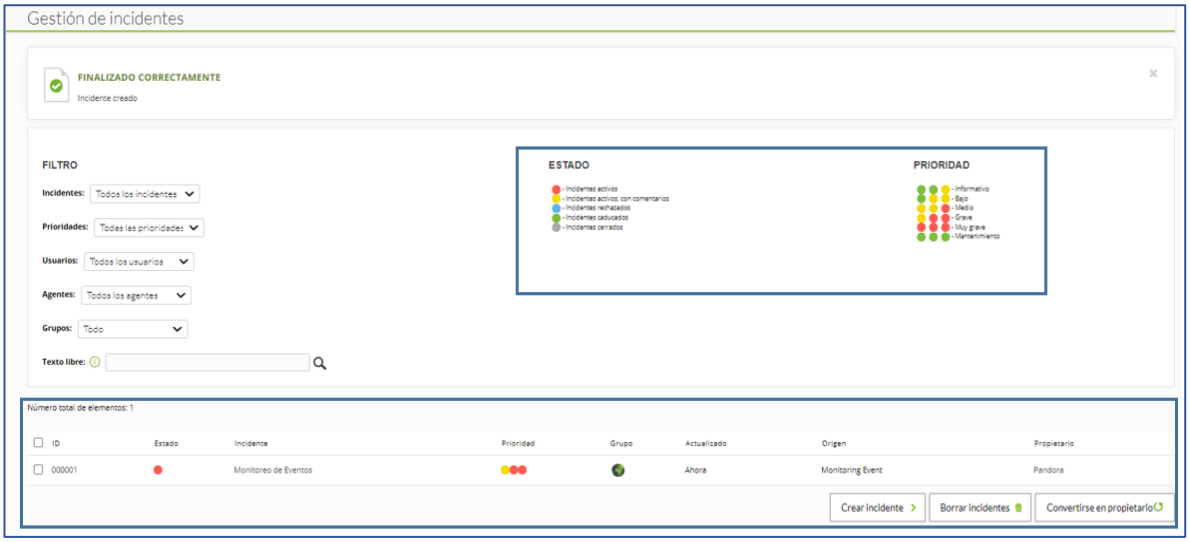
Figura 82. Creación de un incidente.



Fuente: Propia.

Una vez creado el incidente se regresa a la ventana del área de trabajo donde se puede gestionar estos, creando nuevos, borrando, volviéndose propietario de este, también permite realizar filtros a demás muestra las convenciones de estos por estado y prioridad como se puede observar en la siguiente figura.

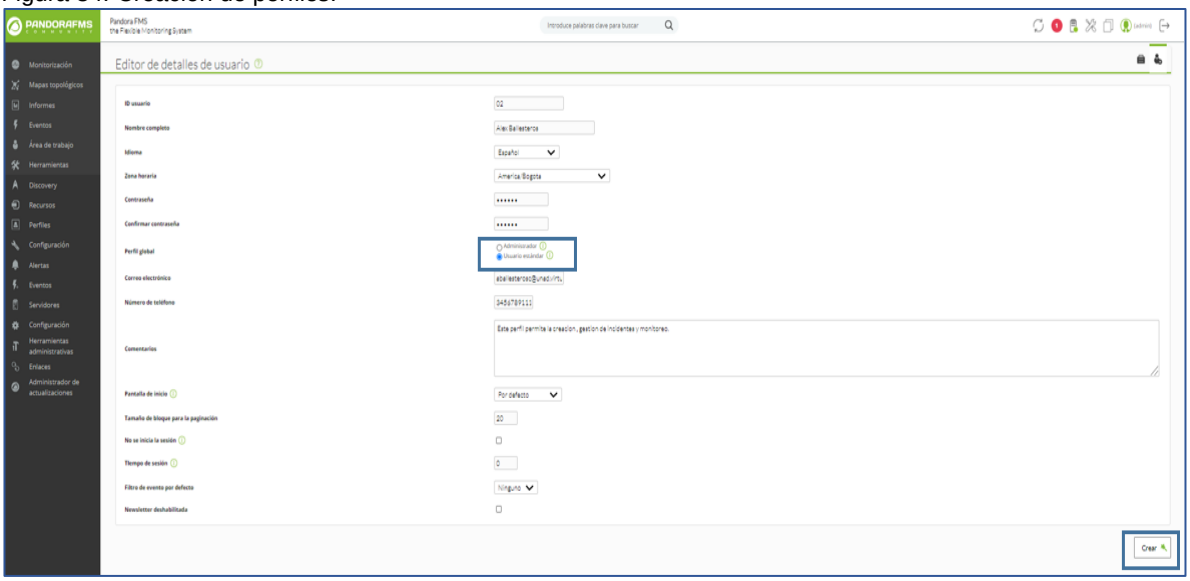
Figura 83. Gestión de incidentes.



Fuente: Propia.

Por el menú perfiles permite la correcta gestión de estos controlar acceso no autorizado, prevenir errores accidentales, sabotaje del sistema, realizar configuraciones innecesarias entre otros, en figura se puede observar la creación de un perfil estándar el cual permite solamente el monitoreo, gestión y creación de incidentes, notas entre otras tareas cotidianas de la herramienta de monitoreo.

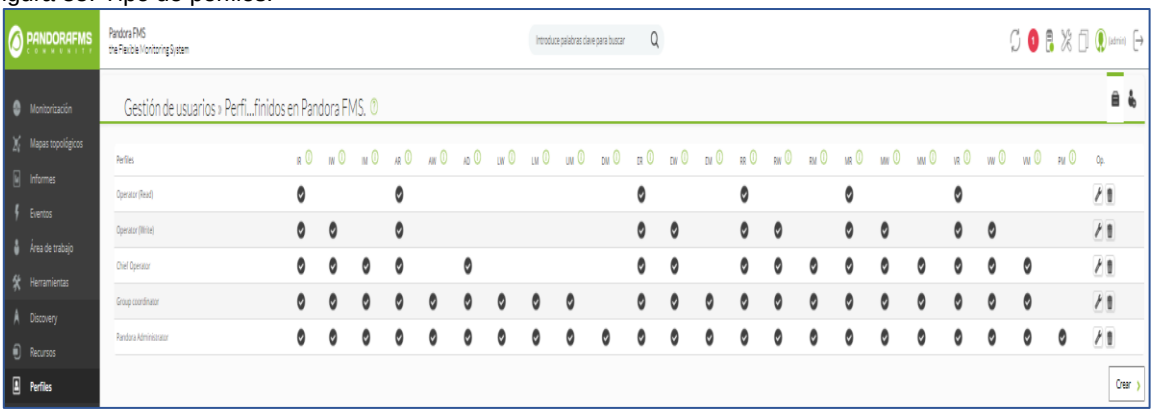
Figura 84. Creación de perfiles.



Fuente: Propia.

A continuación, se observa el tipo de perfiles y las características.

Figura 85. Tipo de perfiles.



Fuente: Propia.

De igual manera se puede realizar la conversión de cada atributo para la creación del perfil, ver figura.

Figura 86. Lista de perfiles.

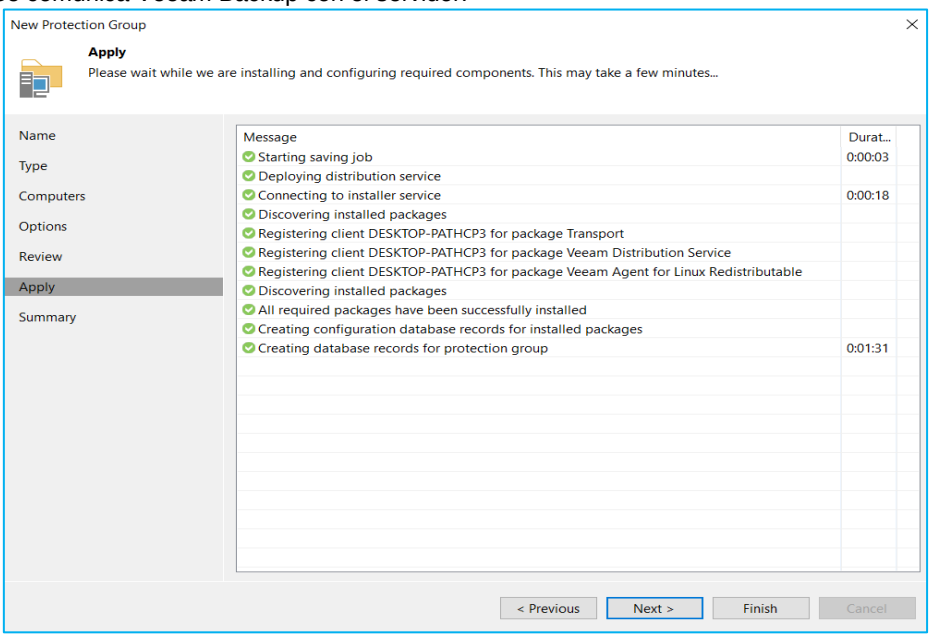
Operación	Bit de acceso
Ver datos agente (todas las vistas)	AR
Vista táctica	AR
Vista de grupos	AR
Crear un visual console	RW
Crear un informe	RW
Crear una gráfica combinada	RW
Ver informe, gráfica, etc	RR
Aplicar una plantilla de informe	RR
Crear una plantilla de informe	RM
Ver evento	ER
Validar/Comentar evento	EW
Borrar evento	EM
Ejecutar respuestas	EW

Fuente: PANDORAFMS. Documentation es: Gestión y Administración. Lista de perfiles. [En linea]. Disponible https://pandorafms.com/docs/index.php?title=Pandora:Documentation_es:Gestion_y_Administracion

VEEAM BACKUP COMMUNITY EDITION

Esta aplicación es interactiva y cuenta con amplia documentación en su portal oficial lo cual permite adquirir experticia de forma gradual realizando las tareas diarias de Backup, se inicia el procedimiento para respaldar el servidor de Pandora FMS, con la instalación del agente de Veeam que permite tener comunicación entre esta aplicación y el servidor virtual al que se requiere hacer el respaldo, como se observa en la siguiente figura en el primer paso la herramienta establece comunicación con el servidor.

