DISEÑO TÉCNICO PARA LA CREACIÓN DE UN EQUIPO DE RESPUESTAS A INCIDENTES DE SEGURIDAD INFORMÁTICA PARA LA EMPRESA CASO DE ESTUDIO CIBERSECURITY DE COLOMBIA LTDA

SANDRA MILENA QUIROGA DIAZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍAS E INGENIERÍAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
VALLEDUPAR–CESAR
2021

DISEÑO TÉCNICO PARA LA CREACIÓN DE UN EQUIPO DE RESPUESTAS A INCIDENTES DE SEGURIDAD INFORMÁTICA PARA LA EMPRESA CASO DE ESTUDIO CIBERSECURITY DE COLOMBIA LTDA

SANDRA MILENA QUIROGA DIAZ

Proyecto de investigación aplicado para optar al título de Especialista en SEGURIDAD INFORMÁTICA

DIRECTOR

Esp. MARIANO ESTEBAN ROMERO TORRES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍAS E INGENIERÍAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
VALLEDUPAR–CESAR
2021

PAGINA DE EXCLUSIÓN DE RESPONSABILIDAD

COMPROMISO DE AUTOR

Yo, Sandra Milena Quiroga Díaz con célula de identidad 49.719.587 y alumno del programa académico Especialización en Seguridad Informática, declaro que:

El contenido del presente documento es un reflejo de mi trabajo personal y manifiesto que, ante cualquier notificación de plagio, copia o falta a la fuente original, soy responsable directo legal, económico y administrativo sin afectar al director del trabajo, a la Universidad y a cuantas instituciones hayan colaborado en dicho trabajo, asumiendo las consecuencias derivadas de tales prácticas.

Firma: _____

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Valledupar, mayo de 2021

DEDICATORIA

"A aquel que es poderoso para hacer muchísimo más de lo que pedimos o pensamos…" Efesios 3,20

A mi amado Juan Sebastián, por el tiempo tuyo que me he tomado.

A mis padres por todo su apoyo.

AGRADECIMIENTOS

Agradezco principalmente al rey de todo el universo, por tantas bendiciones recibidas, por colocarme en el lugar en el que me encuentro ahora.

¡A COMFACESAR, estamos cumpliendo sueños!!!, gracias por el apoyo económico. A mi jefe, por darme ese pequeño impulso que me faltaba.

A mis tutores por su apoyo.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

AMENAZA: De acuerdo con lo expuesto por Gómez[1], este término es utilizado para indicar algún evento que puede ser intencionado o no a través del cual se pretende afectar los sistemas de información el cual puede repercutir en daños materiales, financieros o de otro tipo.

DMZ: En seguridad informática, este término se refiere a la red perimetral conocida como "Zona desmilitarizada", que consiste en la segmentación de una red interna dispuesta en el perímetro entre la red interna y la red externa.

FIREWALL: Es una herramienta de hardware o de software, utilizada en seguridad informática para ejercer control sobre el tráfico entrante y saliente de la red o de los equipos.

INCIDENTE: Es un evento inesperado que produce la interrupción de los servicios, que puede llegar a causar inoperatividad de los sistemas o perdida de datos.

***MALWARE*:** Se considera como malware aquellos programas informáticos, documentos o mensajes, encaminados a causar daño dentro de un sistema informático o redes de comunicaciones, dentro de esta definición se abarcan: virus informáticos, gusanos, caballos de troya, etc.

***PHISING*:** Hace referencia a un tipo de ataque informático, en el que la víctima es afectada por la suplantación de identidad, de una entidad en la que confía.

RIESGO: Es definido de la siguiente manera: "La probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático causando un determinado impacto en la organización"[2].

VULNERABILIDAD: Es un concepto que va ligado al concepto de debilidad, ya que a raíz de éstas se permite la materialización de las amenazas, Gómez lo define como sigue: "Es cualquier debilidad en el sistema informático que pueda a las amenazas causarle daño y producir perdidas en la organización"[3]

[1] GOMEZ VIEITES, Álvaro. Enciclopedia de la Seguridad Informática. 2 ed. Madrid: RA-MA, 2014. p. 60.
[2] Ibíd., p. 63.
[3] Ibíd. p. 61.

RESUMEN

La transformación digital en la actualidad ha permitido que el tema de la seguridad informática tome mayor relevancia, especialmente en el sector empresarial, dado que los procesos de una organización se apalancan en las tecnologías informáticas, y una falla en ellos tendrían consecuencias negativas para el negocio. En los últimos años, se han registrado casos de ataques informáticos que han ocasionado pérdidas millonarias, esta situación ha hecho que las organizaciones inviertan un poco más en seguridad. Sin embargo, las estadísticas reflejan un estado incipiente aún. Esto resulta insuficiente, dado que la complejidad de las amenazas, demanda experiencia en muchos campos tecnológicos, lo cual resulta bastante complejo de lograr en una organización.

Por tal razón es importante que las empresas puedan tener un respaldo adicional ya sea al enfrentar los incidentes de seguridad o cuando requieran consultorías en el tema. Estas soluciones se pueden encontrar en los Equipos de Respuesta ante Incidentes de Seguridad Informática, una meta planteada por la empresa Cibersecurity de Colombia Ltda. con el objetivo de brindar servicios de soporte a sus clientes.

En este proyecto se busca proponer el diseño técnico para la creación de un CSIRT en la empresa, mediante una investigación cuantitativa, con un diseño no experimental, aplicado de manera transversal, que inicialmente tendrá un enfoque exploratorio para investigar las herramientas más usadas en un CSIRT, posteriormente se dará un enfoque descriptivo para determinar mediante pruebas de efectividad las herramientas e infraestructura tecnológica requerida para la operación de un CSIRT.

Palabras clave: Seguridad informática, CSIRT, ataque, ciberseguridad, cibercrimen, amenazas, incidentes, vulnerabilidad.

INTRODUCCIÓN

La importante popularidad que han tomado las herramientas tecnológicas ha transformado la cotidianidad, en un entorno digital en el que todos se conectan, desde interacciones en las redes sociales hasta grandes transacciones económicas empresariales, se encuentran soportadas por las tecnologías de la información y las comunicaciones, lo que puede dar una idea del grado de criticidad que tiene el correcto funcionamiento de estas.

De la misma forma que se popularizan los servicios en internet, también se incrementan las amenazas que circundan el ciberespacio, esencialmente por la posibilidad que tienen los ciberdelincuentes de acceder a sistemas remotos, en donde encuentran una fuente lucrativa de ingresos. La consolidación de un ciberataque indudablemente puede desencadenar una crisis que afecta a varios sectores, tanto dentro como fuera de la organización. Razón por la cual surge la necesidad de cooperación entre las comunidades a nivel general de propender por un ciberespacio seguro, estos esfuerzos conjuntos se has dado a conocer con el nombre CSIRT (Equipo de respuesta ante incidentes de seguridad informática).

Un CSIRT es un grupo multidisciplinario de especialistas, dedicados a la seguridad informática, que se encargan de dar respuesta a los incidentes en el menor tiempo posible. Existen varios tipos de estas organizaciones, dependiendo del ámbito de acción para el cual han sido definidos, entre los cuales se destacan los de tipo comercial, cuya misión es brindar sus servicios a grupo determinado de clientes a cambio de una contraprestación económica.

La creación de un CSIRT comercial es la meta trazada por la empresa Cibersecurity de Colombia Ltda. Para el 2020 con el objetivo de ofrecer servicios de soporte a sus clientes. Para concretarla, es necesario realizar una investigación que permita definir el diseño técnico de este equipo, a la luz del objetivo de la empresa.

1. EL PROBLEMA

1.1 DESCRIPCION DEL PROBLEMA

Los avances experimentados por la tecnología en las últimas décadas han generado cambios en el desarrollo de muchas actividades cotidianas, las cuales se han visto claramente influenciadas por la implementación de herramientas informáticas, que impulsan tanto a los individuos como a las empresas a mejorar la ejecución de sus procesos. De igual forma, la necesidad de interconectividad generada a raíz de la globalización convierte a internet una herramienta primordial para las empresas.

Internet ha facilitado hoy en día la comunicación en tiempo real, tal como lo revela el informe de Digital 2020 Global Overview, el 59% de la población mundial está en línea[4], ya sea para subir fotos, videos, compartir información, hacer transacciones bancarias desde el celular etc. Así mismo, las empresas han logrado mejorar y agilizar sus procesos mediante el tratamiento digital de su información, conquistar nuevos mercados, ofrecer productos y servicios en línea, expandirse regional e internacionalmente, lo que las hace más eficientes y productivas, como consecuencia de ello, se ha llegado hasta el punto de que el logro de sus objetivos dependa en gran medida de su conectividad digital, por estas razones es normal encontrar un departamento dedicado a la gestión de las tecnologías de la información y comunicación en las organizaciones.

Si bien es cierto que las organizaciones deben contemplar riesgos presentes en el escenario físico tales como desastres naturales, daños de origen industrial o social para proteger sus activos, el nuevo escenario digital en el que todo el tiempo se trasmite información, conlleva a ubicarlas en un nuevo campo de batalla “virtual”, cuya lucha consiste en proteger su información, al fin y al cabo, este es su principal activo. En el análisis de la Encuesta Global de Seguridad de la Información de EY 2018-19, se plantea que “la información personal del cliente, la financiera y los planes estratégicos constituyen los tres tipos de información más valiosos que las organizaciones querrían proteger”[5], es decir, la información es valor, y los delincuentes persiguen todo aquello de que tiene o puede generar valor.

Todo esto revela un nuevo desafío que es el aseguramiento de la información, tema que

[4] KEMP, Simón. Digital 2020: Global Digital Overview. Global Overviews [en línea]. 30 de enero 2020. [consultado 26 Marzo 2020]. Disponible en: https://thenextweb.com/podium/2020/01/30/digital-trends-2020-every-single-stat-you-need-to-know-about-the-internet/.

[5] MANCERA S.C. Encuesta Global de Seguridad de la Información 2018-19. [en línea]. México: Ernst & Young Global, 2019. [consultado 2 Octubre 2019]. Disponible en: https://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2018-19/$FILE/ey-encuesta-global-seguridad-informacion-2018-19.pdf.

se ha convertido en un punto de interés para las organizaciones, en vista del vertiginoso crecimiento de los ataques informáticos, que han afectado a muchas de ellas ocasionando cuantiosas pérdidas económicas. Siendo el phising en un 22% y el malware con el 20%, el origen de los problemas cibernéticos más críticos a nivel global[6].

Cada día aparecen nuevas amenazas que ponen en riesgos los sistemas informáticos, los delincuentes actúan de muchas formas, buscando detectar vulnerabilidades para penetrar los sistemas de información y las motivaciones que los impulsan pueden ser de distinta índole, algunos lo hacen por ocio, pero la gran mayoría lo hace con fines delictivos. Frente a esto, las empresas invierten en mecanismos de protección para mitigar los riesgos mediante la implementación de firewall, antivirus, protección por medio de contraseñas, etc. Sin embargo, estas medidas pueden ser insuficientes debido a que las amenazas se mantienen una constante evolución y diversificación.

Los ataques informáticos han evolucionado a la par de la tecnología, de tal manera que se ha disminuido el grado de dificultad para realizarlos, por ejemplo, algunos se encuentran automatizados, documentados y publicados en sitios web al alcance de cualquier persona. Esto ha hecho que industria del cibercrimen haya crecido hasta tal punto que hoy en día es fácil encontrar sitios web que ofrecen sus servicios de para realizar ataques o robar información a pedido.

En Colombia, según un informe del Centro Cibernético Policial, “En 2017 el cibercrimen reportó un incremento del 28.30% respecto al año anterior”[7], además se menciona que las amenazas persistentes en 2017 fueron: El Ransomware, el cual afecto infraestructura critica en más de 150 países mientras que en Colombia afectó principalmente MiPymes del sector productivo; El Ataque a entes gubernamentales a través de malware, en donde las cifras por hurto ascienden a más de 50 mil millones de pesos tan solo en las alcaldías; BEC (Suplantación de correo corporativo) en el que por cada caso presentado, se estima una pérdida de 380 millones de pesos; Carding (comercialización de información financiera), que registra pérdidas anuales por 60,000 millones de pesos.

Ante este panorama, las empresas han realizado intentos para incrementar un poco la inversión en temas de seguridad, pese a esto, los resultados de la Encuesta Global de Seguridad de la Información de EY 2018-19[8] revela que el 87% de las organizaciones no cuentan con el presupuesto para establecer los niveles de seguridad que requieren, “Más

[6] Ibid. p 23.
[7] CENTRO CIBERNETICO POLICIAL. Informe: Balance Cibercrimen en Colombia 2017 [en línea]. POLICIA NACIONAL, 2017. [consultado 2 Octubre 2019]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_201217_1_1_0.pdf.
[8] MANCERA S.C, Op cit P 13.

de la mitad de las organizaciones no tienen a la protección de su organización como parte de sus estrategias y planes de ejecución"[9], esto se debe a que generalmente los gerentes prefieren invertir mayor parte del presupuesto en el Core del negocio, restándole importancia al tema de seguridad informática. Sumado a esto, de las empresas que sí invierten en ciberseguridad, el 77% la manejan en forma limitada, según los datos revelados en la encuesta de EY, estas empresas: "Incluso podrían no tener una imagen clara de cuáles son y dónde está su información crítica y sus activos, ni tampoco tener las debidas medidas de protección para ellos"[10].

Esta situación, es el común denominador entre las empresas clientes de Cibersecurity Ltda., quienes, a raíz de la limitada inversión en seguridad, requieren capacitar al personal de TI al menos en cómo actuar cuando se presenta un ataque, ya que hay vulnerabilidades que la organización no evidencia en primera instancia. Lamentablemente, esto podría no ser suficiente en determinados casos, ya que la complejidad de las amenazas demanda una amplia pericia tecnológica en muchos campos como pueden ser: análisis forense, criptografía avanzada, sistemas de redes, etc. y resulta bastante complejo lograr que una organización reúna tales características.

En consecuencia, se puede deducir que estas empresas aún están muy limitadas en el tema de protección contra amenazas, lo cual supone una desventaja frente a la industria del cibercrimen, de allí la importancia de que estas empresas cuenten con entidades como Cibersecurity que les brinden servicios de respuesta inmediata a través de la contratación de servicios, que les permitan protegerse y responder de manera adecuada ante los incidentes de seguridad informática que se les puedan presentar.

Para que Cibersecurity de Colombia Ltda. pueda consolidar su equipo de respuestas a incidentes de seguridad informática debe contar con estudios previos que permitan la planificación y puesta en marcha de los nuevos servicios para sus clientes, entre los cuales se encuentra un diseño técnico documentado que incluya la estructura tecnológica, herramientas de hardware y software necesarias para el soporte de las operaciones y la realización de una prueba piloto de las herramientas de software mas críticas para la ejecución de los procesos en el CSIRT.

1.2 FORMULACION DEL PROBLEMA

Frente a lo expuesto anteriormente, ¿Cómo puede un Equipo de Respuestas a Incidentes De Seguridad Informática, brindar apoyo a los clientes de la empresa caso de estudio

[9] Ibíd. P 19.
[10] Ibíd. P 17.

Cibersecurity de Colombia Ltda., para resguardar sus activos de información y minimizar el impacto o dar respuesta inmediata ante un ataque informático?

1.3 JUSTIFICACIÓN

El alto volumen y complejidad de los ataques han dado lugar a que se consoliden los equipos de respuestas a incidentes informáticos, cuyo origen data de finales de los años ochenta frente al colapso provocado por el gusano Morris, el cual generó la necesidad de establecer grupos de cooperación para dar frente a las amenazas y en donde el factor tiempo era determinante. La conformación de estos equipos ha dado muy buenos resultados minimizando y controlando los daños ocasionados por un ciberataque, razón por la cual Cibersecurity considera que son de gran relevancia para una empresa que brinda servicios de seguridad informática.

Cibersecurity ha determinado que, para cubrir las deficiencias en ciberseguridad, es necesario que sus clientes puedan tener un respaldo externo a través de un equipo de expertos en seguridad informática, especializado en cada uno de los campos de las tecnologías de la información. Por esta razón, se proyecta para el año 2021 consolidarse como un CSIRT, a fin de que sus clientes cuenten con el apoyo requerido al momento de enfrentar una crisis de seguridad informática o bien para brindar el servicio como asesores en la prevención de éstas.

Hoy en día los Equipos de Respuesta ante Incidentes de Seguridad Informática (CSIRT), han tomado gran importancia a raíz de la demanda generada por los ataques cibernéticos. Su implementación permitirá resolver problemas de seguridad informática que las empresas no pueden solucionar por sí mismas, proporcionando el respaldo para identificar la mejor forma de actuar ante un incidente y recuperar la operatividad de los servicios afectados en el menor tiempo posible. Esta implementación demanda la elaboración de un diseño documental y un diseño técnico, siendo este último el objetivo del presente proyecto.

El diseño técnico requerido por la empresa caso de estudio Cibersecurity de Colombia Ltda., para la creación del CSIRT se constituye en base fundamental para consolidar el objetivo trazado por la empresa para el año 2021, para ello se requiere determinar puntos importantes como lo son la identificación de herramientas de software Open Source que permitan a la empresa ejecutar las actividades propias del CSIRT en la prestación de servicios a sus clientes, del mismo modo se debe determinar el mapa de la estructura tecnológica, a partir de dependencias mínimas entre las que se cuentan: Centro de Datos, centro de operaciones, soporte, salón de formación, etc.

Por otro lado, es preciso que el diseño técnico determine el equipo de hardware sobre el cual se ejecutaran las herramientas de software, con lo cual se conforma la infraestructura requerida por el equipo para la ejecución de sus operaciones. Por último, con la virtualización de un laboratorio controlado en donde se visualice la configuración y las pruebas del software utilizado, se podrá observar su utilidad para el momento en que entre en funcionamiento el CSIRT y se pueda llegar a identificar, contener, erradicar y recuperar los sistemas de información frente a la presencia de cualquier ataque informático, de esta forma ampliará el portafolio de servicios ofrecido a sus clientes.

1.4 OBJETIVOS

1.4.1 **Objetivo general**

Proponer un diseño técnico para la creación de un equipo de respuestas a incidentes de seguridad informática en la empresa caso de estudio Cibersecurity de Colombia LTDA.

1.4.2 **Objetivos específicos**

- Identificar herramientas de software open Source requeridas para el desarrollo de las actividades del equipo de respuestas a incidentes de seguridad informática en la empresa caso de estudio Cibersecurity de Colombia LTDA.
- Diseñar el mapa de la estructura tecnológica con las dependencias mínimas involucradas en el desarrollo de las actividades del equipo de respuestas a incidentes de seguridad informática en la empresa caso de estudio Cibersecurity de Colombia LTDA.
- Determinar los requerimientos tecnológicos de hardware que permitan definir los activos que faciliten el funcionamiento del equipo de respuestas a incidentes de seguridad informática en la empresa caso de estudio Cibersecurity de Colombia LTDA.
- Elaborar el diseño lógico del laboratorio controlado para la ejecución de pruebas de las herramientas de software del CSIRT, mediante la virtualización de los servidores de monitoreo, correlación de eventos, copias de seguridad y Sandbox

2. MARCO DE REFERENCIA

Este capítulo se constituye en una parte importante dentro de la investigación, ya que la sustenta conceptualmente a través de la revisión teórica existente, permitiendo generar nuevos conocimientos. Para tal fin, se presentan los antecedentes referentes al objeto de estudio, así como las bases teóricas y la definición de términos básicos relacionados con el tema.

2.1 ANTECEDENTES

Con el fin de establecer los estudios realizados en cuanto a la creación de equipos de respuestas a incidentes de seguridad informática CSIRT, se hace una revisión de antecedentes, lo cual nos brinda una ampliación del campo de investigación, permitiendo además tener un marco de referencia y punto de partida para el desarrollo del presente estudio.

En primer lugar, el trabajo de grado titulado: "Estrategia y Diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la universidad de las fuerzas armadas ESPE" [11], presentado en la Universidad de Las Fuerzas Armadas en la ciudad de Sangolquí (Ecuador) en el año 2018, cuyo objetivo principal fue la propuesta de un modelo de CSIRT académico en la universidad, presenta entre sus principales conclusiones la necesidad que el plan estratégico del CSIRT se encuentren alineados con el de la universidad, para poder garantizar su adecuado funcionamiento. Esta conclusión resulta interesante considerar dentro de la ejecución de este proyecto, puesto que se trata de un CSIRT que forma parte de la estructura organizacional de la empresa caso de estudio Cibersecurity de Colombia Ltda. Y por lo tanto se debe sujetar a sus lineamientos y objetivos. Su principal contribución radica en los aportes al marco teórico del presente proyecto, así como el diseño del CSIRT en cuanto a la infraestructura propuesta y las herramientas de software empleadas, teniendo en cuenta que los autores optaron por la utilización de herramientas *open Source*, el cual es uno de los objetivos del proyecto.

En segundo lugar, la tesis titulada "Propuesta de diseño e implementación de un Centro de Operaciones de Seguridad (SOC) y un Centro de Repuesta a Incidencias (CSIRT)

[11] DE LA TORRE, Hugo y PARRA, Mario. Estrategia y Diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la universidad de las fuerzas armadas ESPE [en línea]. Trabajo de Grado (Ingeniero de Sistemas e informática). Universidad de las Fuerzas Armadas. Sangolquí (Ecuador), 2018. [consultado 12 abril de 2020]. Disponible en: http://repositorio.espe.edu.ec/handle/21000/15071.

para la Universidad de Ingeniería"[12], presentada en la Universidad Nacional de Ingeniería, de la ciudad de Managua (Nicaragua) en el año 2016, plantea su propuesta de diseño en la que afronta la respuesta a incidentes de seguridad informática separando las actividades: el SOC para el monitoreo de alertas y el CSIRT para la atención a las mismas, sin embargo, el diseño técnico planteado para la empresa caso de estudio Cibersecurity de Colombia, contempla que las actividades del CSIRT cubrirá el monitoreo y atención a incidentes de manera conjunta; pese a esto el trabajo citado anteriormente constituye un aporte a la presente investigación, en cuanto a la infraestructura tecnológica que se plantea para el desarrollo de las actividades del CSIRT.

En tercer lugar, el trabajo de grado denominado "Desarrollo de un marco de trabajo para la protección de un Equipo de Respuesta ante incidencias de Seguridad Informática CSIRT"[13], presentado ante el Centro de Investigación en Matemáticas, A.C. en la ciudad de Zacatecas (México) en el año 2016, plantea como eje principal la protección de la información que se maneja en el CSIRT. Este se considera un punto realmente importante ya que el CSIRT de Cibersecurity de Colombia, al mismo tiempo que ofrece protección frente ante incidentes de seguridad a sus clientes, también puede ser blanco de ataques, razón por la cual se hace indispensable garantizar principalmente su protección y por ende su operatividad proyectando una buena imagen. Como principal aporte de este trabajo se tiene los controles en cuanto a la seguridad física y del entorno, los controles de acceso a las redes.

2.2 MARCO TEÓRICO

2.2.1 Seguridad Informática. Debido a que el punto de partida o razón de ser de los CSIRT está fundamentado en la seguridad informática, a continuación, se aborda este concepto que junto con los conceptos de ataques e incidentes edificarán el referente teórico, para el desarrollo del presente proyecto de investigación. A menudo se suelen confundir los conceptos de seguridad informática con el de seguridad de la información, y aunque están íntimamente relacionados es importante identificar a qué se refiere cada uno y la gran relevancia que ha tomado en la actualidad.

La seguridad informática es un concepto que se encuentra inmerso dentro de la seguridad

[12] GARCIA VELASQUEZ, Javier Antonio. Propuesta de diseño e implementación de un Centro de Operaciones de Seguridad (SOC) y un Centro de Repuesta a Incidencias (CSIRT) para la Universidad de Ingeniería. Trabajo de Grado (Magister en Gestión de la Seguridad de la Información). Universidad Nacional de Ingeniería. Managua (Nicaragua), 2016. [consultado 12 abril 2020]. Disponible en: https://core.ac.uk/download/pdf/250144005.pdf.

[13] RAMIREZ LUNA, Heltton. Desarrollo de un marco de trabajo para la protección de un Equipo de Respuesta ante incidencias de Seguridad Informática CSIRT. Trabajo de Grado (Maestro en Ingeniería de Software). Centro de Investigación en Matemáticas, A.C (CIMAT). Zacatecas (México), 2016. [consultado 5 mayo 2020]. Disponible en: https://cimat.repositorioinstitucional.mx/jspui/handle/1008/442.

de la información, este es un tema clave, que debe ser claramente diferenciado; para una mejor ilustración e identificación de estos conceptos, varios autores consideran que la seguridad de la información hace referencia a los esfuerzos enfocados en preservar la confidencialidad, disponibilidad e integridad de la información que se maneja en una empresa, en este caso se habla de la información en general, sea cual sea el formato en el que se almacene. Por otro lado, "la seguridad informática se encarga de la seguridad del medio informático, según varios autores la informática es la ciencia encargada de los procesos, tecnicas y métodos que buscan procesar, almacenar y transmitir información"[14]. De esta forma, se aclara que la seguridad informática está orientada a todos aquellos datos que se almacena o transmite a través de los medios electrónicos.

Tradicionalmente, la seguridad informática ha centrado su interés en la preservación de las tres principales características que debe mantener la información: confidencialidad, disponibilidad e integridad, sin embargo, teniendo en cuenta el marco de gestión COBIT, "las características que debe poseer la información son: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, apego a los estándares y confiabilidad"[15], adicionalmente como lo menciona Baca[16], en el terreno de la seguridad informática se otorga una característica más a la información: "la privacidad", la cual dista del concepto de "confidencialidad", puesto que mientras esta última se enfoca en la protección frente a accesos no autorizados a la información, la privacidad se ocupa de proteger la dupla identidad del usuario y sus actividades.

2.2.1.1 Tipos De Seguridad Informática. Las medidas en seguridad informática evolucionan en torno a los avances y complejidad que se presentan los ataques informáticos, en este contexto, Iñiguez[17] identifica tres tipos de seguridad informática:

- **Seguridad Online**. Se refiere a las medidas de seguridad que se emplean en el entorno de internet, en donde ocurren múltiples tipos de delitos. En esta categoría se menciona la seguridad online personal, que es de carácter individual, está relacionada con la protección de los datos personales y las transacciones económicas, por otro lado, la seguridad online empresarial, la cual se enfoca más a la protección de los datos como su principal patrimonio.

- **Seguridad de Hardware**. Está relacionada con las medidas preventivas realizadas a nivel físico en los equipos, por ejemplo: los sellos, candados, bloqueos de

[14] ROMERO CASTRO, Martha, et al. Introducción a la seguridad informática y el análisis de vulnerabilidades. Editorial Área de Innovación y Desarrollo. SL, 2018. p 14.
[15] BACA URBINA, Gabriel. Introducción a la seguridad informática. Grupo Editorial Patria, 2016. p 12.
[16] Ibid p 14.
[17] IÑIGUEZ ESTRADA, Héctor. Seguridad Informática y Protección de Datos Personales. EDI: 2020. p 14

equipo, sistemas de control de acceso, bloqueos de USB en los equipos.

- **Seguridad de Software**. Implica las medidas de protección que se deben dar a nivel de software, garantizando características que debe mantener la información para que sea considerada segura: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, apego a los estándares, confiabilidad y privacidad. Para ello se emplean herramientas de software e incluso de hardware, como es el caso de los firewalls, políticas de seguridad, tecnicas de protección teniendo en cuenta los distintos tipos de ataques que ocurren a nivel de software.

2.2.2 Ataque Informático. Un ataque informático se define como la acción o conjunto de acciones orientadas a ocasionar un impacto negativo sobre un sistema informático, el cual se hace posible a través del aprovechamiento de una vulnerabilidad. Tal como lo menciona Vega[18], se tratan de actos deliberados que buscan infringir daño o aprovecharse de cierto tipo de información, los cuales pueden ser de dos tipos:

- Ataque Activo, se refiere a aquellos en los que se compromete el correcto funcionamiento del sistema: hay alteración de los datos, detención de los servicios, etc.
- Ataque Pasivo, es aquel en donde solo se accede a los datos sin realizar modificaciones, situación que los hacen más difíciles de detectar.

Avenía[19] plantea que los ataques pueden ser clasificados en cuatro grupos, partiendo de tipo de daño provocado o bien de la alteración causada sobre la información, como se menciona a continuación:

- Interrupción. Afecta la disponibilidad, debido a que el usuario no puede acceder a los servicios requeridos.
- Interceptación. Compromete la confidencialidad, debido a que se logran capturar la información transmitida en la comunicación.
- Modificación. En este caso se ve afecta la integridad y confidencialidad, ya que por medio de este ataque el sistema es accedido y modificado sus datos por usuario no autorizados.
- Fabricación. Afecta la integridad, debido a que se engaña haciéndose pasar por el destinario de la comunicación, lo que le permite obtener información valiosa.

[18] VEGA BRICEÑO, Edgar. Planificación y ejecución de evaluaciones de seguridad informática desde un enfoque de ethical hacking. Editorial Área de Innovación y Desarrollo. SL, 2020. p 77.
[19] AVENÍA DELGADO, Carlos Arturo. Fundamentos de seguridad informática. Editorial: Fondo editorial Areandino, 2017. p 49.

2.2.2.1 Fases de un Ataque Informático. Los ataques generalmente se desarrollan mediante un comportamiento que se identifica como su ciclo de vida o "Cyber Kill Chain". Este término fue acuñado desde un principio en el entorno militar, para identificar los pasos dados por el enemigo cuando realiza un ataque. En términos de seguridad informática, Incibe[20] identifica fases de un ataque como una secuencia de siete pasos que se mencionan a continuación

1. **Reconocimiento**. Es una fase durante de recopilación de información referente al objetivo para conocerlo en detalle.
2. **Preparación**. Es la fase durante la cual el atacante prepara específicamente el ataque dirigido al objetivo seleccionado.
3. **Distribución**. Es donde se realiza el envío del ataque al objetivo seleccionado.
4. **Explotación**. En esta fase se logra perpetrar el sistema, a través del despliegue del ataque enviado en la fase anterior, basado generalmente en la explotación de una vulnerabilidad conocida.
5. **Instalación**. Consiste en instalar el malware en el sistema atacado, con lo cual busca garantizar la permanencia del atacante en el sistema, para ello altera el sistema de forma que le siga permitiendo el acceso.
6. **Comando y control**. Es la fase en la que el atacante tiene pleno dominio del sistema infectado y a partir de ahí realiza todo tipo de acciones que pueden incluir robar contraseñas, sustraer información, instalar aplicaciones, etc. Las cuales son dirigidas desde un sistema remoto central conocido como C&C (command and control)
7. **Acción sobre los objetivos**. En esta fase el atacante se apropia de la información y busca más objetivos para continuar el ataque.

2.2.3 Incidente de Seguridad. En términos generales, un incidente hace referencia un suceso que se produce repentinamente e impide el desarrollo normal de una situación alterándola o interrumpiéndola. Ahora bien, cuando se trata de incidente de seguridad informática, se delimita a que esta interrupción se presenta en el entorno de las tecnologías de la información. De acuerdo Villalobos, este término se refiere a "Los diferentes ataques que sufren los sistemas conectados a internet"[21]. Ahora bien, en el contexto empresarial, ISO/IEC define un incidente de seguridad de la información como: "un evento o serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información"[22]

[20] INCIBE. [sitio web]. Las 7 fases de un ciberataque. ¿Las conoces?. [En línea]. [Consultado en mayo de 2020]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/las-7-fases-ciberataque-las-conoces

[21] VILLALOBOS MURILLO, Johnny. Gestión De Incidentes De Seguridad Informática Con Agentes Inteligentes. Revista .Seguridad [en línea]. 2018, Julio-Agosto, 14. [consultado mayo 2020]. ISSN 1251478. Disponible en: https://revista.seguridad.unam.mx/numero-14/gesti%C3%B3n-de-incidentes-de-seguridad-inform%C3%A1tica-con-agentes-inteligentes

[22] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO / IEC 2018, 5ta Ed. Genova, Suiza: ISO, 2018 4p.

2.2.4 Gestión de Incidentes. La gestión de incidentes de seguridad de la información es definida por ISO/IEC como el "conjunto de procesos para detectar, informar, evaluar, responder, tratar y aprender de incidentes de seguridad de la información."[23] Es importante resaltar estas actividades inherentes a la gestión de incidentes que conllevan tanto a corregir o detener el incidente como a aprender de él, de este modo se crean las bases para construir un servicio proactivo.

Este tema también es abordado en la librería de infraestructura de tecnologías de la información ITIL, versión 3, el cual es trabajado por Ríos en su manual, quien por su parte la define de la siguiente forma: "La gestión de incidencias tiene como objetivo principal la resolución de los incidentes para restaurar lo más rápidamente el servicio" [24]. De acuerdo con lo anterior se tiene que la gestión de incidentes corresponde a un servicio reactivo, el cual se gestiona a través de un service desk, en donde estas solicitudes proceden de los usuarios del sistema.

2.2.4.1 Proceso De Gestión De Incidentes. El proceso de gestión de incidencias es descrito por Ríos[25] de la siguiente manera:

- Recepción y registro. Esta parte del proceso resulta de gran utilidad, puesto que permite llevar un seguimiento a los incidentes y consiste en registrarlo teniendo en cuenta la siguiente información:
    - Servicios afectados
    - Posibles causas
    - Nivel de prioridad
    - Impacto
    - Recursos asignados para su resolución.
    - Estado de la incidencia.
- Clasificación. En este punto se determina el rango de prioridad que representa el incidente y el impacto que genera para la organización
- Investigación y diagnóstico. Consta de dos fases: la de comparación, que permite determinar mediante una búsqueda en la base de datos de incidencias la existencia de casos similares, para aplicar la mejoras que éste plantea. Mientras que la fase de investigación y diagnostico se encarga de dar solución al incidente presentado teniendo en cuenta los niveles.

[23] Ibid. P 5.
[24] RÍOS HUÉRCANO, Sergio. Itil v3 Manual Integro [En línea]. En: Biable [sitio web]. [consultado 7 Octubre 2019]. Disponible en: https://biable.es/.
[25] Ibid. p 80-81

- Escalado. Consiste en el escalado de la incidencia hacia un nivel superior, cuando el actual no ha podido resolverla.

2.2.5 Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT). Se denomina de esta manera a la conformación de un grupo de expertos en seguridad informática encargados de hacer frente ante los eventuales incidentes de seguridad de la información. Algunos autores, como West-Brown[26] se refieren al concepto de CSIRT haciendo una analogía con el departamento de bomberos, puesto que, una de las principales características, es que deben reaccionar con prontitud, ya que un incidente es como una emergencia donde el tiempo es un factor determinante.

Tal como lo plantean Grobler and BRYK[27], los CSIRT son responsables de recibir, revisar, coordinar y responder ante eventos que comprometen la seguridad informática, buscando responder a las preguntas ¿Qué pasó? Y ¿qué acciones son necesarias para resolver la situación? El marco de acción de un CSIRT primordialmente en identificar y detener las amenazas para posteriormente eliminarla y restablecer en el menor tiempo posible la operatividad de los sistemas vulnerados.

2.2.5.1 Framework de un CSIRT. No existe un estándar específico para la establecer las pautas de operación de un CSIRT, la principal razón radica en que estos equipos dependen en gran medida del entorno, el público y los servicios que éstos requieran. Sin embargo, hay ciertos aspectos que son comunes a todos, por lo que es necesario adaptarlos a las particularidades de cada caso, es decir, cuando se embarca en la labor de crear un CSIRT, se debe establecer su propios criterios y pautas operativas que respalden su entorno y circunscripción.

El Framework básico para la creación de un CSIRT, se identifica a través de las repuestas a las preguntas: "¿Qué hacer?", ¿Para quién?, ¿Cuál es el entorno local?, ¿Quiénes son sus cooperadores?, las cuales West-Brown[28] las considera como la identificación de los siguientes puntos:

- Misión: Corresponde a la identificación de las metas, objetivos y prioridades que tendrá el equipo. El establecimiento de esta misión debe partir de la comprensión básica de lo que quiere lograr, debe estar conformado por tres o cuatro oraciones

[26] WEST-BROWN, Moira J., et al. Handbook For Computer Security Incident Response Team (Technical Report CMU/SEI-2003-HB-002). [en línea] Pittsburgh: Software Engineering Institute, Carnegie Mellon Carnegie Melon University, 2003. p 22. [consultado octubre 2019]. Disponible en: https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf

[27] GROBLER, Marthie and BRYK, Harri. Common Challenges Faced During the Establishment of a CSIRT-[En línea]. [consultado 6 Octubre 2019]. Disponible en: https://researchspace.csir.co.za/dspace/bitstream/handle/10204/4339/Grobler2_2010.pdf?sequence=1.

[28] WEST-BROWN, Moira J., et al. op cit p 10.

como máximo y evitar la ambigüedad, con lo cual se dará el enfoque para las metas y objetivos generales. Además, es muy importante contar con el respaldo de los directivos de la organización, ya que de lo contrario enfrentará una lucha por la consecución de reconocimiento y recursos para el funcionamiento.

– Circunscripción: hace referencia al alcance del CSIRT, es decir, identificar el público objetivo para el cual será establecido y su relación con él. La circunscripción es la entidad o entidades a las cuales brindará su servicio, aunque puede ofrecer sus servicios a cualquiera que los solicite, lo más común es que sea limitada. Los criterios para establecerla se fundamentan en restricciones de tipo: nacional, geográfica, política, técnica (por ejemplo: para un sistema operativo específico), organizacional (por ejemplo, para una empresa especifica), proveedor de servicios o contractual (por ejemplo, cuando un cliente paga por el servicio).

– Lugar en la organización: Se refiere a la posición dentro de la estructura organizacional y especificar su papel dentro de la gestión de riesgos. Se establece el papel que desempeña el CSIRT en la gestión general de riesgos en el contexto del entorno organizacional y de su circunscripción, por ejemplo, a través del establecimiento de las funciones que cumple el equipo frente al departamento de TI de una empresa.

– Interrelación: Por medio de ellas se establecen relaciones de cooperación y coordinación con otros CSIRT ya sea en el ámbito nacional o internacional. Un marco cooperativo de acción para los CSIRT es clave, dado que el ámbito que se maneja es internet, lo cual lo hace global.

  Este tipo de actividades de cooperación, pueden realizarse entre un CSIRT y otro o a través de CSIRT Coordinadores, que los ubica en una especie de estructura jerárquica informal la cual es considerada como un beneficio puesto que brinda la posibilidad de compartir información en forma flexible, rápida y efectiva con otros CSIRT. Un ejemplo claro de estos equipos coordinadores se ve en las fuerzas militares estadounidenses en los que Ejército, Fuerza Aérea y Armada tienen sus equipos ACERT / CC, 12 AFCERT y NAVCIRT, respectivamente que brindan sus servicios a cada institución específica, por su parte, el Departamento de Defensa de este país, cuenta con el DOD-CERT para coordinar en todos los equipos mencionados anteriormente.

2.2.5.2 Servicios de un CSIRT. El núcleo de todas las actividades de un CSIRT es la gestión de Incidentes, por ello en el "Handbook for Computer Security Incident Response Teams (CSIRTs)"[29] se plantea que para que un CSIRT pueda ser considerado como tal, debe por lo menos ofrecer uno o más los servicios relacionados con la gestión de incidentes tales como: análisis de incidentes, respuesta a incidentes en el sitio, soporte de respuesta a incidentes o coordinación de respuesta a incidentes.

Adicionalmente a la gestión de incidentes, los CSIRT ofrecen otros servicios que deben estar acordes con su misión, propósito y circunscripción, sin embargo, hay servicios que son comunes y que se pueden agrupar en tres categorías mencionadas por West-Brown[30] como se muestran a continuación:

Servicios Reactivos

Estos servicios se presentan posterior a la ocurrencia del incidente o amenaza, están diseñados para atender requerimientos de soporte, informes de incidentes de otros CSIRT o incluso ataques dirigidos contra el mismo sistema del CSIRT. Los servicios reactivos se originan a partir de la notificación de terceros, o también cuando son detectados como resultado del monitoreo, alertas o sistemas de detección de intrusos. Algunos servicios reactivos comunes son:

- **Alertas y advertencias:** Este servicio consiste básicamente en proporcionar al cliente, información relativa a cualquier evento que implique un riesgo de seguridad de la información, como pueden ser: alertas de intrusión, malware, existencia de vulnerabilidades de seguridad, etc. Con el objetivo de indicar al usuario, las acciones a corto plazo requeridas para detener la amenaza.[31]

- **Manejo de incidentes:** Abarca las actividades relacionadas con la recepción, clasificación y respuesta a aquellas solicitudes y reportes presentados por los clientes, así como también realizar análisis a incidentes y eventos. West-Brown[32] indica que las actividades de manejo de incidentes dependen del tipo de CSIRT, por ende, lo clasifica en función del tipo de asistencia brindada por el CSIRT de la siguiente manera:

    - **Análisis de incidentes**: radica en elaborar un análisis de toda la información o evidencia disponible, relacionada con el incidente, con el objetivo de identificar la magnitud de éste, es decir, el alcance, naturaleza, extensión del daño causado,

[29] WEST-BROWN, Moira J., et al. op cit p 23
[30] Ibid. P 23
[31] Ibid. P 25
[32] Ibid. P 26

etc. A partir de esto, se plantean las alternativas de respuesta. Como parte de este análisis se tienen dos subservicios:

- **Recolección de evidencia Forense:** consiste en recolectar, preservar, documentar, y analizar la evidencia presente en un sistema informático comprometido, de tal forma que se pueda identificar los cambios efectuados en el sistema para reconstruir la cadena de eventos que conllevaron al compromiso de este.

- **Seguimiento y rastreo:** Busca determinar el cómo ingresa el atacante al sistema, el sistema utilizado para el ingreso, origen del ataque, determinar la identidad del atacante. Este trabajo, aunque puede realizarse independientemente, en general involucra otras entidades como lo son autoridades policiales, proveedores de servicio de internet, etc. [33]

- **Respuesta a incidentes en el sitio**: Consiste en brindar asistencia directamente en el lugar, con el objetivo de ayudar al usuario del CSIRT a recuperarse del incidente, se analiza físicamente, para luego realizar la reparación y recuperación de los sistemas.

- **Soporte de respuesta a incidentes**: consiste en brindar asistencia remota al cliente del CSIRT, para que puedan realizar la recuperación por ellos mismos. Los canales utilizados para brindar esta asistencia, pueden ser teléfono, correo electrónico, documentación, etc. Puede incluir la interpretación de los datos recogidos, no implica acciones directas en sitio.

- **Coordinación de respuesta a incidentes**: el CSIRT se encarga de coordinar las labores de recuperación entre las partes involucradas, que pueden ser: la víctima y otros sitios que recibieron el ataque, los proveedores de servicios, el personal de soporte informático, los administradores del sistema y de las redes. Las actividades de coordinación recopilación de información, estadísticas, notificación, interacción con asesores legales, de recursos humanos, policía, etc., al igual que el anterior no implica la atención en el sitio.

– **Manejo de vulnerabilidades.** Es realizado a través del análisis de informes de vulnerabilidades de hardware y software, buscando determinar naturaleza, mecánica y efectos de dichas vulnerabilidades, a fin de determinar las mejores estrategias de respuesta para detectarlas y repararlas. West-Brown[34], clasifica éste servicio de acuerdo a las actividades y tipo de asistencia que brinda el CSIRT, de la siguiente manera:

[33] Ibid. P 27
[34] Ibid. P 28

- **Análisis de vulnerabilidad**: Consiste en la realización de análisis técnicos y la revisión de las vulnerabilidades de hardware y software para determinar, tanto su ubicación como la manera de explotarla. Este estudio puede incluir la verificación de código fuente, la utilización de depuradores de código, e incluso la recreación de una situación específica en un entorno de prueba o controlado.

- **Respuesta de vulnerabilidad**: Este servicio consiste en identificar la respuesta adecuada para solucionar la vulnerabilidad descubierta, por medio de la investigación de parches liberados por los fabricantes, o en su defecto desarrollándolos. Esta labor requiere la divulgación de la estrategia de mitigación mediante alertas.

- **Coordinación de respuesta a la vulnerabilidad**: Se trata de labores de notificación realizadas por el CSIRT, a las áreas de la empresa o comunidad objetivo, en las que se dan a conocer información sobre cómo solucionar la vulnerabilidad, adicionalmente, se verifica que la estrategia sea implementada correctamente. Este servicio implica la interacción con proveedores, clientes, personal técnico, expertos, otros CSIRT, etc.

– **Manejo de artefactos**

- Análisis de artefactos
- Respuesta a artefactos
- Coordinación de respuesta a

Servicios proactivos

Estos servicios, como su nombre lo indica, tienen como característica principal anticiparse a los problemas, su diseño se enfoca en el mejoramiento de la infraestructura y de los procesos de seguridad de la entidad, previo a que ocurra o se detecte cualquier incidente o evento. En este sentido, estos servicios tienen como principal objetivo evitar los incidentes o en su defecto mitigar su impacto o alcance cuando ocurren. Entre los servicios proactivos mencionados por West-Brown se encuentran:

– Anuncios
– Vigilancia tecnológica
– Auditorías o evaluaciones de seguridad
– Configuración y mantenimiento de herramientas de seguridad, aplicaciones, Infraestructuras y Servicios
– Desarrollo de herramientas de seguridad
– Servicios de detección de intrusiones

– Difusión de información relacionada con la seguridad

Servicios de Gestión de Calidad de Seguridad

Su enfoque está orientado a mejorar la seguridad de una organización a nivel general ya que, a través de estos servicios, los CSIRT aportan su punto de vista y perspectivas únicas, que son el resultado de la experiencia adquirida a lo largo de la ejecución de los servicios reactivos y proactivos. Generalmente estos servicios son ejecutados por el departamento de TI de las empresas, sin embargo, desde la perspectiva de asesoramiento, resulta de gran utilidad dado que proporciona información que permite fortalecer la seguridad organizacional, en la medida que se identifican las debilidades, los riesgos y amenazas latentes.

Con el conocimiento obtenido por los CSIRT al responder incidentes, vulnerabilidades y ataques, se hace posible realizar reflexiones o lecciones aprendidas que contribuyen sustancialmente en la gestión de la calidad de la seguridad, algunos servicios pueden ser:

– Análisis de riesgo
– Continuidad del negocio y planificación de recuperación ante desastres
– Consultoría de seguridad
– Creación de conciencia
– Educación y Entrenamiento

2.2.5.3 Tipos de CSIRT. Existen varios tipos de CSIRT, los cuales se pueden clasificar de acuerdo con su ámbito de acción y al público objetivo, según ENISA[35], los tipos de CSIRT pueden ser:

- **CSIRT del sector académico**. Son aquellos que brindan sus servicios a instituciones académicas tanto el personal como a los estudiantes,
- **CSIRT comercial**. Sus servicios se encuentran orientados a un grupo de clientes, que ofrecen una contraprestación económica por ellos.
- CSIRT del sector de la protección de la información vital y de la información y las infraestructuras vitales (CIP/CIIP). Se orientan básicamente sus servicios a la protección de información vital y de las infraestructuras vitales.
- **CSIRT del sector público**. Son aquellos que orientan sus servicios a agencias del

[35] ENISA[sitio web]. Cómo crear un CSIRT Paso a Paso. [En línea]. [consultado 7 Octubre 2019]. Disponible en: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

estado, y en ocasiones también a los ciudadanos.

- **CSIRT interno**. Es aquel organizado para prestar sus servicios a una organización en particular a la cual pertenecen.
- **CSIRT del sector militar**. Prestan sus servicios a las instituciones militares que tengan responsabilidad sobre estructuras de tecnologías.
- **CSIRT nacional**. Sus servicios son básicamente de coordinación y sirven de punto de contacto de seguridad de todo el país,
- **CSIRT del sector de la pequeña y mediana empresa (PYME)**. Sus servicios se focalizan a atender a este tipo de empresas, que generalmente no cuentan con el recurso para implementar un CSIRT propio. Se crean por iniciativa propia y se focalizan generalmente en empresas de un ramo en particular.
- **CSIRT de soporte**. Están orientados a productos específicos, en donde su objetivo principal es el desarrollo de soluciones, ante vulnerabilidades específicas de éstos productos, esto hace que el público objetivo se centre en los propietarios.

2.2.5.4 ¿Cómo Crear un CSIRT?. Como se ha mencionado anteriormente, cada CSIRT difiere de otros tanto en su funcionamiento como en aspectos tales como personal, experiencia y presupuesto, cada uno es único. Sin embargo, SEI36 publica en 2017 un White paper en donde se pueden identificar ciertas prácticas básicas que se pueden aplicar para la creación, así mismo se deja claro que, aunque se presenten como una serie de pasos, no necesariamente deben seguirse de manera secuencial incluso puede darse en paralelo.

- Paso 1: Obtenga soporte de gestión y aceptación
- Paso 2: Determinar el plan estratégico CSIRT
- Paso 3: recopilar información relevante
- Paso 4: Diseñe la visión CSIRT
- Paso 5: Comunicar la visión y el plan operativo de CSIRT
- Paso 6: Comience la implementación de CSIRT
- Paso 7: Anuncie el CSIRT operativo
- Paso 8: Evaluar la efectividad de CSIRT

2.3 MARCO CONCEPTUAL

En esta sección se revisarán algunos conceptos básicos, relacionados con los temas de seguridad informática, en los cuales se encuentra inmersa las actividades propias de un

[36] SOFTWARE ENGINEERING INSTITUTE, CARNEGIE MELLON CARNEGIE MELON UNIVERSITY. [sitio web]. Create A Csirt.(2017) [en línea]. [consultado 8 octubre 2019]. disponible en: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485693

Equipo de respuestas ante incidentes de seguridad informática, de forma que permitirán apropiar y aplicar los conocimientos en el diseño de la documentación técnica para la creación de un CSIRT

CSIRT (Computer Security Incident Response Team): Equipo de Respuesta ante Incidentes de Seguridad Informática

Service Desk: De acuerdo con su traducción se refiere a Mesa de servicios, Gómez Beas[37] lo define como "Centro de Servicio al usuario (SD) Primer nivel de atención al usuario en metodologías y manuales de buenas prácticas como ITIL".

Opensource: De acuerdo con su traducción, significa "Código Abierto", es un término empleado para identificar aplicaciones de software que son distribuidas bajo una licencia que permite que las personas puedan realizar modificaciones sobre el código fuente.

SIEM (Security Information & Event Management): Es un sistema de gestión de eventos e información de seguridad, que se encargan de realizar escaneo activo y pasivo de redes con el objetivo de descubrir eventos y actividades sospechosas, de forma que se puedan predecir los ataques antes de que ocurran. Este enfoque pretende tener una visión completa de la seguridad de las tecnologías de la información. Este acrónimo "combina funciones de SIM (gestión de información de seguridad) y SEM (gestión de eventos de seguridad) en un sistema de gestión de seguridad"[38].

2.4 MARCO LEGAL

2.4.1 Ley 1273 de 2009. En cuanto al tema de la ciberseguridad y la seguridad de la información el Estado colombiano ha sido consciente de la necesidad de establecer normas que regulen esta materia, en vista del panorama que se enfrenta a nivel mundial del creciente número de incidentes y ataques de seguridad informática. "Es decir, se cuenta con una legislación procesal penal integral y efectiva para abordar los delitos cibernéticos, y reconoce los tratados internacionales con INTERPOL y EUROPOL."[39]. Es así como mediante la Ley 1273, se enmienda el código penal mediante la creación de un nuevo bien jurídico protegido por el derecho, que ha sido denominado "de la protección

[37] GÓMEZ BEAS, Dolores. Resolución de incidencias en redes telemáticas (UF1881). Andalucía: IC Editorial, 2014. p 25.
[38] ROUSE, Margaret. Gestión de eventos e información de seguridad (SIEM). [En línea]. Search Data Center. [consultado 16 noviembre de 2019]. Disponible en: https://searchdatacenter.techtarget.com/es/definicion/Gestion-de-eventos-e-informacion-de-seguridad-SIEM.
[39] COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento Conpes 3854 (2016) Política Nacional De Seguridad Digital [en línea]. Bogotá, D.C. p 21. [Consultado febrero 2020]. Disponible en: https://bibliotecadigital.ccb.org.co/bitstream/handle/11520/14856/DNP-Conpes-Pol%2b%c2%a1tica%20Nacional%20de%20Seguridad%20Digital.pdf?sequence=1&isAllowed=y

de la información y de los datos"[40] añadiéndose como un nuevo título.

2.4.2 Política Nacional de Seguridad Digital. Esta política, se encuentra amparada bajo el documento CONPES 3854 de 2016, en el que según Castillo: "el gobierno viene trabajando desde hace algunos años en el diseño e implementación de una estrategia de ciberseguridad nacional de una forma integral que permita garantiza el desarrollo de un entorno digital y que apalanque aún más el crecimiento económico y la prosperidad social para todos los colombianos"[41].

El principal objetivo de esta política es fortalecer las capacidades de los sectores involucrados en el campo de la mitigación de riesgo y vulnerabilidades de la seguridad de la información. A partir de esto se establece unos lineamientos institucionales enfocados en la seguridad digital, principalmente enfocado a la gestión de riesgos.

2.5 MARCO ESPACIAL

El desarrollo del presente trabajo busca dar respuesta al propósito establecido por la empresa caso de estudio Cibersecurity de Colombia LTDA para el año 2021. En virtud de esto, se propone el diseño de la documentación técnica, para la creación de un equipo de respuestas a incidentes de seguridad informática, el cual será un CSIRT de tipo comercial, cuya población objetivo, estará constituida por los clientes de la empresa, a quienes se ofrecerá, en su primera fase, una línea de servicios de tipo reactivos, comprendiendo fundamentalmente gestión de incidentes y de vulnerabilidades.

[40] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273 de 2009 (enero 5 de 2009) [en línea]. Diario Oficial. Bogotá, D.C., 2009. [Consultado febrero 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[41] CASTILLO PARRA, Xenia. Normatividad De Ciberseguridad En El Sector Financiero Colombiano [en línea]. Seminario de investigación aplicada de la gestión de la seguridad y el riesgo. Universidad Piloto de Colombia. p 2. [consultado febrero 2020]. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/8625

3. **MARCO METODOLÓGICO**

En todo proyecto de investigación, es de suma importancia definir la metodología a implementar para el logro de los objetivos propuestos, debido a que esta ofrece un conjunto de procedimientos sistemáticos, para realizar la recolección de la información, así como también su posterior clasificación y análisis, los cuales se constituyen en el insumo principal para la interpretación de resultados que han motivado la investigación.

Para el desarrollo de este proyecto, se empleará la metodología de la investigación cuantitativa con alcance descriptivo, por cuanto se efectuará la recolección y análisis de información a través del cual se pretende identificar, cuáles son las herramientas de hardware y software más indicadas para hacer parte de la propuesta del diseño técnico para la creación de un CSIRT

A partir de este planteamiento inicial, se debe definir el plan de acción que indique los procedimientos requeridos para responder a la pregunta de investigación; este plan es lo que se constituye como el diseño de la investigación.

Por ello, para lograr el objetivo propuesto, se recurrirá a un diseño no experimental, el cual se aplicará de manera transversal, iniciando con un enfoque exploratorio mediante el cual se buscará conocer los diferentes tipos de herramientas de hardware y software utilizadas por CSIRT oficiales a nivel internacional. Posteriormente, desde un enfoque transversal descriptivo se buscará determinar cuáles de estas herramientas presentan mejor efectividad y a partir de ellas, proponer el diseño de la documentación técnica requerida para la creación de un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT).

De acuerdo con Hernández, Fernández y Baptista, en la investigación no experimental es aquella en donde no se manipulan las variables deliberadamente, “Lo que hacemos en la investigación no experimental es observar fenómenos tal como se dan en su contexto natural, para analizarlos”[42], así mismo, señalan que “Los diseños de investigación transeccional o transversal recolectan datos en un solo momento, en un tiempo único”[43]

[42] HERNÁNDEZ SAMPIERI, Roberto; FERNÁNDEZ COLLADO, Carlos y BAPTISTA LUCIO, Pilar. Metodología de la investigación 6a. ed. México D.F.: McGraw-Hill Interamericana, 2014. p 152.
[43] Ibíd. P 154

4. RESULTADOS

4.1 INFORMACIÓN SOBRE HERRAMIENTAS DE SOFTWARE PARA EL DESARROLLO DE ACTIVIDADES DEL CSIRT

El alcance definido para el CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA, está orientado a servicios de tipo reactivos, que incluyen: Monitoreo de seguridad informática, Alertas y advertencias, Manejo de incidentes y Manejo de vulnerabilidades. Cada una de estas actividades precisan herramientas de software que permitan una ejecución eficiente y oportuna de sus procesos para lo cual se requiere realizar una búsqueda de aplicaciones en la web, capaces soportar los mencionados servicios, a la luz de ciertos criterios específicos.

La identificación de estas herramientas se realiza teniendo en cuenta que la principal característica que deben cumplir es ser open Source, además de contar con soporte y actualizaciones permanentes puesto que es un indicador de madurez y estabilidad; adicional a ello la disponibilidad y asequibilidad de la documentación, tanto en sitios oficiales como en foros de la comunidad, es un punto importante dado que se constituye en el respaldo idóneo al momento de realizar el despliegue de las aplicaciones para la puesta en marcha del CSIRT. En esta sección, se describen las herramientas de software necesarias para el equipo de la empresa.

4.1.1 Herramientas de Monitoreo de Seguridad Informática. El CSIRT responde a solicitudes de servicios que generalmente son reportadas por los usuarios afectados, sin embargo, también se pueden generar a través del servicio de monitoreo. Este servicio pretende garantizar a los clientes, la tranquilidad de una vigilancia constante sobre la infraestructura tecnológica, que permita tomar acciones correctivas, frente a las amenazas, en el menor tiempo. Esta tarea se puede llevar a cabo a través de un sistema de gestión de eventos e información de seguridad, más conocidos como SIEM.

AlienVault OSSIM. Es una herramienta, incluye funciones completas de recopilación, normalización y correlación de eventos. Esta herramienta se considera adecuada para desarrollar las funciones de monitoreo del CSIRT de Cibersecurity de Colombia LTDA, ya que es un SIEM de código abierto que proporciona, en una plataforma integrada, capacidades de seguridad esenciales, tales como Monitoreo, detección de intrusos, correlación de eventos, descubrimiento de activos, y evaluación de vulnerabilidades.[44]

[44] AT&T CYBERSECURITY [sitio web]. AlienVault OSSIM [En línea]. [consultado 16 noviembre 2019]. Disponible en: https://www.alienvault.com/products/ossim.

Mediante la herramienta **Zabbix**, se puede realizar monitoreo en tiempo real de la infraestructura de TI de las empresas tanto hardware como software, redes y servicios, presenta alertas y visualización de gráficos que ayudan al análisis.[45]

4.1.2 Herramienta de Mensajería Masiva. El servicio de alertas y advertencias resulta de gran importancia, ya que, a través de él, se pueden mantener informado a los clientes de la organización, acerca de las distintas amenazas a la seguridad informática que puedan afectar el correcto funcionamiento de sus sistemas de información. Para su ejecución, se hace necesario contar con una herramienta de mensajería, que permita la opción de envíos masivos, de tal forma que, al momento de enviar información a todos los clientes, no se corra el riesgo de ser catalogados como spam, situación que evitaría el cumplimiento del objetivo de este servicio.

Las herramientas de monitoreo descritas en el ítem anterior cuentan con servicio de envío de correos con alertas y notificaciones que se configuran dentro de las mismas e incluso algunas poseen la opción de realizar acciones recomendadas de acuerdo al caso que se presente. Esta opción se constituye en un insumo para la realización de las notificaciones a los usuarios.

Para este caso, se empleará **OpenEMM**[46], es una herramienta basada en la web, con licencia pública general de Affero (AGPLv3), que permite la automatización de la comunicación de correo electrónico, a través de ella, el CSIRT puede crear y enviar los boletines de seguridad informática a todos los clientes, en los casos en los que, por ejemplo, se descubre una nueva vulnerabilidad sobre un sistema operativo.

4.1.3 Herramienta de Software Para La Gestión De Incidentes. Según Ocampo[47], Laverde y Caicedo (2009) un incidente es un suceso inusual dentro del comportamiento habitual de un sistema o servicio, en este orden de ideas, la gestión de incidentes busca brindar el tratamiento adecuado frente a un evento que pone en riesgo la continuidad del negocio.

[45] ZABBIX LLC [sitio web]. Zabix [en línea]. [consultado 25 noviembre 2019]. Disponible en: https://www.zabbix.com/features.

[46] AGNITAS [sitio web]. OpenEMM 2019: Email Marketing for Free [En línea]. [consultado 16 noviembre 2019]. Disponible en: https://www.agnitas.de/en/e-marketing_manager/email-marketing-software-variants/openemm/

[47] OCAMPO, Carlos; LAVERDE, Ricardo y CAICEDO, Sandra. Implementación de modelo de procesos de gestión de servicios con itil (information technology infrastructure library). Scientia et technica [en línea].2009, Vol. 1 núm 41. [consultado 16 noviembre de 2019]. Disponible en: https://revistas.utp.edu.co/index.php/revistaciencia/article/view/2913.

Este tipo de servicios generalmente se inician en el momento de la ocurrencia del evento, a partir del cual se inicia un proceso de tratamiento y mitigación del incidente. Las entradas del proceso de gestión de incidentes pueden provenir de múltiples fuentes, como lo son de las herramientas de monitoreo o bien de los reportes que presentados por los usuarios finales. Dado el alto volumen que puede implicar estas entradas, y con el fin de brindar un óptimo seguimiento de cada caso particular, es necesario la utilización de herramientas para llevar una adecuada gestión de los incidentes.

GLPI. Es una herramienta de ITSM (Gestión de servicios de TI), open Source, distribuido bajo la Licencia Pública General de GNU. La cual permite, realizar la planificación y administración de los cambios de TI, y además resolver incidentes de manera eficiente tan pronto como presentan. Entre las principales funciones que ofrece, se tiene la gestión de inventario, activos y dispositivos móviles, y adicionalmente, provee de una completa información del estado de los equipos como PC, servidores, impresoras, monitores, consumibles etc.[48]

Dado que el CSIRT de la empresa se enfocará en la prestación de servicios reactivos, las labores de gestión de incidentes implican desarrollar actividades de análisis post mortem, es decir, un análisis posterior a la ocurrencia de los incidentes de seguridad informática. Debido a esto, se requiere la implementación de herramientas de análisis forense, que permitan determinar la causa-raíz de los incidentes estudiados, de forma que se puedan corregir y así evitar que los clientes queden nuevamente expuestos ante las amenazas. Entre estas herramientas tenemos:

SIFT Workstation. Se trata de un conjunto de herramientas open Source para la respuesta a incidentes y herramientas forenses, que permite realizar exámenes forenses digitales detallados, en una gran variedad de entornos; utiliza técnicas forenses digitales de inmersión profunda. Tiene la capacidad de examinar, de forma segura, discos sin formato o con múltiples sistemas de archivos como ntfs, raw, swap, memoria ram, entre otros.[49]

Blazescan. Es una herramienta de respuesta a incidentes y escaneo de malware de servidores web Linux, adicionalmente, cuenta con soporte integrado para servidores cPanel.[50] , utiliza firmas personalizadas para detectar webshells, correos de spam y kits

[48]GLPI. (2019) [sitio web]. ITSM software – GLPI [En línea]. [consultado 25 noviembre 2019]. Disponible en: https://glpi-project.org/features/
[49] SANS. (2019) [sitio web]. SIFT Workstation. [En línea]. [consultado 09 diciembre 2019]. Disponible en: https://digital-forensics.sans.org/community/downloads
[50] LASKOWSKI-TECH.(2019) [sitio web]. Blazescan - Utilidad de escaneo de malware de Linux. GLPI. [En línea]. [consultado 25 noviembre 2019]. Disponible en: https://laskowski-tech.com/2018/05/29/blazescan-linux-malware-scanning-utility/

de phishing. Además, también se apoya en ClamAV, el cual es un motor antivirus, de código abierto para detectar troyanos, virus, malware y otras amenazas maliciosas.

