# DISEÑO DE UN CENTRO DE OPERACIÓN DE SEGURIDAD – SOC PARA LA EMPRESA PLATINO SISTEMA

MAILON PÉREZ FERNÁNDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SINCELEJO - SUCRE
2022

# DISEÑO DE UN CENTRO DE OPERACIÓN DE SEGURIDAD – SOC PARA LA EMPRESA PLATINO SISTEMA

MAILON PEREZ FERNANDEZ

Proyecto de Grado – proyecto aplicado presentado para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMATICA

Director de proyecto
MSC. KATERINE MARCELES VILLALBA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SINCELEJO - SUCRE
2022

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Sincelejo., 05/07/22

## DEDICATORIA

Con amor dedico este trabajo a mi padre, que con sus buenos consejos y constante apoyo me ha ayudado a seguir adelante con este proceso académico, a mi madre que con su amor y dedicación ha sido el pilar para que siga adelante en cada uno de los tropezones que he tenido y a mi hermana que siempre ha sido mi apoyo moral en las buenas y en las malas situaciones por las que he atravesado.

## AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, al tutor Eduard Antonio Mantilla Torres y director Fernando Zambrano Hernández quienes me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

## CONTENIDO

pág.

## CONTENIDO DE CUADROS

pág.

## CONTENIDO DE ILUSTRASIONES

pág

## GLOSARIO

**Backup:** Son copias de seguridad que se le realizan a un archivo o sistema a nivel general o especifico con el fin de realizar recuperación de información en caso de que se presenten algún fallo especifico en afecte estos recursos.

**Centro de Respuesta a Incidentes Cibernéticos:** Se puede definir como un conjunto de dependencias relacionadas con la seguridad informática o un grupo de expertos en seguridad de la información que tiene como objetivo mitigar, gestionar y controlar los incidentes informáticos en todos sus aspectos, tanto documenta, como procedimental y practico.

**Centro de operaciones de seguridad (SOC):** Los centros de operaciones de seguridad son un conjunto de expertos en seguridad informática enfocados en la parte técnica de la identificación de delitos informáticos en tiempo real y la detección de vulnerabilidades en sistemas de información, que pueda ser críticos para la integridad de la información y la continuidad del negocio de esta.

**Confidencialidad:** Es la característica de la seguridad de la información la cual tiene como objetivo garantizar que la información solo pueda ser accedida por las personas que tenga autorización a esta.

**Correlacionador de eventos**: Servicio encargado de realizar gestión de reportes en base a infraestructura lógica o fisca de la organización, con el fin de tener acciones preventivas y correctivas respecto a estos.

**Integridad:** Es la propiedad de la seguridad de la información la cual tiene como

objetivo garantizar que la información al momento de ser enviada de un entorno a otro no presente alteraciones en su contenido o cualquier otro atributo.

**Seguridad informática:** Procedimiento por el cual se busca mantener la integridad, disponibilidad y confiabilidad de la información en los activos digitales de una organización.

**Seguridad de la información:** Conjunto de medidas de prevención que permitan resguardar la información tanto física como digital en una organización.

**Servidor:** Puede entenderse como servidor tanto el software que realiza ciertas tareas en nombre de los usuarios, como el ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer y gestionar datos de algún tipo de forma que estén disponibles para otras máquinas que se conecten a él.

**Servidor de monitoreo:** Servicio especializado en realizar monitoreo a los recursos físico y digitales de un host.

**Virtualización:** La virtualización es un medio para crear una versión virtual de un dispositivo o recurso, como un servidor, o una red, en una máquina física, generalmente con el apoyo de un software que implementa una capa de abstracción para que la maquina física y la virtual puedan comunicarse y compartir recursos.

**Sandbox:** Entorno seguro de pruebas predispuesto para realizar ejecución y validación de programas y archivos, con el fin de identificar la funcionalidad y el buen uso seguro que tiene con los sistemas del entorno.

## RESUMEN

Platino Sistemas, es una organización colombiana que presta servicios de seguridad para la protección de la Información. Una de las metas para el año 2022 es crear un Centro de Respuesta a Incidentes Cibernéticos en el ámbito de CSIRT, el cual tendrá como propósito crear y gestionar las funciones de respuesta a incidentes cibernéticos, ofreciendo servicios que permitan dar soporte a sus clientes teniendo presente el nivel de servicio contratado, los cuales pueden ser de respuesta a incidentes o de gestión a vulnerabilidades.

Dado que la empresa Platino Sistemas cuenta con empleados capacitados, entre ellos un experto en seguridad informática dentro del equipo de trabajo, el cual se le ha asignado la tarea de liderar el diseño técnico que permita dar desarrollo a las actividades propias del CSIRT, enfocándose en la primera etapa en el diseño de un Centro de Operaciones de Seguridad – SOC y en la Segunda Etapa, en la propuesta de Hardware y Software a usar para el desarrollo de las actividades propias del CSIRT.

Teniendo claro la problemática planteada por la empresa Platino Sistemas, y la necesidad evidente de aplicar diferentes controles, medidas y servicios que solventes la necesidad de seguridad en la organización, primeramente se planteó la propuesta de diseño de un centro de operaciones de seguridad SOC; esto tomando los diferentes marcos conceptuales, legales y estandarizados que permitieron en base a una propuesta técnica, seleccionar la infraestructura, composición, estructuración y aplicación de herramienta acordes a las necesidades serviciales de seguridad con las que carecía la organización.

Para lograr el desarrollo de la propuesta antes mencionada, en primer lugar se definió una estructura de roles operacionales que componen el equipo de trabajo de centro de operaciones de seguridad (SOC) para apoyar al desarrollo de los servicios de seguridad especificados en el enfoque técnico con el fin de apoyar la salvaguarda de la información de la organización, Seguido de esto, se estableció una propuesta de tecnología para las operaciones propias desarrolladas para un centro de operaciones de seguridad teniendo en cuenta las necesidades de seguridad y servicios de la empresa. Por otra parte se realizó la identificación de las herramientas de hardware comercial y software libres utilizadas para el desarrollo de las actividades propias del SOC haciendo énfasis puntual en el enfoque técnico de servicios de seguridad establecido por la organización y finalmente se realizó un diseño lógico de laboratorio controlado y virtualizado utilizando máquinas virtuales en VirtualBox para solventar los servicios de Monitoreo, correlacionador de eventos, servidor de copias de seguridad y servicio de Sandox.

El desarrollo de las actividades para el cumplimiento de las necesidades organizaciones en el empleo de servicios de servicios orientados a la seguridad aplicados en centros de operaciones de seguridad, se realizaron bajo una metodología de investigación cualitativa utilizando métodos inductivos, está sustentada por la identificación de artículos científicos, grabaciones de audios, documentación web, las cuales sustentan en sus resultados la correcta aplicación de centros de respuestas a incidentes cibernéticos así como los centros de operaciones de seguridad, utilizando servicios que ayuden a solventar necesidades generales de seguridad, y a su vez que apoyen al desarrollo de las actividades que soportan un CSIRT.

Sintonizando lo anterior, se puede concluir que la aplicación de un Centro de Operaciones de Seguridad basado en criterio técnicos y utilizando herramientas libres, pueden solventar las necesidades de servicio de organizaciones a mediana escala, permitiéndoles así ejecutar actividades propias de un SOC, sin la necesidad

de realizar adquisición de herramientas comerciales que puedan generar un desequilibrio en factores de costo-beneficio y que imposibilitarían la idea de adquisición de servicios de seguridad de Ti y mucho menos el soporte ya sea semana, mensual o anual de las mismas.

## ABSTRACT

Platino Sistemas, is a Colombian organization that provides security services for the protection of Information. One of the goals for the year 2022 is to create a Cyber Incident Response Center in the CSIRT field, the purpose of which will be to create and manage cyber incident response functions, offering services that allow it to support its clients, bearing in mind the level of contracted service, which can be incident response or vulnerability management.

Since the company Platino Sistemas has trained employees, including an expert in computer security within the work team, who has been assigned the task of leading the technical design that allows the development of the CSIRT's own activities, focusing on the first stage in the design of a Security Operations Center - SOC and in the Second Stage, in the proposal of Hardware and Software to be used for the development of the CSIRT's own activities.

Being clear about the problems raised by the company Platino Sistemas, and the evident need to apply different controls, measures and services that solve the need for security in the organization, firstly, the design proposal for a SOC security operations center was proposed; this taking the different conceptual, legal and standardized frameworks that allowed, based on a technical proposal, to select the infrastructure, composition, structuring and application of the tool more in line with the serviceable security needs that the organization lacked.

To achieve the development of the aforementioned proposal, first a structure of operational roles was defined that make up the security operations center (SOC) work team to support the development of the security services specified in the

technical approach with In order to support the organization's information safeguarding, Following this, a technology proposal was established for its own operations developed for a security operations center, taking into account the company's security and service needs. On the other hand, the identification of the commercial hardware and free software tools used for the development of the SOC's own activities was carried out, with specific emphasis on the technical approach of security services established by the organization and finally a logical laboratory design was carried out. controlled and virtualized using virtual machines in VirtualBox to solve the Monitoring services, event correlator, backup server and Sandox service.

The development of activities to meet the needs of organizations in the use of security-oriented services applied in security operations centers, were carried out under a qualitative research methodology using inductive methods, supported by the identification of articles scientists, audio recordings, web documentation, which support in their results the correct application of response centers to cyber incidents as well as security operations centers, using services that help solve general security needs, and in turn that support to the development of the activities that support a CSIRT.

Tuning the above, it can be concluded that the application of a Security Operations Center based on technical criteria and using free tools, can solve the service needs of medium-scale organizations, thus allowing them to carry out activities typical of a SOC, without the need of acquiring commercial tools that can generate an imbalance in cost-benefit factors and that would make the idea of acquiring IT security services impossible, much less their weekly, monthly or annual support.

# INTRODUCCIÓN

La información en la actualidad es uno de los activos de vital importancia para los procesos de una organización, desde un ámbito meramente técnico, hasta aspectos enteramente administrativos, aun así, también presentan numerosos riesgos con relación a su integridad, disponibilidad y confiabilidad en casos de delitos informáticos que apunten a estos directamente. Debido a este tipo de situaciones, las empresas deberían emplear un conjunto estandarizado, de procedimientos, técnicas, practicas, grupos, entre otras modalidades enfocadas a la seguridad de la información que permitan implementar un mayor control sobre todos los activos de una organización y su infraestructura tecnológica y física.

Platino sistemas es una organización colombiana posicionada a nivel nacional, la cual tienen como modelo de negocios la prestación de servicios de seguridad para la protección de la información de diferentes tipos de organización. Siendo este su principal fundamento en su modelo de negocios, la necesidad de automatizar, gestionar y controlar la seguridad de la información y los datos en una organización se hace vital para todos los procesos que la constituyen, evaluación de riesgos, respuestas a incidentes, gestión de vulnerabilidades, entre otros temas que precisan de unos niveles de operatividad y transparencia importantes.

Con base en lo anterior, el presente proyecto tiene como finalidad la creación de un centro de respuesta a incidentes cibernéticos en el ámbito CSIRT, sobre el cual se fundamentará el desarrollo de un centro de operaciones de seguridad SOC partiendo desde la creación del diseño técnico del CSIRT y seguido por una etapa de desarrollo hardware-software que dé cumplimiento a las actividades propias de CSIRT.

# 1. DEFINICIÓN DEL PROBLEMA

Actualmente la ciberseguridad es uno de los factores más importantes en esta era digital, puesto que la idea de mantener la continuidad del negocio de la organización es cada vez más significativa sobre los sistemas, aplicaciones, software y hardware. La empresa Platino sistemas al ser una de las principales empresas en prestación de servicios de seguridad para la protección de la información, se topa con muchos casos relacionados a incidentes informático y a vulnerabilidades existentes en sistemas de información. Por ende, la idea de constituir y/o constituir una herramienta, grupo, aplicativo o artefacto para suplir esta necesidad es necesaria.

Una de las iniciativas que pretende acoger esta organización es la creación de un centro de respuestas a incidentes cibernéticos, el cual le permitirá por medio de un centro de operaciones de Seguridad realizar actividades de gestión, control y detección de incidentes cibernéticos y gestión de vulnerabilidades, los cuales presentan un factor crítico para la seguridad de la información y continuidad de negocio de la organización.

## 1.1 ANTECEDENTES DEL PROBLEMA

Como primer antecedente problema para la aplicación de este tipo de centros de respuestas a incidentes cibernéticos, se basan en la falta de gestión de incidentes cibernéticos que tienen las organizaciones actualmente, ya que, la poca conciencia frente al tema y las repercusiones que pueden conllevar a ser víctima de uno de estos actos delictivos se debe a que están muy desinformadas.

Seguido de esto, se tiene la poca gestión con base a las vulnerabilidades de la infraestructura cibernética que tienen las organizaciones actualmente, en lo que

respecta al uso de herramientas o dispositivos sin previo asesoramiento y dejando entradas a terceros a que realicen actos delictivos en la organización.

Otro aspecto o antecedente del problema y no menos importante que los anteriores, es la falta de cultura con relación a temas de seguridad informática y ciberseguridad en el ámbito organizacional.

## 1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo influiría la creación de un Centro de Respuesta a Incidentes Cibernéticos en el ámbito CSIRT, en el mejoramiento de las problemáticas relacionadas a la detección de incidentes cibernéticos y la gestión de vulnerabilidades tecnológicas en las organizaciones que cuenta con los servicios de seguridad de la empresa Platino Sistemas?

# 2 JUSTIFICACIÓN

A partir del problema planteado se hace necesario la creación de un Centro de Respuesta a Incidentes Cibernéticos en el ámbito CSIRT, el cual permitirá realizar una mejor gestión sobre los incidentes cibernéticos identificados sobre una superficie de ataque interna o externa de la organización. Lo anterior con el fin de preservar los principios de seguridad de información en los diferentes activos de tecnología de información identificados. Por lo tanto, para la ejecución de las necesidades antes mencionadas, se precisa la aplicación de un Centro de Operaciones de Seguridad – SOC, que tiene como función prevenir, monitorear y controlar los eventos de seguridad relacionados con los sistemas y la redes en las organizaciones, mediante actividades que permiten la constitución del CSIRT.

La creación de este tipo de centros presenta beneficios organizacionales importantes cuando hablamos de ciberseguridad, puesto que permite a la organización orientar la seguridad en ámbitos específicos técnicos que apoyen a la protección y mitigación de sucesos informáticos críticos para la continuidad de negocio de una empresa. Más específicamente hablando, estos grupos de apoyo permiten mitigar el suceso de ataques informáticos, el monitoreo en tiempo real de actividad no natural en una red de información, la detección de vulnerabilidades en harás de buscar soluciones a estas, entre otras actividades en beneficio a la detección temprana de amenazas que puedan significar un peligro para la organización.

# 3 OBJETIVOS

## 3.1 OBJETIVOS GENERAL

Diseñar un centro de operación de seguridad – SOC para la empresa platino sistemas

## 3.2 OBJETIVOS ESPECÍFICOS

1. Definir los roles del equipo de trabajo del centro de operaciones de seguridad en la empresa platino sistemas.

2. Establecer una propuesta de tecnología para las operaciones propias del centro de operaciones de seguridad en la empresa platino sistemas.

3. Identificar las herramientas de hardware y software libre para el desarrollo de las actividades del SOC.

4. Realizar un diseño lógico de laboratorio controlado y virtualización de las siguientes herramientas: Servidor de Monitoreo, correlacionador de eventos, servidor de copias de seguridad y Servicio de Sandbox.

# 4 MARCO REFERNCIAL

## 4.1 MARCO TEÓRICO

En la actualidad con el auge de la tecnología y su constante crecimiento exponencial tanto física como virtual, se plantean nuevas formas de explosión de vulnerabilidades por parte de los ciberdelincuentes para adquirir beneficios específicos de cada una de estas nuevas tecnologías. Es por ello, que la creación de nuevas técnicas, grupos, herramientas, entre otros métodos de protección es cada vez más necesario, pues la gran mayoría de las organizaciones buscan prevenir y mitigar ciber ataques o incidentes cibernéticos que incurran a vulnerar la integridad, disponibilidad y confiabilidad de la información que estas manejan.

Para este tipo de acontecimientos se han probado diversos sistemas que en su medida son efectivos tomando como base su foco de especialidad. Actualmente en el mercado se encuentran varios, sistemas de gestión de seguridad de la información, Centro de Respuesta a Incidentes Cibernéticos, centro de operaciones de seguridad, entre muchos otros, que tiene diferentes focos de estudio, pero todos apuntan a una protección en general, seguridad de la información con relación a su integridad, disponibilidad y confiabilidad.

En este apartado se tomará específicamente como referencia los Centros de respuestas a incidentes cibernéticos, los cuales a nivel mundial hoy en día se caracterizan por brindar medidas de contención contra ataques cibernéticos, enfatizando en detección oportuna de ataques cibernéticos, detección de vulnerabilidades en sistemas de información, capacidad de realización de pruebas de penetración para identificar puertas de acceso no validadas, prevención de crisis y muchas otras funcionalidades que permitan la protección en pro a la información graduada por niveles de criticidad en las organizaciones.

Estos centros a nivel particular se constituyen de varios componentes para su funcionalidad en general. Uno de estos es el centro de operaciones de seguridad (SOC), los cuales se constituyen como la parte técnica operacional que trabaja con numerosas herramientas de gestión y control de incidentes de seguridad con el fin de salvaguardar la información en las organizaciones. Estos centros permiten formar mediante un conjunto de tareas la concepción y ejecución del centro de respuestas a incidentes cibernéticos en el ámbito CSIRT. Estas tareas se ejecutan desde herramientas para el monitoreo de servidores web, como herramientas para desarrollo de copias de seguridad y herramientas de análisis forense.

## 4.2 MARCO CONCEPTUAL

**4.2.1. Centro de Respuesta a Incidentes Cibernéticos:** Se puede definir como un conjunto de dependencias relacionadas con la seguridad informática o un grupo de expertos en seguridad de la información que tiene como objetivo mitigar, gestionar y controlar los incidentes informáticos en todos sus aspectos, tanto documenta, como procedimental y practico.[1]

**4.2.2. Centro de operaciones de seguridad (SOC):** Los centros de operaciones de seguridad son un conjunto de expertos en seguridad informática enfocados en la parte técnica de la identificación de delitos informáticos en tiempo real y la detección de vulnerabilidades en sistemas de información, que pueda ser críticos para la integridad de la información y la continuidad del negocio de esta.[2]

[1] GOBIERNO DIGITAL. [Sitio web]; Bogotá: Ministerio de Tecnologías de la Información y las Comunicaciones. [Consulta: 20 de marzo 2022]. Disponible: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/CSIRT-Gobierno/
[2] ORACLE. [Sitio web]. Redwood Shores, CA. Oracle Corporation. [Consulta: 20 de marzo 2022]. Disponible: https://www.oracle.com/es/database/security/que-es-un-soc.html

**4.2.3. Seguridad informática:** Procedimiento por el cual se busca mantener la integridad, disponibilidad y confiabilidad de la información en los activos digitales de una organización.[3]

**4.2.4. Seguridad de la información:** Conjunto de medidas de prevención que permitan resguardar la información tanto física como digital en una organización.[4]

**4.2.5. Confidencialidad:** Es la característica de la seguridad de la información la cual tiene como objetivo garantizar que la información solo pueda ser accedida por las personas que tenga autorización a esta.[5]

**4.2.6. Integridad:** Es la propiedad de la seguridad de la información la cual tiene como objetivo garantizar que la información al momento de ser enviada de un entorno a otro y no presente alteraciones en su contenido o cualquier otro atributo. [6]

**4.2.7. Disponibilidad:** Es un atributo de la seguridad de la información el cual tiene como objetivo garantizar que la información esté disponible

[3] CAVALLI, Enrico, *et a*l. Information security concepts and practices: the case of a provincial multi-specialty hospital. Elsevier. [Consulta: 20 de marzo 2022]. Disponible: https://www.sciencedirect.com/science/article/abs/pii/S1386505603002132#!

[4] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Sistemas de Gestión de Seguridad de la información. NTC-ISO/IEC 27000:2016. Bogotá D.C., Colombia. [Consulta: 20 de marzo 2022]. Disponible: https://www.iso27000.es/glosario.html

[5] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Guía 5 para la Gestión y Clasificación de Activos de Información. [Sitio web]. Bogotá. [Consulta: 20 de marzo 2022]. Disponible: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

[6] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Guía 5 para la Gestión y Clasificación de Activos de Información. [Sitio web]. Bogotá. [Consulta: 20 de marzo 2022]. Disponible: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

siempre que se solicite por el personal que tenga acceso a esta. [7]

**4.2.8. Backup**: Son copias de seguridad que se le realizan a un archivo o sistema a nivel general o específico con el fin de realizar recuperación de información en caso de que se presenten algún fallo particular que afecte los recursos.[8]

**4.2.9. Servidor de monitoreo**: Servicio especializado en realizar monitoreo a los recursos físico y digitales de un host.[9]

**4.2.10. Correlacionador de eventos:** Servicio encargado de realizar gestión de reportes en base a infraestructura lógica o física de la organización, con el fin de tener acciones preventivas y correctivas respecto a estos.[10]

**4.2.11. Sandbox:** Entorno seguro de pruebas predispuesto para realizar ejecución y validación de programas y archivos, con el fin de identificar la funcionalidad y el buen uso seguro que tiene con los sistemas del entorno.[11]

**4.2.12. Gestión de incidentes:** La gestión de incidentes es el proceso de gestionar las interrupciones del servicio de TI y restaurar los servicios

[7] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Guía 5 para la Gestión y Clasificación de Activos de Información. [Sitio web]. Bogotá. [Consulta: 20 de marzo 2022]. Disponible: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

[8] CISCO. Backing Up and Restoring Data. [Sitio web]. EE.UU. [Consulta: 20 de marzo 2022]. Disponible: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/unity_exp/rel3_1/administration/guide/voicemail/11bkrst.html

[9] NORTH NETWORKS. ¿Qué es Nagios?. Ciudad de México. [Consulta: 20 de marzo 2022]. Disponible: https://www.north-networks.com/que-es-nagios/

[10] GLPI. GLPI Network Cloud. Paris, Île-de-France. [Consulta: 20 de marzo 2022]. Disponible: https://glpi-project.org/es/recursos/

[11] ROSENCRANCE, Linda. Sandbox (software testing and security). [Consulta: 20 de marzo 2022]. Disponible: https://www.techtarget.com/searchsecurity/definition/sandbox

dentro de los acuerdos de nivel de servicio (SLA) acordados.[12]

**4.2.13. Ciberdefensa:** capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. La ciberdefensa implica el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética.[13]

**4.2.14. Respuesta a incidentes:** La mitigación de violaciones de políticas de seguridad y prácticas recomendadas.[14]

**4.2.15. CISO CHIEF:** El CISO (Chief Information Security Officer) es el director de seguridad de la información. Básicamente es un rol desempeñado a nivel ejecutivo y su función principal es la de alinear la seguridad de la información con los objetivos de negocio. De esta forma se garantiza en todo momento que la información de la empresa está protegida adecuadamente.[15]:

**4.2.16. Remediación de seguridad:** arreglar o parchear la vulnerabilidad

[12] MANAGEENGINE, ¿Qué es la gestión de incidentes ITIL?. SERVICEDESK PLUS. [En línea]. Proveedor de productos comerciales. 2020. [Consulta: 30 de mayo de 2022]. Disponible: https://www.manageengine.com/latam/service-desk/itil-incident-management/que-es-la-gestion-de-incidentes-itil.html#:~:text=La%20gesti%C3%B3n%20de%20incidentes%20es,de%20servicio%20(SLA)%20acordados.