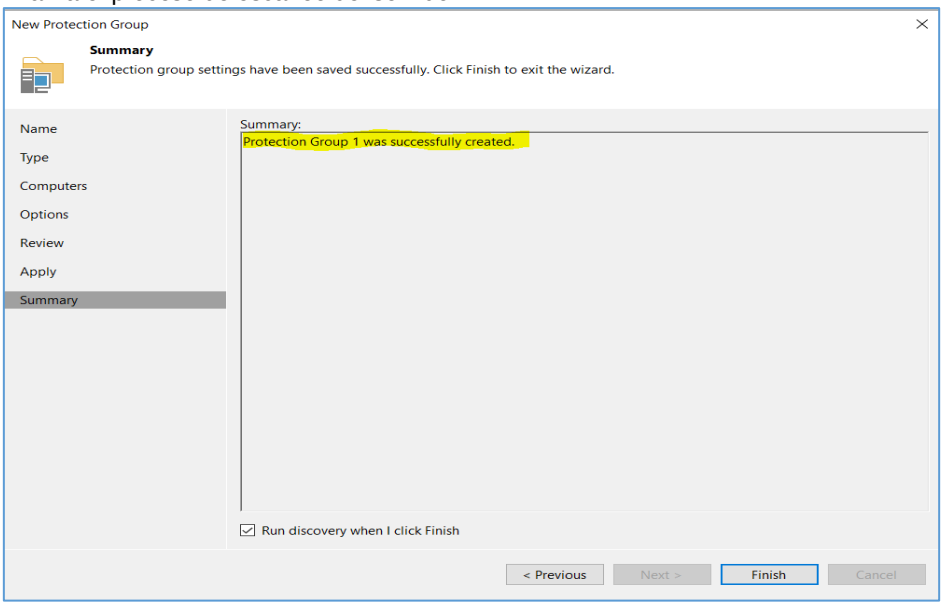
Figura 87. Se comunica Veeam Backup con el servidor.



Fuente: Propia.

Termina la configuración de forma correcta, ver figura.

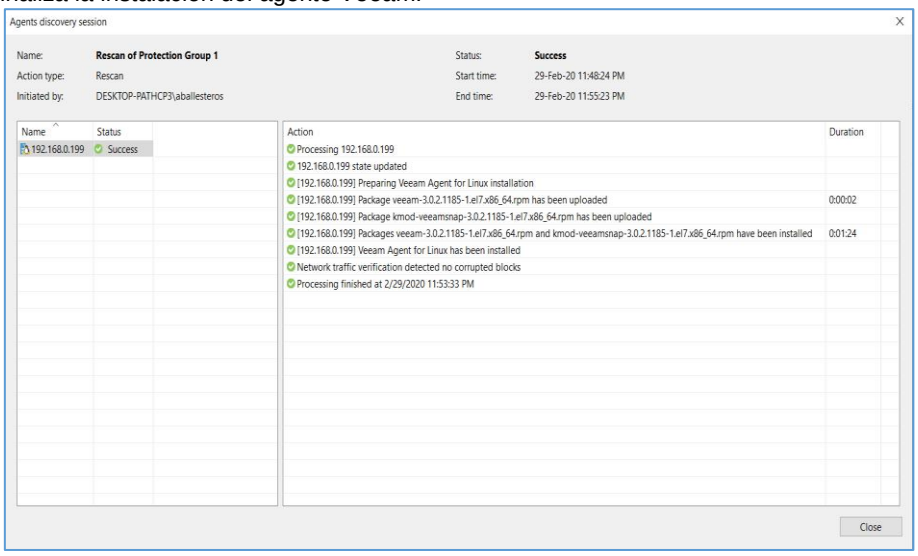
Figura 88. Finaliza el proceso de escaneo del servidor.



Fuente: Propia.

Se procederá a instalar el paquete en el servidor virtual de pandora FMS, ver figura.

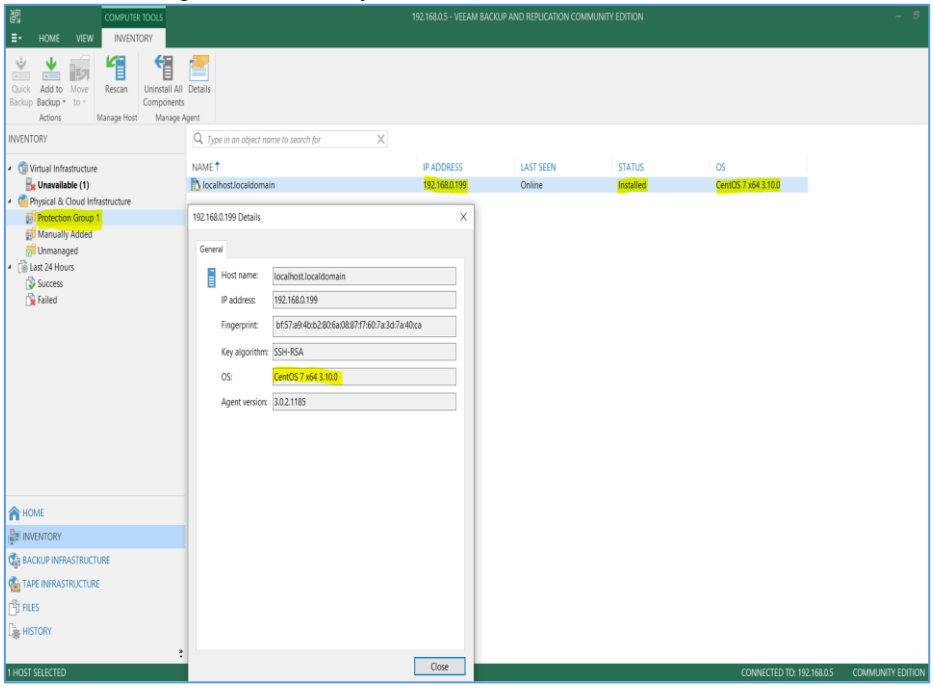
Figura 89. Finaliza la instalación del agente Veeam.



Fuente: Propia.

En la siguiente figura muestra la información de uso del Agente.

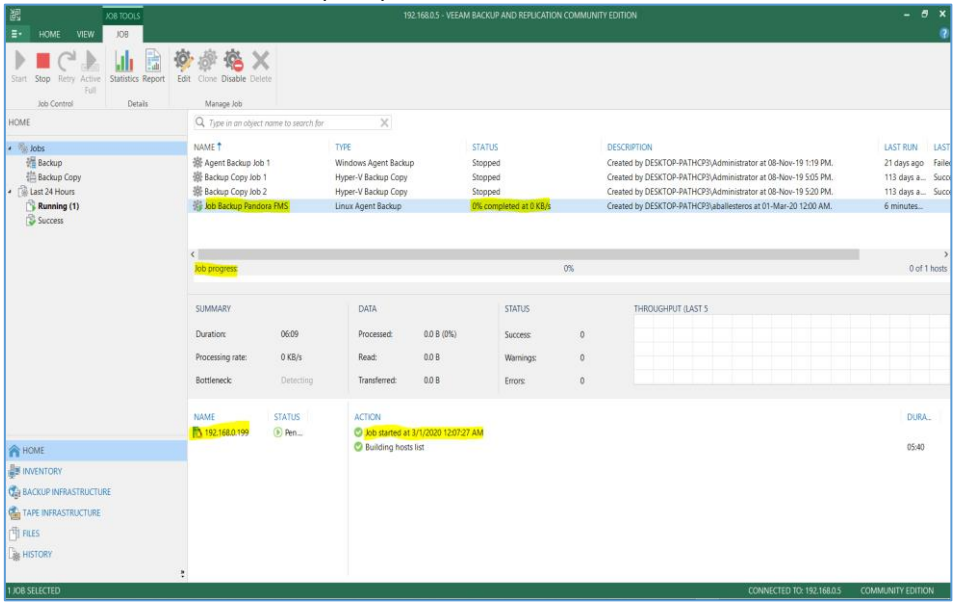
Figura 90. Información del agente de Veeam y servidor virtual Pandora FMS.