Guymager. El análisis de incidentes es uno de los procesos críticos en los servicios ofrecidos por el CSIRT, éste incluye una actividad imprescindible que está relacionada con la recolección de evidencia forense, la cual generalmente es obtenida a través de la adquisición de imágenes de los discos. Para este proceso, es indispensable contar con una herramienta de hardware denominada duplicador de discos, que a través de un software se encarga de realizar el proceso. **Guymager**[51] es una de estas aplicaciones de software que permite la generación de imágenes de disco forense. Es una herramienta de código abierto que viene preinstalada entre las utilidades de Kali Linux.

4.1.4 Herramienta de Análisis De Gestión De Vulnerabilidades. La gestión de vulnerabilidades es una parte crucial dentro de las actividades de un CSIRT, ya que proporciona el insumo para el desarrollo de los procesos de aseguramiento de la infraestructura tecnológica. Actualmente existen en el mercado un amplio número de herramientas, tanto comerciales como open Source, que permiten gestionar las vulnerabilidades, y que abarcan desde el análisis de todo un sistema completo, escaneo de redes, hasta el análisis de puntos neurálgicos y específicos como lo son las bases de datos y las aplicaciones web. A continuación, se tienen:

Nmap: Network Mapper. Es una utilidad de software open Source, empleada en el proceso de escáner de redes y desarrollo de auditorías de seguridad. Esta herramienta es de gran utilidad para la administración de redes, dado que permite la realización de inventario, supervisión de equipos respecto al tiempo de actividad, hosts disponibles, ejecución de servicios, firewalls etc.[52]

Cuenta con un potente motor denominado Nmap Scripting Engine (NSE), por medio del cual se ejecutan scripts para la automatización de tareas de red que permiten la realización de auditorías y detección de vulnerabilidades. Aunque permite al usuario escribir y compartir scripts propios, Nmap trae una extensa variedad de scripts, entre los que se encuentran[53]:

- Auth: evalúa credenciales de autenticación.
- Discovery: obtiene información del sistema objetivo

[51] KALILINUX [sitio web]. Kali Linux (2020). [En línea]. {09 diciembre 2019}. Disponible en: https://www.kalilinux.in/2019/10/guymager-forensic-disk-imager-kali-linux.html
[52] LYON, Gordon. Nmap. [En línea]. [consultado 25 noviembre 2019]. Disponible en: https://nmap.org/
[53] Ibid

- External: Utilización de recursos externos
- Intrusive: funciones intrusivas para el sistema objetivo
- Malware: verifica existencias de backdoors
- Safe: ejecuta scripts que no son intrusivos
- Vuln: Escanea vulnerabilidades
- All: ejecuta scripts .NSE

Scuba Database Vulnerability Scanner. Es software de escáner de base de datos, gratuita, empleada para detectar vulnerabilidades en motores de bases de datos, a través del análisis del sistema objetivo, es posible conocer tanto vulnerabilidades como configuraciones erróneas o incorrectas, la mayor ventaja que presenta esta herramienta es que combina los resultados entregados con las recomendaciones de mejores prácticas del estándar CIS Controls.

Los controles de CIS, consolida un conjunto de buenas prácticas para la defensa en profundidad, que resultan de gran utilidad, para neutralizar el impacto de los ataques de más comunes, a los que se enfrentan los sistemas de TI. Estos controles, disponen adicionalmente de los documentos denominados benchmark, en los que hay uno específico para cada motor y versión de base de datos.[54]

Por lo anterior, se considera la herramienta Scuba como un gran aliado para la auditoria de sistemas de bases de datos, puesto que no solo realiza detección de vulnerabilidades, sino que también se evalúan aspectos relacionados con las malas configuraciones del motor de base de datos. Con base en esto, se genera el informe del resultado de la evaluación, en donde cada ítem se relaciona con los controles CIS. Esta situación permite agilizar el trabajo, puesto que el informe combinado con los benchmark, dan como resultado una gestión optimizada de las vulnerabilidades de los sistemas de bases de datos.

WireShark. Es una herramienta que permite realizar el análisis de protocolos, que permite la inspección profunda de un amplio número de protocolos, entre sus ventajas se puede mencionar que es una herramienta intuitiva, permite capturar el tráfico en tiempo real y posteriormente analizarlo, su nivel de detalle permite al investigador conocer exactamente qué es lo que está pasando en la red. Resulta útil para el evento que se requiera identificar el tráfico generado en una red que esté siendo atacada

[54] CENTER FOR INTERNET SECURITY [sitio web]. CIS Controls [En línea]. [consultado 26 noviembre 2019]. Disponible en: https://www.cisecurity.org/controls/

4.1.5 Herramienta de Seguridad Interna del CSIRT. El tema de la seguridad informática, tano dentro de las propias instalaciones de la empresa Cibersecurity tanto como dentro del CSIRT, constituye un punto sumamente importante, puesto que, de la robustez de la seguridad interna de la empresa, dependerá la imagen proyectada hacia sus clientes. Es por ello que se considera indispensable la implementación de las herramientas de seguridad necesarias para proteger los sistemas de la empresa, entre las que tenemos:

IDS/IPS (Sistemas de Detección Y Prevención De Intrusión). Entre los mecanismos de defensa para la seguridad informática en las organizaciones, se encuentran los IDS/IPS, que son herramientas que permiten la detección y solución de vulnerabilidades que surgen cada día[55]. En este sentido, es sumamente importante realizar el monitoreo del tráfico de red, de forma que permita la detección de comportamientos anómalos relacionados con un ataque informático

Snort. Es una herramienta de detección de intrusión popularmente utilizado ya que proporciona una completa descripción de las actividades maliciosas registradas en la red, adicionalmente genera alertas para el administrador de la red. Con esta herramienta es posible detectar ataques de red, ataques semánticos a URL, detecta intentos de Denegación de Servicios por medio de la detección de desbordamientos de búfer, ataques de inyección SQL, entre otros. Sin embargo, Snort se maneja a través de línea de comandos, por lo que requiere una interfaz gráfica para facilitar su uso, por ésta razón se indaga la manera alternativa de implementación de Snort, para el CSIRT de la empresa.

Security Onion. Es Otra herramienta IDS *opensource* gratuita de Linux que permite el monitoreo de la seguridad, detección de intrusos y amenazas, respuesta de incidentes y gestión de registros. El beneficio de esta herramienta es la integración de otras reconocidas como *Snort*, *Wazuh*, *Sguil* y *Suricata* entre otras.[56] Esta herramienta resulta una alternativa interesante para el desarrollo de las actividades del CSIRT.

Sistema AAA. La implementación de una arquitectura de autenticación y autorización, a través de la implementación del protocolo *RADIUS*, es una técnica de seguridad cada vez más extendida. Su funcionamiento implica la interacción de tres componentes: el **punto de acceso a la red** remota que se encarga de pasar la información de autenticación que recibe del usuario final hacia el **servidor de autenticación**, haciendo

[55] CHICANO TEJADA. Op Cit p 24.
[56] SECURITY ONION SOLUTIONS [sitio web]. Security Onion [En línea]. [consultado 25 noviembre 2019]. Disponible en: https://securityonion.readthedocs.io/en/latest/introduction.html

uso de los **protocolos de autenticación** como por ejemplo RADIUS y TACACS/+.[57]

Esta implementación permite ejercer el control de acceso de los usuarios a los recursos y aplicaciones de la organización, autenticación de redes privadas virtual, acceso a la red inalámbrica entre otros. El establecimiento de controles de acceso para los usuarios se constituye en una importante medida de seguridad para CSIRT, puesto que busca salvaguardar la información sensible de los clientes.

Clam AV. Es una herramienta antivirus de código abierto, compuesta por un núcleo de motor de antivirus dispuesto en forma de biblioteca compartida, actualiza automáticamente la base de datos de firmas de virus. Para los entornos Linux, proporciona protección en tiempo real, cuenta con escaneo de correo electrónico, escaneo por medio de línea de comandos. Adicionalmente escanea dentro de archivos comprimidos y soporta diversos formatos de archivos.[58] Esta aplicación, se considera apropiada para usar en el entorno de la empresa caso de estudio, puesto que brinda la funcionalidad de actualización permanente de las bases de datos de firmas de virus, siendo una característica imprescindible en este tipo de herramientas.

Bacula. Es un conjunto de herramientas de software que permiten gestionar el sistema de copias de seguridad, está basado en el modelo cliente servidor con opciones avanzadas de gestión del almacenamiento. Su diseño es escalable, por lo cual se adapta a cualquier tipo de sistema, esta es una característica que hace atractiva a la herramienta para ser aplicado en el caso de estudio, ya que puede adaptarse fácilmente a medida que crece el sistema y adicionalmente está disponible bajo la licencia GNU.[59]

Firejail. Mediante esta herramienta se pueden ejecutar aplicaciones de forma segura aislando su entorno de ejecución, con lo cual se reduce drásticamente el riesgo de infracciones de seguridad sobre el sistema. Dicho entorno aislado es conocido como sandbox o caja de arena, que se logra con Firejail a través del uso de espacios de nombre de Linux y seccomp-BFP, los cuales permiten establecer sobre un proceso y todos sus subprocesos un filtro para las llamadas al sistema de tal forma que tenga una vista

[57] DÍAZ, Gabriel. Procesos y herramientas para la seguridad de redes [en línea]. Madrid: UNED - Universidad Nacional de Educación a Distancia, 2014. 568 p. [consultado 26 noviembre 2019]. Disponible en: https://buscador.biblioteca.uned.es/primo-explore/fulldisplay?vid=34UNED_VU1&search_scope=TAB1_SCOPE1&tab=tab1&docid=34UNED_ALMA2195110980004215&lang=es_ES&context=L

[58] CLAMAV [sitio web]. Clam AntiVirus-Documentation [En línea]. [consultado 2 mayo 2020]. Disponible en: https://www.clamav.net/documents/introduction

[59] BACULA.ORG [sitio web]. What is Bacula? [En línea]. [consultado 2 mayo 2020]. Disponible en: https://www.bacula.org/what-is-bacula/

privada de los recursos del kernel que se comparten a nivel general[60]

Entre las amenazas que son abordadas por Firejail se encuentra el acceso a los directorios de archivos personales en la máquina, las cuales se previenen a través de la tecnología de espacios de nombres de Linux y el módulo de seguridad seccomp-bfp: se simula un árbol de directorios que limita el ingreso al sistema home y crea una estructura de archivos temporal, el cual se elimina cuando se cierra la aplicación

4.1.6 Herramienta Soporte a las Operaciones del CSIRT. Se requieren las siguientes herramientas para la operatividad del centro:

- Apache
- Php
- Mysql
- Bind (dns)
- Sistemas operativos: Kali y Ubuntu

Proxmox VE. Es una plataforma de virtualización de código abierto, empleada a nivel empresarial, para implementar sistemas operativos virtualizados.[61]

4.2 DISEÑO DE LA ESTRUCTURA TECNOLÓGICA DEL CSIRT.

La definición de la estructura tecnológica que soportará las actividades del CSIRT, resulta del análisis de los requerimientos que deben cumplir las dependencias mínimas que formarán parte de este equipo. A partir de la definición de las dependencias, se pueden establecer la distribución física de las oficinas y sus parámetros de seguridad, así mismo, el diseño, configuración y seguridad de la red, teniendo en cuenta el grado de importancia de la información que manejará.

4.2.1 Dependencias del CSIRT. La estructura tecnológica para el CSIRT de Cibersecurity de Colombia se diseña teniendo en cuenta las dependencias mínimas con las que debe contar para el desarrollo de sus operaciones, las cuales requieren de una infraestructura locativa, técnica, y la dotación de equipos informáticos y de

[60] FIREJAIL [sitio web]. Firejail Security Sandbox [en linea]. [Consultado en enero 2021]. Disponible en https://firejail.wordpress.com/

[61] PROXMOX [sitio web]. Proxmox Virtual Environment [En línea]. [consultado 2 mayo 2020]. Disponible en: https://proxmox.com/en/proxmox-ve

comunicaciones que permitan ofrecer los servicios del centro, entre las que se pueden destacar:

Dirección General. En esta se encuentra el despacho del director, en donde podrá reuniones con los asesores externos, y estará dividida para establecer el puesto de trabajo con la persona de atención al cliente del CSIRT. Esto es, dos puestos que deben contar con:

- 2 pc de escritorio
- 2 teléfonos VoIP
- Impresora

Coordinador de TI. Se encarga de administrar los sistemas de información e infraestructura tecnológica de redes y comunicaciones del centro, requiere estar dotado de un pc, impresora de red y teléfono VoIP. Desde esta oficina se lideran las siguientes áreas:

- **Soporte Técnico de TI**. Área encargada de dar soporte técnico y mantener en funcionamiento el equipamiento tecnológico del CSIRT a nivel de hardware y software operativo. Con dos puestos de trabajo equipados con pc y herramientas requeridas para las actividades realizadas:
  - 2 Pc Escritorio
  - 1 teléfono VoIP
  - Herramientas de soporte técnico

- **Centro de Computo,** en donde se alojarán todos los servidores necesarios para la operación de los servicios del CSIRT, éstos son:

  - **Gabinete 1**: para los servidores de la red corporativa: que contendrá los servidores: Web, Intranet, Correo y DNS
  - **Gabinete 2**: para los servidores del CSIRT, que incluye:
    –
      - Servidor SIEM
      - Servidor Monitoreo
      - Servidor de Backup
      - Servidor SandBox
      - Servidor de Archivos
      - Servidor de Registro y Seguimiento de Incidentes

Coordinación Seguridad informática. El Coordinador encabeza el equipo de seguridad informática manejando el servicio de respuestas a incidentes y vulnerabilidades de seguridad, requiere un puesto de trabajo dotado de un pc, impresora de red y teléfono VoIP. Dirige el centro de operaciones del CSIRT que se encuentra formado por las siguientes dependencias:

- **Laboratorio de Análisis de Amenazas**. En esta área se llevan a cabo operaciones delicadas que pueden implicar cierto riesgo de seguridad para el resto de la organización, ya que se realiza tratamiento de incidentes, análisis de sus consecuencias, para recuperar los sistemas afectados en el menor tiempo posible. Esta área requiere mínimo 4 puestos de trabajo que deben dotarse con:

    - 4 Pc de escritorio con sistema operativo Kali Linux y Ubuntu 20.04
    - 4 Teléfono VoIP
    - 1 Herramienta forense duplicador de discos
    - 1 Impresora de red

- **Sala de Monitoreo**, en donde se ubicarán los analistas encargados de detectar de manera eficaz los incidentes de seguridad, vulnerabilidades y dar soporte a los clientes del CSIRT. Requiere:

    - 2 pc con sistema operativo Kali Linux 2020 para analistas de monitoreo
    - 1 pc con sistema operativo Kali Linux 2020 para recepción solicitudes de soporte remoto clientes
    - 1 teléfono VoIP
    - 1 impresora de red

- **Sala de Crisis,** este espacio es designado para que se reúnan los grupos de trabajo cuando se activan las alertas de seguridad, desde donde se establece el centro de control y comando para dar respuesta inmediata ante una crisis
    - Mobiliario para reuniones: sillas y mesas
    - Pantalla multipropósito HD de 60”
    - Tablero acrílico
    - Access point para conexión a internet

Coordinación de Investigación y Desarrollo. Se encuentra a cargo del Coordinador de Investigaciones quien tiene entre sus funciones principales el fortalecimiento de los procesos de investigación del CSIRT, con el objetivo de promover la generación y

publicación de alertas de seguridad, así como diseñar en implementar proyectos de investigación y establecer programas de capacitación del talento humano del CSIRT, conformando de esta manera el sistema de Investigación, Desarrollo innovación (I+D+i). Dirige las siguientes áreas:

- **Laboratorio de investigación**. En esta área se habilitan 1 puesto de trabajo para el coordinador y 2 puestos de trabajo para analistas de seguridad que se encargan de desarrollar tareas de investigación y desarrollo de proyectos diseñados por el Coordinador, dotada con los siguientes elementos:
    - 3 pc con sistema operativo Kali Linux 2020
    - 1 teléfono VoIP
    - 1 Impresora de red

- **Salón de Formación**, en donde se reúne el personal técnico para recibir capacitación o actualización en ciberseguridad sobre técnicas, herramientas, amenazas, etc. que surjan a lo largo del tiempo.
    - Mobiliario para reuniones: sillas y mesas
    - Pantalla multipropósito HD de 60”
    - Tablero acrílico
    - Access point para conexión a internet

4.2.2 **Plano de las instalaciones del CSIRT.** se destaca la importancia de contar con espacios de trabajos separados para las dependencias del CSIRT, los cuales se deben ubicar de manera estratégica para garantizar la confidencialidad como aspecto fundamental en el tratamiento de la información manejada dentro de las instalaciones, esto incluye definir reglas de seguridad física claras para el acceso a cada dependencia. Las instalaciones del CSIRT de Cibersecurity de Colombia debe contar principalmente con los siguientes espacios de trabajo, cuya distribución física se puede observar en la Figura 1:

- Oficina de Dirección
- Oficinas para los coordinadores de Área: Coordinador de TI, Coordinador de I+D+i, Coordinador de Seguridad informática
- Oficina para los investigadores de proyectos de seguridad Informática
- Salón de formación para las capacitaciones del personal
- Sala de monitoreo y alertas
- Laboratorio de Análisis de amenazas y manejo de incidentes
- Sala de crisis
- Centro de computo
- Zona de soporte técnico de TI interno.

Figura 1. Distribución Oficinas Áreas del CSIRT.

Fuente: elaboración propia.

4.2.3 **Seguridad en el Espacio Físico.** Debido a la sensibilidad de la información que se manejará en el CSIRT, es necesario dotar de seguridad los espacios locativos en donde se desarrollan sus actividades. En este sentido, se deben implementar medidas que incluyen:

- Asegurar el control perimetral de las instalaciones **mediante un circuito** de cámaras de vigilancia y control de acceso principal
- Sistema de control y monitoreo de acceso biométrico en: el centro de cómputo, laboratorio de análisis de amenazas y Sala de Monitoreo, por razones de confidencialidad.
- El centro de cómputo debe contar además con sistemas de UPS redundantes, aire acondicionado de respaldo, sistema de control de incendios.

4.2.4 Diseño de la Red. El diseño de la infraestructura tecnológica, definido para el CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA, debe estar encaminado a la protección, tanto de los datos recogidos de los clientes, como de los datos propios de la empresa. Por tanto, es necesario que la información recopilada durante sus operaciones, deba ser almacenada y administrada por el propio CSIRT, preferiblemente dentro de sus instalaciones, es por ello que se estima conveniente, contar con un centro de datos, aislado de la red, una zona de laboratorios, en la que se desarrollaran las actividades relacionadas con la gestión de incidentes, gestión de vulnerabilidades, salón de monitoreo de alertas y demás especificaciones mostradas en la Figura 2, las cuales se detallan a continuación:

- Una fuente redundante del servicio de internet.

- Un router

- Sistema integrado IDS/IPS, para la detección de posibles amenazas y ataques a la red, el cual se ubica en la zona perimetral.

- Se establecen dos zonas desmilitarizadas:

    - DMZ: una para los servicios corporativos que requieren acceso a internet, como lo son servidor web, DNS, correo electrónico e intranet.
    - DMZ interna CSIRT: en donde se contará con el sistema correlacionador de eventos y demás servicios que serán publicados en la red interna del CSIRT.

- Segmentación de la red basada en cortafuegos, ubicándose de la siguiente manera:

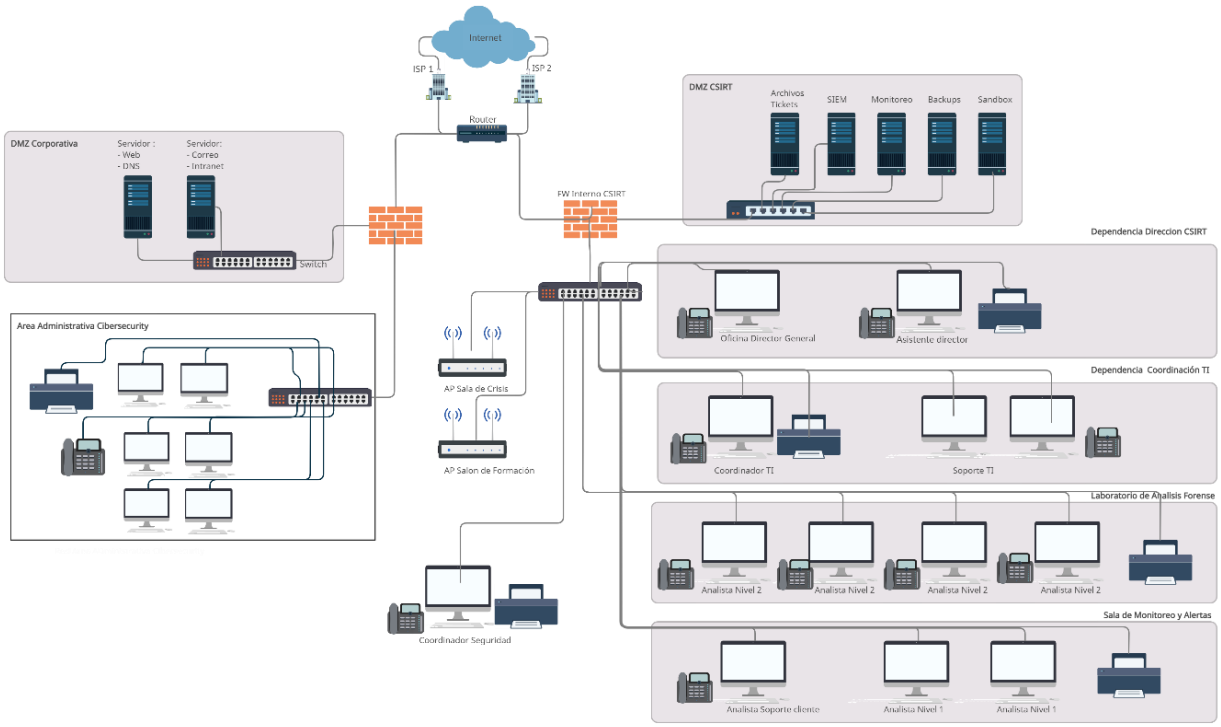
    - Firewall perimetral para aislar los equipos de la empresa de internet, en el cual se tienen 2 VLAN:

        - DMZ Corporativa, servidores esenciales
        - Red Administrativa, que estará conformada por el área administrativa, soporte de TI, logística.

    - Firewall Interno: para la red interna del CSIRT, la cual se encuentra segmentada en 5 VLANs

        - DMZ interna CSIRT, para aislar los servidores de operaciones del CSIRT.
        - Red Laboratorio de análisis: en la que se llevaran a cabo las labores de análisis, investigación, análisis de vulnerabilidades
        - Red Sala de Monitoreo de alertas, para las labores de seguimiento y soporte a incidentes.
        - Red del Area de TI
        - Red del área de I+D+i

Figura 2. Mapa Infraestructura Tecnológica CSIRT.



Fuente: elaboración propia.

4.2.5 Configuración de la Red. El diseño de la red está basado en la segmentación de redes para cada grupo de trabajo tanto de la empresa como del CSIRT. Teniendo en cuenta el carácter de los procesos que desarrolla el CSIRT, se debe garantizar tanto la confidencialidad de la información manejada, como la seguridad de toda red, por lo que se emplean VLAN's para cada subred, lo cual permite además reducir el tráfico de broadcast y mejorar el rendimiento de la red. En este sentido, se emplea un switch con soporte para VLAN, en donde se definen el número y nombre para cada red virtual, se designan los puertos requeridos para cada una y se configura una dirección ip para fines administrativos que permita al área de TI gestionarlo.

Se utilizará direccionamiento clase A, en donde se estructuran siete subredes, de acuerdo con las áreas definidas para el CSIRT, con capacidad para 30 host en cada una de ellas previendo un futuro crecimiento de las áreas, esta segmentación se puede apreciar en la tabla 1.

Tabla 1. Segmentación de la red Cibersecurity de Colombia Ltda.

Segmento	Vlan	Red	Gateway		Ip Broadcast
DMZ corporativa	10	19.10.0.0/27	19.10.0.1	19.10.0.2-19.10.0.30	19.10.0.31
Red administrativa	20	19.10.0.32/27	19.10.0.33	19.10.0.34-19.10.0.62	19.10.0.63
DMZ Interna CSIRT	30	19.10.0.64/27	19.10.0.65	19.10.0.66-19.10.0.94	19.10.0.95
Laboratorios	40	19.10.0.96/27	19.10.0.97	19.10.0.98-19.10.0.126	19.10.0.127
Sala de Monitoreo	50	19.10.0.128/27	19.10.0.129	19.10.0.130-19.10.0.158	19.10.0.159
Coordinación y soporte TI	60	19.10.0.160/27	19.10.0.161	19.10.0.162-19.10.0.190	19.10.0.191
Coordinación I+D+i	70	19.10.0.192/27	19.10.0.193	19.10.0.194-19.10.0.222	19.10.0.223

Fuente: elaboración propia.

Teniendo en cuenta lo anterior, se establece la VLAN 10 para la DMZ corporativa, asignando a los servidores el direccionamiento IP dentro de la red 19.10.0.0/27, como se muestra en la tabla 2; por otra parte, los equipos de la red administrativa se configuran con IP fija dentro de la red 19.10.0.32/27, en la VLAN 20 dejando la ip 19.10.0.33 para el switch que funcionara como Gateway.

Tabla 2. Direccionamiento IP Servidores DMZ corporativa

Servidor	VLAN	IP	Gateway
Web	10	19.10.0.2	19.10.0.1
Intranet	10	19.10.0.3	19.10.0.1
Correo	10	19.10.0.4	19.10.0.1
DNS	10	19.10.0.5	19.10.0.1

Fuente: elaboración propia.

En la tabla 3, se desglosa el direccionamiento los servidores internos del CSIRT

Tabla 3. Direccionamiento IP DMZ interna del CSIRT

Servidor	VLAN	IP	Gateway
Servidor SIEM	30	19.10.0.66	19.10.0.65
Servidor Monitoreo Zabbix	30	19.10.0.67	19.10.0.65
Servidor de Backup	30	19.10.0.68	19.10.0.65
Servidor SandBox	30	19.10.0.69	19.10.0.65
Servidor de Archivos	30	19.10.0.70	19.10.0.65
Servidor de Registro y Seguimiento de Incidentes	30	19.10.0.71	19.10.0.65

Fuente: elaboración propia.

Los equipos de los analistas encargados de las operaciones del CSIRT, se configuran igualmente con direccionamiento estático, como se muestra en la tabla 4, y la navegación debe estar controlada según las políticas definidas por el CSIRT.

Tabla 4. Direccionamiento IP equipos Laboratorio de Análisis y Sala de Monitoreo

Equipo	VLAN	IP	Gateway
Coordinador Seguridad	40	19.10.0.98	19.10.0.97
Analista nivel 2	40	19.10.0.99	19.10.0.97
Analista nivel 2	40	19.10.0.100	19.10.0.97
Analista nivel 2	40	19.10.0.101	19.10.0.97
Analista nivel 2	40	19.10.0.102	19.10.0.97
Analista nivel 1	50	19.10.0.130	19.10.0.129
Analista nivel 1	50	19.10.0.131	19.10.0.129
Analista nivel 1	50	19.10.0.132	19.10.0.129

Fuente: elaboración propia.

Se destina una vlan para el área de TI y una vlan para el área Investigación con el direccionamiento descrito en la tabla 5.

Tabla 5. Direccionamiento IP equipos del area de TI y del area de I+D+i

Equipo	VLAN	IP	Gateway
Coordinador TI	60	19.10.0.162	19.10.0.161
Técnico Soporte TI	60	19.10.0.163	19.10.0.161
Técnico Soporte TI	60	19.10.0.164	19.10.0.161
Coordinador I+D+i	70	19.10.0.194	19.10.0.193
Analista de Investigación	70	19.10.0.195	19.10.0.193
Analista de Investigación	70	19.10.0.196	19.10.0.193

Fuente: elaboración propia.

4.2.6 Seguridad de la Red. Es necesario establecer reglas dentro de la red de la empresa en general en aras de proteger la confidencialidad, integridad y disponibilidad de la información manejada tanto en el área administrativa como en el área de operaciones del CSIRT.

- En este sentido, se utilizará un Firewall UTM, dentro del cual se gestione, las DMZ definidas en la infraestructura con sus reglas, y adicionalmente se realizará la segmentación de las VLAN

- Se requiere que el área de laboratorio, sala de monitoreo y área administrativas se encuentren aisladas, para lo cual, se debe establecer ACL, que niegue todo el tráfico hacia las redes 19.10.0.96/27 y 19.10.0.128/27

- Se empleará un sistema de prevención de intrusos, a través de la herramienta SNORT, la cual se encargará de ejecutar el análisis del tráfico en todos los segmentos de red predefinidos.

- Se debe aplicar seguridad en los puertos de los conmutadores de tal forma que solo se puedan conectar los equipos autorizados, se permite solo un equipo máximo en un puerto y se establece política de violación “Shutdown”, en caso de que se presente un acceso no autorizado

4.3 REQUERIMIENTOS TECNOLOGICOS DE HARDWARE DEL CSIRT

A partir del diseño de la estructura tecnológica y los requerimientos funcionales de las herramientas de software, se definen en esta sección, las necesidades de equipamiento de hardware mínimo para el desarrollo de las actividades del CSIRT.

4.3.1 Infraestructura del Centro de Computo Se requieren los siguientes elementos de hardware para el centro de cómputo:

4.3.1.1 Servidores. Como solución de hardware para los servidores se plantea la implementación de tecnologías de virtualización que mediante el uso de un hypervisor se ejecuta directamente sobre el hardware, evitando la elevación de otro sistema operativo. Para este propósito se plantea dos servidores con las siguientes características mínimas:

- Procesador Intel® Xeon® W-3275 (caché de 38,5 M, 2,50 GHz) de 28 núcleos
- Memoria Ram 512GB DDR4-2933, 2933 MHz/
- Arreglo de 8 Discos Duros de 8 TB SATA Read Intensive 6Gbps 512 2.5in Hot-plug Drive
- Tarjeta Red 2 Port 10Gb Base

4.3.1.2 Storage Area Network SAN (Red de Area de Almacenamiento). un sistema de almacenamiento de red, que realice la organización y gestion de las unidades de almacenamiento de respaldo en una sola unidad virtual de forma que garantice la tolerancia a fallos y el restablecimiento de la operatividad de los servidores. Para lo cual se recomienda el siguiente dispositivo:

- SAN HPE MSA 2050, con un arreglo de 16 discos de 8 TB.

4.3.1.3 Sistemas de alimentación ininterrumpida. Requerida para suministrar respaldo de energía a los servidores del CSIRT en caso de presentarse falla en el suministro, que proporcione una autonomía mínima de 30 minutos. Estas características pueden variar en torno a los dispositivos conectados, teniendo en cuenta que a medida que crece la infraestructura se deben ampliar las capacidades descritas para soporta su optimo funcionamiento. Por ello para respaldar los dos servidores de virtualización se recomienda:

- 1 UPS On-line 20 KVA 220 VA

4.3.1.4 Dispositivos de Conectividad de red

- Router perimetral para la conexión al servicio de internet y la administración del trafico
- 2 Next Generation Firewall, para el filtrado del tráfico de red, que soporte funciones de inspección profunda de paquetes para cubrir la identificación de ataques, prevención de intrusiones y otros aspectos de seguridad de la red. Adicionalmente debe soportar la segmentación VLAN's.
- Switch Core Fibra óptica de 48 puertos de 10GbE y 8 puertos de 100 GbE.
- Cableado estructurado de red.

4.3.2 Infraestructura del Laboratorio y Sala De Monitoreo. Se requieren los siguientes elementos de hardware:

4.3.2.1 Estaciones de trabajo. Equipos requeridos para el desarrollo de las labores propias del Laboratorio técnico (4 equipos), y para la sala de monitoreo (2 equipos), los cuales deben contar con las siguientes características:

- Procesador de 8 núcleos
- Memoria Ram 8GB (1x8GB) 2666MHz
- Disco Duro Disco duro SATA de 3,5 GB - 2 TB de 7200 RPM
- Tarjeta Red integrada
- Monitor led de 28"

4.3.2.2 Sistemas de alimentación ininterrumpida. Requerida para suministrar respaldo de energía en caso de presentarse falla en el suministro, que proporcione una autonomía mínima de 5 minutos, para cada una de las 6 estaciones de trabajo del laboratorio y la sala de monitoreo del CSIRT, que tengan las siguientes características:

- 6 UPS Interactivas de 3 Kva.

4.3.2.3 Herramienta Forense. Herramienta de hardware, para la generación de duplicados de discos duros, o imágenes forenses. Es requerida para la prestación de los servicios de análisis de incidentes el cual implica la recolección de evidencia presente en los dispositivos informáticos, debe tener las siguientes características:

- Puertos: IDE / PATA, USB 2.0, USB 3.0, eSATA, Ethernet
- Tipo de unidades compatibles: PATA / IDE 3.5, Unidades SATA de 2.5 " y 3.5 ", iSCSI (SCSI conectado a la red), SSD SATA (unidades de estado sólido), Memorias USB (USB 3.0 / 2.0 / 1.1) Entre otras

- Compatibilidad del sistema operativo: Windows, Mac OS X 10.4.xo superior, iOS Tabletas / teléfonos, Android Tabletas / teléfonos, La mayoría de las versiones de Linux

4.3.2.4 Elementos Audiovisuales. Para el desarrollo de las capacitaciones permanentes que deben realizar el personal del CSIRT, a través éstas, se puede transmitir de manera didáctica y explicita los conocimientos provenientes de las actualizaciones en el campo de la ciberseguridad. Se requiere como mínimo las siguientes:

- Televisor UltraHD de 60”
- Tablero acrílico de 1.20 * 80 cm,
- Access point

4.4 DISEÑO LOGICO DEL LABORATORIO CONTROLADO PARA EL CSIRT

En este apartado se documentan las pruebas de software realizadas a las herramientas propuestas para el CSIRT, a partir del diseño de un laboratorio controlado a pequeña escala, mediante el cual se puede verificar las funcionalidades y efectividad ofrecidas por las herramientas.

A continuación, se detalla la arquitectura empleada para la virtualización de los servidores de monitoreo, correlación de eventos, copias de seguridad y sandbox, utilizando las herramientas de software descritas en la sección 4.1, el despliegue de estos servidores permite mostrar el proceso de configuración y la ejecución de pruebas de funcionamiento de las herramientas de software.

4.4.1 Preparación de la plataforma de virtualización. Para el desarrollo de este objetivo se diseña el Laboratorio Lógico controlado a partir de la virtualización de algunas de las herramientas empleadas en el CSIRT como lo son: Servidor de monitoreo, Correlacionador de Eventos, Servidor de Copias de Seguridad, Servidor Sandbox, para la ejecución de las pruebas de software a cada una de ellas. Se emplea la herramienta de virtualización VirtualBox Versión 6.1 en una maquina física, sobre la cual se levantarán las máquinas virtuales para los servidores mencionados cuyas características se detallan en la tabla 6.

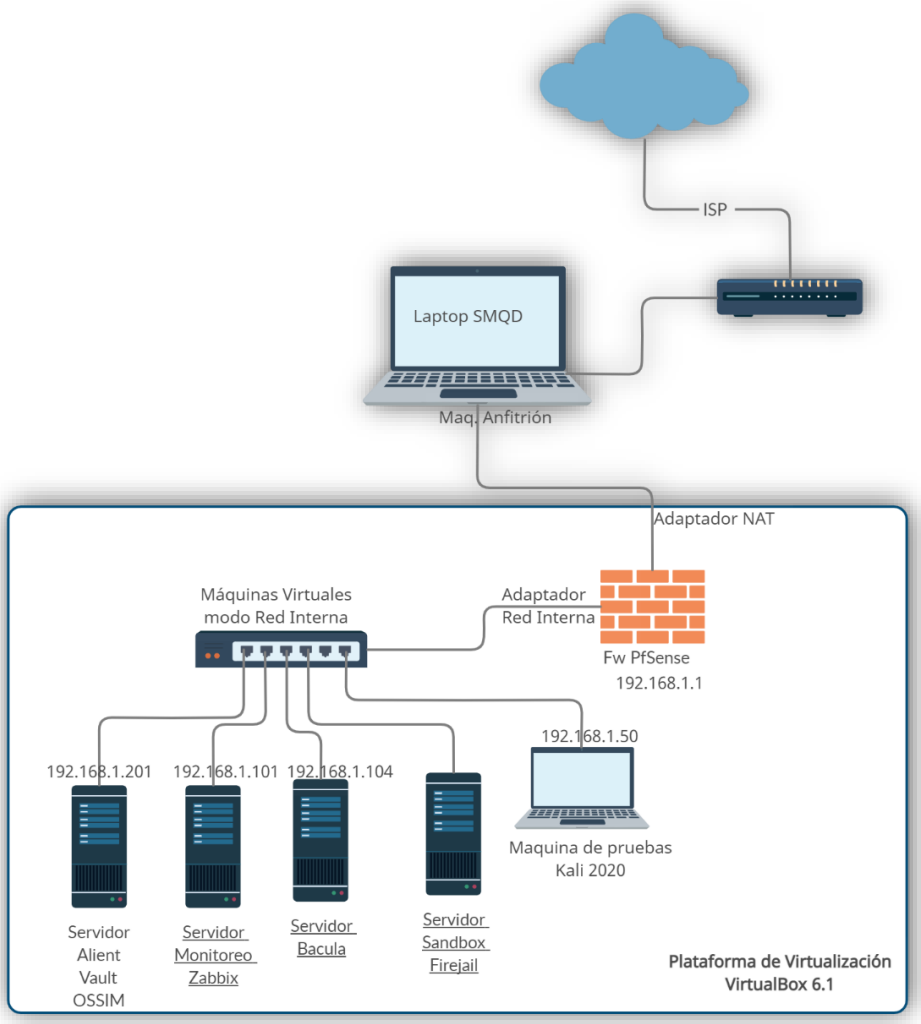
Tabla 6. Detalle Máquinas Virtualizadas

Maquina Física	Maquinas Virtualizadas en VirtualBox 6.1					
	Servidor	**Sistema Operativo**	**RAM**	**Disco Duro**	**Procesador**	**Interfaz LAN**
HP Laptop 15-da0xxx Procesador: Intel Core i5-8250U 1.60GHz Memoria (RAM) : 16,00 GB Disco duro: 1 Tb SO: Windows 10 Home Single	Monitoreo ZABBIX	Ubuntu Server 20.04	2 Gb	20 Gb	1 CPU	Adaptador LAN Red interna
	Correlacionador de Eventos OSSIM	OSSIM	4 Gb	25 Gb	3 CPU	2 adaptador LAN Red interna
	Servidor Sandbox Firejail	Ubuntu Server 20.04	2 Gb	20 Gb	1 CPU	Adaptador LAN NAT
	Servidor de Backup Bacula	Ubuntu Server 20.04	2 Gb	36 Gb	1 CPU	Adaptador LAN Red interna
	Firewall pfSense	FreeBSD	1 Gb	16 Gb	1 CPU	1 Adaptador LAN NAT 1 Adaptador LAN Red interna
	Maquina Pruebas	Kali Linux 2020	2 Gb	30 Gb	1 CPU	Adaptador LAN Red interna

Fuente: elaboración propia.

En la topología empleada para el laboratorio controlado, se configuran los servidores en un segmento de red aislado de la red del equipo anfitrión, a través de la virtualización de adaptadores en modo Red Interna. Los servidores se conectan a un firewall tipo software virtualizado, a través del cual tienen salida a internet. En la Figura 3 se visualiza el mapa de la topología descrita anteriormente.

Figura 3. Topología Laboratorio Lógico Controlado.



Fuente: elaboración propia.

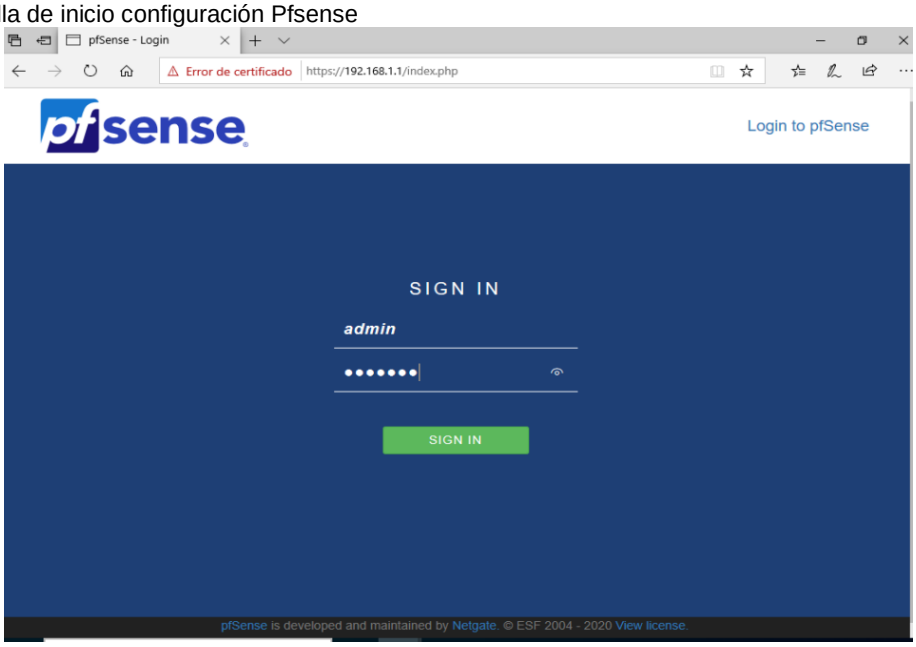
4.4.2 Configuración y puesta en marcha de los servidores. Una vez realizado el proceso de instalación de los servidores, el cual se describe en el anexo A, se procede a realizar la configuración de estas máquinas para adecuar cada herramienta de software a las funciones requeridas por el CSIRT para los procesos que desarrolla.

4.4.2.1 Firewall. Se inicia con la configuración de un firewall tipo software denominado Pfsense, basado en el sistema operativo FreeBSD, el cual es útil para la implementación de pruebas del servidor de correlación de eventos, los pasos de la instalación se encuentran en el anexo A.1.

Una vez instalada la herramienta, se accede al dashboard para realizar la configuración

a través de un navegador web, accediendo por medio de la dirección ip que se configuró en la interfaz LAN: https://192.168.1.1. Se debe tener en cuenta aceptar la advertencia de seguridad que emite el navegador, dado que Pfsense utiliza un certificado auto firmado, luego se inicia sesión con las credenciales por defecto usuario: Admin, contraseña: pfsense, se muestra una pantalla como se muestra a continuación.

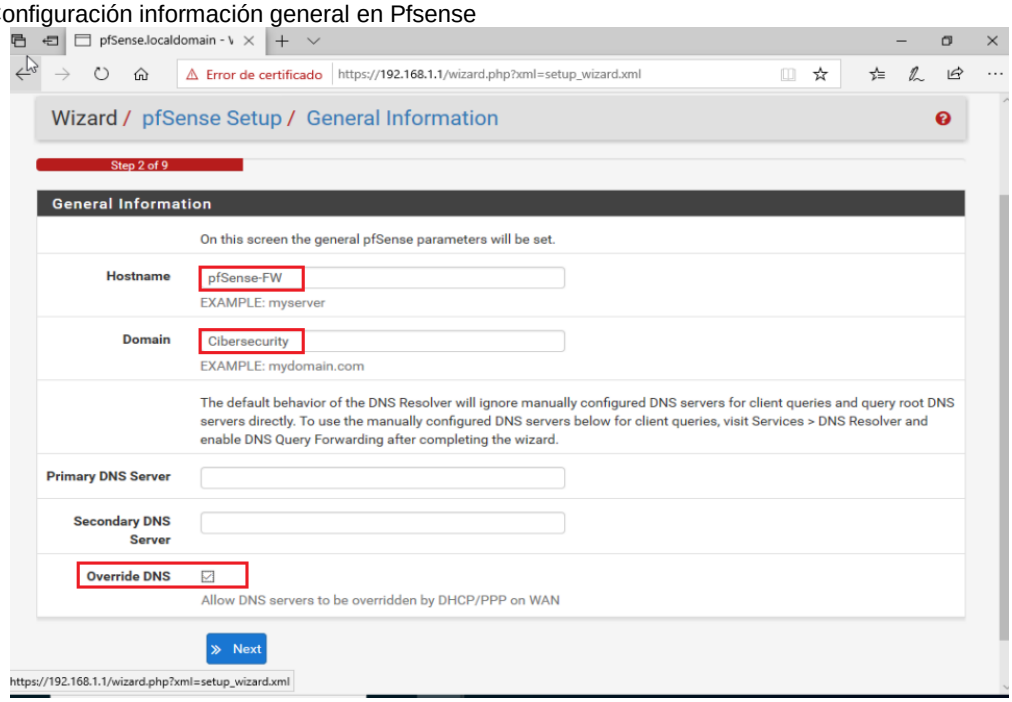
Figura 4. Pantalla de inicio configuración Pfsense



Fuente: elaboración propia.

Al iniciar sesión se muestra un asistente de configuración en donde se despliega un mensaje de bienvenida, en donde se presiona el botón siguiente en las dos primeras opciones. Seguidamente, se requiere establecer las opciones de nombre de host, nombre de dominio y la configuración de los servidores DNS, para este caso se selecciona la opción de sobreescritura DNS, dado que se activó el DHCP (ver Figura 5).

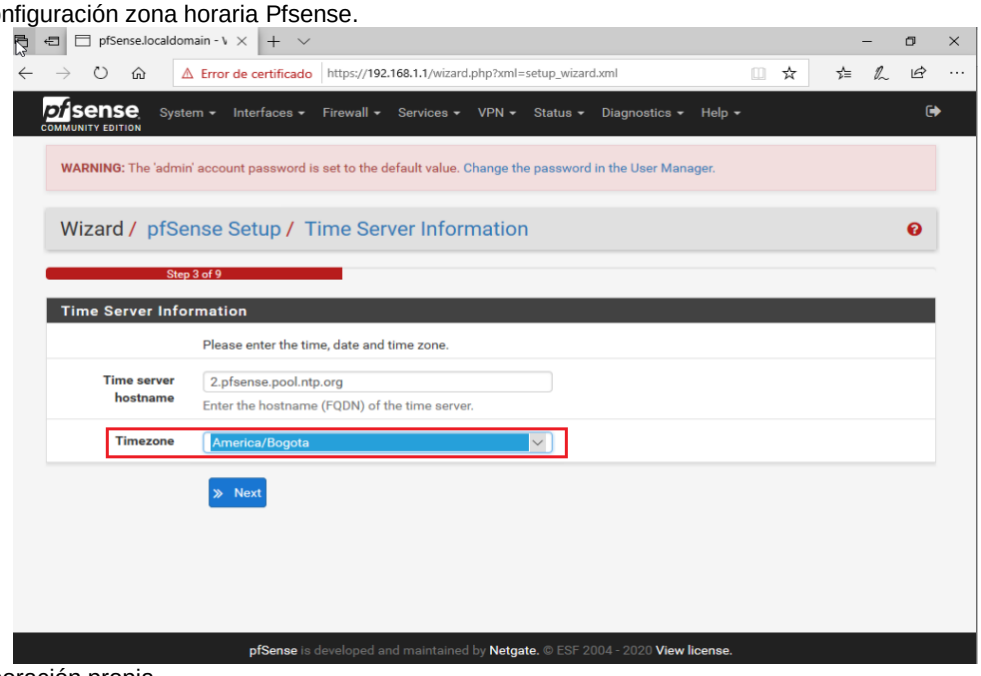
Figura 5. Configuración información general en Pfsense



Fuente: elaboración propia.

En el siguiente paso se selecciona la zona horaria en el campo TimeZone, como se observa en la siguiente Figura y se presiona el botón next.

Figura 6. Configuración zona horaria Pfsense.



Fuente: elaboración propia.

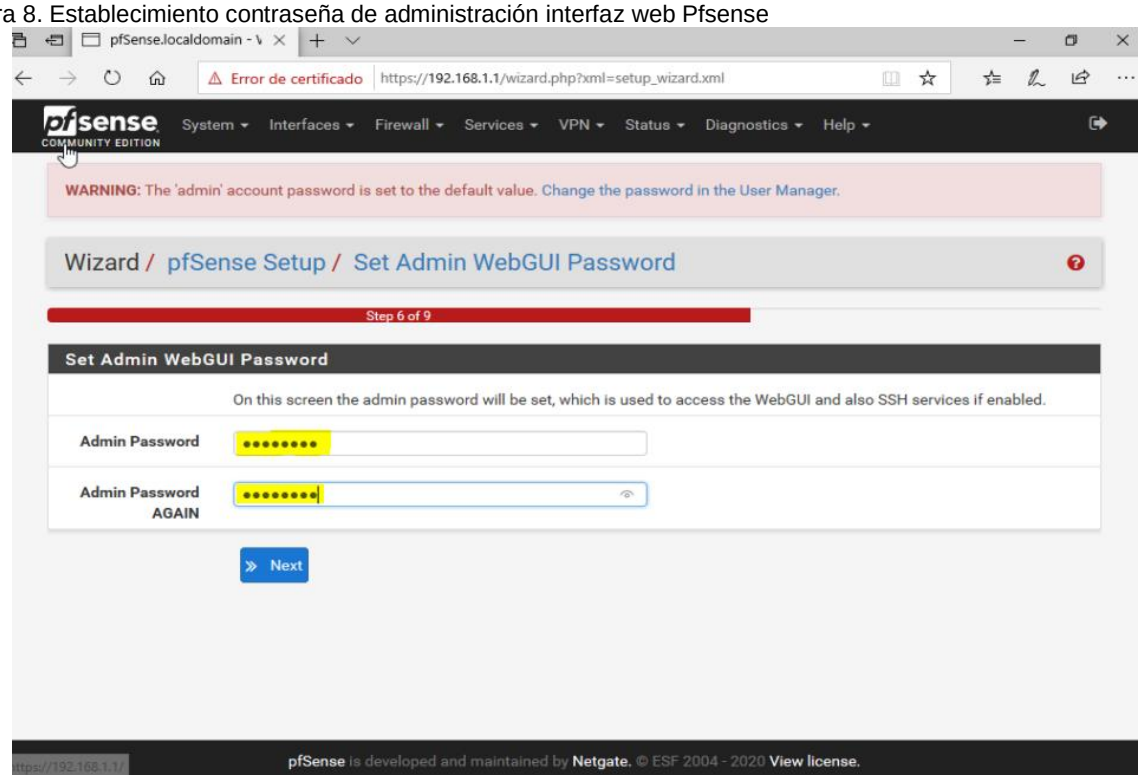
En el cuarto paso, se establece la configuración de la interfaz WAN, que para este caso se selecciona el tipo DHCP, en entornos empresariales se recomienda utilizar una dirección ip estática proporcionada por el proveedor de internet.

Figura 7. Configuración de la interfaz WAN de Pfsense

Fuente: elaboración propia.

En el siguiente paso, se muestra la configuración de la interfaz LAN, donde se confirma la ip 192.168.1.1, se presiona en el botón siguiente, para dar paso a la configuración cambiar la contraseña por defecto por una más robusta para el usuario de administración del pfsense, como se indica en la Figura 8.

Figura 8. Establecimiento contraseña de administración interfaz web Pfsense



Fuente: elaboración propia.

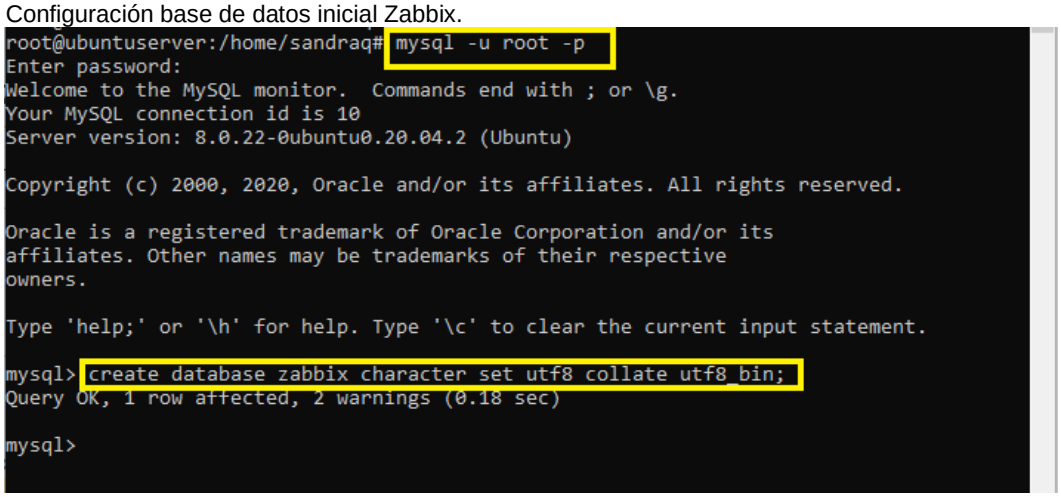
Posteriormente se pide recargar todas las configuraciones que se han establecido presionando en el botón “Reload”, finalmente se muestra que se ha terminado la configuración base por medio del asistente con el mensaje: “Congratulations pfSense is now configured”.

4.4.2.2 Servidor de monitoreo Zabbix. Se emplea para esta máquina la herramienta Zabbix version 5.01, el proceso de instalación y preparación preliminar se detalla en el anexo A.2, en donde se puede observar que se requiere una instalación previa de un servidor MySql que se encargará de gestionar la base de datos generada por Zabbix. A continuación, se describen los pasos necesarios para la configuración:

- **Configuración base de datos**. Se inicia creando la base de datos en donde Zabbix almacenará la información, se utiliza la codificación UTF-8 que es la única compatible con Zabbix y sobre la cual se conoce que funciona sin fallas de seguridad[62] . Utilizando los comandos “mysql -uroot -p” y “mysql> create database zabbix character set utf8 collate utf8_bin;” como se observa en la Figura a continuación:

[62] ZABBIX. [sitio web]. Zabbix Documentation 5.0 [En línea]. [consultado 16 diciembre 2020]. Disponible en: https://www.zabbix.com/documentation/5.0/manual/appendix/install/db_scripts#mysql

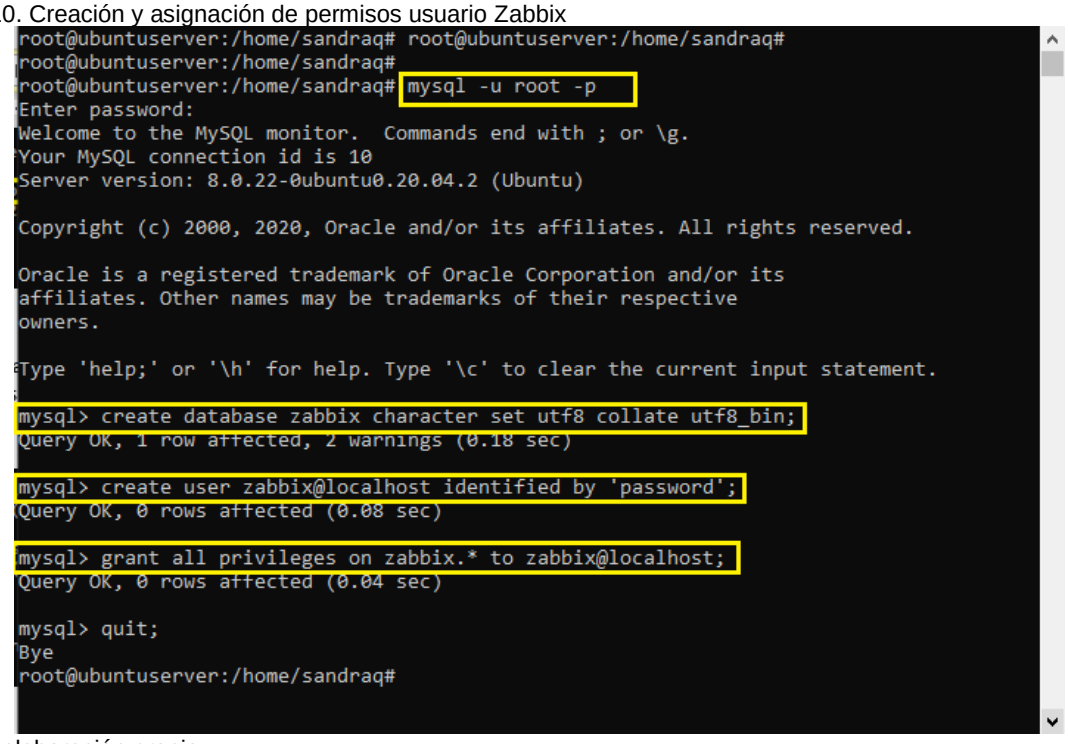
Figura 9. Configuración base de datos inicial Zabbix.



Fuente: elaboración propia

Posterior a ello, se procede a la creación del usuario para Zabbix con su respectiva contraseña y se conceden todos los privilegios como se observa en la siguiente figura:

Figura 10. Creación y asignación de permisos usuario Zabbix



Fuente: elaboración propia

Se requiere importar el esquema y los datos iniciales, para lo cual se debe proporcionar la contraseña asignada al usuario recién creado, empleando la siguiente instrucción “zcat

/usr/share/doc/zabbix-server-mysql*/create.sql.gz | mysql -uzabbix -p zabbix”

Figura 11. Esquema de datos iniciales de Zabbix

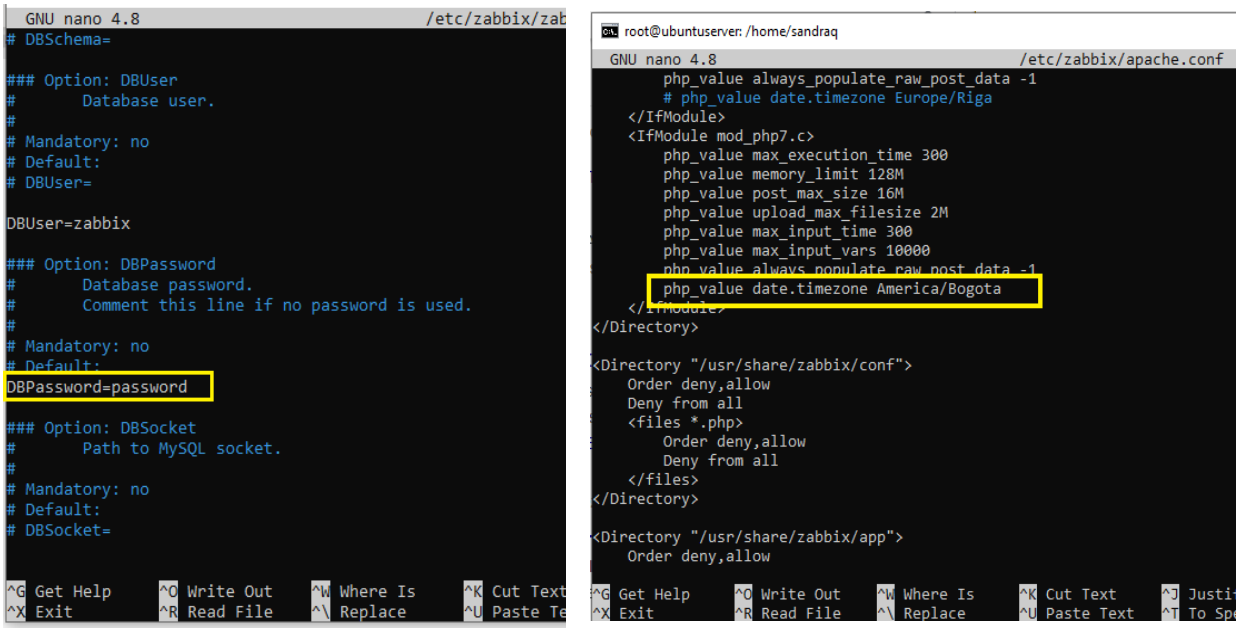
```
root@ubuntuserver:/home/sandraq# zcat /usr/share/doc/zabbix-server-mysql*/create.sql.gz | mysql -uzabbix -p zabbix
Enter password:

root@ubuntuserver:/home/sandraq#
```

Fuente: elaboración propia

– **Preparación archivos de configuración de Zabbix**.

Es necesario editar el archivo de configuración del servidor Zabbix para indicar la información sobre la base de datos, este archivo se encuentra en la ruta: /etc/zabbix/zabbix_server.conf, en donde se debe establecer la contraseña del usuario Zabbix, como se observa en el lado derecho de la Figura 12. De igual forma se debe establecer en el archivo de configuración de apache la zona horaria del servidor, en la forma como se aprecia en la Figura 12 lado izquierdo.