[13] COMPES 3995. POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL. Consejo Nacional De Política Económica Y Social República De Colombia Departamento Nacional De Planeación. [En Línea]. Departamento nacional de Planeación. 2020. [Consulta: 30 de mayo de 2022]. Disponible: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

[14] CICHONSKI P, MILLAR T, *at ep*. Computer Security Incident Handling Guide. National Institute of Standards and Technology. 2012. [Consulta: 30 de mayo de 2022]. Disponible: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[15] INCIBE. CEO, CISO, CIO ¿Roles en ciberseguridad?. Instituto nacional de ciberseguridad. [En línea]. 2016. [Consulta: 30 de mayo de 2022]. Disponible: https://www.incibe.es/protege-tu-empresa/blog/ceo-ciso-cio-roles-ciberseguridad

antes de que pueda llegar a ser una amenaza de seguridad. Por lo general, es el equipo de seguridad de una organización, los propietarios de los sistemas y los administradores de sistemas quienes se reúnen para determinar qué acciones son las más apropiadas.[16]

**4.2.17. Brechas de seguridad**: Una brecha de seguridad es un incidente que permite el acceso no autorizado a datos informáticos, aplicaciones, redes o dispositivos. Es decir, permite acceder sin autorización a información. Normalmente, se produce cuando un intruso logra sortear los mecanismos de seguridad.[17]

**4.2.18. Cacería de amenazas complejas:** Threat hunting, también conocida como caza de amenazas cibernéticas, es un enfoque proactivo para identificar amenazas previamente desconocidas o no remediadas en curso, dentro de la red de una organización.[18]

## 4.3 ANTECDENTES O ESTADO ACTUAL

Teniendo en cuenta la información antes mencionada, se citan algunos casos de organizaciones las cuales implementaron para sus actividades aseguramiento a la información y/o algún sistema de protección para esta. Primeramente, se tiene el Diseño y planificación de un centro de operaciones de seguridad informática aplicado como servicio por la organización A3SEC bajo marcos de trabajo propuestos por Sans, ISACA y NIST, el cual fue desarrollado con la finalidad de realizar una aplicación de estos bajo los términos de la organización A3SEC,

[16] SITCAWICH T, Vulnerability Remediation vs. Mitigation: What's the Difference?. RAPID1. [En línea]. Articulos POST. 2020. [Consulta: 30 de mayo 2022]. Disponible: https://www.rapid7.com/blog/post/2020/09/14/vulnerability-remediation-vs-mitigation-whats-the-difference/

[17] KASPERSKY. ¿Qué es una brecha de seguridad?. [En línea]. Corporación. [Consulta: 30 de mayo 2022]. Disponible: https://www.kaspersky.es/resource-center/threats/what-is-a-security-breach

[18] IBM. What is threat hunting?. [En línea]. Corporación. . [Consulta: 30 de mayo 2022]. Disponible: https://www.ibm.com/topics/threat-hunting

buscando así mitigar los accidentes relacionados con la seguridad de la información.[19]

Seguido se encuentra el proyecto Inteligencia local en un centro de operaciones de ciber-seguridad el cual tiene como base de estudio realizar una comparación entre cuales son los beneficios que tiene trabajar con herramientas individuales específicas en base a la mitigación de incidentes informáticos y los beneficios de tener una estructuración de un SOC, el cual cumple meramente con actividades de monitoreo. en cambio se debe enfocar a temas de testing, monitoreo en tiempo real, capacitaciones constantes, detección de puertas traseras, entre otros sucesos que ayuden a la protección de la información en la organización.[20]

A continuación, se tiene la empresa SECUINFOR S.A, la cual realizó la Definición del proceso de clasificación de los activos de información para el centro de operaciones de seguridad informática Secuinfor s.a., este proceso tuvo como objetivo la realización de la caracterización adecuada de la clasificación de la información para un centro de operaciones de seguridad informática con el fin de establecer parámetros de revisión mucho más efectivos y eficaces al momento de tomar decisiones en base a esta.[21]

---

[19] BONILLA, Billy y ROJAS, Anthony. Diseño y planificación de un centro de operaciones de seguridad informática aplicado como servicio por la organización A3SEC bajo marcos de trabajo propuestos por Sans, ISACA y NIST. [En línea]. Trabajo especialidad. Bogotá, Universidad Piloto de Colombia. 2019. [Consulta: 20 de marzo 2022]. Disponible: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/5814/00005153.pdf?sequence=1&isAllowed=y

[20] VILCAR ROMERO, Ladi y VILCHEZ, Evit. Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones. [En línea]. Trabajo Magister. Lima. Universidad peruana de ciencias aplicadas. 2018. [Consulta: 20 de marzo 2022]. Disponible: https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/624832/VilcarromeroZ_L.pdf?sequence=11&isAllowed=y

[21] PRENDES MORENO, Michelle Ivette. “DEFINICIÓN DEL PROCESO DE CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN PARA EL CENTRO DE OPERACIONES DE SEGURIDAD INFORMÁTICA SECUINFOR S.A. [En línea]. Trabajo magister. Escuela Superior Politécnica Del Litoral. 2016. [Consulta: 20 de marzo 2022]. Disponible: http://www.dspace.espol.edu.ec/xmlui/bitstream/handle/123456789/37400/D-103388.pdf?sequence=-1&isAllowed=y

También se presenta una propuesta de un modelo de centro de operaciones de seguridad (SOC) para la fuerza aérea colombiana, el cual tenía como objetivo principal la inclusión de estos centros para permitir el monitoreo constante y la gestión de procedimientos de gestión de la seguridad informática con aras de mantener la confiabilidad, integridad y disponibilidad de la información en tiempo real.[22]

Y por último el proyecto de Proceso para Definir y Establecer un Centro de Operaciones de Seguridad (SOC) en una Organización Financiera, el cual se fundamenta en relación a los lineamientos, procesos y necesidades que tienen las entidades financieras con relación al manejo y seguridad que se le suministra a su información crítica; por ende propone la implementación de centros de operaciones de seguridad con el fin de mitigar los temas relacionados con la seguridad de la información y la seguridad de los servicios y sistemas que gestionan esta.[23]

Teniendo en cuenta este panorama histórico y actual con relación a la seguridad de la información, la ciberseguridad y los mecanismos utilizados para la gestión de estos, se puede evidenciar un importante número de casos relacionados a la implementación de herramientas en pro de la gestión, seguimiento y control de la seguridad en sistemas de información. Esto demuestra que cada día la seguridad en las tecnologías e información están siendo cada vez más requeridas, puesto que, la idea de mantener los sistemas seguros y confiables se ha vuelto un punto

[22] MORALES, Carlos, *et al*. PROPUESTA DE UN MODELO DE CENTRO DE OPERACIONES DE SEGURIDAD (SOC) PARA FUERZA AEREA COLOMBIANA. [En línea]. Trabajo especialidad. Bogotá. Universidad Piloto de Colombia. 2014. [Consulta: 20 de marzo 2022]. Disponible: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2786/trabajo%20de%20grado1627.pdf?sequence=1&isAllowed=y

[23] TORRES, Román y María José. Proceso para Definir y Establecer un Centro de Operaciones de Seguridad (SOC) en una Organización Financiera. [En línea]. Trabajo Master. Guayaquil. Universidad internacional de la roja. 2019. [Consulta: 20 de marzo 2022]. Disponible: https://reunir.unir.net/bitstream/handle/123456789/8169/ROMAN%20TORRES%2c%20MARIA%20JOSE.pdf?sequence=1&isAllowed=y

prioritario para la integridad y confiabilidad tanto de la información como el manejo de esta.

## 4.4 MARCO CIENTÍFICO O TECNOLÓGICO

En el desarrollo del SOC, se utilizaron los siguientes recursos tecnológicos:

**4.4.1 Computadora.** Dispositivo electrónico utilizado para realizar cualquier tipo acción, ya sea, desde buscar información, hasta realizar programas informáticos que ayuden con una necesidad especifica.

**4.4.2 Internet.** Red mundial de comunicaciones interconectada, que permite tener acceso de información desde cualquier parte del mundo o cualquier tipo de dispositivo que cumpla con las características.

**4.4.3 Motor de búsqueda web.** Herramienta utilizada para realizar búsquedas web por medio de internet en millones de páginas web al tiempo.

**4.4.4 Bases de datos virtuales.** Repositorios virtuales de información que permiten la adquisición de esta, para ser usada o de carácter investigativo según interés.

## 4.5 MARCO LEGAL

Los delitos informáticos son considerados una violación grabe a la información y a los datos que manejan, ya sean sistemas de información o personas a nivel general. Este concepto se aplica a nivel mundial y el estado colombiano no es la excepción. En este país existen leyes que protegen a las personas que se vean afectadas a este tipo de actos delictivos, más específicamente la ley 1273:2009, que tiene como función establecer pautas, reglas y sanciones en contra de delincuentes que estén relacionados directamente con tratado de información, violación de esta y manipulación no autorizada de sistemas de información.

Teniendo en cuenta esto a la fecha los delitos informáticos más comunes y que influyen directamente a la violación de las leyes planteadas en la ley 1273[24] son:

- ✓ Estafas.
- ✓ Acoso contra menores de edad.
- ✓ Falsificación de documentos.
- ✓ Falsificación de ID.
- ✓ El Skimming.
- ✓ Smishing.

Este tipo de situaciones cada día son más frecuentes por la falta de cultura en seguridad con la que cuenta el estado colombiano. Medidas de prevención de acceso, culturalización de ciberseguridad y la actualización en temáticas relacionadas con Ciberseguridad, son factores que influyen a la incurrencia de estos casos sin ninguna base de apoyo por el desconocimiento de las leyes que soportan la ejecución de estos actos ilícitos.

Uno de los casos no relacionados, pero también muy conocidos por su ejecución a nivel mundial es el DDoS, el cual consiste en denegar servicios de un aplicativo o un sistema de información por medio de Botnets con el fin de crear entradas a sistemas y adquirir información crítica que puedan usar para un beneficio en específico.

Empresas a nivel nacional y mundial se exponen a este tipo de sucesos cibernéticos por no presentar medidas de contingencia contra este tipo de acción. Por ende, entran las organizaciones como Platino sistemas, la cual, por medio de

[24] COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 1273. (5, enero, 2009). por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". (Diario Oficial No. 51945 - 11 de febrero de 2022).

centros de apoyo contra incidentes y vulnerabilidades cibernéticas, buscará mitigar este tipo de concurrencias en las organizaciones que soliciten sus servicios.
En base a lo anterior, estas son unas de las penas o sanciones a las cuales están relacionados la ejecución de cualquiera de los delitos cibernéticos que atenten contra la integridad, disponibilidad y confiabilidad de la información y la organización misma.

1. Acceso abusivo a un sistema informático. Este delito está relacionado con el acceso no autorización a un sistema, el cual incurriría a una pena de 48 a 96 meses de cárcel y una multa de 1000 salarios mínimos legales mensuales vigentes.

2. Obstaculización ilegítima de sistema informático o red de telecomunicación. Este delito está relacionado con el impedimento del funcionamiento natural de un sistema, el cual incurriría a una pena de 48 a 96 meses de cárcel y una multa de 1000 salarios mínimos legales mensuales vigentes.

# 5 DISEÑO METODOLOGICO

La metodología empleada para el desarrollo del proyecto es la cualitativa utilizando métodos inductivos. Este busca establecer tendencias narrativas causales dentro de los diferentes hechos correlacionados con la solución al objetivo general plasmado, para luego de esto realizar análisis en base a las soluciones y establecer patrones de soluciones que puedan solventar la necesidad de la empresa en cuestión.[25]

La base de la investigación cualitativa utilizando métodos inductivos se sustenta en su mayoría por la identificación de referencias de artículos científicos, grabaciones de audio, documentación web, los cuales tuvieron como antecedentes significativos aspectos positivos en la aplicación de Centro de Respuesta a Incidentes Cibernéticos y la utilización de Centro de Operaciones de Seguridad (SOC) que apoyen al desarrollo de las actividades que constituyen el CRIC en ámbito de CSIRT.

Este tipo de metodología investigativa se articula de manera idónea al desarrollo del proyecto, puesto que permite por medio de extracción documental investigativa, de proyectos aplicados de CSRIT y SOC'S, establecer un punto de congruencia que se acople a las medidas tanto en tamaño como en desarrollo de las necesidades en materia de seguridad de la empresa PLATINO.

[25] ABREU, José Luis. Análisis al Método de la Investigación. [En línea]. Nuevo León. International Journal of Good Conscience. 2015. [Consulta: 20 de marzo 2022]. Disponible: http://www.spentamexico.org/v10-n1/A14.10(1)205-214.pdf

# 6 DESARROLLO DE LOS OBJETIVOS

## 6.1. ROLES DEL EQUIPO DE TRABAJO DEL CENTRO DE OPERACIONES DE SEGURIDAD (SOC) EN LA EMPRESA PLATINO SISTEMAS.

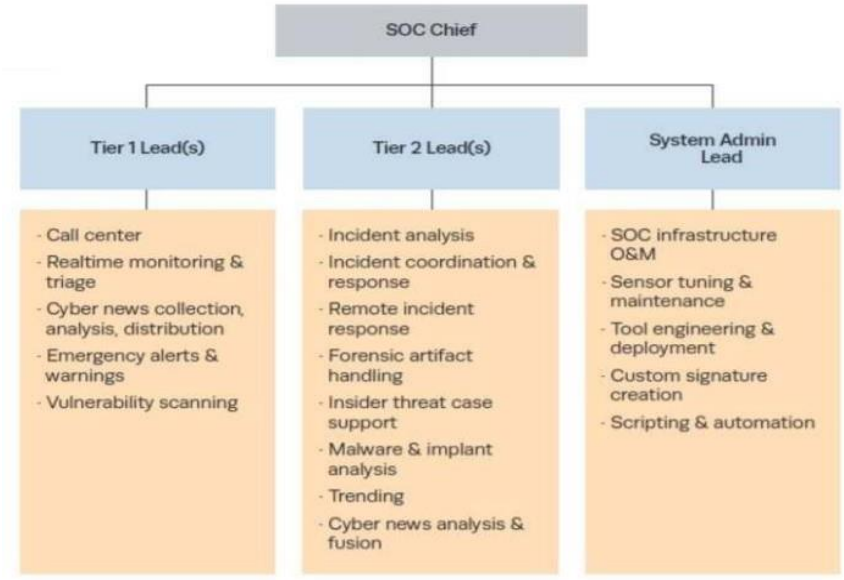
Los grupos de SOC como otros grupos de trabajo también tienen una persona específica que realiza actividades concretas en pro al desarrollo de todas las actividades ejecutadas en este grupo. Pero en esta particularidad, se presentan grupos dependiendo al tamaño de la organización o el tamaño del SOC con el que cuente esta.

6.1.1. SOC pequeños. Este tipo de SOC no es tan grande y no requiere de tanto personal puesto que sus procedimientos son muchos más reducidos que los medianos y grandes SOC'S. En estos grupos pequeños son necesarios los siguientes trabajadores en orden Jerárquico:

1) El SOC Chief que es la cabeza más alta de todo el grupo, el jefe, el organizador de todo el SOC
2) Seguido se tiene al líder de Nivel 1 o Tier 1
3) Al igual nivel, pero con diferentes funciones tenemos al líder de Tier 2.
4) Por último, se tiene al líder administrador de sistemas.

A continuación, se presenta una gráfica explicativa donde muestra cómo se comportan a nivel general los roles en el SOC y las funciones relacionadas.

Figura 1. SOC pequeño.



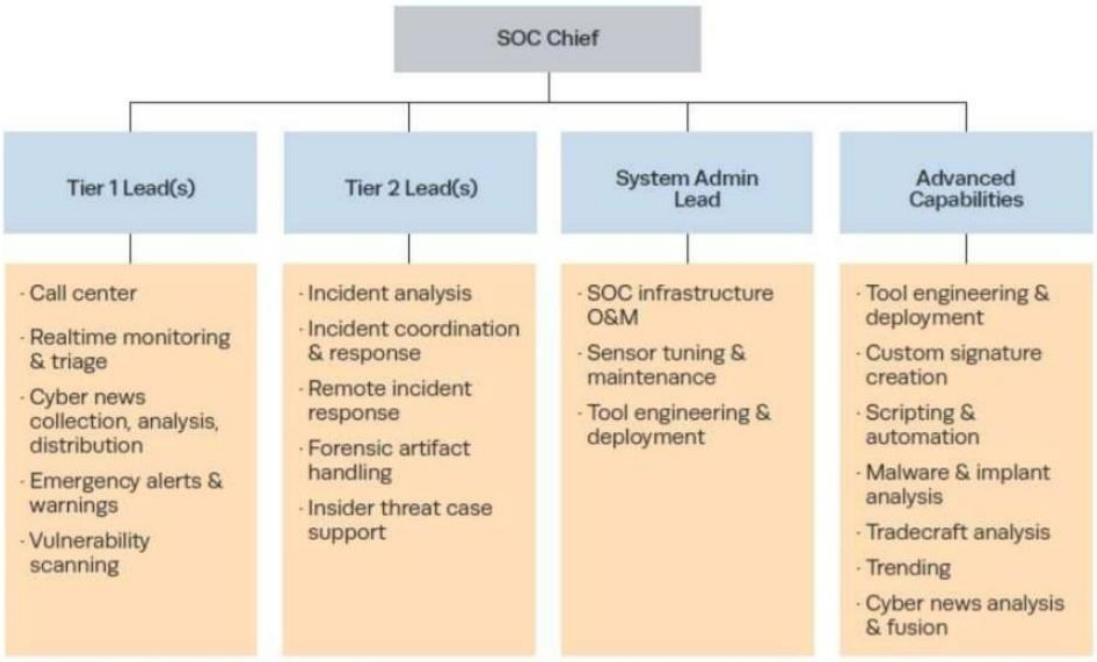

Fuente: SHEIKH, Shah. Building a Ciber Security Operations Center [En línea]. 2018. Confluence. Internet community. (Consulta: 15 de abril de 2020) Disponible en: https://es.slideshare.net/ShahSheikh/dts-solution-building-a-soc-security-operations-center

6.1.2. SOC Mediano. Este tipo de SOC es un poco más grande que el primero y más pequeño que el grande, este requiere un poco más de personal puesto que sus procedimientos son muchos más que los SOC'S pequeños y menos que los grandes SOC'S. En estos grupos medianos son necesarios los siguientes trabajadores en orden Jerárquico:

1) El SOC Chief que es la cabeza más alta de todo el grupo, el jefe, el organizador de todo el SOC.
2) Seguido se tiene al líder de Nivel 1 o Tier 1.
3) Al igual nivel, pero con diferentes funciones se tiene al líder de Tier 2.
4) Así mismo, se tiene al líder administrador de sistemas.
5) Y para finalizar se tiene unas capacidades avanzadas.

A continuación, se presenta una gráfica explicativa donde muestra cómo se comportan a nivel general los roles en el SOC y las funciones relacionadas.

Figura 2. SOC Mediano.




Fuente**:** SHEIKH, Shah. Building a Ciber Security Operations Center [En línea]. 2018. Confluence. Internet community. (Consulta: 15 de abril de 2020) Disponible en: https://es.slideshare.net/ShahSheikh/dts-solution-building-a-soc-security-operations-center

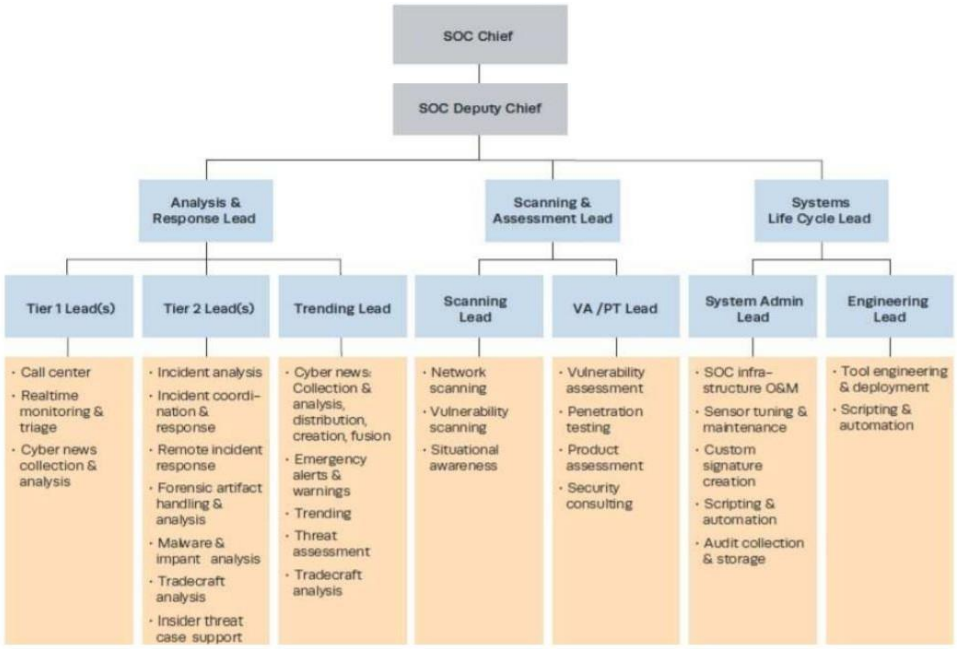
6.1.3. SOC Grande. Este tipo de SOC es el más grande que se puede encontrar en una organización, puesto que presenta la particularidad de que contiene todos los puestos y actividades necesarias para desarrollar un SOC en su totalidad. Para este grupo son necesarios los siguientes trabajadores en orden Jerárquico:

1) El SOC Chief que es la cabeza más alta de todo el grupo, el jefe, el organizador de todo el SOC.
2) El SOC delupy Chief, que vendría siendo el segundo al mando en este grupo.
3) Seguido de esto se tiene al líder de análisis y respuesta.
4) En la misma línea del líder analista, se tiene al líder de escaneo y evaluación.
5) Para completar se tiene al líder de ciclo de vida de los sistemas.

6) El líder de análisis tiene a su cargo a un conjunto de técnicos los cuales son, los Técnicos de Nivel 1, Técnicos de Nivel 2 y Líder de tendencia.
7) A su vez el líder de escaneo tiene a su cargo a otro conjunto de técnicos los cuales son, el líder de escaneos y los VA/PT líder.
8) Y para finalizar el líder de ciclo de vida de sistemas tiene a su cargo al conjunto de técnicos de administrador de sistemas e ingeniería.

A continuación, se presentan una gráfica explicativa donde muestra cómo se comportan a nivel general los roles en el SOC y las funciones relacionadas.

Figura 3. SOC Grande.

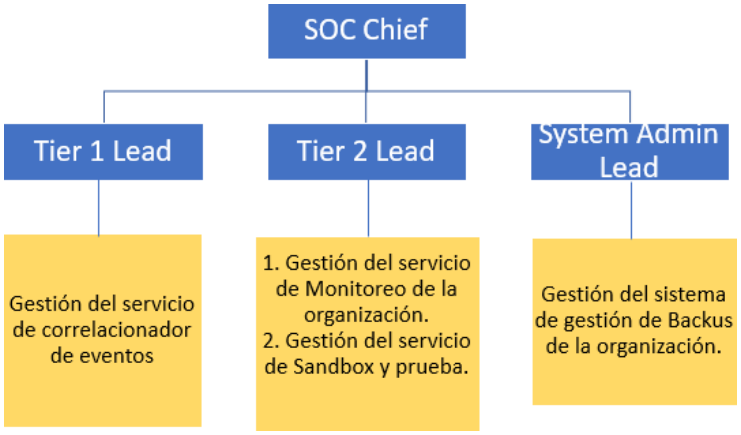



Fuente: SHEIKH, Shah. Building a Ciber Security Operations Center [En línea]. 2018. Confluence. Internet community. (Consulta: 15 de abril de 2020) Disponible en: https://es.slideshare.net/ShahSheikh/dts-solution-building-a-soc-security-operations-center

Finalmente a partir de lo mencionado, se puede concluir que el SOC que se adecuaba teniendo en cuento los tipos de SOC especificados, es un SOC de pequeña escala, puesto que, teniendo en cuenta que son 4 los servicios establecidos por la empresa PLATINO SISTEMS, la operación se podría distribuir perfectamente entre tres frentes de gestión como lo plantea el SOC de pequeña

escala. La siguiente es una propuesta de SOC a pequeña escala que satisface las necesidades de la empresa PLATINO SISTEMAS:

Figura 4. Propuesta Modelo SOC pequeño - Empresa Platino Sistema.




Fuente: Propia del autor

En estos grupos pequeños son necesarios los siguientes trabajadores en orden Jerárquico:

1) El SOC Chief que es la cabeza más alta de todo el grupo, el jefe, el organizador de todo el SOC
2) Seguido se tiene al líder de Nivel 1 o Tier 1, el cual está encargado de gestionar todo lo relacionado a gestión de servicios de correlacionador de eventos en la organización.
3) Al igual nivel, pero con diferentes funciones tenemos al líder de Tier 2, el cual está encargado de la gestión del monitoreo y el servicio de Sandox en la organización.
4) Por último, se tiene al líder administrador de sistemas, el cual está encargado de la administración del sistema de Backups con que cuenta la organización.

## 6.2. PROPUESTA DE TECNOLOGÍA PARA LAS OPERACIONES PROPIAS DEL CENTRO DE OPERACIONES DE SEGURIDAD EN LA EMPRESA PLATINO SISTEMAS

Para la ejecución adecuada de los centros de operaciones de seguridad, son necesarios un conjunto de operaciones propias o que lo constituyen, las cuales apoyan al correcto funcionamiento de todas las tareas que este realiza. Estas operaciones son:

- ✓ Programas.
- ✓ Instrumentación.
- ✓ Análisis y detección.
- ✓ Monitoreo.
- ✓ Evaluación de amenazas.
- ✓ Escalada, respuesta e informes.
- ✓ Conciencia situacional.
- ✓ Prevención.

Ahora se explicará de manera detallada cada una de las actividades o atributos que tienen cada una de estas operaciones sobre el SOC.

6.2.1. Programa. Describe las cualidades del programa general de SOC la cual está interrelacionada con diferentes áreas funcionales. Esta operación se divide en los siguientes ítems.

- La documentación especificada por el SOC tiene un poder de jefe ejecutivo para la ejecución de una actividad especifica.
- La documentación emitida, nunca será enviada o establecida como una orden a ejecutar si no se ha ejecutado antes por el SOC en sí.

- El SOC debe implementar los elementos de ataque a redes computaciones, como monitoreo en tiempo real, análisis, coordinación y respuesta de incidentes, recopilación y análisis de inteligencia cibernética, ajuste y gestión de sensores, scripting y automatización, ingeniería e implementación de nuevas herramientas SOC.
- Definición del SOC con una estructura organizativa y de gestión interna, dividida por funciones y responsabilidades.
- Las tareas diarias, las inversiones en recursos y el presupuesto del SOC, se basan en estudios realizados dentro del SOC mismo.
- El personal SOC no presenta una idea fija de que las situaciones presentadas son juego o no, toman la situación como verídica y actual al respecto.
- La implementación del SOC presenta un grupo reducido de expertos que permiten llevar a cabo las actividades relacionadas a este.

6.2.2. Instrumentación. En esta sección se presentan las cualidades de los sistemas y los procedimientos que se utilizan al realizar seguimiento a cada etapa del ciclo de vida de un ataque cibernético. Esta etapa está constituida por los siguientes aspectos:

- El SOC es capaz de articular el valor que deriva de cada uno de sus sensores o fuentes de datos,
- Todas las capacidades de monitoreo reciben atención regular de analistas y herramientas analíticas.
- Todos los nuevos programas, proyectos y propietarios de sistemas se ven obligados mediante el proceso o el mandato de solicitar la asistencia del SOC en la aplicación de la supervisión de la SOC.
- Los nuevos programas, proyectos y propietarios de sistemas buscan proactivamente asistencia del SOC en la aplicación de las capacidades de monitoreo de las redes de distribución de contenido en sus sistemas.

- Evaluaciones de dificultades en la detección de amenazas.
- Conocimiento de los cambios en la arquitectura de SOC, configuración, redes y hosts.

6.2.3. Análisis y detección. En esta sección se presentan las cualidades presentes en cada una de las herramientas de análisis y detección utilizadas por el SOC. Esta etapa está constituida por los siguientes aspectos:

- El SOC aplica la minería de datos y otras técnicas para examinar los datos históricos en busca de evidencia de actividad misteriosa o maliciosa en la red o sistemas.
- El contenido incorpora conocimiento sobre el entorno de amenazas y vulnerabilidades.
- Todas las capacidades de detección basadas en firmas del SOC, como IDS y listas de indicadores, se ajustan o actualizan con nuevas firmas al menos una vez a la semana.
- El SOC crea reglas personalizadas para mejorar sus esfuerzos de monitoreo más allá de lo proporcionado por los proveedores.
- Las actualizaciones de firmas y contenido se realizan un seguimiento a través de un proceso de firmas electrónicas avanzadas.
- Los indicadores de compromiso recopilados de fuentes abiertas y de otros SOC se integran regularmente en firmas y análisis personalizados.
- Las firmas personalizadas y otras herramientas analíticas se devuelven a los SOC asociados.

6.2.4. Monitoreo. En esta sección se presentan las diferentes características presentes en el SOC en todos los procesos de monitoreo de sistemas a nivel general. Esta etapa está constituida por los siguientes aspectos:

- Nivel 1. Responsable de monitorear las fuentes de datos en tiempo real y aumentar el potencial casos al Nivel 2.
- Monitoreo de alertas en tiempo real, triaje, correlación y desglose de eventos.
- Consulta de eventos históricos y minería de datos.
- Análisis y reconstrucción del tráfico de red.
- Ejecución y detonación de malware en tiempo de ejecución.
- Emisión de tickets y seguimiento de incidentes.
- Seguimiento de campañas de indicadores y adversarios.
- En nivel 1 los casos presentados son divididos equitativamente entre todos, no hay una elección especifica por algún operador.