Fuente: Propia.

Para iniciar el proceso de configuración y programación del Respaldo de forma automatizada se debe crear un Job (tarea) como se puede observar en la siguiente figura.

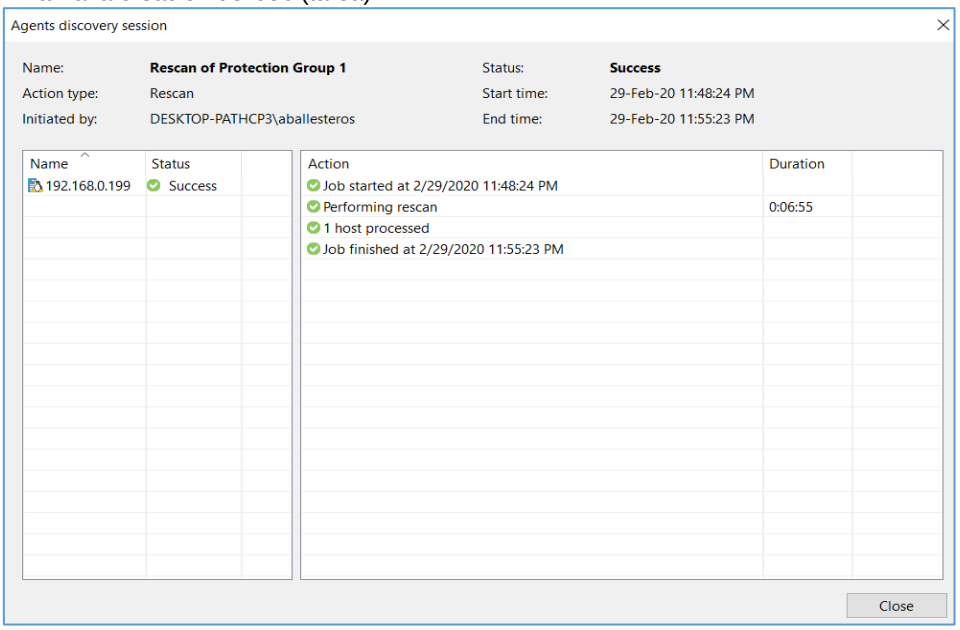
Figura 91. Se realiza la creación de Job (tarea).



Fuente: Propia.

A continuación, se observa el Job (tarea) del Backup Full para la VM Pandora FMS finalizo de forma correcta.

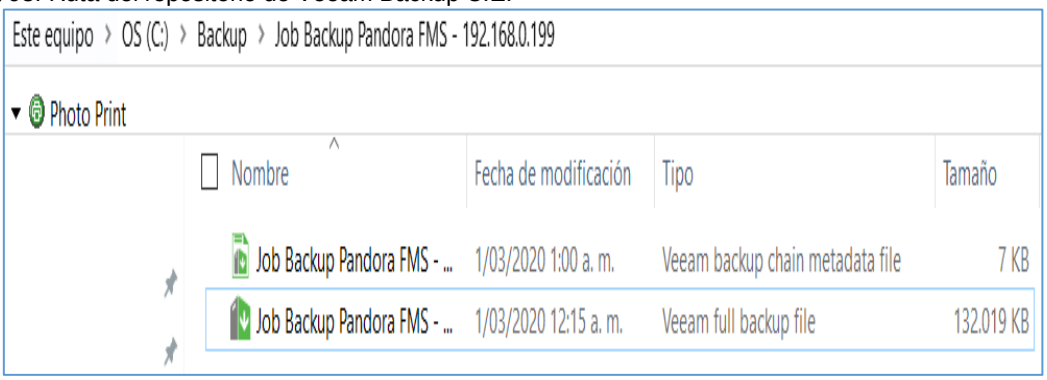
Figura 92. Finaliza la creación del Job (tarea).



Fuente: Propia.

Seguidamente se observar la ruta del respaldo de toda la máquina virtual del backup Full realizado.

Figura 93. Ruta del repositorio de Veeam Backup C.E.

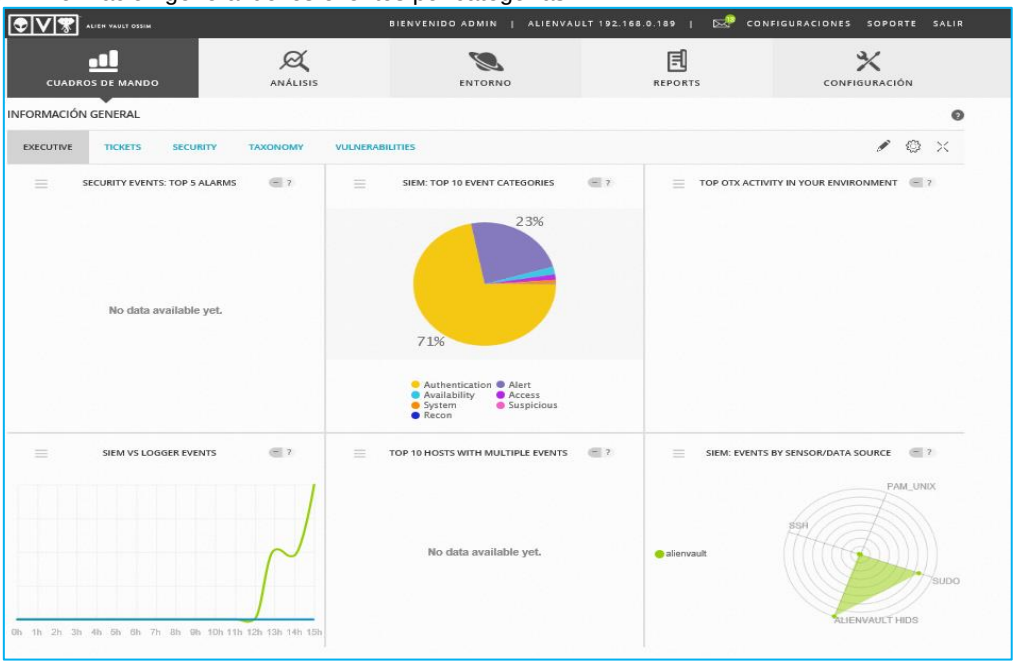


Fuente: Propia.

8.2 ALIENT VAULT OSSIM

Esta aplicación es interactiva y cuenta con amplia documentación en su portal oficial lo cual permite adquirir experticia de forma gradual realizando las tareas diarias del correlacionador de eventos, en la siguiente figura se observa el ingreso al panel de instrumentos, encuentra el menú principal que permite navegar hacia las deferentes características de la aplicación, se visualizan los eventos por categorías como son (autenticación, sistema, alertas, de acceso, sospechosos y habilitados) ver figura.

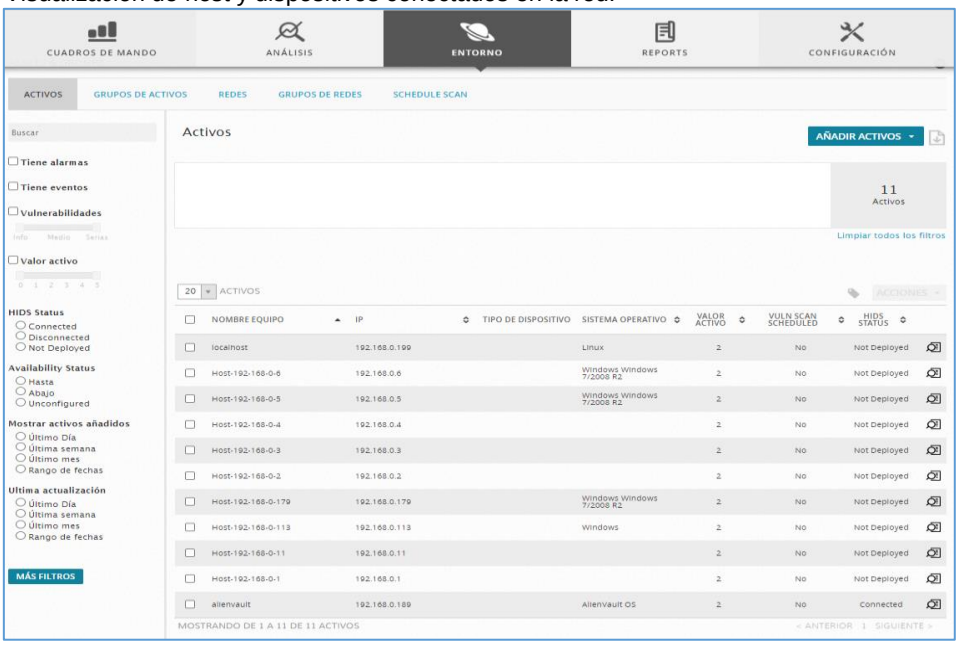
Figura 94. Información general de los eventos por categorías.