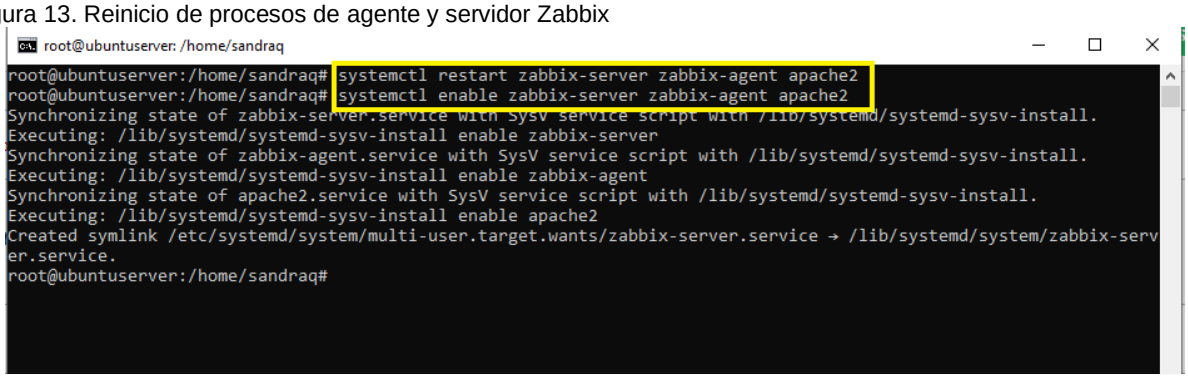
Figura 12. Modificación archivo de configuración Zabbix



Fuente: elaboración propia

Al finalizar lo anterior, se procede a iniciar los procesos del agente y del servidor Zabbix y configurarlos para que se inicien con el sistema. (ver Figura 13)

Figura 13. Reinicio de procesos de agente y servidor Zabbix

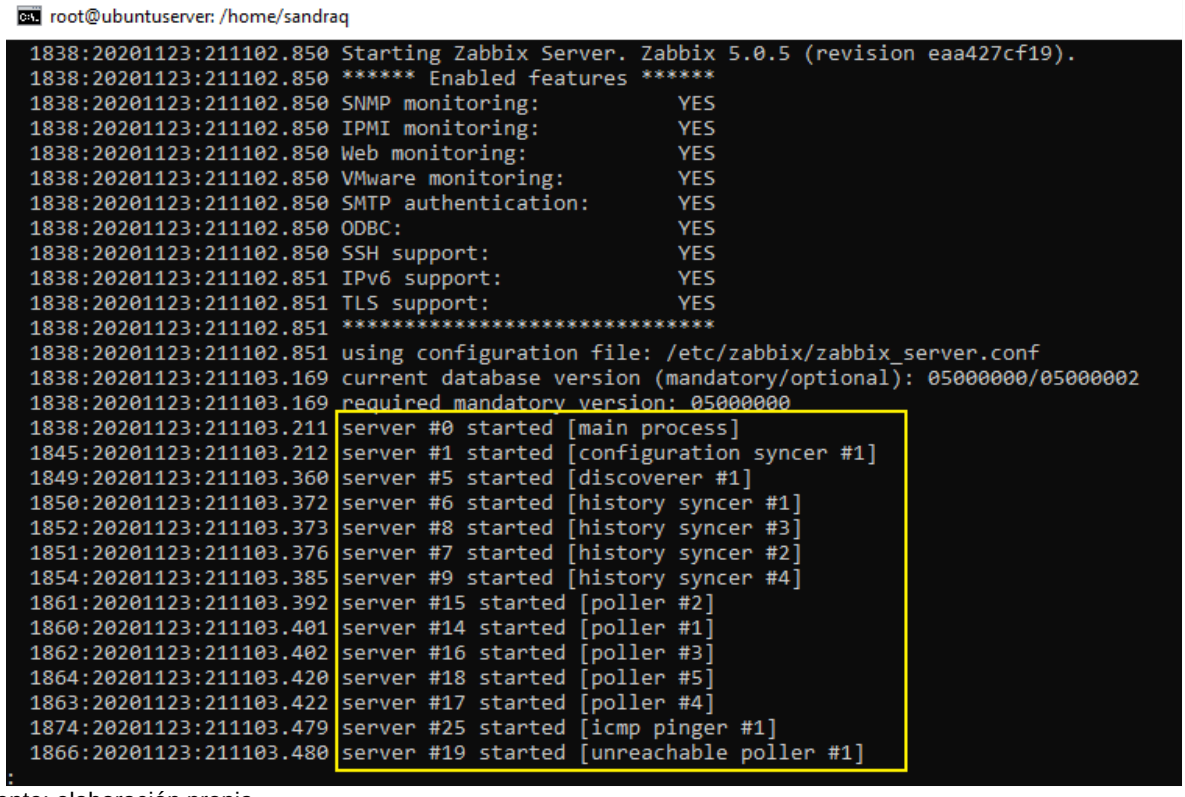


Fuente: elaboración propia

– Verificación de funcionalidad del servidor

Para comprobar que el servidor Zabbix esté funcionando correctamente se realiza una revisión de los archivos de registro de Zabbix, se emplea el comando “less” para visualizar el contenido del log ubicado en /var/log/zabbix/zabbix_server.log, como se muestra en la Figura 14, Zabbix inicia sus procesos correctamente

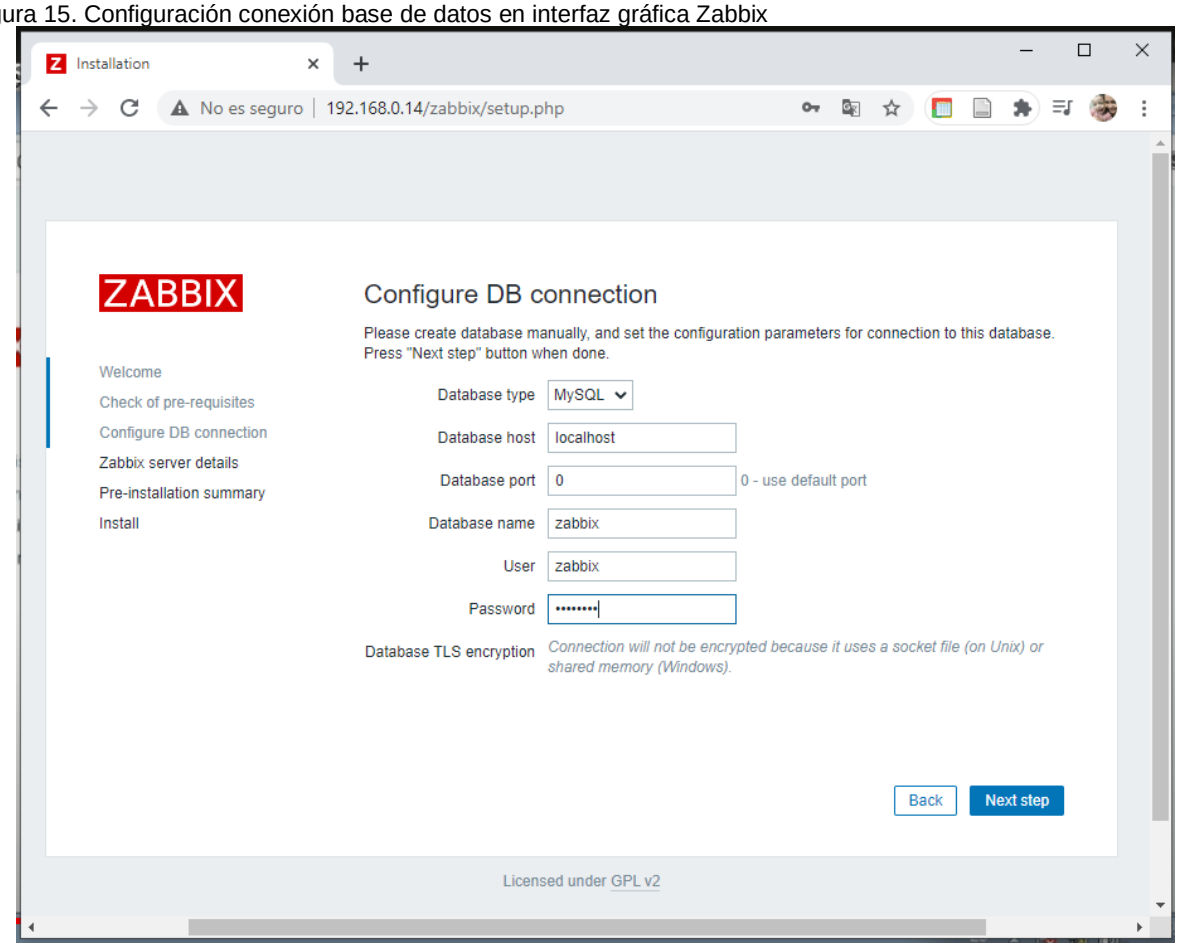
Figura 14. Verificación funcionalidad servidor Zabbix



Fuente: elaboración propia

– **Configuración interfaz gráfica**. Finalmente es necesario configurar la interfaz de zabbix_ el front-end, para esto se debe ingresar desde un navegador en la ruta http://server_ip_or_name/zabbix, en donde se muestra un asistente de configuración que lo que hace crear un nuevo archivo de configuración, al presionar en el botón siguiente se observan algunos parámetros de PHP requeridos para el funcionamiento de Zabbix, se pulsa en el botón siguiente para continuar al punto del establecimiento de los parámetros de conexión a la base de datos, como se observa en la Figura 15.

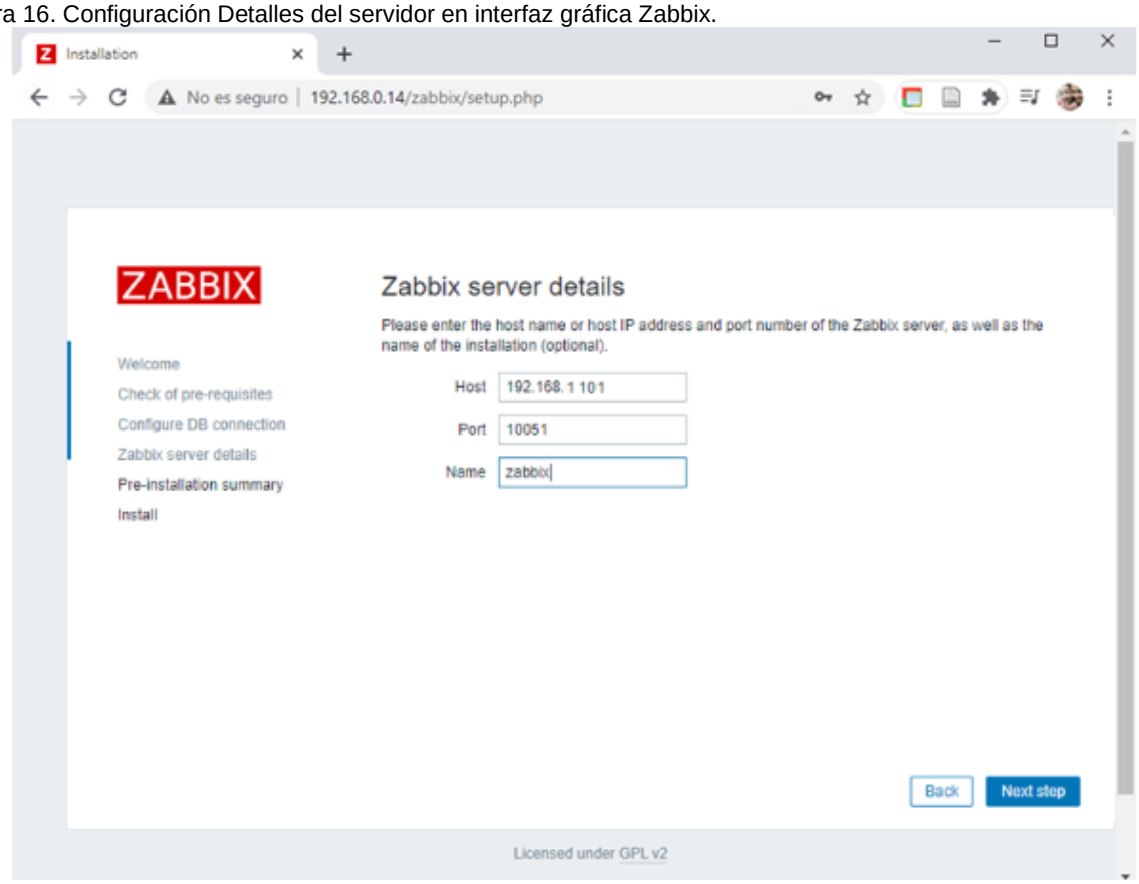
Figura 15. Configuración conexión base de datos en interfaz gráfica Zabbix



Fuente: elaboración propia

Al presionar en el botón siguiente, se piden los detalles del servidor zabbix como la ip, el puerto 10051 y se define un nombre para el mismo, como se muestra en la siguiente Figura.

Figura 16. Configuración Detalles del servidor en interfaz gráfica Zabbix.



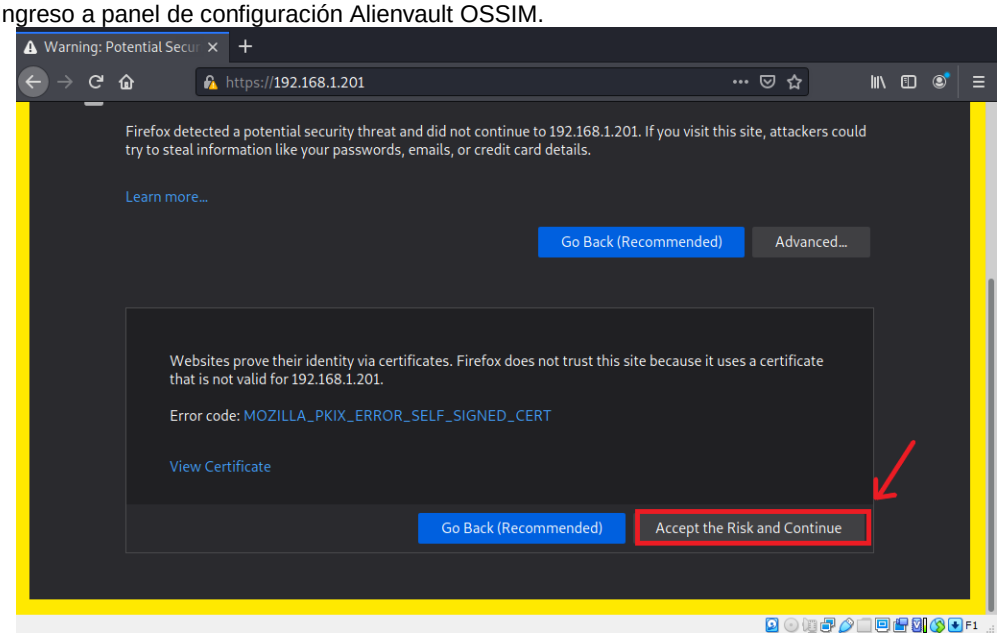
Fuente: elaboración propia

Al finalizar los procedimientos mencionados, en una nueva pantalla se indica un resumen de la configuración proporcionada, en donde finalmente se debe presionar el botón siguiente y se muestra la ruta en donde se guarda la información de la configuración

4.4.2.3 Correlacionador de Eventos AlienVault OSSIM Se utiliza la herramienta Open Source denominada Alienvault OSSIM version 5.8.5 de 64 bits, la instalación se lleva a cabo a través de una imagen ISO descargada desde la página oficial, este proceso se observa en detalle en el anexo A.3, donde se evidencia que los requisitos de hardware son exigentes para un funcionamiento adecuado.

Al finalizar la instalación, se procede a acceder al panel de configuración del servidor desde otra máquina de la red, por medio de un navegador de internet en la dirección ip establecida para fines de administración, como se observa en la Figura 17, se debe ingresar la ruta https://192.168.1.201 aceptar las advertencias de seguridad que muestra el navegador, debido a que OSSIM emplea un certificado auto firmado.

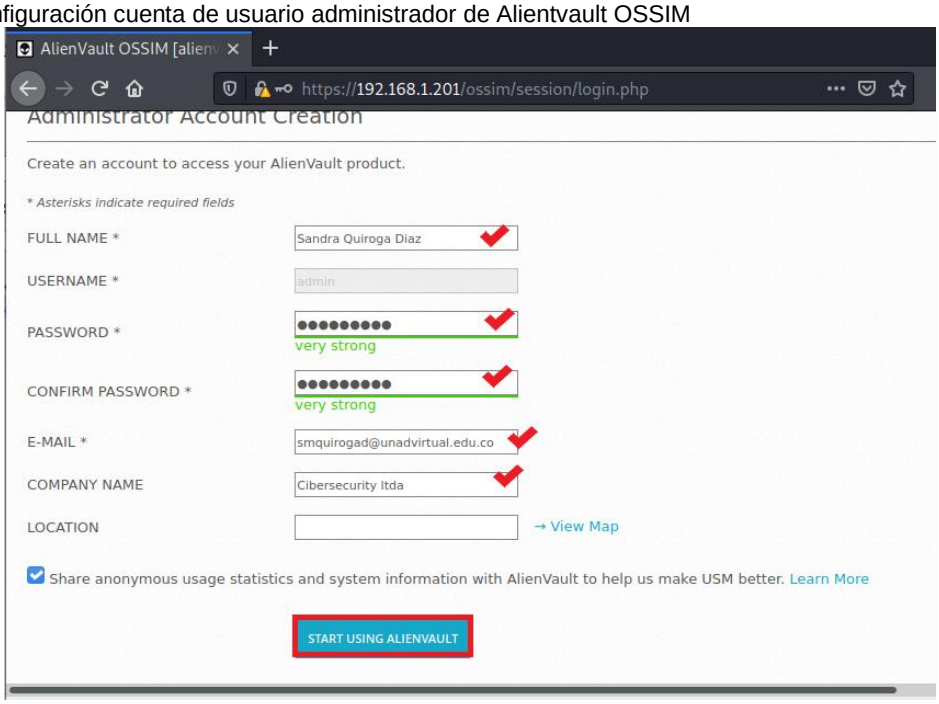
Figura 17. Ingreso a panel de configuración Alienvault OSSIM.



Fuente: elaboración propia

En la Figura 18, se indican los datos para completar la información de la cuenta de usuario de administración del servidor, se presiona el botón “iniciar usando Alienvault”, con lo cual abrirá la pantalla de login del servidor.

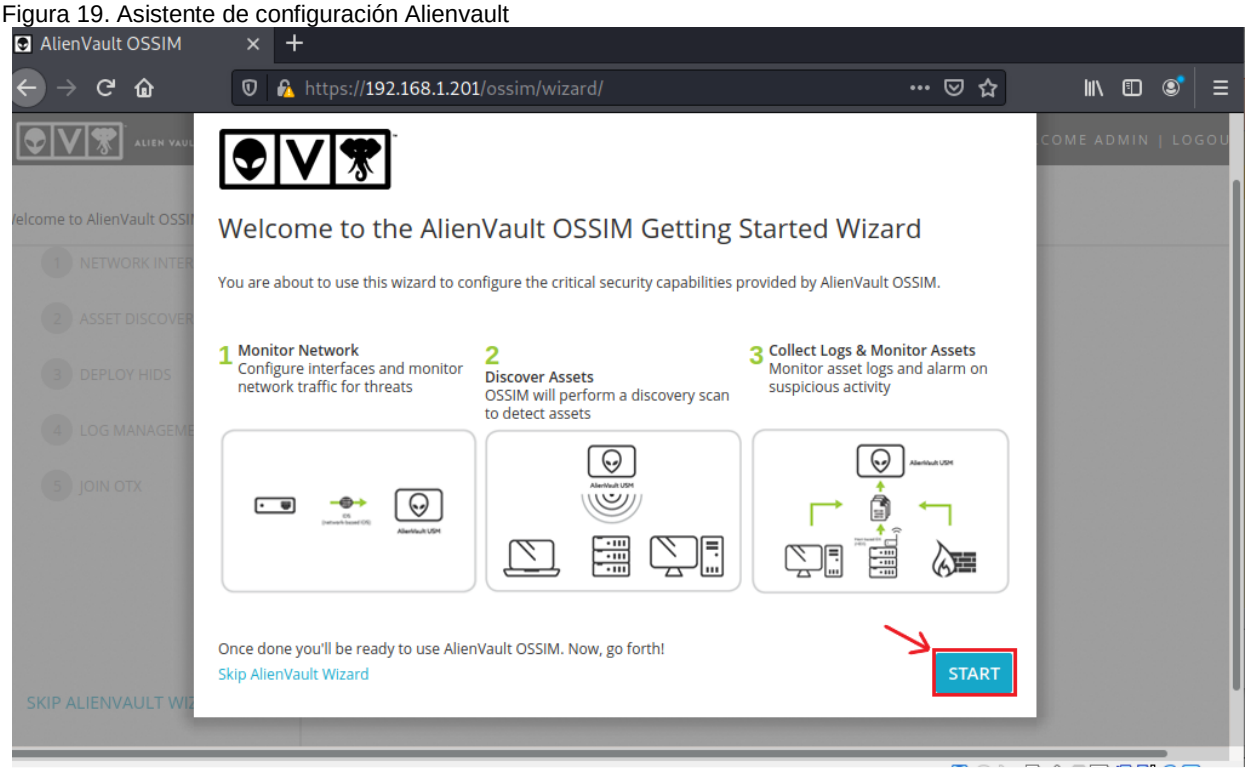
Figura 18. Configuración cuenta de usuario administrador de Alientvault OSSIM



Fuente: elaboración propia

Después de iniciar sesión desde el login del navegador, aparece un asistente de configuración que muestra el despliegue inicial de la herramienta, donde indica los tres principales pasos a realizar, como se observa en la Figura 19. En primer lugar, se debe indicar la interfaz de red por donde se recolectarán los logs y se realizara el monitoreo de amenazas, en segundo lugar, se realiza el descubrimiento de nodos de la red o los activos a monitorear y por último se configuran los plugins requeridos para que el software reconozca los logs recolectados.

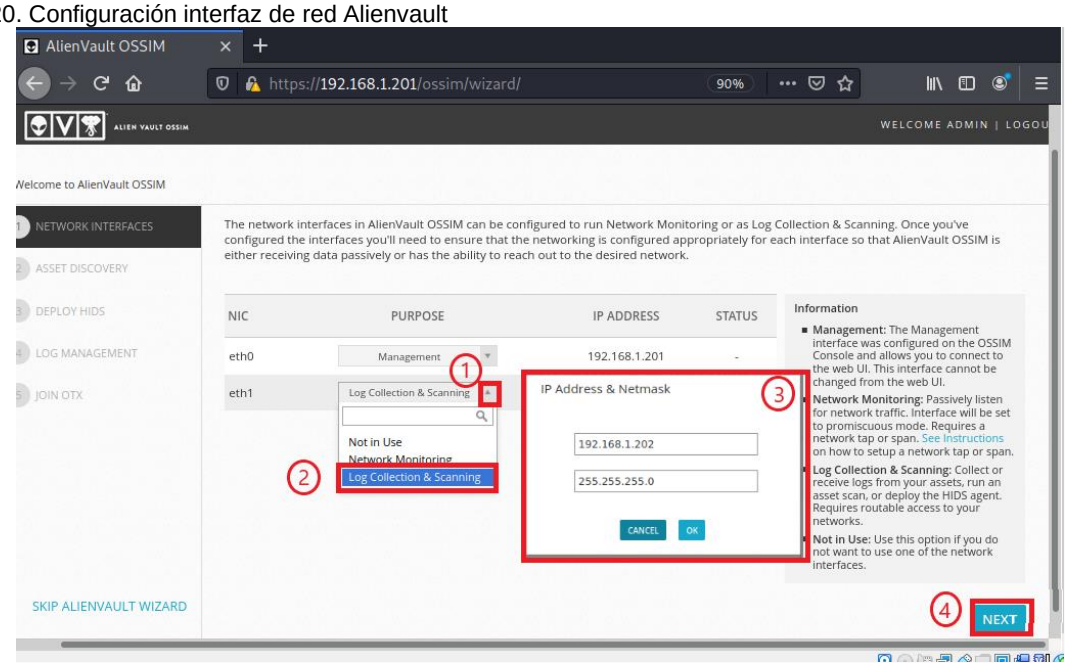
Figura 19. Asistente de configuración Alienvault



Fuente: elaboración propia

Al presionar en el botón inicio, se abre una nueva ventana en donde se debe establecer la configuración de la interfaz de red que se encargara de recolectar los logs, para este caso, como muestra la Figura 20, se selecciona en la interfaz eth1 dentro de la lista desplegable, la opción “Log Collection and Scanning”, en la ventana flotante se establece la ip y mascara de subred y se presiona el botón ok.

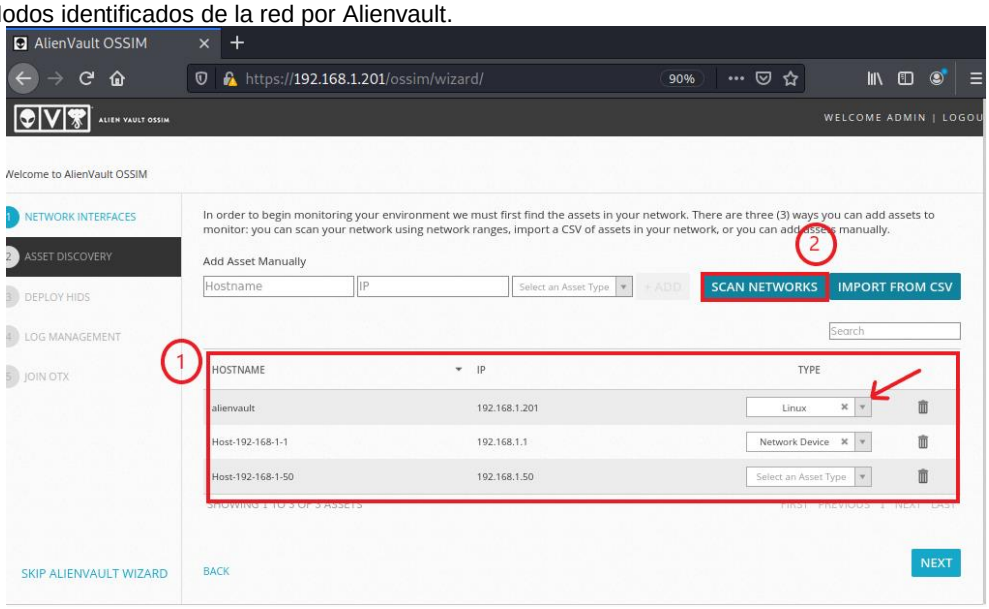
Figura 20. Configuración interfaz de red Alienvault



Fuente: elaboración propia

A finalizar este proceso se presiona el botón next, esto muestra una nueva ventana en la que se realiza un escaneo de toda la red, identificando algunos de los nodos conectados como se observa en la Figura 21. Es muy importante conocer la infraestructura de la red para hacer una identificación y configuración acertada de ellos a través de la selección del tipo de activo que corresponda para cada nodo.

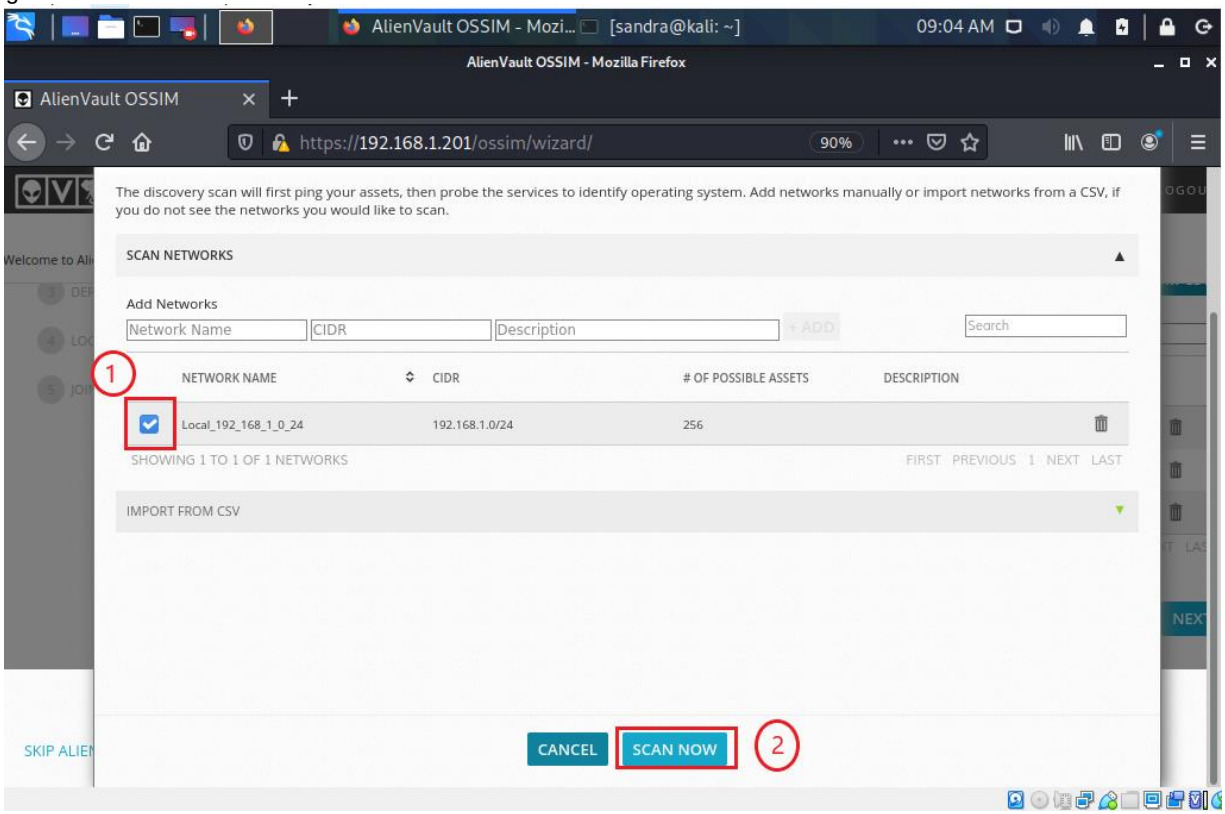
Figura 21. Nodos identificados de la red por Alienvault.



Fuente: elaboración propia

Dentro de la lista que se despliega, se deben identificar los nodos de la red y en caso de no estar presentes todos, es posible realizar un escaneo presionando el botón scan que se encuentra resaltado o adicionarlos manualmente. El proceso de escaneo se inicia activando el botón “scan”, se debe seleccionar la red a escanear y luego el botón “scan now”, siguiendo la secuencia indicada en la Figura 22, esto muestra una barra de progreso que indica el porcentaje de avance.

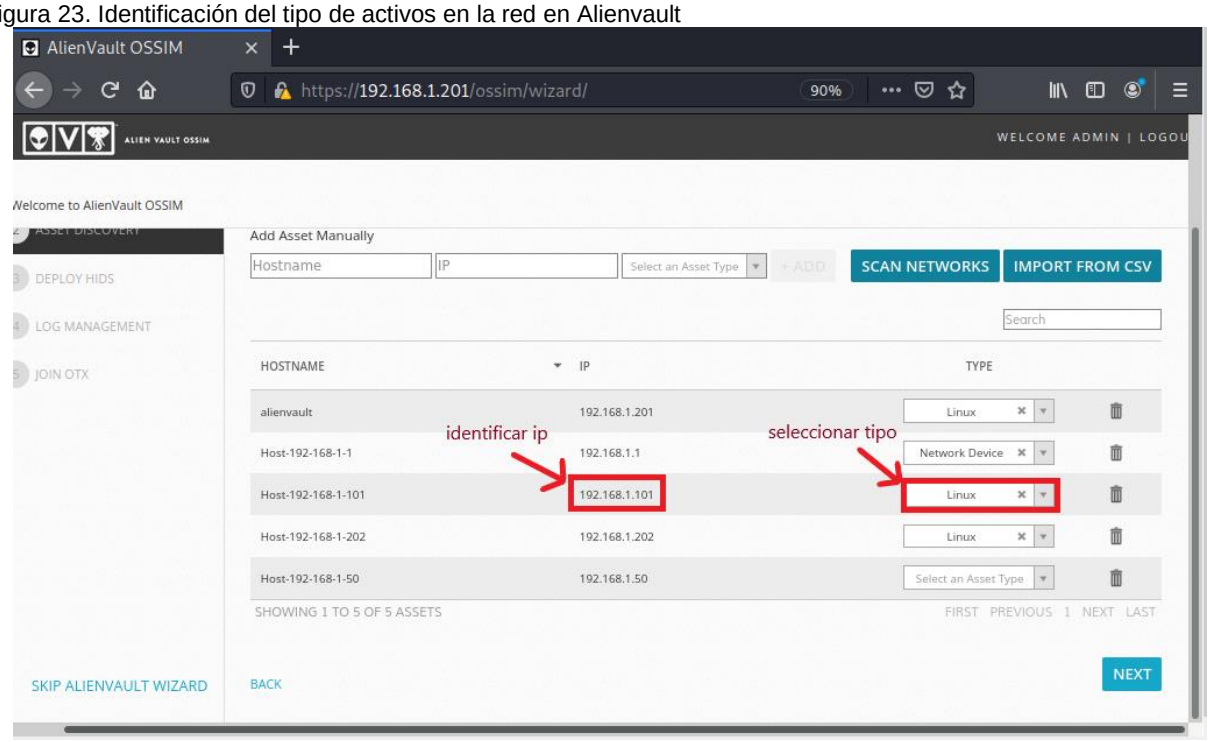
Figura 22. Pantalla de escaneo de la red en Alienvault



Fuente: elaboración propia

Al finalizar el proceso anterior se muestra un listado con los dispositivos activos en la red, aquí se debe identificar la ip del activo y seleccionar el tipo de activo correspondiente como se muestra en la siguiente figura:

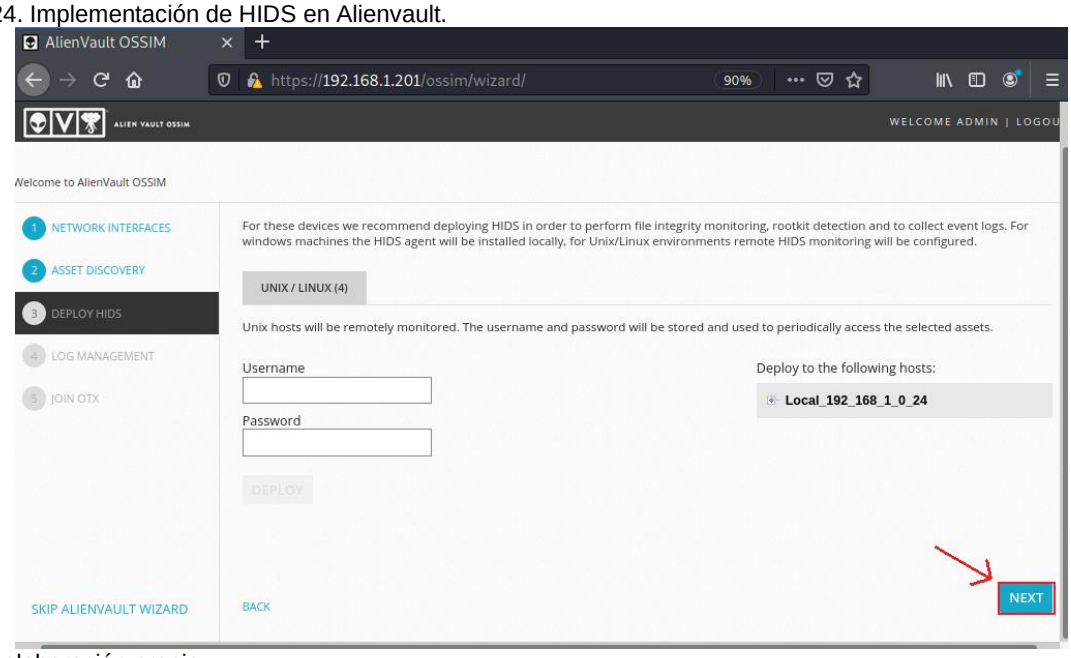
Figura 23. Identificación del tipo de activos en la red en Alienvault



Fuente: elaboración propia

Posteriormente se presiona el botón “next” y el siguiente paso consiste en la implementación de los HIDS o agentes para la detección de amenazas, verificación de integridad de archivos, monitoreo y recopilación de logs de eventos, para lo cual se requiere indicar el nombre de usuario y contraseña del activo para que se realice el despliegue de los agentes en los sistemas Linux y Windows. Se puede omitir este paso y hacer posteriormente la instalación manual de los agentes presionando en el botón “next” como se observa en la Figura 24, dado que para éste laboratorio controlado se requiere una instalación personalizada de los agentes.

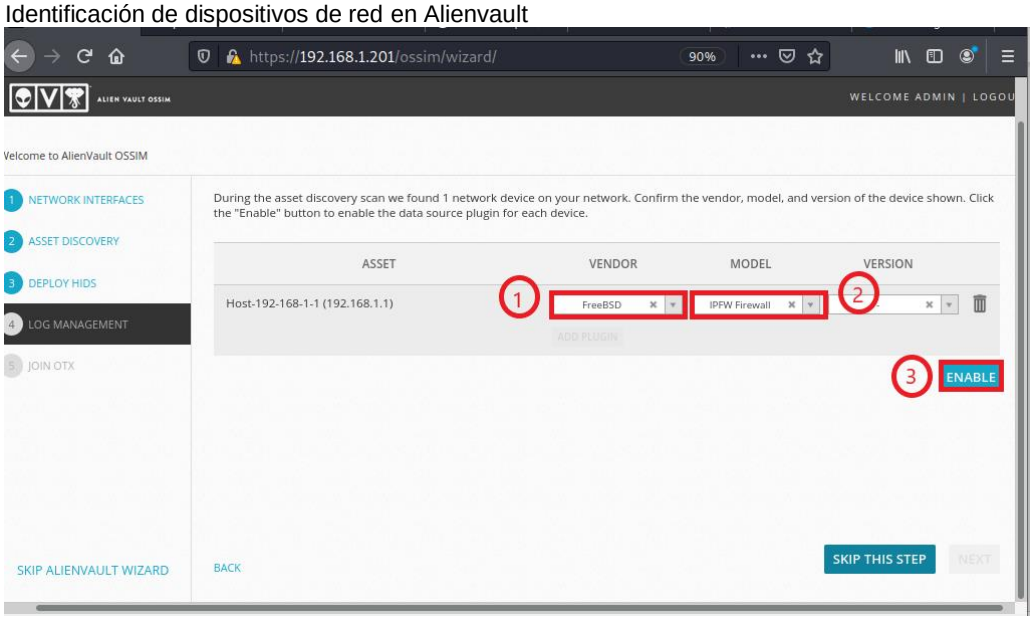
Figura 24. Implementación de HIDS en Alienvault.



Fuente: elaboración propia

En la siguiente pantalla OSSIM identifica los dispositivos de red para los cuales se debe seleccionar el plugin adecuado para que la aplicación pueda entender los logs que allí se recolectan. En este caso, se tiene un firewall pfsense, el cual esta basado en FreeBSD, se seleccionan las opciones como se observan en la secuencia mostrada en la Figura 25 y se presiona el botón “enabled” para que se ejecute el proceso.

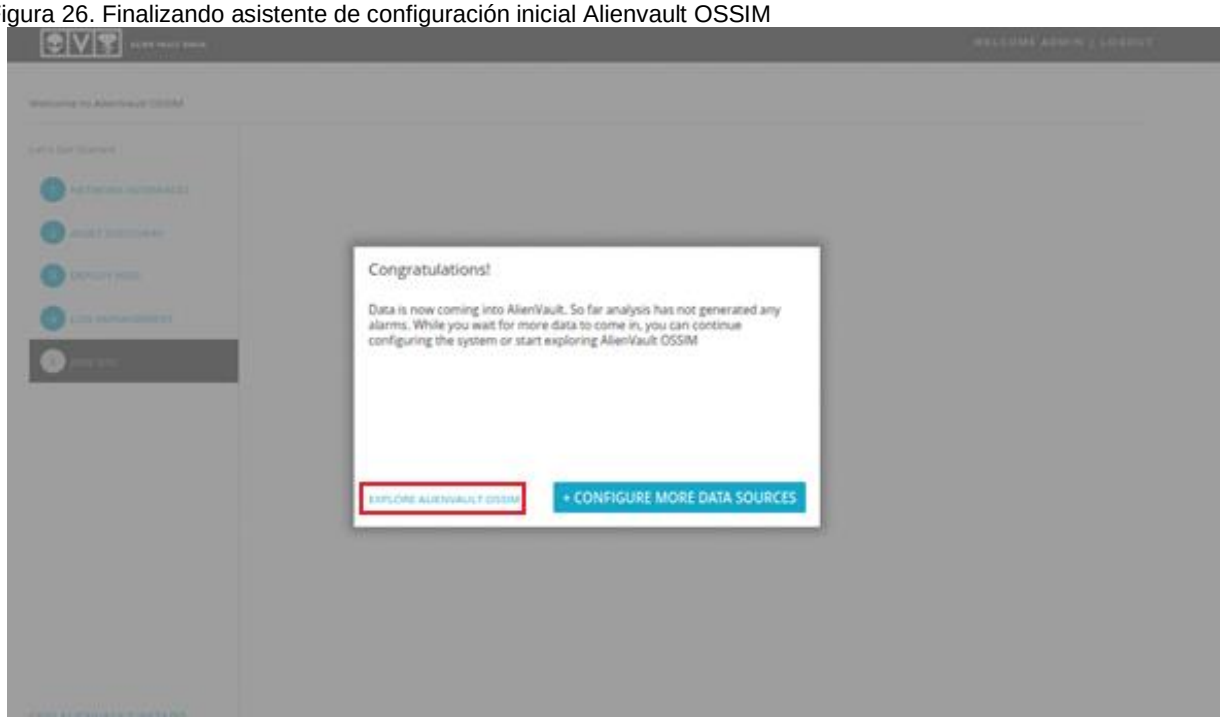
Figura 25. Identificación de dispositivos de red en Alienvault



Fuente: elaboración propia

Como parte final en la configuración previa de Alienvault, el asistente pregunta si desea registra la cuenta de la comunidad en el despliegue realizado, se procede a omitir este paso y posteriormente en la ventana que aparece se presiona en el botón “explore alienvault OSSIM” como se observa en la siguiente Figura.

Figura 26. Finalizando asistente de configuración inicial Alienvault OSSIM



3Fuente: elaboración propia

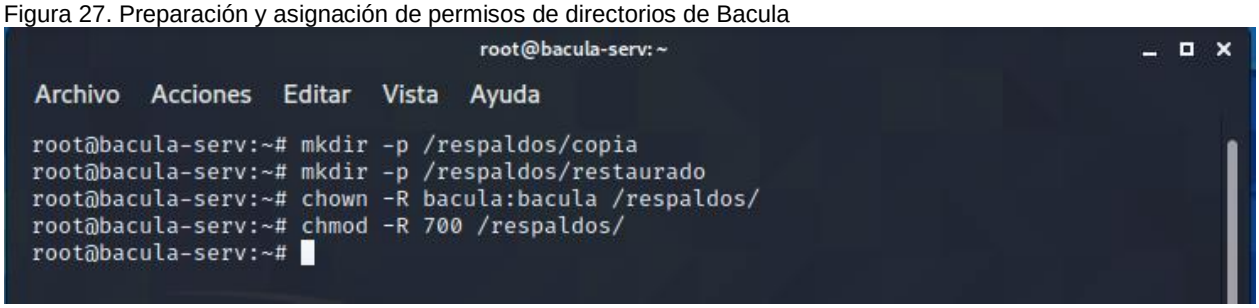
4.4.2.5 Servidor de copias de seguridad Bacula. Para este servidor se emplea la aplicación Bacula, es un software integrado por varias herramientas que permiten gestionar las copias de seguridad, respaldo y restauración de datos en red, utiliza el modelo cliente/servidor. Posee un diseño modular que facilita la escalabilidad de la herramienta en grandes redes de computadores, se compone principalmente de cinco módulos: Bacula Director, Bacula Console, Bacula File, Bacula Storage, Bacula Monitor, cada uno de ellos cumple su propia función, para lo cual requiere una configuración adecuada. El proceso de instalación de éste servidor, se puede detallar en el anexo A.4, se define previamente la función de cada uno de sus módulos para comprender mejor su configuración:

- Bacula Director: supervisa todas las operaciones copia, restauración y comprobación
- Bacula Console: permite al administrador configurar e interactuar con Bacula Director.
- Bacula File: es la aplicación instalada en la maquina cliente, que a través del File

Daemon (FD) entrega al Director los atributos y datos del archivo
- Bacula Storage: a través del Storage Daemon (SD) realiza la labor de almacenamiento y recuperación de datos en los medios que se han designado para tal fin (discos, cintas, etc.).
- Bacula Monitor: Permite supervisar el estado de todos los componentes del sistema

Configuración módulos de Bacula. Al finalizar el asistente de instalación de la herramienta (ver Anexo A.4.1), se procede a preparar el directorio en donde se almacenarán las copias de seguridad y un directorio para la restauración de archivos, posteriormente se establece la propiedad del directorio para el usuario Bacula y los permisos respectivos, como se observa en la siguiente Figura.

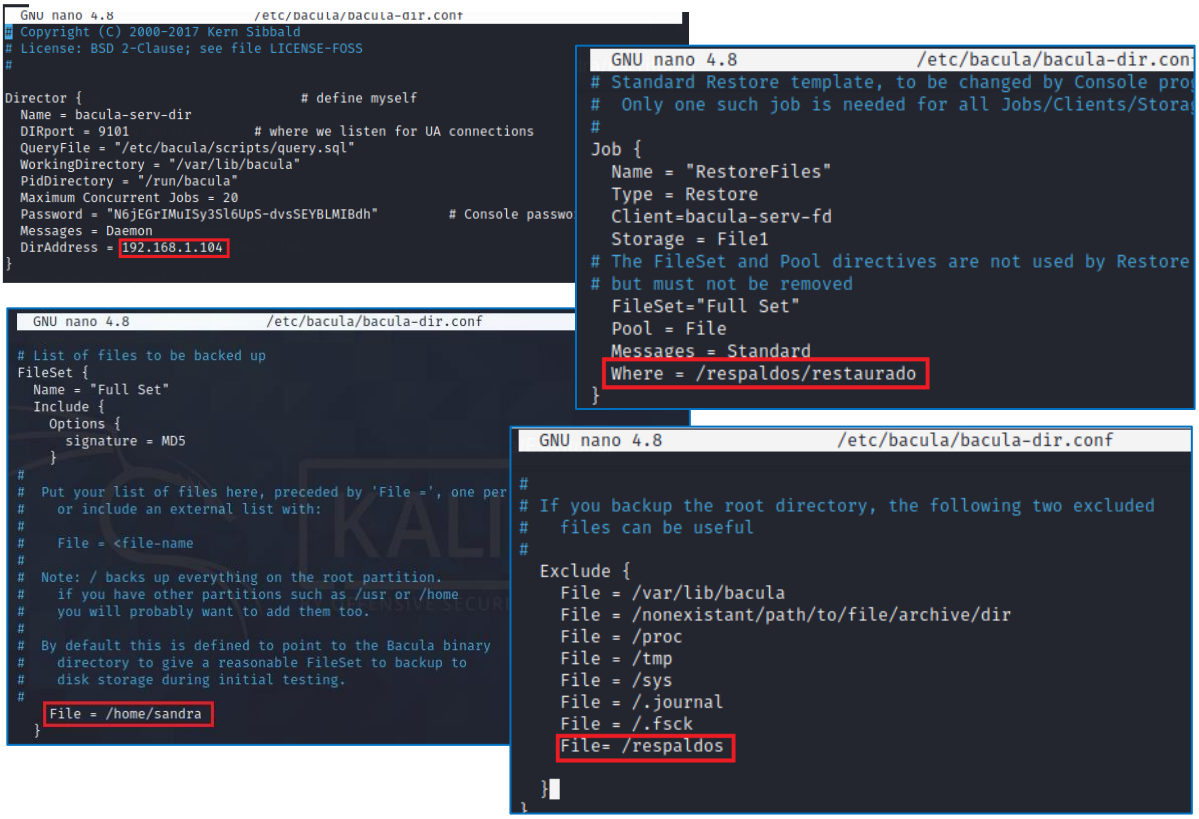
Figura 27. Preparación y asignación de permisos de directorios de Bacula



Fuente: elaboración propia

Se procede configurar el servicio Bacula Director, indicando los directorios recién creados, para la restauración de archivos así como determinar los directorios que se respaldaran y los que se excluyen. Se debe modificar el archivo de configuración bacula-dir.conf, en los parámetros denominado “director”, “job”, “File” y “Exclude”, como se observa en la Figura a continuación:

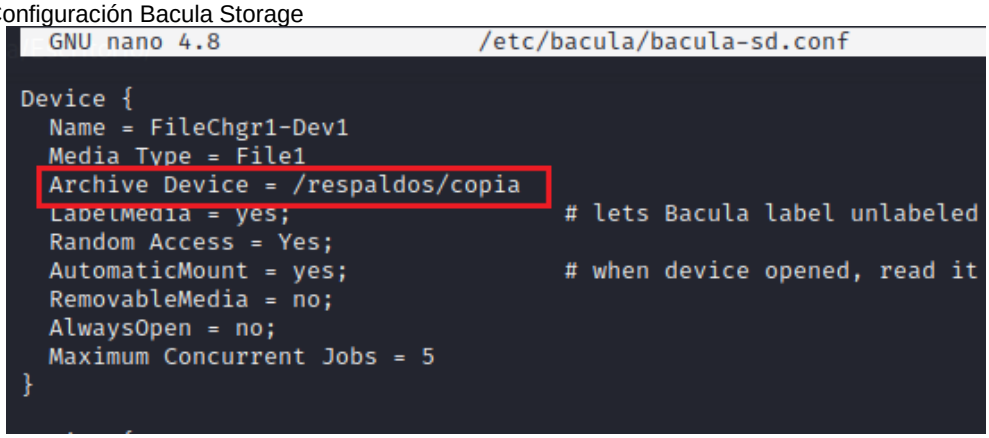
Figura 28. Configuración Bacula Director



Fuente: elaboración propia

Para el caso del módulo Bacula Storage, se establece la ruta en donde se guardarán las copias, para ello se modifica el archivo de configuración bacula-sd.conf en el parámetro denominado “device”, como se observa en la Figura a continuación:

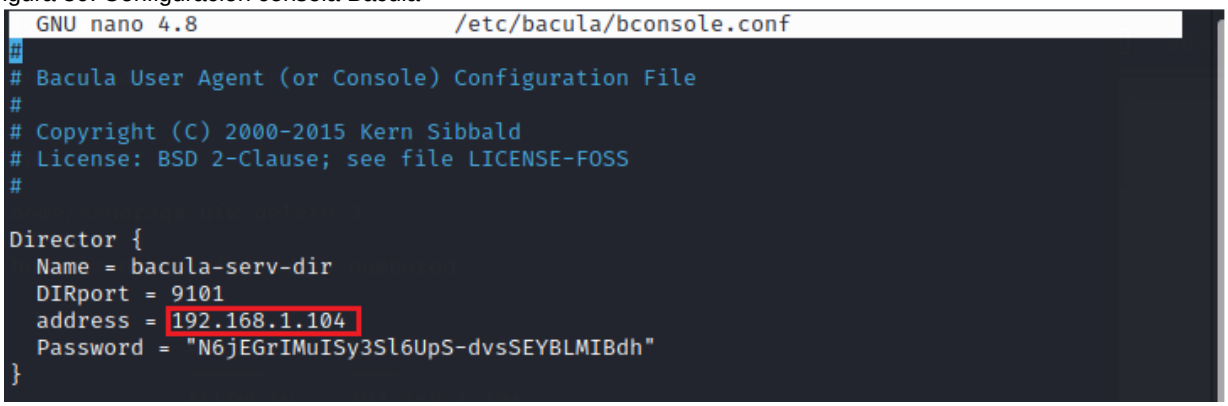
Figura 29. Configuración Bacula Storage



Fuente: elaboración propia

El módulo de configuración Bacula Console, se configura indicando la dirección ip asignada al servidor bacula en el archivo de configuración bconsole.conf, como se evidencia en la siguiente Figura.

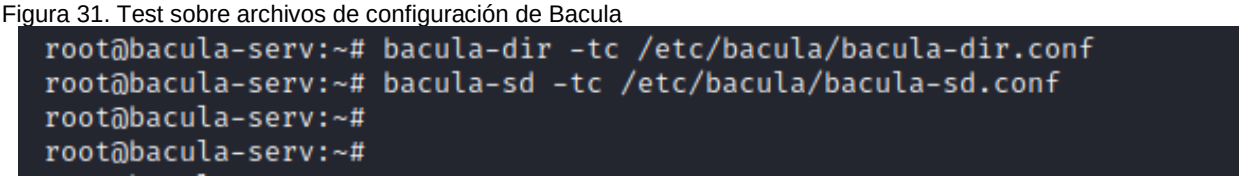
Figura 30. Configuración consola Bacula



Fuente: elaboración propia

Para comprobar la configuración establecida se realiza un test al archivo de configuración como se observa en busca de errores utilizando la instrucción que se observa en la siguiente Figura.

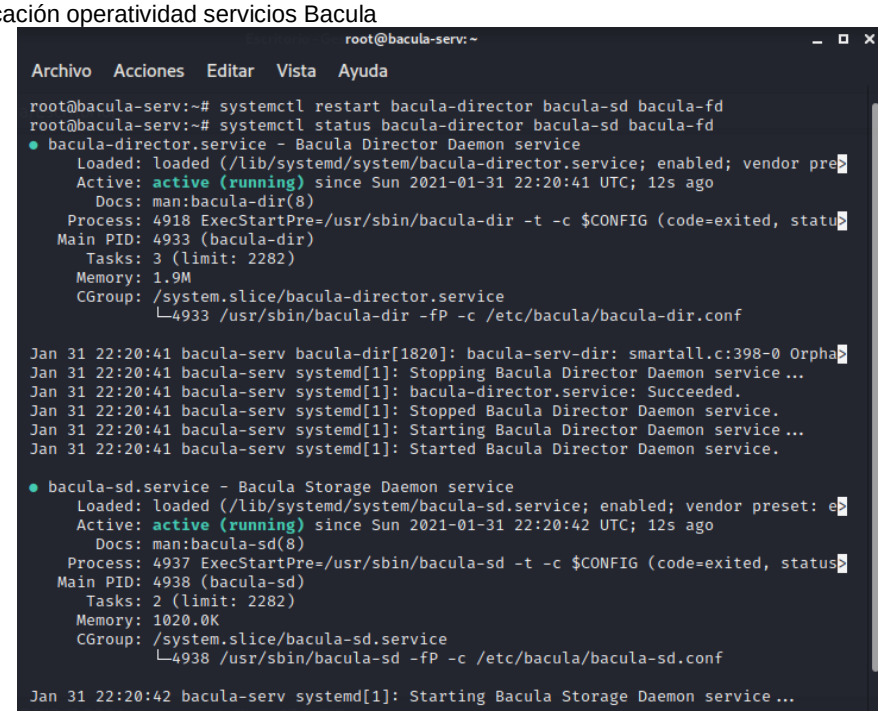
Figura 31. Test sobre archivos de configuración de Bacula



Fuente: elaboración propia

Se reinician los servicios con el comando systemctl y se verifica la operatividad como se muestra a continuación

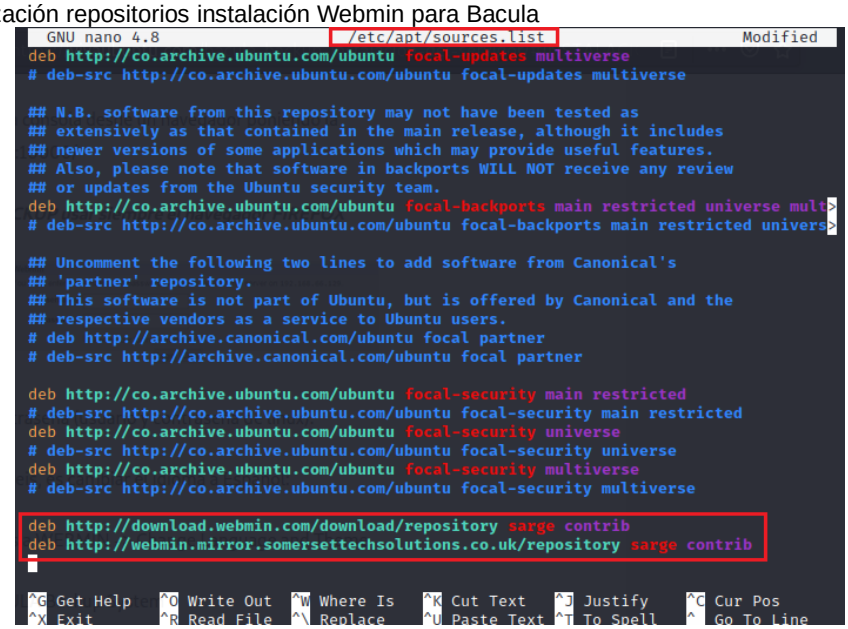
Figura 32. Verificación operatividad servicios Bacula



Fuente: elaboración propia

Instalación de la herramienta de administración Web para Bacula. Se instala la herramienta de administración, Webmin. Para ello se edita la lista de origen de apt con la url de descarga como se observa en la Figura 33.

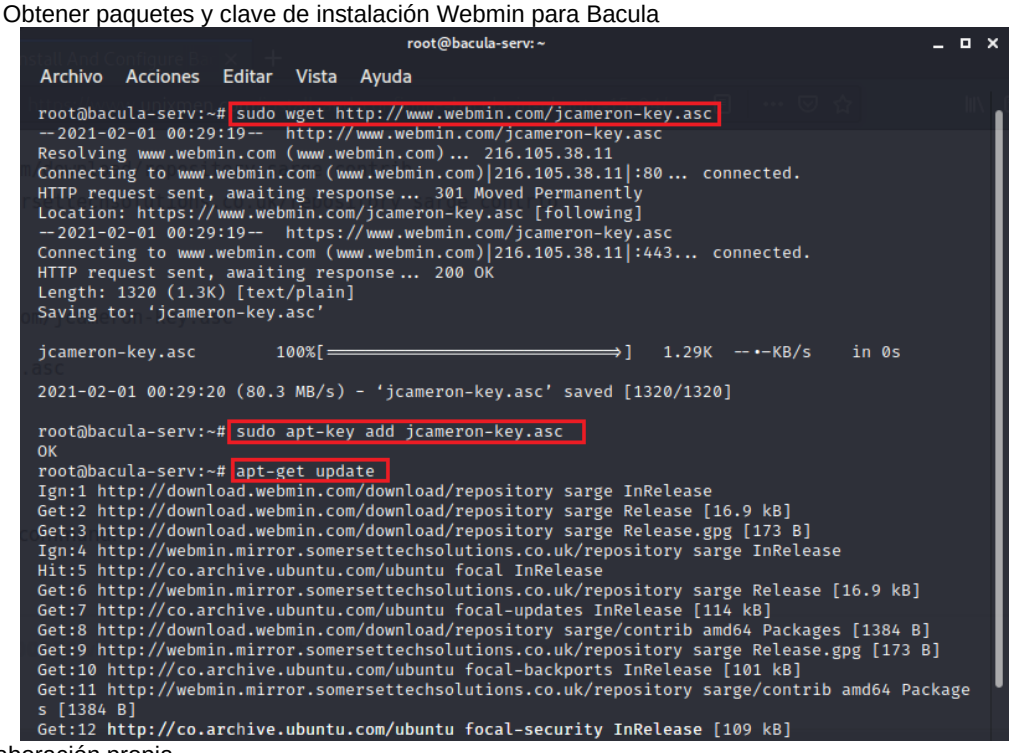
Figura 33. Actualización repositorios instalación Webmin para Bacula



Fuente: elaboración propia

Se guardan los cambios del archivo y se ejecutan los comandos para agregar la GPG key, ejecutando las siguientes instrucciones que se resaltan en la Figura 34, y posteriormente se realiza la actualización.

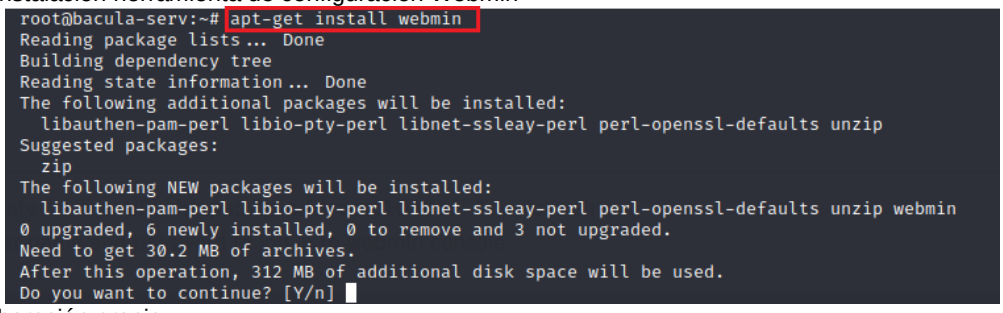
Figura 34. Obtener paquetes y clave de instalación Webmin para Bacula



Fuente: elaboración propia

Se procede a ejecutar la instrucción de instalación de la aplicación webmin, como se muestra a continuación:

Figura 35. Instalación herramienta de configuración Webmin



Fuente: elaboración propia

Al finalizar, se habilita en el firewall el puerto predeterminado de webmin 10000

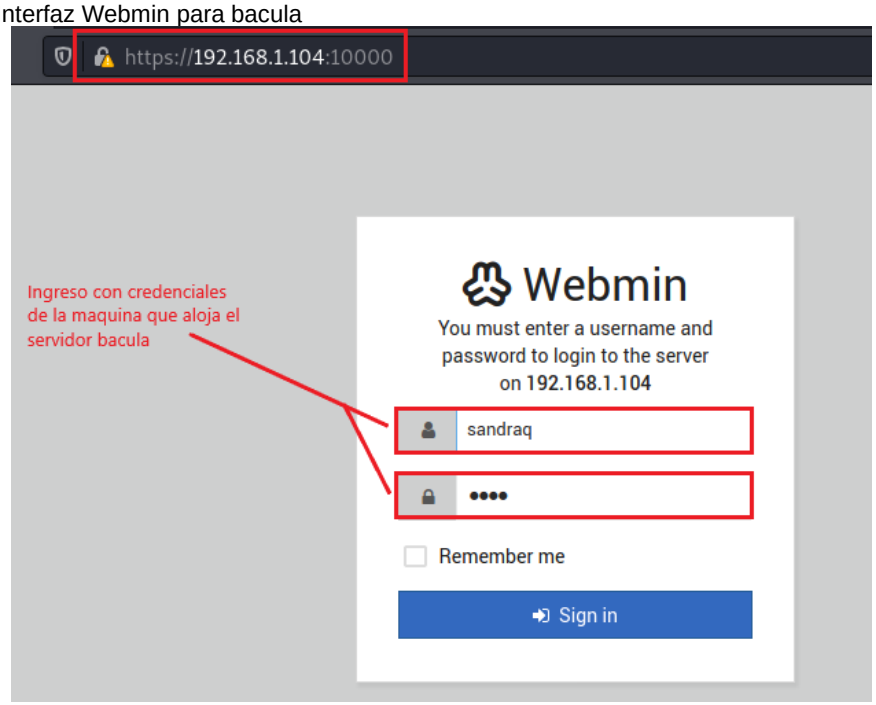
Figura 36. Configuración permisos de firewall puerto Webmin para Bacula

```
root@bacula-serv:~# ufw allow 10000
Rules updated
Rules updated (v6)
root@bacula-serv:~#
```

Fuente: elaboración propia

Iniciar la interfaz web de bacula ingresando en un navegador web la ip del servidor y el puerto predeterminado se muestra la interfaz observada en la siguiente Figura en donde se accede al login con las credenciales de inicio del servidor

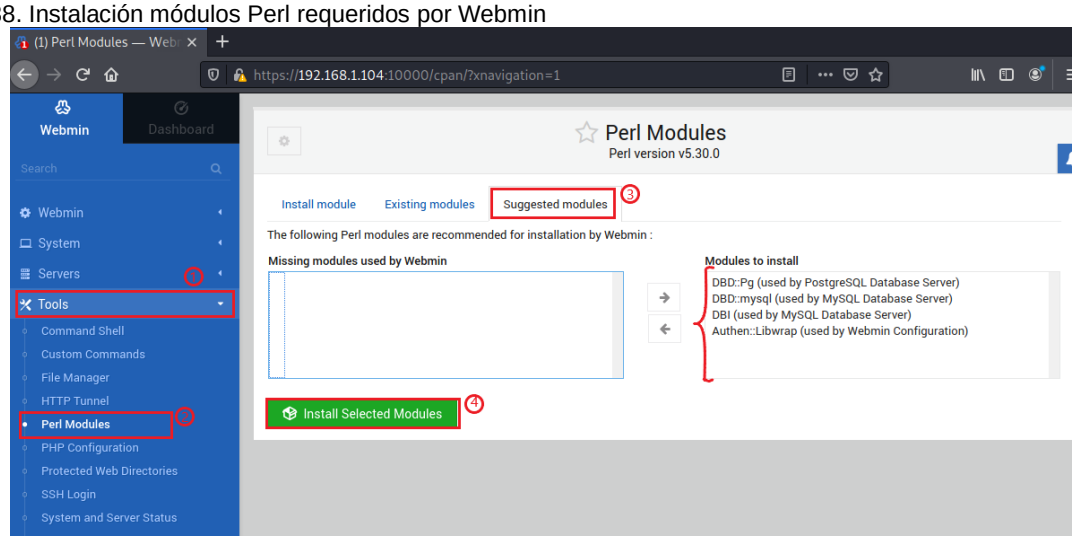
Figura 37. Login Interfaz Webmin para bacula



Fuente: elaboración propia

Finalizada la instalación de la herramienta web de configuración para Bacula, se procede a iniciar sesión en la misma, y como primera acción, se instalan algunos módulos sugeridos por la misma aplicación para un correcto funcionamiento, para lo cual se accede al menú “Tools”, en la opción “PerlModules” dentro de la pestaña “Suggested Modules”, como se observa en la Figura siguiente.