6.2.5. Evaluación de amenazas. Esta etapa presenta una mirada de como el SOC analiza correctamente al atacante y acciona correctamente sobre sus acciones. Esta etapa está constituida por los siguientes aspectos:

- El SOC ejerce la capacidad de observar el comportamiento del adversario y determinar la verdadera naturaleza y el alcance de los incidentes, sin ser impulsado a responder con ciertas contramedidas.
- El SOC tiene los medios para medir el alcance del daño, los motivos de los atacantes, el vector de ataque y la probable atribución del atacante.
- El SOC tiene herramientas que admiten el análisis rápido en tiempo de ejecución del comportamiento del malware, como un sistema de detonación de contenido.
- El SOC tiene la experiencia, las herramientas y los recursos para realizar ingeniería inversa de malware.
- El SOC tiene la experiencia, las herramientas y los recursos para realizar un análisis forense digital a profundidad de los medios relevantes para las principales intrusiones, como el análisis forense del disco duro.

6.2.6. Escalada, respuesta e informes. Esta etapa es la encargada de describir cómo se presentan los incidentes en el SOC, cómo se responden y cómo se informan al respecto. Esta etapa está constituida por los siguientes aspectos:

- El SOC sigue su concepto de operaciones y lo actualiza al menos cada 36 meses.
- El SOC tiene alimentación a través de Ethernet de escalamiento interno y respuesta para los incidentes que trata con más frecuencia.
- El SOC puede ponerse en contacto con las partes involucradas en un incidente sospechoso en cuestión de minutos después de necesitar hacerlo.
- Los datos del caso del SOC no son solicitados ni accesibles por partes que no son partes del SOC.
- El SOC sirve como punto de distribución para las directivas de contramedidas rutinarias.

6.2.7. Conciencia situacional. Esta etapa es la encargada de describir las soluciones de ciberseguridad y como socializar la conciencia del uso de estas en partes externas. Esta etapa está constituida por los siguientes aspectos:

- El SOC publica información de conciencia de situaciones cibernéticas en su sitio web, a disposición de los miembros designados de la circunscripción.
- El SOC puede articular los límites de sus situaciones cibernéticas en detalle, en términos de monitoreo de la cobertura, cobertura del ciclo de vida de ataques cibernéticos y paridad de amenazas.
- El SOC capacita al nuevo personal en detalle según las redes de circunscripción, los activos y la misión, asegurando así un profundo conocimiento que se extiende desde los veteranos hasta los analistas junior.
- El SOC revisa activamente los informes de inteligencia cibernética y los pasos de inteligencia cibernética externos para asegurarse de que son de

alta fidelidad antes de la aceptación en los repositorios y sensores de inteligencia de amenazas cibernéticas del SOC.

6.2.8. Prevención. Esta etapa es la encargada de describir todos los procesos en base a la prevención de los incidentes cibernéticos que regula el SOC. Esta etapa está constituida por los siguientes aspectos:

- El SOC utiliza su conciencia de situación cibernética para impulsar la resolución de vulnerabilidades y prácticas de seguridad.
- El SOC proporciona consultoría sobre amenazas cibernéticas, arquitectura de seguridad y mejores prácticas para los programas de TI y líneas de negocio.
- El SOC participa en la formulación (y posiblemente proporcionar) capacitación y educación en materia de buen uso de seguridad a los electores, como la navegación segura y consejos de correo electrónico.
- El SOC es consultado regularmente sobre cuestiones de política de ciberseguridad por los directivos.
- El SOC es considerado por los mandantes como una organización que ayuda a la misión de circunscripción y a las operaciones comerciales, en lugar de obstaculizarlas.
- El SOC aloja capacidades de en su sitio web para facilitar su descarga por componentes.

Finalmente se puede establecer que la propuesta de operación antes mencionada es la ideal para que un SOC en base a su modelo de operación pueda ejecutar sus diferentes procesos de manera correcta, contemplado desde la identificación de programas, seguido del análisis de la Instrumentación utilizada en el centro, el análisis y detección por medio de herramientas utilizadas en el centro de operaciones, el monitoreo de sistemas a nivel general, la evaluación de amenazas a nivel general, la escalada, respuesta e informes generados por el

mismo centro, la conciencia situacional enfocada en las soluciones de ciberseguridad y finalmente ese proceso de prevención enfocado a los incidentes cibernéticos que regula el SOC.

## 6.3. IDENTIFICAR LAS HERRAMIENTAS DE HARDWARE Y SOFTWARE LIBRE PARA EL DESARROLLO DE LAS ACTIVIDADES DEL SOC.

A continuación se definen herramientas de software libre para el desarrollo de las actividades del SOC:

Para el desarrollo de las actividades que componen un SOC, se necesitan de un conjunto de herramientas y servicios que apoyen a la composición estructural y operativa del centro de operaciones de seguridad. Estos artefactos están constituidos por una parte hardware y software sobre las cuales se montan y ejecutan los servicios necesarios para la implantación de un SOC en una organización. Estos instrumentos son:

6.3.1. Apache Web Service. Es servidor web potente, flexible y compatible con el protocolo HTTP, el cual permite implementar los protocolos actuales relacionados con éste. Tiene la particularidad de ser un aplicativo altamente configurable y extensible según las necesidades internas o externas del proyecto esto mediante la API modular de apache. Uno de sus atributos más significativos es su proporción de código fuente completo y su licencia sin restricciones, permitiendo así su configuración global para la facilidad del administrador. Este servidor cuenta con las siguientes características.

- Permite su ejecución en entornos desde Windows 2000, OS/2 hasta la mayoría de las versiones de UNIX.
- Permite una sencilla configuración para páginas protegidas por contraseñas sin envolverse directamente con el servidor.

- Personalización de respuestas a errores y problemas generales del servidor web.
- Permite al servidor realizar una diferenciación entre host virtuales mediante escaneo de IP solicitantes.
- Permite configurar el servidor web para generar registros en diferentes tipos de formatos según su necesidad.[26]

Teniendo en cuenta la concepción y las características planteadas anteriormente con respecto a este servicio web, se plantean un conjunto de ventajas y desventajas.

✓ Ventajas
    - Consta de una fácil configuración.
    - Permite la utilización de una gran cantidad de módulos funcionales según necesidad.
    - Contiene un entorno amigable para los principiantes.
    - Software de código abierto.
    - Multiplataforma.
    - Software confiable y estable.

✓ Desventajas
    - Pueden presentarse problemas al momento de tener un alto tráfico de interacción en la página web.
    - Su alta variabilidad de configuración puede generar nuevos y frecuentes huecos de seguridad.

Ya visto la concepción y caracterización de la herramienta en función de las necesidades para implantación de un servidor web, a continuación, se presentarán

[26] ATLASSIAN CONFLUENCE 7.5.0. realizado a Apache Software Foundation [En línea]. 2019. Confluence. Internet community. (Consulta: 12 de octubre de 2020) Disponible en https://cwiki.apache.org/confluence/display/httpd/FAQ#FAQ-WhatisApache?

un conjunto de requerimientos mínimos de hardware para la correcta ejecución de este servicio.

1. CPU: 1
2. CPU(GHz): 2.6
3. RAM: 1 GB.
4. HARD DISK: 50 GB.
5. NUCLEOS: 2 Núcleos.

6.3.2. Postfix. Es un agente de transferencia de correos (MTA) predispuesto en Ubuntu para él envió y recepción de correos electrónicos. Así como en el caso del servidor Web Apache, este agente cuenta con la particularidad de ser rápido, seguro y flexible para su administración y configuración. Sus múltiples configuraciones permiten hasta llegar el punto de poder configurar el servicio de tal forma que solo permita el envió de notificaciones específicas por medio de aplicativos. Las principales características que reflejan un buen papel en la implementación de un servicio Mail son:

- Presenta un diseño modular.
- Facilidad de configuración.
- Contiene bastante documentación relacionada a su estructura y configuración.
- Cuenta con una buena integración con los antivirus.
- Multiforme respecto a la obtención de información para la resolución de problemas.
- Cuenta con soporte para el formato de buzones de Email.

Teniendo en cuenta la concepción y las características planteadas anteriormente con respecto a este servicio mail, se plantean un conjunto de ventajas y desventajas.

- ✓ Ventajas
    - Resolución de problemas con más rapidez, puesto que al tener acceso completo al servidor para poder explorar los logs y encontrar errores.
    - Es OpenSource.
    - Utilización de lista de correos y grupos sin ninguna restricción o limite.
    - No tendrás limitaciones en envío y recepción de correos a menos que se configuren.
    - Fácil implementación.
- ✓ Desventajas
    - Es necesario un mayor trabajo de configuración.
    - Se necesita una gran capacidad de almacenamiento.

Ya visto la concepción y caracterización de la herramienta en función de las necesidades para implantación de un servidor mail, a continuación, se presentarán un conjunto de requerimientos mínimos de hardware para la correcta ejecución de este servicio.

1. CPU: 1
2. CPU(GHz): 2.6
3. RAM: 512 MB.
4. HARD DISK: 20 GB.
5. NUCLEOS: 2 Núcleos.[27]

[27] FREDERICK P. Brooks, Jr. The Postfix Home Page [En línea]. 2018. Carolina del Norte. POSTFIX (Consulta: 12 de octubre de 2020) Disponible en: http://www.postfix.org/documentation.html

6.3.3. Samba. Es una implementación de código abierta basada en el protocolo SMB. Esta herramienta permite proporcionar servicios de interconexión de archivos e impresoras seguras, estables y rápidos entre sistemas operativos Windows y Unix utilizando protocolos SMB/CIFS. Se considera como un componente importante para la integración de servidores y escritorios Linux en entornos de Active Directory. Este tipo de servicio de archivos consta de las siguientes características:

- Autentificación a conexión con dominios Windows.
- Se establece como un miembro servidor de dominio de Active Directory.
- Proporciona soluciones de servidores basado en Microsoft Windows que ejecutan el Servicio de nombres Internet de Windows.
- Permite asistir en la navegación realizada en la red.
- Procede como un controlador de dominio primario.

Teniendo en cuenta a la concepción y las características planteadas anteriormente con respecto a este servicio de archivos, se plantean un conjunto de ventajas y desventajas.

- ✓ Ventajas
    - Cuenta con un buen soporte de uso compartido de archivos.
    - Permite el acceso a diferentes clientes a sistemas de archivos común de Internet.
    - Cuenta con niveles aceptables de seguridad en la parte de autentificación y uso compartido de archivos.
- ✓ Desventajas
    - No cuenta con un protocolo de encriptación en la capa de transporte.
    - De no instalarse Microsoft Server Message Block los escenarios de uso compartido de archivos se pueden ver comprometidos.

Ya visto la concepción y caracterización de la herramienta en función de las necesidades para implantación de un servidor de archivos, a continuación, se presentarán un conjunto de requerimientos mínimos de hardware para la correcta ejecución de este servicio:

1. CPU: 1
2. CPU(GHz): 2.6
3. RAM: 2 GB.
4. HARD DISK: 250 GB.
5. NUCLEOS: 4 Núcleos.[28]

6.3.4. Bacula. Es una suite de programas informáticos que permite gestionar la copia de seguridad, recuperación y verificación de datos informáticos a través de una red de equipos de diferentes tipos. Bacula también puede ejecutarse completamente en un solo equipo y puede realizar copias de seguridad en varios tipos de medios, incluyendo cinta y disco. Las principales características de la herramienta a destacar y que la consolidan como una herramienta de copia de seguridad sólida son:

- Tiene una operabilidad hasta de 2000 equipos.
- Respaldos y recuperación en red.
- Permite una administración centralizada.
- Fácil acceso a la información respaldada.
- La comunicación entre componentes puede ser cifrada.
- Su licencia es GPL.
- Soporte para la mayoría de los dispositivos de almacenamiento mercado.

[28] HERTEL, Chris. Samba: An Introduction. [En línea]. 2001. The Samba Team. (Consulta: 12 de octubre de 2020) Disponible: https://www.samba.org/samba/docs/SambaIntro.html

Teniendo en cuenta a la concepción y las características planteadas anteriormente con respecto a este servicio de copias de seguridad, se plantean un conjunto de ventajas y desventajas.

- ✓ Ventajas
    - Permite realizar copias de seguridad bastante completas y exactas.
    - Permite tener un control del versionado de los archivos respaldados.
    - Permite realizar copias de seguridad incrementales.
    - Fácil administración de todos los recursos por medio de diferentes entornos gráficos de control que la componen.
- ✓ Desventajas
    - Requiere un ancho de banda adicional puesto que, al realizar copias de seguridad tan completas, el uso de éste es indispensable.
    - Si falla una copia de seguridad no se puede realizar su respectiva recuperación.

Ya visto la concepción y caracterización de la herramienta en función de las necesidades para implantación de un servidor de copias de seguridad, a continuación, se presentarán un conjunto de requerimientos mínimos de hardware para la correcta ejecución de este servicio:

1. CPU: 1
2. CPU(GHz): 2.6
3. RAM: 1 GB.
4. HARD DISK: 1 TB.
5. NUCLEOS: 8 Núcleos.[29]

[29] BACULA. What is Bacula?. Documentation. [En línea]. 2009. (Consulta: 12 de octubre de 2020) Disponible: https://www.bacula.org/what-is-bacula/

6.3.5. Nagios. Es una herramienta de monitorización de redes la cual permite supervisar toda la infraestructura TI de una organización, con el fin de garantizar que los servicios, las aplicaciones, los servicios y los procesos funcionen de forma correcta. Además de estos atributos, Nagios posibilita la monitorización remota mediante SSL o SSH. En caso de presentarse fallos específicos en los sistemas la herramienta tiene un sistema de alertas personalizado para acción inmediata de los administradores del sistema de monitorización, con el objeto de reducir los riesgos y evitar una eminente afectación en la continuidad del negocio de una organización.

Las principales características que constituyen este tipo de sistemas de monitorización son:

- Permite un monitoreo integral.
- Permite una remediación de problemas en tiempos reducidos.
- El sistema generador de informes en éste, le permite accionar con mayor veracidad sobre fallas o auditorias de vulnerabilidades.
- Presenta una arquitectura extensible posibilitando la integración con aplicaciones propias del sistema y de terceros.
- Cuenta con una comunidad de más de 1 millón de usuarios en todo el mundo en constante actividad para resolución de nuevos problemas.

Teniendo en cuenta a la concepción y las características planteadas anteriormente con respecto a este servicio de monitorización, se plantean un conjunto de ventajas y desventajas.

✓ Ventajas

- Herramienta de código abierto y libre.
- Contiene interfaz web para mejor gestión de recursos de monitorización.

- Flexible con plugin internos y externos.
- Permite la modificación de código interno.
- Visibilidad general de todos los recursos de infraestructura TI con que cuenta una organización.

✓ Desventajas

- La alta variabilidad de uso y configuraciones tiende a tener una curva de aprendizaje elevada.
- Al trabajar con miles de nodos en ejecución, el mantenimiento de estos se hace bastante pesado.

Ya visto la concepción y caracterización de la herramienta en función de las necesidades para implantación de un servidor de monitorización, a continuación, se presentarán un conjunto de requerimientos mínimos de hardware para la correcta ejecución de este servicio:

1. CPU: 1
2. CPU(GHz): 2.6
3. RAM: 1 GB.
4. HARD DISK: 100 GB.
5. NUCLEOS: 6 Núcleos.[30]

6.3.6. Bind9. Es uno de los servidores DNS más utilizado en la actualidad, ya que presenta un conjunto de herramientas y funcionalidades bástate robusta y completa con relación a la prestación de servicios DNS. Esta herramienta es más utilizada en sistemas GNU/Linux, siendo bastante practico y portable respecto a el desarrollo de sus funcionalidades y las nuevas extensiones de seguridad (DNSSEC). Este servicio cuenta con la particularidad de ser

[30] NAGIOS. The Industry Standard In IT Infrastructure Monitoring. Nagios Features and Capabilities. [En línea]. 2020. (Consulta: 12 de octubre de 2020) Disponible: https://www.nagios.org/about/features/

transparente de código abierto, dándole la capacidad a los usuarios de añadir funcionalidades a Bind9 y realizar contribuciones atreves del Gitlab de la comunidad abierta de Bind. Las principales características de esta herramienta son:

- Cuenta con la implementación del protocolo TSIG.
- Permiten realizar notificaciones DNS.
- Soportan el protocolo IPv6.
- Permiten los procedimientos en paralelo.
- Mejor portabilidad con base en su arquitectura.

Teniendo en cuenta a la concepción y las características planteadas anteriormente con respecto a este servicio DNS, se plantean un conjunto de ventajas y desventajas.

- ✓ Ventajas
    - Esta centralizado y se puede utilizar todos sus recursos en un mismo lugar.
    - Es confiable, seguro y robusto.
    - Consistencia en la información.
    - Evita la duplicidad de nombres.
    - Evita la carga excesiva en la red y los hosts.
- ✓ Desventajas
    - Se pueden presentar errores en logs si no son configurados de manera idónea.

Ya visto la concepción y caracterización de la herramienta en función de las necesidades para implantación de un servidor DNS, a continuación, se presentarán

un conjunto de requerimientos mínimos de hardware para la correcta ejecución de este servicio:

1. CPU: 1
2. CPU(GHz): 2.5
3. RAM: 512 MB.
4. HARD DISK: 20 GB.
5. NUCLEOS: 4 Núcleos.[31]

6.3.7. GLPI. Es una herramienta que suministra servicios de TI, capaz de manejar y controlar cambios en la infraestructura informática de una organización de manera eficiente, eficaz y sencilla. Además de esto, es una de las pocas herramientas OpenSource de este calibre que permite manejar grandes infraestructuras TI, permitiendo la segmentación en la entidad respecto a políticas administrativas y la resolución de inconvenientes en tiempo real. Esto sin dejar a un lado los grandes aspectos serviciales con los que cuenta como lo es la gestión de inventarios, compatibilidad con ITILv2, herramientas completas de gestión para toma de decisiones por administradores, entre otras. Las características que constituyen el buen funcionamiento de esta herramienta son:

- Compatibilidad con ITILv2.0
- Manejo de activos automáticos de TI.
- Control de calidad de los datos.
- Manejo administrativo y financiero de los activos.
- Reportes automatizados.
- Integración profunda con nuevas funcionalidades.

[31] INTERNET SYSTEMS CONSORTIUM. BIND 9. Why use BIND 9?. [En línea]. Nwemarket. NH. 2020. (Consulta el 12 de octubre de 2020). Disponible: https://www.isc.org/bind/

Teniendo en cuenta a la concepción y las características planteadas anteriormente con respecto a este servicio de registro y seguimiento de Incidentes, se plantean un conjunto de ventajas y desventajas.

- ✓ Ventajas
    - OpenSource.
    - Permite relacionar datos financieros de los activos.
    - Permite la conexión a otras redes.
    - Incorporación de archivos de múltiples tipos.
    - Contiene una herramienta estadística donde se puede disponer de datos y gráficos para realizar comparaciones parametrizadas.
- ✓ Desventajas
    - No permite cargar archivos más pesados a 2MG.
    - Solo permite inventariado de activos informáticos.

Ya visto la concepción y caracterización de la herramienta en función de las necesidades para implantación de un servicio para registro y seguimiento de Incidentes, a continuación, se presentarán un conjunto de requerimientos mínimos de hardware para la correcta ejecución de este servicio:

1. CPU: 1
2. CPU(GHz): 2.5
3. RAM: 1 GB.
4. HARD DISK: 100 GB.
5. NUCLEOS: 6 Núcleos.[32]

6.3.8. SNORT. Es el sistema de prevención de intrusiones (IPS) de código abierto más importante del mundo. Snort IPS utiliza una serie de reglas que ayudan

[32] GLPI TECLIB. Características de GLPI. Gestión de TI basado en tecnologías de código abierto. [En línea]. 2020. (Consulta: 13 de octubre de 2020). Disponible: https://glpi-project.org/es/caracteristicas/

a definir la actividad maliciosa de la red y utiliza esas reglas para encontrar paquetes que coincidan con ellos y genera alertas para los usuarios. Snort también se puede implementar en línea para detener estos paquetes.

Snort tiene tres usos principales: como rastreador de paquetes como tcpdump, como registrador de paquetes, que es útil para la depuración del tráfico de red, o se puede usar como un sistema de prevención de intrusiones de red en toda regla. Snort se puede descargar y configurar para uso personal y empresarial por igual.. Las características que constituyen el buen funcionamiento de esta herramienta son:

- Monitor de tráfico en tiempo real.
- Registro de paquetes.
- Análisis de protocolo.
- Coincidencia de contenido.
- Huellas digitales del SO.
- Puede instalarse en cualquier entorno de red.
- Crea registros.
- Fuente abierta.

Teniendo en cuenta a la concepción y las características planteadas anteriormente con respecto a este servicio de registro y seguimiento de Incidentes, se plantean un conjunto de ventajas y desventajas.

- ✓ Ventajas
    - Snort puede funcionar como un Sniffer (es decir que podemos ver en consola y en tiempo real el tráfico de la red), registro de paquetes (guardar archivos logs) o como un NIDS normal.
    - Snort utiliza un lenguaje de descripción de reglas sencillo y ligero que es flexible y bastante potente.

- Hay un número de pautas simples a recordar al desarrollar las reglas de Snort que ayudarán a salvaguardar su cordura.

✓ Desventajas.

- Como desventajas solo podemos decir que Snort no cuenta por defecto con un GUI o interfaz gráfica de usuario por defecto, por tanto no es tan fácil de administrar como otras.

Ya visto la concepción y caracterización de la herramienta en función de las necesidades para implantación de un servicio para registro y seguimiento de Incidentes, a continuación, se presentarán un conjunto de requerimientos mínimos de hardware para la correcta ejecución de este servicio:

1. CPU: 1
2. CPU(GHz): 2.5
3. RAM: 1 GB.
4. HARD DISK: 100 GB.
5. NUCLEOS: 6 Núcleos.[33]

6.3.9. WAZUH. E Wazuh es una plataforma gratuita y de código abierto utilizada para la prevención, detección y respuesta de amenazas. Es capaz de proteger las cargas de trabajo en entornos locales, virtualizados, en contenedores y basados en la nube.

La solución wazuh consiste en un agente de seguridad de endpoints, desplegado en los sistemas monitoreados, y un servidor de administración, que recopila y analiza los datos recopilados por los agentes. Además, Wazuh se ha integrado completamente con Elastic Stack, proporcionando un motor

[33] ARTEGA, JOSE. EVALUACIÓN DE LAS FUNCIONALIDADES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS BASADOS EN LA RED DE PLATAFORMAS OPEN SOURCE UTILIZANDO LA TÉCNICA DE DETECCIÓN DE ANOMALÍAS. Escuela Superior Politécnica De Chimborazo. 2018. [En línea]. Trabajo Magister. [Consulta: 30 de mayo 2022]. Disponible: http://dspace.espoch.edu.ec/bitstream/123456789/8748/1/20T01065.pdf

de búsqueda y una herramienta de visualización de datos que permite a los usuarios navegar a través de sus alertas de seguridad. Las principales características de este tipo de sistemas son:

- Análisis de seguridad.
- Detección de intrusos.
- Análisis de datos de registro.
- Monitoreo de integridad de archivos.
- Detección de vulnerabilidades.
- Evaluación de la configuración.
- Respuesta al incidente.
- Cumplimiento normativo.

Teniendo en cuenta a la concepción y las características planteadas anteriormente con respecto a este servicio de registro y seguimiento de Incidentes, se plantean un conjunto de ventajas y desventajas.

✓ Ventajas

- Administración centralizada de registros de seguridad para todos los registros de puntos finales (servidores, dispositivos de red, clientes y aplicaciones).
- Tiene un agente patentado, que se puede instalar en puntos finales de Linux o Windows para recopilar registros de seguridad y enviarlos formateados al administrador de Wazuh para análisis de registros.
- El agente escanea el sistema monitoreado en busca de rootkits, malware, anomalías sospechosas, etc., proporcionando un HIDS (detección de intrusos basado en host) completo y lo hace de manera muy efectiva.
- El agente extrae los datos del inventario de software en los puntos finales y envía esta información al administrador, donde se evalúa

frente a las bases de datos CVE de código abierto, como NVD, que se actualizan continuamente. Proporciona una detección de vulnerabilidades completa basada en agentes en todos sus sistemas monitoreados.

- ✓ Desventajas.
    - Aunque Wazuh proporciona respuestas activas listas para usar para realizar varias contramedidas para hacer frente a las amenazas activas, como bloquear el acceso a un sistema desde la fuente de la amenaza cuando se cumplen ciertos criterios, esta área aún es nueva en Wazuh y aún no está suficientemente maduro para activarlo en un entorno de producción real.
    - Falta de suficientes materiales de capacitación para toda la pila. Por ejemplo, en muchos casos, uno debe continuar y definir sus propios decodificadores (coincidencias basadas en RegEx para extraer los campos obligatorios) y reglas para esas decodificaciones, y créanme, ¡no es tan fácil! Sin embargo, vale la pena aprender.

Ya visto la concepción y caracterización de la herramienta en función de las necesidades para implantación de un servicio para registro y seguimiento de Incidentes, a continuación, se presentarán un conjunto de requerimientos mínimos de hardware para la correcta ejecución de este servicio:

1. CPU: 1
2. CPU(GHz): 2.5
3. RAM: 1 GB.
4. HARD DISK: 100 GB.

5. NUCLEOS: 6 Núcleos.[34]

6.3.10. AlienVault OSSIM 1. Es una herramienta que suministra servicios de TI de código abierto la cual permite la recopilación de eventos, normalización y correlación de eventos. Es un proyecto lanzado por ingenieros de seguridad, debido a la poca demanda en el mercado de este tipo de herramientas en la modalidad OpenSource. Este sistema fue creado con el objetivo de abordar la realidad en base a temas de recopilación de eventos en los sistemas de seguridad, permitiendo aumentar la visibilidad de la seguridad y el control de la red de una organización. Las principales características de este tipo de sistemas son:

- Permite describir los activos.
- Realizar evaluación de vulnerabilidades.
- Detección de intrusos.
- Monitoreo conductual.
- Correlacionador de eventos SIEM.

Teniendo en cuenta a la concepción y las características planteadas anteriormente con respecto a este servicio de correlación de eventos, se plantean un conjunto de ventajas y desventajas.

- ✓ Ventajas
    - Integración de varias apps de seguridad relacionadas a eventos de seguridad informática.
    - Permite realizar análisis forense con los datos almacenados.

[34] FARSHID S, Elastic Stack Wazuh Manager Pros and Cons. [En línea]. 2020. Stay curious. Foro. [Consulta: 30 de Mayo 2022]. Disponible: https://seyfm.medium.com/elastic-stack-wazuh-manager-pros-and-cons-e26874393d3

- Soporte mundial con una gran comunidad activa para realizar nuevos avances en la tecnología.
- Disminución de falsos positivos y negativos con el correlacionador de eventos.

✓ Desventajas

- Solo ejecuta actividades de almacenamiento y reporte de eventos, no realiza ninguna acción para detener ataques.

Ya visto la concepción y caracterización de la herramienta en función de las necesidades para implantación de un servicio para correlación de eventos, a continuación, se presentarán un conjunto de requerimientos mínimos de hardware para la correcta ejecución de este servicio:

1. CPU: 1
2. Procesadores: 2
3. CPU(GHz): 2
4. RAM: 2 G B.
5. HARD DISK: 20 GB.
6. NUCLEOS: 4 Núcleos.[35]

Teniendo en cuenta lo desarrollado en este apartado, se puede concluir que las herramientas que permiten suplir las necesidades de implementación de servicios de SOC en la empresa platino sistema, son las de GLPI por parte de la solución correlacionador de eventos, Nagios por parte de la solución para el monitoreo de las redes, Bacula por parte de la solución para la creación de Backups y por último el servicio de Sandboxie para suplir la necesidad del Sandox.