Fuente: Propia.

Al ingresar por entorno activos nos permite visualizar los host y dispositivos detectados permitiendo realizar filtros por alarmas, eventos, vulnerabilidades entre otros, como se observa en la siguiente figura.

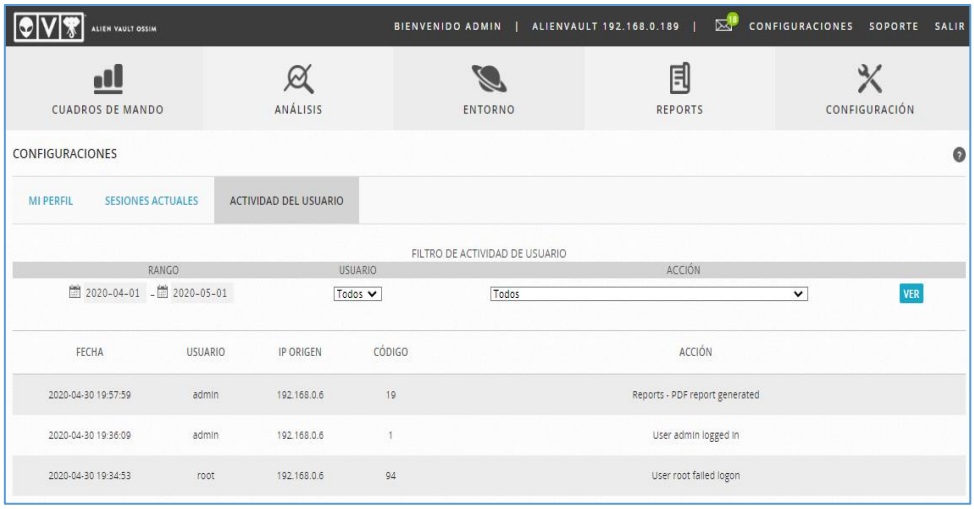
Figura 95. Visualización de host y dispositivos conectados en la red.



Fuente: Propia.

Al realizar un filtro por actividades del usuario del 30 de abril 2020, se evidencia las acciones realizadas como por ejemplo que desde el host ip finalizada en .6, se generó un reporte en formato pdf, ver figura.

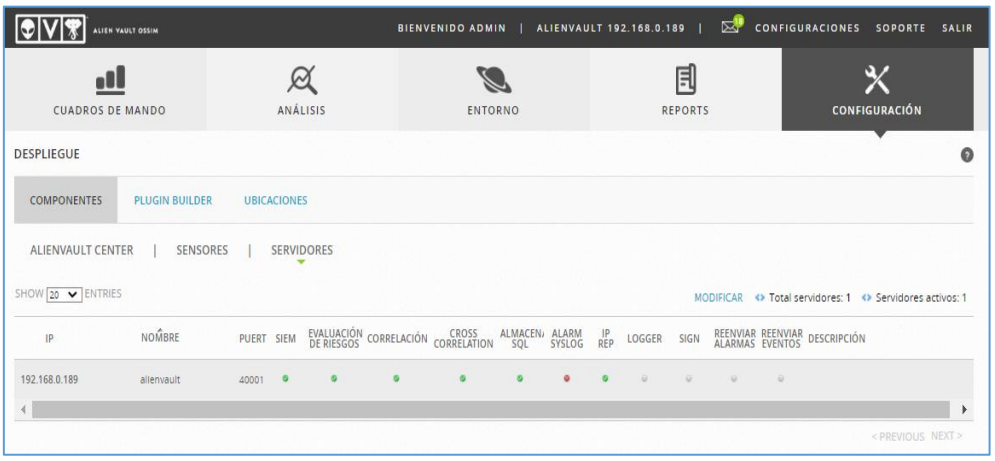
Figura 96. Filtro de actividad de usuario en la red.



Fuente: Propia.

Al ingresar a la opción de configuración en componentes, servidores se puede observar el estado de los parámetros del servidor teniendo información para identificar algún comportamiento inusual en este.

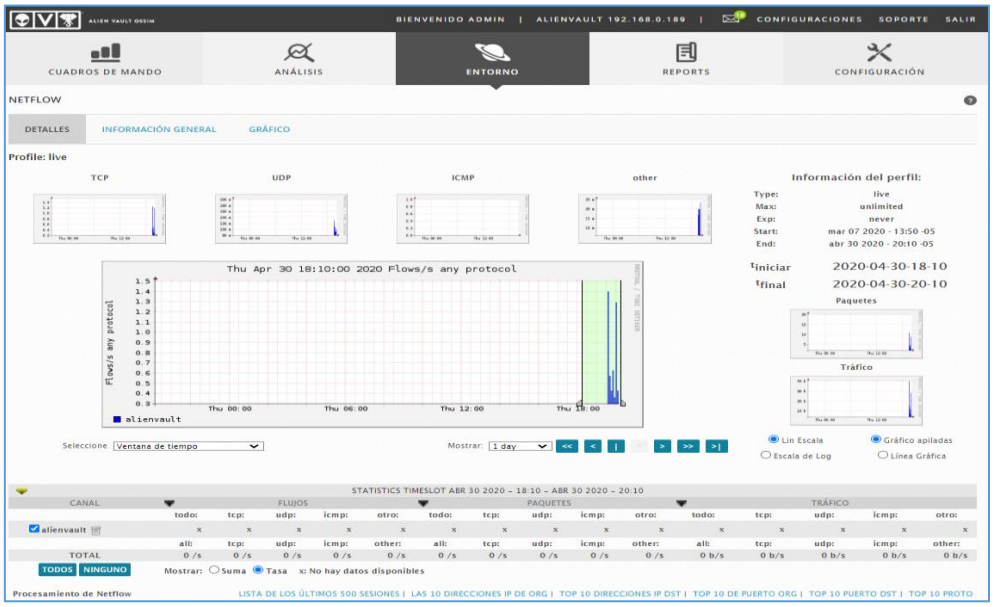
Figura 97. Estado servidor correlacionador de eventos.



Fuente: Propia.

Cuando se ingresa por el menú entorno, submenú Netflow detalles permite recolectar la información sobre el tráfico IP permitiendo monitorizar la red y visualizar las cargas de los distintos protocolos como TCP, UDP, ICMP entre otros.

Figura 98. Detalles Netflow.



Fuente: Propia.

En la siguiente figura muestra por el menú entorno, submenú Netflow, graficas, poder visualizar el tráfico de la red por intervalos de 6 horas, días, semanas y meses.

Figura 99. Graficas tráfico de la red.

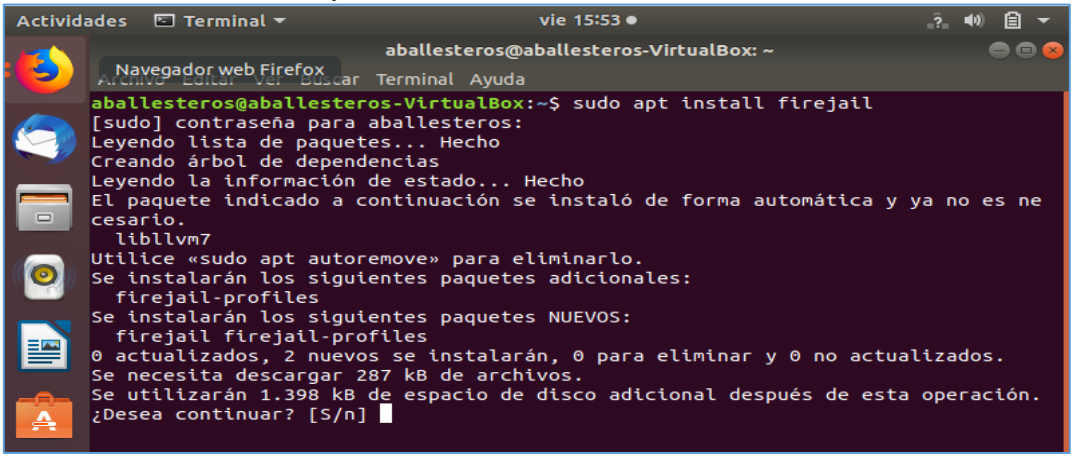
Fuente: Propia.

8.3 SANBOX FIREJAIL

Esta herramienta permite en las diferentes distribuciones de Linux utilizarla cuenta con documentación en su foro oficial de la comunidad lo cual permite ir configurando la herramienta a la medida para realizar las tareas en el CSIRT como es la prueba de programas en un entorno controlado aislado de las redes de la organización.