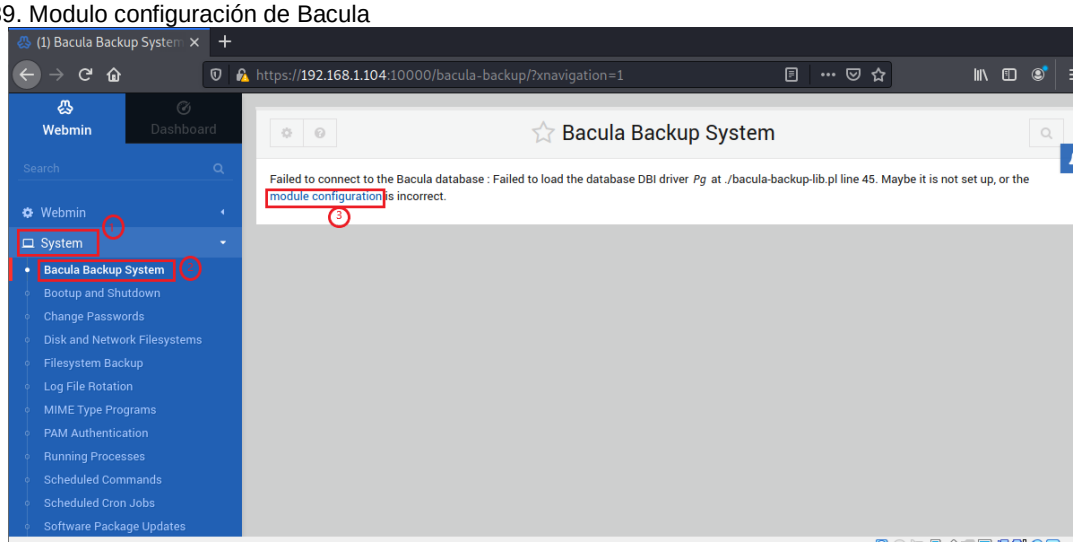
Figura 38. Instalación módulos Perl requeridos por Webmin



Fuente: elaboración propia

Una vez iniciada la sesión se debe dirigir al menú “System”, en la opción “Bacula Backup System” y presionar el link “module configuration”

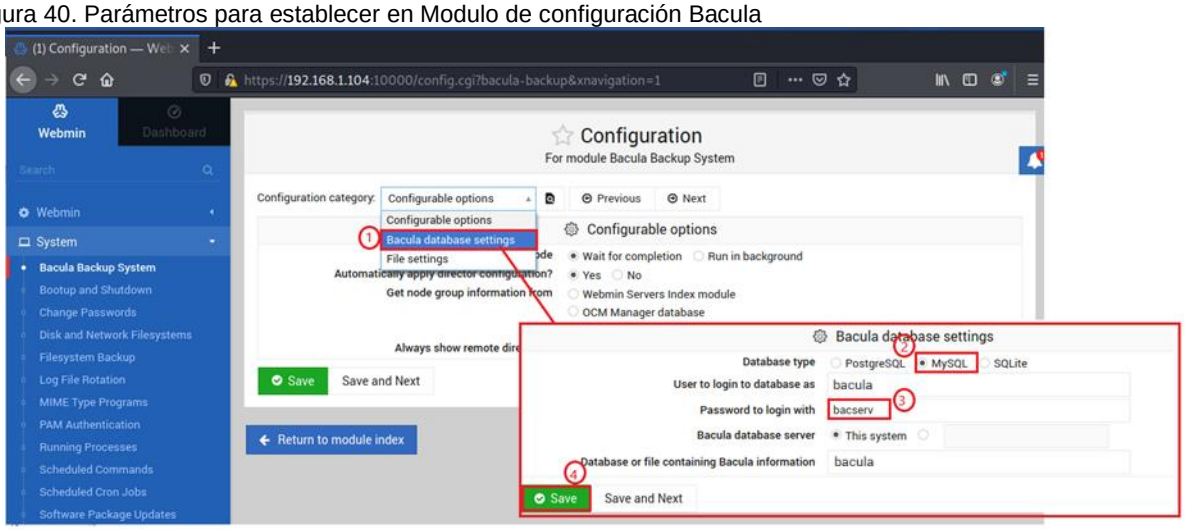
Figura 39. Modulo configuración de Bacula



Fuente: elaboración propia

Dentro del módulo de configuración seleccionar la opción “Bacula database setting”, establecer la base de datos mysql, digitar la contraseña y presionar en guardar, siguiendo la secuencia que se muestra en la Figura 40.

Figura 40. Parámetros para establecer en Modulo de configuración Bacula

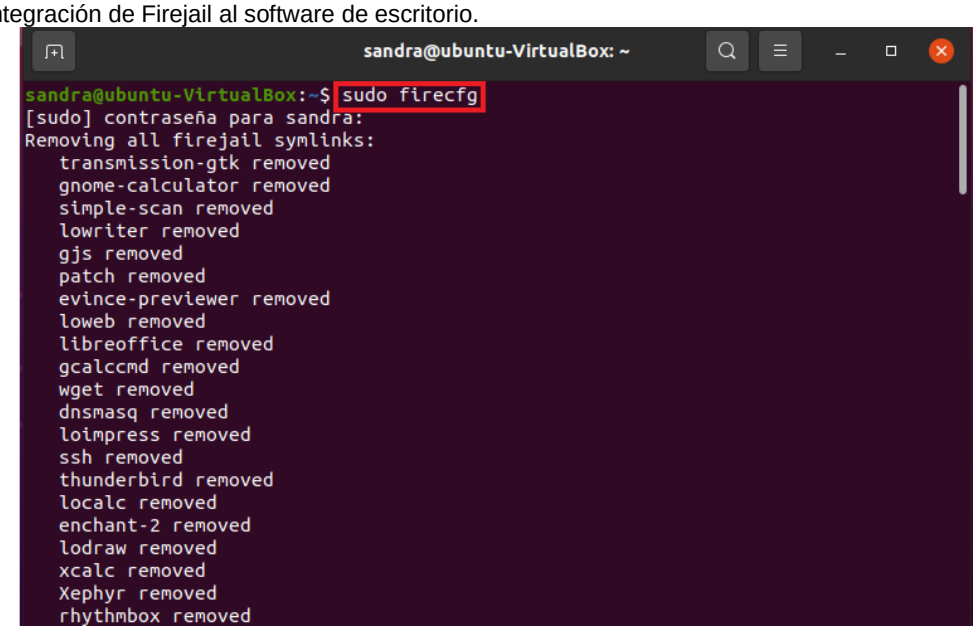


Fuente: elaboración propia

4.4.2.6 Servidor Sandbox Este servidor se implementa a través de la herramienta Firejail, en una máquina virtual completamente independiente de los otros servidores. Entre las principales ventajas de Firejail se tiene que es eficiente aislando procesos y liviana debido a que aprovecha los módulos de seguridad del kernel del Linux Apparmor y el uso de espacios de nombre de Linux para ejecutarlos. Estas características permiten que un determinado proceso tenga una vista privada de los recursos del sistema, lo cual mantiene aislado el entorno de ejecución de las aplicaciones, sin embargo, es importante conocer qué tipo de permisos se van a otorgar a la aplicación al momento de ejecutarse, de modo que quien los gestiona es responsable de su óptimo funcionamiento. Los pasos para la instalación se encuentran en el anexo A.5, a continuación, se observa el proceso de configuración de la herramienta.

Inicialmente, como se observa en la Figura 41, se procede a ejecutar el comando: “sudo firecfg”, esto permite integrar el software de escritorio instalado en la máquina de tal manera que al ejecutarse se convierten en un espacio aislado automáticamente.

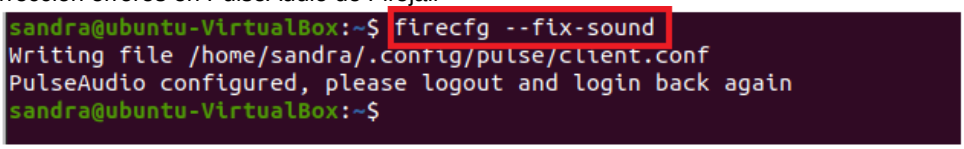
Figura 41. Integración de Firejail al software de escritorio.



Fuente: elaboración propia

Se emplea el comando “firecfg --fix-sound” para corregir ciertos errores existentes en el software PulseAudio, la figura 42 indica que se debe reiniciar la máquina para que surta efecto la corrección.

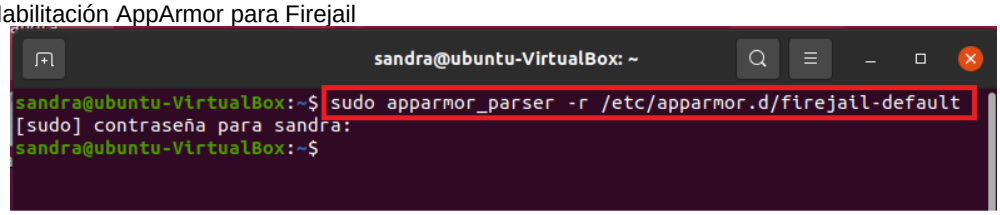
Figura 42. Corrección errores en PulseAudio de Firejail



Fuente: elaboración propia

Seguidamente se requiere habilitar el módulo de seguridad del kernel de Linux “AppArmor”, que permitirá gestionar el sistema restringiendo las capacidades de una aplicación o proceso, para ello se emite en la terminal el comando: “sudo apparmor_parser -r /etc/apparmor.d/firejail-default”

Figura 43.Habilitación AppArmor para Firejail

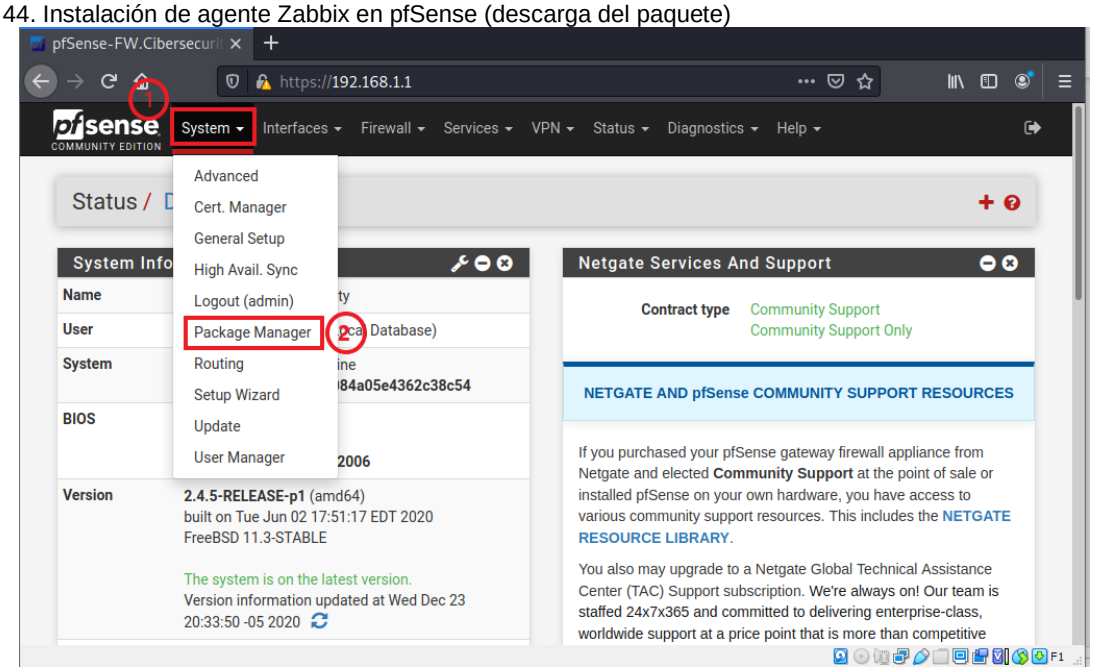


Fuente: elaboración propia

4.4.3 Configuración de Agentes para servidor Zabbix Para que el servidor zabbix pueda realizar las funciones de monitoreo es necesario hacer el despliegue de los agentes en cada uno de los servidores y de ésta forma, se envié la información sobre su estado y alertas. En primer lugar, se debe realizar la instalación del agente en cada servidor y posteriormente habilitarlos en Zabbix.

4.4.3.1 Agente Zabbix en pfSense Se abre la interfaz web del servidor pfsense en la ruta https://192.168.1.1 se procede a introducir las credenciales, para realizar el proceso se debe seleccionar en el menú “System”, la opción “package manager”, y en la ventana desplegada, seleccionar la pestaña Available Packages, tal como se observa en la secuencia indicada en la siguiente Figura.

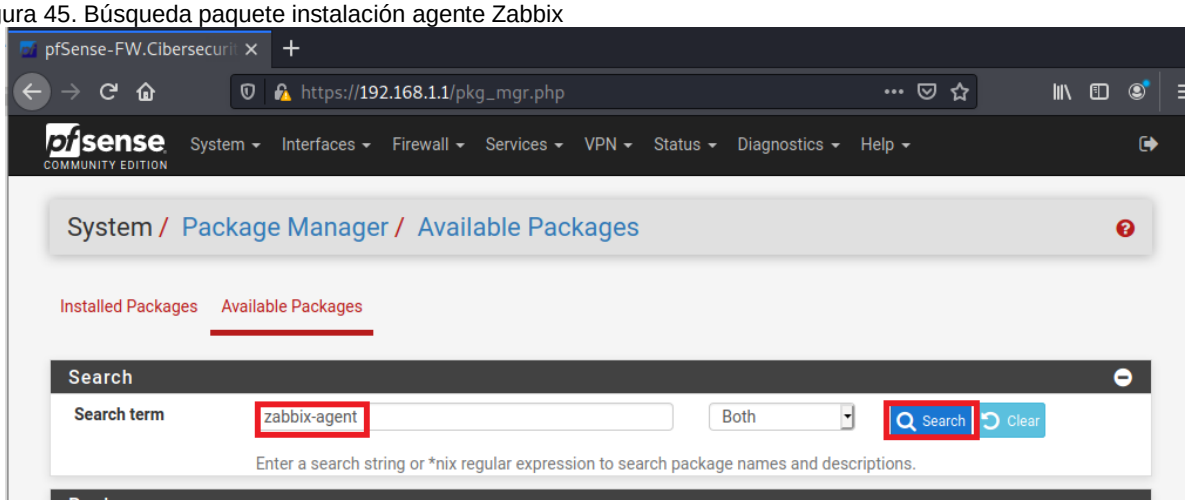
Figura 44. Instalación de agente Zabbix en pfSense (descarga del paquete)



Fuente: elaboración propia

Se muestra una lista con los paquetes que se encuentran disponibles, allí se debe buscar Zabbix version 5.0, el cual corresponde a la version instalada en el servidor, escribiendo dentro del cuadro “search term”, y presionando el botón “Search”, como se observa en la Figura.

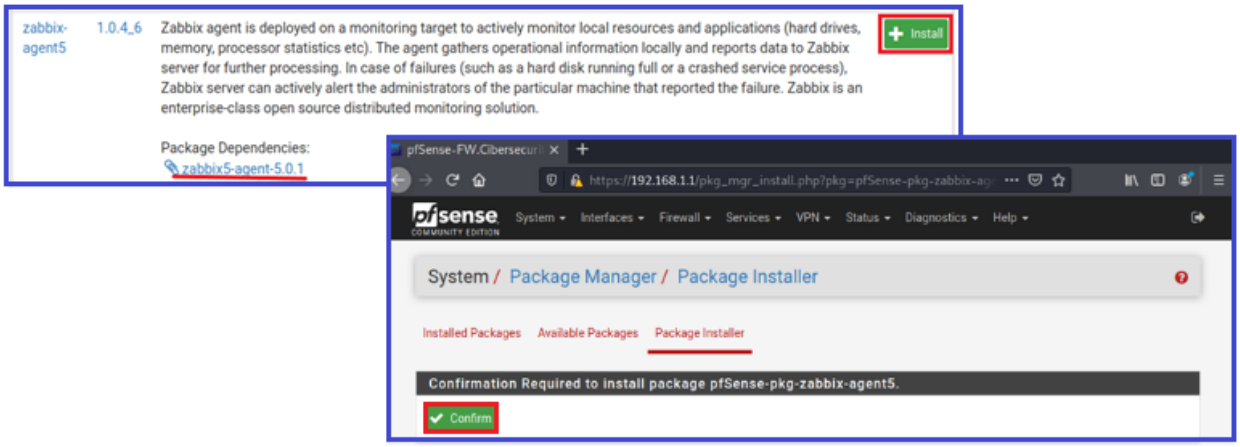
Figura 45. Búsqueda paquete instalación agente Zabbix



Fuente: elaboración propia

Dentro de los resultados se encuentra el paquete requerido tal como se observa en la Figura 46, allí se debe presionar el botón install y en la siguiente pantalla el botón “confirm”, posteriormente se muestra un mensaje de instalación exitosa.

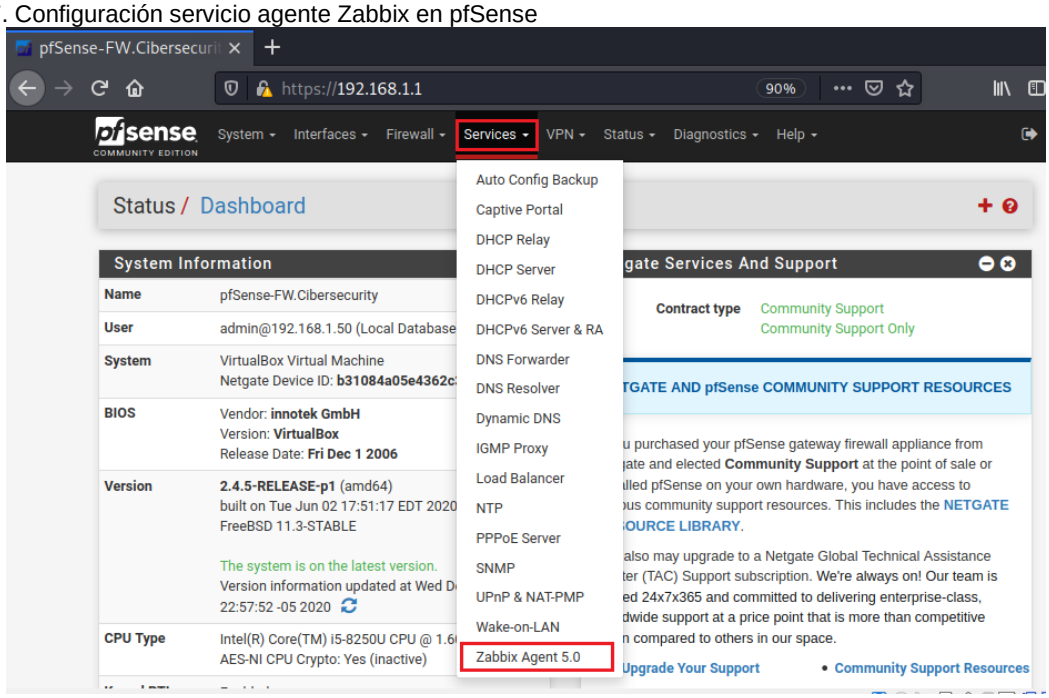
Figura 46. Selección paquete a instalar agente Zabbix en pfSense



Fuente: elaboración propia

Para finalizar la instalación del agente se debe configurar el servicio Zabbix dentro de pfSense, ingresando en el menu Services, luego Zabbix Agent 5.0, como se observa a continuación:

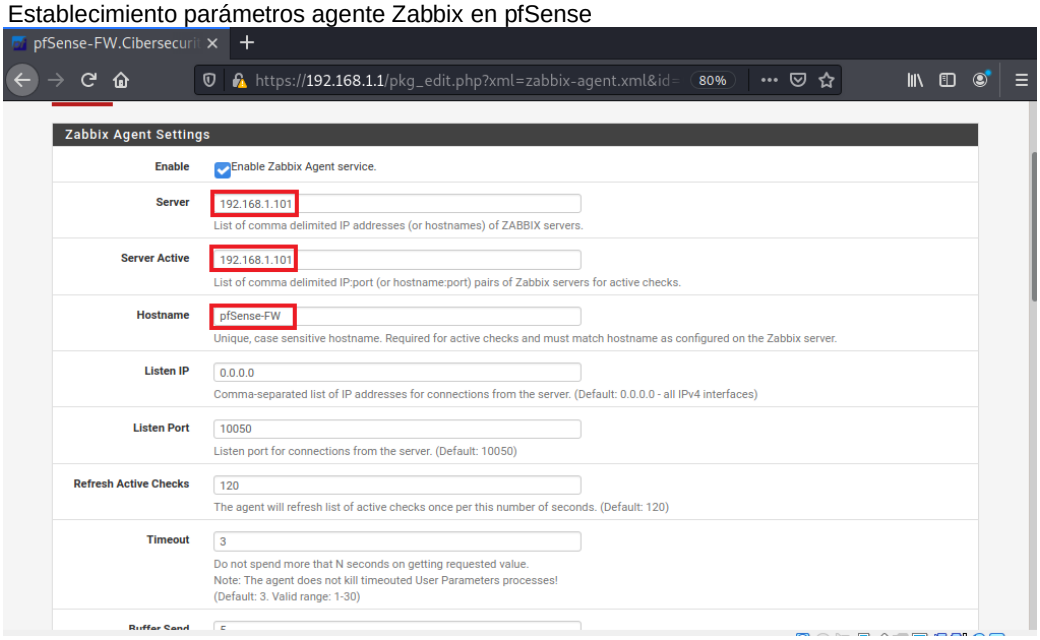
Figura 47. Configuración servicio agente Zabbix en pfSense



Fuente: elaboración propia

En esta nueva pantalla se establecen la dirección ip del servidor zabbix, el nombre de host en donde se ejecutará este agente, la ip 0.0.0.0 en el parámetro “Listen IP” para escuchar todas las ip y el puerto por defecto del agente (ver Figura 48).

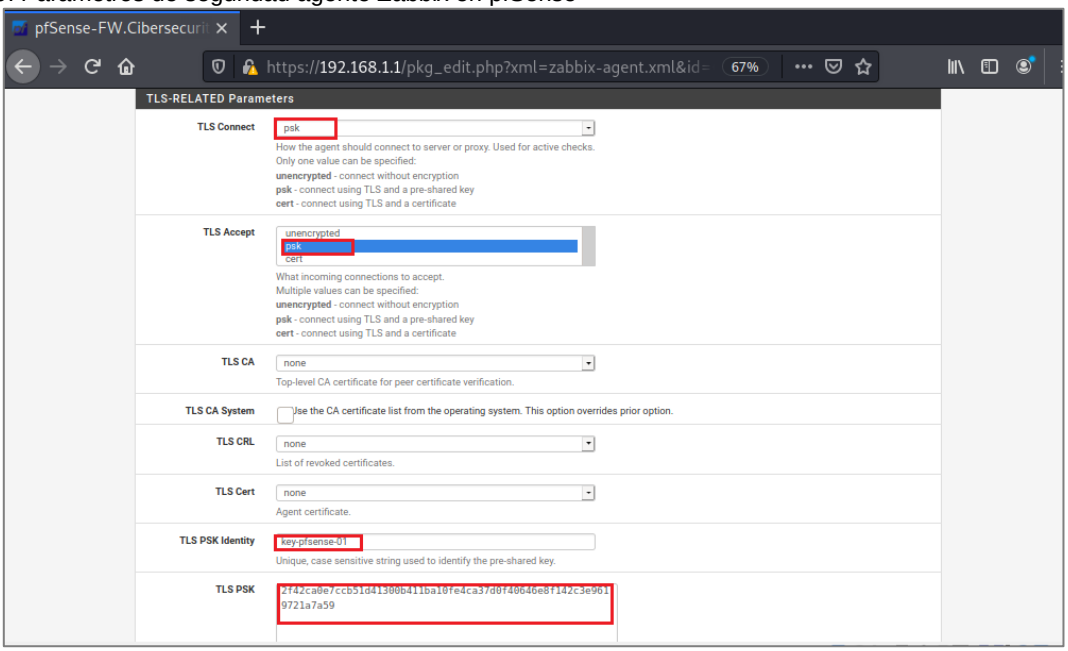
Figura 48. Establecimiento parámetros agente Zabbix en pfSense



Fuente: elaboración propia

Se establecen los parámetros de seguridad para la comunicación entre el agente y el servidor, en este caso se utiliza el protocolo TLS con una clave precompartida PSK, Se genera la PSK, para el caso se empleará: 2f42ca0e7ccb51d41300b411ba10fe4ca37d0f40646e8f142c3e9619721a7a59, posteriormente se seleccionan los parámetros como se muestra en la Figura a continuación, estableciendo una identificación para la clave PSK, por último, se presiona el botón “save” para guardar la configuración.

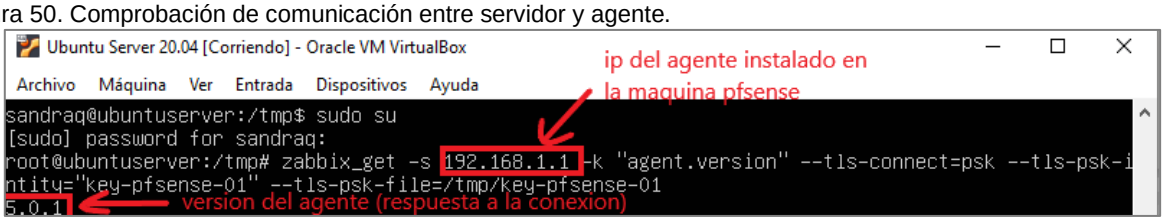
Figura 49. Parámetros de seguridad agente Zabbix en pfSense



Fuente: elaboración propia

Para probar la comunicación exitosa entre el agente y servidor, se ingresa al servidor zabbix, se crea un archivo temporal con el nombre “key-pfsense-01”, que contenga la clave TLS PSK generada, y se utiliza el comando siguiente: zabbix_get -s ip_agente -k "agent.version" --tls-connect=psk --tls-psk-identity="key-pfsense-01" --tls-psk-file=/tmp/key-pfsense-01, como se observa en la siguiente Figura, como resultado de una conexión exitosa en la siguiente línea se puede observar la version del agente instalado

Figura 50. Comprobación de comunicación entre servidor y agente.



Fuente: elaboración propia

Una vez se tiene instalado el agente en la maquina pfsense, se procede a agregarlo en

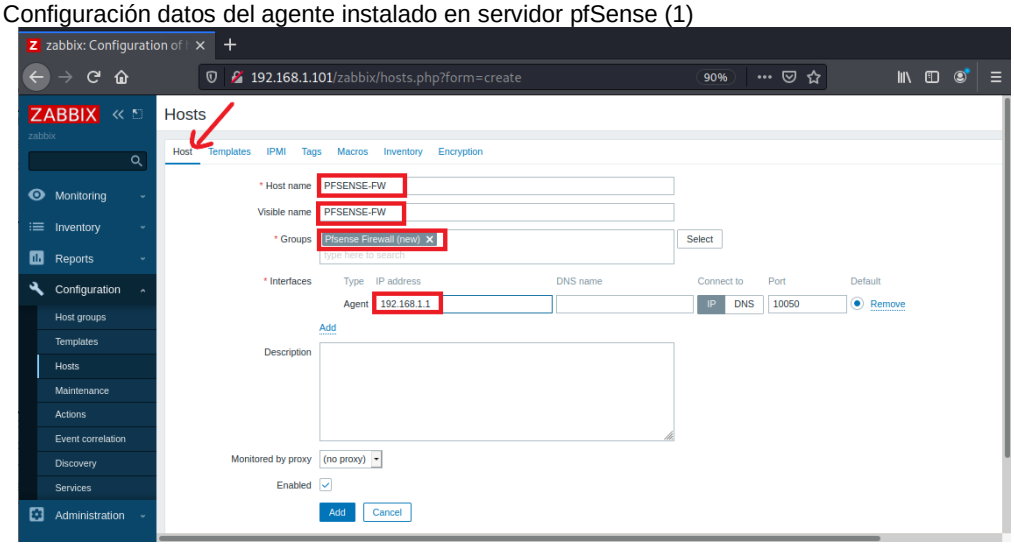
la consola de administración de zabbix, para ello se debe ingresar desde un navegador (1), en el menú “configuración” (2) seleccionar la opción “Hosts” (3) y por ultimo presionar el botón “create host”(4), como se observa en la siguiente Figura.

Figura 51. Agregar agente Zabbix de servidor pfSense.

Fuente: elaboración propia

En la pantalla que aparece se debe diligenciar los campos, asignando un nombre al host, se establece un nombre para identificar un grupo de equipos similares, colocar la ip del agente en el servidor pfsense a monitorear, tal como se muestra en la Figura 52.

Figura 52. Configuración datos del agente instalado en servidor pfSense (1)

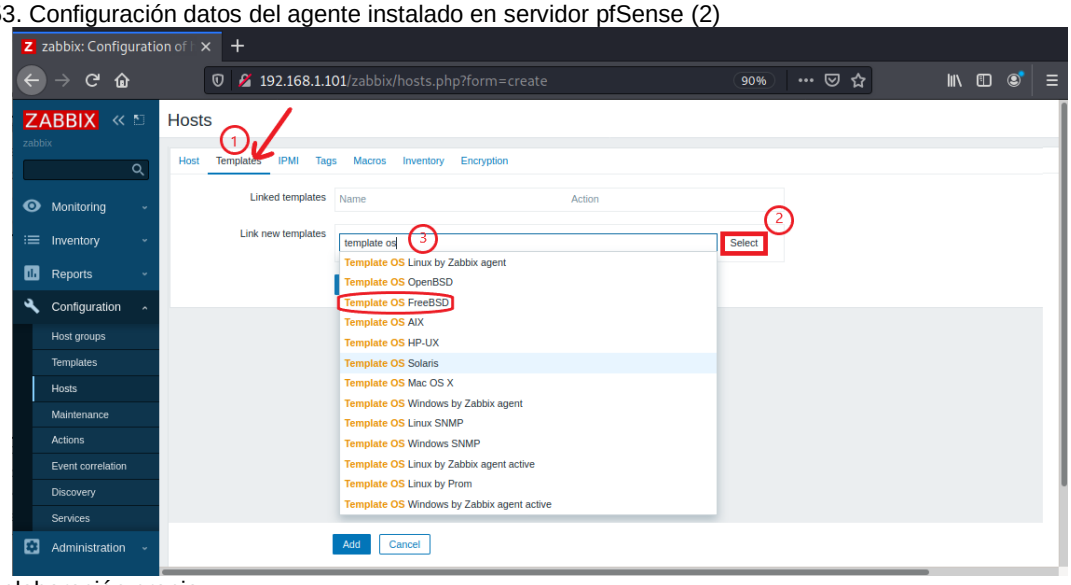


Fuente: elaboración propia

En la siguiente pestaña denominada “Templates”, presionar en el botón “select”, escribir

en el recuadro para la búsqueda de la plantilla FreeBSD, seleccionar de la lista que se despliega, como se muestra en la Figura.

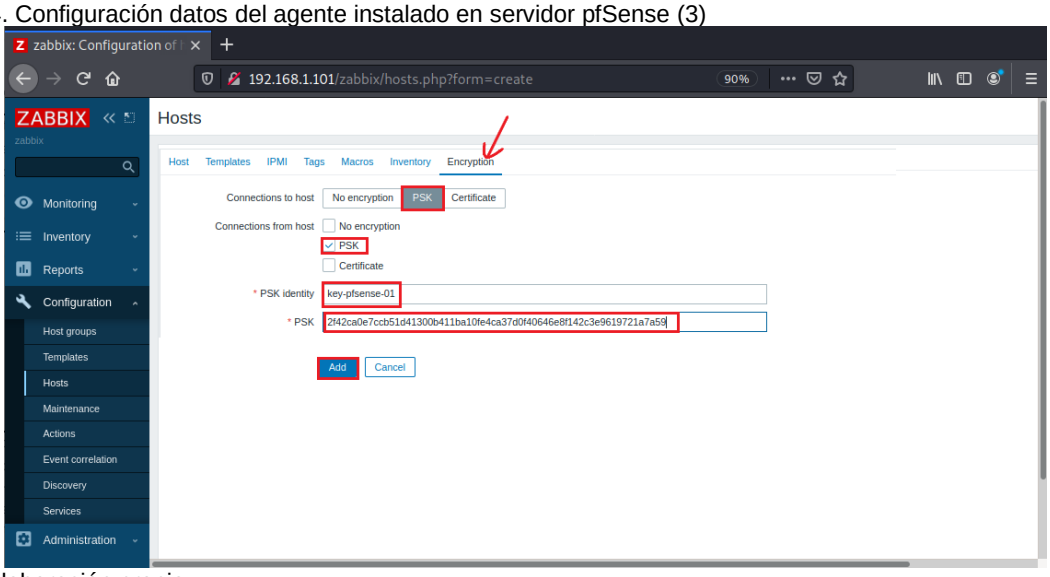
Figura 53. Configuración datos del agente instalado en servidor pfSense (2)



Fuente: elaboración propia

Posteriormente se procede a seleccionar las opciones de cifrado de la comunicación presionando en la pestaña “Encryption”, se establecen las opciones presentadas en la Figura 54 y por último presionar el botón “Add”.

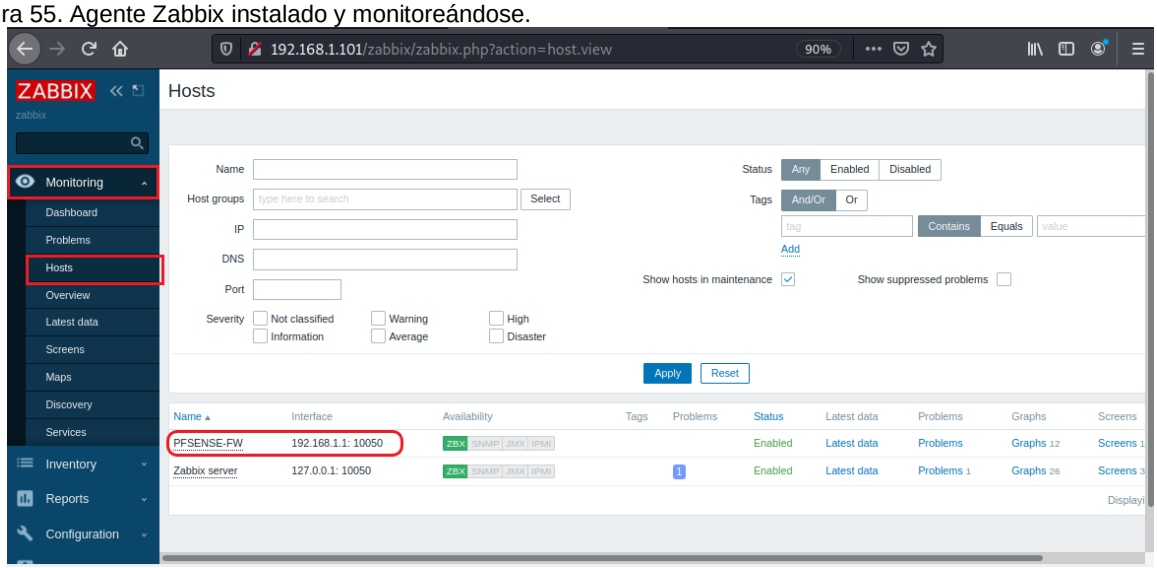
Figura 54. Configuración datos del agente instalado en servidor pfSense (3)



Fuente: elaboración propia

Se revisa en el menú de monitoreo en la opción host, se puede observar en el listado el nuevo servidor que se está monitoreando como se evidencia a continuación.

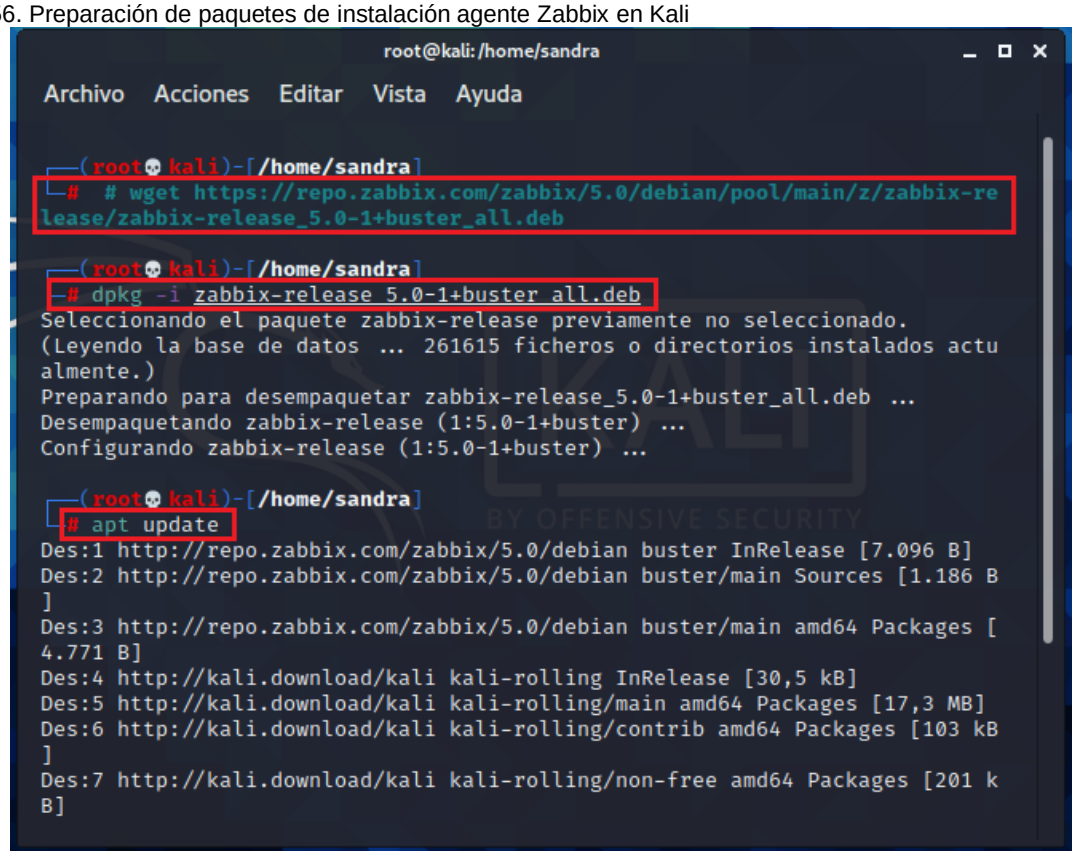
Figura 55. Agente Zabbix instalado y monitoreándose.



Fuente: elaboración propia.

4.4.3.2 Agente Zabbix en Cliente Kali. Se inicia descargando el repositorio oficial de Zabbix, teniendo en cuenta la version del software instalada en el servidor y el sistema operativo de la maquina en donde será instalado el agente, que para este caso es la 5.0. Una vez se obtienen dichos repositorios se procede a la instalación de los paquetes y actualización tal como se observa en la secuencia resaltada en la Figura 56.

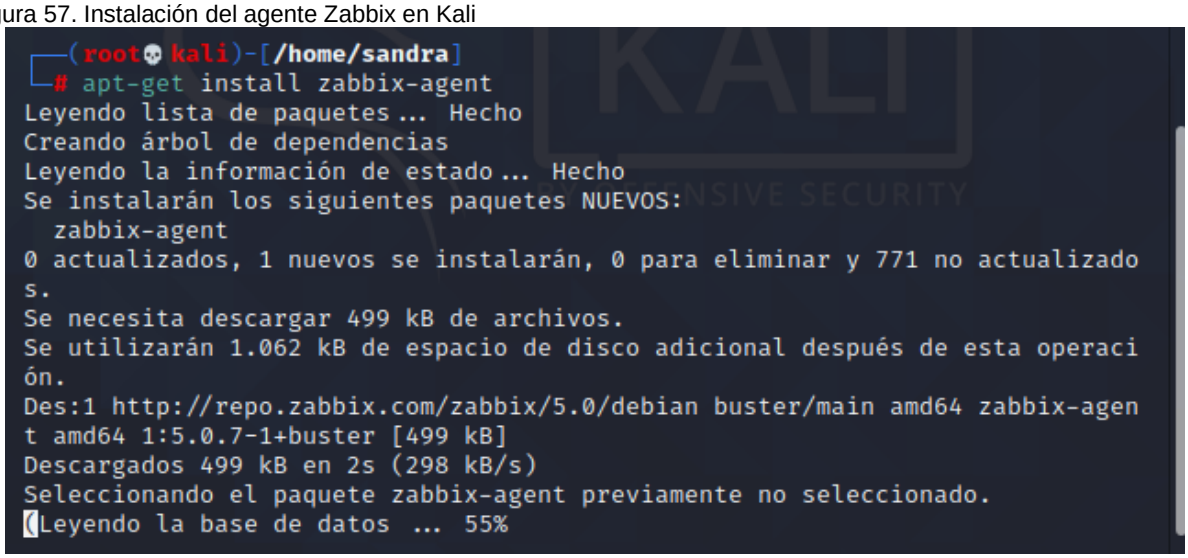
Figura 56. Preparación de paquetes de instalación agente Zabbix en Kali



Fuente: elaboración propia.

Posteriormente, se procede a la instalación propiamente del agente Zabbix, mediante la instrucción observada en la siguiente Figura:

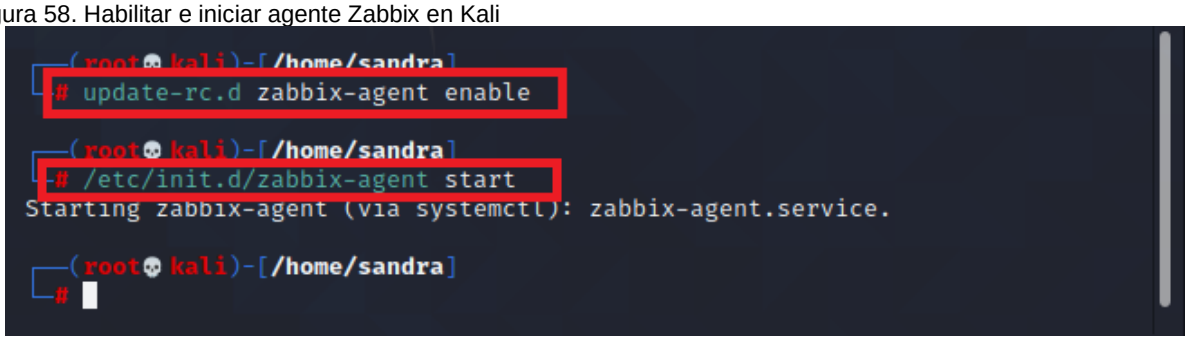
Figura 57. Instalación del agente Zabbix en Kali



Fuente: elaboración propia.

Se habilita el agente y se inicia como se muestra en la Figura 58:

Figura 58. Habilitar e iniciar agente Zabbix en Kali



Fuente: elaboración propia.

Una vez instalado el agente se realiza la configuración de este editando el archivo /etc/zabbix/zabbix_agentd.conf, estableciendo los parámetros Server y Hostname para que coincida con la dirección ip y nombre del servidor Zabbix, como se observa en la Figura.

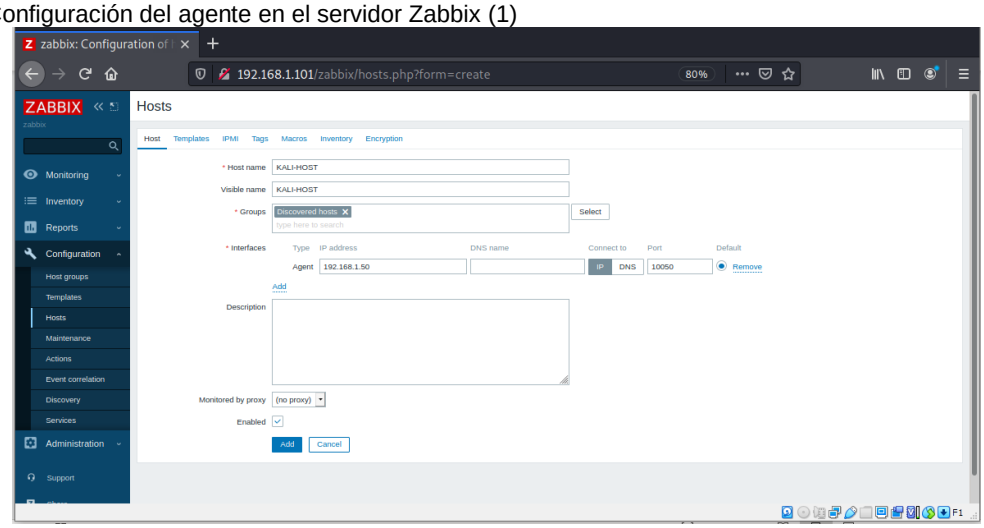
Figura 59. Parámetros archivo de configuración del agente Zabbix

Fuente: elaboración propia.

Desde la interfaz gráfica del servidor Zabbix, se realiza la configuración del agente, para lo cual se accede al menú configuración en la pestaña host, y se procede a indicar los

valores: nombre de host, ip de la interfaz del agente como se observa en la siguiente Figura.

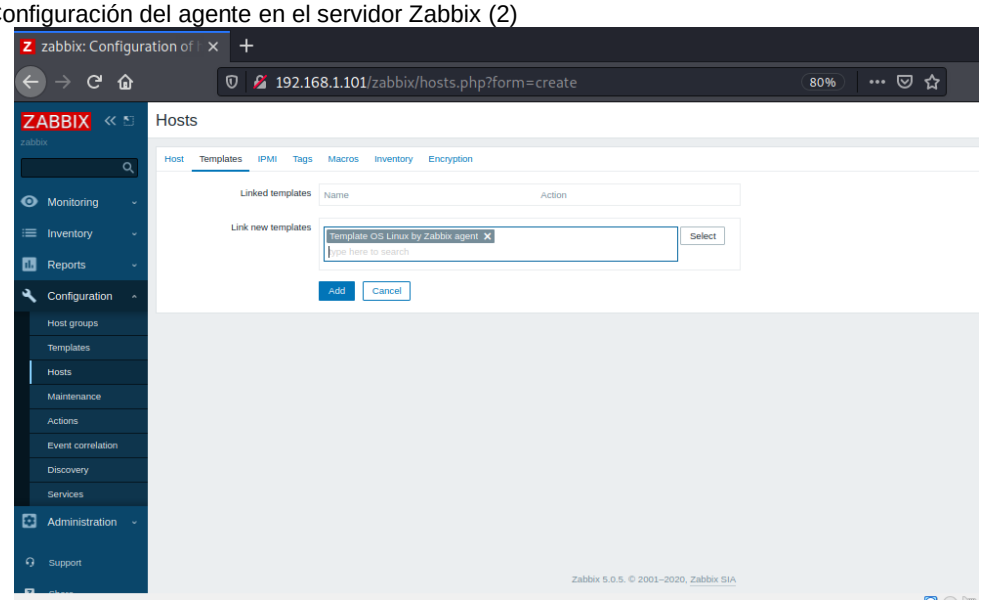
Figura 60. Configuración del agente en el servidor Zabbix (1)



Fuente: elaboración propia.

Se habilita la plantilla basada en sistema operativo Linux accediendo a la pestaña “template”, finalizando con el botón “Add”, como se observa en la Figura a continuación:

Figura 61. Configuración del agente en el servidor Zabbix (2)

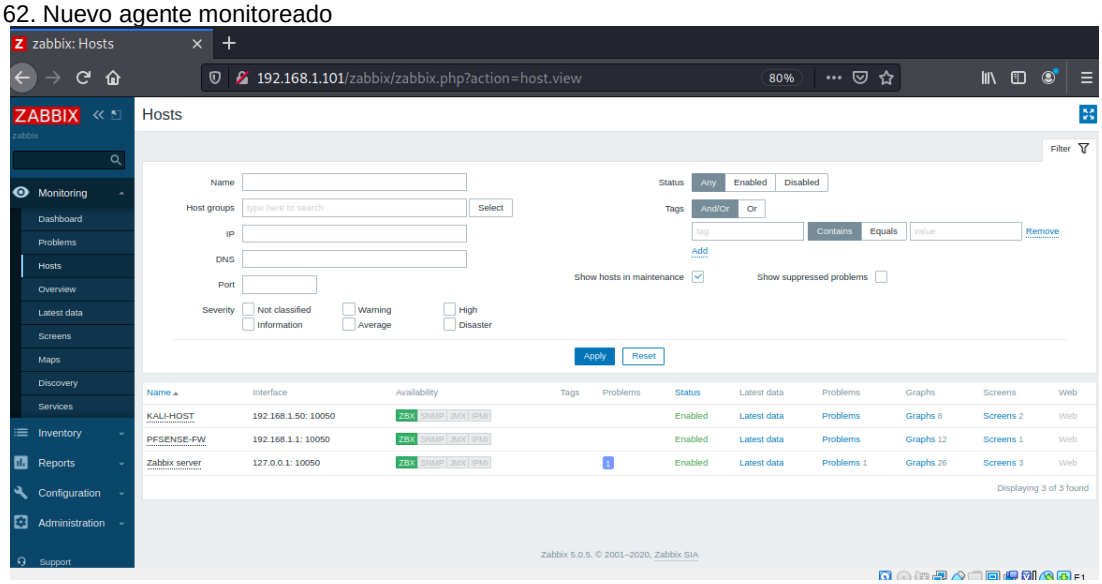


Fuente: elaboración propia.

Con esto, se puede observar en el meno de monitoreo de la interfaz grafica de Zabbix, dentro de la opción “host”, que ya se encuentra habilitado y funcionando el agente

instalado, tal como se aprecia en la siguiente Figura.

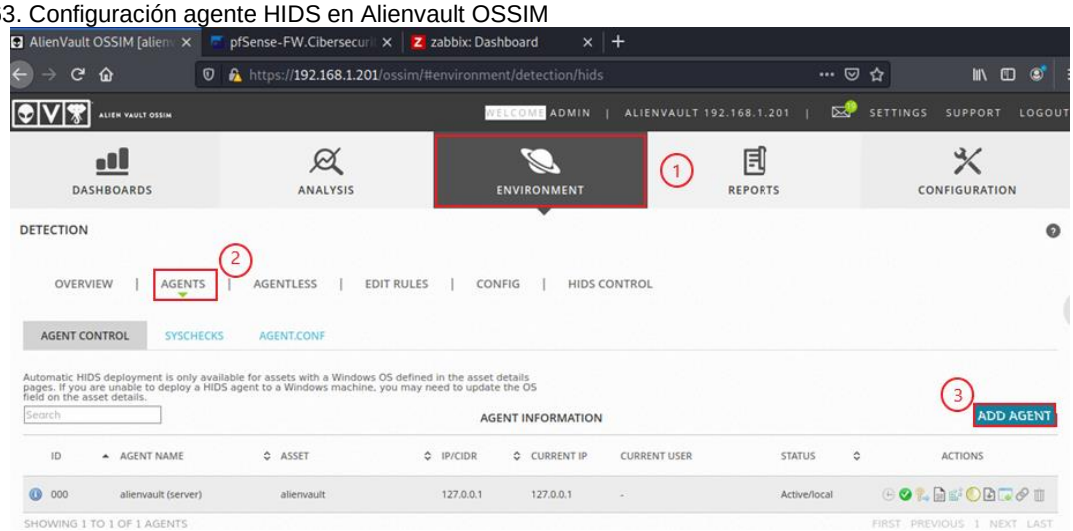
Figura 62. Nuevo agente monitoreado



Fuente: elaboración propia.

4.4.4 Configuración de agentes para Alienvault OSSIM los agentes HIDS, sistema de detección de intrusos basado en host, permite a Alienvault detectar amenazas a través del despliegue de una herramienta como OSSEC. Este proceso se inicia en la consola de administración de Alienvault OSSIM, accediendo al menú “Environment”, opción “Detection”, ingresar a la pestaña “agents”, presionar en el botón “Add agent” como se observa en la siguiente Figura.

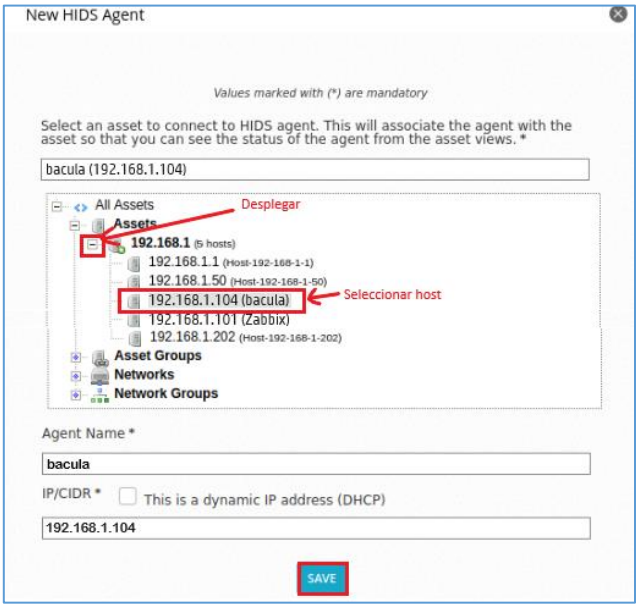
Figura 63. Configuración agente HIDS en Alienvault OSSIM



Fuente: elaboración propia.

En la ventana se selecciona desde el árbol de activos “assets”, el host del servidor bacula, posteriormente se presiona el botón “save”, como se muestra en la siguiente Figura.

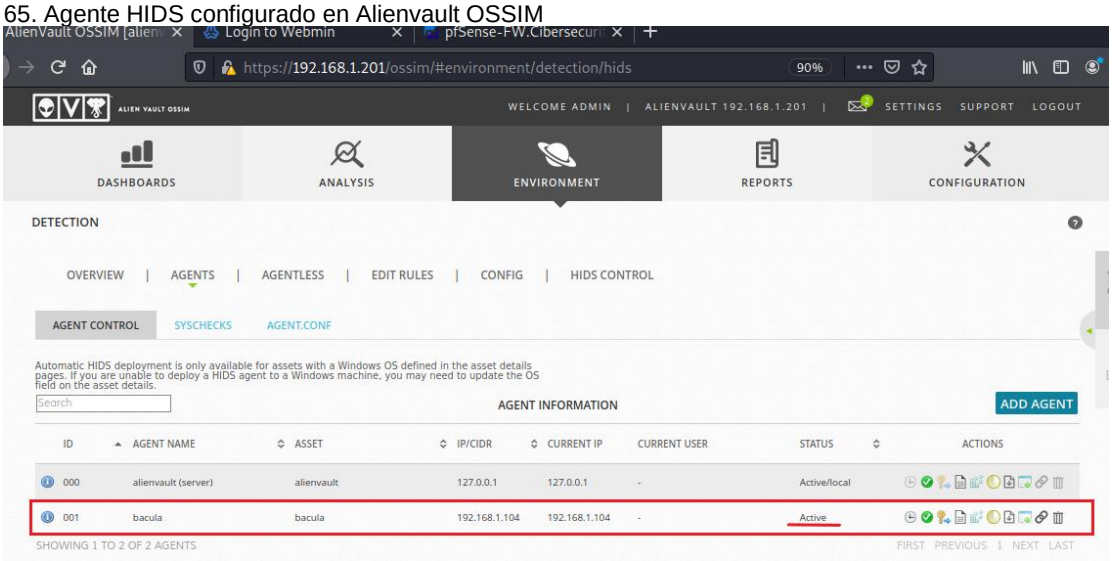
Figura 64. Selección host para HIDS



Fuente: elaboración propia.

Al finalizar se puede observar el nuevo agente configurado como se observa a continuación:

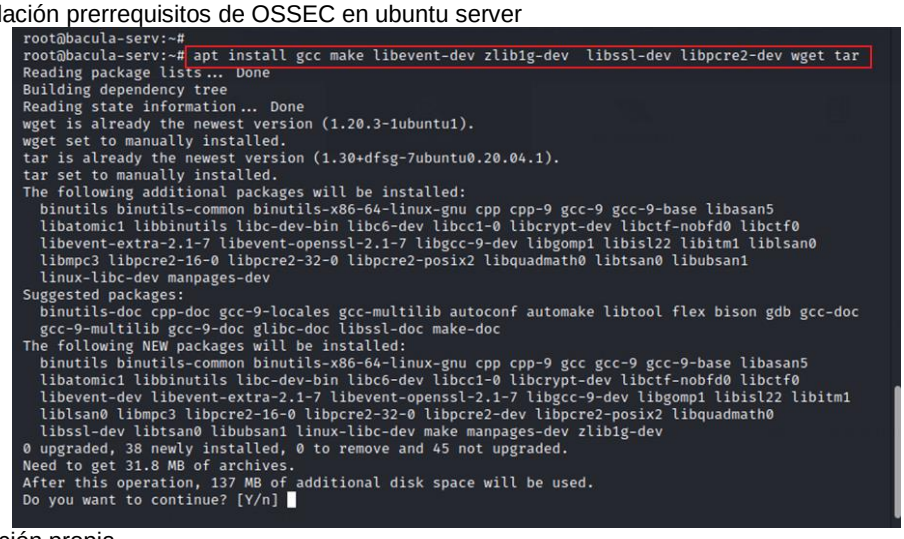
Figura 65. Agente HIDS configurado en Alienvault OSSIM



Fuente: elaboración propia.

4.4.4.1 OSSEC HIDS en Cliente Ubuntu Server. Desde el servidor bacula, se procede a la instalación del agente OSSEC en un servidor Ubuntu 20.04; en primer lugar, se procede a la instalación de algunas dependencias requeridas por OSSEC, como lo son: GCC, Make, Libevent-dev, Zlib-dev, Libssl-dev, Libpcre2-dev, Wget, Tar, ejecutando el comando resaltado en la siguiente Figura.

Figura 66. Instalación prerrequisitos de OSSEC en ubuntu server



Fuente: elaboración propia.

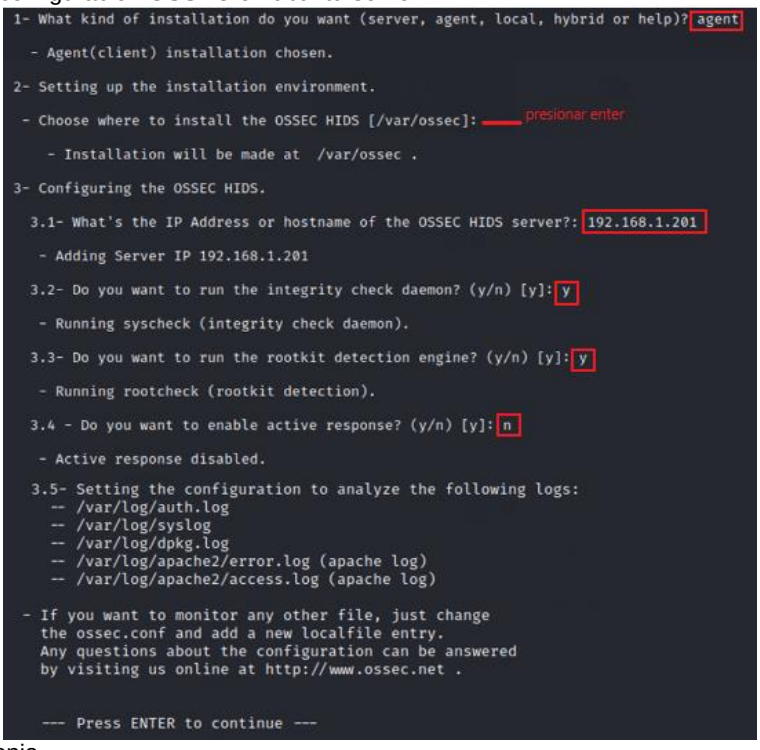
Posteriormente se obtiene el código fuente de OSSEC, ejecutando la instrucción descrita en la siguiente Figura

Figura 67. obtención OSSEC en ubuntu server

Fuente: elaboración propia.

Al finalizar este proceso, se accede, descomprime e instala el paquete obtenido. La instalación inicia con la selección del idioma, seguidamente muestra la información del sistema en el cual se instalará, y posteriormente se establecen los diferentes parámetros de la configuración como se puede apreciar en la siguiente Figura.

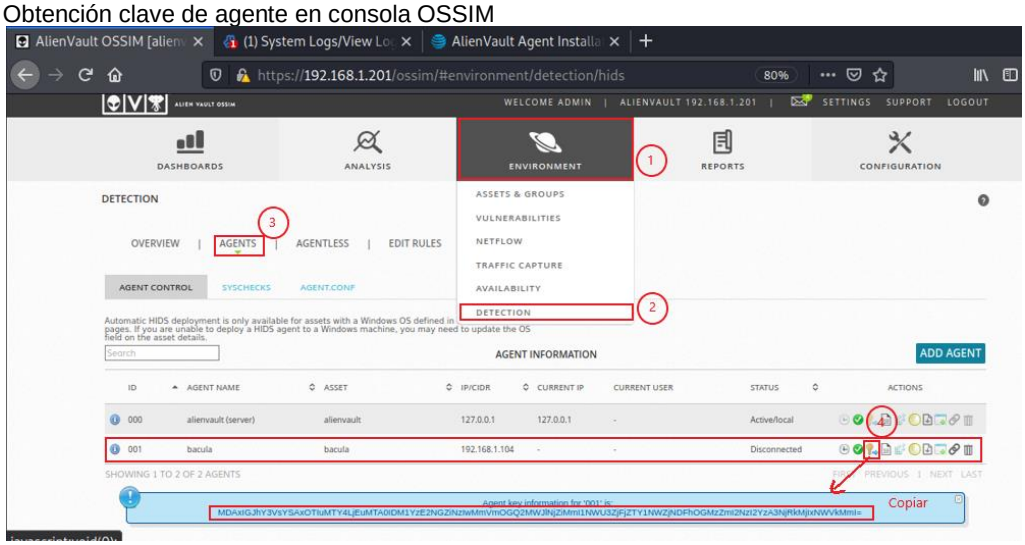
Figura 68. Parámetros configuración OSSEC en ubuntu server



Fuente: elaboración propia.

Luego de la instalación, es necesario habilitar la comunicación entre el servidor y el agente, para lo cual se ingresa nuevamente a la consola de administración de OSSIM, en la opción agentes se obtiene la clave de autenticación, asignada por el servidor, siguiendo la secuencia descrita en la siguiente Figura

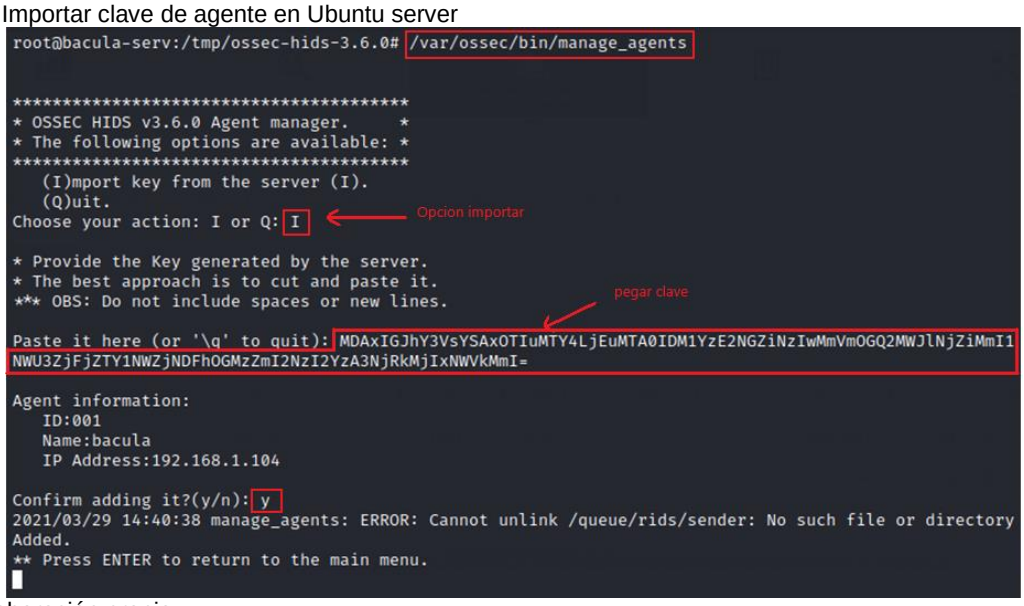
Figura 69. Obtención clave de agente en consola OSSIM



Fuente: elaboración propia.

Se procede a importar la clave copia al agente, ejecutando el comando mostrado en la siguiente Figura y siguiendo los pasos como se describen allí.

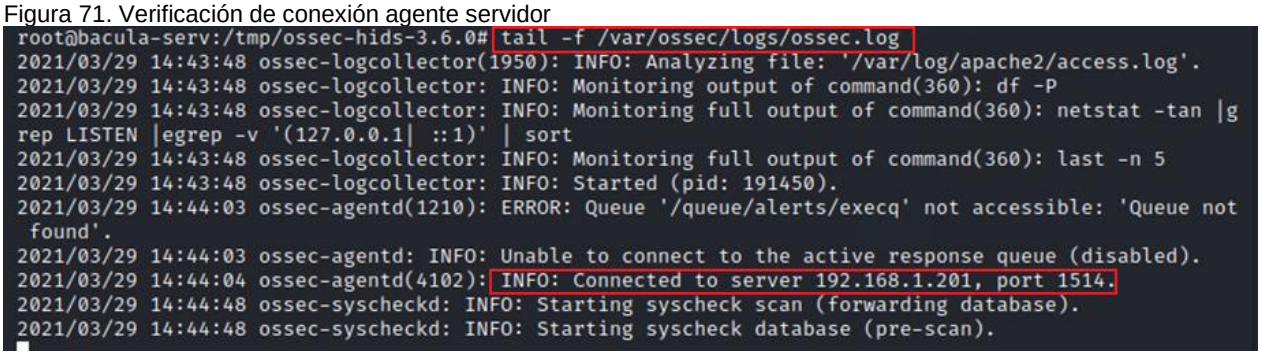
Figura 70. Importar clave de agente en Ubuntu server



Fuente: elaboración propia.