[35] DAVIES Nahla. AlienVault OSSIM. The world's most widely used open source SIEM. [En línea]. 2020. AT&T Alien Labs. (Consulta: 13 de octubre de 2020) Disponible: https://cybersecurity.att.com/products/ossim

## 6.4. HERRAMIENTA HARDWARE PARA EL DESARROLLO DE LAS ACTIVIDADES DEL SOC

Para el desarrollo de las actividades que componen el SOC, es necesario de una herramienta física que apoye la sostenibilidad estructural y operativo del centro de operaciones de seguridad. Teniendo en cuenta la actualidad de hoy, las tecnologías de hardware para las infraestructuras de TI son variadas y adaptables según la necesidad del servicio. Puntualmente refiriéndose a los SOC y la aplicación de uno o varios dispositivos para la ejecución de las actividades que lo componen se pueden encontrar dos tipos de modalidades sobre la cual se podrían suplir estas necesidades.

6.4.1. Servidor DELL EMC Blade PowerEdge M630. Es una de las grandes nuevas herramientas de la familia de servidores Blade que desarrollo DELL, la cual permite tener un mayor ancho de banda en la memoria y el doble de la capacidad de memoria SSD en comparación con las anteriores versiones Blades. Cabe recalcar, que las nuevas actualizaciones especificadas en esta versión de servidores traen un plus en la ampliación, administración y flexibilidad de sus sistemas. Este tipo de sistema cuenta con unas características específicas que lo califican como una herramienta óptima y eficiente al momento de presentar servicios específicos, que son:

- Amplía con facilidad su capacidad de carga de trabajo
- Cuenta con más núcleos para una mayor densidad de virtualización.
- Gran capacidad de memoria.
- Impulsión de aplicación con mayor capacidad de memoria flash.
- Permite la elección del almacenamiento de servidores según necesidad o comodidad.
- Simplifica y automatiza las actividades de administración de las tecnologías de información.
- Mejora la aceleración de las implementaciones de servicios de TI.

- Adaptación a nuevas innovaciones.
- Confiabilidad.
- Aumento en los índices de eficiencias en base a la productividad de sus servicios,

Este dispositivo cuenta con las siguientes especificaciones técnicas.

Cuadro 1. Server Blade PowerEdge M630.

| |
|---|
| ***Procesador*** |
| Familia de productos del procesador Intel® Xeon® E5-2600 v3 |
| ***Sistema operativo*** |
| ✓ Microsoft Windows Server® 2008/2012 R2 (con Hyper-V® habilitado)<br>✓ Microsoft Windows Server 2012 (con Hyper-V habilitado)<br>✓ Microsoft Windows Server 2008/2012 Datacenter (con Hyper-V habilitado)<br>✓ Microsoft Windows Server 2008 R2 SP1 (con Hyper-V habilitado)<br>✓ Microsoft Windows Server 2008 R2 SP2 x64/x86 (con Hyper-V habilitado)<br>✓ Novell® SUSE® Linux Enterprise Server<br>✓ Red Hat® Enterprise Linux |
| ***Chipset*** |
| Chipset Intel serie C610 |
| ***Memoria*** |
| 1.5TB (24 DIMM slots): 4GB/8GB/16GB/32GB/64GB DDR4 |
| ***Hipervisor integrado (opcional)*** |
| Citrix® XenServer®<br>VMware vSphere® ESXiTM |
| ***Almacenamiento*** |
| Opciones de disco duro con conexión en marcha: SSD PCIe PowerEdge Express Flash NVMe, HDD/SSD SATA o HDD/SSD SAS<br>✓ 4 SSD de 1,8"<br>✓ 2 SSD PCIe de 2,5" |
| ***Compartimientos de unidades*** |
| 4 SSD de 1,8"; 2 SSD PCIe de 2,5" |
| ***Módulos de E/S del gabinete*** |
| Ethernet, canal de fibra e Infiniband |
| ***Opciones de tarjetas intermedias de E/S*** |
| 2 tarjetas intermedias PCIe 3.0 (x8) |
| ***Controladoras RAID*** |
| ✓ PERC S130 (RAID SW),<br>✓ PERC H330,<br>✓ PERC H730,<br>✓ PERC H730P |
| ***Comunicaciones*** |
| ***Opciones de adaptador de red selecto de Dell (NDC):***<br>✓ NDC blade KR Broadcom® 57810S-k de dos puertos y 10 Gb<br>✓ NDC blade convergente KR Broadcom 57840 de cuatro puertos<br>✓ NDC blade KR Intel X520-k de dos puertos y 10 Gb |

| |
|---|
| ✓ NDC QLogic® QMD8262-k de dos puertos y 10 Gb<br>***Canal de fibra:***<br>✓ Emulex® LPe1205-M (FC8)<br>✓ Emulex LPm16002B-D (FC16)<br>✓ QLogic QME2572 (FC8)<br>✓ QLogic QME2662 (FC16)<br>***Adaptadores de 1 Gb/10 Gb:***<br>✓ KR Broadcom 57810S-k de dos puertos y 10 Gb<br>✓ CNA Brocade® BR1741M-k de dos puertos y 10 Gb<br>✓ Broadcom 5719 de cuatro puertos y 1 Gb<br>✓ Intel Ethernet X520-K de dos puertos y 10 Gb<br>✓ Intel I350 de cuatro puertos y 1 Gb<br>✓ CNA KR QLogic QME8262-k de dos puertos y 10 Gb<br>***InfiniBand:***<br>✓ FDR10 Mellanox® ConnectX® -3 de dos puertos<br>✓ FDR Mellanox ConnectX-3 de dos puertos<br>✓ QDR Mellanox ConnectX-3 de dos puertos<br>✓ Blade KR Mellanox ConnectX-3 de dos puertos y 10 GbE |
| ***Alimentación*** |
| ***Nivel de chasis:*** opciones de PSU M1000e Platinum de 2700 W y Titanium de 3000 W |
| ***Tarjeta de video*** |
| Tipo de video: Matrox G200 integrado con iDRAC8<br>***Memoria de video:*** 16 MB de memoria compartida con la aplicación iDRAC8 |
| Chasis |
| Blade de altura media hasta con 16 nodos en un chasis M1000e; hasta 4 nodos en infraestructura convergente VRTX<br>***Altura:*** 197,9 mm (7,8 pulg) x Ancho: 50,35 mm (2 pulg) x Profundidad: 544,32 mm (21,4 pulg) |
| Administración |
| **Administración de sistemas:**<br>✓ Cumple con IPMI 2.0<br>✓ Dell OpenManage Essentials<br>✓ Dell OpenManage Mobile<br>✓ Centro de alimentación Dell OpenManage<br>✓ Administración remota iDRAC8 con controladora de ciclo de vida,<br>✓ iDRAC8 Express (predeterminado), iDRAC8 Enterprise (actualización)<br>✓ Medios vFlash de 8 GB (actualización), medios vFlash de 16 GB (actualización)<br>**Integraciones de Dell OpenManage:**<br>✓ Conjunto de integración Dell OpenManage para Microsoft® System Center.<br>✓ Integración Dell OpenManage para VMware® vCenterTM.<br>**Conexiones de Dell OpenManage :**<br>✓ HP Operations Manager, IBM Tivoli® Netcool® , CA Network y administración de sistemas.<br>✓ Complemento de Dell OpenManage para Oracle® Database Manager. |
| Fuente: DELL. Servidor blade PowerEdge M630. [En línea]. 2018. (Consulta: 13 de octubre de 2020) Disponible: https://www.dell.com/co/empresas/p/poweredge-m630/pd |

En base a las necesidades de la implementación adecuada, eficiente y escalable que puede tener un centro de operaciones de seguridad, se puede establecer que la utilización de este dispositivo de hardware (Server Blade PowerEdge M630) es óptimo para la ejecución de las actividades conjuntas que

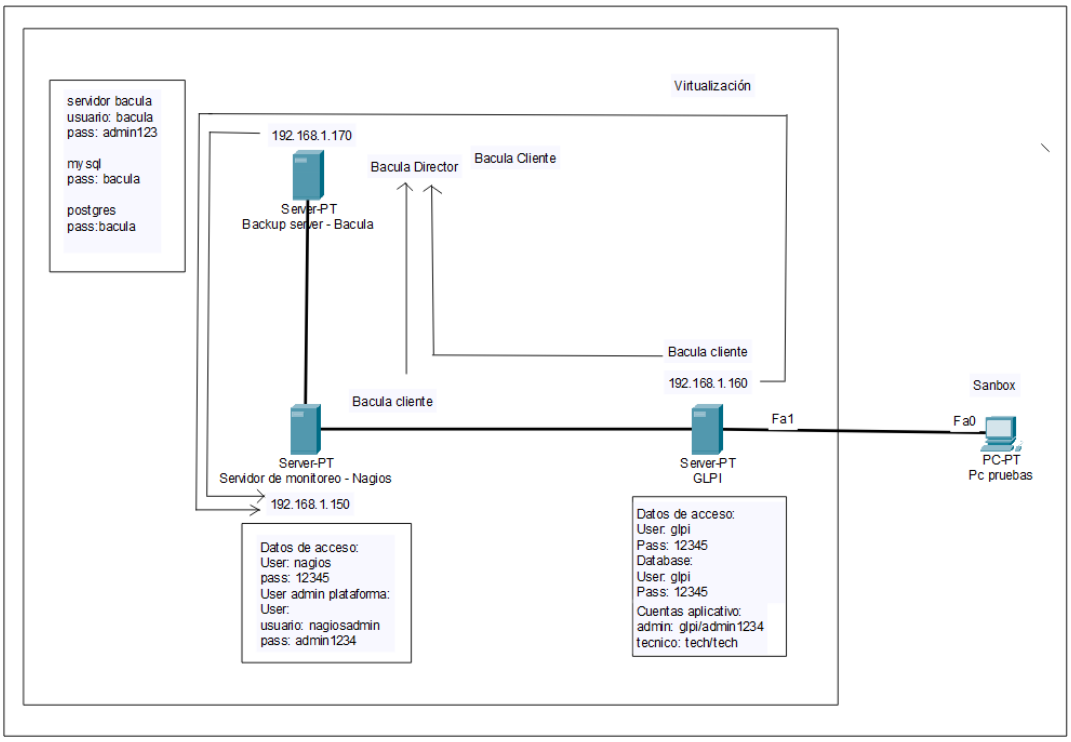
constituyen un SOC, brindándole características de ampliación, administración y flexibilidad en los diferentes servicios y aplicativos que constituyen la implantación en un entorno organizacional.

## 6.5. DISEÑO LÓGICO Y MANUALES DE INSTALACIÓN DE ESCENARIO CONTROLADO

El siguiente apartado plasma tanto el diseño lógico como los manuales de instalación para realizar la representación del escenario controlado que supla las necesidades establecidas de los servicios del SOC para la empresa platino sistemas.

### 6.5.1. Diseño lógico general

Figura 5. Diseño lógico del laboratorio virtualizado.




Fuente: Propia del autor.

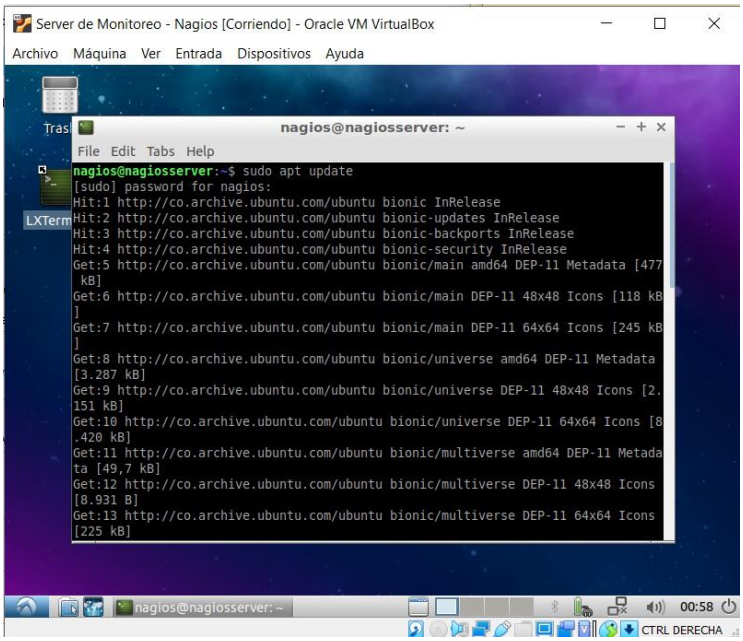
6.5.2. Manual de instalación y configuración de NAGIOS (servidor de monitorización). En este manual se presenta la guía tecnica de la instalación y configuración de un servidor Nagios, el cual permite monitorizar una red y sus recursos tanto a nivel de host como a nivel de servicios. A continuación, se evidencia la línea de comandos guíados de Linux para realizar la instalación de esta herramienta Nagios utilizando un la distribución de Ubuntu Server 18.04 LT.

Primeramente, se debe realizar la instalación del servidor Ubuntu server 2018. Luego de esto se obtienen los siguientes datos de instalación:

- **Etiqueta – Nombre equipo:** Servidor de monitoreo.
- **Nombre del servidor:** nagiosserver.
- **Nombre del usuario administrador:** nagios.
- **Contraseña:** 12345

Siguiendo con el proceso de instalación, se aplica el comando de actualización en el terminar ***sudo apt update*** y se obtiene el siguiente resultado:

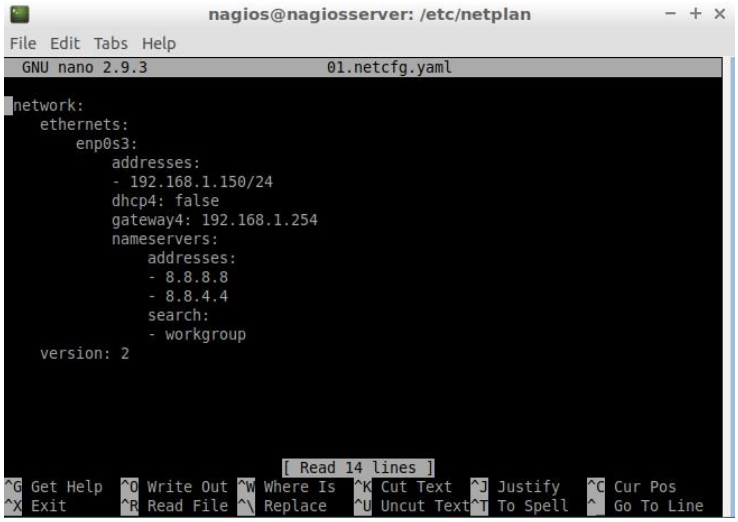
Figura 6. Actualización del servidor - update.




Fuente: Propia del autor

Ya actualizado el sistema, se procederá a realizar a establecer la IP del servidor de forma estática, esto con el objeto de puntualizar una IP fija (192.168.1.150) para el acceso al servidor de monitoreo. Para esto se digita el comando ***Sudo nano /etc/netplan/01.netcfg.yaml*** el cual permitirá establecer una IP fija en la interfaz gráfica del servidor, esto diligenciando la siguiente información sobre el archivo mencionado.

Figura 7. Configuración de interfaz de red estática.

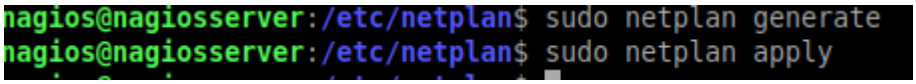



Fuente**:** Propia del autor

**Nota:** la información debe estar exactamente en la posición mostrada en el archivo, puesto que los archivos YAML al realizar configuraciones de red, requieren en posicionamiento exacto de las líneas de texto en función a la interfaz gráfica, es decir, los espacios y comandos están relacionados directamente con la interfaz.

Ya hecha la configuración antes vista, se procede aplicar los siguientes comandos que permitirán generar las configuraciones realizadas en el archivo creado y respectivamente aplicarlas al sistema.

Figura 8. Comandos para generar y aplicar la interfaz de red estática.

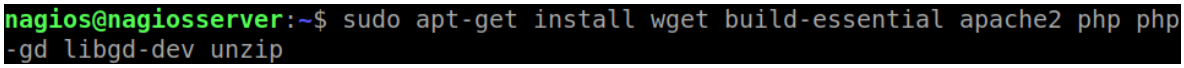



Fuente**:** Propia del autor

Después de generada y aplicadas las configuraciones de la interfaz estática del servidor, se procede a ingresar el comando ***sudo shutdown now -r***, el cual reiniciará el servidor para que los cambios realizados se hagan efectivos.

Realizado los pasos anteriores y configurado el servidor en temas de iniciación e interfaz gráfica. Ahora se procede a realizar la instalación del servidor de monitorización Nagios, para esto se ingresa en la consola en comando ***Sudo apt-get install wget build-essential apache2 php php-gh libgd-dev unzip***, correspondiente al conjunto de dependencias y paquetes necesarios para el funcionamiento de este sistema de monitorización.

Figura 9. Instalación de dependencias y paquetes de Nagios.




Fuente**:** Propia del autor

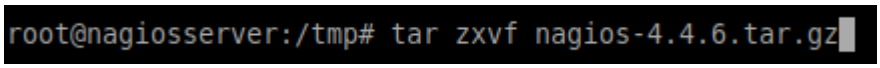
Ya realizado lo anterior, se procede a descargar Nagios en la carpeta ***tmp*** directamente de la página web utilizando el comando ***wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.6.tar.gz*** y al ejecutar éste el resultado a presentar es el siguiente:

Figura 10. Instalación de Nagios.


Fuente: Propia del autor

Ya descargado el aplicativo, se procede a descomprimirlo utilizando el comando ***tar zxvf nagios-4.4.6.tar.gz*** como se muestra a continuación:

Figura 11. Descomprimir Nagios.




Fuente: Propia del autor

Seguido de este se procede a ingresar a la carpeta descomprimida con el comando ***cd nagios-4.4.6*** y se ejecuta el siguiente ***./configure --with-command-group=nagcmd --with-mail=/usr/bin/sendmail --with-httpd-conf=/etc/apache2/*** comando para poner a funcionar el script de configuración de Nagios y crear la carpeta ***Make*.**

Figura 12. Ejecución del script de configuración para crear la carpeta Make.

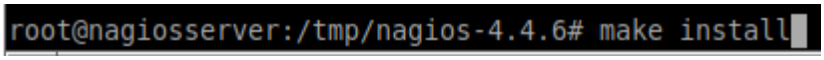

Fuente: Propia del autor

Después de ejecutado el script y creada la carpeta Make, se procede a generar el programa con los siguientes comandos.

1. make all
2. make install
3. make install-init
4. make install-config
5. make install-commandmode
6. make install-webconf

Lo anterior se puede visualizar de la siguiente forma en la consola de Linux.

Figura 13. Make install.




Fuente: Propia del autor

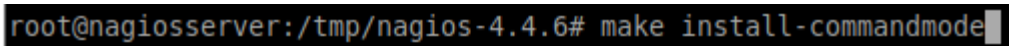
Figura 14. Make install-init


Fuente: Propia del autor

Figura 15. Make install-config


Fuente: Propia del autor

Figura 16. Make install commandmode




Fuente: Propia del autor

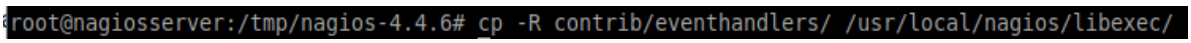
Figura 17. Make install-webconf


Fuente: Propia del autor

Ya generado el programa, se procede a copiar los controladores de eventos y cambiar los permisos para dar la propiedad al usuario Nagios, esto mediante los comandos:

1. ***cp -R contrib/eventhandlers/ /usr/local/nagios/libexec/***

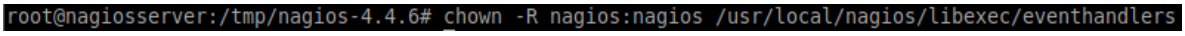
Figura 18. Copiar los controladores de eventos.




Fuente: Propia del autor

2. ***chown -R nagios:nagios /usr/local/nagios/libexec/eventhandlers***

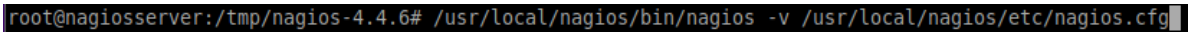
Figura 19. Cambiar permisos de usuario Nagios.




Fuente: Propia del autor

Seguido, se procede a comprobar la configuración de nagios utilizando el comando ***/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg*** . Si la configuración es correcta, no debería presentar ningún mensaje de error.

Figura 20. Comprobación de configuración.

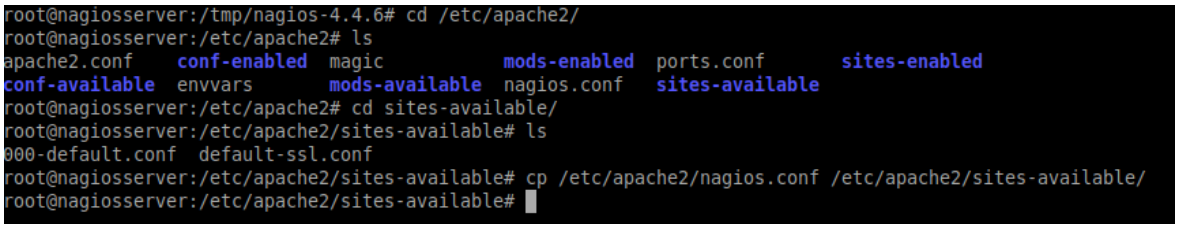



Fuente: Propia del autor

Continuando con el proceso de instalación, ahora se activa el virtual host de apache. Para esto se ingresa a la carpeta ***apache2/sites-available*** y se copia aquí en el host virtual con el siguiente comando ***cp /etc/apache2/nagios.conf /etc/apache2/sites-available*** y después de esto reiniciar el apache 2 y ejecutarlo

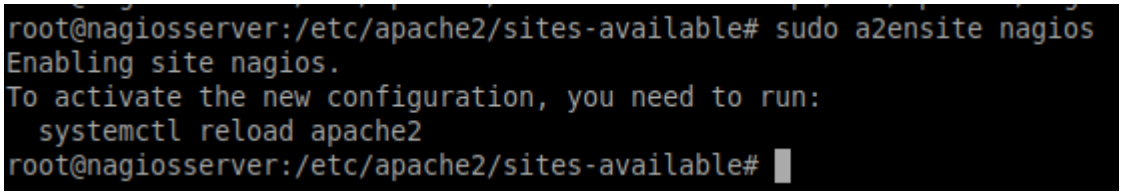
con el comando ***sudo a2ensite nagios***. Este procedimiento se evidencia en las siguientes ilustraciones:

Figura 21. Agregar host virtual al servidor apache2.




Fuente: Propia del autor

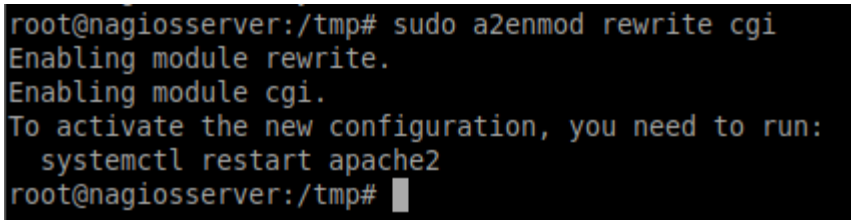
Figura 22. Reiniciar el servidor apache2.




Fuente: Propia del autor

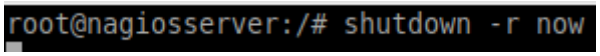
Realizo los pasos anteriores, ahora se activará el módulo cgi mediante el comando ***sudo a2enmod rewrite cgi*** y finalmente se reinicia la máquina virtual con el comando ***shutdown now -r***.

Figura 23. Instalación del módulo cgi.




Fuente: Propia del autor

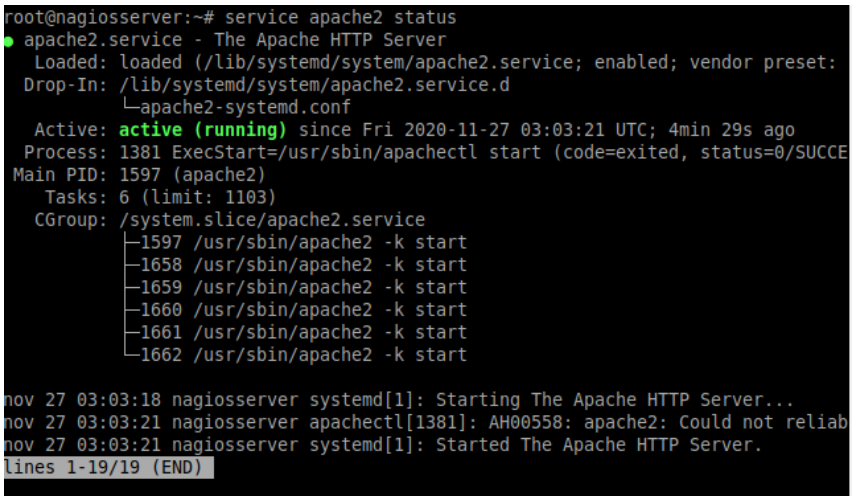
Figura 24. Reinicio de la máquina.




Fuente: Propia del autor

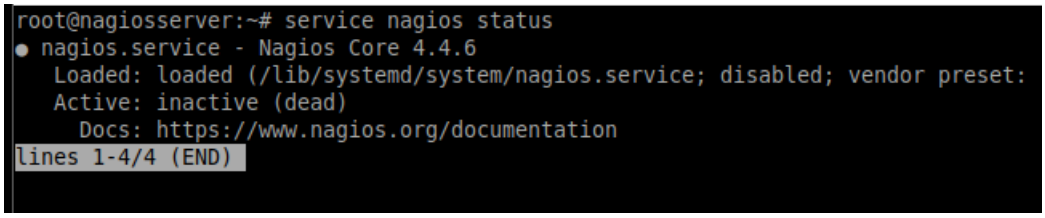
Seguido se realiza la verificación del funcionamiento de los servicios y en caso de que no se encuentre activo el nagios, se procede a activarlo con el comando ***Service nagios start***

Figura 25. Verificación de apache2.