Después finalizada y configurada la red del servidor virtual, se procede ejecutar el siguiente comando para iniciar la instalación del Sandbox Firejail, como se observa en la siguiente figura.[77]

Figura 100. Inicio instalación de Firejail.

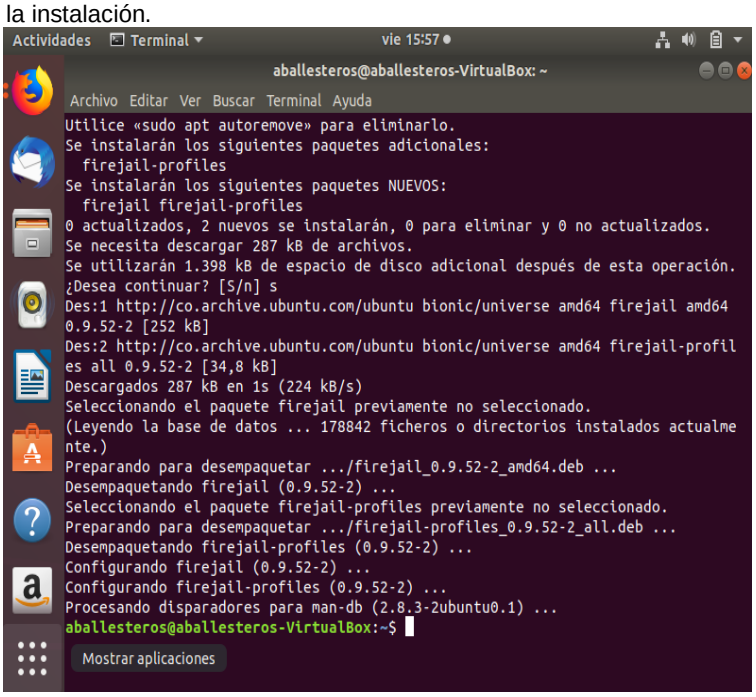


Fuente: Propia.

[77] CARLES, J. Geekland Blog de tecnología. Firejail, un sandbox para Linux para ejecutar programas de forma segura. [En línea] Disponible https://geekland.eu/firejail-sandbox-para-linux/

Seguidamente continua con el desempaquetado, utiliza el disparador man-db y finaliza la instalación, como se puede observar en la siguiente figura.

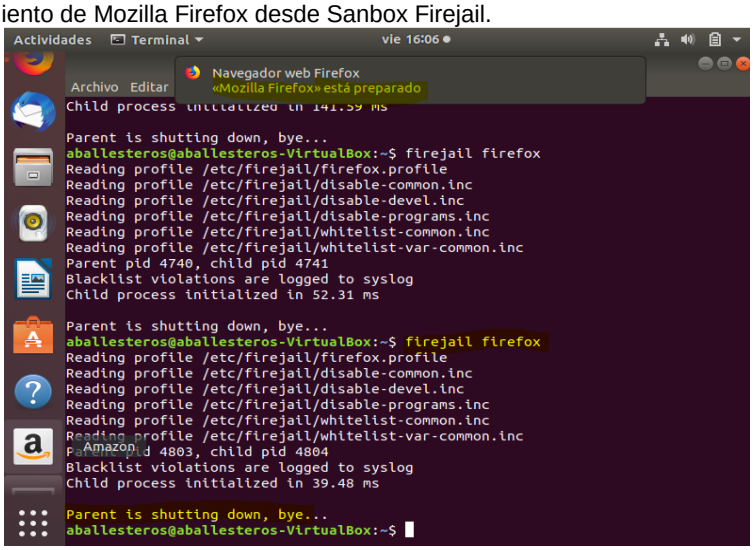
Figura 101. Finaliza la instalación.



Fuente: Propia.

8.3.1 Pruebas con Sanbox Firejail. Para hacer uso del Sandbox se debe anteponer la palabra “Firejail” seguido el nombre de la aplicación que se requiera iniciar por ejemplo se accede al navegador Mozilla Firefox, como se puede observar en la siguiente imagen.

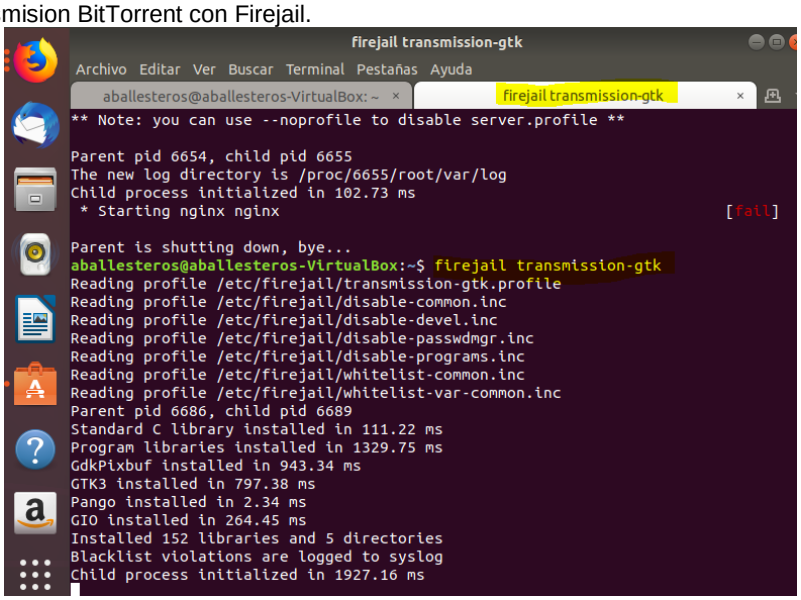
Figura 102. Lanzamiento de Mozilla Firefox desde Sanbox Firejail.



Fuente: Propia.

En esta prueba se inicia el proceso de transmisión con BitTorrent.

Figura 103. Transmision BitTorrent con Firejail.



Fuente: Propia.

8.4 VIDEO DE EXPLICACIÓN Y FUNCIONAMIENTO DEL PROYECTO APLICADO

En el siguiente video se realiza la explicación y funcionamiento del proyecto aplicado, a continuación, se encuentra el link de acceso al video publicado en la plataforma YouTube.

Se sugiere reproducir este desde el navegador Google Chrome o Mozilla Firefox en sus últimas versiones.

https://youtu.be/OFg0dJ4Mqmo

9 RESULTADOS

Dando cumplimiento a la primera etapa del proyecto de seguridad informática I, se realizó la recopilación y elaboración del listado de herramientas de software para desarrollar las diferentes actividades en el CSIRT, teniendo en cuenta la característica principal que son con software libre, las cuales están descritas en la tabla 1.

Se realiza el diseño de la estructura tecnológica de CSIRT, aplicando el modelo de segmentación de Zonas con redes independientes desde su entrada y salida a internet, para no comprometer la Red de producción de la Empresa, en la figura 5, se puede apreciar el diseño de la red para el CSIRT.

Al realizar la instalación y parámetros iniciales para acceder a las aplicaciones que proporcionan los servicios mínimos requeridos para ejecutar las tareas técnicas en el CSIRT (monitoreo, correlacionador de eventos, copias de seguridad y Sandbox). Con Pandora FMS permite tener un monitoreo constante de estos servicios generando alertas y enviándolas a través del protocolo SMTP al correo del administrador de estos servicios.

Alien Vault OSSIM permite tener monitoreados los servicios antes mencionados y dispositivos de RED por medio los sensores HIDs correlacionando los eventos para detectar vulnerabilidades, intrusiones entre otros de esta manera garantiza que estos servicios estén disponibles.

Veeam Backup Community Edition realiza los respaldos de los servicios que están virtualizados para de esta manera permitir restaurar estos en caso de un evento de fuerza mayor que se dañe el servidor o la aplicación que contiene este.

Sandbox Firejail es el entorno aislado del ambiente de producción que permite realizar las pruebas de software de dudosa procedencia, navegar en sitios de los cuales no se tiene la certeza de su procedencia y autenticidad, también permite probar y medir los riesgos de utilizar estos en producción.
En la siguiente tabla se relaciona los resultados y el indicador para la empresa caso de estudio Cibersecurity de Colombia Ltda.

Tabla 10. Resultado producto esperado CSIRT.

RESULTADO/PRODUCTO ESPERADO	INDICADOR	BENEFICIARIO
1. Listado de herramientas hardware y software para el desarrollo de las actividades del CSIRT.	Herramientas hardware y software para el desarrollo de las actividades del CSIRT.	Empresa Cibersecurity de Colombia Ltda.