Finalmente se inicia el agente con la instrucción “/var/ossec/bin/ossec-control start” y se verifica en el log que se haya conectado al servidor, como se observa en la siguiente Figura.

Figura 71. Verificación de conexión agente servidor

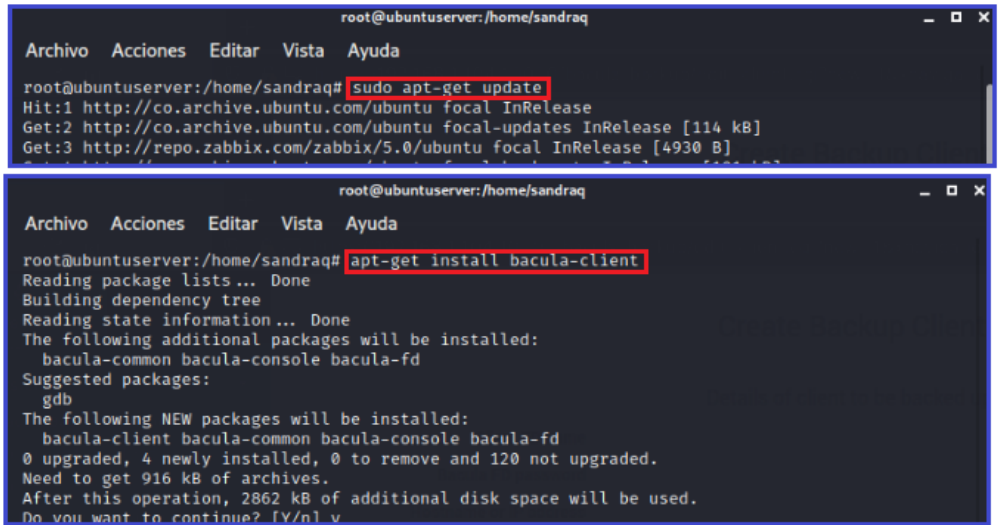


Fuente: elaboración propia.

4.4.5 Configuración de agentes Bacula Para el optimo desempeño de la herramienta Bacula se requiere la configuración del servicio File Daemon en cada uno de los clientes que se van a respaldar, este servicio se encargará de comunicarse con el servicio Bacula Director para indicarle y enviar los archivos que serán respaldados.

4.4.5.1 Agente Bacula en Cliente Ubuntu Server. Se inicia con la instalación del software bacula client, para lo cual se actualizan los repositorios, y se ejecuta las instrucciones que se observan en la Figura

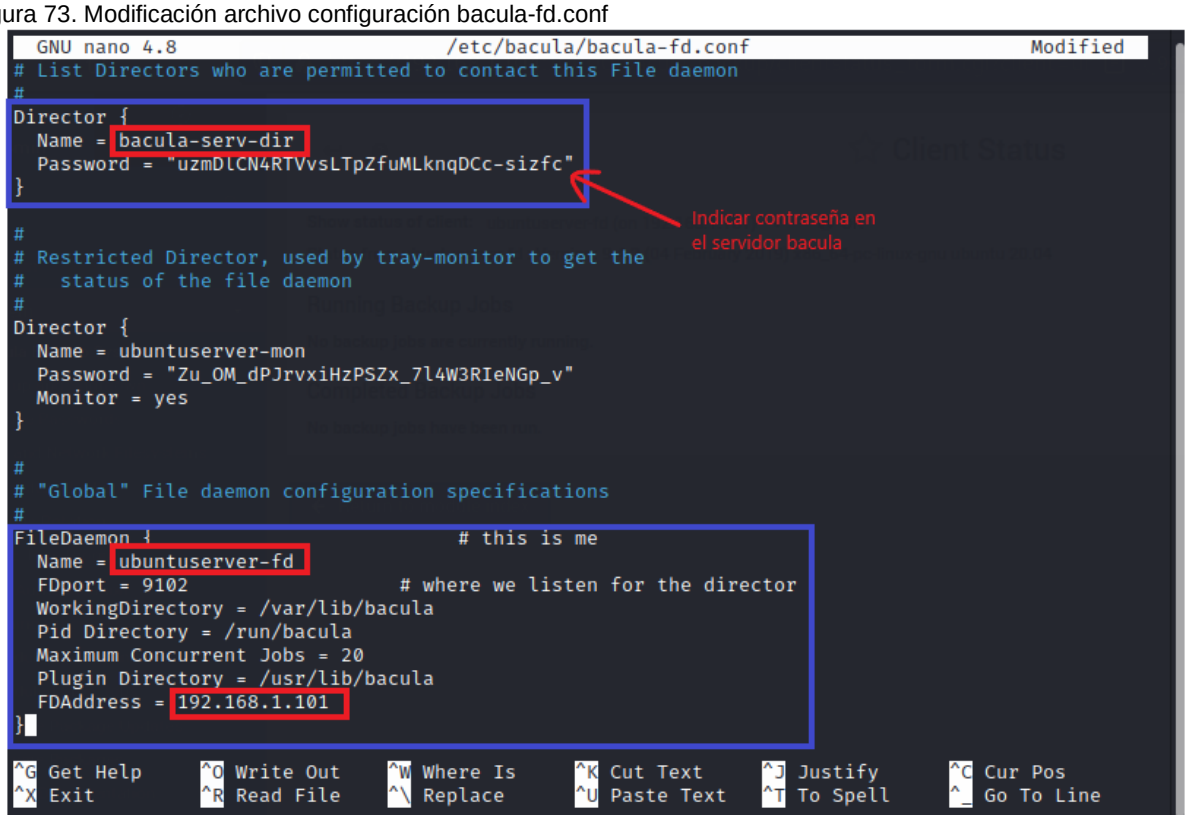
Figura 72. Actualización de repositorios e instalación cliente Bacula



Fuente: elaboración propia.

Una vez instalado se procede a modificar el archivo de configuración del File Daemon del lado del cliente, estableciendo los parámetros del bloque Director, de tal forma que concuerden con la configuración del bacula director en el servidor, esto es, definir el nombre del servidor bacula y la contraseña por medio de la cual se conectará al cliente. De igual forma, el parámetro name en el bloque FileDaemon, para indicar un nombre representativo del cliente para su fácil identificación, y la dirección ip de escucha del cliente, tal como se observa en la Figura

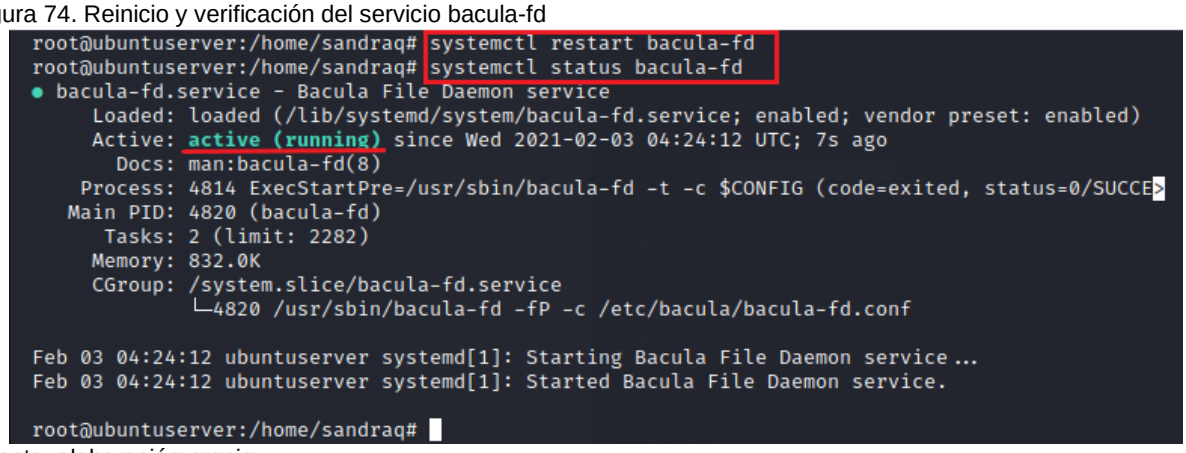
Figura 73. Modificación archivo configuración bacula-fd.conf



Fuente: elaboración propia.

Se guardan los cambios en el archivo de configuración, se reinicia el servicio y se verifica el estado, ejecutando las instrucciones resaltadas en la siguiente Figura.

Figura 74. Reinicio y verificación del servicio bacula-fd



Fuente: elaboración propia.

Se agrega una regla de entrada en el firewall para permitir las conexiones del director de

bacula en el puerto 9102, como se observa en la Figura, posteriormente se recargan las reglas.

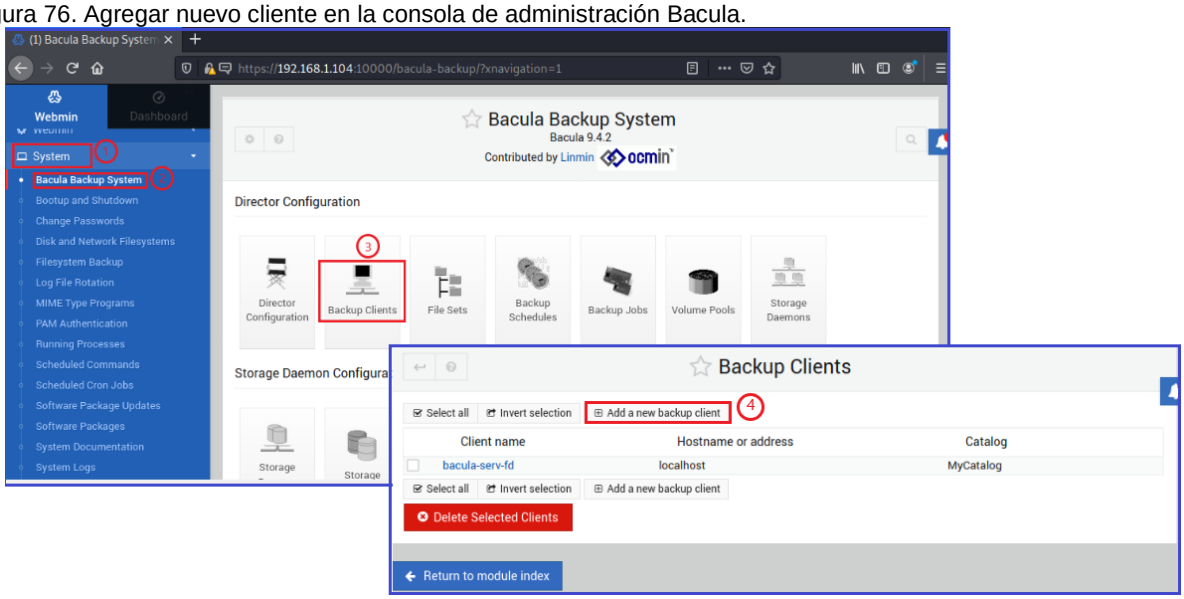
Figura 75. Configuración reglas de Firewall en el cliente

```
root@ubuntuserver:/home/sandraq# ufw allow from 192.168.1.104 to any port 9102
Rule added
root@ubuntuserver:/home/sandraq# ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 9102                       ALLOW IN    192.168.1.104

root@ubuntuserver:/home/sandraq# ufw reload
Firewall reloaded
root@ubuntuserver:/home/sandraq#
```

Fuente: elaboración propia.

En siguiente paso es indicar al servidor el nuevo cliente, para ello desde la consola de administración web se accede a la opción “Backup Clients” luego “Add a new backup client”, siguiendo la secuencia que se muestra en la Figura a continuación:

Figura 76. Agregar nuevo cliente en la consola de administración Bacula.

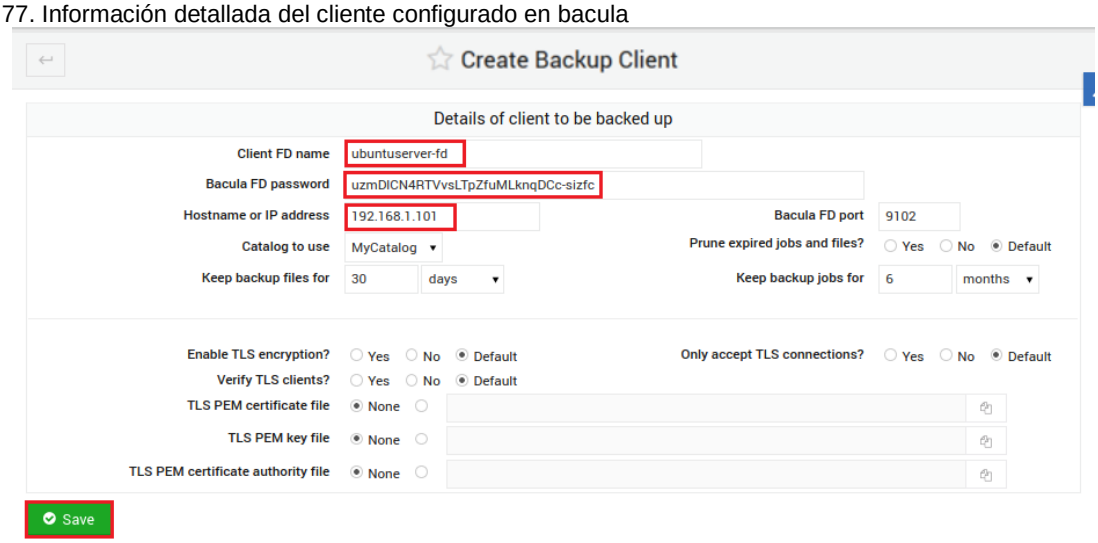


Fuente: elaboración propia.

En este punto se debe indicar a la consola de bacula director los parámetros configurados en el cliente, tales como el nombre definido para el cliente, la dirección ip y la contraseña de conexión con el bacula-director, como se observa en la siguiente Figura.

Adicionalmente es posible indicar en este punto la configuración de retención de las copias de seguridad.

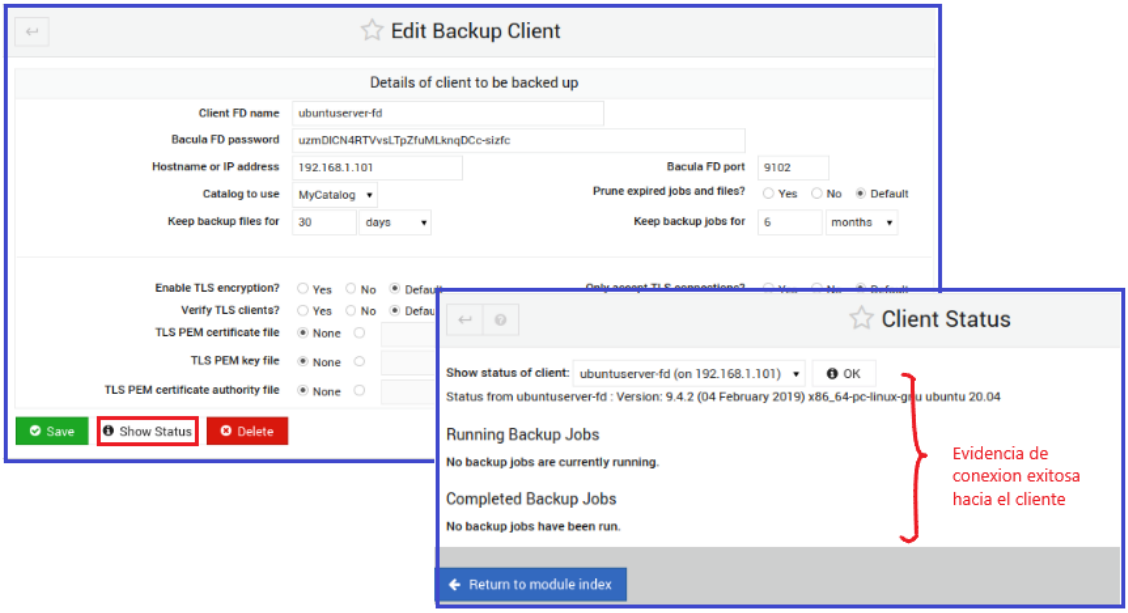
Figura 77. Información detallada del cliente configurado en bacula



Fuente: elaboración propia.

Para verificar que se esté agregado correctamente se selecciona el cliente agregado de la lista y presionar el botón status, el cual arrojaría error o un mensaje que indica la conexión exitosa como en la siguiente Figura

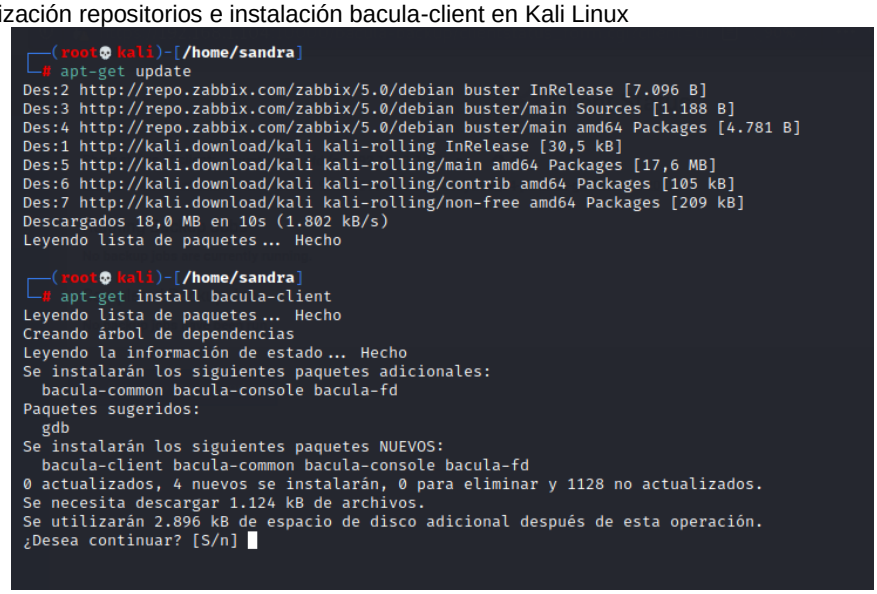
Figura 78. Verificación estatus del cliente Ubuntu server



Fuente: elaboración propia.

4.4.5.2 Agente Bacula en cliente Kali Linux. Se inicia con la actualización de repositorios e instalación del paquete bacula-client como se observa a continuación.

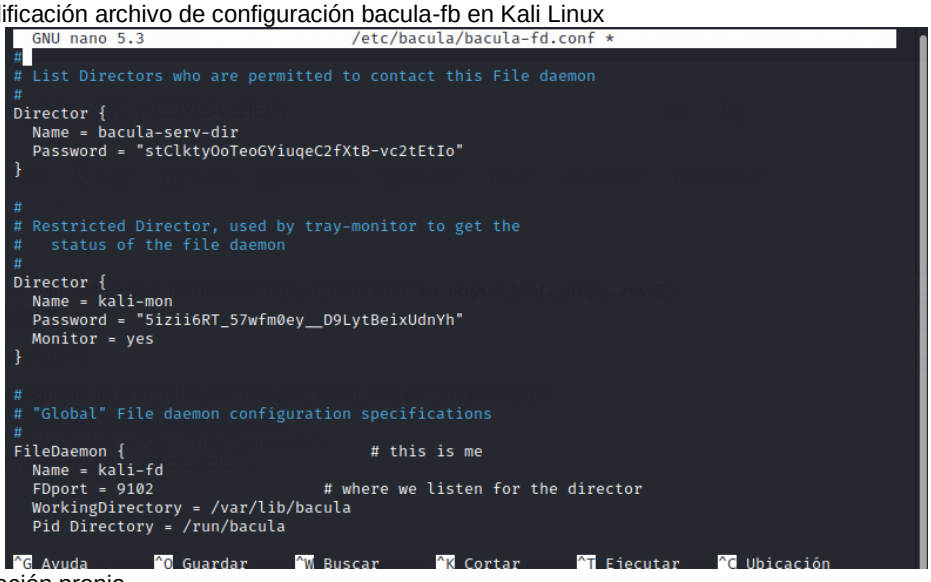
Figura 79. Actualización repositorios e instalación bacula-client en Kali Linux



Fuente: elaboración propia.

Se procede a modificar el archivo de configuración en el cliente para indicar los parámetros que permitirán la conexión con el servidor, esto es, indicar el nombre de Host donde se ejecuta el Director y el nombre host donde se ejecuta el FileDaemon, esto se puede observar en la siguiente Figura.

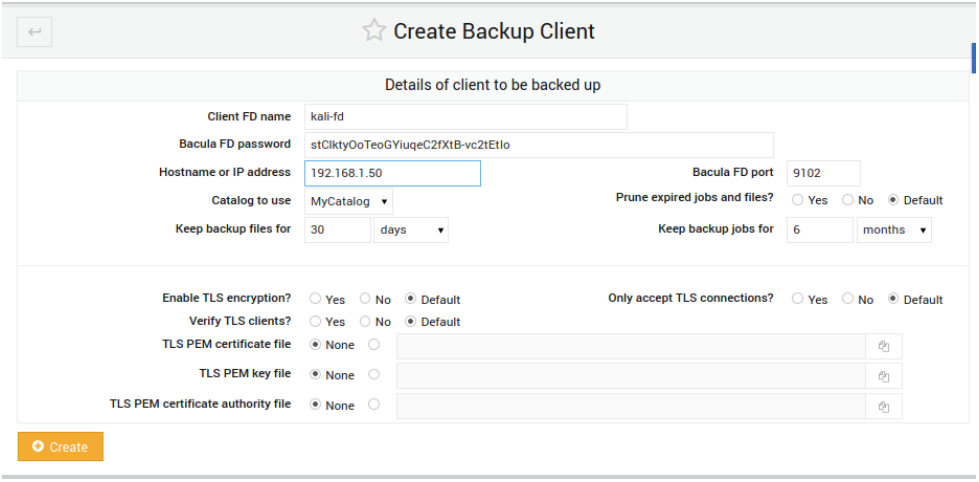
Figura 80. Modificación archivo de configuración bacula-fb en Kali Linux



Fuente: elaboración propia.

Se verifica el estatus de conexión con el cliente desde la consola de configuración como se observa en la siguiente Figura:

Figura 81. Verificación estatus del cliente Kali Linux



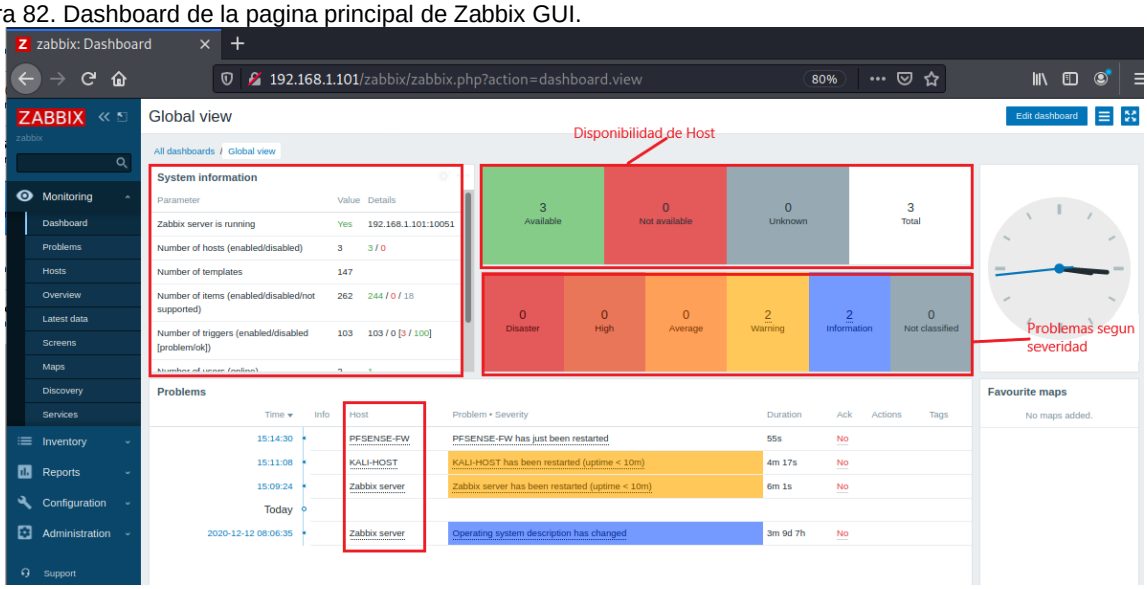
Fuente: elaboración propia.

4.4.6 Ejecución de pruebas de Software

4.4.6.1 Servidor de monitoreo Zabbix. La aplicación Zabbix viene dotada con una interfaz gráfica de usuario que permite monitorear y administrar los activos de la infraestructura tecnológica que cuenten con el respectivo agente Zabbix instalado.

- **Principales funciones.** Para ingresar se hace desde un navegador web en la ruta https://ip-servidor-zabbix/zabbix, digitando las credenciales del administrador, se muestra en la página inicial el Dashboard, en donde se visualizan de manera resumida algunos datos como lo son información sobre el estado del sistema, disponibilidad de los host monitoreados, el indicador actual de los problemas según la gravedad, así como una bitácora de errores o problemas que se han presentado en los host, indicando la hora de ocurrencia y la severidad de los mismos, tal como se observa en la siguiente Figura.

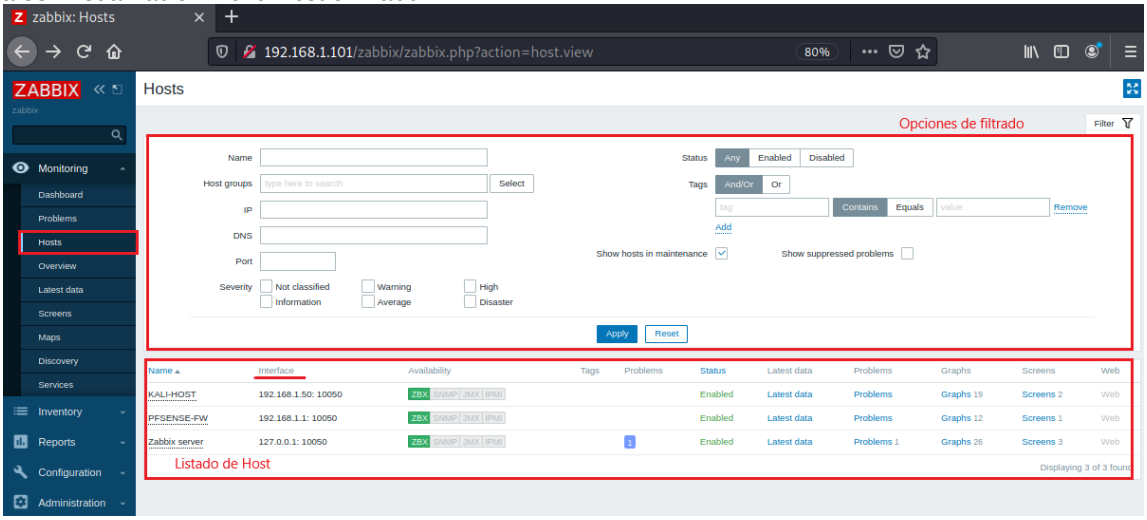
Figura 82. Dashboard de la pagina principal de Zabbix GUI.



Fuente: elaboración propia.

Al presionar clic sobre el nombre de uno de los hosts se puede obtener mas detalles sobre su estado, de igual forma desde el menú “Monitoring”, se puede acceder a mas información específica y detallada, entre las opciones mas usadas se tiene “Host” y “Problems”. Desde la opción “host” se puede acceder a un listado de los activos monitoreados, en donde se indica la interfaz, status actual, acceso a los datos mas recientes respecto al hardware, los problemas asociados, entre otros. En la parte superior se puede filtrar el listado, lo cual es de gran utilidad cuando la infraestructura monitoreada es bastante grande, en la siguiente Figura se puede visualizar lo expuesto.

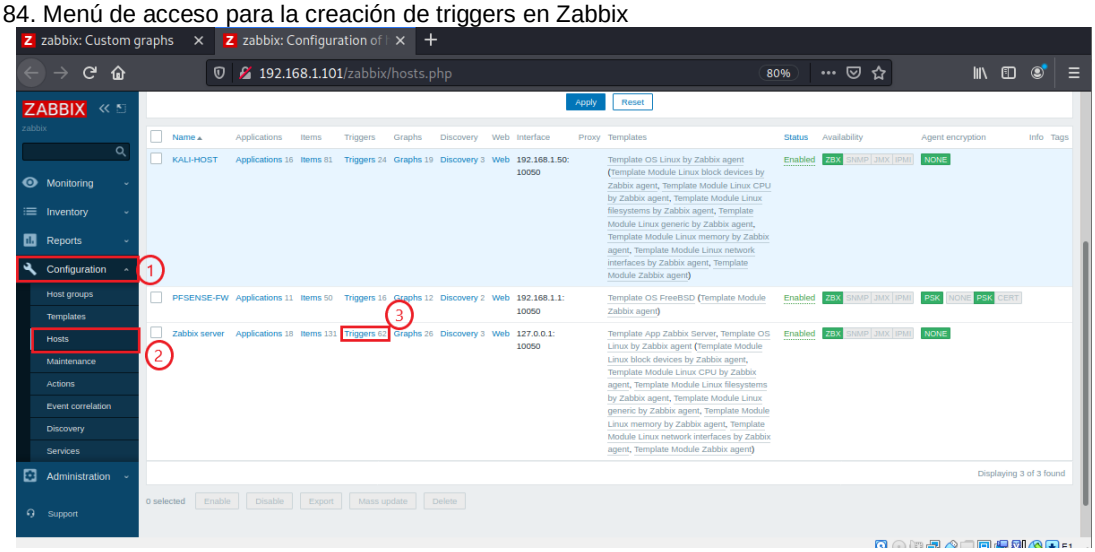
Figura 83. Visualización menú Host en Zabbix



Fuente: elaboración propia.

- **Creación de acciones y notificaciones de email**. Zabbix permite configurar acciones y generar notificaciones cuando se detectan problemas en los hosts monitoreados, esto ayuda al administrador a dar respuesta rápida en el restablecimiento de los servicios en cada host. Para hacerlo se debe contar como requisito principal con un host, que cuente con un ítem o elemento sobre el cual se realizara la recolección de datos. A partir de allí se crean los disparadores o trigger que por medio de los cambios de estado en los eventos permitirán la definición de acciones. En la siguiente Figura, se muestra los pasos iniciales para la creación de un trigger: en el menú “configuration” → “host”, clic en la columna “triggers”.

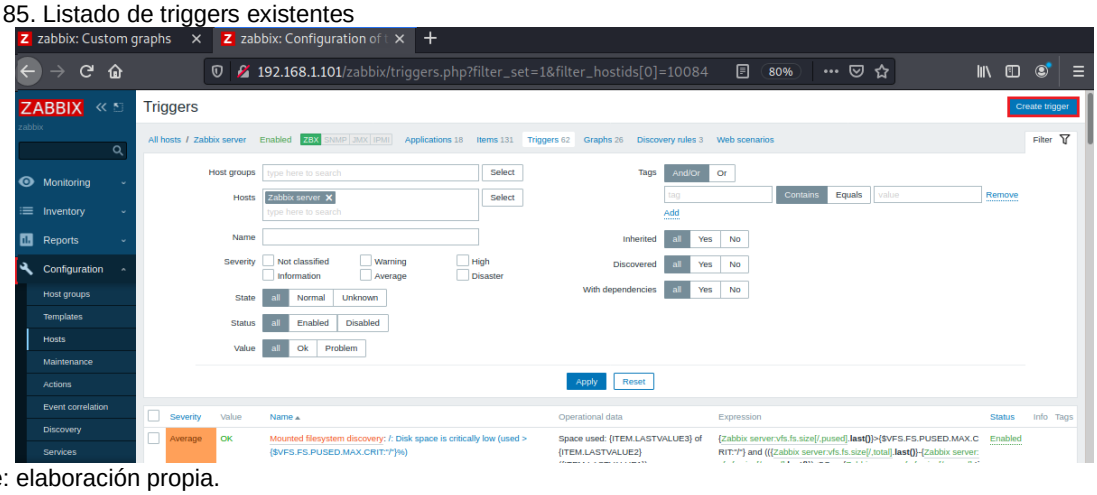
Figura 84. Menú de acceso para la creación de triggers en Zabbix



Fuente: elaboración propia.

Se muestra una nueva ventana donde se presiona en el botón “create Trigger”

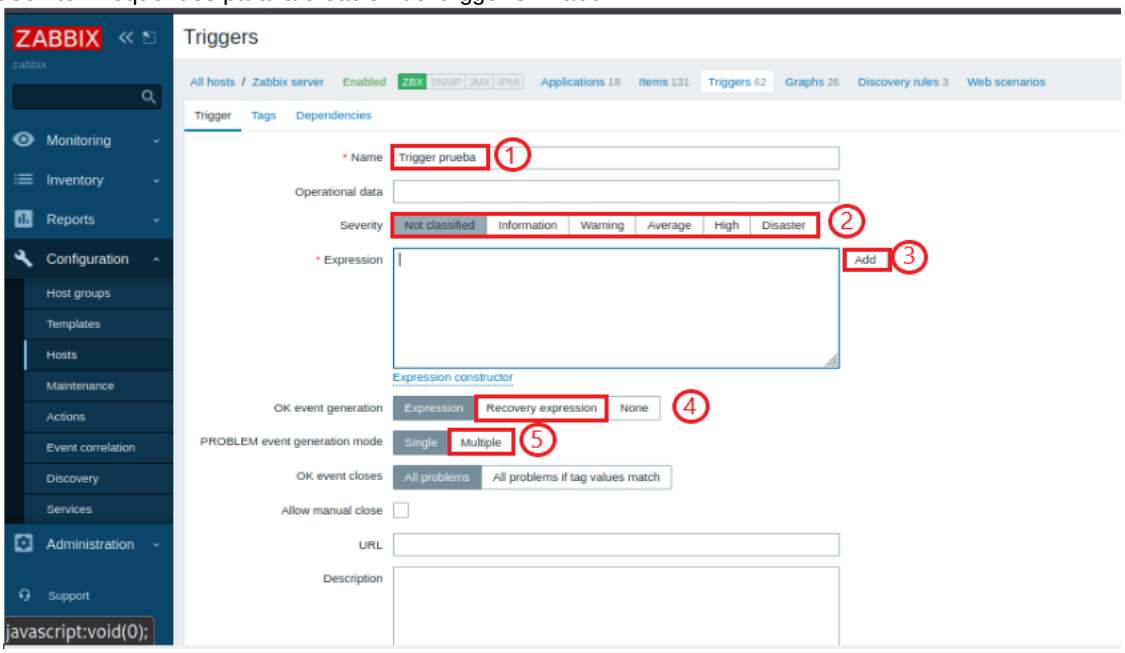
Figura 85. Listado de triggers existentes



Fuente: elaboración propia.

Siguiendo con la secuencia marcada en la Figura 76, en primer lugar se define el nombre para el Trigger, el grado de importancia del evento generado, entre las opciones existentes, en el tercer paso con el botón “add” se ingresa a generar una expresión adecuada. La opción 4 denominada “ok evento generation”, es donde se indica la condición que se debe cumplir para que este trigger vuelva a un estado ok.

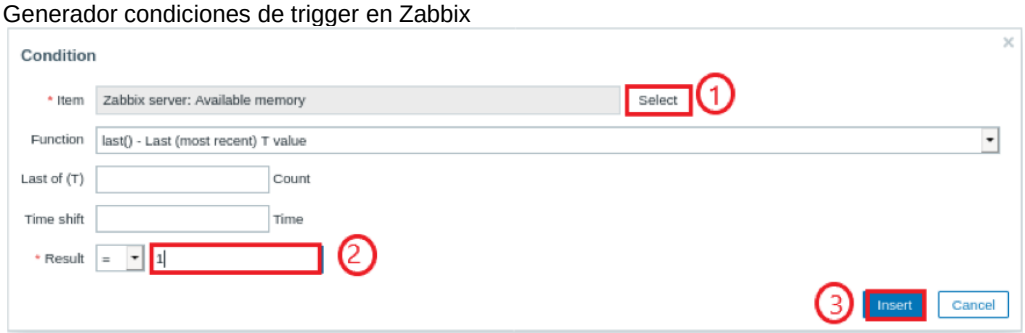
Figura 86. Item requeridos para la creación del trigger en Zabbix



Fuente: elaboración propia.

Cuando se accede en el generador de expresiones marcada con tercer paso en la Figura 76, se muestra una ventana como la Figura 77, donde se debe como primer paso elegir el ítem sobre el cual se colectaran datos, seguidamente el valor que debe cumplir la condición y por ultimo el botón insertar

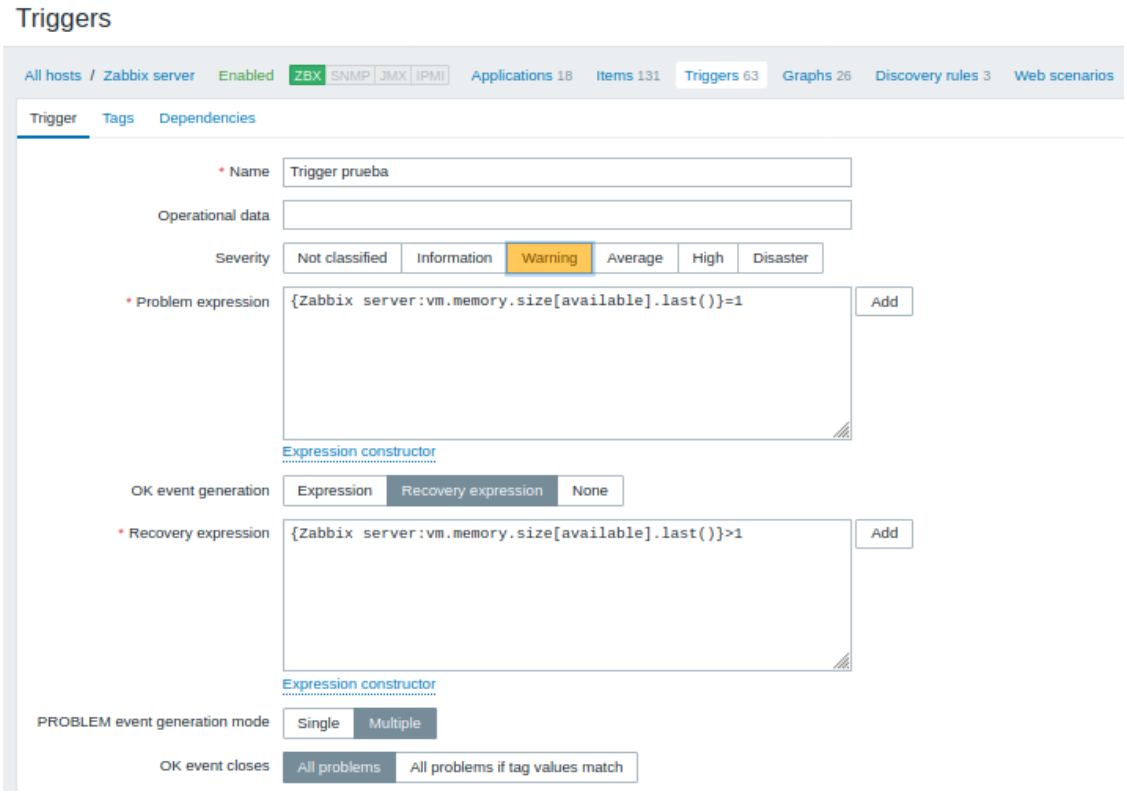
Figura 87. Generador condiciones de trigger en Zabbix



Fuente: elaboración propia.

De forma similar a la anterior son los pasos requeridos para la creacion de la “Recovery expresión”, con lo cual quedaría la pestaña inicial como se muestra en la siguiente Figura, para guardar se presiona el botón “Add” que se encuentra al final.

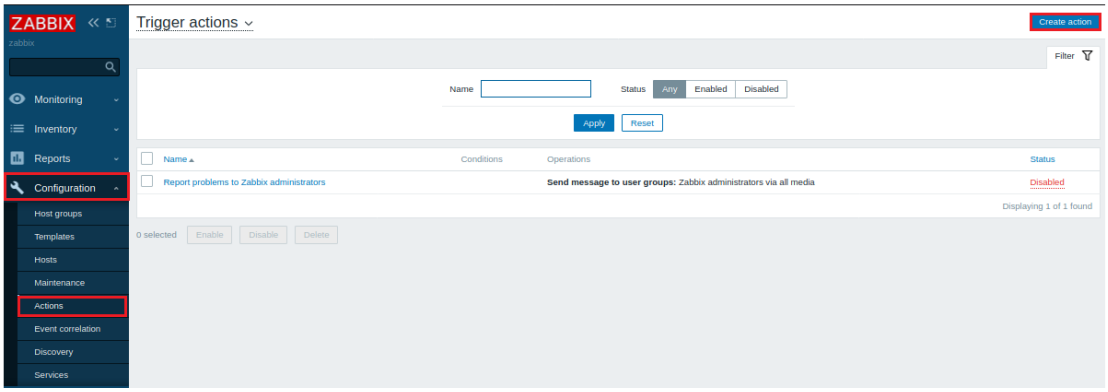
Figura 88. Definición inicial del trigger creado en Zabbix



Fuente: elaboración propia.

El siguiente paso consiste en la creación de acciones, ingresando en el menu “configuration” → “Actions”, y presionar el botón “create action”, tal como se observa en la secuencia demarcada en la siguiente Figura.

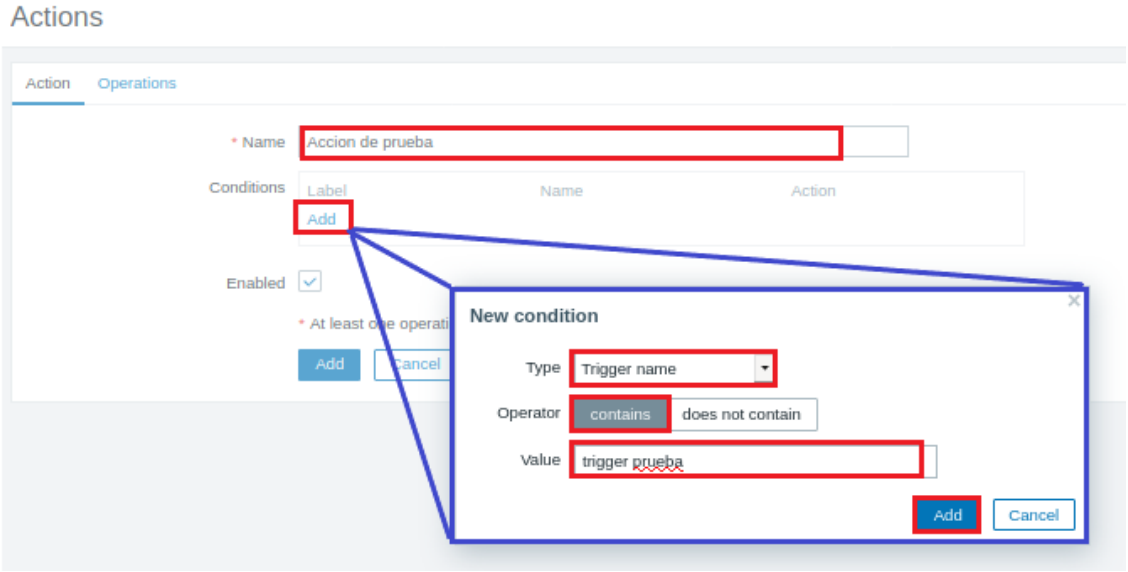
Figura 89. Creación de Actions en Zabbix



Fuente: elaboración propia.

En la nueva ventana, se define el nombre de la acción y se crean las condiciones para su realización presionando en el botón add. Como se observa en la siguiente Figura, se crea una primera condición.

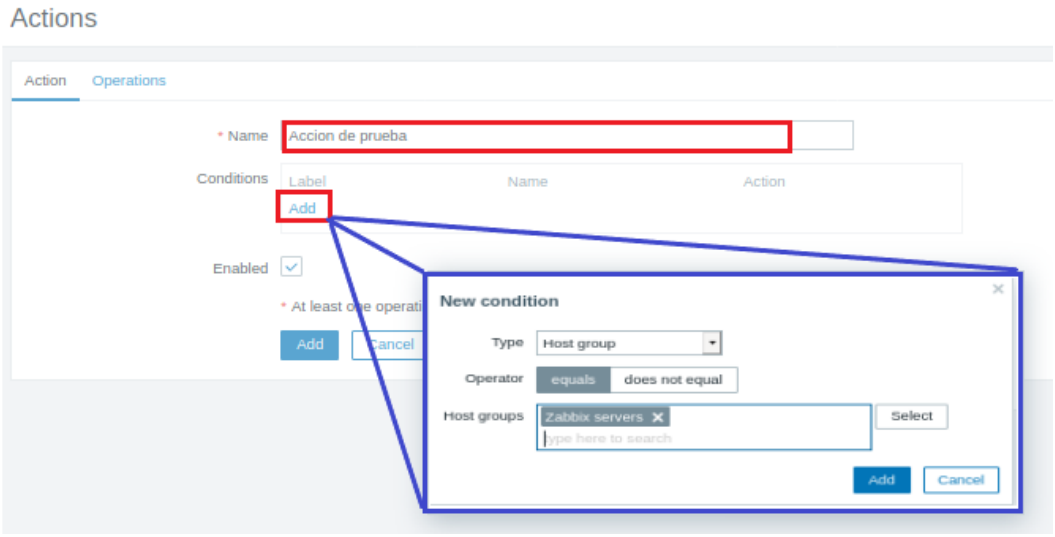
Figura 90. Definición de condición 1 para la acción en Zabbix



Fuente: elaboración propia.

De igual forma que la anterior se crea una segunda condición como se muestra en la siguiente Figura.

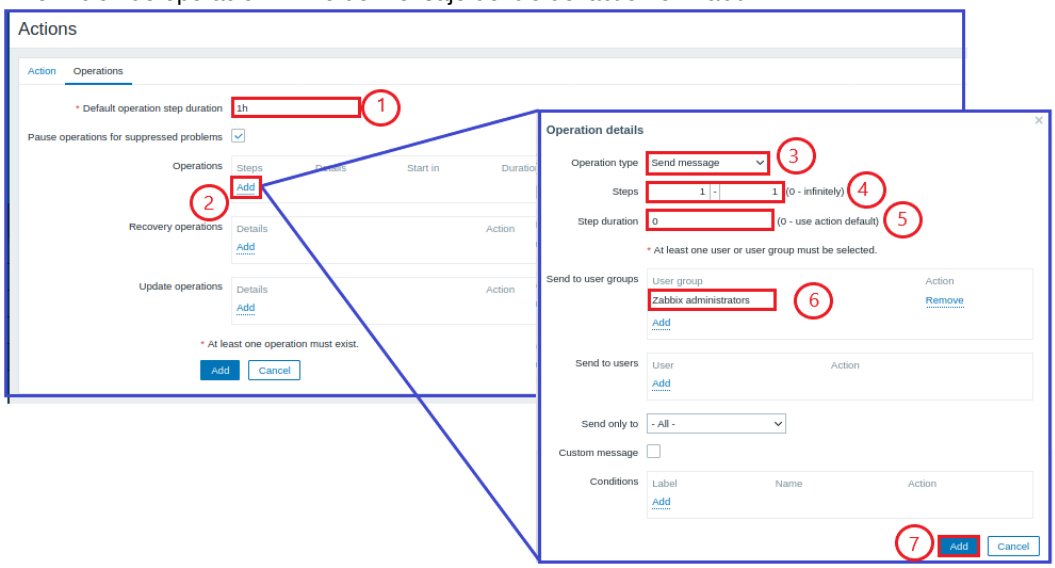
Figura 91. Definición de condición 2 para la acción en Zabbix



Fuente: elaboración propia.

Posterior a la definición inicial de la accion, se procede a ingresar en la pestaña operación, en donde se define las actividades a realizar cuando se genere un evento que dispara el trigger. Como primer paso se define la duración por defecto que tendrá el paso, en este caso una hora, seguidamente se presiona el botón “add”, para agregar los detalles de la operación: que será del tipo enviar mensaje, se identifica qué paso es y se establece 0 para definir la duración del paso como default, se seleccionan los usuarios destinatarios del mensaje y para concretar se presiona en el botón “Add”. En la Figura 82 se ilustra la secuencia de pasos descritas en este parte.

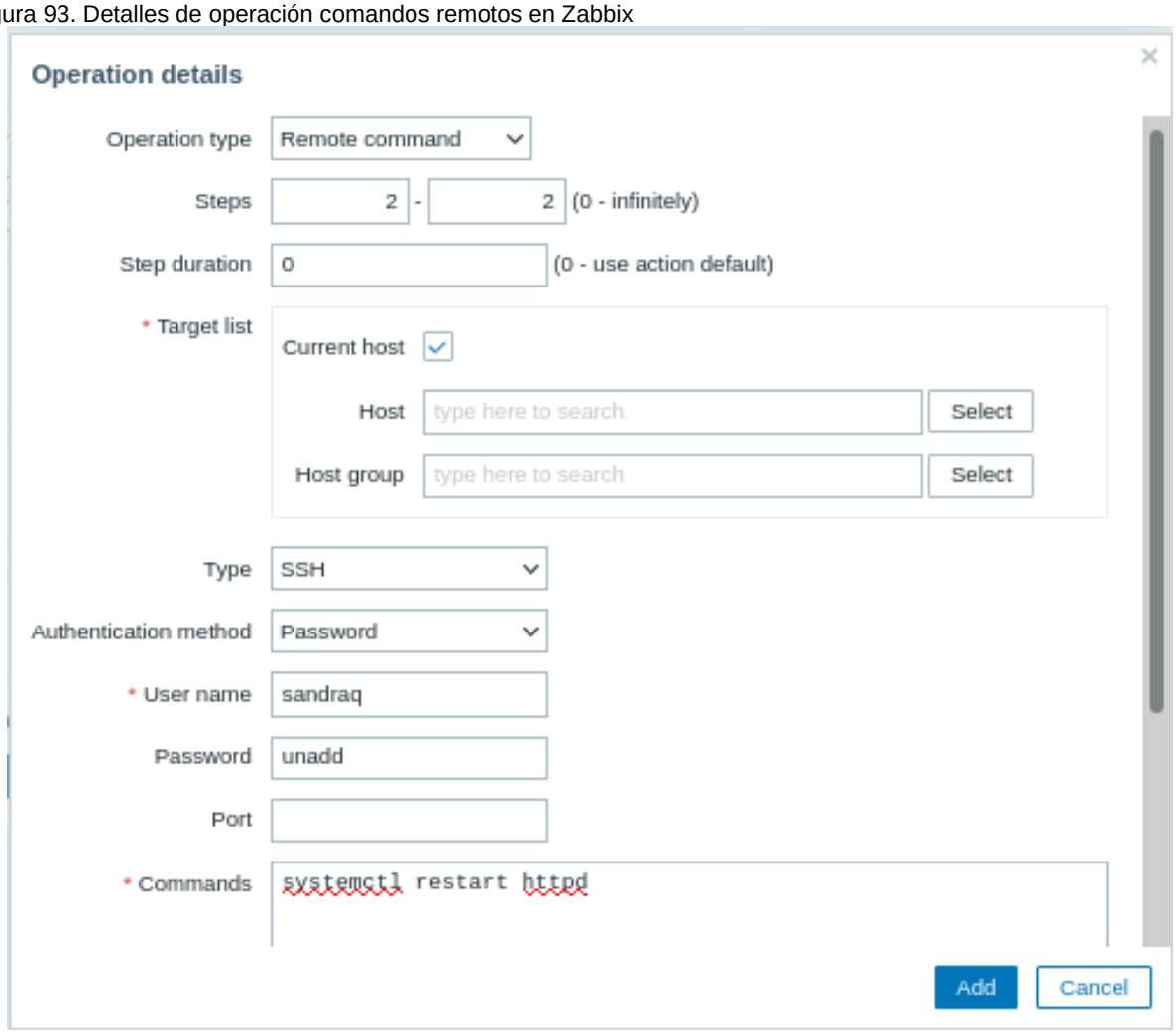
Figura 92. Definición de operación Envío de mensaje dentro del action en Zabbix .



Fuente: elaboración propia.

Otro tipo de operación útil es el envío de comandos remotos, para hacerlo se presiona nuevamente el botón add ubicado en la sección “operations”, seleccionar el tipo de operación como “remote Command”, se identifica el paso como numero 2, como target para la ejecución se selecciona “current host”. Entre las opciones de tipo de comando se tiene: IPMI, telnet, SSH, etc. Para este ejemplo se utilizará SSH, utilizando los parámetros mostrados en la siguiente Figura.

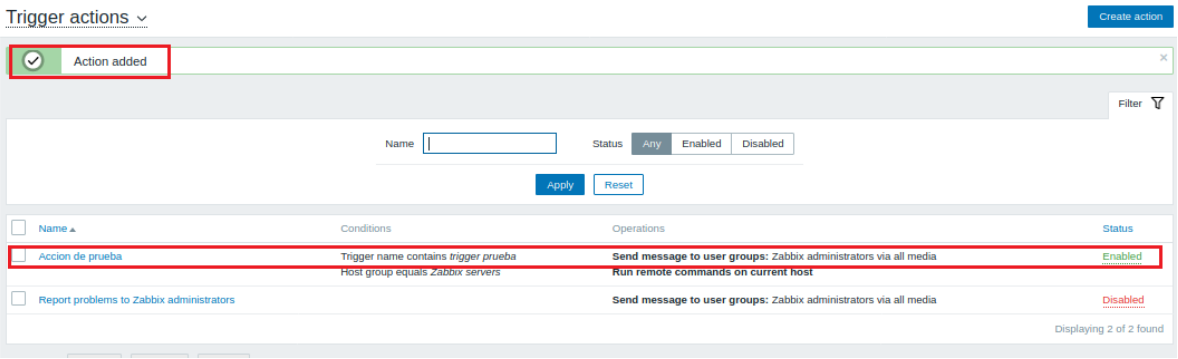
Figura 93. Detalles de operación comandos remotos en Zabbix



Fuente: elaboración propia.

Al final se presiona el botón add, se observa un mensaje como se muestra en la siguiente Figura, en donde también se evidencia la nueva acción creada cuyo estado es habilitado.

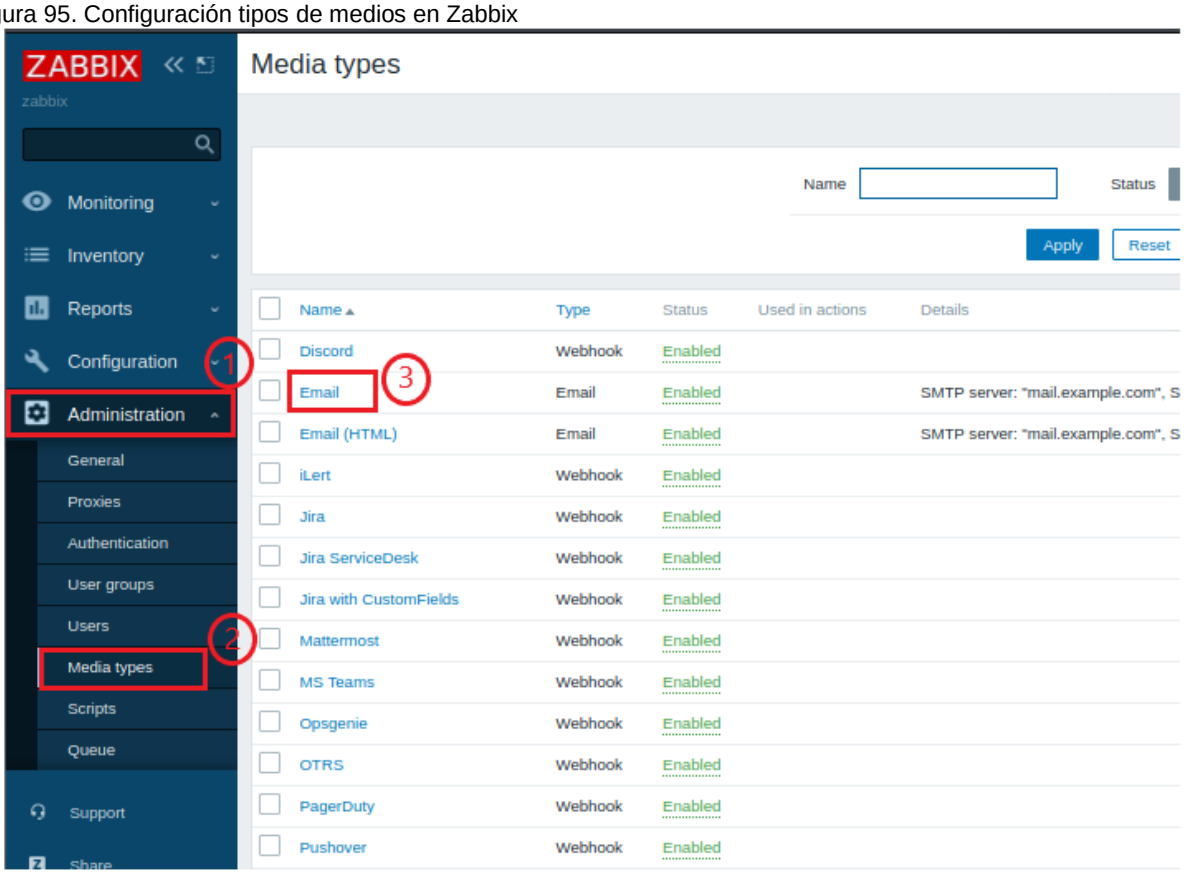
Figura 94. Visualización de action creada



Fuente: elaboración propia.

Para que se pueda completar acciones como el envío de correos de notificación, se requiere configurar los tipos de medios que utilizara Zabbix, para ello, se ingresa al menú "administration", → "Media types", seleccionar del listado de medios la opción "Email", para editar su configuración, tal como se observa en la secuencia descrita en la siguiente Figura.

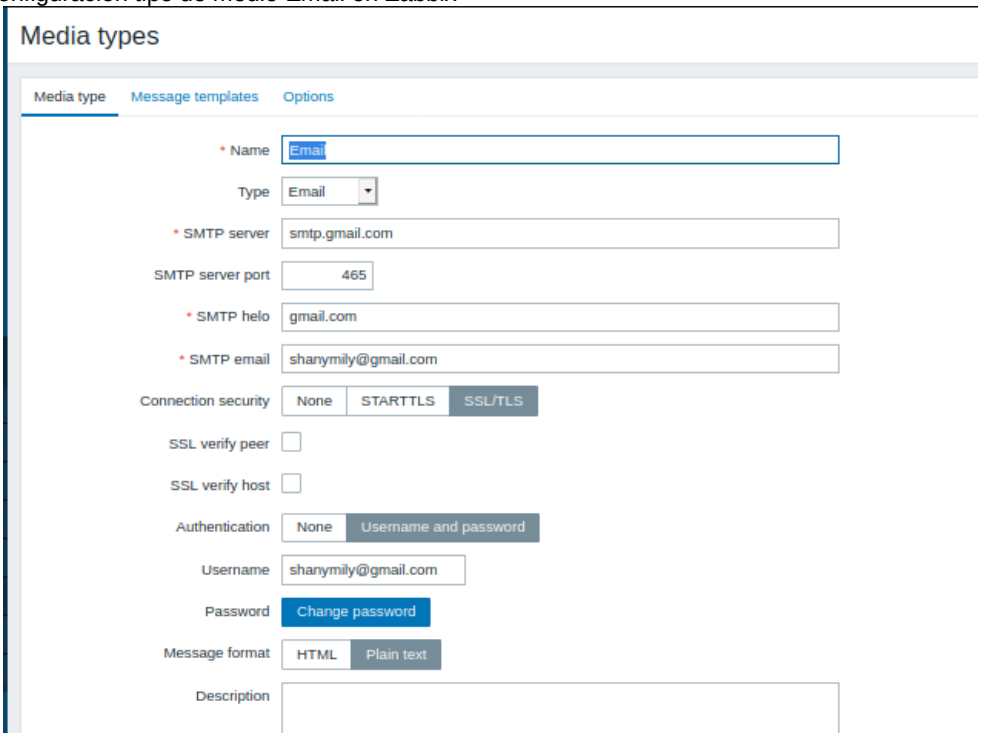
Figura 95. Configuración tipos de medios en Zabbix



Fuente: elaboración propia.

En esta nueva pantalla se ingresan los datos para la configuración del servidor de correo corporativo, o bien se puede utilizar un servicio de correo público a modo de prueba, en este caso Gmail, se establecen los datos correspondientes a servidor, puerto y opciones de seguridad, según se observa en la siguiente Figura.

Figura 96. Configuración tipo de medio Email en Zabbix



Fuente: elaboración propia.

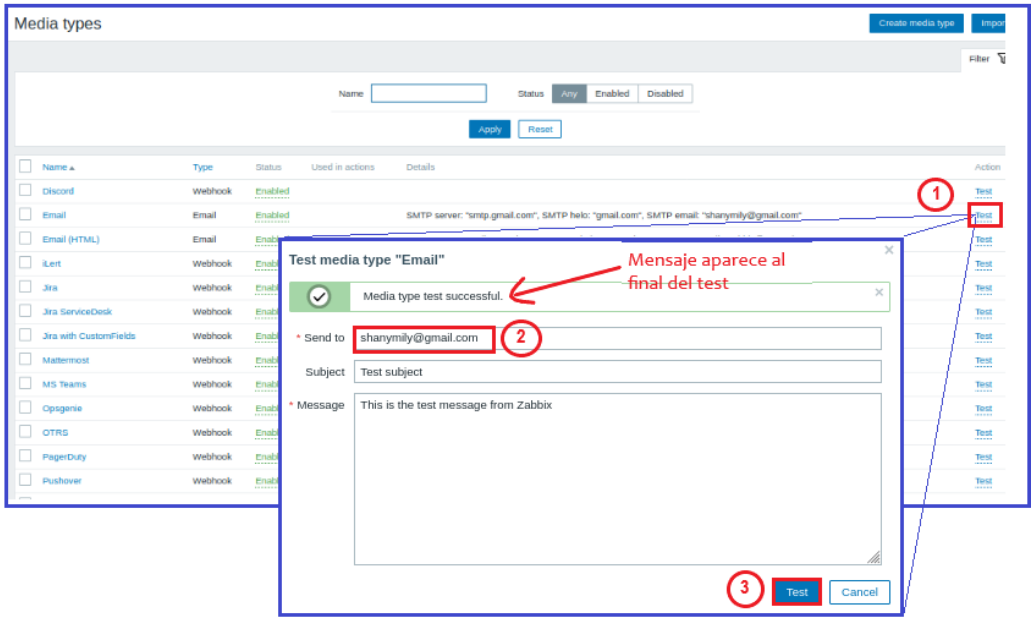
Cabe anotar, que el servidor Zabbix debe tener instalado y configurado el servicio ssmtp, para ello se debe desde la consola ejecutar los comandos de actualización y posteriormente instalación. Una vez instalada la herramienta se edita el archivo de configuración ssmtp.conf con los datos de servidor de correo a utilizar, tal como se observa en la siguiente Figura.

Figura 97. Configuración servicio ssmtp en servidor Zabbix

Fuente: elaboración propia.

Ahora se debe entrar nuevamente a la interfaz gráfica de Zabbix para realizar un test de envío y así corroborar que la configuración de envío de email sea funcional, para esto presionar la opción “test, que se encuentra en el listado “Media Types”, y seguir la secuencia mostrada en la siguiente Figura

Figura 98. Test envío email en MediaTypes en Zabbix



Fuente: elaboración propia.