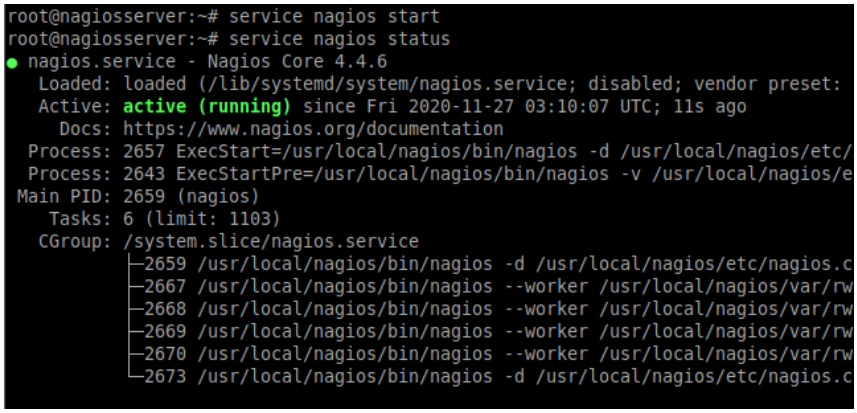

Fuente: Propia del autor

Figura 26. Verificación de Nagios.




Fuente: Propia del autor

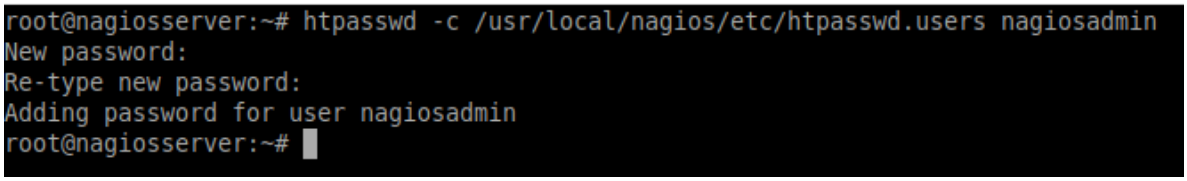
Figura 27. Activación de Nagios.



Fuente: Propia del autor

Ya con el servicio activo, se procede a realizar la creación del usuario administrador de nagios con el comando ***htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin***, este solicitará una contraseña para lo cual se usa **admin1234**.

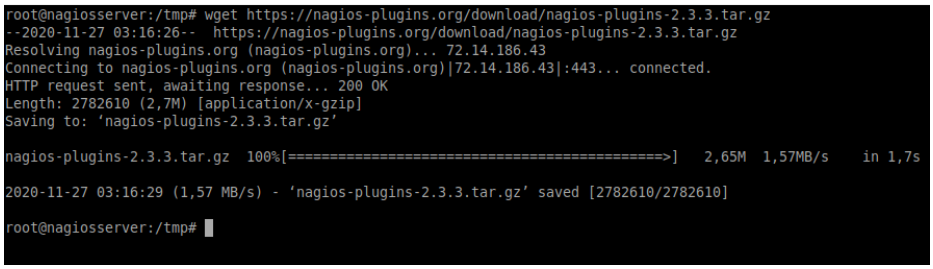
Figura 28. Instalación del usuario admin de Nagios.




Fuente: Propia del autor

Creado ya el usuario, se procede a realizar la instalación de los plugin de Nagios desde la página en la carpeta **tmp**, esto con el fin de obtener atributos de optimización y mejora con respecto al servidor. Se utiliza el comando ***wget https://nagios-plugins.org/download/nagios-plugins-2.3.3.tar.gz*** y a su vez se descomprimen con el comando ***tar zxvf nagios-plugins-2.3.3.tar.gz***.

Figura 29. Descarga de los Plugings.



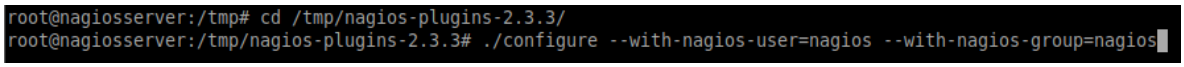

Fuente: Propia del autor

Figura 30. Descomprensión de los plugin.


Fuente: Propia del autor

Seguido de la extracción del plugin, se procede a realizar la ejecución del script de configuración mediante el comando ***cd /tmp/nagios-plugins-2.1.4 ./configure --with-nagios-user=nagios --with-nagios-group=nagios***

Figura 31. Ejecutar script de configuración de plugin.



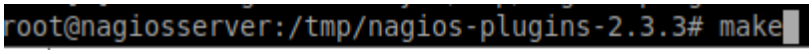

Fuente: Propia del autor

Después de ejecutado el script, se procede a ejecutar el plugin con los siguientes comandos.

1. make all
2. make install
3. make install-init
4. make install-config
5. make install-commandmode
6. make install-webconf

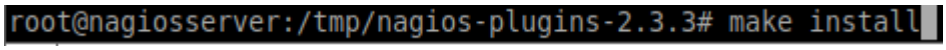
Lo anterior se puede visualizar de la siguiente forma en la consola de Linux.

Figura 32. Make plugin.




Fuente: Propia del autor

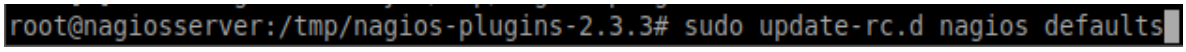
Figura 33Plugin make install.




Fuente: Propia del autor

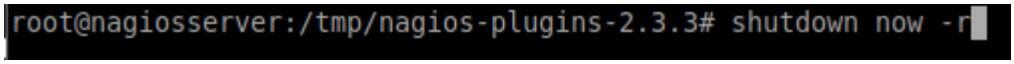
Terminada la instalación, ahora se procede a establecer un registro de ejecución automática del servicio por medio del comando ***sudo update-rc.d nagios defaults*** y se reinicia la máquina con ***shutdown now -r.***

Figura 34. Registro de ejecución automática del servicio.




Fuente: Propia del autor

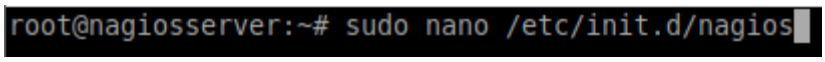
Figura 35. Reinicio de máquina.




Fuente: Propia del autor

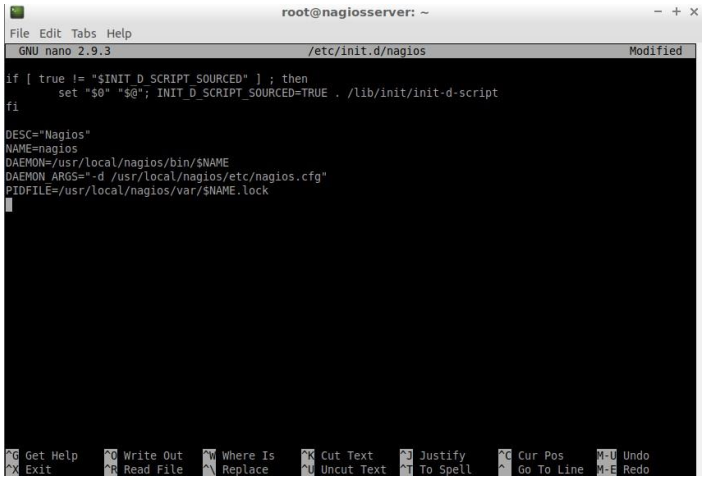
En el siguiente paso se creará un Daemon con el siguiente script para que el nagios inicie automáticamente, para esto se ingresa el comando ***vi /etc/init.d/nagios***, luego se guarda y se asignan privilegios al Daemon con ***chmod +x nagios.***

Figura 36. Creación del Daemon.



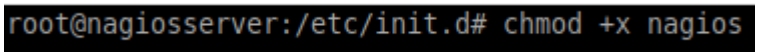

Fuente: Propia del autor

Figura 37. Configuración del Daemon.




Fuente: Propia del autor

Figura 38. Asignación de privilegios al Daemonio.




Fuente: Propia del autor

En este apartado se establece un registro de ejecución automática del servicio enlazado al Daemon por medio del comando ***sudo update-rc.d nagios defaults.***

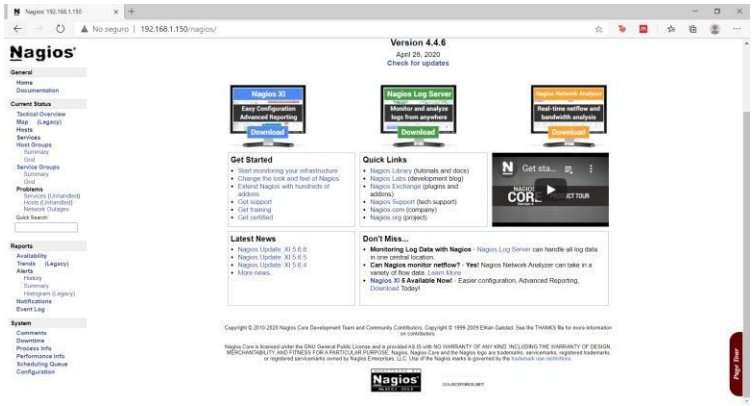
Figura 39. Ejecución automática del servidor por medio del Daemon.

```
root@nagiosserver:/# sudo update-rc.d nagios defaults
```

Fuente: Propia del autor

Luego de realizar todos los pasos anteriores se procede a ingresar a la IP suministrada al servidor y se deberá desplegar la siguiente pantalla de ejecución en el navegador.

Figura 40. Nagios.




Fuente: Propia del autor

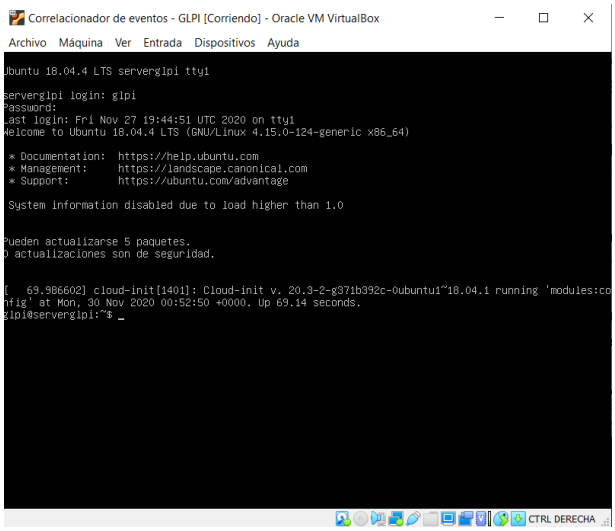
6.5.3. Manual de instalación y configuración de GLPI (servidor de correlacionador de eventos). En este manual se presenta la guía técnica de la instalación y configuración de un servidor LGPI, el cual permite manejar y controlar cambios en la infraestructura informática de una organización de manera eficiente, eficaz y sencilla. A continuación, está la línea de comandos de Linux para realizar la instalación de esta herramienta utilizando Ubuntu Server 18.04 utilizando de intermediario un servidor SSH.

Primeramente, se debe realizar la instalación del servidor Ubuntu server 2018 (Ver guía de instalación de ubuntu server 2018). Luego de esto se obtienen los siguientes datos de instalación:

- **Etiqueta – Nombre equipo:** Servidor – correlacioandor de eventos.
- **Nombre del servidor:** serverglpi.
- **Nombre del usuario administrador:**glpi.
- **Contraseña:** 12345

Siguiendo con el proceso de instalación, se aplica el comando de actualización en el terminar sudo apt update y se obtiene el siguiente resultado:

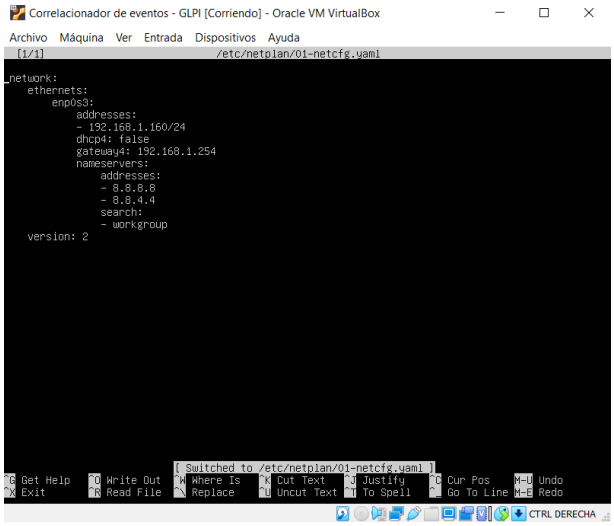
Figura 41. Máquina Ubuntu Server 18.04 - Server GLPI




Fuente: Propia del autor

Ya actualizado el sistema, se procede a realizar el establecimiento de la IP del servidor de forma estática, esto con el objeto de puntualizar una IP fija para el acceso al servidor de monitoreo. Para esto se digita el comando ***Sudo nano /etc/netplan/01.netcfg.yaml*** ,el cual permitirá establecer una IP fija (192.168.1.160) en la interfaz gráfica del servidor, ésto diligenciando la siguiente información en el archivo mencionado.

Figura 42. Configuración IP estática - Server GLPI




Fuente: Propia del autor

**Nota:** la información debe estar exactamente en la posición mostrada en el archivo, puesto que los archivos YAML al realizar configuraciones de red, requieren en posicionamiento exacto de las líneas de texto en función a la interfaz gráfica, es decir, los espacios y comandos están relacionados directamente con la interfaz.

Ya hecha la configuración antes vista, se procede a aplicar los siguientes comandos que permitirán generar las configuraciones realizadas en el archivo creado y respectivamente aplicarlas al sistema.

Figura 43. Generación y aplicación de conf. Red.

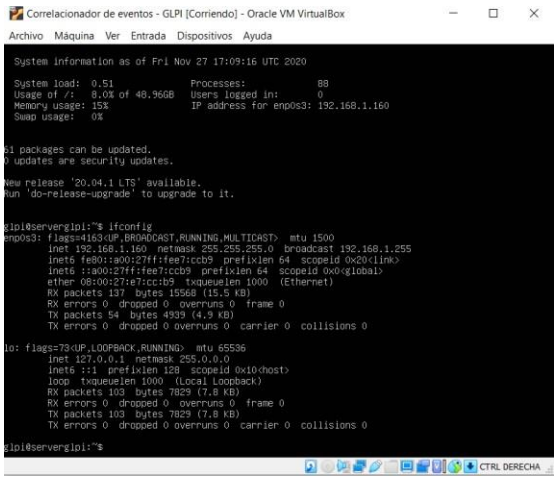
```
glpi@serverglpi:/etc/netplan$ sudo netplan generate
glpi@serverglpi:/etc/netplan$ sudo netplan apply
```

Fuente: Propia del autor

Después de generada y aplicadas las configuraciones de la interfaz estática del servidor, se procede a ingresar el comando ***sudo shutdown now -r***, el cual reiniciará el servidor para que los cambios realizados se hagan efectivos.

Por siguiente, se realiza la verificación de la interface de red de la máquina y se valida si efectivamente los cambios que se realizaron anteriormente.

Figura 44. Confirmación cambios a IP estática.

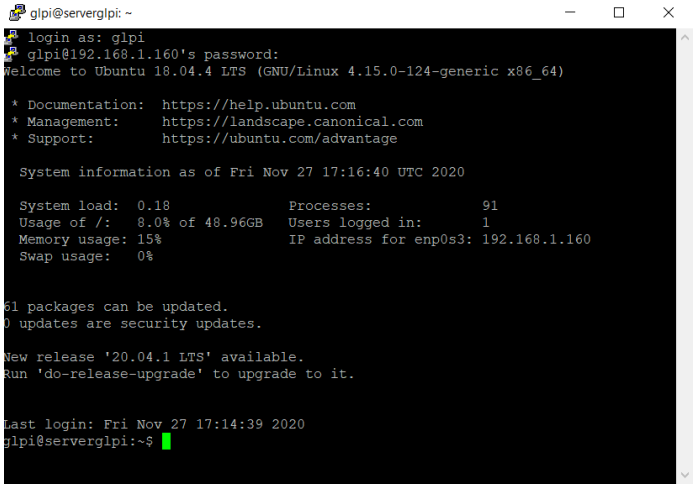



Fuente: Propia del autor

**Nota:** En caso de que no se haya realizado el servidor SSH para conexión remota al instalar ubuntu server, se debe instalar con el comando ***sudo apt-get install openssh-server***.

Luego de hacer la verificación de la ip de la máquina, se procede a realizar acceso remoto mediante la herramienta putty desde windows y el resultado del acceso será el siguiente, como se visualiza en la Figura 40.

Figura 45. Acceso remoto - Putty Windows.



Fuente: Propia del autor

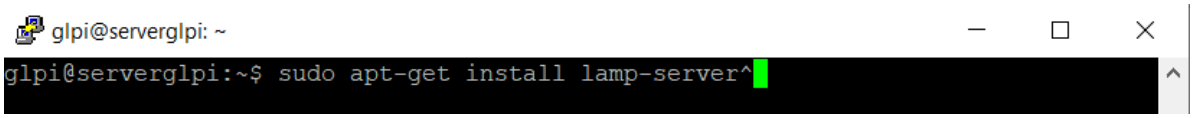
En el acceso remoto, se procede a realizar la actualización del servidor en su totalidad con la combinación de comando sudo ***apt-get update && sudo apt-get upgrade***, seguido de ésto se pulsa el comando ***shutdown now -r*** para confirmar los cambios y se accede nuevamente de manera remota.

Figura 46. Actualización total server Ubuntu 18.04.


Fuente: Propia del autor

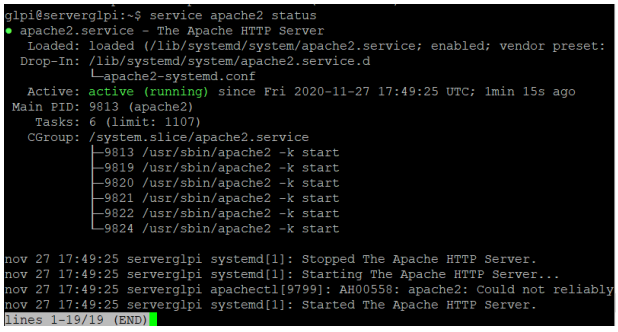
Ya realizada la actualización del Ubuntu server, se procede a realizar la instalación con permisos administrativos del conjunto de paquetes del servidor lamp con el comando ***sudo apt-get install lamp-server^*** y seguido de eso se verifica la instalación del conjunto de aplicativos que constituyen el servicio (apache2 y MySQL).

Figura 47. Instalación de los paquetes del servidor LAMP.



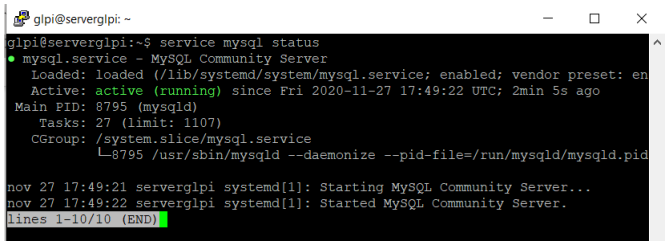

Fuente: Propia del autor

Figura 48. Verificación de instalación de apache2.




Fuente: Propia del autor

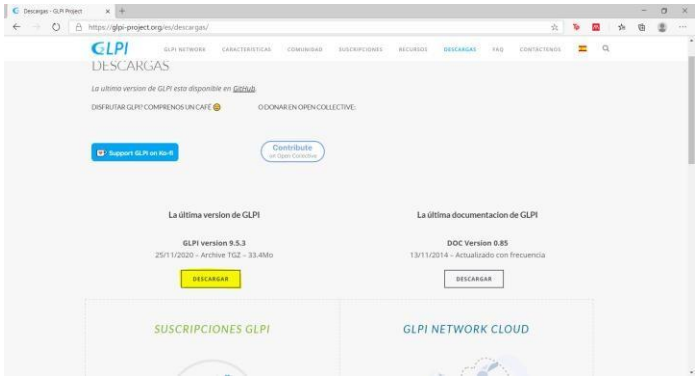
Figura 49. Verificación de instalación de MySQL.




Fuente: Propia del autor

Después de instalar con éxito el paquete del servidor LAMP, se accede al navegador de la máquina Windows sobre la cual se está usando el SSH para conectar la máquina Ubuntu server y se descarga la herramienta de GLPI. Lo anterior, como se muestra en la siguiente Figura:

Figura 50. Página de GLPI.



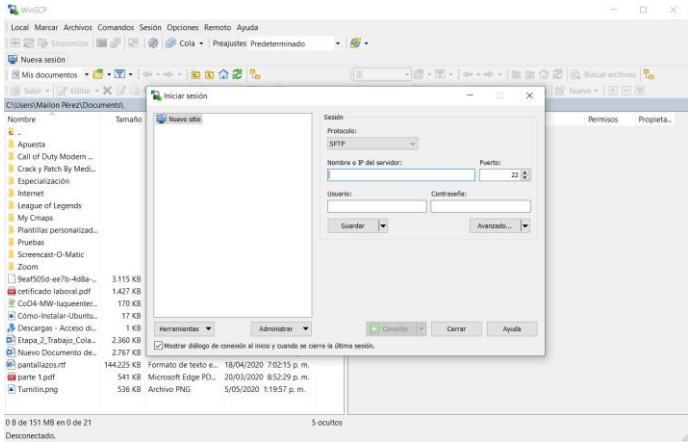

Fuente: Propia del autor

Figura 51. Descarga de la GLPI.


Fuente: Propia del autor

Luego de realizado la descarga y ubicado el archivo en una ubicación de preferencia, se procede a realizar instalación del aplicativo WinSCP.

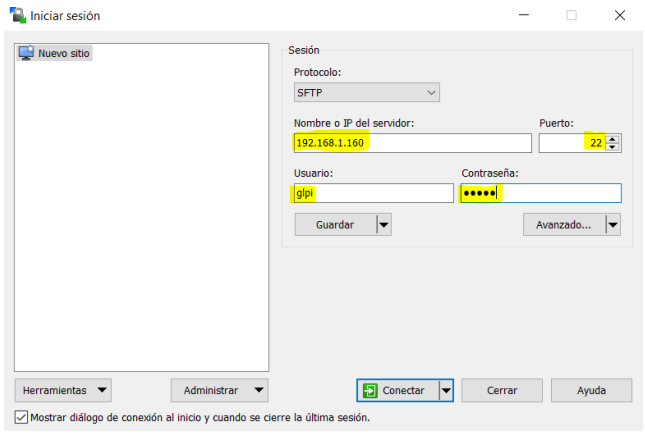
Figura 52. App WinSCP



Fuente: Propia del autor

Luego de realizar la instalación de este, se procede a iniciar sesión en el servidor Ubuntu server, del mismo modo que la conexión SSH para acceso remoto utilizando la IP del servidor (***192.168.1.160***), el puerto (**22**) y el usuario y contraseña del servidor, como se muestra en la Figura siguiente:

Figura 53. Configuración WinSCP

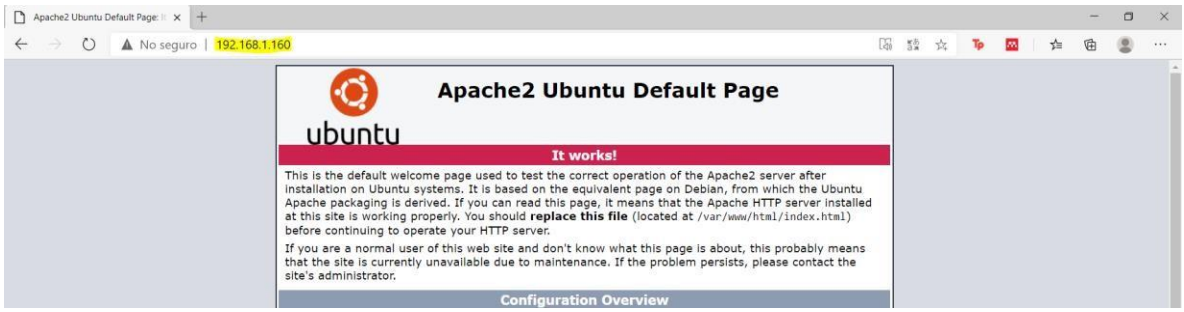



Fuente: Propia del autor

Al tener el acceso satisfactorio en el aplicativo WinSCP, se verifica el acceso a el servidor apache y a su vez en el acceso remoto de SSH se le asignan privilegios de modificación a la carpeta ***/var/www*** de este, con la finalidad de poder ingresar

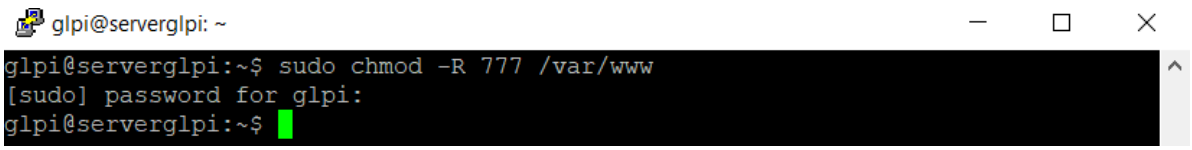
los archivos descargados anteriormente en la página de GLPI, los cuales permitirán realizar el proceso de instalación del servicio.

Figura 54. Validación de funcionamiento de apache2.




Fuente: Propia del autor

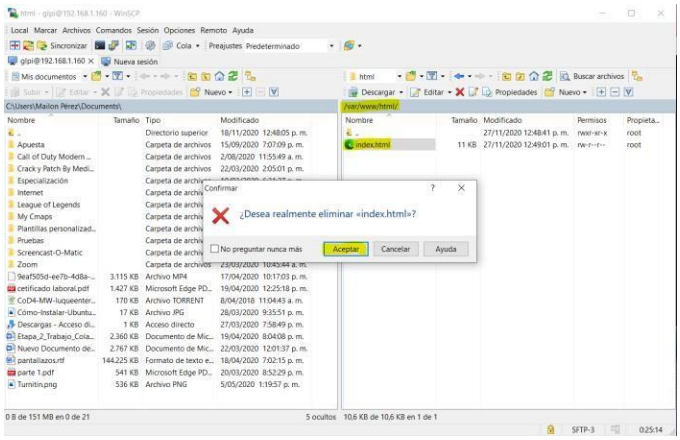
Figura 55. Asignación de privilegios de modificación a la carpeta www.




Fuente: Propia del autor

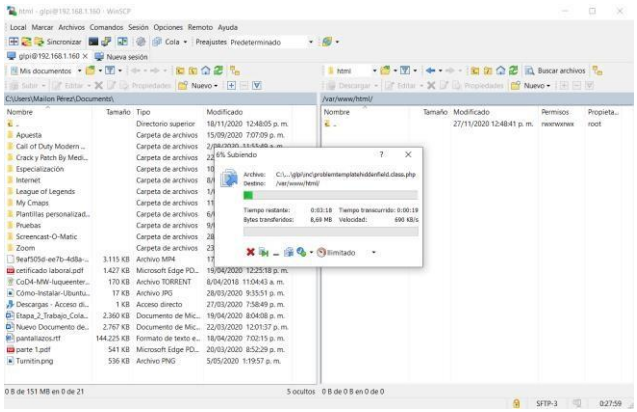
Después de asignados los permisos, se accede a WinSCP con el acceso ya realizado, se busca el directorio de apache ***/var/www/html/*** y se elimina el índex correspondiente al apache2 para luego pegar la carpeta descomprimida de GLPI.

Figura 56. Eliminación de índex original de Apache2.