2. Diseño mapa de la estructura tecnológica del CSIRT, con las mínimas dependencias.	Elaboración diseño mapa de la estructura tecnológica del CSIRT.	Empresa Cibersecurity de Colombia Ltda.
3. Presentación de laboratorio con servicios virtualizados (monitoreo, correlacionador de eventos, copias de seguridad y Sandbox), para realizar pruebas con el software que se utilizara en el CSIRT y un Video en el cual se explique cómo utilizar estas.	Servicios virtualizados funcionales (monitoreo, correlacionador de eventos, copias de seguridad y Sandbox) para el CSIRT.	Empresa Cibersecurity de Colombia Ltda.
4. Presentación de documentación técnica para realizar tareas en el CSIRT.	Documentación técnica para realizar cada tarea.	Empresa Cibersecurity de Colombia Ltda.

Fuente: Propia.

10 CONCLUSIONES

I. A través de la recopilación de información desde las diferentes fuentes documentales se realizó la elaboración del listado de herramientas para el desarrollo de las actividades y dar respuesta a incidentes activos y proactivos del CSIRT, con la característica que estas son de software Open source.

II. Se evidencia que en la actualidad se debe tener mucha precaución al seleccionar las aplicaciones a utilizar según su licenciamiento como es el caso de MYSQL la cual tiene licenciamiento de software Libre GPL y Comercial proporcionada por la Empresa Oracle, para la primera es importante no exceder las limitación del licenciamiento GPL de los contrario se debe adquirir una licencia comercial, otro ejemplo es el caso de Hyper-V server el cual mientras su funcionalidad sea exclusiva hospedar y administrar máquinas virtuales no requiere adquirir licencia de Windows Server siempre y cuando las máquinas virtuales contengan sistemas operativos de libre distribución.

III. Se realizó el diseño de la estructura tecnológica del CSIRT haciendo énfasis en el centro de operaciones de seguridad (SOC) con las dependencias mínimas para el funcionamiento de este y evidenciando que es la columna vertebral del CSIRT.

IV. También se aplicó las buenas prácticas para el diseño del CSIRT proporcionadas por la OEA en donde considera el mínimo de segmentaciones de RED que debe tener este (DMZ Externa, DMZ interna, Red LAN y RED de pruebas), mínimo de servicios y áreas requeridas entre otras recomendaciones.

V. En la etapa 2 del proyecto se está desarrollando la parte técnica con la instalación del mínimo de servicios virtualizados que permite ejecutar las tareas del CSIRT con Monitoreo de estos por medio de la aplicación Pandora FMS, Correlacionador de eventos con la recolección de Logs con los sensores HIDs proporcionados por la aplicación de Alient Vault OSSIM, Tener respaldos automatizados de los servicios virtuales con Veeam Backup C.E. y realizar uso de aplicaciones cuando están en pruebas, desarrollo, con conexiones de alto riesgo a la seguridad informática como son de punto a punto como son las herramientas de Chat , navegación a los sitios web, transferencia de video, por medio del SANBOX Firejail ya que permite realizar lo anterior mencionado en entorno aislado de la Red y no utilizando el ambiente de Producción.

VI. Se realiza el montaje de laboratorio controlado con el mínimo de servicios virtualizados como son monitoreo, correlacionador de eventos, backup y Sandbox para ejecutar las tareas del CSIRT para la empresa caso de estudio

Cybersecurity de Colombia Ltda. realizando un video y socializándolo en la entre de la fase 1 en el curso de proyecto de grado 2.

VII. Los manuales técnicos son muy importantes para ejecutar las tareas del CSIRT ya permiten guiar a los colaboradores, también sirven para tener en cuenta puntos claves en el desempeño de las funciones de los diferentes cargos, sirve de apoyo en el momento de realizar un empalme, reemplazos, vacaciones entre otros eventos fortuitos en los diferentes cargos del CSIRT, además que previenen el cometer errores humanos por falta de practica o desconocimiento de alguna actividad.

VIII. La documentación técnica de los sitios oficiales de los servicios que proporciona el CSIRT de la empresa caso de estudio son relevantes para que los miembros de este según sus funciones para realizar un autoaprendizaje con la finalidad de adquirir habilidades y destrezas lo que permite eficacia y eficiencia a la hora de dar respuestas a los incidentes activos y proactivos de este.

11 RECOMENDACIONES

I. Se ha evidenciado por parte del gobierno nacional la gestión e inversión para la creación de CSIRTs (Centro de respuesta a incidentes informáticos) como es el caso del COLCERT de la policía Nacional, por esta razón se debe sensibilizarse y concientizarse a la empresa privada y en especial al sector financiero de invertir recursos en la creación de estos.

II. El Gobierno y la empresa privada deben apoyar los proyectos que permitan el desarrollo, implementación y puesta en marcha de los CSIRT en Colombia.

III. Mantener en las últimas versiones y en óptimo funcionamiento las aplicaciones virtualizados que proporcionan el mínimo de servicios para ejecutar las tareas técnicas en el CSIRT de esta manera se minimiza la indisponibilidad de estos.

IV. Elaborar una Base del Conocimiento de todos los incidentes reactivos y proactivos para ser compartido a través de todos los CSIRT a nivel nacional y que sea una guía para la mejora continua en estos.

V. Es pertinente al realizar la implementación de las máquinas virtuales para la instalación del mínimo de servicios para el CSIRT que son Monitoreo (Pandora FMS), Copias de Seguridad (Veeam Backup C.E.) Correlacionador de eventos (Alient Vault OSSIM) y Sandbox (Firejail) asignar el direccionamiento IP estático durante la instalación debido a que es un poco más dispendioso pos instalación efectuar esta modificación como es el caso en distribuciones de Linux la cual por buenas practicas se configura desde la terminal quedando permanente y previniendo errores al cargar el sistema operativo cuando se reinicia o encienda el servidor.

VI. También es beneficioso en el montaje de aplicaciones sobre distribuciones de Linux que para este caso se utilizó UBUNTU al terminar la instalación y configurada el direccionamiento IP estático con acceso a internet, ejecutar el comando **upgrade** y después **update** esto garantiza que se está trabajando con la último reléase de la distribución de Linux disponible desde los sitios de descarga oficiales ,aplicando la instalación de forma automática de las últimas actualizaciones de seguridad y complementos para las distintas aplicaciones que utilizan como por ejemplo: Apache (servicio web) Php (que es el lenguaje en que está desarrollada la aplicación) Mysql que corresponde a la base de datos entre otros.

VII. Debido a que se realizó el montaje del mínimo de servicios para el CSIRT antes mencionados al realizar la planeación para la instalación de estos es importante a cada servidor virtual asignar el mínimo de memoria virtual teniendo en cuenta que es tomada del host físico dejando una cantidad

considerable para que este último funcione en óptimas condiciones según las especificaciones mínimas requeridas por el fabricante del sistema Operativo.

VIII. Por otro parte los recursos asignados de procesamiento virtual estas aplicaciones requieren en su configuración entre 2 y 4 cores virtuales para garantizar un funcionamiento óptimo.

IX. Para la asignación del almacenamiento es preciso que al crear los discos virtuales de cada aplicación se aplique la característica de almacenamiento Dinámico ya que esto permite utilizar del almacenamiento real solamente lo que se va utilizando en el disco virtual, por ejemplo, sin un disco virtual es de 50 G.B. y solamente se ha utilizado 10 G.B. El uso real de este disco físicamente seria 10 G.B. no bloqueado las otras 40 G.B. del Host físico, aplicar esta característica es muy útil en ambientes virtualizados.

X. Es importante elaborar listas de chequeos de las actividades diarias y periódicas que se realizan en el CSIRT con el fin de facilitar la realización de estas en caso que se requiera apoyo por alguna eventualidad que suceda a un miembro del equipo, también para prevenir errores humanos al realizar actividades rutinarias.

BIBLIOGRAFIA

ALIENVAULT. AlienVault Unified Security Management (USM) for Security Engineers. LAN Guide. AlienVault USM for Security Engineers v5.3.4 Rev A. [En linea] 2017.Pag. 1. [Citado: 5 abril. 2020] [En linea].Disponible https://www.dbi-services.com/wp-insides/uploads/2017/09/AlienVault-USM-5.3.4-Rev-A-for-Security-Engineers-Lab-Guide.pdf

APACHE. HTTP Server Project. Apache httpd 2.4.41 Released 2019-08-14. [En linea]. Disponible https://httpd.apache.org/

APACHE. HTTP Server Project. Compilar e instalar. [En linea]. Disponible http://httpd.apache.org/docs/2.4/es/install.html

AT&T CYBERSECURITY. USM Appliance Deployment Types. AlienVault USM Appliance deployment solutions. [En linea] Disponible https://cybersecurity.att.com/documentation/usm-appliance/deployment-plan/about-usm-deployment-types.htm?tocpath=Documentation%7CAlienVault%C2%AE%20USM%20Appliance%E2%84%A2%7CDeployment%20Guide%7CUSM%C2%A0Appliance%20Deployments%7C_____1

AT&T. Alienvault is now AT&T cybersecurity. [En linea]. Disponible https://www.alienvault.com/products/ossim