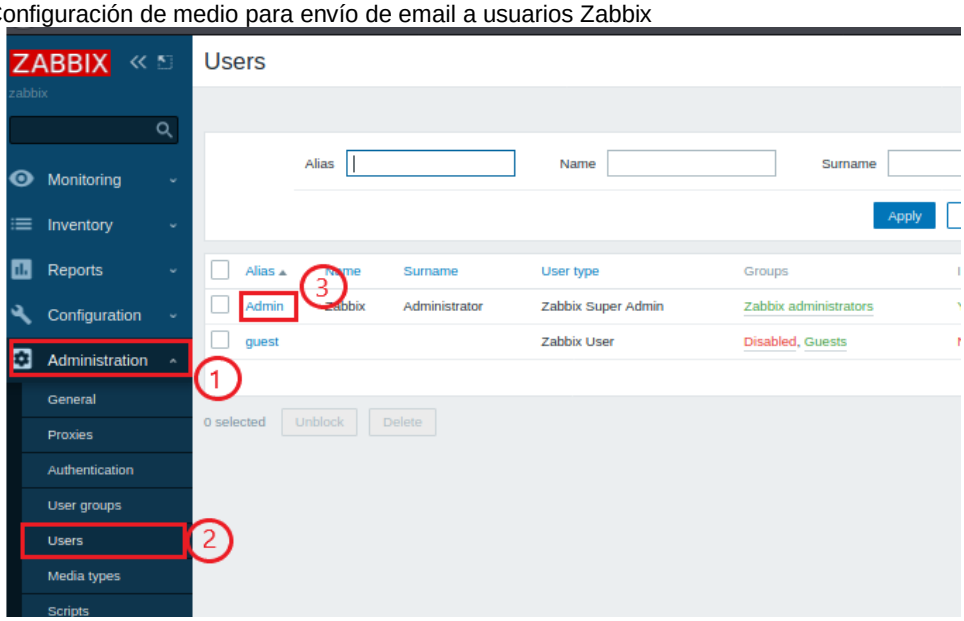
El cual se observa de la siguiente forma en el buzón de correo:

Figura 99. Evidencia de recepción test de mensaje de zabbix

Fuente: elaboración propia.

Ahora se deben configurar los tipos de medios de los usuarios Zabbix, desde el menú “administration”, opción “User”, seleccionar el usuario “Admin”, para editar los medios para el usuario, tal como se observa en la secuencia descrita en la siguiente Figura.

Figura 100. Configuración de medio para envío de email a usuarios Zabbix

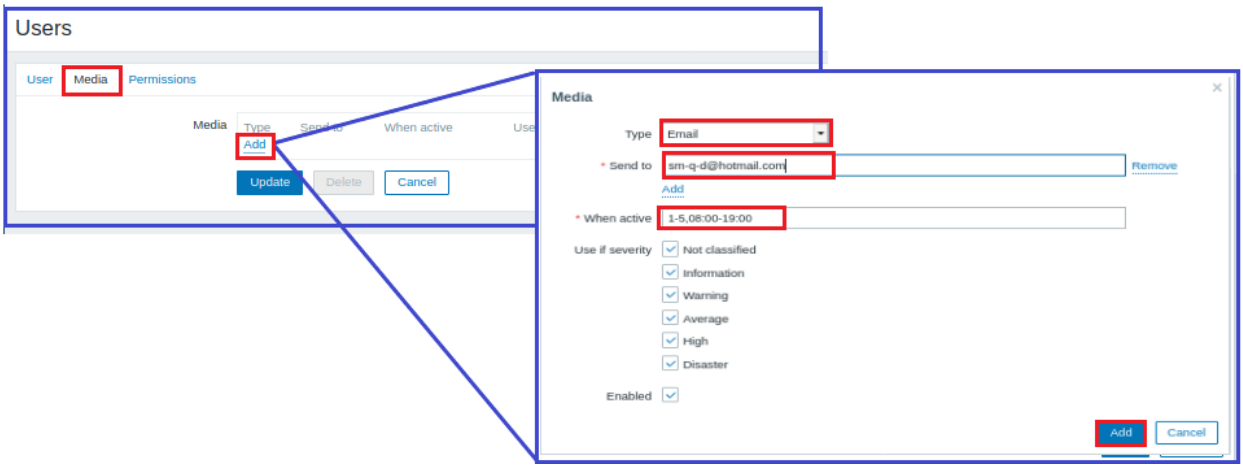


Fuente: elaboración propia.

Desde allí se selecciona la pestaña denominada “Media”, se presiona en el botón “Add”, en donde se pueden establecer el destinatario de la alerta, y el horario en el cual está activo de acuerdo con la severidad de esta. Por ejemplo, en la siguiente Figura se observa que la opción “when active” se define un string en donde 1-5 representa los días de la semana y 08:00-19:00 es el horario definido para esta cuenta de correo, se presiona el

botón add para agregarlo, y se tiene la posibilidad de agregar otros horarios y/o destinatarios para los horarios no hábiles y los tipos de alerta.

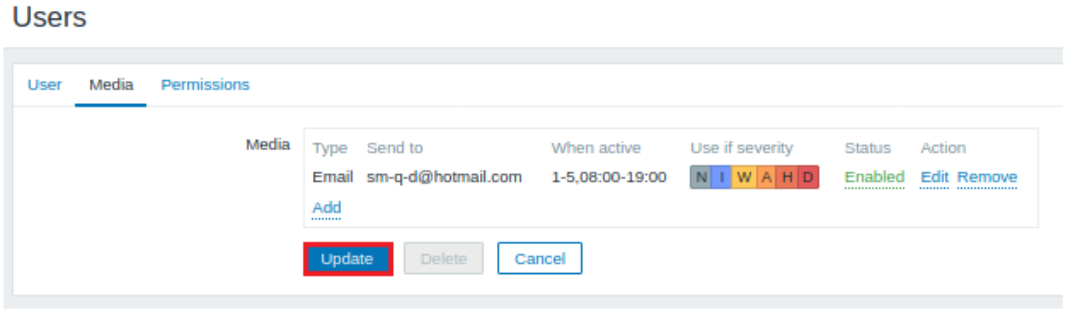
Figura 101. Definición destinario de alertas en Zabbix



Fuente: elaboración propia.

Cuando se han definido los destinatarios y horarios, se presiona el botón update para guardar los cambios como se muestra en la siguiente Figura

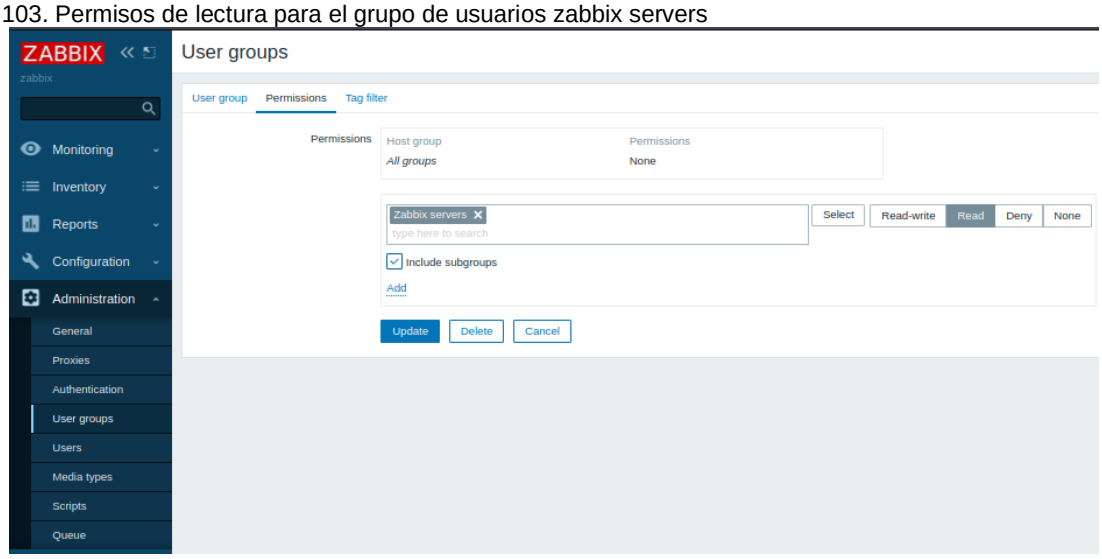
Figura 102. Medios types: definición destinatario y horario activo en Zabbix



Fuente: elaboración propia.

Además los usuarios del grupo Zabbix administrator, deben tener al menos permisos de lectura, para habilitarlo se accede al menú “Administration”, opción “user group”, pestaña “permissions”, seleccionar “zabbix servers” y finalmente clic en el botón “update”. Como se observa en la siguiente Figura. Con toda esta configuración finalmente en el momento que ocurra el problema descrito en el trigger se realiza el envío de correo en las condiciones establecidas en los pasos anteriores.

Figura 103. Permisos de lectura para el grupo de usuarios zabbix servers

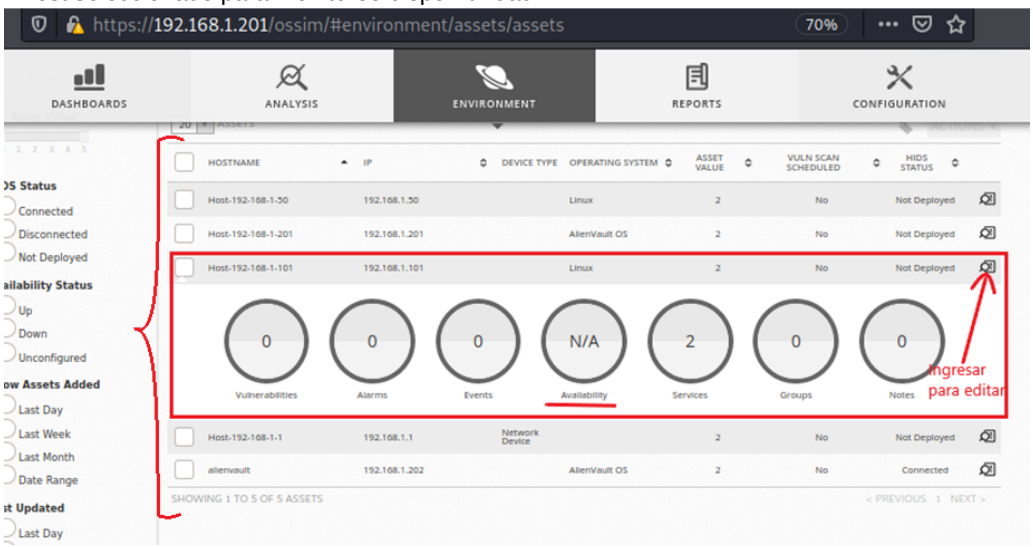


Fuente: elaboración propia.

4.4.6.2 Servidor de correlación Alienvault OSSIM. La herramienta Alienvault OSSIM, ofrece múltiples opciones de gran utilidad para la prestación de los servicios del CSIRT que la convierten en una herramienta open Source completa para la detección de intrusiones y correlación de eventos de seguridad informática sobre la infraestructura TI. Sin embargo, como ocurre con otras herramientas, es necesario realizar una correcta configuración, a través de la definición de políticas que permitan identificar comportamientos inusuales a partir de los logs recolectados. Con esto, la labor del analista de seguridad se optimiza, al no tener que revisar los cientos de logs generados y permitirle centrar su atención en eventos desencadenados por comportamientos maliciosos.

- **Monitorear disponibilidad de activos.** Es una opción que permite al administrador ver el estado de disponibilidad de los hosts de la red, Para habilitar el monitoreo de disponibilidad de los activos se accede al menú “Environment”, luego la opción “Assets and groups”, con lo cual se despliega una lista de activos, como se muestra a continuación, al seleccionar un host se puede editar presionando en el icono señalado en la Figura.

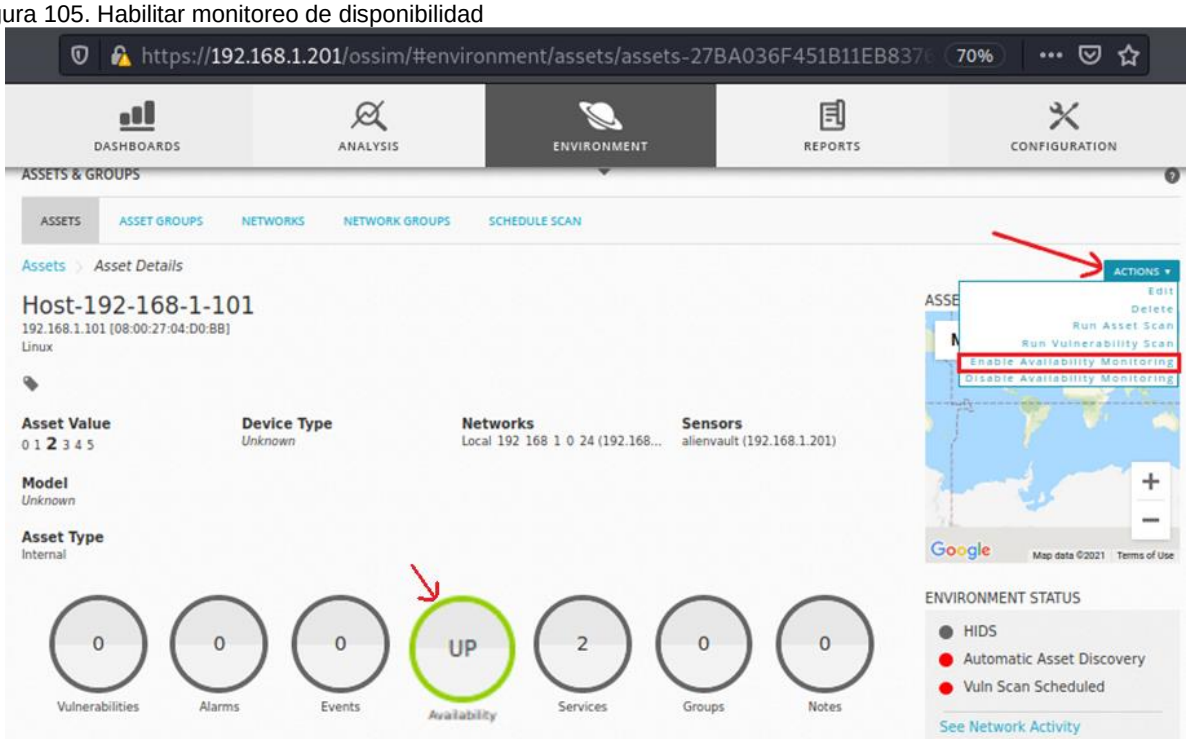
Figura 104. Host seleccionado para monitoreo disponibilidad



Fuente: elaboración propia.

En la pantalla de detalles del activo se accede al menú “Actions”, seleccionar la opción “Enable availibility monitoring”. Esta acción emite un mensaje en pantalla que indica se ha habilitado el monitoreo exitosamente, y de igual manera el icono “Availability” muestra un estado de “pending”, que posteriormente cambia a “up”.

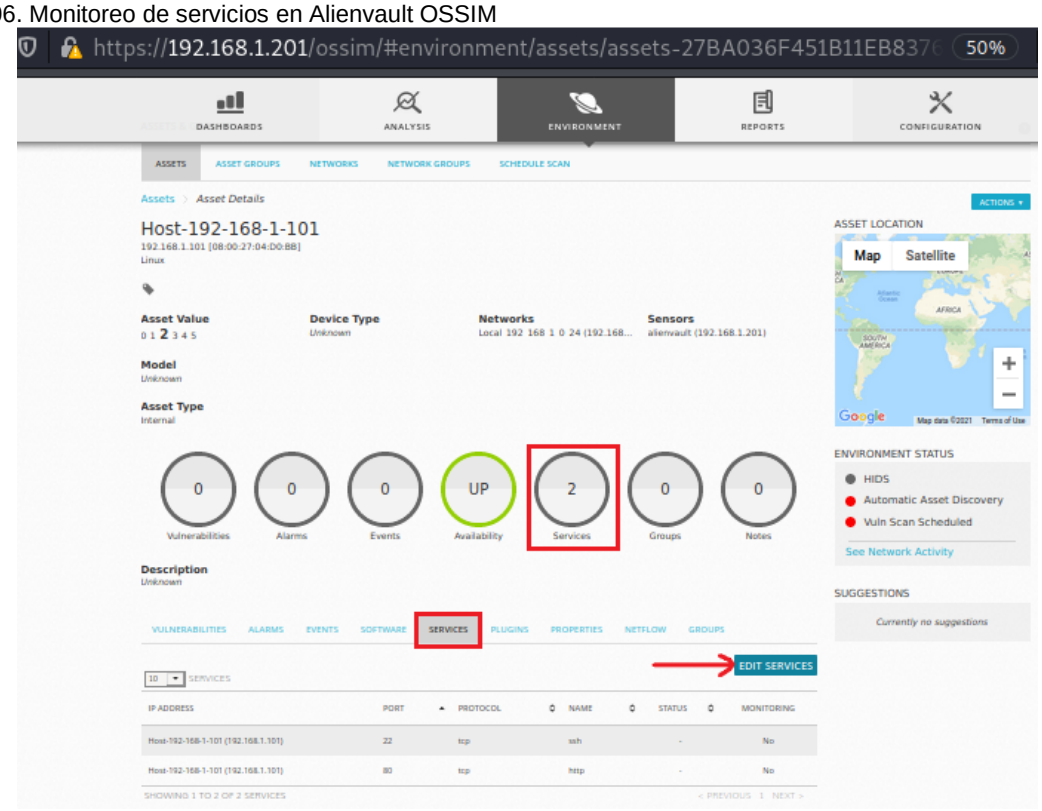
Figura 105. Habilitar monitoreo de disponibilidad



Fuente: elaboración propia.

- **Monitorear servicios.** Permite evaluar el estado de los servicios de los hosts, esta opción se encuentra en los detalles de host, donde se visualiza la detección de servicios que están ejecutando actualmente, a los cuales es posible habilitar su monitoreo. Para ello se selecciona el icono o el submenú denominado “services”, luego se selecciona el servicio y se presiona en el botón “Edit services” como se observa en la siguiente Figura.

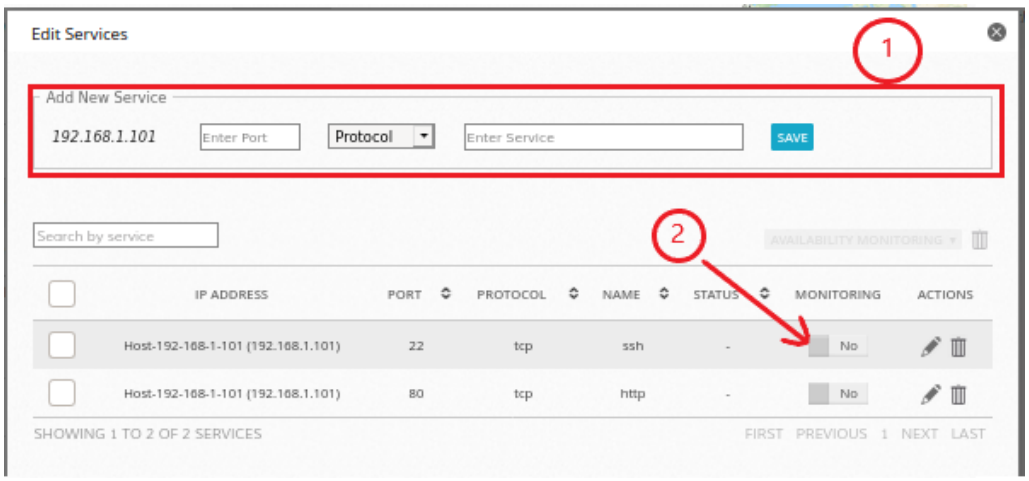
Figura 106. Monitoreo de servicios en Alienvault OSSIM



Fuente: elaboración propia.

En la ventana emergente, se tienen las opciones de agregar un nuevo servicio que no se encuentre listado desde el ítem 1 señalado en la siguiente Figura, o habilitar los que se encuentran listados, a través del switch demarcado en el ítem 2.

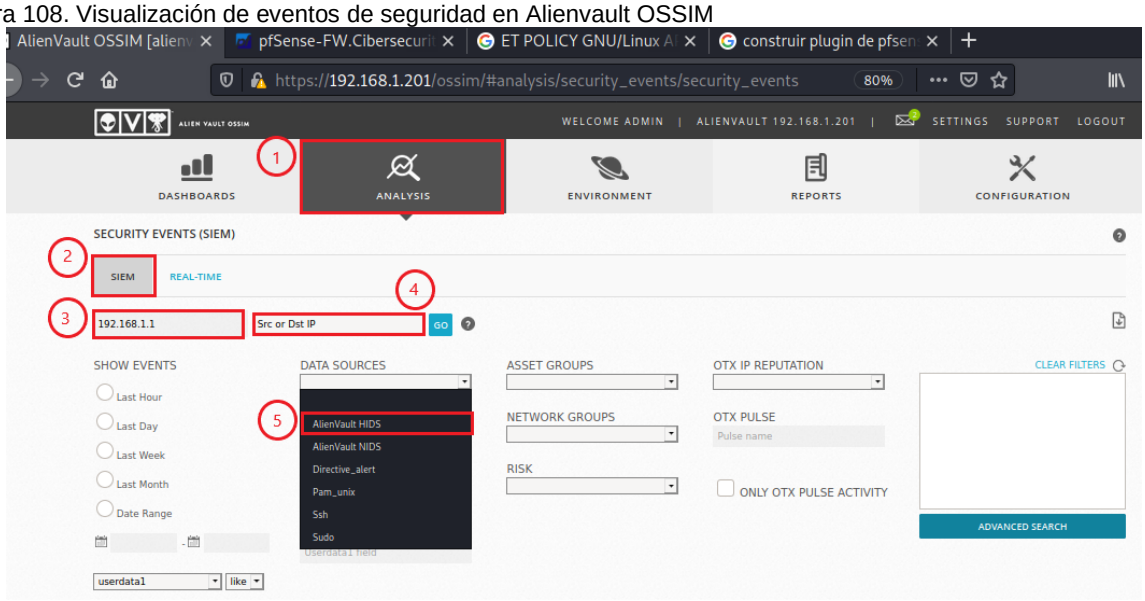
Figura 107. Habilitar monitoreo de servicios en Alienvault OSSIM



Fuente: elaboración propia.

- **Análisis de amenazas en pfSense con datasource generico**. Para evaluar el uso de Alienvault OSSIM frente a los intentos de intrusión, se dirigen algunos ataques controlados a los hosts monitoreados, como por ejemplo, intentos de autenticación fallida, con el objetivo de observar la forma cómo se interpretan este tipo de eventos. Inicialmente desde la consola de administración web del firewall pfSense, se realizan varios intentos de autenticación con datos erróneos, posterior a ello se observa en Alienvault ingresando al menú “Analysis” opción “security events SIEM”, donde se proporcionan información para filtrar los resultados de los eventos captados. En este caso, como se observa en la siguiente Figura, se ingresa la dirección ip del firewall pfSense, como tipo de parámetro se indica “Src or Dst IP, y se selecciona como “Data Source” la opción “Alienvault HIDS”, que es un plugin genérico proporcionado por la herramienta para el caso de dispositivos como pfSense que no cuentan con un datasource específico para la interpretación de los logs generados.

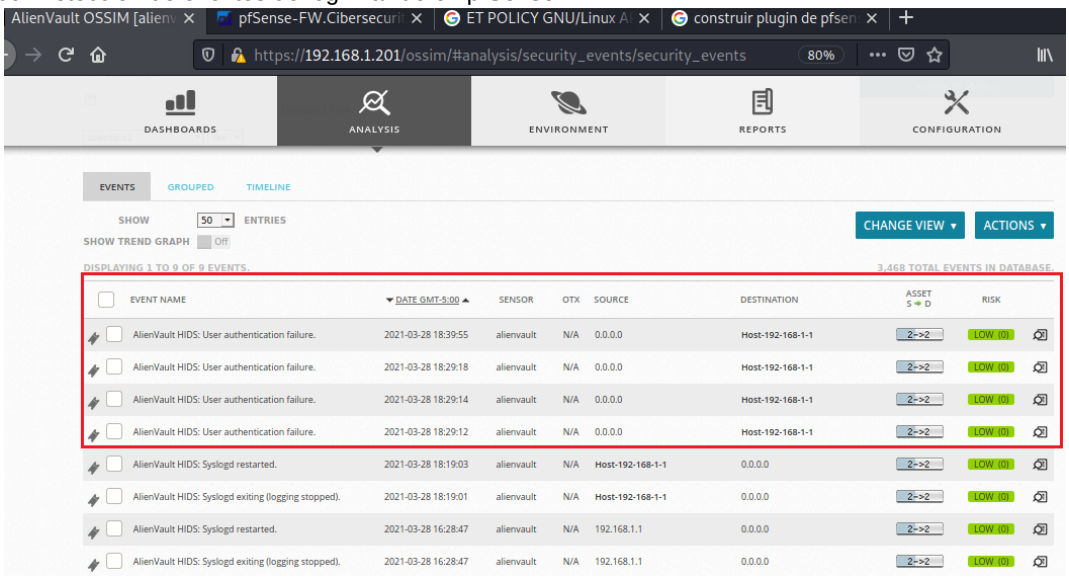
Figura 108. Visualización de eventos de seguridad en Alienvault OSSIM



Fuente: elaboración propia.

De esta manera en la parte inferior se muestra un listado con los eventos que cumplen las condiciones establecidas; en el recuadro de la siguiente Figura se puede observar, cómo la herramienta identifica este tipo de comportamiento

Figura 109. Detección de eventos de login fallido en pfSense



Fuente: elaboración propia.

Es posible obtener información detallada del log que será útil para la creación de las

políticas seleccionando uno de los registros para mostrar los detalles, tal como se muestra en la siguiente Figura, en donde se debe tener en cuenta los siguientes datos: Data Source Name, Data Source ID, y Event Type ID.

Figura 110. Detalles del evento detectado en Alienvault

Fuente: elaboración propia.

- **Creación de políticas de correlación**. Como primer paso para la creación de políticas de correlación se inicia creando una "acción" ingresando al menú "Configuration", opción "Threath Intellegence", en la nueva pantalla seleccionar la pestaña "Actions", y luego "New", tal como se muestra en la secuencia de la siguiente Figura.

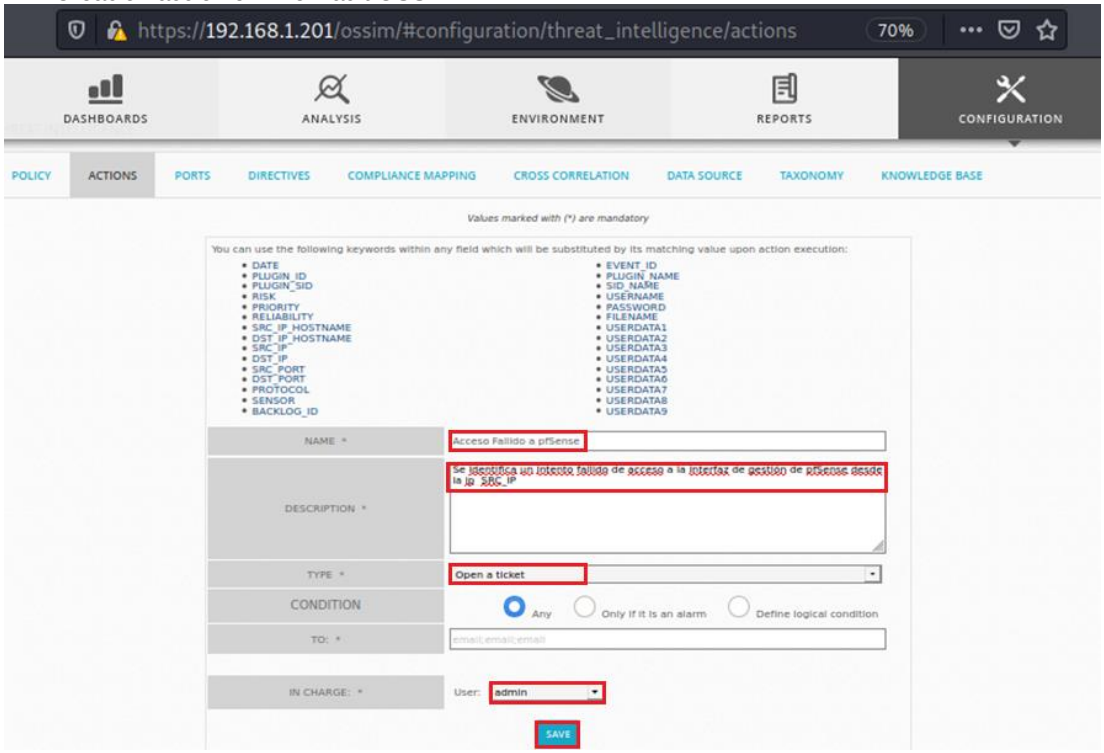
Figura 111. Pasos para crear acción en Alienvault OSSIM

Fuente: elaboración propia.

Se proporciona un nombre la acción que se va a crear, en la descripción se detalla información relacionada con el evento, en donde se pueden usar palabras claves como SRC_IP, el cual trae la dirección ip origen que viene en el log. Seguidamente se selecciona como tipo de acción "open a ticket", y se asigna a cargo del usuario "admin",

por último, se presiona el botón “save”, como se observa en la siguiente Figura.

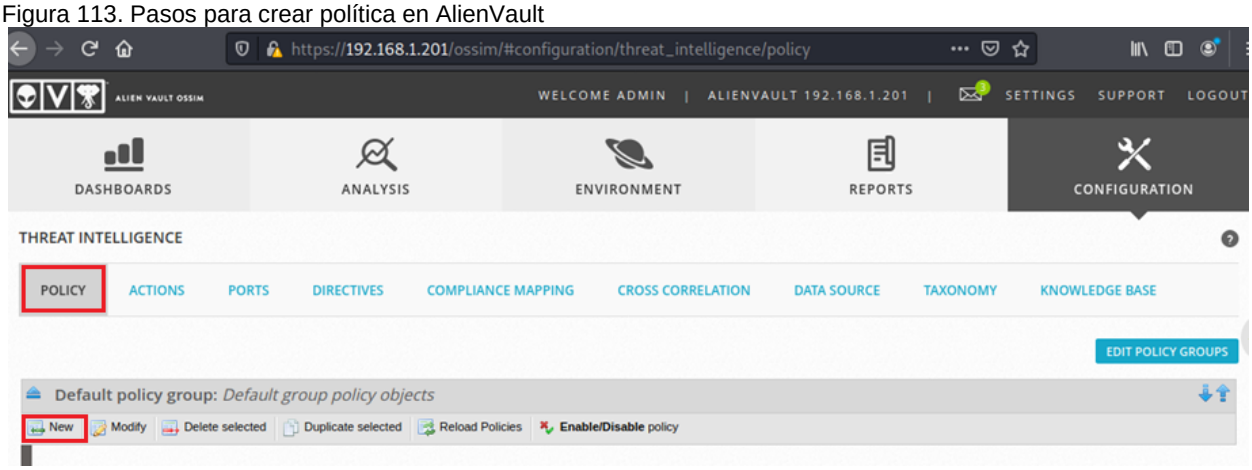
Figura 112. Creación acción en Alienvault OSSIM



Fuente: elaboración propia.

Ahora se procede a crear la política, accediendo a la opción “policy”, opción “new”, como se observa en la siguiente Figura.

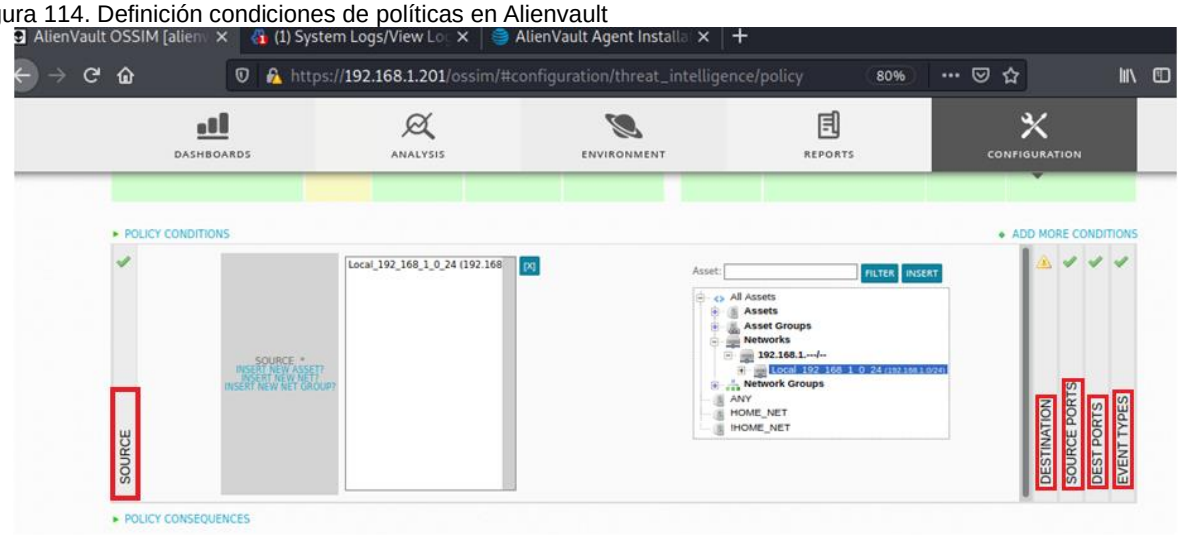
Figura 113. Pasos para crear política en AlienVault



Fuente: elaboración propia.

Se indica un nombre para la política, se desplaza a la sección denominada “Policy conditions” en donde se establecen cada uno de los parámetros que se resaltan en la siguiente Figura. En “Source” se define la red local, en “destination” se selecciona el host perteneciente a pfSense, en los puertos origen y destino se selecciona la opción “any”

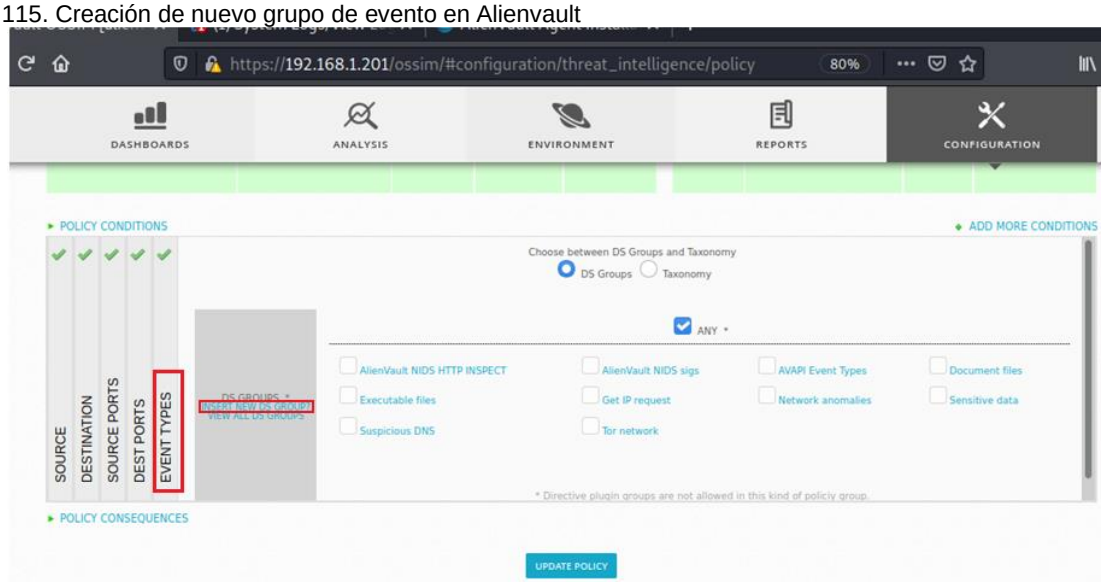
Figura 114. Definición condiciones de políticas en Alienvault



Fuente: elaboración propia.

Es de gran importancia la definición de tipo de eventos, puesto que aquí se indicará el tipo de comportamiento detectado que activará la política definida. Dentro de la opción “evento types”, y se presiona en la opción “insert new DS group”, como se indica en la siguiente Figura

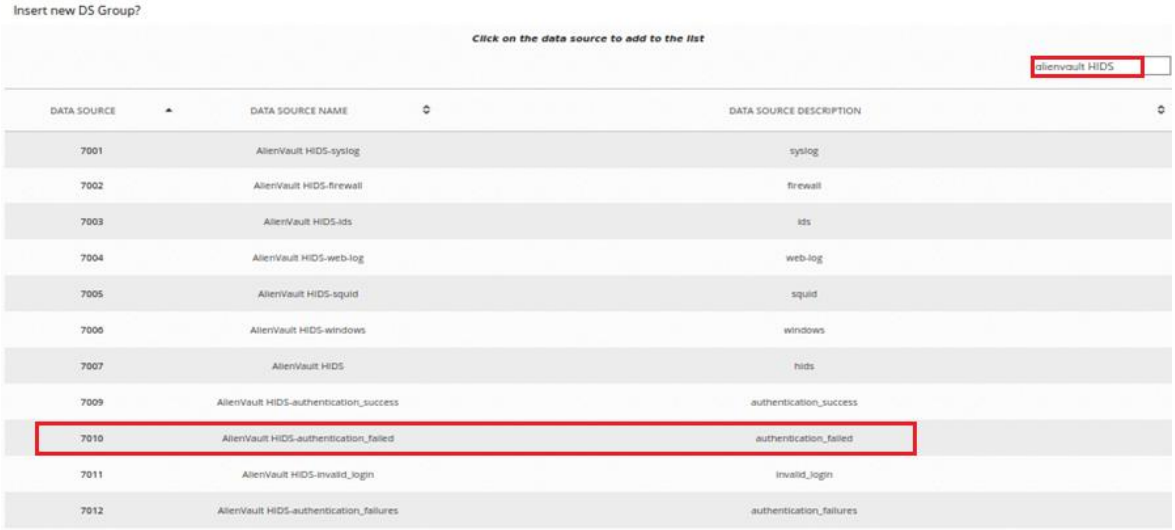
Figura 115. Creación de nuevo grupo de evento en Alienvault



Fuente: elaboración propia.

El objetivo de esta política está dirigido a crear una acción especifica (crear ticket) en cuanto se detecte un intento de autenticación fallida en el firewall pfSense, en este punto se utilizará la información extraída del análisis de eventos, de forma que identifique concretamente este evento. Con el nombre y el ID del data Source se realiza la búsqueda como se observa en la siguiente Figura

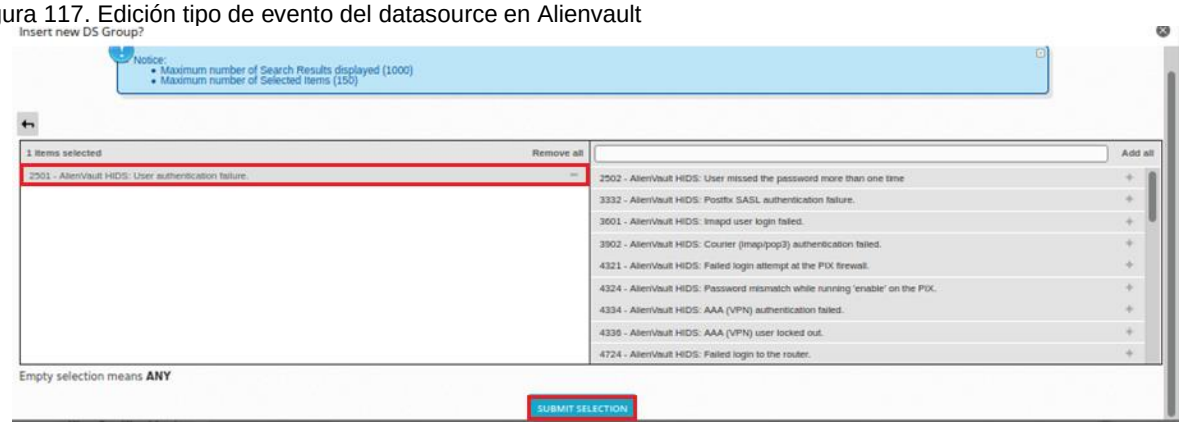
Figura 116. Definición datasource del event type en Alienvault



Fuente: elaboración propia.

Una vez seleccionado el datasource, se procede a editar para seleccionar entre los eventos que tiene definidos el id 2501, el cual identifica específicamente el evento de autenticación fallida como se muestra en la siguiente Figura

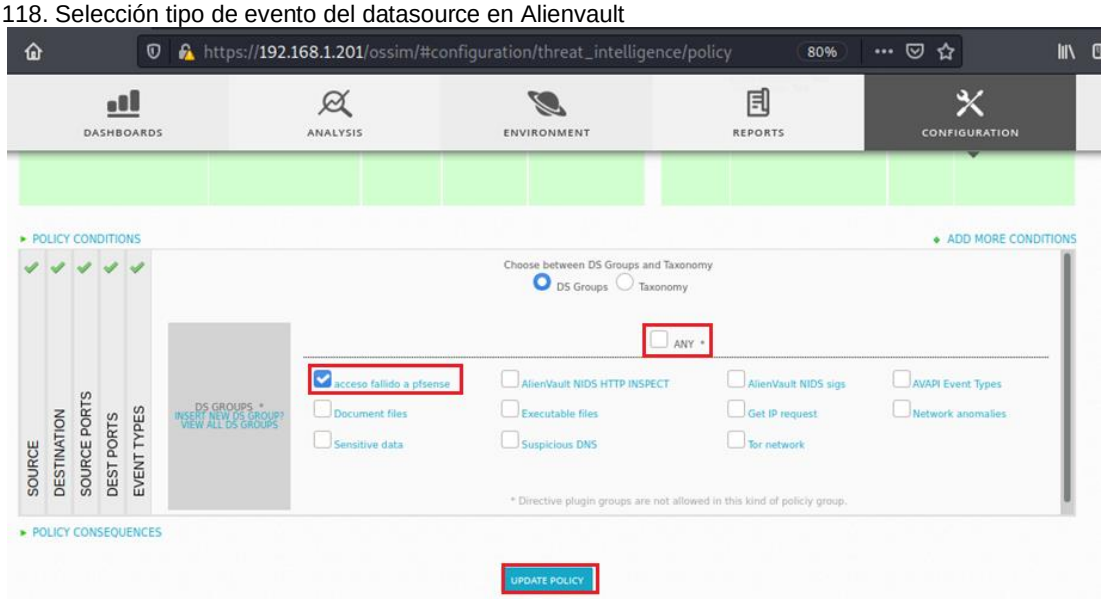
Figura 117. Edición tipo de evento del datasource en Alienvault



Fuente: elaboración propia.

Luego de agregar el datasource, se procede a seleccionarlo, desmarcando la opción “any” y marcando la opción que representa el nuevo tipo de evento, como se observa en la siguiente Figura

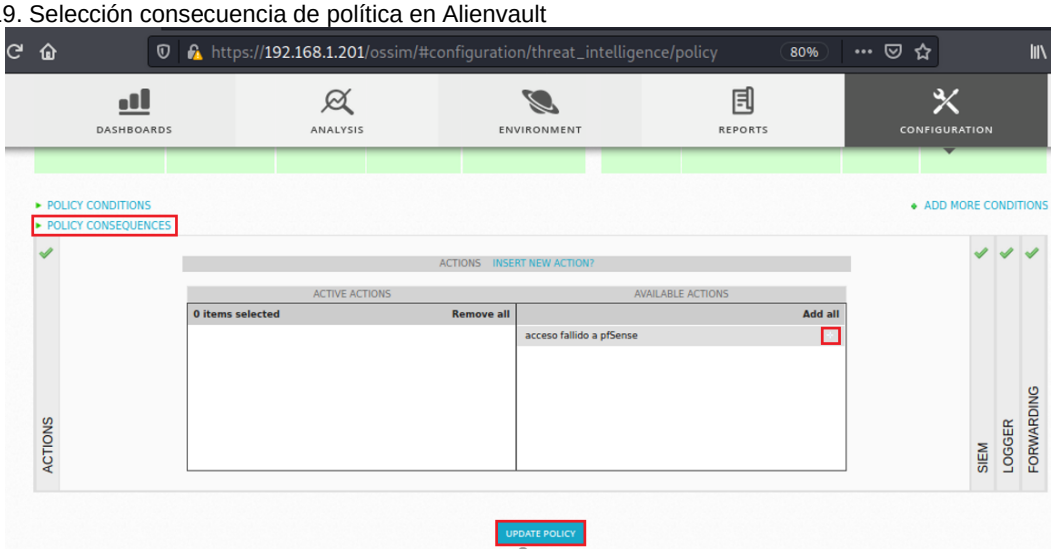
Figura 118. Selección tipo de evento del datasource en Alienvault



Fuente: elaboración propia.

Para completar la política se selecciona una consecuencia, la cual será la accion creada en el paso anterior, en la opción “Policy Consequences”, se selecciona la acción creada y se presiona en el botón más, como se observa en la Figura.

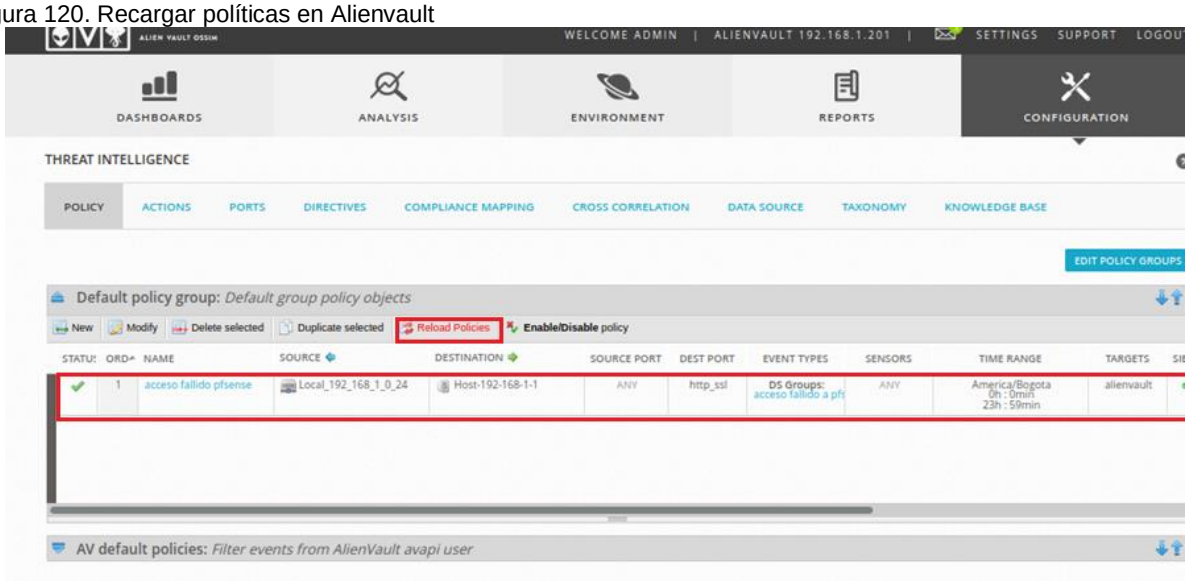
Figura 119. Selección consecuencia de política en Alienvault



Fuente: elaboración propia.

Con los pasos anteriores queda la política creada, solo resta presionar el botón “reload policies” para activarla, como se observa en la siguiente Figura

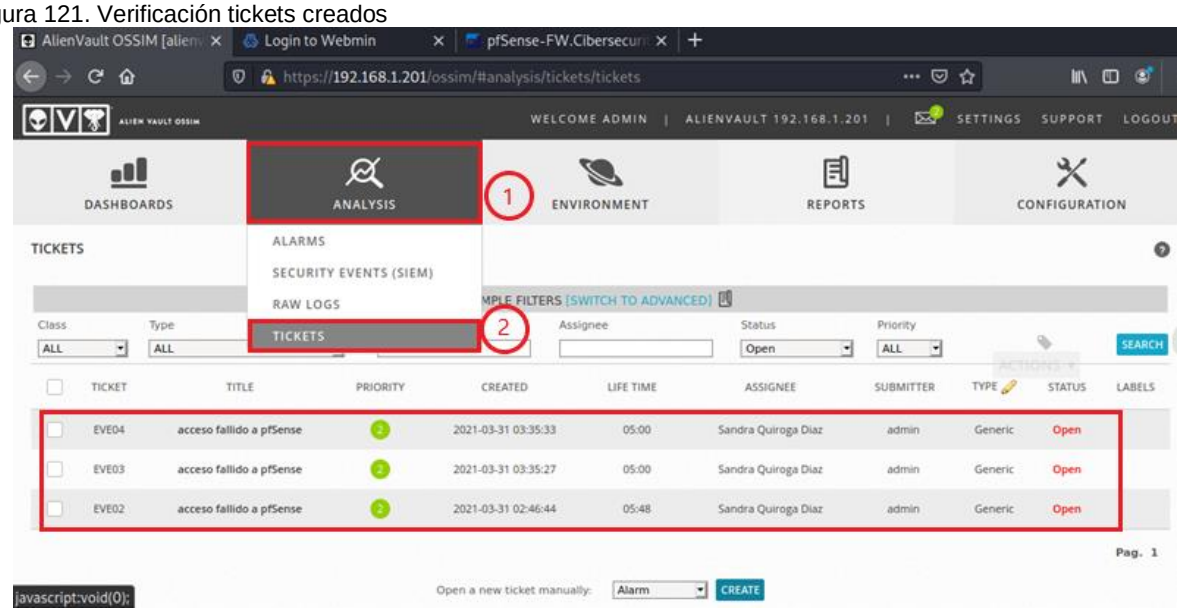
Figura 120. Recargar políticas en Alienvault



Fuente: elaboración propia.

Una vez creada la política que identificará el intento de acceso fallido al firewall pfSense, se procede a realizar nuevamente el ataque controlado para verificar que la política ejecuta la creación de un ticket en torno a dicho evento. Para ello se ingresa al menú “Analysis”, opción “Tickets”, como se observa en la siguiente Figura dentro del recuadro se observan los tickets que han sido creados.

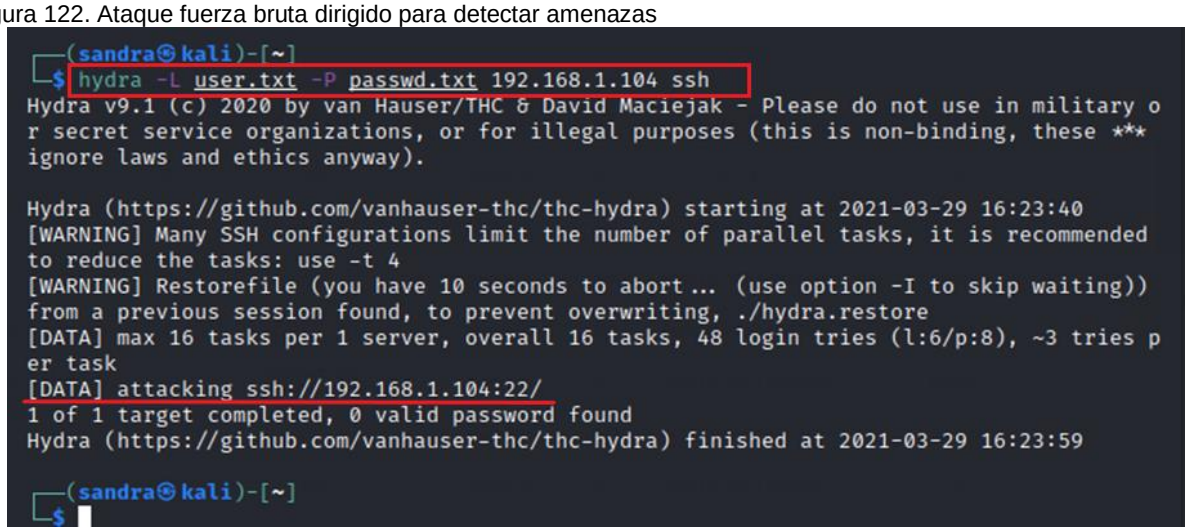
Figura 121. Verificación tickets creados



Fuente: elaboración propia.

- **Análisis de amenazas en host con agentes HIDS**. Se procede a verificar el comportamiento de las amenazas dirigidas a un host que posee un agente de detección de amenazas en ejecución y enviando información al servidor Alienvault, en este caso se dirige un ataque de fuerza bruta hacia el servidor de copias de seguridad cuya ip es 192.168.1.104. Desde la maquina Kali Linux que se encuentra en la red local se realiza el ataque con la herramienta hydra, como se observa en la siguiente Figura.

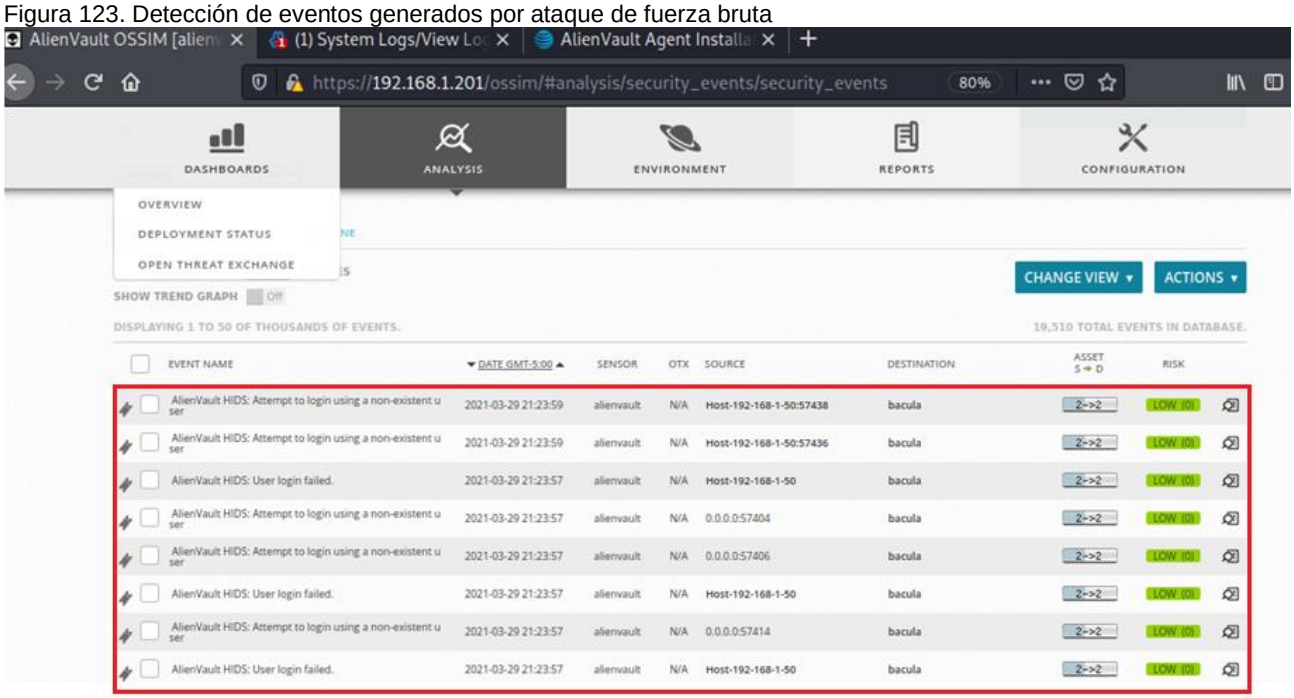
Figura 122. Ataque fuerza bruta dirigido para detectar amenazas



Fuente: elaboración propia.

Se ingresa en el menú de análisis para observar el reconocimiento del ataque lanzado por parte de Alienvault, como se observa en la siguiente Figura, el datasource genérico detecta una serie de eventos que por sí solos no aportan información concreta de lo sucedido.

Figura 123. Detección de eventos generados por ataque de fuerza bruta

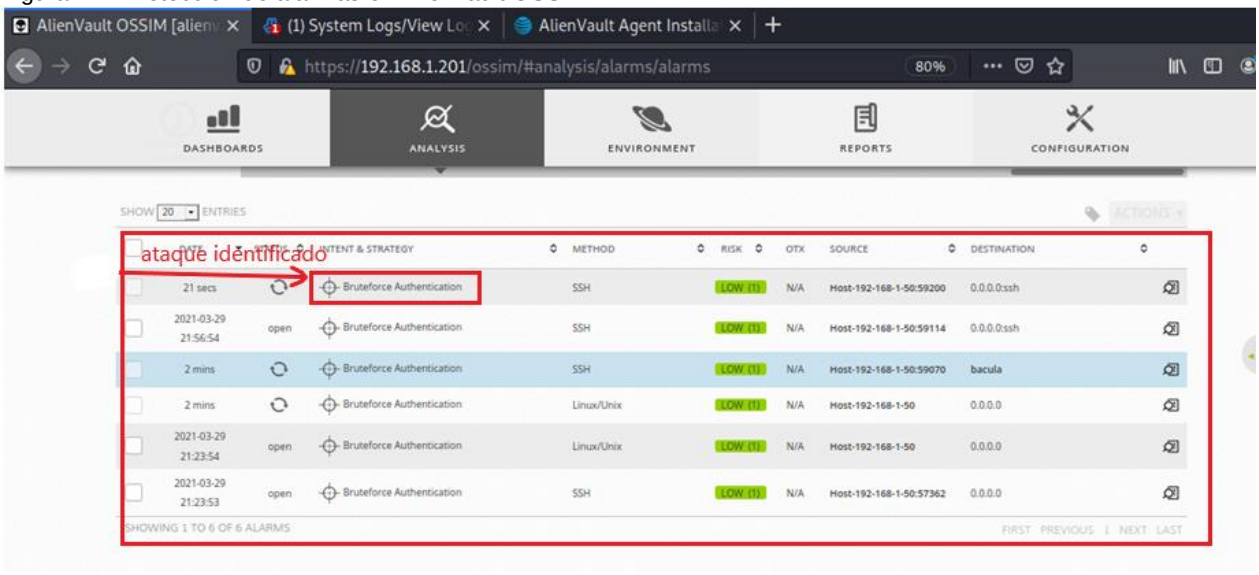


Fuente: elaboración propia.

En este caso, se procede a observar la detección de alarmas ya que este host cuenta con un agente de detección de amenazas que permite identificar ciertos ataques de acuerdo con el comportamiento de los eventos enviados al servidor

- **Detección de alarmas**. Se accede al menú “Analysis”, opción “Alarms”, como se observa en el recuadro de la siguiente Figura, se identifica el ataque lanzado de forma correcta

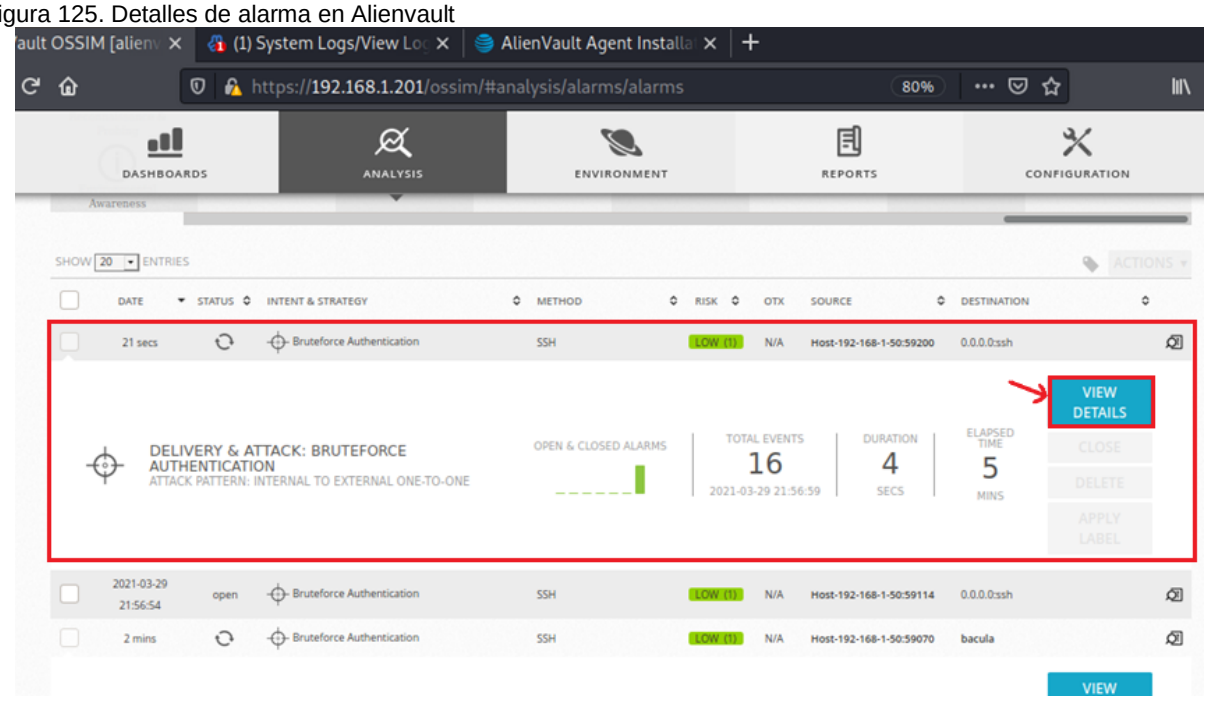
Figura 124. Detección de alarmas en Alienvault OSSIM



Fuente: elaboración propia.

Para obtener más detalles sobre la amenaza se selecciona un ítem de la lista y se presiona el botón denominado “view details”

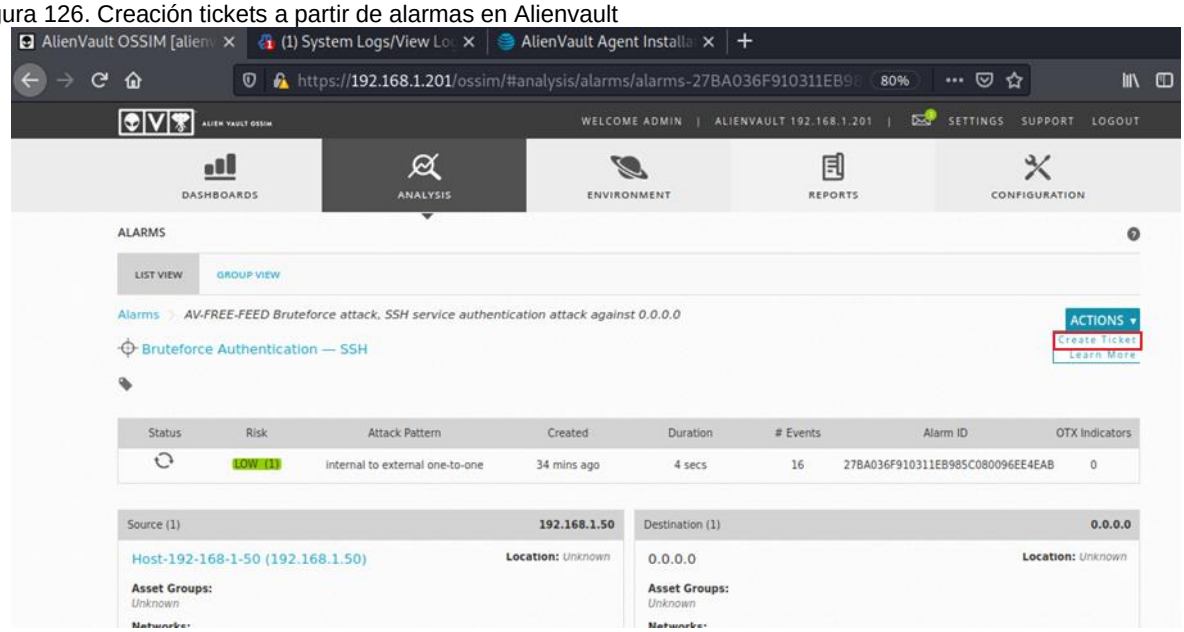
Figura 125. Detalles de alarma en Alienvault



Fuente: elaboración propia.