Fuente: Propia del autor

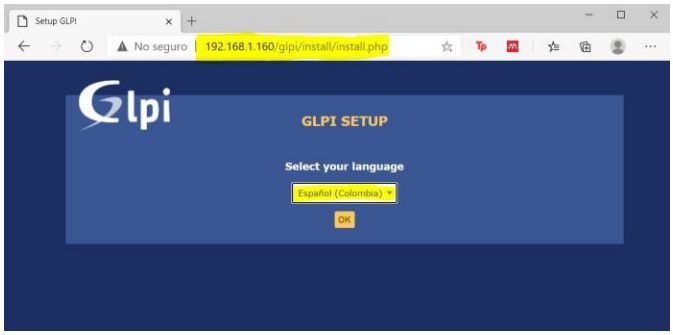
Figura 57. Inserción de GLPI en apache.



Fuente: Propia del autor

Luego de realizar el proceso anterior, se ingresa la siguiente dirección ***(Ip Servidor)/glpi/install/install.php*** en este caso (***192.168.1.160/glpi/install/install.php***) y esto desplegará el Setup de instalación web de la herramienta.

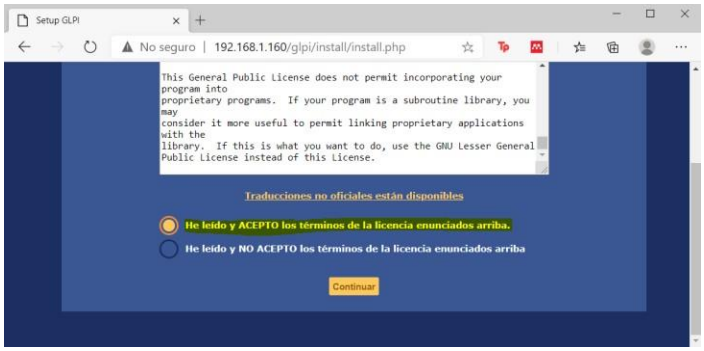
Figura 58. SETUP GLPI.




Fuente: Propia del autor

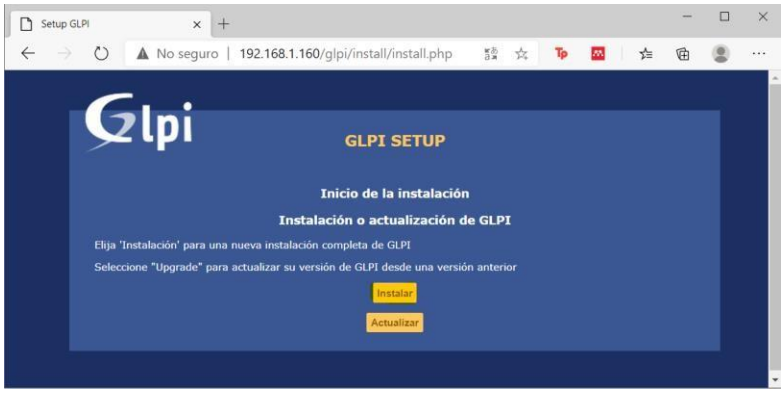
A continuación, se presentarán un conjunto de ilustraciones guiadas para la correcta instalación del aplicativo:

Figura 59. Aceptación de términos – GLPI.




Fuente: Propia del autor

Figura 60. Ejecutar instalador - GLPI.




Fuente: Propia del autor

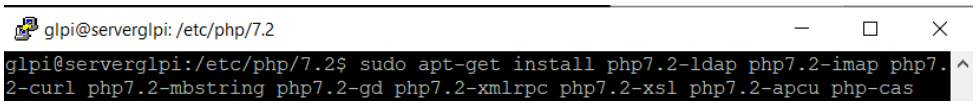
Al realizar la primera instalación del aplicativo por defecto según el servidor y las herramientas, muestra este conjunto de atributos indispensables para el funcionamiento correcto de la GLPI.

Figura 61. Atributos faltantes GLPI


Fuente: Propia del autor

Como primera solución se deben de instalar manualmente las extensiones que aparecen con signos rojos y naranjas como se muestra en la siguiente Figura. Cabe recalcar que se instalan por su nombre en específico.

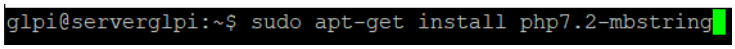
Figura 62. Instalación de extensiones faltantes.




Fuente: Propia del autor

En caso de que falte algún complemento al momento de darle en el botón de abajo del instalador refresh, se procede a instalarlo manualmente con ***sudo apt-get install (extension)***.

Figura 63. Instalación manual de extensiones.




Fuente: Propia del autor

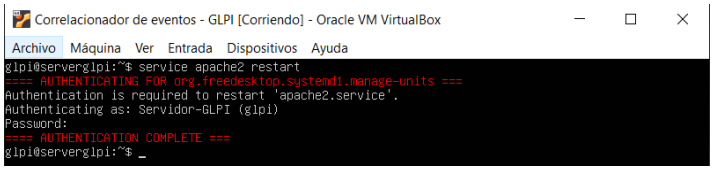
Para resolver el problema con la parte de pruebas, verificaciones y comprobaciones, se procede a asignarle privilegios a la carpeta glpi con el comando ***sudo chown ww-data:www-data /var/www/html/glpi/* -R*** y se refresca el proceso de instalación y se solventara ese error.

Figura 64. Asignación de privilegios GLPI.


Fuente: Propia del autor

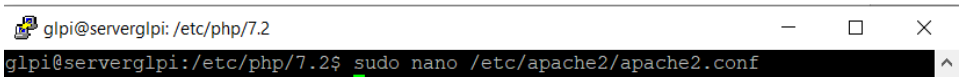
Luego se reinicia el servidor apache2 y después de esto, se ingresa al archivo de configuración de apache con el comando ***sudo nano /etc/apache2/apache2.conf*** y se modifica en el directorio **/var/www/** los Allowoverride de None a **All.**

Figura 65. Reinicio de apache2.



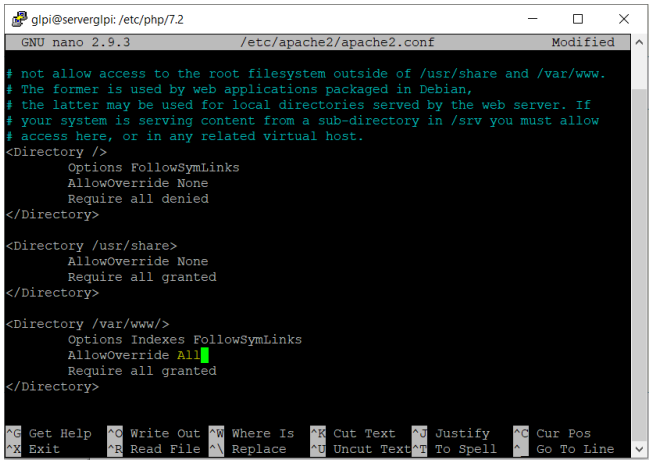

Fuente: Propia del autor

Figura 66. Ingreso a archivo de configuración de apache2.




Fuente: Propia del autor

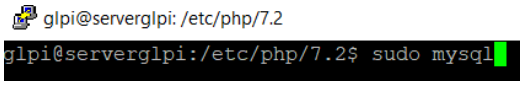
Figura 67. Modificación del acrhivo Apache2.




Fuente: Propia del autor

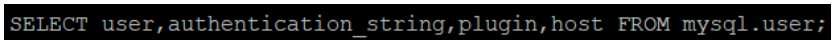
En la mayoría de las instalaciones de MySQL al no instalarse con el instalador de seguridad no se le asigna una contraseña al usuario root y puede acceder a la DB sin una, pero para esta instalación en especial, se requiere que el usuario root presente una contraseña para lo cual se seguirán los comandos presentados en las siguientes ilustraciones para suministrarle una y evitar problemas futuros con la instalación. Finalmente se reinicia apache y se sigue con la instalación.

Figura 68. Ingreso a MySQL.




Fuente: Propia del autor

Figura 69. Selección de autentificación de usuario.

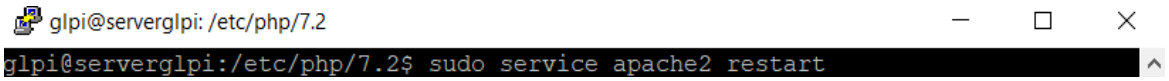



Fuente: Propia del autor

Figura 70. Asignación de contraseña a usuario Root.


Fuente: Propia del autor

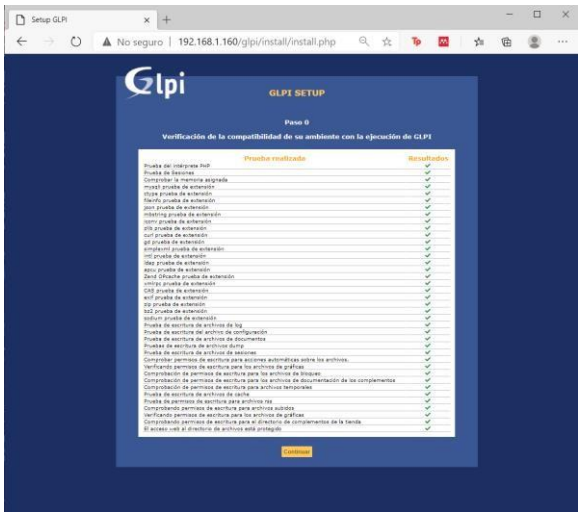
Figura 71. Reinicio de apache2.



Fuente: Propia del autor

El resultado de la ejecución y las configuraciones de todos los pasos realizados anteriormente será la siguiente:

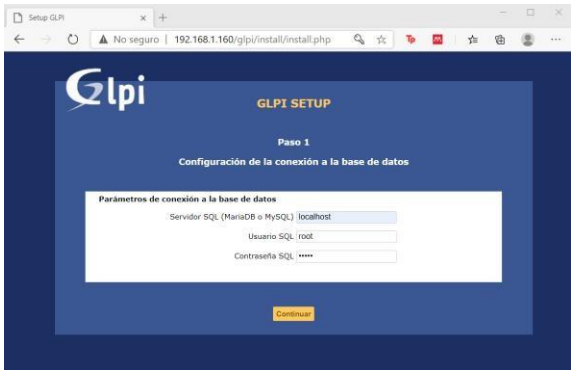
Figura 72. Configuración correcta de GLPI




Fuente: Propia del autor

Seguido de la confirmación correcta de todos los elementos del servicio, se procede a configurar la base de datos, sobre la cual solicitará datos Servidor SQL (***localhost***), Usuario SQL: ***root*** y Contraseña SQL: ***12345***

Figura 73. Configuración de la base de datos.

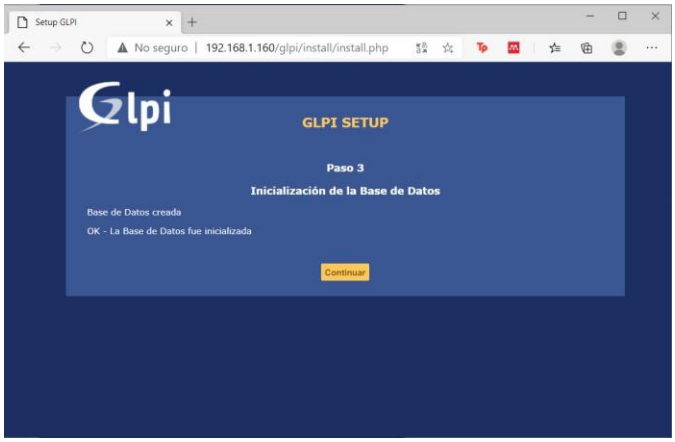



Fuente: Propia del autor

Figura 74. Creación de la base de datos GLPI.


Fuente: Propia del autor

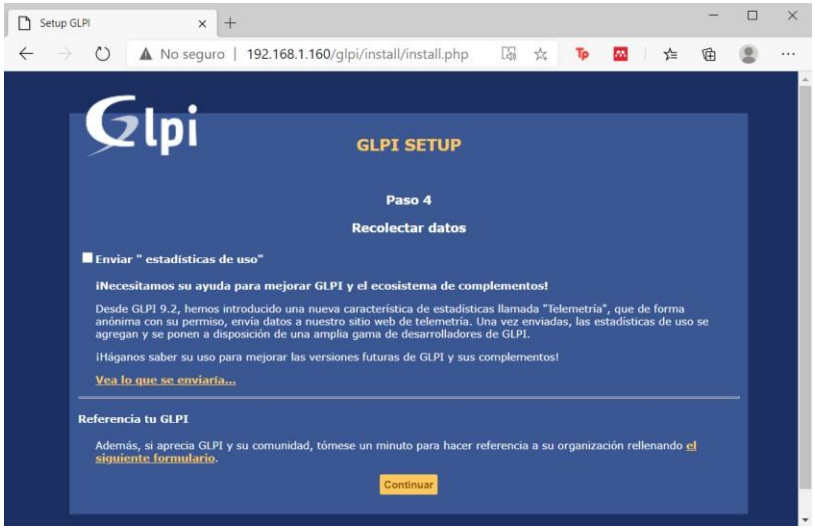
Figura 75. Confirmación de la creación de la base de datos.




Fuente: Propia del autor

Después de a la confirmación de la creación de la base de datos, el aplicativo redireccionará el recordatorio de casos, para el cual se presiona continuar y se omite este paso.

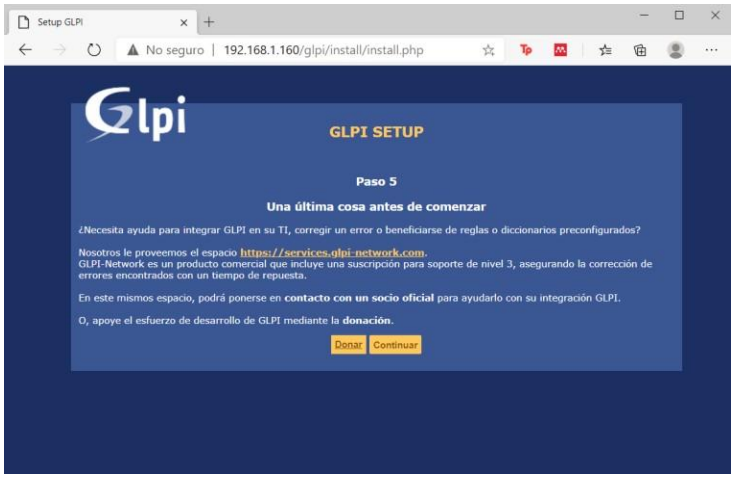
Figura 76. Recordar datos.




Fuente: Propia del autor

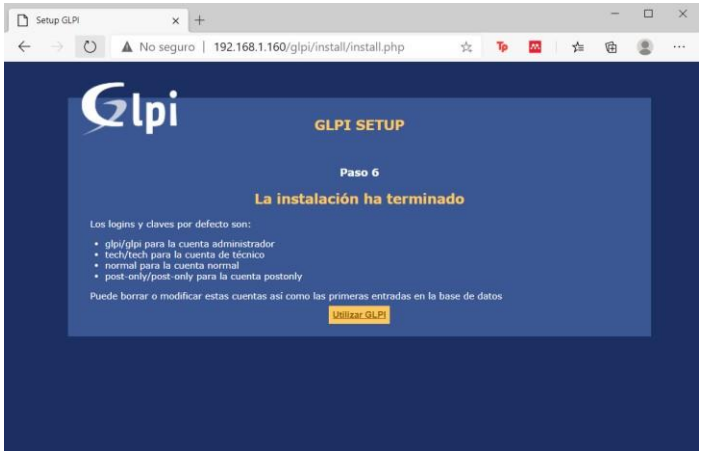
Este apartado es totalmente opcional del aplicativo, donde se establece si se realizará alguna donación al respecto, el cual se puede omitir o realizar una donación a la causa.

Figura 77. Donar.




Fuente: Propia del autor

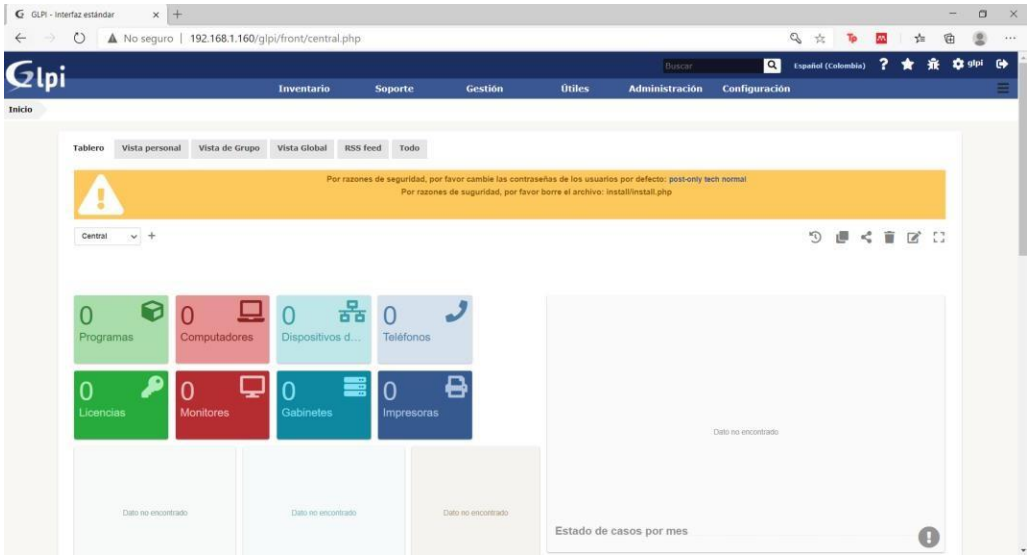
Figura 78. Confirmación de instalación correcta.




Fuente: Propia del autor

Ya terminado el proceso de instalación, se procede a presionar el botón utilizar GLPI y se debe presentar la siguiente pantalla de carga:

Figura 79. Ejecución de aplicativo GLPÏ




Fuente: Propia del autor

**Nota:** El acceso a esta es ***192.168.1.160/glpi/***

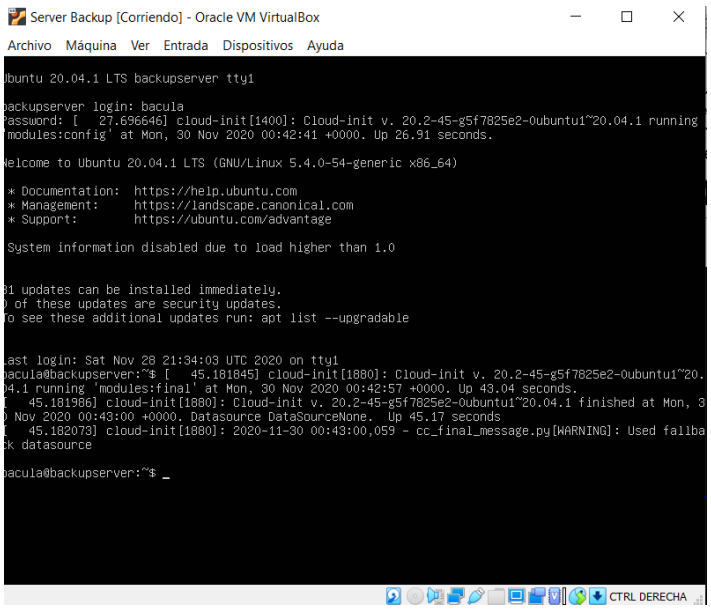
6.5.4. Manual de instalación y configuración de BACULA (servidor de Backup). En este manual se presenta la guía técnica de la instalación y

configuración de un servidor Bacula, el cual permite gestionar la copia de seguridad, recuperación y verificación de datos informáticos a través de una red de equipos de diferentes tipos. A continuación, está la línea de comandos de Linux para realizar la instalación de esta herramienta utilizando Ubuntu Server 20.04 por medio de un servidor SSH.

Primeramente, se debe realizar la instalación del servidor Ubuntu server 2018 (Ver guía de instalación de ubuntu server 2018). Luego de esto se obtienen los siguientes datos de instalación:

- **Etiqueta – Nombre equipo:** Servidor de backup
- **Nombre del servidor:** backupserver.
- **Nombre del usuario administrador:**bacula.
- **Contraseña:** admin123

Figura 80. Instalación Maquina Ubuntu Server 20.04

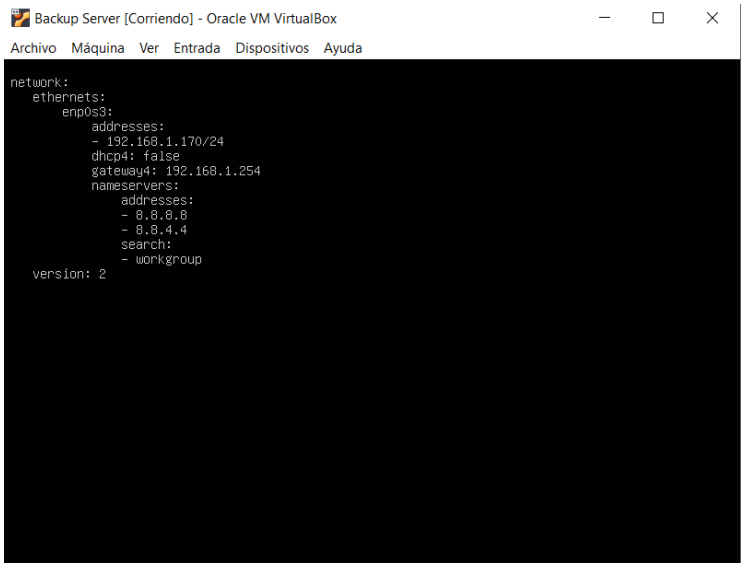



Fuente: Propia del autor

Ya actualizado el sistema, se procederá a realizar a establecer la IP del servidor de forma estática, esto con el objeto de puntualizar una IP fija para el acceso al

servidor de monitoreo. Para esto se digita el comando ***Sudo nano /etc/netplan/01.netcfg.yaml*** el cual permitirá establecer una IP fija (192.168.1.170) en la interfaz gráfica del servidor, esto diligenciando la siguiente información en el archivo mencionado.

Figura 81. Configuración de red estática.

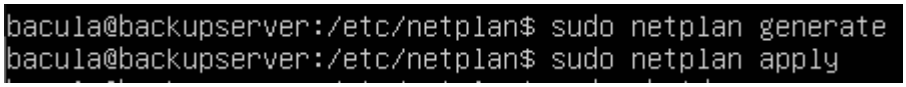



Fuente: Propia del autor

**Nota:** la información debe estar exactamente en la posición mostrada en el archivo, puesto que los archivos YAML al realizar configuraciones de red, requieren en posicionamiento exacto de las líneas de texto en función a la interfaz gráfica, es decir, los espacios y comandos están relacionados directamente con la interfaz.

Ya hecha la configuración antes vista, se procede a aplicar los siguientes comandos que permitirán generar las configuraciones realizadas en el archivo creado y respectivamente aplicarlas al sistema.

Figura 82. Generación y aplicación de cambios en la red.

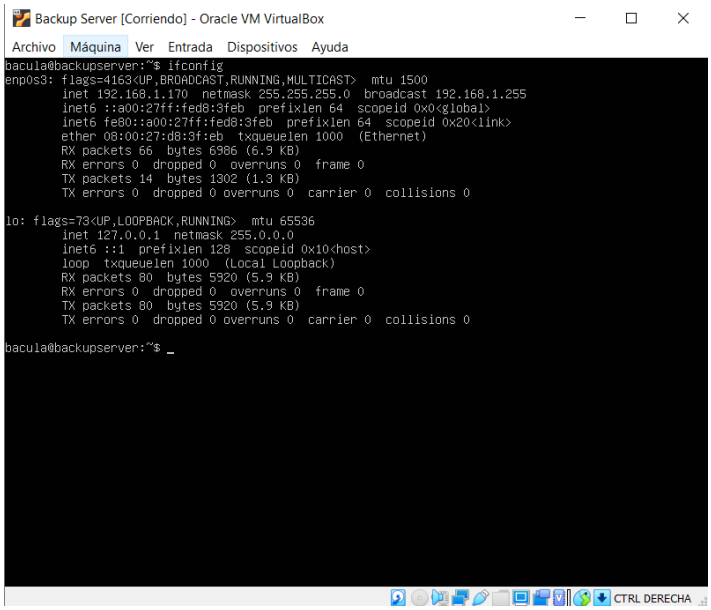



Fuente: Propia del autor

Después de generada y aplicadas las configuraciones de la interfaz estática del servidor, se procede a ingresar el comando ***sudo shutdown now -r***, el cual reiniciará el servidor para que los cambios realizados se hagan efectivos.

Por siguiente, se realiza la verificación de la interface de red de la máquina y se valida si en efecto los cambios realizados anteriormente se efectuaron.

Figura 83. Validación de IP estática.

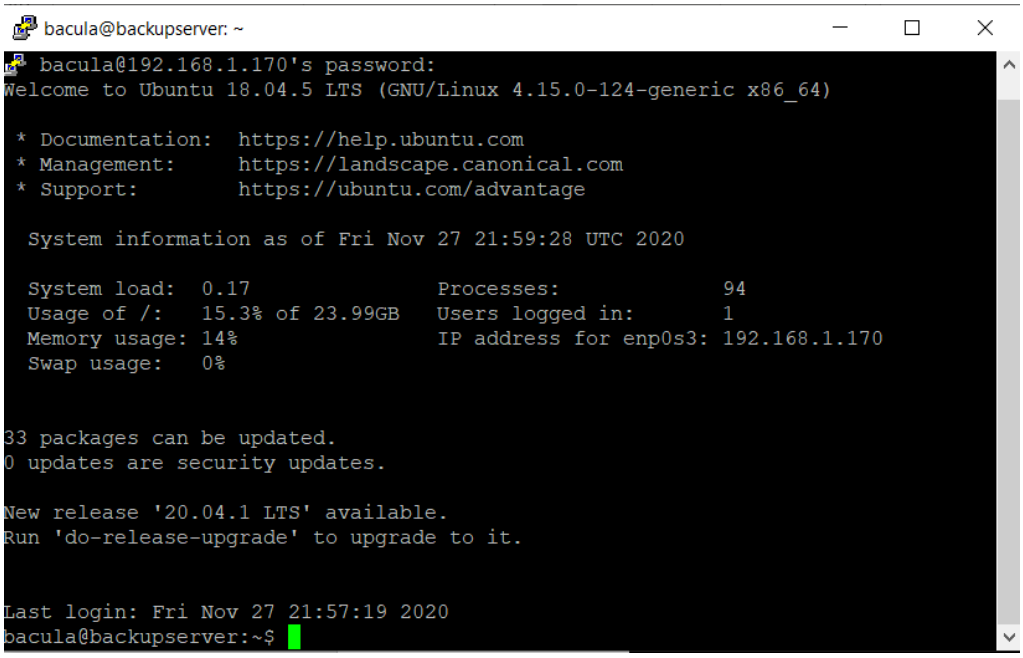



Fuente: Propia del autor

**Nota:** En caso de que no se haya realizado el servidor SSH para conexión remota al instalar ubuntu server, se debe instalar con el comando ***sudo apt-get install openssh-server.***

Luego de hacer la verificación de la ip de la máquina, se procede a realizar acceso remoto mediante la herramienta **PuTTy** desde Windows y el resultado del acceso será el siguiente.