BBC. News-Mundo. Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país. Mayo 6 2017. Recuperado https://www.bbc.com/mundo/noticias-39800133

CANONICAL. Ubuntu. Ubuntu Server 18.04.3 LTS. [En linea]. Disponible https://ubuntu.com/download/server

CARLES, Joan. Geekland Blog de tecnología. Firejail, un sandbox para Linux para ejecutar programas de forma segura. [En línea] 4 de septiembre 2017. Disponible https://geekland.eu/firejail-sandbox-para-linux/

CERTICAMARA. Ciberseguridad Corporativa así está el panorama. 13 de septiembre de 2019. [En linea]. Disponible https://web.certicamara.com/sala_de_prensa/noticia/385

CISA CYBER INFRAESTRUCTURE. (2019, Noviembre 25). US CERT GOV. Retrieved from Official website of the Department of Homeland Security: https://www.us-cert.gov/ncas/bulletins/sb19-336

CUCKOO. Automated Malware Analisys. [En linea] Disponible https://cuckoosandbox.org/

COLOMBIA. MINISTERIO DEL INTERIOR Y DE JUSTICIA. Ley 1273 de 2009 (5, enero, 2009). Diario oficial Bogotá D.C., 2009 No 47.223 {22 de abril de 2016} [En linea]. Disponible http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

COMUNIDAD FIREJAIL. Firejail Security Sandbox. Firejail Usage. [En linea] Disponible https://firejail.wordpress.com/documentation-2/basic-usage/

COMMVAULT. Commvault Backup & Recovery. [En linea] Disponible https://www.commvault.com/complete-data-protection/backup-and-recovery

DIARIO DE SEVILLA. Aniversario del gusano Morris. sábado, 21 de septiembre, 2019. [En linea]. Disponible https://www.diariodesevilla.es/efemerides/gusano-Morris-malware-internet_0_1296170714.html

DIARIO EL PAÍS. Tecnología. Cae la red cibercriminal 'Mariposa', que controlaba millones de ordenadores 'zombis' en 190 países. Marzo 3 de 2010. [En linea]. Disponible https://elpais.com/tecnologia/2010/03/02/actualidad/1267524068_850215.html

DINERO. Tendencias. 4 de cada 10 empresas en América Latina sufrieron ciberataques en los últimos años. 7 de abril 2019. [En linea]. Disponible https://www.dinero.com/tecnologia/articulo/empresas-en-colombia-sufren-de-ataques-ciberneticos-regularmente/273870

DNP. Conpes 3701 de 2011. p..22. [En linea]. Disponible https://mintic.gov.co/portal/604/articles-3510_documento.pdf

DR. LUQUE JUÁREZ, José María. Programa de doctorado en Ciencias Sociales. [En linea]. Universidad Católica de Murcia, octubre de 2019.p. 298. Disponible http://repositorio.ucam.edu/bitstream/handle/10952/4239/Tesis.pdf?sequence=1&isAllowed=y

FIREJAIL. Features. Firejail Security Sandbox. [En linea] Disponible https://firejail.wordpress.com/features-3/

GEEKLAND. BLOG DE TECNOLOGÍA. Firejail, un sandbox para Linux para ejecutar programas de forma segura. [En linea]. Disponible https://geekland.eu/firejail-sandbox-para-linux/

GITHUB. FRASER. N. Documentation. [En linea] Disponible https://github.com/NeilFraser/JS-Interpreter

INVESTIGACIÓN CIENTÍFICA. ¿Qué es la investigación documental? Definición y objetivos. Investigación Documental. [En linea]. Disponible https://investigacioncientifica.org/que-es-la-investigacion-documental-definicion-y-objetivos/

ISOTOOLS. (2015, enero 13). ISO 27001: Pilares fundamentales de un SGSI. [En linea]. Disponible https://www.isotools.org/2015/01/13/iso-27001-pilares-fundamentales-sgsi/

JOOMLA. Downloads. [En linea]. Disponible https://downloads.joomla.org/co/

LINTI, Laboratorio de Investigación en Nuevas Tecnologías Informáticas, Facultad de Informática, Universidad Nacional de La Plata. Pág. 33. [En linea]. Disponible http://sedici.unlp.edu.ar/bitstream/handle/10915/19431/Documento_completo.pdf?sequence=1&isAllowed=y

LOGDNA. Open Source SIEM Solutions. [En linea] Disponible https://logdna.com/open-source-siem-tools/

MA-NO.ORG. Ubuntu 18.04 LTS Tendrá 10 Años de Soporte! [En línea] Disponible https://www.ma-no.org/es/redes/servers/ubuntu-18-04-lts-tendra-10-anos-de-soporte
MANTIS BUG TRACKER. MantisBT 2.22.1. [En linea]. Disponible https://www.mantisbt.org/download.php

MC GUINNESS, Damien. BBC NEWS Mundo. Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país. Mayo 6 2017. [En linea]. Disponible https://www.bbc.com/mundo/noticias-39800133

MICROSOFT. Commercial Licensing reference Guide. Server licensing overview. [En linea] 2007, p. 6 [Citada: 30 abril, 2020] Disponible http://download.microsoft.com/download/E/6/4/E64F72BF-55E9-4D85-9EFE-39605D7CE272/WindowsServer2016-Licensing-Guide.pdf

MICROSOFT. Microsoft Hyper-V Server. Description. Microsoft Hyper-V Server is a free product. [en linea] Disponible https://www.microsoft.com/en-us/evalcenter/evaluate-hyper-v-server-2016

MINTIC. Compes 3701. Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación. [En linea]. Bogotá D.C., 14 de julio de 2011. p. 43. Disponible https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

MINTIC. Decreto 0032 de 2013. "Por la cual se crea la Comisión Nacional Digital y de Información Estatal". [En linea]. Disponible https://www.mintic.gov.co/portal/604/articles-3602_documento.pdf

MYSQL COMMUNITY EDITION. The MySQL Community Edition includes. [En linea] [Citada: 04 abr. 2020] Disponible https://www.mysql.com/products/community/

MYSQL. Documentation. Changes in MySQL 8.0.18 (2019-10-14, General Availability). [En linea]. Disponible https://dev.mysql.com/doc/relnotes/mysql/8.0/en/news-8-0-18.html

NORMAL POPAYÁN. (n.d.). Recursos Normal Popayán. Retrieved from Aislamiento de procesos (informática). [En linea]. Disponible http://recursos.normalpopayan.edu.co:8983/wikipedia_es_all_2017-08/A/Aislamiento_de_procesos_(inform%C3%A1tica).html

ON OPTICAL NETWORKS. Optical Networks es reconocida por Fortinet como uno de sus socios de negocio más destacados. [En linea]. Disponible https://www.optical.pe/optical-networks-es-reconocida-por-fortinet-como-uno-de-sus-socios-de-negocio-mas-destacados/

ORG ATIGMA. Caso de éxito: Integración de Ciberseguridad a sistema de ventas multinivel. 31 de octubre de 2017. [En linea]. Disponible https://www.aticma.org.ar/caso-exito-integracion-ciberseguridad-sistema-ventas-multinivel/.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Buenas Prácticas para establecer un CSIRT nacional. [En linea] 2016. p. 55 [Citada: 04 abr. 2020] Disponible https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf
PANDORA FMS, Arquitectura de Pandora FMS. Agente de software. [En linea]. Disponible https://pandorafms.com/docs/index.php?title=Pandora:Documentation_es:Arquitectura

PANDORA FMS. Monitoring. Pandora: Documentation. Parte 2 Instalación y configuración. [En linea]. Disponible https://pandorafms.com/docs/index.php?title=Pandora:Documentation

PANDORA FMS.Pandora FMS Community Downloads. [En linea]. Disponible https://pandorafms.org/features/free-download-monitoring-software/

PANDORA FMS. Zabbix vs Nagios vs Pandora FMS: una comparativa en profundidad. [En linea] Disponible: https://pandorafms.com/blog/es/zabbix-vs-nagios-vs-pandorafms-una-comparativa-en-profundidad/

PERIODISTA DIGITAL . El Gusano Morris y los daños que causó en Internet. [En linea]. julio 2019. Disponible https://www.periodistadigital.com/tecnologia/tec-internet/20190726/gusano-morris-danos-causo-internet-noticia-689404036001/

PHP. News Archive – 2019. PHP 7.3.11 Released. [En linea]. Disponible https://www.php.net/archive/2019.php#2019-10-24-2

PORTAFOLIO. Empresas. El secuestro de información desangra a las empresas del país.29 de enero de 2019. [En linea]. Disponible https://www.portafolio.co/negocios/empresas/ciberataques-a-las-empresas-en-colombia-525729

PROFESORA ASOCIADA CASTILLO. L. Universidad de Valencia. Biblioteconomía. Segundo cuatrimestre. Curso 2004-2005. Tema 5. Análisis documental.pp. 5-9. [En linea]. Disponible https://www.uv.es/macas/T5.pdf