- **Crea ticket a partir de alarmas**. Para crear el ticket manualmente, clic en “Actions”, opción “Create Ticket”

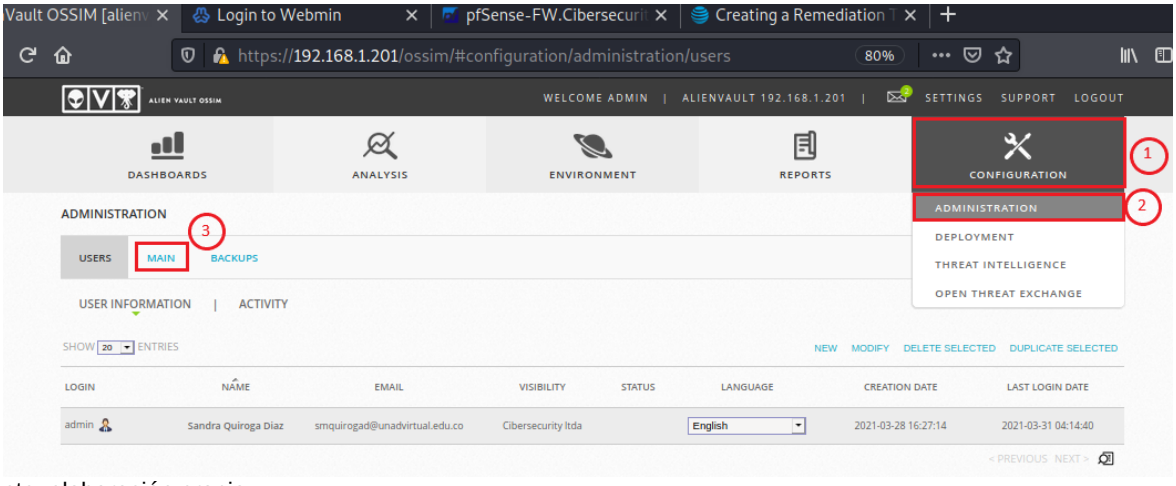
Figura 126. Creación tickets a partir de alarmas en Alienvault



Fuente: elaboración propia.

Es posible la generación de tickets de forma automática cuando se detectan alarmas. Para habilitar la creación automática de tickets se ingresa al menú “Configuration”, opción “Administration”, pestaña denominada “Main” como se observa en la secuencia descrita en la siguiente Figura.

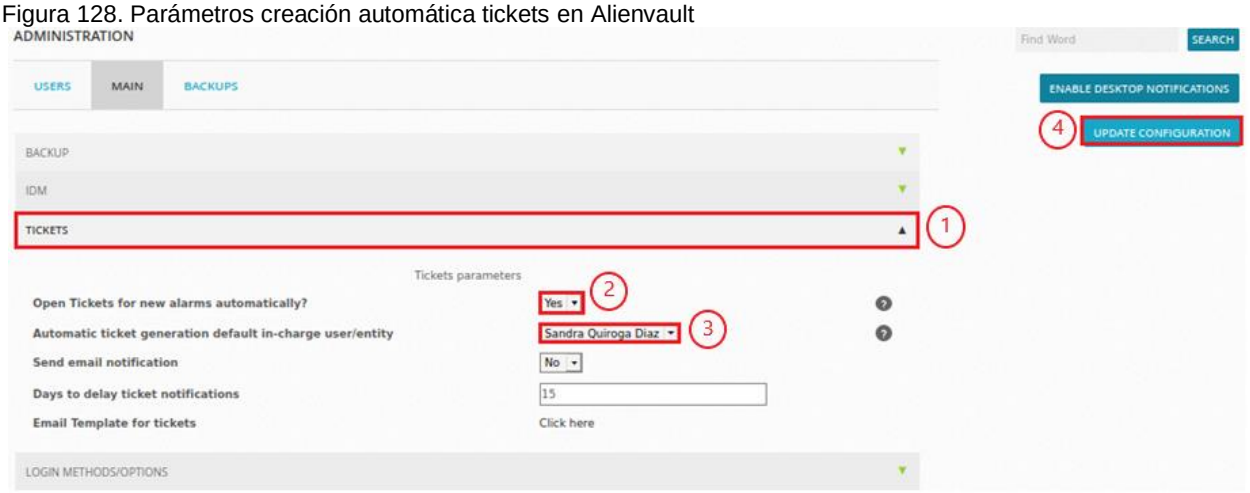
Figura 127. Acceso a la creación automática de tickets en Alienvault



Fuente: elaboración propia.

Se ingresa en el menú tickets, se habilita la apertura automática a partir de alarmas, seleccionar el usuario al que se asignara y por último presionar el botón “update configuration”, como se observa en la siguiente Figura.

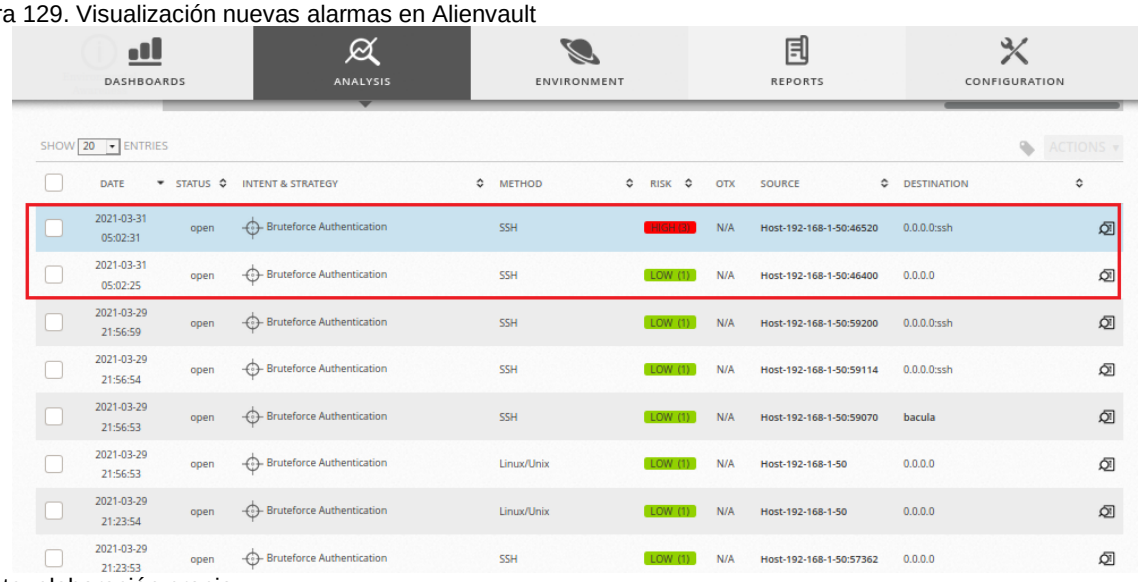
Figura 128. Parámetros creación automática tickets en Alienvault



Fuente: elaboración propia.

De esta manera, si se intenta nuevamente un ataque con hydra se generan nuevamente las alarmas que se visualizan desde la opción de “Alarms”, como se observa a continuación.

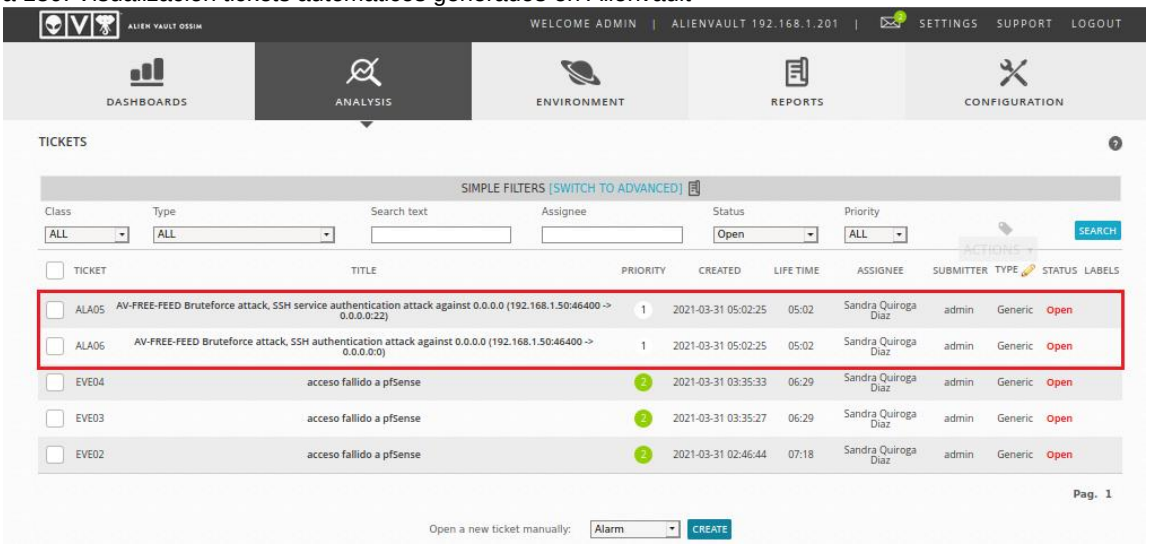
Figura 129. Visualización nuevas alarmas en Alienvault



Fuente: elaboración propia.

Así mismo, al ingresar al menú “Analysis" opción “Tickets” se visualizan los nuevos tickets generados.

Figura 130. Visualización tickets automáticos generados en Alienvault



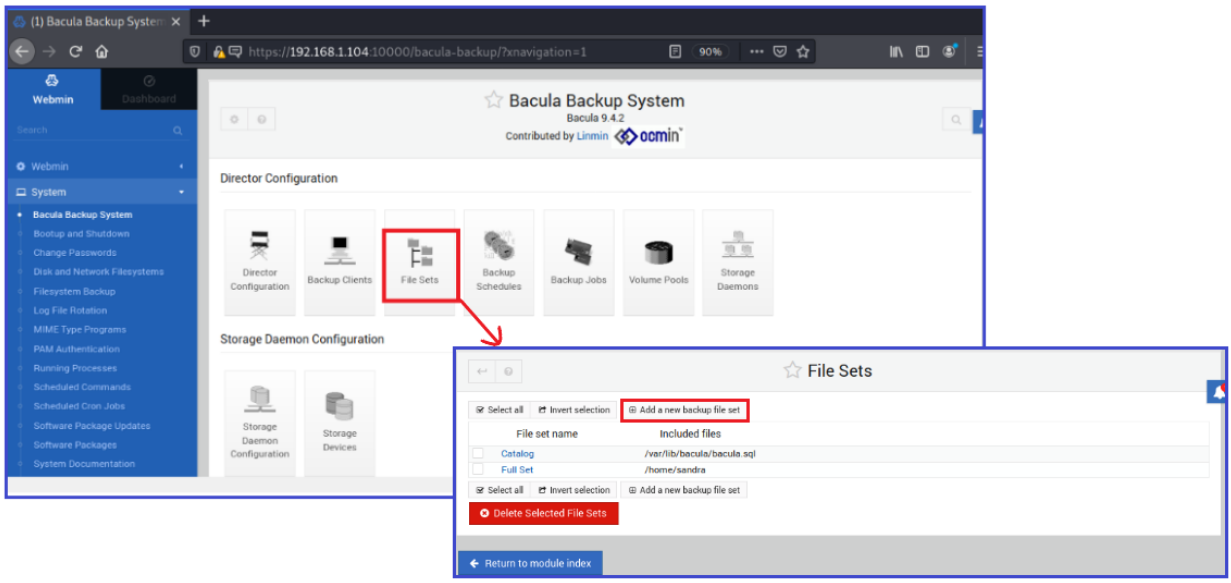
Fuente: elaboración propia.

4.4.6.3 Servidor Bacula. Una vez configurado el servidor, los agentes de copias de seguridad y confirmada la comunicación entre ellos, se definen los parámetros para la ejecución de los principales procesos que se llevaran a cabo en él: creación de copias y restauración,

- **Creación de copias de Seguridad**

Definición de archivos a respaldar. Una vez agregado el cliente se define el conjunto de archivos al cual se le aplicara la copia de seguridad con cada trabajo, presionando la opción “File Set” luego el botón “Add a new backup file set”, como se observa en la siguiente Figura

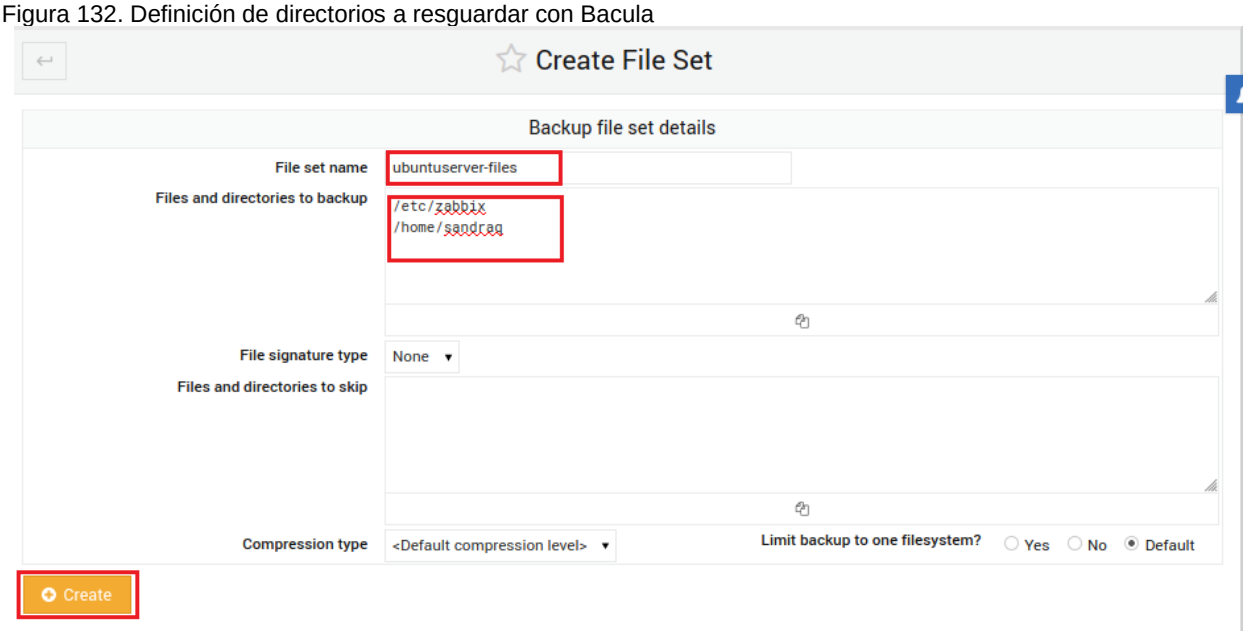
Figura 131. Definición FileSet de copia de seguridad en Bacula



Fuente: elaboración propia.

En la página que se abre se establece un nombre que identifique al fileset, en el segundo recuadro se enumeran las rutas en donde se encuentran los archivos a respaldar, adicionalmente se puede establecer el tipo de compresión y si se quiere limitar el tamaño de la copia, para este caso, se dejan los valores por defecto en estas últimas opciones y se presiona en el boton “create” como se observa en la Figura

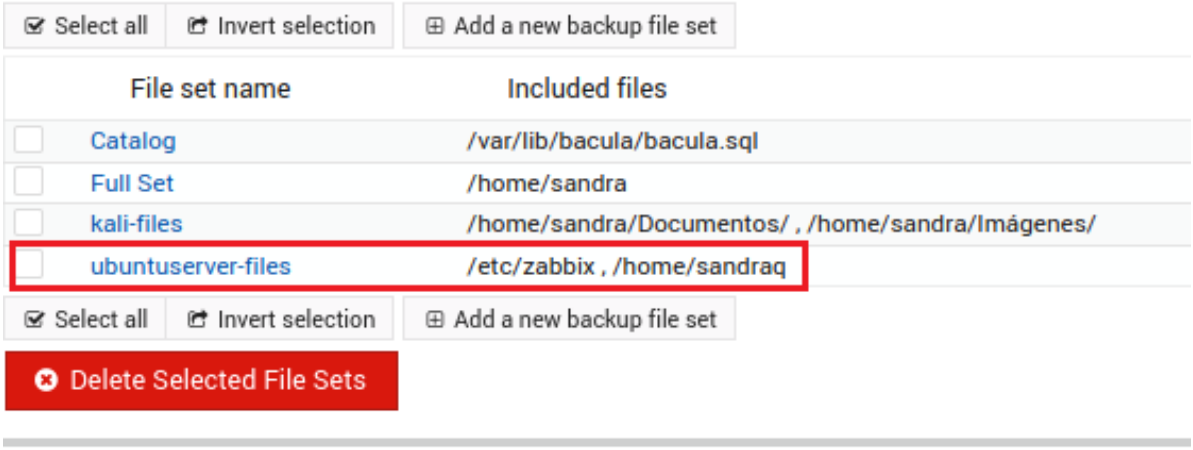
Figura 132. Definición de directorios a resguardar con Bacula



Fuente: elaboración propia.

Al terminar se observa que aparece los nuevos file set en el listado como se evidencia en la siguiente Figura

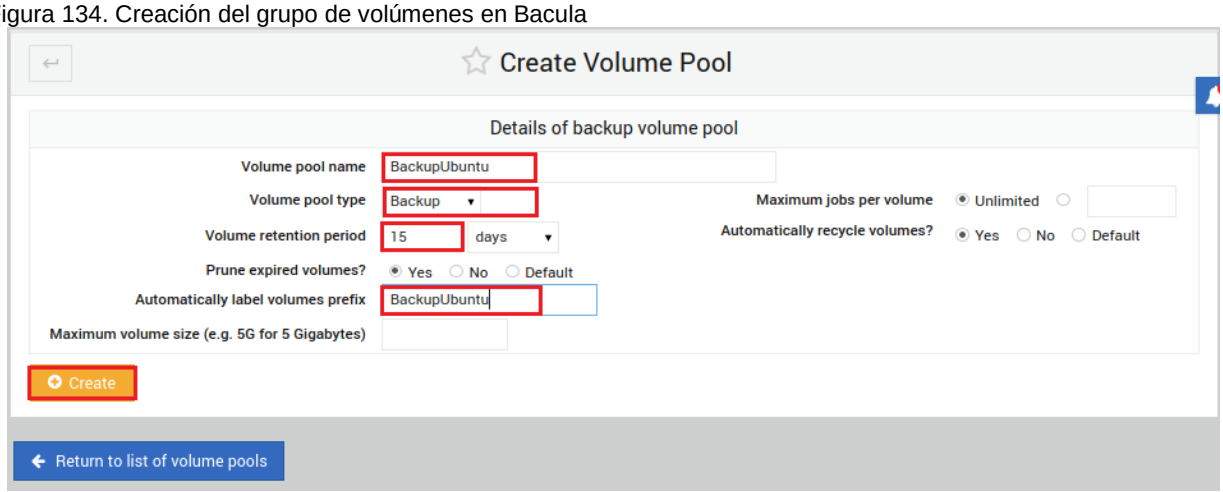
Figura 133. Nuevo Fileset agregado en Bacula



Fuente: elaboración propia.

Definición de Volumenes. Volume Pools, son unidades de almacenamiento que solo puede entender bacula, que permiten definir el grupo de volúmenes que se utilizaran para un trabajo en particular, facilitando también la delimitación de trabajos o clientes a cierto volumen o grupo de volúmenes. La configuración se inicia presionando el botón “Volume Pools” , luego en la opción “Add a new volumen pool”. En la nueva página se configuran el nombre del volumen, el tipo que será backup, el periodo de retención del volumen entre otras opciones, de acuerdo con lo que se observa en la siguiente Figura

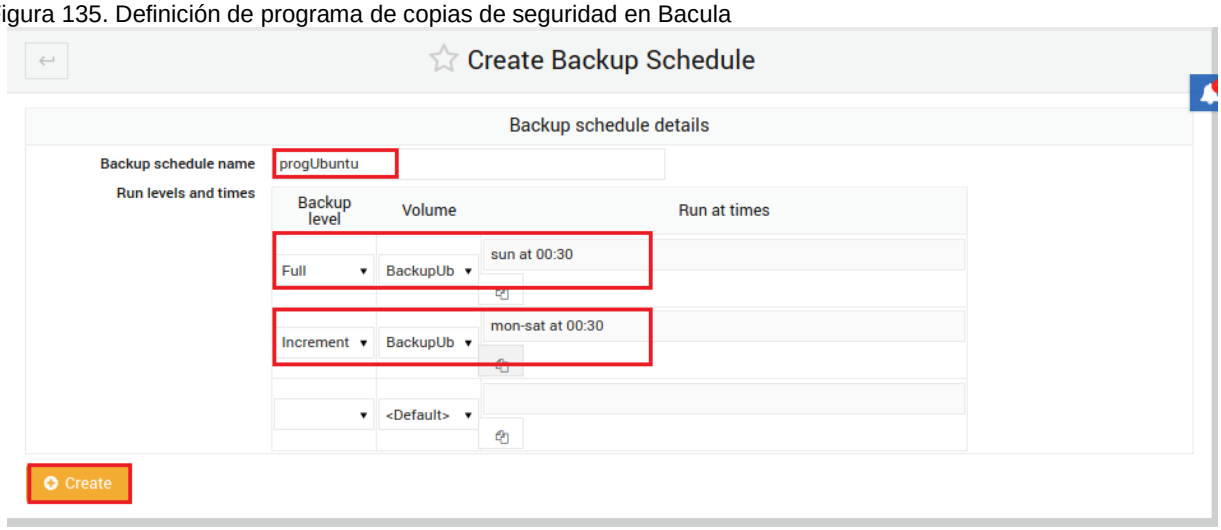
Figura 134. Creación del grupo de volúmenes en Bacula



Fuente: elaboración propia.

Definición de programa de copias. Posteriormente se configura la opción de programación de horario de realización de las copias, seleccionando la opción “Backup Schedules”, luego “Add a new backup Schedule”. Allí se establecen las propiedades como: nombre para la programación, nivel de la copia de seguridad, volumen en el que se guardará y el horario en el cual se realizará, para éste caso se crea una programación para el servidor Ubuntu, en la cual se realice una copia full, todos los domingos de cada semana, y una copia incremental de lunes a sábado después de medianoche.

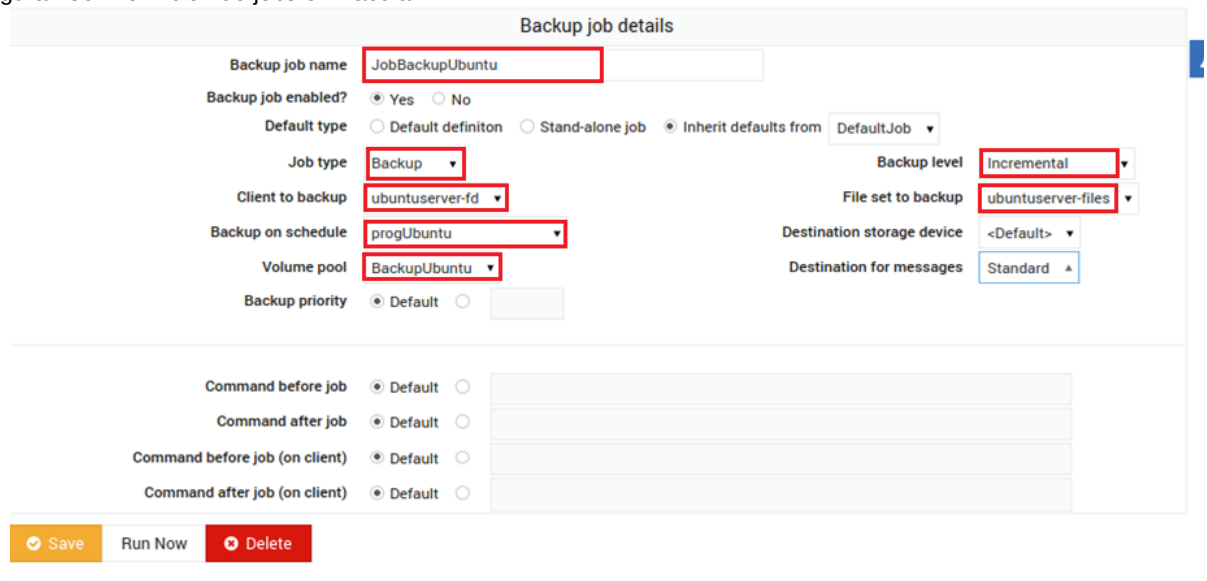
Figura 135. Definición de programa de copias de seguridad en Bacula



Fuente: elaboración propia.

Definición de trabajos a realizar. En la opción Backup Jobs, se define los trabajos que se realizarán para cada cliente, esto permite personalizar cada agente de acuerdo con sus necesidades particulares. Una vez ingresa en Backups Jobs se presiona en la opción “**add a new backup job**”, con lo cual se abre una nueva ventana como se observa en la Figura 136, en donde se debe iniciar estableciendo un nombre para el trabajo, el tipo de trabajo, indicar el cliente sobre el cual se ejecutará, los archivos a copiar, la programación definida previamente y el volumen en donde se guardará la información. Para finalizar se presiona el botón “create”

Figura 136. Definición de jobs en Bacula



Fuente: elaboración propia.

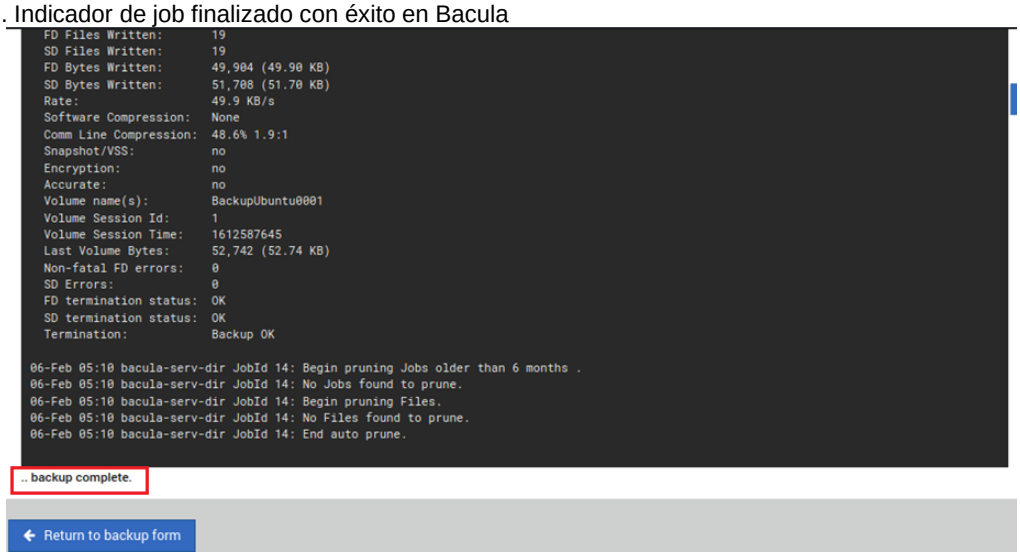
Ejecución de trabajos. Después de definir el trabajo la ejecución se pone en marcha ingresando en el menú “Bacula Backup System”, luego en el icono “Backup Jobs”, por último la opción “Run Backup Job”, esto desencadenara la ejecución del proceso en el servidor y se muestra el conjunto de tareas realizadas como se muestra en la siguiente Figura.

Figura 137. Ejecución de jobs en Bacula

Fuente: elaboración propia.

El indicador de que la operación fue exitosa se puede observar en el mensaje resaltado en la siguiente Figura

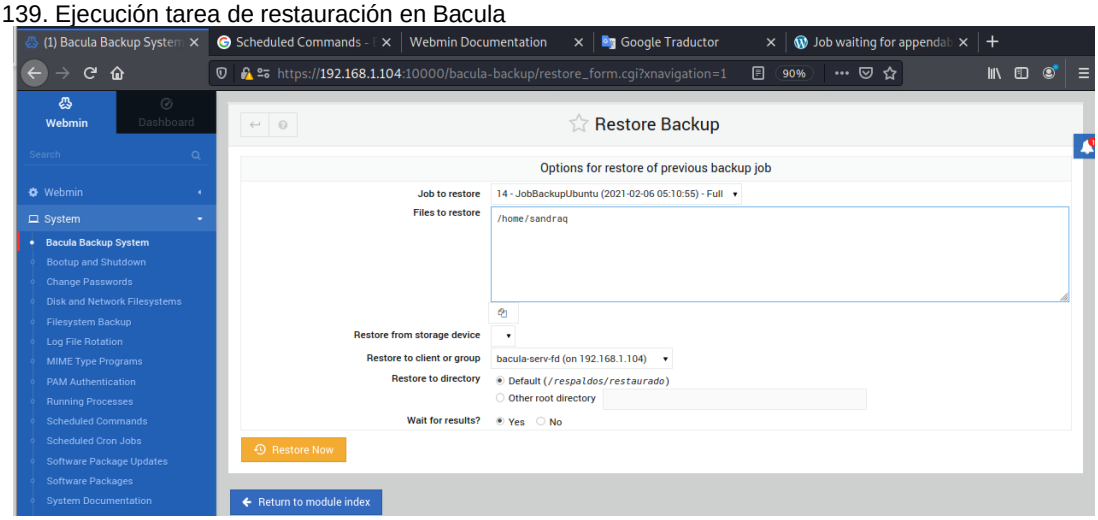
Figura 138. Indicador de job finalizado con éxito en Bacula



Fuente: elaboración propia.

- **Restauración de copias de Seguridad.** La restauración de las copias realizadas se ejecuta desde el menú “Bacula Backup System”, en la opción “Restore Backups”, se despliega una ventana en donde se debe indicar el nombre del trabajo que se desea restaurar y se presiona el botón “Restore Now”, como se observa en la Figura 139. este proceso realiza la restauración de los archivos en la ubicación que fue definida al momento de configurar el Director de bacula en el servidor.

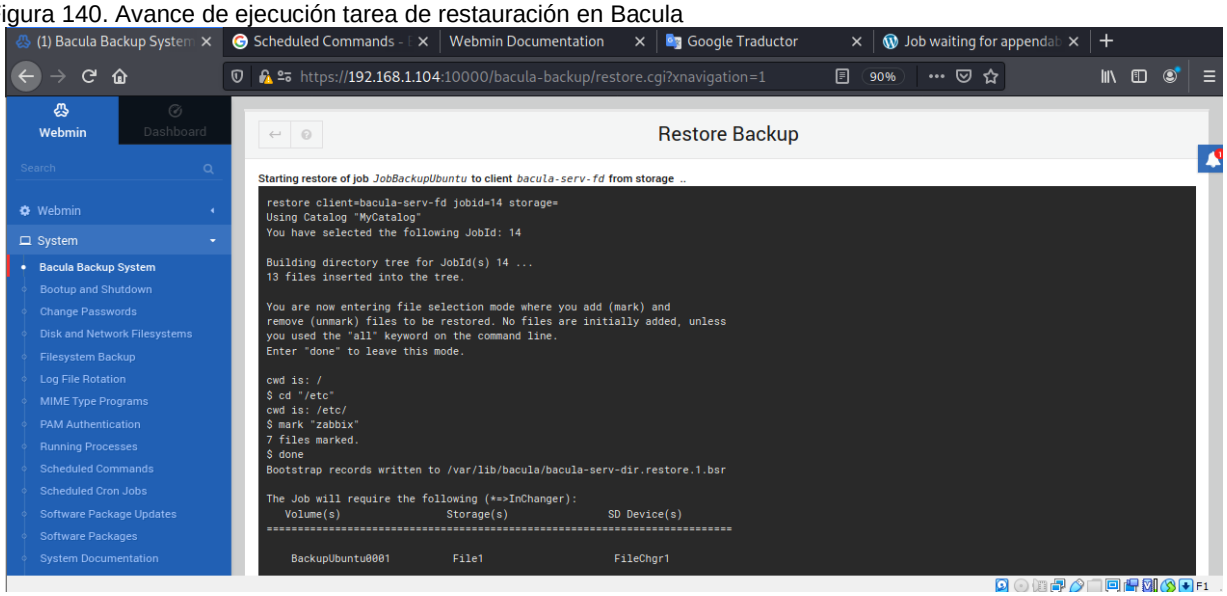
Figura 139. Ejecución tarea de restauración en Bacula



Fuente: elaboración propia.

Cuando se inicia el proceso se muestra el avance de las tareas realizadas como se observa en la siguiente Figura.

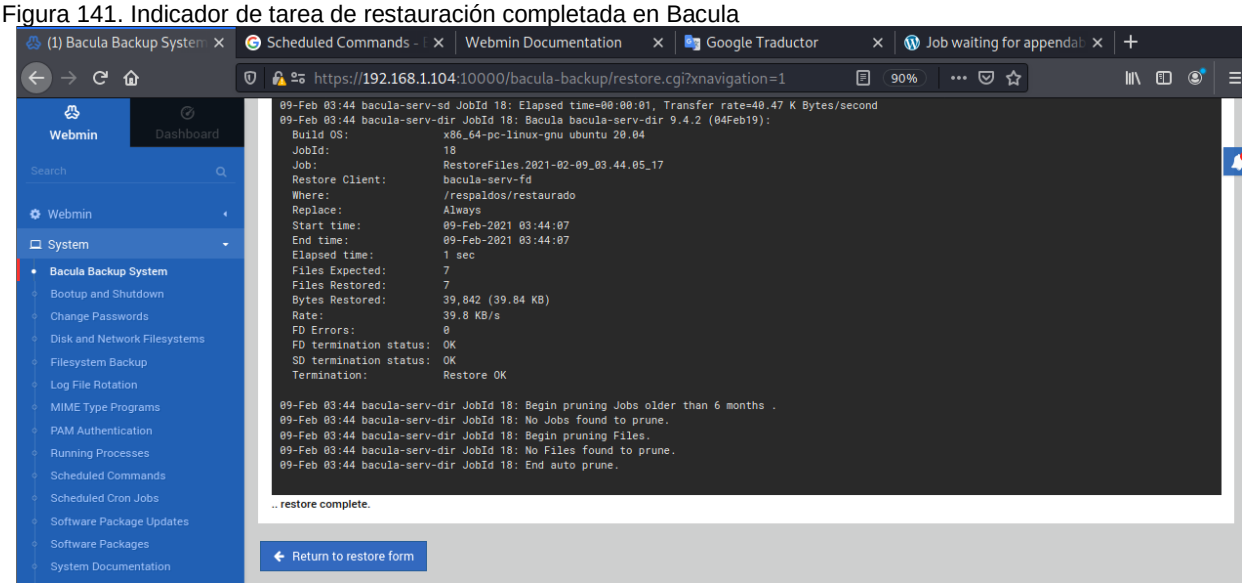
Figura 140. Avance de ejecución tarea de restauración en Bacula



Fuente: elaboración propia.

Como indicador de la finalización exitosa del proceso, se muestra un mensaje al final: "…restore complete." como se observa en la siguiente Figura.

Figura 141. Indicador de tarea de restauración completada en Bacula

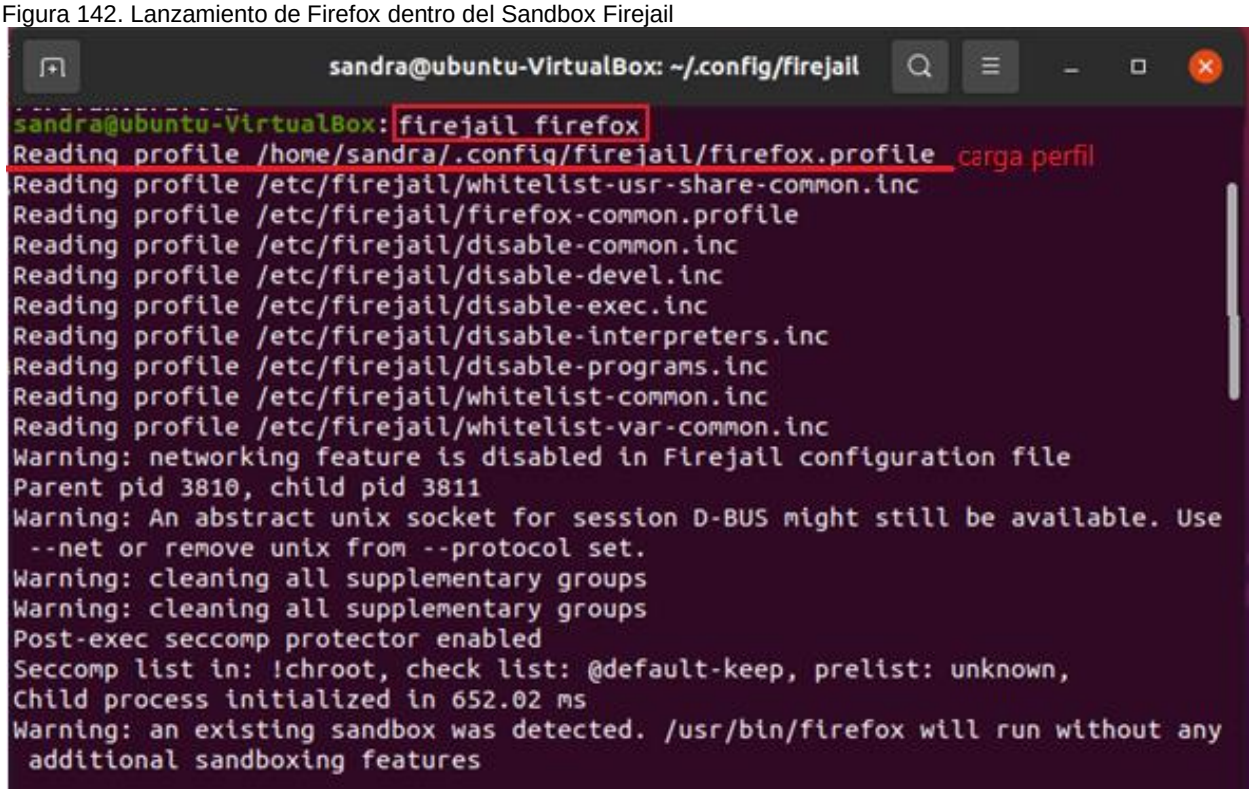


Fuente: elaboración propia.

4.4.6.4 Servidor sandbox Firejail.

- **Lanzar aplicación en la caja de arena**. Para lanzar una aplicación dentro del sandbox, se abre una ventana de terminal y se emite el comando firejail, seguido del nombre de la aplicación, por ejemplo, en la Figura 142 se observa cómo lanzar Firefox.

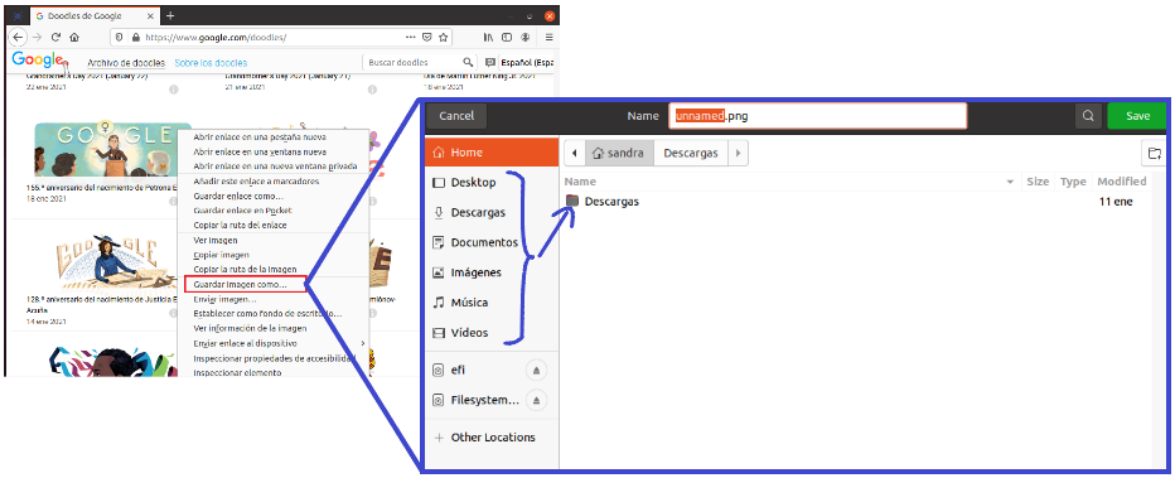
Figura 142. Lanzamiento de Firefox dentro del Sandbox Firejail



Fuente: elaboración propia.

Lo que sucede exactamente es que Firejail cargó un perfil denominado Firefox.profile, que va a determinar con precisión las diferentes cosas a las que Firefox tiene acceso, ya sea la red o los directorios en la máquina. El perfil de seguridad preconfigurado restringe el acceso a los archivos contenidos en el directorio home, para comprobarlo intentamos guardar localmente archivo desde cualquier página web, como se observa en la siguiente Figura, cualquier directorio que se selecciones abrirá solamente el directorio de descargas, el cual es el único permitido.

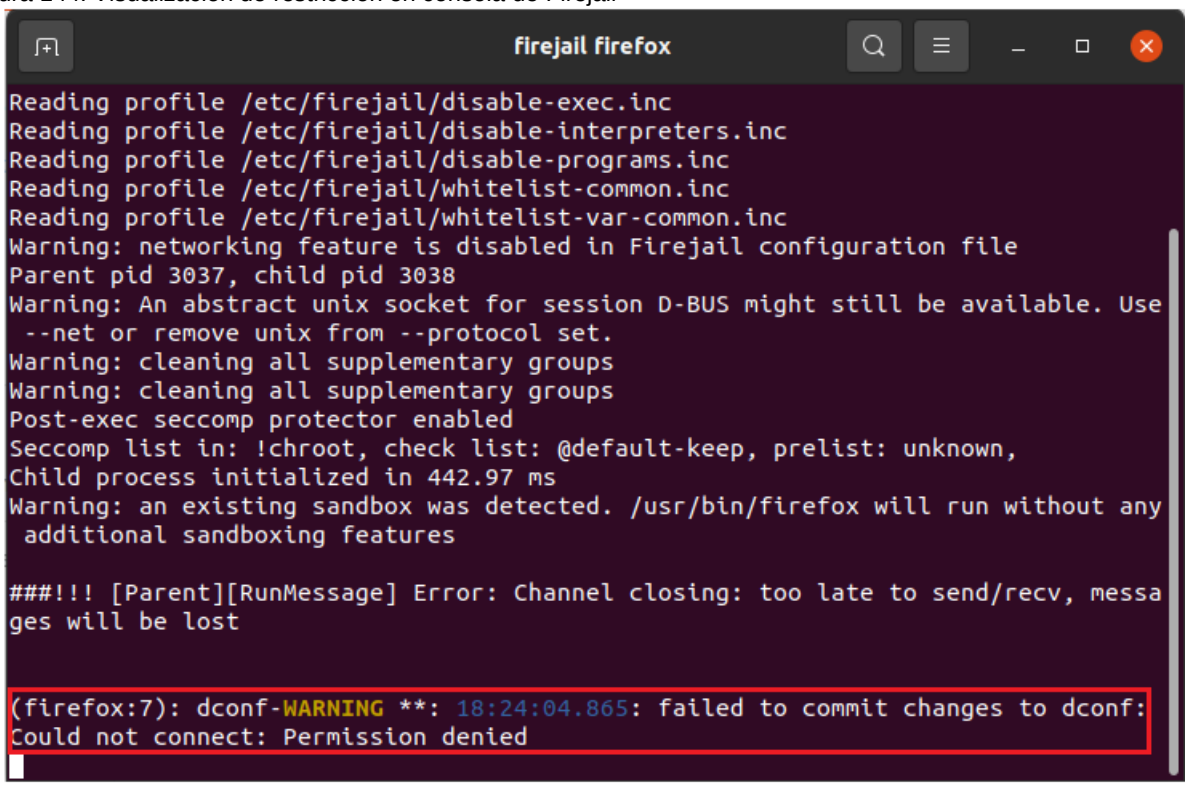
Figura 143. Prueba de restricción de acceso de Firejail



Fuente: elaboración propia.

En la ventana de comandos se observa que se emite un mensaje de error al intentar guardar en otro directorio como se evidencia a continuación, con lo cual se consigue un aislamiento total de navegador, y si por ejemplo, se da el caso de que exista una extensión maliciosa en Firefox, ésta no podría acceder al directorio de documentos.

Figura 144. Visualización de restricción en consola de Firejail

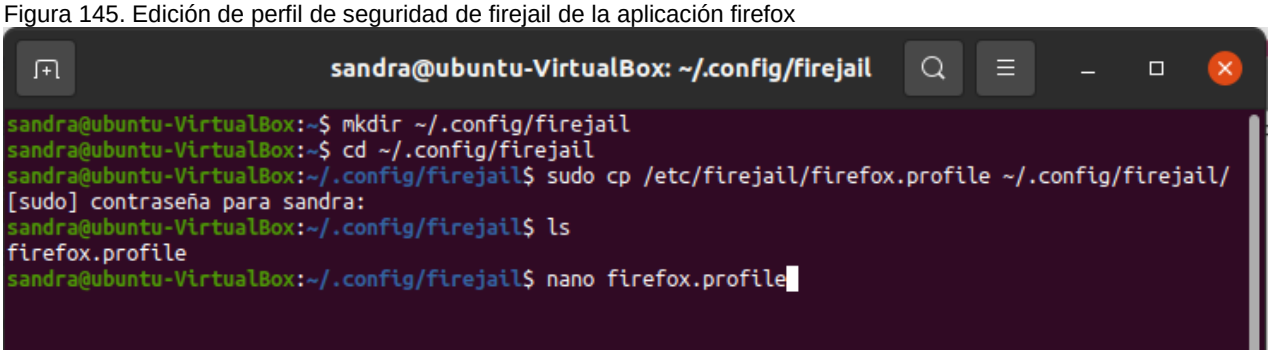


Fuente: elaboración propia.

- **Configuración perfiles de seguridad.** Firejail permite generar entornos aislados para la ejecución de aplicaciones, pero no trabaja por si solo, es importante definir en los perfiles de cada aplicación la configuración que se adecue a las necesidades propias de cada situación. Firejail tiene preconfigurados dentro del directorio /etc/firejail, más de 400 perfiles de seguridad para las aplicaciones más comunes de Linux, que permiten definir las capacidades particulares para cada una de ellas, lo cual incluye aspectos como sockets, acceso a la red o al sistema de archivos.

Para configuración de un perfil de firejail, se recomienda crear una copia del original en el directorio ~/.config/firejail y posteriormente editarlo, como se puede apreciar en la siguiente Figura con el perfil de Firefox

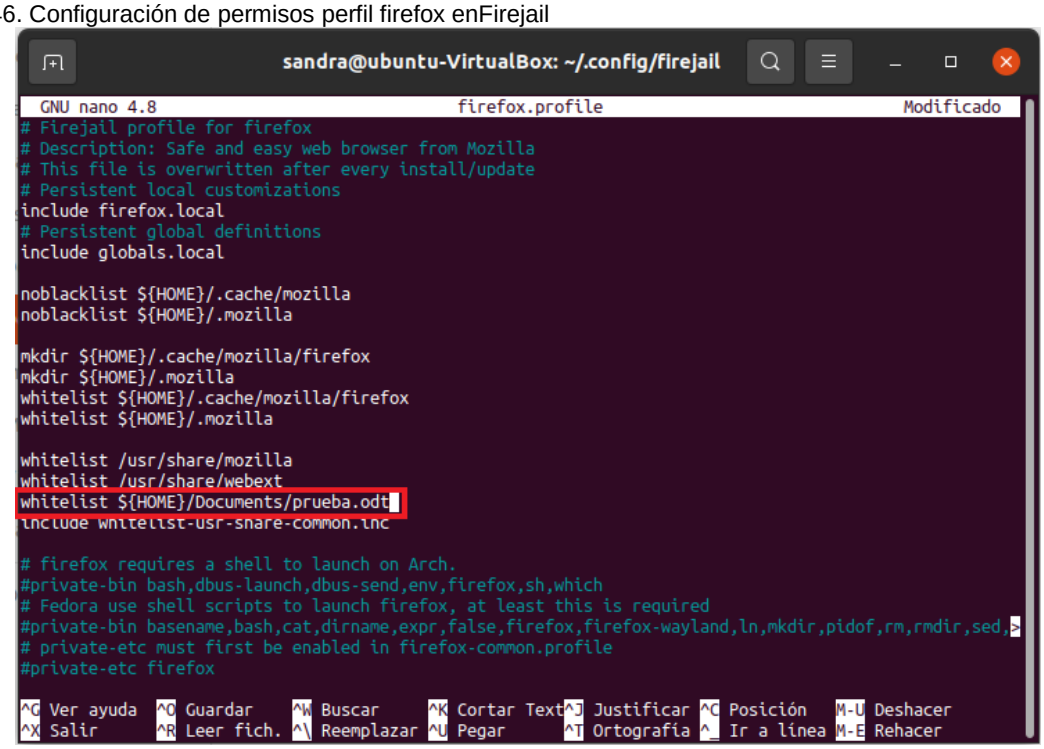
Figura 145. Edición de perfil de seguridad de firejail de la aplicación firefox



Fuente: elaboración propia.

Si por ejemplo se quiere permitir que Firefox cargue un archivo específico del directorio documentos se debe agregar una entrada de lista blanca para éste, como se resalta en la siguiente Figura 146, posterior a ello se guardan los cambios, y se lanza la aplicación para realizar las pruebas.

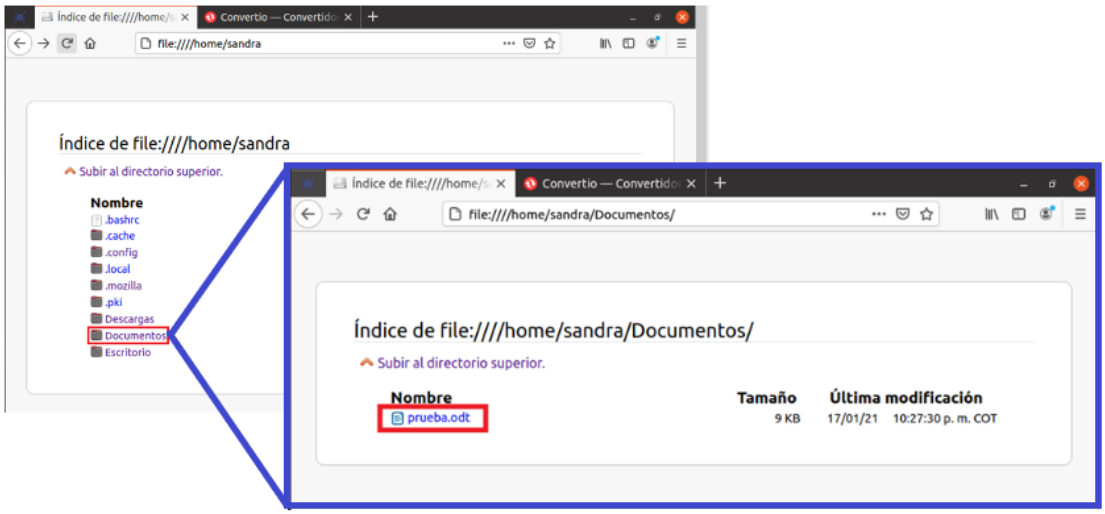
Figura 146. Configuración de permisos perfil firefox enFirejail



Fuente: elaboración propia.

Al abrir Firefox, en la barra de direcciones es posible navegar dentro directorio de archivos home, en donde se puede observar las carpetas predeterminadas como escritorio y descargas, adicionalmente se encuentra el directorio Documentos, y al hacer clic muestra el archivo al cual se le permitió el acceso, tal como se observa en la siguiente Figura.

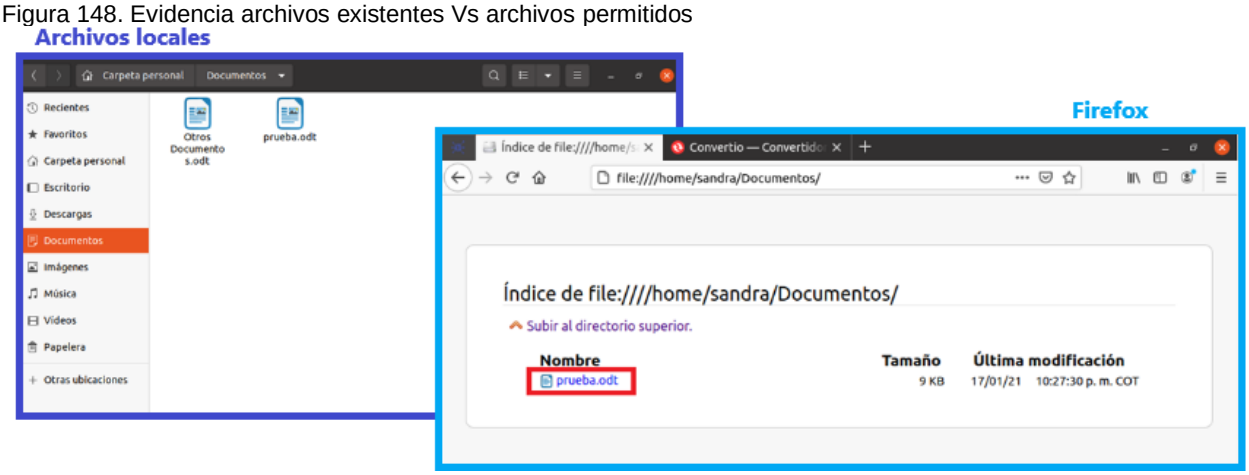
Figura 147. Acceso solo al archivo permitido en perfil de firejail



Fuente: elaboración propia.

En la siguiente Figura se evidencia la forma en que firejail aísla a Firefox, puesto que a pesar de que en el directorio mis documentos (parte izquierda de la Figura) existe otro archivo, al navegar desde la aplicación solo se muestra acceso que tiene definido en el perfil de seguridad (parte derecha de la Figura)

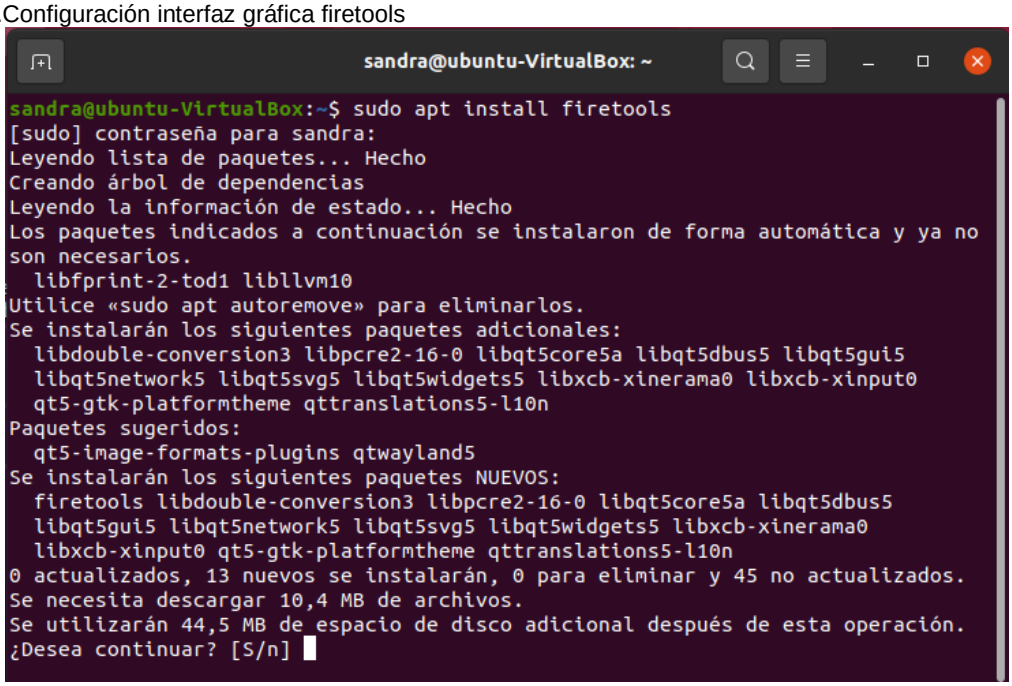
Figura 148. Evidencia archivos existentes Vs archivos permitidos



Fuente: elaboración propia.

- **Pruebas con Firetools**. Firejail cuenta con una interfaz gráfica de usuario denominada firetools, a través de la cual se pueden lanzar y gestionar el entorno de pruebas de las aplicaciones que no son de confianza, para su instalación se ejecuta el comando sudo apt install firetools, como se observa en la siguiente Figura

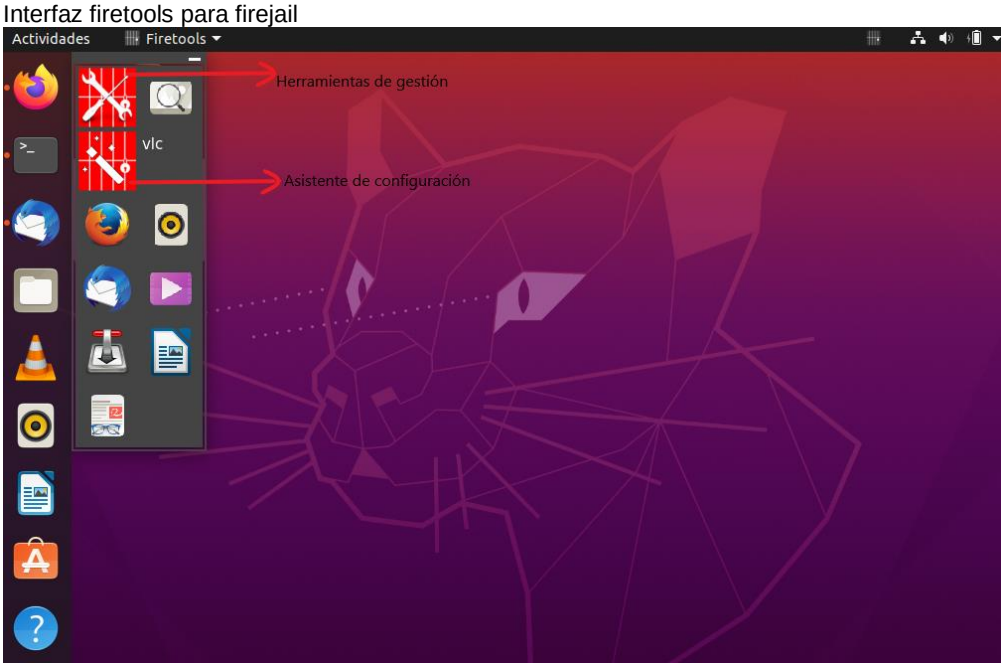
Figura 149.Configuración interfaz gráfica firetools



Fuente: elaboración propia.

Posteriormente al ejecutar la aplicación se muestra un menú de opciones en el que se encuentran las herramientas de gestión y de configuración, así como el acceso a las aplicaciones que se encuentren instaladas en el sistema, ver la siguiente Figura

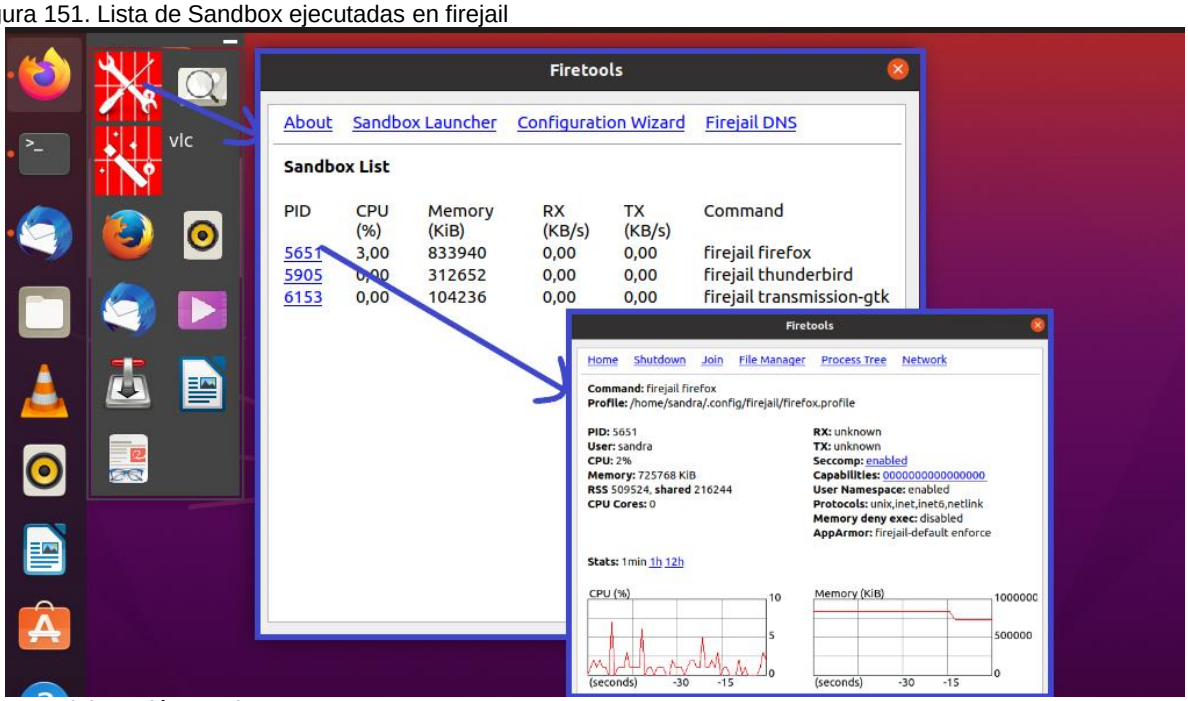
Figura 150. Interfaz firetools para firejail



Fuente: elaboración propia.

Presionando en el botón firetools podemos acceder al listado de sandbox que se encuentren en ejecución en determinado momento, las cuales se encuentran identificadas por un id de proceso (PID), al presionar sobre el PID, se muestra el detalle consumo de cpu y memoria, gestor de archivos, árbol de procesos, uso de red, etc. Y desde aquí mismo se puede finalizar

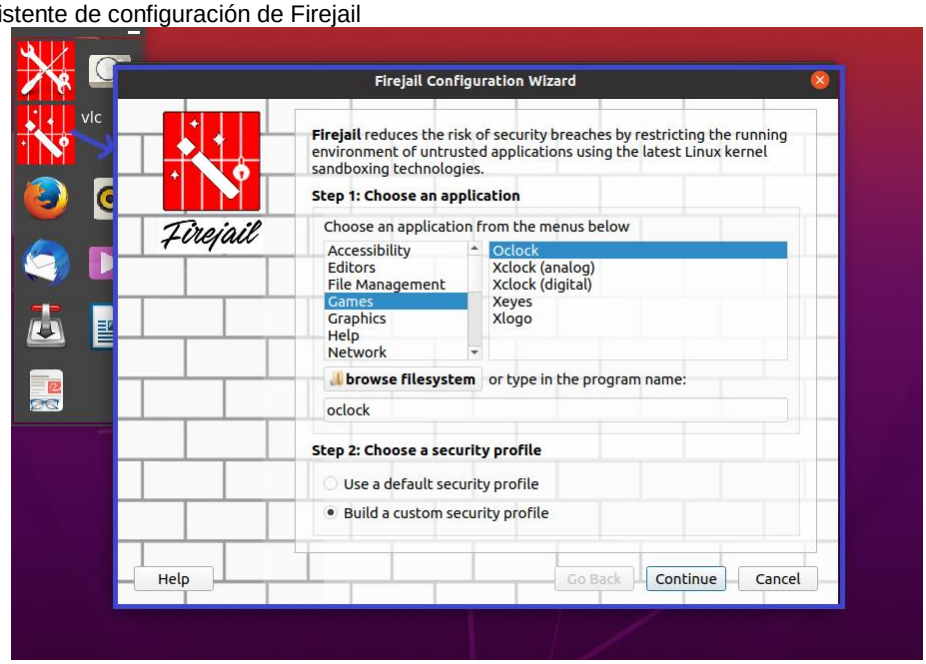
Figura 151. Lista de Sandbox ejecutadas en firejail



Fuente: elaboración propia.

El asistente de configuración permite personalizar los perfiles de seguridad de las aplicaciones instaladas, permitiendo establecer restricciones sobre el sistema de archivos, el uso de la red, multimedia, etc. Así como también los módulos de seguridad del kernel que se desee habilitar.

Figura 152. Asistente de configuración de Firejail



Fuente: elaboración propia.