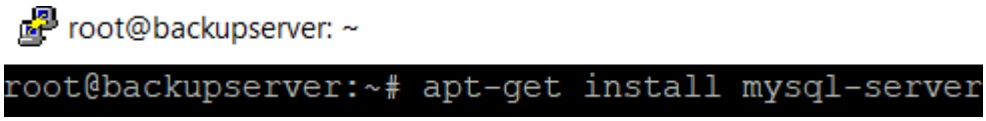
Figura 84. Ingreso máquina virtual por SSH




Fuente: Propia del autor

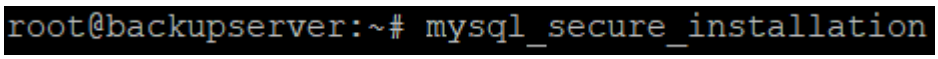
En el acceso remoto, se procede a realizar la actualización del servidor con el comando ***sudo apt-get update***. Ya actualizado el sistema se procederá a realizar la instalación de las herramientas y el servicio de Backup, para esto primeramente se realizará la instalación seguirá del MySQL, por medio del comando ***sudo apt-get install mysql-server***, seguido del comando ***mysql_sucure_installation***.

Figura 85. Instalación de MySQL.




Fuente: Propia del autor

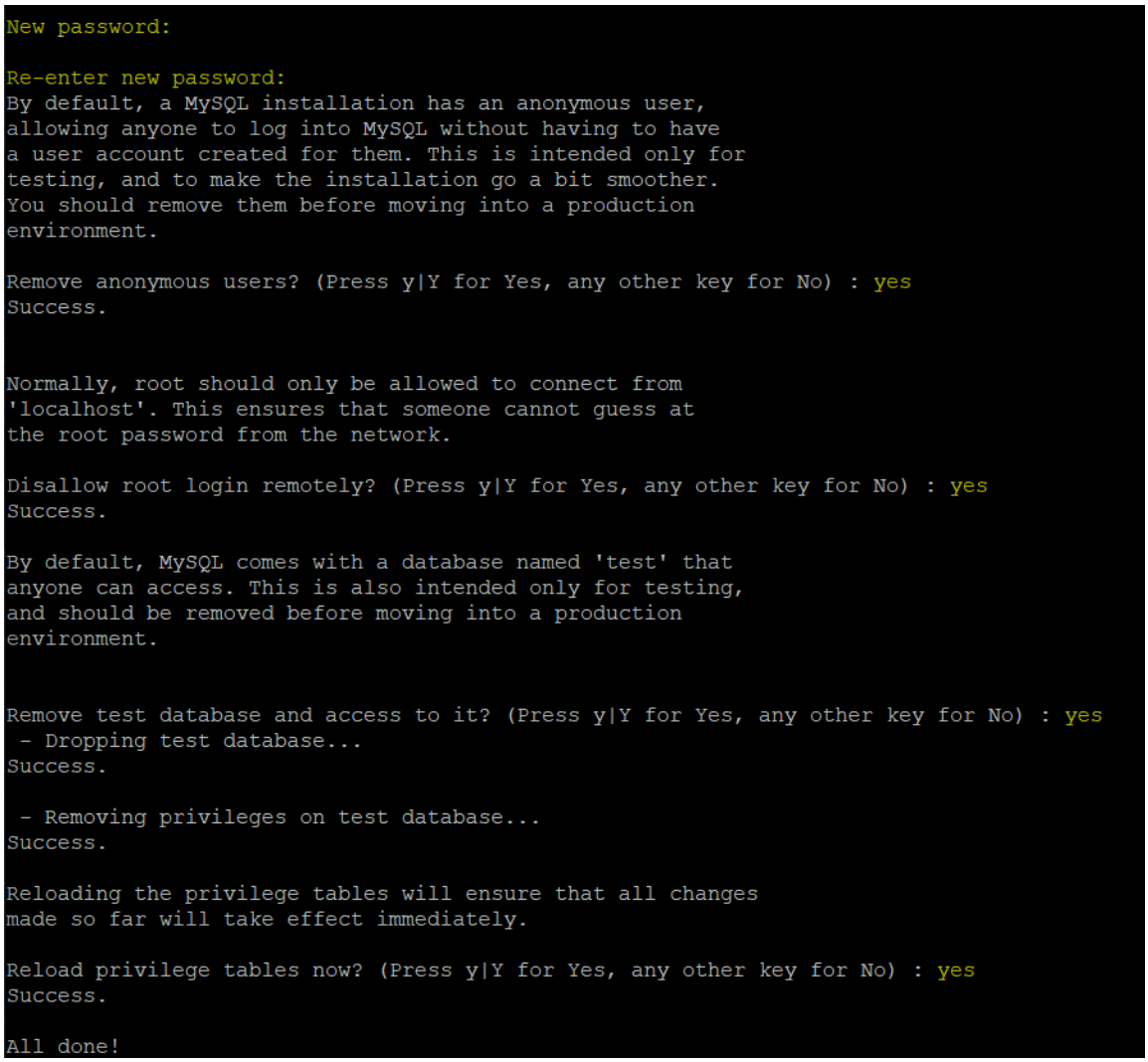
Figura 86. Instalación segura de MySQL




Fuente: Propia del autor

Al ejecutar el comando para la instalación de MySQL, se desplegará un conjunto de opciones las cuales son de la siguiente forma:

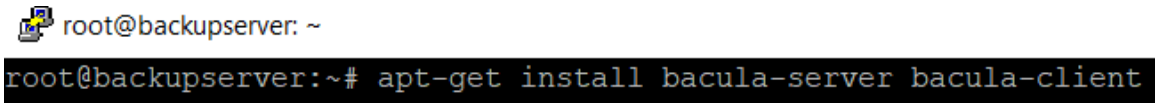
Figura 87. Líneas de verificación de MySQL secure.




Fuente: Propia del autor

Terminado con la instalación adecuada de MySQL, ahora se continúa con la instalación del servidor de respaldo (BACULA) y su cliente utilizando el comando ***apt-get install bacula-server bacula-cliente*** como se muestra a continuación:

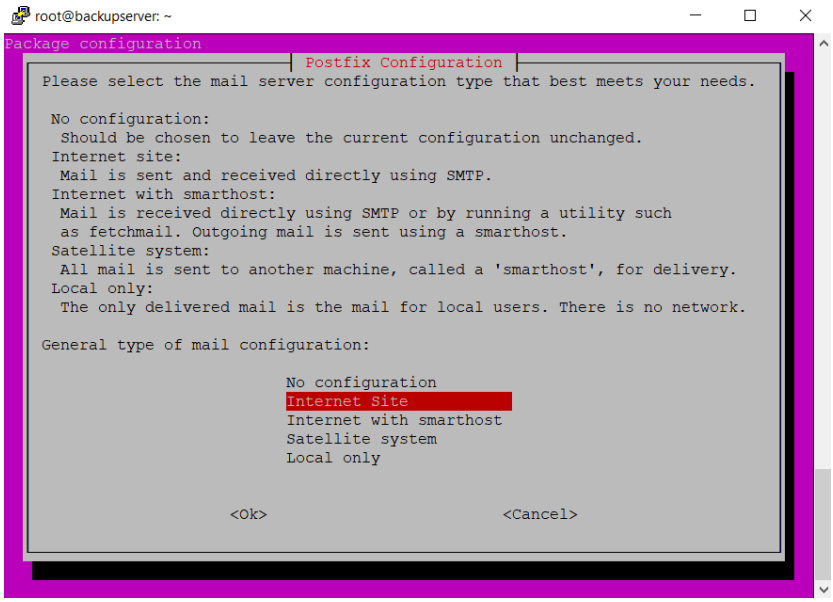
Figura 88. Instalación de Bacula y su cliente.




Fuente: Propia del autor

Luego de la ejecución del comando se desplegará el primer menú de instalación relacionado al servidor postfix para las notificaciones, para este caso se seleccionará ***Internet site*** y se sigue con la instalación.

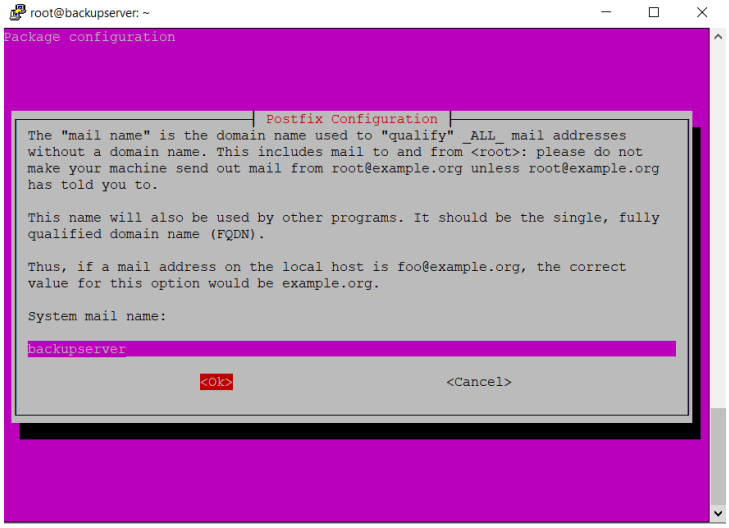
Figura 89. Postfix Bacula.




Fuente: Propia del autor

Como no se hará énfasis en la instalación del servicio main, se deja el nombre por defecto como se presenta la aplicación y se pulsa ***ok***

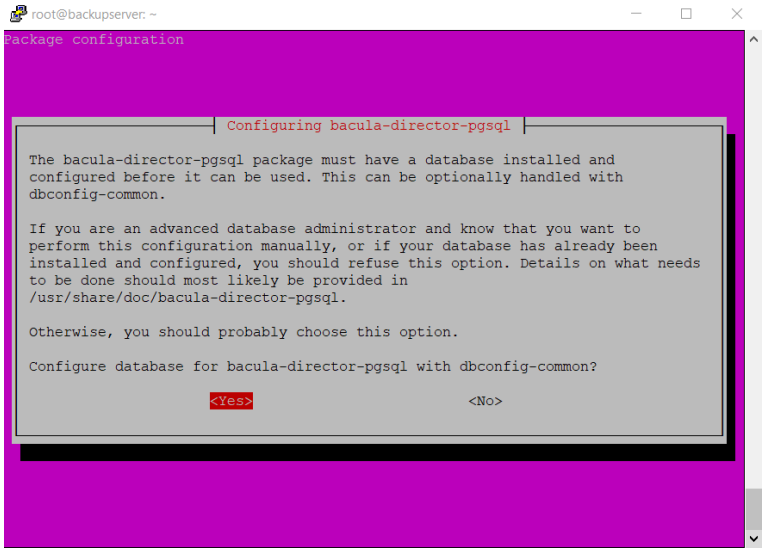
Figura 90. System mall name.




Fuente: Propia del autor

Ya seguido, se presentará una pantalla de carga y seguirá la ejecución con la configuración por defecto de la aplicación para el director de Bacula, para lo cual selecciona ***yes*** y se sigue con el proceso.

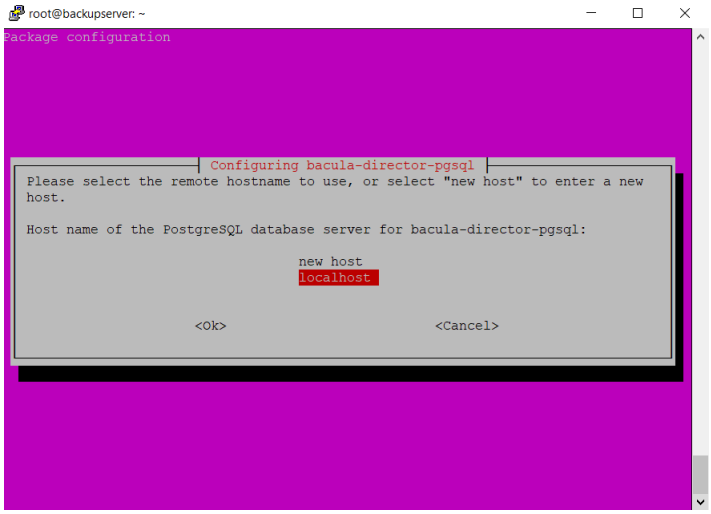
Figura 91. Bacula director - Postgres.




Fuente: Propia del autor

Se le pedirá que seleccione el host del servidor ***PostgreSQL*** como se muestra a continuación:

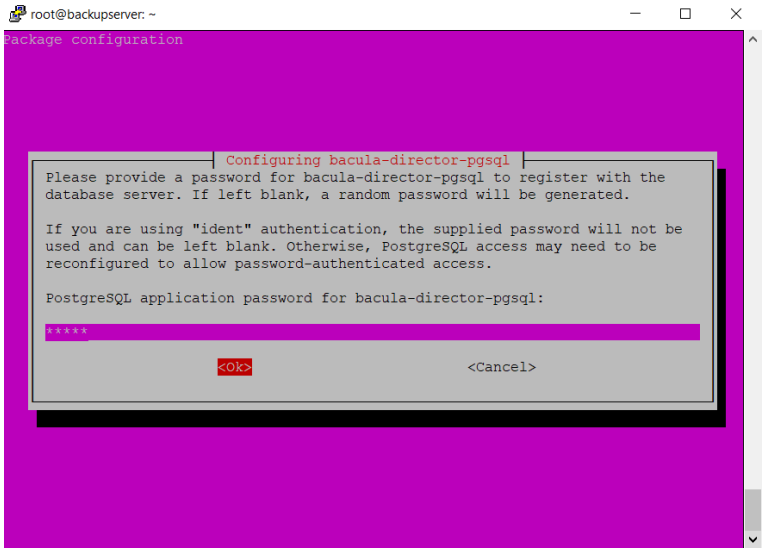
Figura 92. Host.




Fuente: Propia del autor

Seleccione ***localhost*** y haga clic en el botón Aceptar. Se le pedirá que proporcione la contraseña de PostgreSQL como se muestra a continuación:

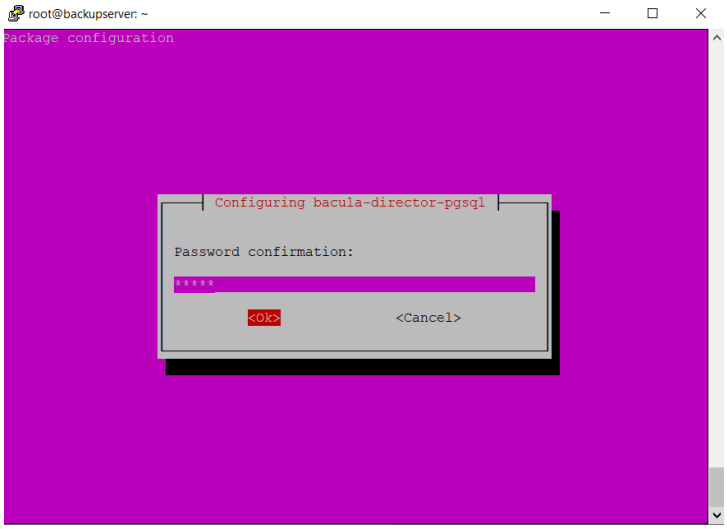
Figura 93. Contraseña de Postgres.



Fuente: Propia del autor

Se le proporcionará una password a Postgres(bacula), se seleccionará ***Ok*** y se continuará con la instalación.

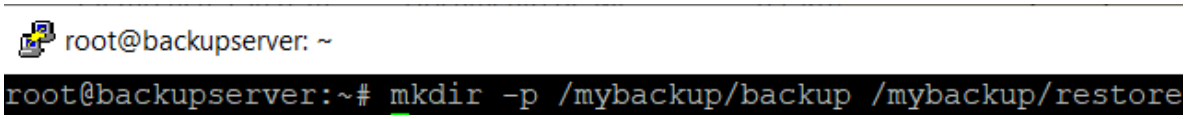
Figura 94. Confirmación de contraseña.




Fuente: Propia del autor

Ya realizado esto, se procederá a realizar las configuraciones del almacenamiento de bacula, para lo cual como primer paso, se crea un directorio para almacenar los archivos de copia de seguridad. Esto se puede crear con el siguiente comando: ***mkdir -p /mybackup/Backup /mybackup/restore***

Figura 95. Crear el directorio de almacenamiento.




Fuente: Propia del autor

A continuación, cambie la propiedad del directorio bacula al usuario de bacula y el group con el siguiente comando: ***chown -R bacula:bacula /mybackup***

Figura 96. Cambio de propiedades de directorio bacula.

```
root@backupserver:~# sudo chown -R bacula:bacula /mybackup/
```

Fuente: Propia del autor

Seguido de esto, se le asignará a la carpeta de almacenamiento permiso los archivos de este tenga permiso para todos los usuarios, esto mediante el comando: ***sudo chmod -R 700 /mybackup/***

Figura 97. Asignación de privilegios - Carpeta de almacenamiento.

```
root@backupserver:~# sudo chmod -R 700 /mybackup/
```

Fuente: Propia del autor

A continuación, se debe editar el archivo de configuración predeterminado de almacenamiento de bacula y definir el dispositivo y la ubicación del almacenamiento, eso utilizando el comando ***nano/***

Figura 98. Edición de archivo bacula-director.

```
root@backupserver:~# nano /etc/bacula/bacula-dir.conf
```

Fuente: Propia del autor

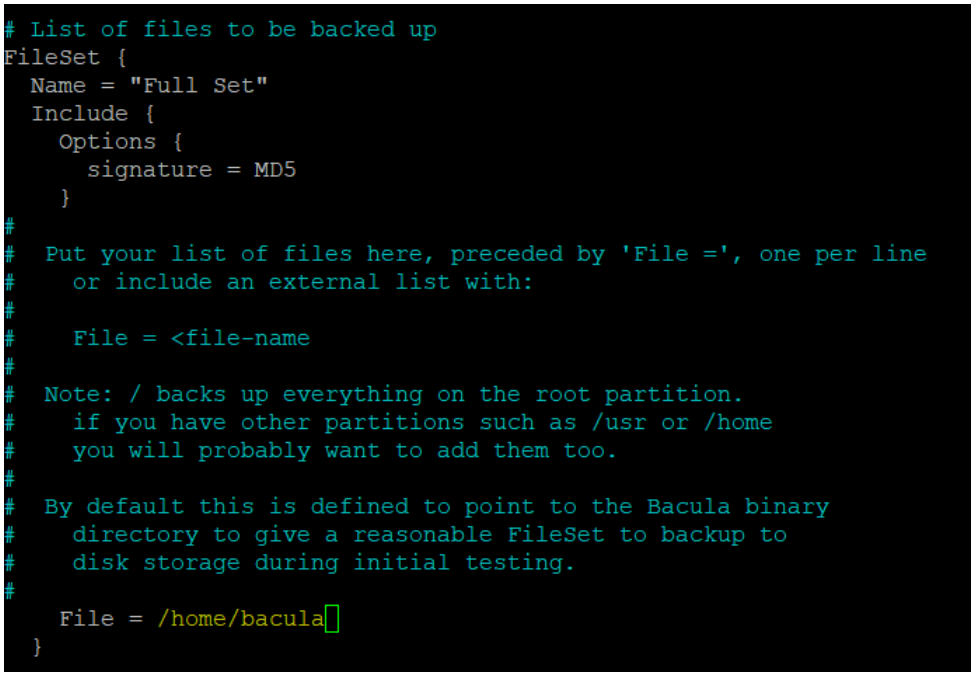
Después estando en el archivo de configuración, realizar las siguientes modificaciones dentro del archivo.

Figura 99. Modificación RestoreFiles.

```
Job {
  Name = "RestoreFiles"
  Type = Restore
  Client=backupserver-fd
  Storage = File1
# The FileSet and Pool directives are not used by Restore Jobs
# but must not be removed
  FileSet="Full Set"
  Pool = File
  Messages = Standard
  Where = /mybackup/restore
}
```

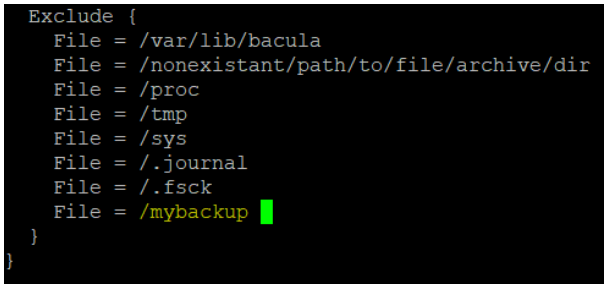
Fuente: Propia del autor

Figura 100. Modificación FileSet.




Fuente: Propia del autor

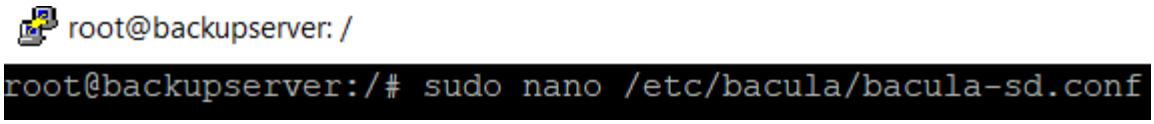
Figura 101. Modificación Exclude.




Fuente: Propia del autor

Todas las modificaciones presentes anteriormente están relacionadas directamente a el directorio principal donde esta alojada el espacio creado para el acoplamiento. Seguido de esto se procederá a realizar la siguiente modificación sobre el Daemon sd de Bacula

Figura 102. Configuración del Daemon de Bacula.




Fuente: Propia del autor

Figura 103. Modificación del archivo.

```
Device {
  Name = FileChgr1-Dev1
  Media Type = File1
  Archive Device = /mybackup/backup
  LabelMedia = yes;                   # lets Bacula label unlabeled media
  Random Access = Yes;
  AutomaticMount = yes;               # when device opened, read it
  RemovableMedia = no;
  AlwaysOpen = no;
  Maximum Concurrent Jobs = 5
}
```

Fuente: Propia del autor

Seguido de realizar los cambios pertinentes tanto en director como en el daemon, se procede a realizar la verificación de la configuración, para validar que los archivos están configurados correctamente, esto mediante las siguientes líneas de comando mostradas a continuación. Cabe recalcar, si al ejecutar esto y se presenta un error, significa que hubo un fallo al momento de modificar los archivos antes mencionados.

Figura 104. Validación de configuración de bacula-dir.

```
root@backupserver:/home/bacula# bacula-dir -tc /etc/bacula/bacula-dir.conf
```

Fuente: Propia del autor

Figura 105. Validación de configuración de bacula-sd.

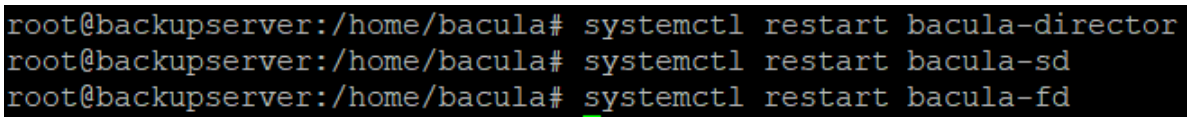
```
root@backupserver:/home/bacula# bacula-sd -tc /etc/bacula/bacula-sd.conf
```

Fuente: Propia del autor

Ya realizada la verificación se procede a reiniciar el cliente de Backup (bacula-fd), el daemon (bacula-sd) y el supervisor de los backups (bacula-dir), esto mediante los siguientes comandos.

- Systemctl restart bacula-director
- Systemctl restart bacula-sd
- Systemctl restart bacula-fd

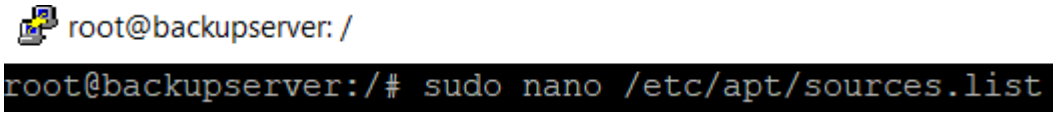
Figura 106. Comandos para reiniciar los servicios de bacula.




Fuente: Propia del autor

Ya realizado todo el proceso de configuración de los actuantes de bacula, se procede a realizar la instalación de WEBMIN para gestionar bacula de manera gráfica y amigable. Se debe tener en cuenta que la instalación directa no es posible pues que los repositorios de Ubuntu no cuentan con los archivos necesarios para instalar el aplicativo. Para solventar esto el primer paso que se debe realizar es ingresar el siguiente archivo de configuración con el comando ***sudo nano /etc/apt/source.list***.

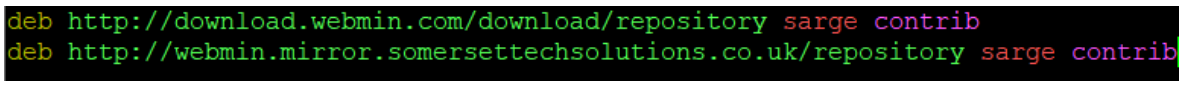
Figura 107. Configuración repositorio sourse.




Fuente: Propia del autor

Ya ubicados en el interior del archivo, se le agrega en la parte final de éste, las siguientes líneas de comando:

Figura 108. Agregar Librería para descargar WEBADMIN.



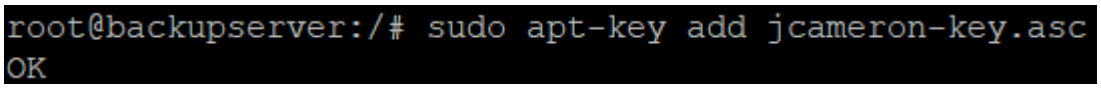

Fuente: Propia del autor

Después de realizar lo anterior, se procede a descargar y agregar la clave PGP de Webmin para que su sistema confíe en el nuevo repositorio, esto mediante el comando ***wget http://www.webmin.com/jcameron-key.asc*** para descargarla y ***sudo apt-key add jcameron-key.asc*** para agregarla.

Figura 109. Confirmación de descarga de clave.


Fuente: Propia del autor

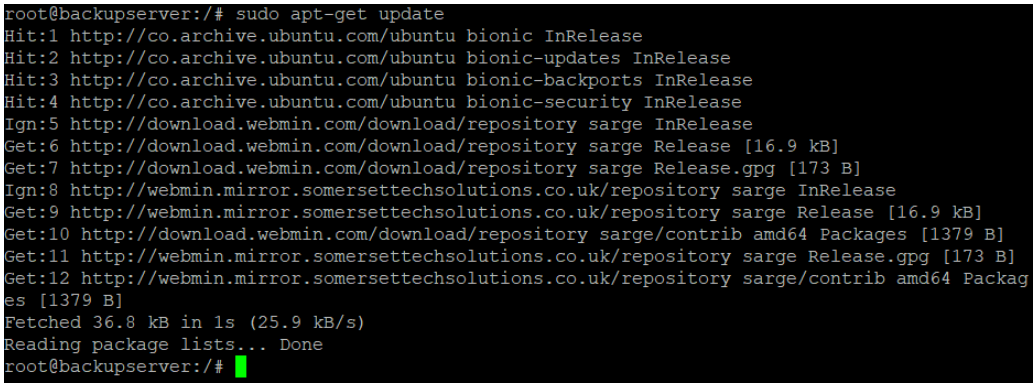
Figura 110. Agregar la clave.