RED HAT ENTERPRISE Linux 4: Manual de Referencia. (n.d). Capítulo 14. Samba. Web.mit.edu. [En linea]. Disponible https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-samba.html

RED IRIS. La seguridad en la familia de protocolos SNMP. La seguridad en la versión 3 del protocolo. [En linea] [Citada: 04 abr. 2020] Disponible https://www.rediris.es/difusion/publicaciones/boletin/50-51/ponencia16.html

REPÚBLICA DE COLOMBIA DEPARTAMENTO NACIONAL DE PLANEACIÓN. Bogotá D.C., 11 de abril de 2016 Mintic. Compes 3854, pág. 13. Consejo Nacional de Política Económica y Social. [En linea]. Disponible https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

SANS DFIR. Digital Forensics and Incident Response. [En linea]. Disponible https://digital-forensics.sans.org/

SOC COLOMBIA. (n.d.). Security Operation Center. Retrieved Noviembre 12, 2019.[En linea]. Disponible http://www.soccolombia.com/documentos.php

STALLMAN, Richard. M. Software libre para una sociedad libre. Introducción de Lawrence Lessig. 2004. p.232. [En linea]. Disponible ttps://biblioweb.sindominio.net/pensamiento/softlibre/softlibre.pdf

TELEFONICA EQUIPO EDITORIAL. (17 de diciembre de 2018). reportedigital.com. [En linea]. Disponible https://reportedigital.com/cloud/internet-service-provider-isp/

UNM . Trabajos. Administración de Sistemas operativos. Servidor Samba Ubuntu 18.04 LTS, Tutorial. Disponible https://unmtrabajos.blogspot.com/2019/01/servidor-samba-ubuntu-1804-lts-tutorial.html

VEEAM. Backup & Replication Best Practices. Compute requirements. [En linea]. Disponible https://www.veeambp.com/backup_server_introduction/backup_server_sizing

VEEAM. Backup & Replication Community Edition. El backup GRATUITO imprescindible para VMWare y Hyper-V. [En linea]. Disponible https://www.veeam.com/es-lat/virtual-machine-backup-solution-free.html

VEEAM. Cuadrante mágico de Gartner 2020. [En linea] Disponible https://www.veeam.com/es-lat/2020-gartner-magic-quadrant.html

VEEAM. Descargar productos de Veeam. [En linea]. Disponible https://www.veeam.com/es-lat/downloads.html

VEEAM. Veeam Availability Suite. Comparación de productos. [en linea] Disponible https://www.veeam.com/es-lat/products-edition-comparison.html

VERITAS. Backup Exec. [En linea] Disponible https://www.veritas.com/content/dam/Veritas/docs/data-sheets/V1001_GA_ENT_DS_Backup-Exec.pdf

VICENTE, Carlos. Universidad de Oregon. Gestión de Traps SNMP. [En linea]. Disponible https://nsrc.org/workshops/2008/walc/presentaciones/gestion_traps.pdf

ZIMBRA. Synacor porduct. Downloads. [En linea]. Disponible https://www.zimbra.com/downloads/

RESUMEN ANALÍTICO ESPECIALIZADO -RAE

Fecha de Realización:	01/10/2020
Programa:	Especialización en Seguridad Informática
Línea de Investigación:	Infraestructura Tecnológica y Seguridad en Redes
Título:	Propuesta Técnica para la creación de un centro de respuesta a Incidentes cibernéticos para la empresa caso de estudio CIBERSECURITY DE COLOMBIA LTDA.
Autor(es):	BALLESTEROS CÁRDENAS, Alex Augusto
Palabras Claves:	CSIRT, CERT, Seguridad informática. Incidente, Vulnerabilidad.
Descripción:	Se desarrolló el Proyecto Aplicado como preferencia para optar por el título de Especialización en Seguridad Informática a través de la alternativa de grado ofrecida por la UNAD , este tuvo la finalidad de diseñar la propuesta Técnica para la creación de un centro de respuesta a Incidentes cibernéticos para la empresa caso de estudio CIBERSECURITY DE COLOMBIA LTDA, realizando el listado de herramientas de software , hardware la primera de estas con software libre también se diseñó la estructura tecnológica donde se incluyó el mínimo de dependencias para el desarrollo de las actividades además se hizo la presentación un laboratorio controlado con los servicios virtualizados como son monitoreo con la aplicación PANDORA FMS C.E. Correlacionador de eventos ALIENT VAULT OSSIM, backup con la herramienta de VEEAM backup C.E. y Sanbox con FIREJAIL de esta manera se elaboró la documentación técnica que permita el uso de los anteriores servicios para ejecutar la tareas y dar respuesta a los incidentes reactivos y proactivos del CSIRT.

Fuentes bibliográficas destacadas:

DIARIO DE SEVILLA. Aniversario del gusano Morris. sábado, 21 de septiembre, 2019. [En linea]. Disponible https://www.diariodesevilla.es/efemerides/gusano-Morris-malware-internet_0_1296170714.html

DIARIO EL PAÍS. Tecnología. Cae la red cibercriminal 'Mariposa', que controlaba millones de ordenadores 'zombis' en 190 países. Marzo 3 de 2010. [En linea]. Disponible https://elpais.com/tecnologia/2010/03/02/actualidad/1267524068_850215.html

MINTIC. Compes 3701. Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación. [En linea]. Bogotá D.C., 14 de julio de 2011. p. 43. Disponible https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Buenas Prácticas para establecer un CSIRT nacional. [En linea] 2016. p. 55 [Citada: 04 abr. 2020] Disponible https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

SOC COLOMBIA. (n.d.). Security Operation Center. Retrieved Noviembre 12, 2019.[En linea]. Disponible http://www.soccolombia.com/documentos.php

STALLMAN, Richard. M. Software libre para una sociedad libre. Introducción de Lawrence Lessig. 2004. p.232. [En linea]. Disponible https://biblioweb.sindominio.net/pensamiento/softlibre/softlibre.pdf

Contenido del documento:	PLANTEAMIENTO DEL PROBLEMA JUSTIFICACION OBJETIVOS: General y Específicos. MARCO REFERENCIAL: Conceptual, Teórico, Legal, Tecnológico, Metodológico y Técnica de recolección de información. DESARROLLO DE ACTIVIDADES EN UN CSIRT Incidentes Reactivos y Proactivos. HERRAMIENTAS DE SOFTWARE OPEN SOURCE MAPA DE LA ESTRUCTURA TECNOLÓGICA INSTALACIONES DE UN CSIRT DISEÑO DEL CSIRT Plano de las Instalaciones, descripción de cada área, características de la red, Firewall o cortafuegos, DMZ. DISEÑO LÓGICO DE LABORATORIO CONTROLADO MONITOREO, BACKUP, CORRELACIONADOR DE EVENTOS Y SANDBOX: Arquitectura, instalación, configuración, pruebas de uso de la aplicación y video laboratorio controlado: DOCUMENTACIÓN TÉCNICA PARA EJECUTAR LAS TAREAS DEL CSIRT Video de funcionamiento del proyecto aplicado. RESULTADOS CONCLUSIONES

	RECOMENDACIONES
Marco Metodológico:	Para el desarrollo de este Proyecto Aplicado se utilizó la Investigación documental de tipo cualitativa enfocada desde lo interpretativo, aplicando el uso de fuentes primarias y secundarias, garantizando su autenticidad, confiabilidad del autor o entidad origen ,también en donde a las fuentes no se pudieron aplicar los elementos de **autenticidad, credibilidad, representatividad y significado**, se realizó lo inverso llamado método de confianza donde se comprueba que esta fuente no es auténtica, no es creíble y no es representativa.
Conceptos adquiridos :	EL CSIRT es todo un complejo de infraestructura tecnológica en la que también se incluye elementos, procesos, procedimientos, protocolos, documentación entre otros que permite dar respuesta a los incidentes proactivos, reactivos de una manera eficiente, rápida, eficaz, se resalta la importancia de este en el ámbito de la Ciberseguridad con la creación del primero en el país de nombre COLCERT logro a través del CONPES 3701, catalogando el Gobierno nacional a un Ciberataque a una entidad pública como un atentado a la seguridad nacional.
Conclusiones:	Se realizó el diseño de la estructura tecnológica con el mínimo de dependencias aplicando las buenas prácticas dadas por la OEA y SOC Colombia. A través de la simulación del laboratorio controlado con los servicios virtualizados antes mencionados se evidencio el funcionamiento, practicidad de las herramientas de software libre para ejecutar las tareas del CSIRT. La documentación técnica y manuales de elaboración propia o consultada en los portales oficiales de las herramientas para ejecutar las tareas de CSIRT es importante tenerlas de forma organizada y acceder a estas para que los empleados puedan realizar un autoaprendizaje, guía en las actividades cotidianas, base de conocimiento entre otras.