5. CONCLUSIONES

- La revisión documental realizada sobre el tema del CSIRT, evidencian que el panorama relacionado con la seguridad informática en nuestro país goza cada vez de mayor atención por parte del Estado y aunque es incipiente, se considera que los esfuerzos realizados con la creación de centros de atención a incidentes de seguridad informática tanto estatales como de la empresa privada, representan buenos cimientos en la construcción de mecanismo de ciberdefensa. Sin embargo, en el ámbito empresarial existe un gran camino por recorrer, dado que son muy pocas las organizaciones que destinan recursos al tema de la ciberseguridad, a pesar de que las estadísticas han demostrado que cualquier tipo de empresa puede ser blanco de un ciberataque.

- La necesidad identificada por la empresa caso de estudio Cibersecurity de Colombia LTDA en sus clientes, permite establecer el eje sobre el cual se edifica el diseño técnico del CSIRT: su circunscripción y los servicios a ofrecer; a partir de esto es posible la definición de estructura tecnológica, las herramientas de software y equipamiento tecnológico requerido para su puesta en marcha.

- Para el desarrollo de operaciones del CSIRT se requiere la implementación de varias herramientas de software acordes con los servicios ofrecidos, algunas de ellas integran diferentes funcionalidades que pueden hacerlas ver como un todo en uno, sin embargo, en ocasiones no alcanzan el grado de eficiencia requerido para la ejecución de un determinado servicio, es por ello que se precisa identificar la mayor fortaleza de cada herramienta para encaminarla a la ejecución de procesos en donde se obtenga su máximo aprovechamiento.

- Existen herramientas open Source que pueden llegar a ser tan poderosas como las aplicaciones comerciales, tal es el caso de las funcionalidades que se pueden emplear con herramientas como bacula, que permite tanto un despliegue pequeño a nivel local, como uno a gran escala en redes de área amplia más extensas, asegurando la continuidad en el servicio mediante la instalación de proxys en las sedes alternas para garantizar la continuidad en el servicio.

- La ejecución de pruebas de software en un entorno virtualizado permite tener obtener una idea más clara sobre el funcionamiento de las aplicaciones seleccionadas y su desempeño en un entorno real. A partir de esta experiencia se pueden soportar las decisiones de carácter técnico o administrativo durante la ejecución del proyecto en la empresa.

6. RECOMENDACIONES

Para la puesta en marcha en CSIRT, es necesario que adicionalmente a la parte técnica, se tengan en cuenta, la parte administrativa del mismo, puesto que a partir de estas pautas se definen, elementos tan importantes como lo son el recurso humano, la parte operativa que se constituye en eje fundamental de este tipo de organizaciones. En consecuencia, complementar este proyecto con un enfoque administrativo permite la consolidación del objetivo proyectado por la empresa Cibersecurity de Colombia.

Al momento de la elección del equipamiento de hardware, se debe tener en cuenta el despliegue tecnológico acorde con el alcance inicial del CSIRT, que sea escalable a través del tiempo y que permita el crecimiento paulatino del equipo. Cabe destacar que los recursos de hardware de los servidores Bacula y Alienvault OSSIM tienen una alta demanda por la naturaleza de los servicios que ejecutan, por ello se debe considerar la asignación de recursos de hardware alta, para lo cual es necesario tener en cuenta los agentes atendidos.

BIBLIOGRAFÍA

AGNITAS [sitio web]. OpenEMM 2019: Email Marketing for Free [En línea]. [consultado 16 noviembre 2019]. Disponible en: https://www.agnitas.de/en/e-marketing_manager/email-marketing-software-variants/openemm/

AT&T CYBERSECURITY [sitio web]. AlienVault OSSIM [En línea]. [consultado 16 noviembre 2019]. Disponible en: https://www.alienvault.com/products/ossim.

AVENÍA DELGADO, Carlos Arturo. Fundamentos de seguridad informática. Editorial: Fondo editorial Areandino, 2017. 96 p. ISBN 978-958-5459-61-8.

BACA URBINA, Gabriel. Introducción a la seguridad informática. Grupo Editorial Patria, 2016. 360 p. ISBN 978-607-744-471-8

BACULA.ORG [sitio web]. What is Bacula? [En línea]. [consultado 2 mayo 2020]. Disponible en: https://www.bacula.org/what-is-bacula/

CASTILLO PARRA, Xenia. Normatividad De Ciberseguridad En El Sector Financiero Colombiano [en línea]. Seminario de investigación aplicada de la gestión de la seguridad y el riesgo. Universidad Piloto de Colombia. p 2. [consultado febrero 2020]. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/8625

CENTER FOR INTERNET SECURITY [sitio web]. CIS Controls [En línea]. [consultado 26 noviembre 2019]. Disponible en: https://www.cisecurity.org/controls/

CENTRO CIBERNETICO POLICIAL. Informe: Balance Cibercrimen en Colombia 2017 [en línea]. POLICIA NACIONAL, 2017. [consultado 2 Octubre 2019]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_201217_1_1_0.pdf

CLAMAV [sitio web]. Clam AntiVirus-Documentation [En línea]. [consultado 2 mayo 2020]. Disponible en: https://www.clamav.net/documents/introduction

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273 de 2009 (enero 5 de 2009) [en línea]. Diario Oficial. Bogotá, D.C., 2009. [Consultado febrero 2020]. Disponible en:

http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento Conpes 3854 (2016) Política Nacional De Seguridad Digital [en línea]. Bogotá, D.C. p 21. [Consultado febrero 2020]. Disponible en: https://bibliotecadigital.ccb.org.co/bitstream/handle/11520/14856/DNP-Conpes-Pol%2b%c2%a1tica%20Nacional%20de%20Seguridad%20Digital.pdf?sequence=1&isAllowed=y

DE LA TORRE, Hugo y PARRA, Mario. Estrategia y Diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la universidad de las fuerzas armadas ESPE [en línea]. Trabajo de Grado (Ingeniero de Sistemas e informática). Universidad de las Fuerzas Armadas. Sangolquí (Ecuador), 2018. [consultado 12 abril de 2020]. Disponible en: http://repositorio.espe.edu.ec/handle/21000/15071

DÍAZ, Gabriel. Procesos y herramientas para la seguridad de redes [en línea]. Madrid: UNED - Universidad Nacional de Educación a Distancia, 2014. 568 p. [consultado 26 noviembre 2019]. Disponible en: https://buscador.biblioteca.uned.es/primo-explore/fulldisplay?vid=34UNED_VU1&search_scope=TAB1_SCOPE1&tab=tab1&docid=34UNED_ALMA2195110980004215&lang=es_ES&context=L

ENISA[sitio web]. Cómo crear un CSIRT Paso a Paso. [En línea]. [consultado 7 Octubre 2019]. Disponible en: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

FIREJAIL [sitio web]. Firejail Security Sandbox [en linea]. [Consultado en enero 2021]. Disponible en https://firejail.wordpress.com/

GARCIA VELASQUEZ, Javier Antonio. Propuesta de diseño e implementación de un Centro de Operaciones de Seguridad (SOC) y un Centro de Repuesta a Incidencias (CSIRT) para la Universidad de Ingeniería. Trabajo de Grado (Magister en Gestión de la Seguridad de la Información). Universidad Nacional de Ingeniería. Managua (Nicaragua), 2016. [consultado 12 abril 2020]. Disponible en: https://core.ac.uk/download/pdf/250144005.pdf.

GLPI. (2019) [sitio web]. ITSM software – GLPI [En línea]. [consultado 25 noviembre 2019]. Disponible en: https://glpi-project.org/features/

GÓMEZ BEAS, Dolores. Resolución de incidencias en redes telemáticas (UF1881). Andalucía: IC Editorial, 2014. 144 p. ISBN 978-84-16433-41-4

GOMEZ VIEITES, Álvaro. Enciclopedia de la Seguridad Informática. 2 ed. Madrid: RA-MA, 2014. 825 p. ISBN 978-604-707-181-5.

GROBLER, Marthie and BRYK, Harri. Common Challenges Faced During the Establishment of a CSIRT-[En línea]. [consultado 6 Octubre 2019]. Disponible en: https://researchspace.csir.co.za/dspace/bitstream/handle/10204/4339/Grobler2_2010.pdf?sequence=1.

HERNÁNDEZ SAMPIERI, Roberto; FERNÁNDEZ COLLADO, Carlos y BAPTISTA LUCIO, Pilar. Metodología de la investigación 6a. ed. México D.F.: McGraw-Hill Interamericana, 2014. 600 p.

INCIBE. [sitio web]. Las 7 fases de un ciberataque. ¿Las conoces?. [En línea]. [Consultado en mayo de 2020]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/las-7-fases-ciberataque-las-conoces

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO / IEC 2018, 5ta Edicion. Genova, Suiza: ISO, 2018 4p.

IÑIGUEZ ESTRADA, Héctor. Seguridad Informática y Protección de Datos Personales. EDI, 2020.114 p. ISBN 978-9917-0-0493-6

KALILINUX [sitio web]. Kali Linux (2020). [En línea]. {09 diciembre 2019}. Disponible en: https://www.kalilinux.in/2019/10/guymager-forensic-disk-imager-kali-linux.html

KEMP, Simón. Digital 2020: Global Digital Overview. Global Overviews [en línea]. 30 de enero 2020. [consultado 26 Marzo 2020]. Disponible en https://thenextweb.com/podium/2020/01/30/digital-trends-2020-every-single-stat-you-need-to-know-about-the-internet/.

LASKOWSKI-TECH.(2019) [sitio web]. Blazescan - Utilidad de escaneo de malware de Linux. GLPI. [En línea]. [consultado 25 noviembre 2019]. Disponible en: https://laskowski-

tech.com/2018/05/29/blazescan-linux-malware-scanning-utility/

LYON, Gordon. Nmap. [En línea]. [consultado 25 noviembre 2019]. Disponible en: https://nmap.org/

MANCERA S.C. Encuesta Global de Seguridad de la Información 2018-19. [en línea]. México: Ernst & Young Global, 2019. [consultado 2 octubre 2019]. Disponible en: https://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2018-19/$FILE/ey-encuesta-global-seguridad-informacion-2018-19.pdf

OCAMPO, Carlos; LAVERDE, Ricardo y CAICEDO, Sandra. Implementación de modelo de procesos de gestión de servicios con Itil (information technology infrastructure library). Scientia et technica [en línea].2009, Vol. 1 núm 41. [consultado 16 noviembre de 2019]. Disponible en: https://revistas.utp.edu.co/index.php/revistaciencia/article/view/2913.

PROXMOX [sitio web]. Proxmox Virtual Environment [En línea]. [consultado 2 mayo 2020]. Disponible en: https://proxmox.com/en/proxmox-ve

RAMIREZ LUNA, Heltton. Desarrollo de un marco de trabajo para la protección de un Equipo de Respuesta ante incidencias de Seguridad Informática CSIRT. Trabajo de Grado (Maestro en Ingeniería de Software). Centro de Investigación en Matemáticas, A.C (CIMAT). Zacatecas (México), 2016. [consultado 5 mayo 2020]. Disponible en: https://cimat.repositorioinstitucional.mx/jspui/handle/1008/442.

RÍOS HUÉRCANO, Sergio. Itil v3 Manual Integro [En línea]. En: Biable [sitio web]. [consultado 7 octubre 2019]. Disponible en: https://biable.es/.

ROMERO CASTRO, Martha, et al. Introducción a la seguridad informática y el análisis de vulnerabilidades. Editorial Área de Innovación y Desarrollo. SL, 2018. 121 p. ISBN 978-84949306-1-4

ROUSE, Margaret. Gestión de eventos e información de seguridad (SIEM). [En línea]. Search Data Center. [consultado 16 noviembre de 2019]. Disponible en: https://searchdatacenter.techtarget.com/es/definicion/Gestion-de-eventos-e-informacion-de-seguridad-SIEM

SANS. (2019) [sitio web]. SIFT Workstation. [En línea]. [consultado 09 diciembre 2019]. Disponible en: https://digital-forensics.sans.org/community/downloads

SECURITY ONION SOLUTIONS [sitio web]. Security Onion [En línea]. [consultado 25 noviembre 2019]. Disponible en: https://securityonion.readthedocs.io/en/latest/introduction.html .

SOFTWARE ENGINEERING INSTITUTE, Carnegie Mellon Carnegie Melon University. [Sitio web]. Create A Csirt.(2017) [en línea]. [Consultado 8 octubre 2019]. Disponible en: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485693

VEGA BRICEÑO, Edgar. Planificación y ejecución de evaluaciones de seguridad informática desde un enfoque de ethical hacking. Editorial Área de Innovación y Desarrollo. SL, 2020. 96 p. ISBN: 978-84-121459-4-6.

VILLALOBOS MURILLO, Johnny. Gestión De Incidentes De Seguridad Informática Con Agentes Inteligentes. Revista .Seguridad [en línea]. 2018, Julio-Agosto, 14. [consultado mayo 2020]. ISSN 1251478. Disponible en: https://revista.seguridad.unam.mx/numero-14/gesti%C3%B3n-de-incidentes-de-seguridad-inform%C3%A1tica-con-agentes-inteligentes

WEST-BROWN, Moira J., et al. Handbook For Computer Security Incident Response Team (Technical Report CMU/SEI-2003-HB-002). [en línea] Pittsburgh: Software Engineering Institute, Carnegie Mellon Carnegie Melon University, 2003. p 22. [consultado octubre 2019]. Disponible en: https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf

ZABBIX LLC [sitio web]. Zabix [en línea]. [consultado 25 noviembre 2019]. Disponible en: https://www.zabbix.com/features.

ANEXOS

ANEXO A

INSTALACION SERVIDORES

A continuación, se indica el proceso de instalación de los servidores empleados para el desarrollo del laboratorio controlado sobre los cuales se efectuaron las pruebas del software para el CSIRT de Cibersecurity.

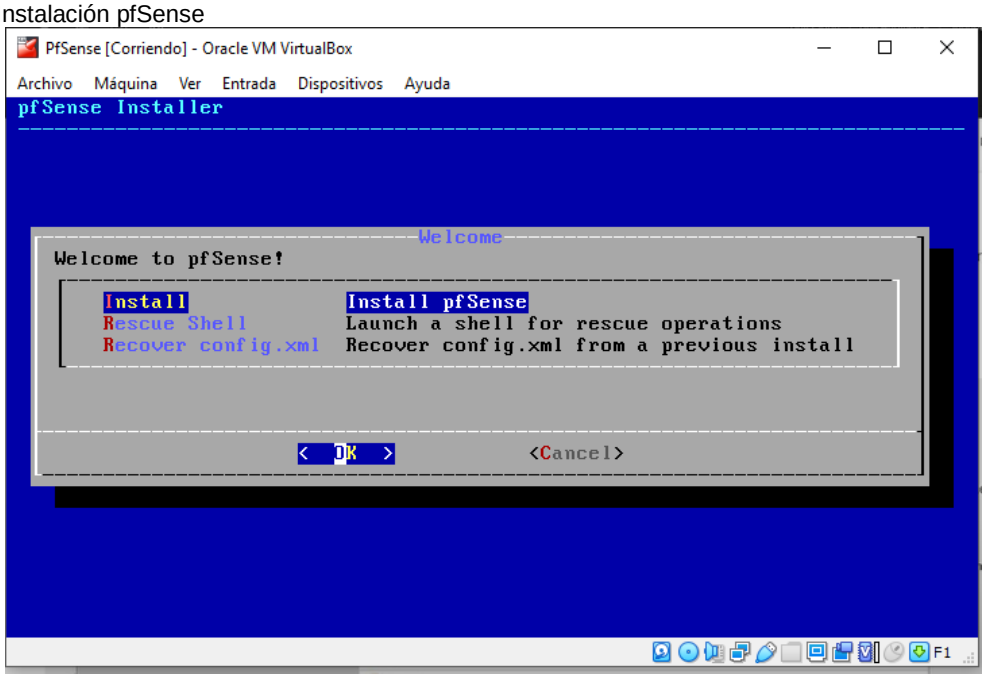
A.1 INSTALACIÓN FIREWALL PFSENSE

La herramienta firewall será de gran utilidad para la recolección de eventos de Alienvault OSSIM. Por tal razón, se implementa el firewall pfSense, para el laboratorio controlado, basado en el sistema operativo FreeBSD, Se prepara una máquina virtual con las siguientes características de hardware en virtual box:

- Sistema operativo BSD FreeBSD 64 bits
- Memoria Ram 1 GB
- Procesador: 1 CPU
- Disco duro VDI 16 GB
- Unidad óptica
- 1 adaptadores de red en modo NAT
- 1 adaptadores de red en modo red interna

Se inicia la maquina con la iso descargada y se siguen los pasos de instalación, en la primera pantalla se muestran los términos y condiciones de uso, seleccionar aceptar. En la siguiente pantalla se selecciona la opción “install pfSense”, como se observa en la siguiente Figura:

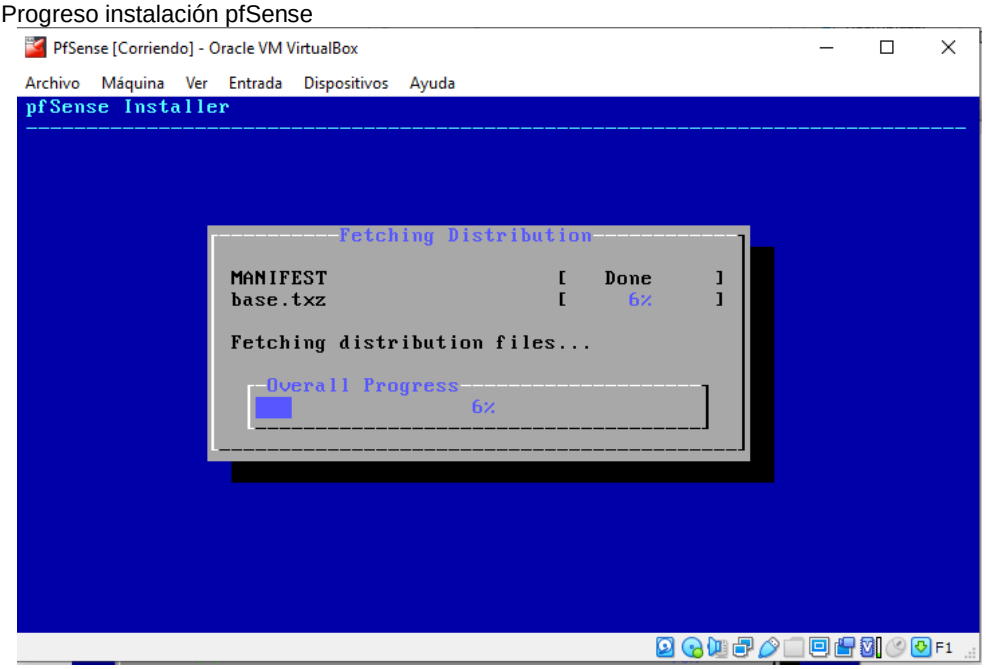
Figura 153. Instalación pfSense



Fuente: elaboración propia.

Se elige el idioma del teclado, en la siguiente pantalla se procede a seleccionar la instalación guiada en la opción Auto UFS, y se inicia el progreso de instalación tal como se observa en la Figura

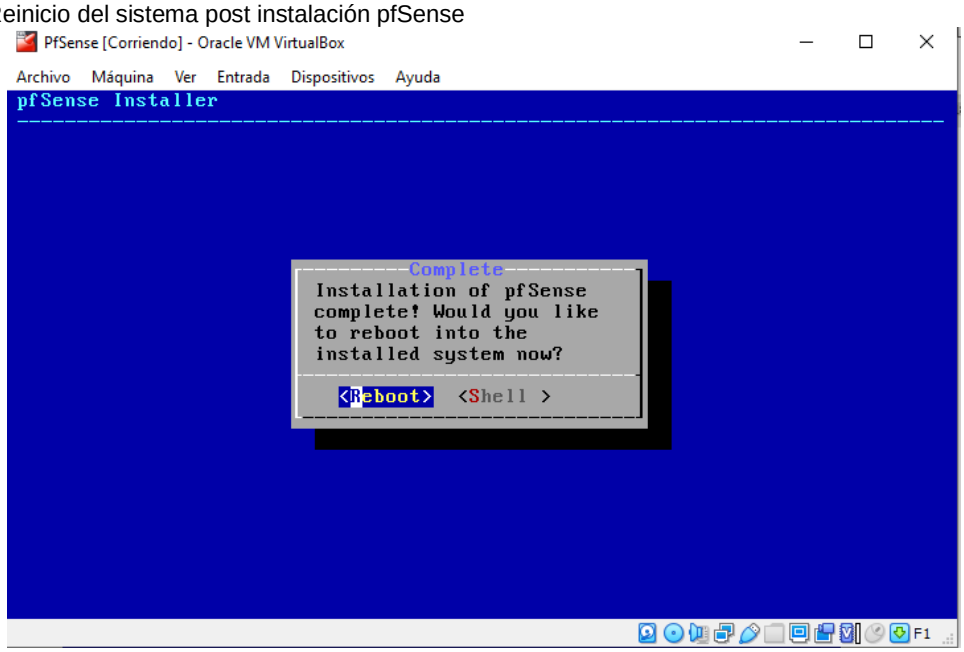
Figura 154. Progreso instalación pfSense



Fuente: elaboración propia.

Al finalizar la instalación el programa pregunta si se desea realizar alguna configuración adicional desde la línea de comandos, lo cual se omite. Seguidamente se solicita el reinicio del sistema, como se aprecia a continuación:

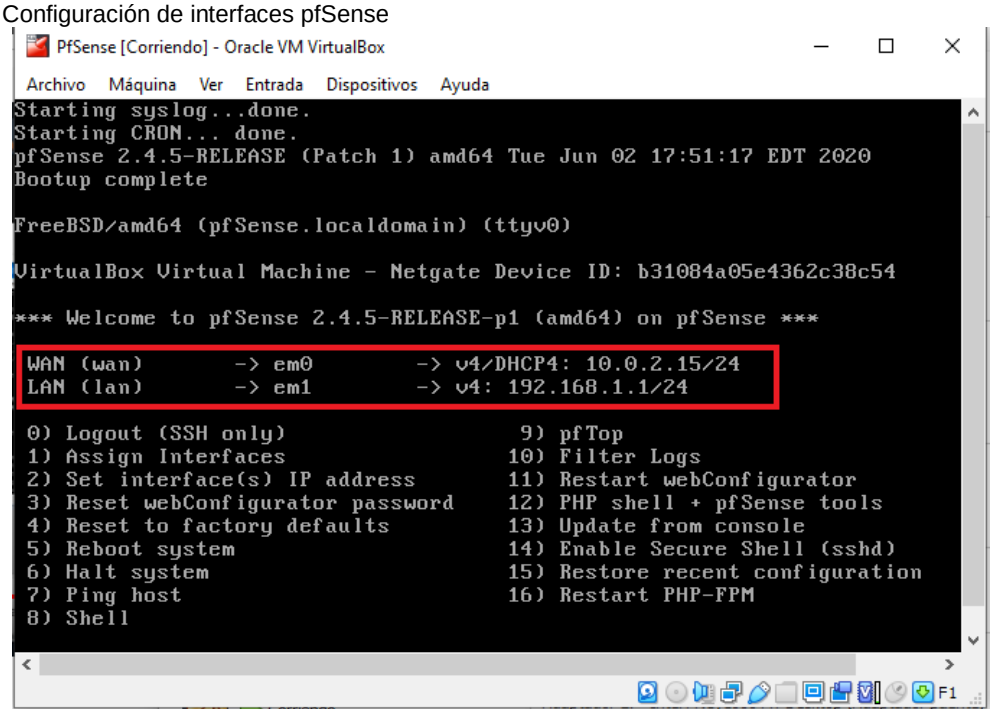
Figura 155. Reinicio del sistema post instalación pfSense



Fuente: elaboración propia.

Posteriormente al arrancar nuevamente la máquina, se tiene la pantalla que se muestra en la Figura, en donde se presenta la información de configuración ip de las interfaces de red configuradas en la máquina, en donde “em0” se emplea para la red WAN de salida a internet y la em1 para la red LAN. Seguidamente se lista un menú de opciones en donde se pueden configurar diferentes opciones para el PfSense

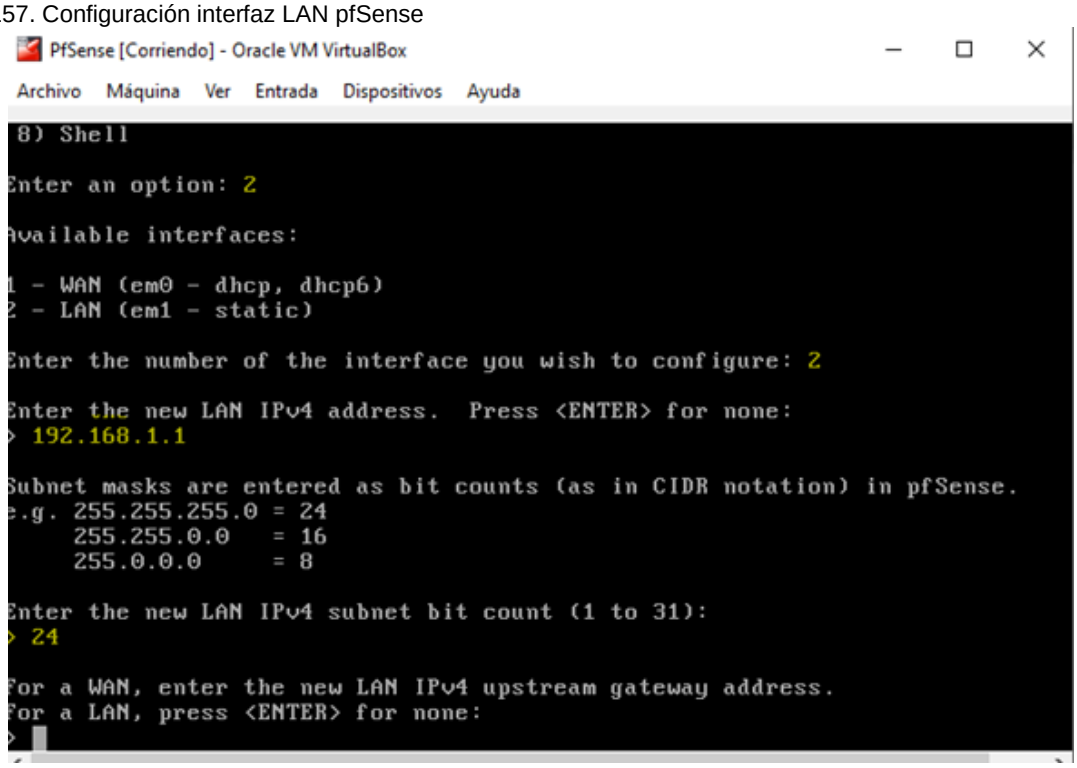
Figura 156. Configuración de interfaces pfSense



Fuente: elaboración propia.

Se realiza la configuración de la ip de la interfaz LAN dentro de la red local para lo cual se selecciona la opción 2, luego pulsa nuevamente el numero 2 para seleccionar LAN, se establece la ip 192.168.1.1, una máscara de subred de 24 bits, como se muestra en la siguiente Figura

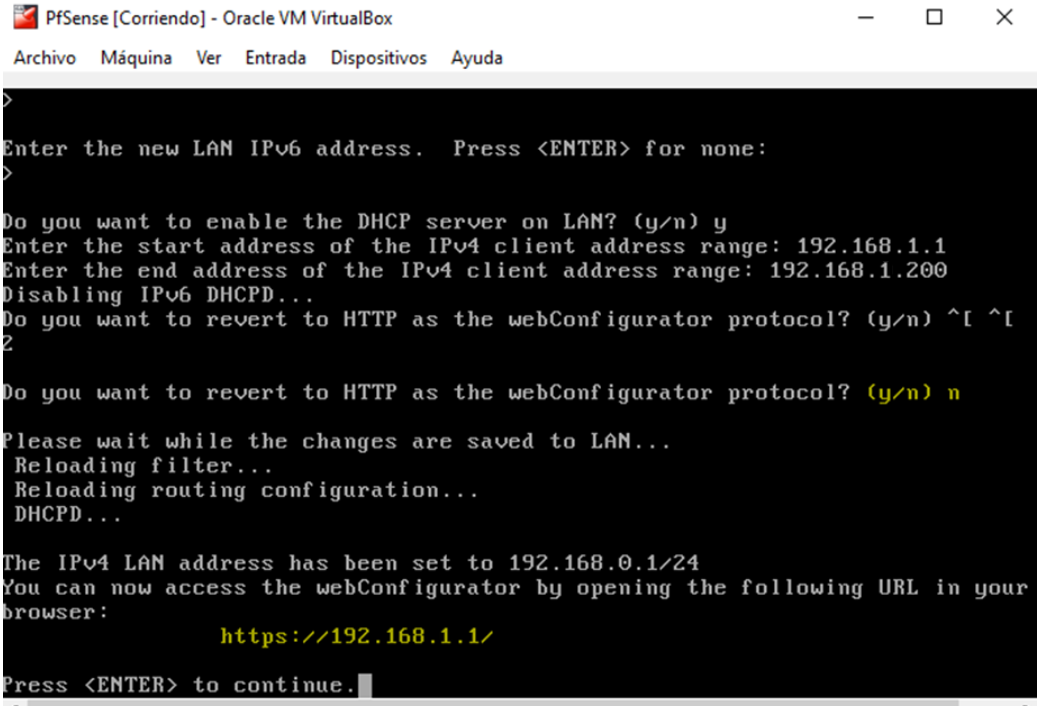
Figura 157. Configuración interfaz LAN pfSense



Fuente: elaboración propia.

Se preguntará si se desea establecer una ip para la interfaz WAN, se omite presionando la tecla enter. Luego preguntara si se desea configurar la IPv6, lo cual se omite de igual forma. Seguidamente el programa pregunta si se activara DHCP en la interfaz, en este caso se presiona la tecla “y”, se escriben el rango de IP inicial y Final para el mismo, como punto final se pregunta si se quiere revertir el protocolo http, se pulsa la tecla “n”, una vez hecho el proceso se muestra el resultado de la configuración realizada tal como se observa en la Figura

Figura 158. Configuración establecida en pfSense



Fuente: elaboración propia.

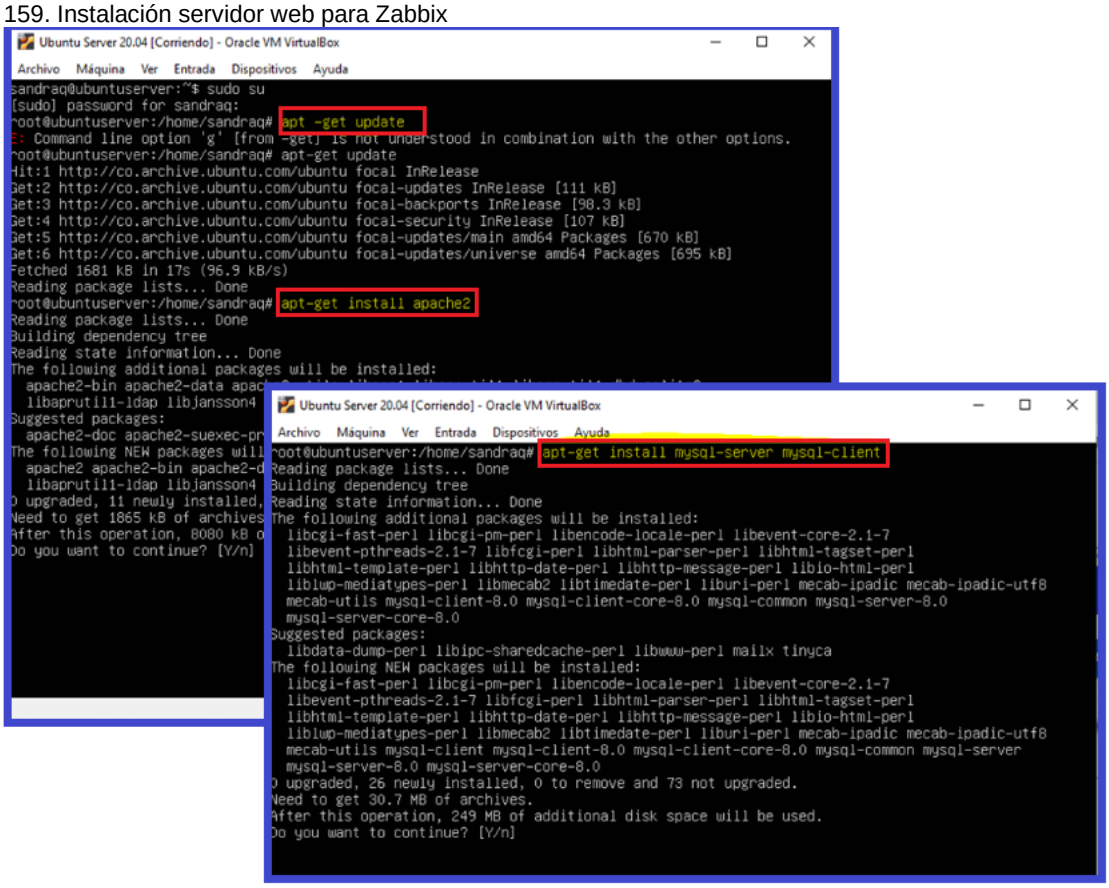
A.2 INSTALACIÓN SERVIDOR ZABBIX

Este servidor de monitoreo se instala sobre el sistema operativo Ubuntu Server version 20.04, montado sobre la herramienta VirtualBox 6.1, al que se le configuraran las siguientes características de hardware:

- Sistema operativo Linux Ubuntu Server 64 bits
- Memoria Ram 2 GB
- Procesador: 1 CPU
- Disco duro VDI 20 GB
- Unidad óptica
- Adaptador de red en modo red interna

A2.1 Instalación servidor web LAMP. La herramienta Zabbix tiene dentro de sus requerimientos contar con los aplicativos que componen un servidor web, para el despliegue de sus funcionalidades, por ello es uno de los primeros pasos a realizar antes del montaje en sí de la aplicación. En primer lugar, se requiere actualizar los repositorios, posteriormente se ejecutan las instrucciones para la instalación de apache y mysql. Esto se puede observar en la siguiente Figura.

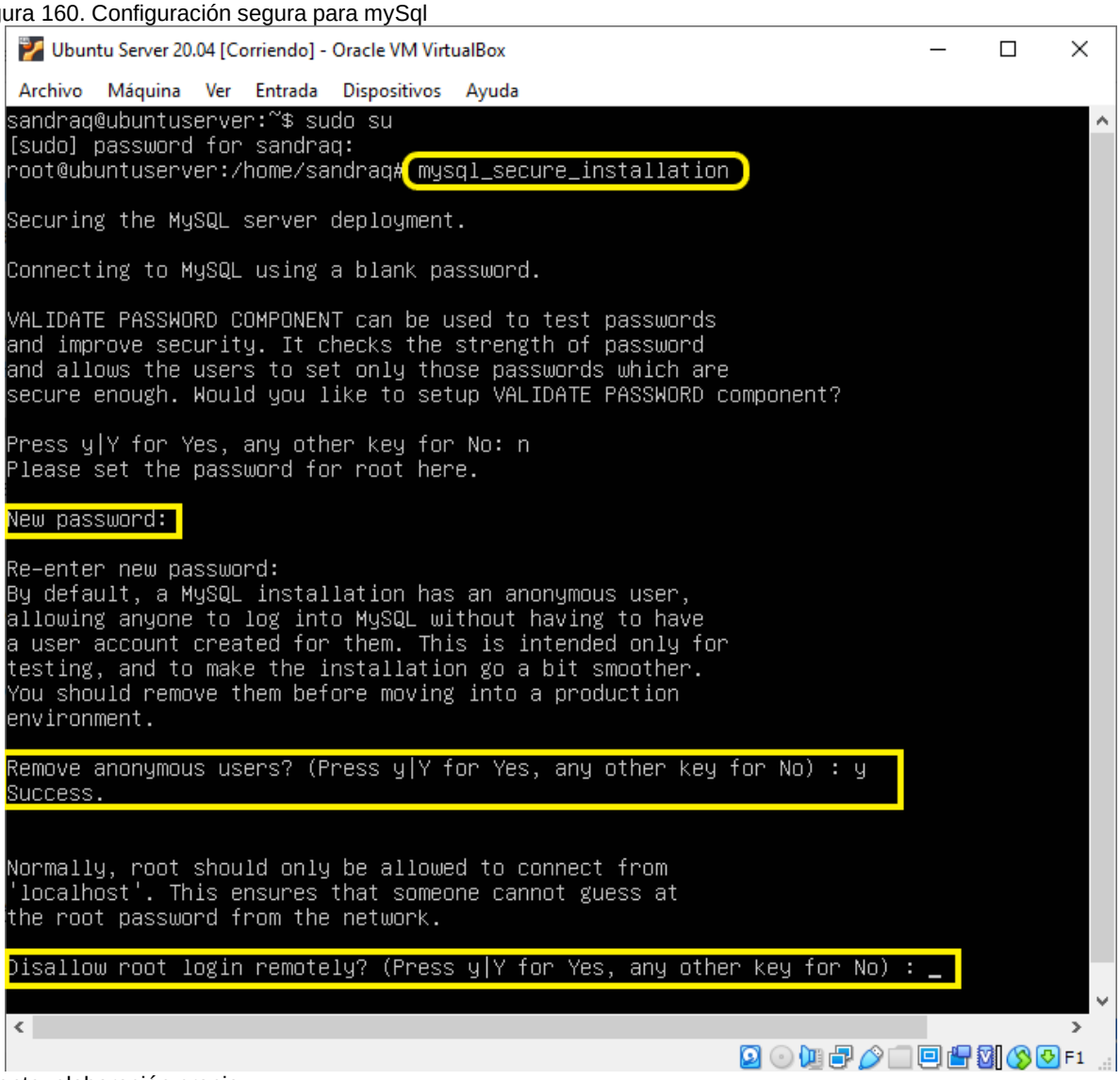
Figura 159. Instalación servidor web para Zabbix



Fuente: elaboración propia.

A2.2 Configuración segura de MySql. Se ejecuta serie de instrucciones de seguridad que viene preinstalada en MySQL con la que se eliminarán ciertas configuraciones predeterminadas, ejecutando la siguiente instrucción interactiva “mysql_secure_ installation”, luego se pedirá un nuevo password para el usuario root de mysql, eliminar el usuario anónimo e inhabilitar el login remoto, entre las principales opciones. La secuencia se puede observar en la siguiente Figura.

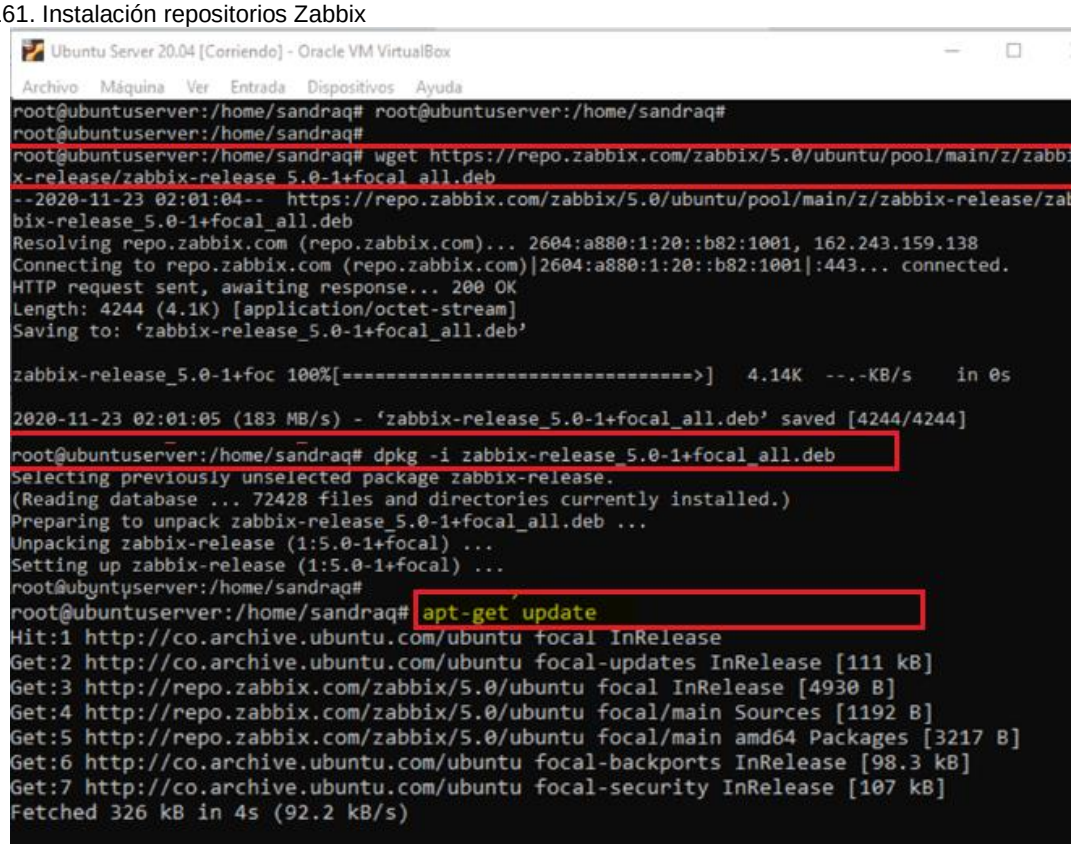
Figura 160. Configuración segura para mySql



Fuente: elaboración propia.

A2.3 Instalación repositorio de Zabbix. A través de las instrucciones mostradas en la Figura siguiente, se observa cómo obtener, desempaquetar y actualizar los repositorios que permitirán la instalación de la aplicación.

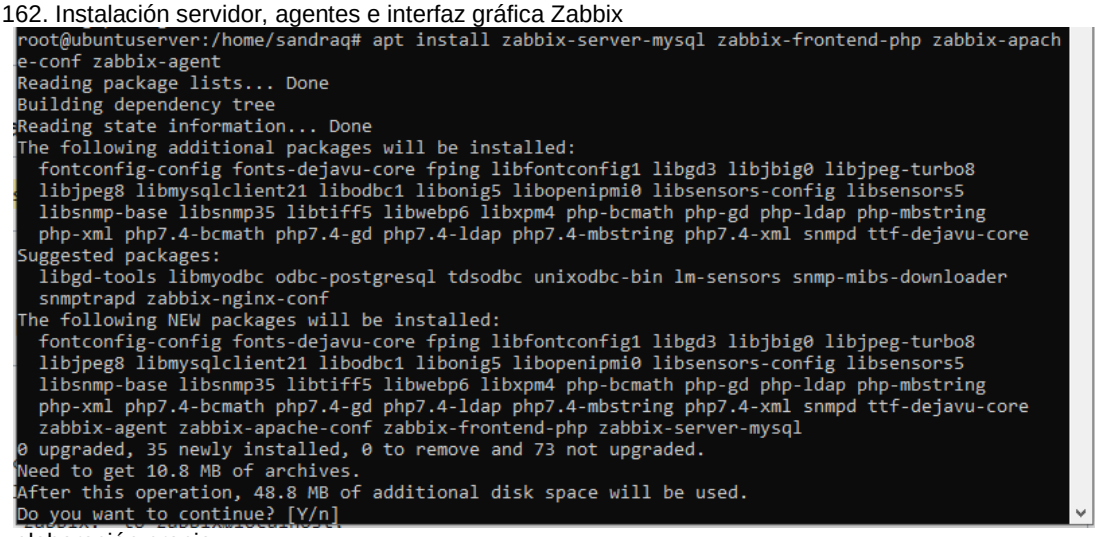
Figura 161. Instalación repositorios Zabbix



Fuente: elaboración propia.

A2.4 Instalación Servidor Zabbix, la interfaz gráfica y el agente. Finalmente, se procede a ejecutar el comando de instalación como se observa en la siguiente Figura.

Figura 162. Instalación servidor, agentes e interfaz gráfica Zabbix



Fuente: elaboración propia.

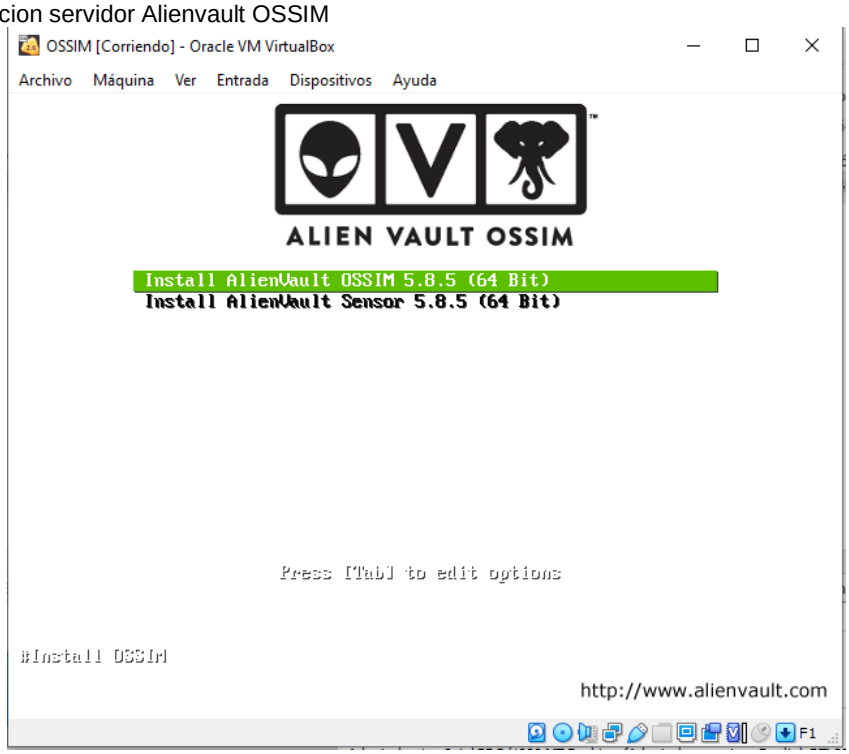
A.3 INSTALACIÓN SERVIDOR CORRELACIONADOR DE EVENTOS ALIENVAULT OSSIM

Alienvault OSSIM es una herramienta compuesta de varias aplicaciones cuyo instalador se encuentra integrado dentro de un sistema operativo basado en Debian/GNU Linux y que se encuentra disponible tanto para la arquitectura de 32 y 64 bits. Para su instalación se prepara una máquina virtual en Virtualbox con las siguientes características de hardware:

- Sistema operativo Linux Debian 64 bits
- Memoria Ram 4 GB
- Procesador: 3 CPU
- Disco duro VDI 25 gb
- Unidad óptica
- 2 adaptadores de red en modo red interna

Se inicia la máquina virtual creada con el medio de instalación de descargado de la página oficial, se procede a seleccionar la primera opción para la instalación en modo servidor, según se muestra en la siguiente Figura.

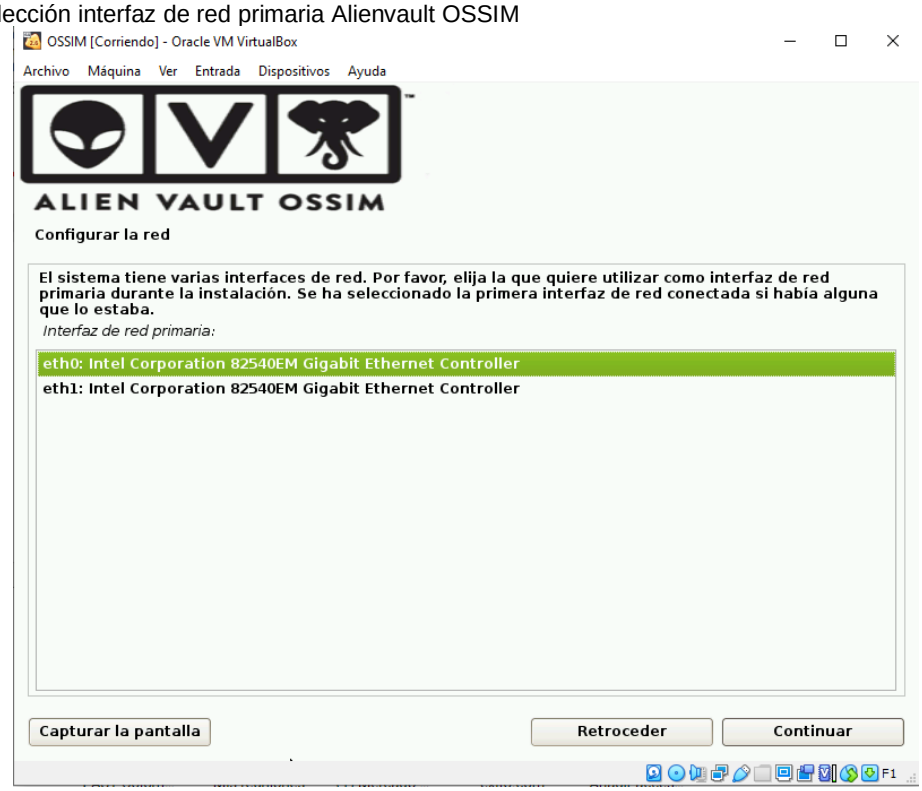
Figura 163. Instalacion servidor Alienvault OSSIM



Fuente: elaboración propia.

El proceso de instalación es sencillo, basta con seleccionar las opciones que se van indicando como lo son: el idioma, país y distribución de teclado según sea el caso, posteriormente se establece la configuración de red de una de las dos interfaces de red habilitadas en la máquina, destinada para efectos de administración del servidor OSSIM, en este caso se selecciona la interfaz eth0, se presiona el botón continuar, como se observa en la siguiente Figura.

Figura 164. Selección interfaz de red primaria Alienvault OSSIM



Fuente: elaboración propia.

En la siguiente pantalla se establece la dirección ip que tendrá el servidor, para este caso se utiliza 192.168.1.201, la máscara de subred pertinente 255.255.255.0, la puerta de enlace y servidor DNS como 192.168.1.1

Figura 165. Configuración de red interface primaria Alienvault OSSIM

Fuente: elaboración propia.

Una vez configurada la interfaz de red, en la siguiente pantalla se procede a configurar la contraseña del usuario root de este servidor, se presiona el botón continuar y se espera a terminar el proceso, se observará una pantalla de login como se observa en la siguiente Figura.

Figura 166. Pantalla login consola Alienvault OSSIM

Fuente: elaboración propia.

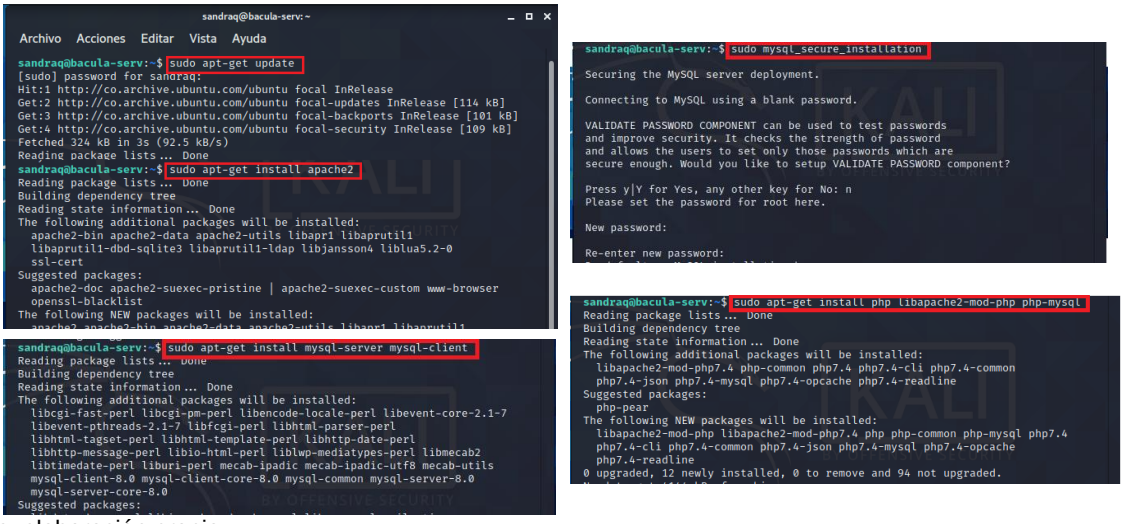
A.4 INSTALACION SERVIDOR BACKUPS BACULA

El servidor de copias de seguridad se virtualiza en una maquina Linux dentro de VirtualBox con las siguientes características:

- Sistema operativo Ubuntu server 20.04 64 bits
- Memoria Ram 2 GB
- Procesador: 1 CPU
- Disco duro VDI 35 GB
- Unidad óptica
- 1 adaptadores de red en modo red interna

A4.1 Instalación Lamp y opciones de seguridad para mysql. Una vez se culmina la instalación del sistema operativo, se inicia configurando un servidor lamp como requisito previo a la instalación del servidor Bacula. Aplicando de igual manera que con el servidor Zabbix las opciones de seguridad básicas de mysql, comol se observa en la siguiente Figura:

Figura 167. Instalación servidor LAMP y configuración seguridad MySql



Fuente: elaboración propia.

A 4.2 Instalación Bacula server y Bacula Cliente. Instalación de bacula, se ejecuta la instrucción sudo apt install bacula-server bacula-client, presionar “y” cuando se indique la pregunta de continuar.

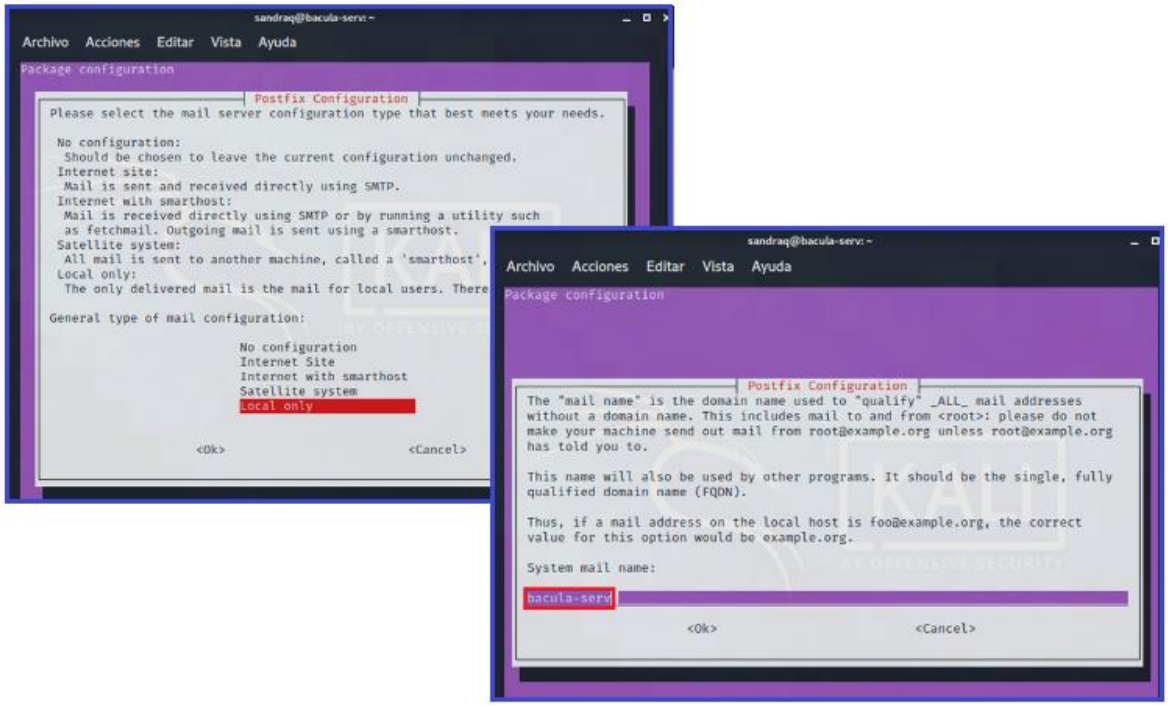
Figura 168. Instalación servidor Bacula

```
sandraq@bacula-serv:~$ sudo apt install bacula-server bacula-client
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
The following additional packages will be installed:
  bacula-bscan bacula-common bacula-common-pgsql bacula-console bacula-director
  bacula-director-pgsql bacula-fd bacula-sd bsd-mailx dbconfig-common dbconfig-pgsql
  libllvm10 liblockfile-bin liblockfile1 libpq5 libsensors-config libsensors5 mt-st
  mtx postfix postgresql postgresql-12 postgresql-client postgresql-client-12
  postgresql-client-common postgresql-common sysstat
Suggested packages:
  gdb bacula-doc dds2tar scsitools lm-sensors procmail postfix-mysql postfix-pgsql
  postfix-ldap postfix-pcre postfix-lmdb postfix-sqlite sasl2-bin | dovecot-common
  resolvconf postfix-cdb postfix-doc postgresql-doc postgresql-doc-12 libjson-perl
  isag
The following NEW packages will be installed:
  bacula-bscan bacula-client bacula-common bacula-common-pgsql bacula-console
  bacula-director bacula-director-pgsql bacula-fd bacula-sd bacula-server bsd-mailx
  dbconfig-common dbconfig-pgsql libllvm10 liblockfile-bin liblockfile1 libpq5
  libsensors-config libsensors5 mt-st mtx postfix postgresql postgresql-12
  postgresql-client postgresql-client-12 postgresql-client-common postgresql-common
  sysstat
0 upgraded, 29 newly installed, 0 to remove and 3 not upgraded.
Need to get 34.0 MB of archives.
After this operation, 133 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Fuente: elaboración propia.

Cuando aparezca el asistente de configuración de Postfix, seleccionar la opción “Local only”, seguidamente establecer el nombre de correo del sistema y seleccionar la opción ok, como se muestra a continuación:

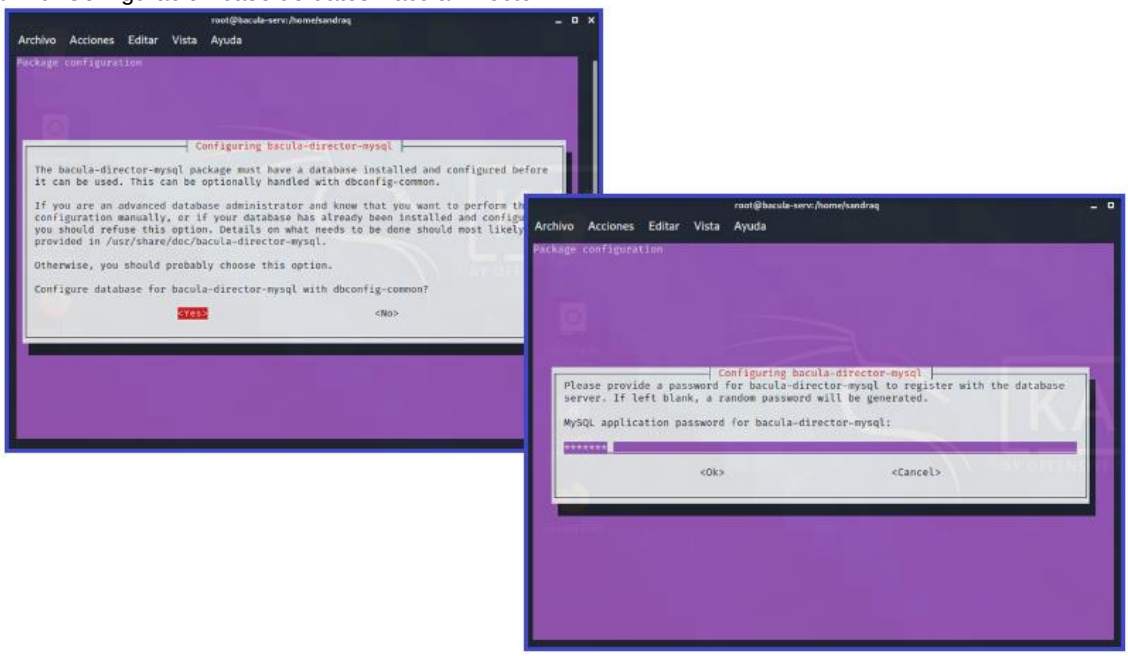
Figura 169. Configuración Postfix en servidor Bacula



Fuente: elaboración propia.

Una vez hecho esto se sigue el proceso de instalación hasta pedir que se inicie la configuración de la base de datos de bacula, como se muestra en la Figura a continuación, en donde se selecciona la opción “yes” y en la siguiente pantalla se establece y confirma la contraseña para la conexión con el servidor de la base de datos de bacula

Figura 170. Configuración base de datos Bacula Director



Fuente: elaboración propia.

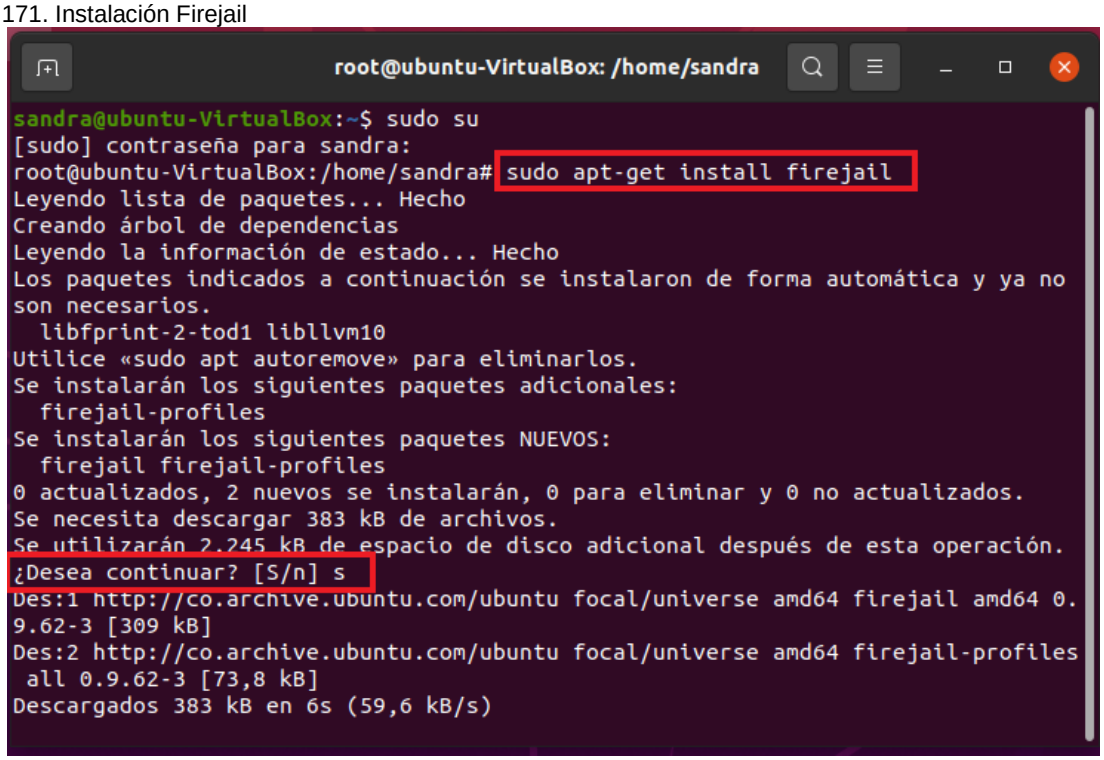
A.5 INSTALACION SERVIDOR SANDBOX

El servidor Sandbox se habilita en una máquina virtual con sistema operativo Ubuntu sobre el cual se realiza la instalación la herramienta open Source denominada Firejail la cual hace uso de las opciones de seguridad de Linux para aislar los procesos. Las características de la maquina virtualizada para este servidor, en VirtualBox son las siguientes:

- Sistema operativo Ubuntu Desktop 64 bits
- Memoria Ram 2 GB
- Procesador: 1 CPU
- Disco duro VDI 20 GB
- Unidad óptica
- 1 adaptadores de red en modo red interna

Para el proceso de instalación de Firejail, se inicia sesión en la maquina Linux, se procede a abrir un terminal y se escribe el comando: sudo apt-get install firejail, cuando se solicite la confirmación se presiona la tecla si, como se observa en la siguiente Figura

Figura 171. Instalación Firejail



Fuente: elaboración propia.

ANEXO B

Link Sustentación Proyecto : https://youtu.be/vGZR-CnuiWA