Fuente: Propia del autor

Luego de realizar la adición de la clave, se procede a realizar la actualización del repositorio con la nueva adición de WEBMIN utilizando el comando ***sudo apt-get update***

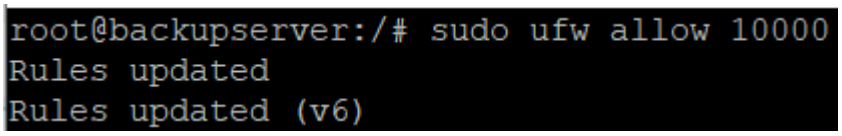
Figura 111. Actualización del repositorio.




Fuente: Propia del autor

Observando en la Figura anterior, los repositorios de WEBMIN están disponibles para descargar, se procede a realizar la instalación de WEBMIN con el comando ***apt-get install webmin*** y seguido de esto se abrirá un puerto en el firewall para que el puerto 10000 pueda ser utilizado externamente sin ningún problema mediante el comando ***sudo ufw allow 10000***.

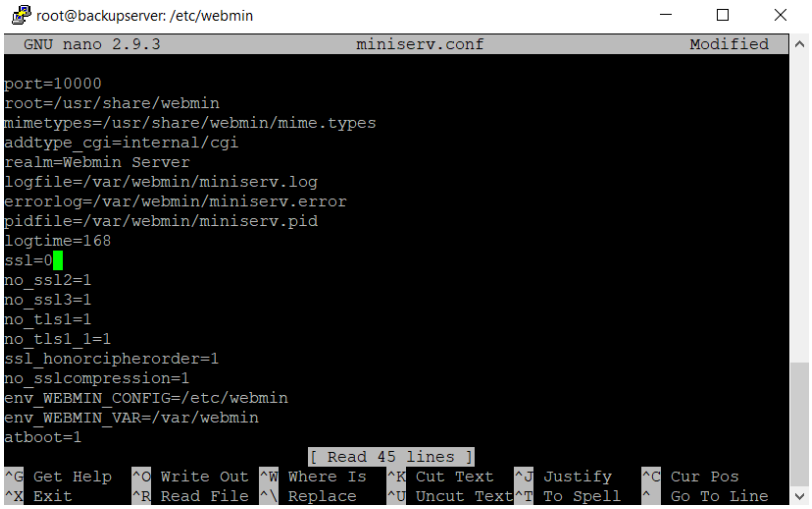
Figura 112. Validación de puerto WEBMIN en firewall.




Fuente: Propia del autor

En muchas ocasiones se presenta que el WEBMIN inicia en modo consola por lo cual iniciarlo por el navegador se dificulta, para solventar esta necesidad, se procede a realizar la siguiente configuración en el siguiente archivo ***sudo nano /etc/webmin/miniserv.conf*** en el cual se cambiará la opción SSL de 1 a 0 y se guardarán los cambios.

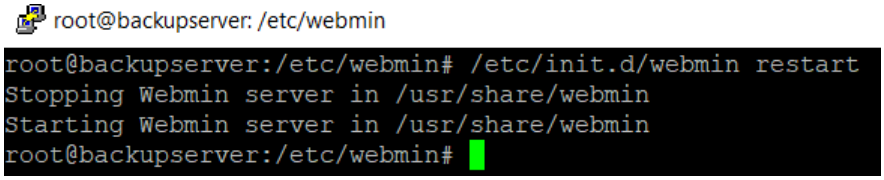
Figura 113. Habilitar modo navegador en WEBMIN.




Fuente: Propia del autor

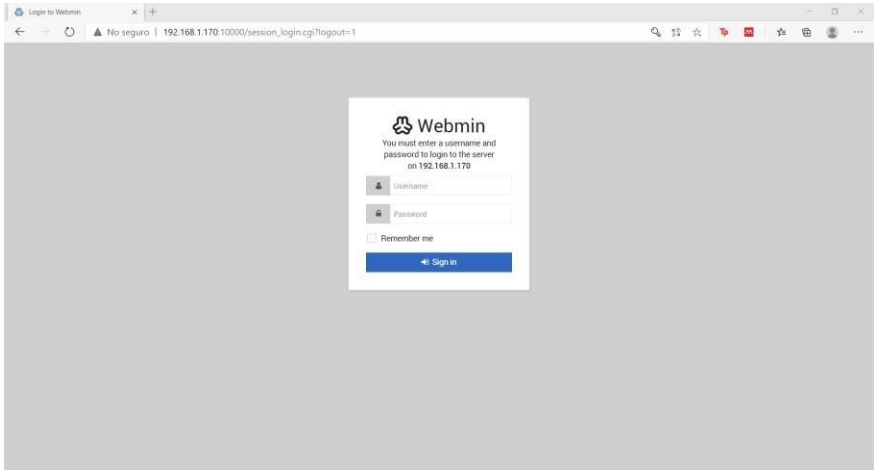
Como último paso se reiniciará el WEBMIN y se procede a acceder al servidor por medio de la ip asignada + : + 10000 en este caso práctico ***192.168.1.1870:10000***.

Figura 114. Reinicio del servicio WEBMIN.



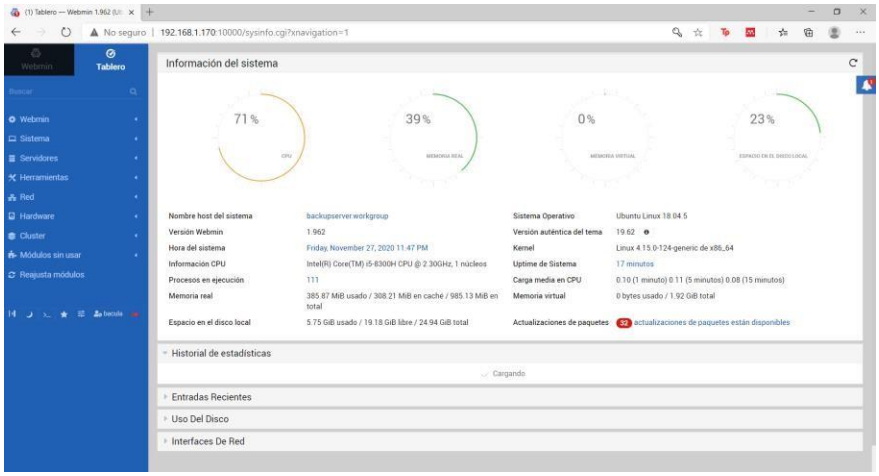

Fuente: Propia del autor

Figura 115. Navegando con Bacula.




Fuente: Propia del autor

Figura 116. Pantalla de inicio de Bacula.

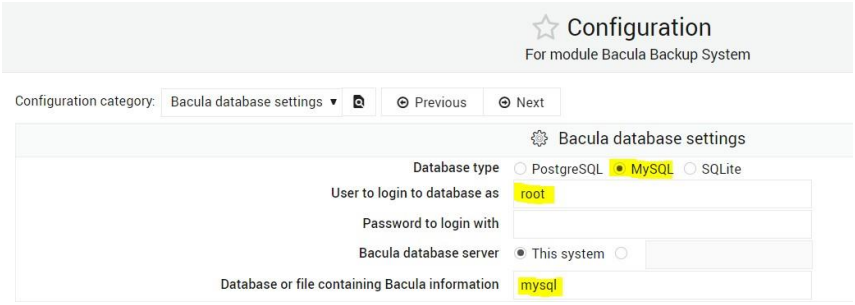



Fuente: Propia del autor

**Nota:** El inicio de sesión al servidor en WEBMIN es el mismo del servidor original.

La configuración por defecto de Bacula en WEBMIN no está configurada adecuadamente, por lo cual se debe dirigirse a la opción ***System***, seguido ingresar a la opción ***Bacula Backup System*** e ingresar en la opción module configuration, el cual desplegará un banner como el que se encuentra a continuación:

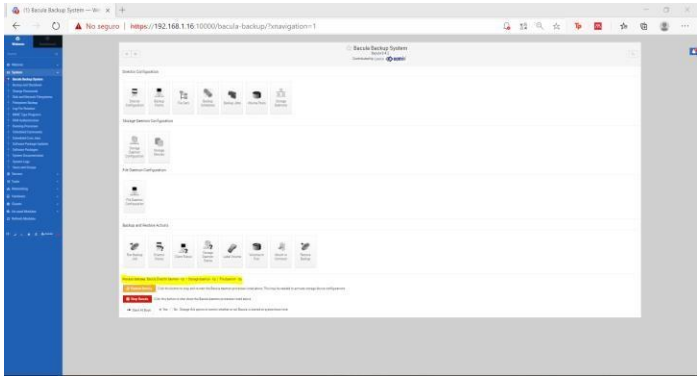
Figura 117. Configuración Webmin almacenamiento.




Fuente: Propia del autor

En este banner se debe escoger la opción ***Bacula database settings*** y seleccionar la opción ***MySQL***, en el apartado User to login to dabatase as, se colocará el usuario ***root*** y en la contraseña se procede a colocar la asignada a MySQL en el proceso de MySQL Secure, en este caso ***bacula*** y esto permitirá el acceso exitoso como se presenta a continuación.

Figura 118. Bacula en ejecución.



Fuente: Propio del autor.

## 6.6. CONEXIÓN ENTRE SERVIDORES

6.6.1. Agregar servidores de correlacionador de eventos (GLPI) y Backup (BACULA) a servidor de monitoreo NAGIOS. Este apartado presenta el proceso de agregación de los servidores de correlacionador de eventos y Backup al servidor de monitoreo NAGIOS, esto, con la finalidad de monitorizar los servidores propuestos en un ambiente controlado.

Para cumplir con el objetivo anterior, primeramente se tiene que ingresar a ruta de los objetos de NAGIOS, donde se almacenan los archivos cfg (configuración de hots) con las reglas de aplicación de la identificación de los servicios y máquina monitorizadas por el servidor de monitoreo. Esto mediante el comando ***Sudo cd /usr/local/nagios/etc/objects***.

Ya ubicados en el siguiente directorio, se procede a crear el archivo que contendrá los nuevos hosts a agregar en el servidor, en este caso el servidor GLPI y el servidor Bacula. Lo anterior, utilizando el comando ***sudo nano linux.cfg***.

Siguiendo el proceso de agregación, en el archivo nuevo creado para la agregación de lo host, se deben colocar las siguientes datos necesaria para cada uno de los servidores a agregar:

```
#################################################
#
#       SERVIDOR CORRELACIONADOR DE EVENTOS
#
#################################################

define host{
   use                     linux-server
   host_name               servidor_correlaeventos
   alias             Servidor de Monitoreo
   check_interval 1
   address           192.168.1.160
}
```

```
    ###############################################
    #
    #           SERVICIOS DE SERVIDOR DE
    #
    ###############################################

    define service{
      use                     generic-service
      host_name               servidor_correlaeventos
      service_description     Disco Duro
      check_interval 1
      check_command           check_local_disk!-w10%-c5%-p/
    }

    define service{
      use                     generic-service
      host_name               servidor_correlaeventos
      service_description     SSH
      check_interval 1
      check_command           check_ssh![-4|-6][-t <10>] [-r <OpenSSH 7.6p1>] [-p
<port>] <192.168.1.160>
    }

    define service{
      use                     generic-service
      host_name               servidor_correlaeventos
      service_description     Carga
      check_interval 1
      check_command           check_local_load!-w 5.0,4.0,3.0 -c 10.0,6.0,4.0
    }

    define service{
      use                     generic-service
      host_name               servidor_correlaeventos
      service_description     Swap
      check_interval 1
      check_command           check_local_swap!20!10
    }

    define service{
      use                     generic-service
      host_name               servidor_correlaeventos
      service_description     Ping
      check_interval 1
```

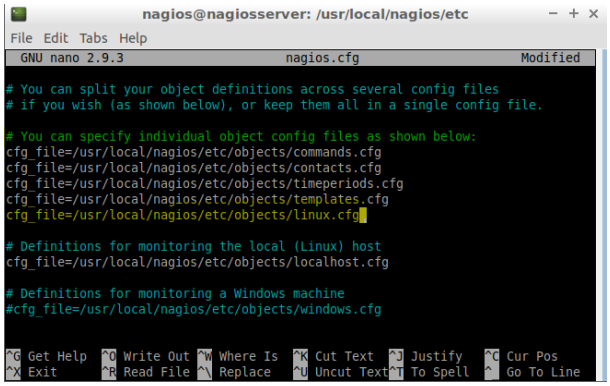
```
  check_command      check_ping!500.0,20%!800.0,60%
}

define service{
  use                    generic-service
  host_name              servidor_correlaeventos
  service_description    SSH
  check_interval 1
  check_command      check_ssh!500.0,20%!800.0,60%
}

########################################################
#
#                SERVIDOR DE BACKUP
#
########################################################

define host{
  use                    linux-server
  host_name              servidor_backup
  alias              Servidor de Backup
  check_interval 1
  address        192.168.1.170
}

########################################################
#
#           SERVICIOS HOST 2
#
########################################################

define service{
  use                    generic-service
  host_name              servidor_backup
  service_description    Disco duro
  check_interval 1
  check_command      check_local_disk!-w10%-c5%-p/
}

define service{
  use                    generic-service
  host_name              servidor_backup
  service_description    Ping
  check_interval 1
  check_command      check_ping!500.0,20%!800.0,60%
```

```
}

define service{
  use                   generic-service
  host_name             servidor_backup
  service_description   SSH
  check_interval 1
  check_command         check_ssh!check_ssh![-4|-6][-t <10>] [-r <OpenSSH
8.2p1>] [-p <22>] <192.168.1.170>
}

define service{
  use                   generic-service
  host_name             servidor_backup
  service_description   Swap
  check_interval 1
  check_command         check_local_swap!20!10
}

define service{
  use                   generic-service
  host_name             servidor_backup
  service_description   Carga
  check_interval 1
  check_command         check_local_load!-w 5.0,4.0,3.0 -c 10.0,6.0,4.0
}
```

Despues de diligenciar toda la información antes mencionada se procede a guardar los cambios y cerrar el modo editable. Ahora bien, estos nuevos servidores con sus servicios fueron agregados pero nagios aún no los reconoce como equipo, por lo cual se debe ingresar al siguiente directorio ***/usr/local/nagios/etc*** y realizar la edición del archivo ***nagios.cfg***.

Abierta la consola nano de moficiación, se procede a agregar la siguiente línea en el apartado ***#You can specify individual config files as show below:***

Figura 119. Agregar nuevos hosts a archivo nagios.cfg.




Fuente: Propia del autor

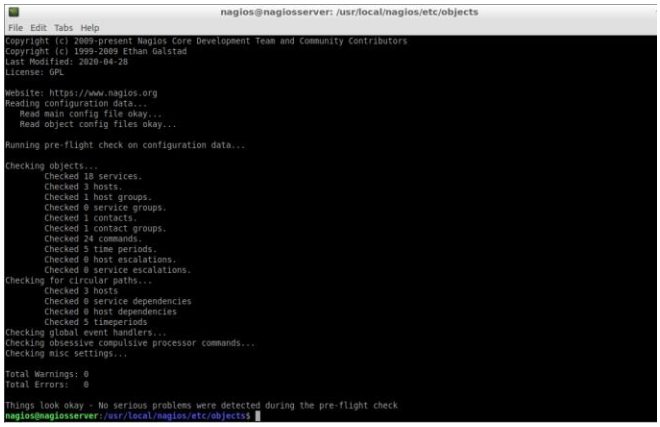
Luego de esto, se guardan los cambios y se procede a digitar el comando de verificación de configuración de nagios para validar que no se presente ningun error. Para esto se digita el siguiente comando como se muestra en esta Figura.

Figura 120. Comando de verificación de configuración - Nagios.


Fuente: Propia del auto

Ejecutado el comando de verificación, el resultado adecuado para la configuración nueva de nagios será el siguiente:

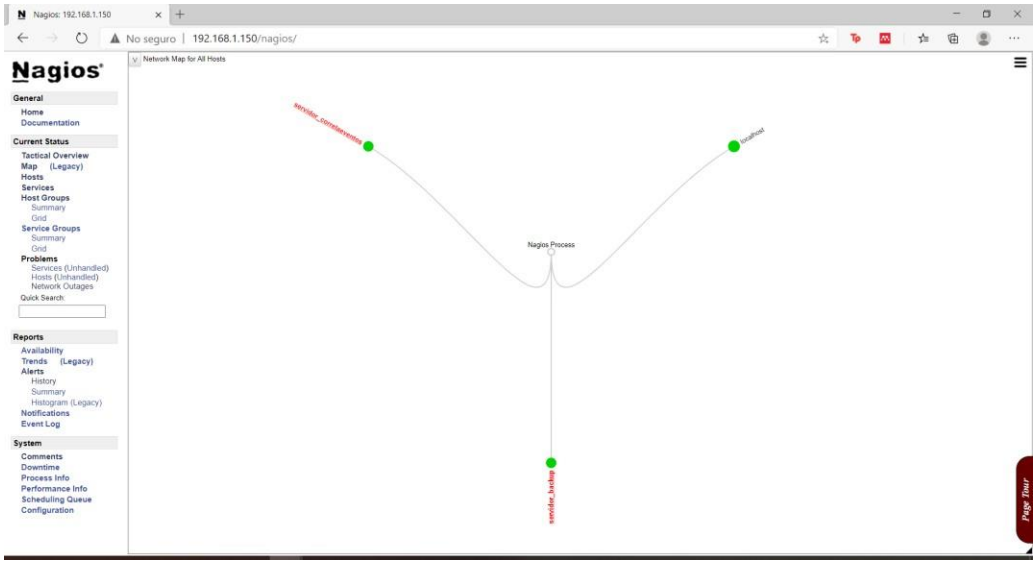
Figura 121. Validación de OK de configuración.




Fuente: Propia del autor

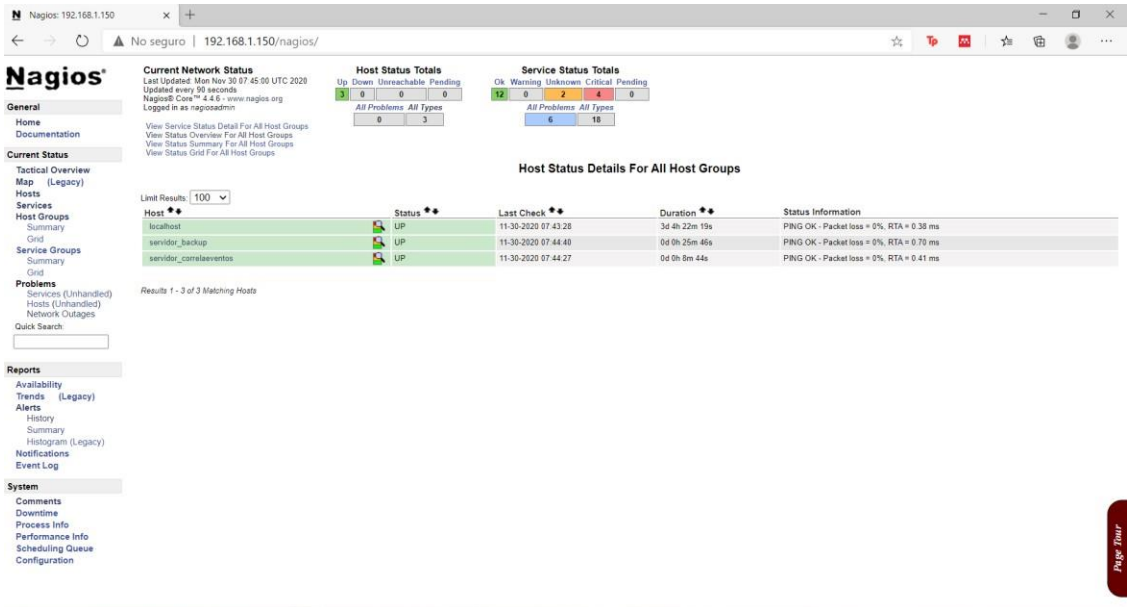
Al realizar los pasos ejecutados anteriormente, y validando el archivo de configuración de NAGIOS con éxito, lo siguiente será reiniciar el servidor nagios con el comando ***systemctl restart nagios*** y luego validar en el navegador si efectivamente se hizo efectivo la adición de los servidores esperados a el NAGIOS.

Figura 122. Mapa de enlace de servidores.



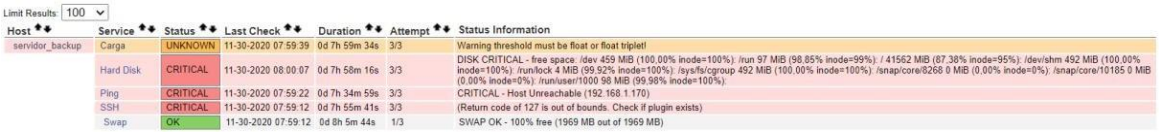

Fuente: Propia del autor

Figura 123. Validación de adición de nuevos host - Nagios.




Fuente: Propia del autor

Figura 124. Validación de servicios analizados.



Limit Results: 100

| Host | Service | Status | Last Check | Duration | Attempt | Status Information |
|---|---|---|---|---|---|---|
| servidor_backup | Carga | UNKNOWN | 11-30-2020 07:59:39 | 0d 7h 59m 34s | 3/3 | Warning threshold must be float or float triplet! |
| | Hard Disk | CRITICAL | 11-30-2020 08:00:07 | 0d 7h 58m 16s | 3/3 | DISK CRITICAL - free space: /dev 459 MiB (100,00% inode=100%): /run 97 MiB (98,85% inode=99%): / 41562 MiB (87,38% inode=95%): /dev/shm 492 MiB (100,00% inode=100%): /run/lock 4 MiB (99,92% inode=100%): /sys/fs/cgroup 492 MiB (100,00% inode=100%): /snap/core/8268 0 MiB (0,00% inode=0%): /snap/core/10185 0 MiB (0,00% inode=0%): /run/user/1000 98 MiB (99,98% inode=100%): |
| | Ping | CRITICAL | 11-30-2020 07:59:22 | 0d 7h 34m 59s | 3/3 | CRITICAL - Host Unreachable (192.168.1.170) |
| | SSH | CRITICAL | 11-30-2020 07:59:12 | 0d 7h 55m 41s | 3/3 | (Return code of 127 is out of bounds. Check if plugin exists) |
| | Swap | OK | 11-30-2020 07:59:12 | 0d 8h 5m 44s | 1/3 | SWAP OK - 100% free (1969 MB out of 1969 MB) |

Fuente: Propia del autor

En los resultados mostrados anteriormente, se evidencia la adecuada adición de los servidores de correlacionador de eventos y backup a Nagios.

En la Figura de validación de servicios aparecen en critical puesto que la máquina esta apagada y los servicios que se encuentran en estado critical necesitan que la máquina este encendida.

6.6.2. Agregar servidores de correlacionador de eventos (GLPI) y monitoreo (NAGIOS) a servidor de Backup BACULA. El desarrollo de este apartado, permitirá realizar la instalación de los clientes de bacula para poder realizarles posteriormente los respectivos backups. En este laboratorio en particular se utilizaron servidores montados en Ubuntu Server 18.04 y para lo cual se presentan las siguientes configuraciones.

El primer paso por realizar es instalar la herramienta para gestión de firewalls firewalld, ésta se instala mediante el uso del comando sudo apt-get install firewalld. Seguido de estos se proceden habilitar los puertos en el cliente por donde escucha el aplicativo bacula en función de su cliente, su esclavo y la consola, utilizando los comandos mostrados a continuación:

Figura 125. Reglas de firewalld.

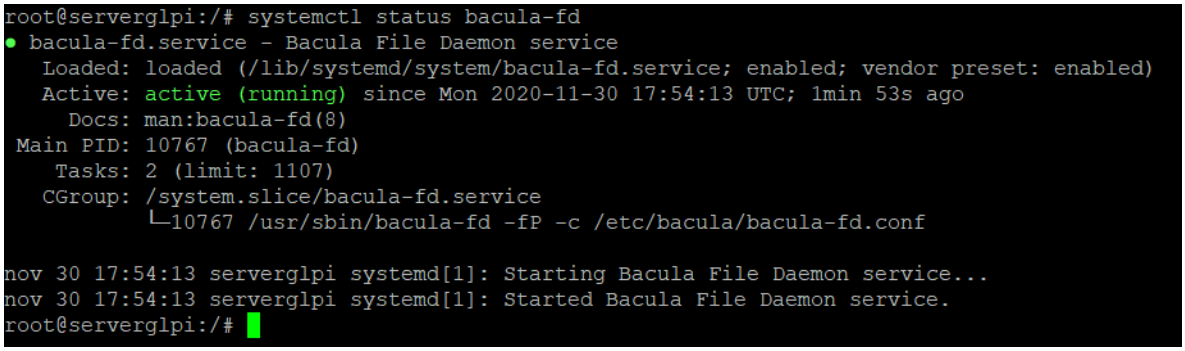
```
bacula@backupserver:~$ sudo firewall-cmd --add-port=9102/tcp --permanent
success
bacula@backupserver:~$ sudo firewall-cmd --add-port=9103/tcp --permanent
success
bacula@backupserver:~$ sudo firewall-cmd --add-port=9101/tcp --permanent
success
bacula@backupserver:~$ sudo firewall-cmd --reload
success
```

Fuente: Propia del autor.

Ya aplicadas las reglas, se procede a reiniciar el servidor con el comando sudo shutdown now -r.

Siguiendo con el proceso de configuración, ahora se procede realizar la instalación del cliente de bacula, por medio del cual se realizará la conexión con el servidor de Backup. Esto por medio del comando sudo apt-get install bacula-client. Para finalizar se valida el estado del nuevo servicio instalado con el comando sudo systemctl status bacula-fd, sobre el cual se obtendrá como resultado lo siguiente que se muestra en la Figura:

Figura 126. Validación de estado de cliente bacula.

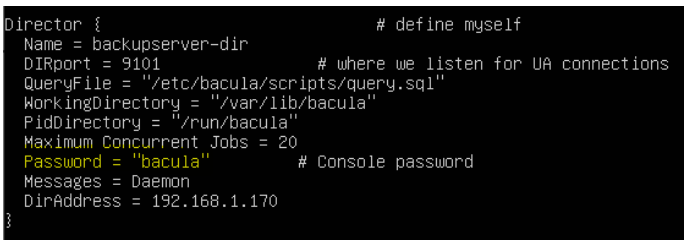



Fuente: Propia del autor.

Después de realizar todos los procesos mencionados anteriormente, se debe ingresar al servidor al siguiente archivo del servidor y realizar las siguientes modificaciones con el comando ***sudo nano /etc/bacula/bacula-dir.conf***.

1. Realizar el cambio de TODAS las contraseñas en los archivos bacula-dir.conf, bacula-sd.conf, bacula-fd.conf y bconsole.conf por la contraseña “bacula”, como se muestra a continuación.

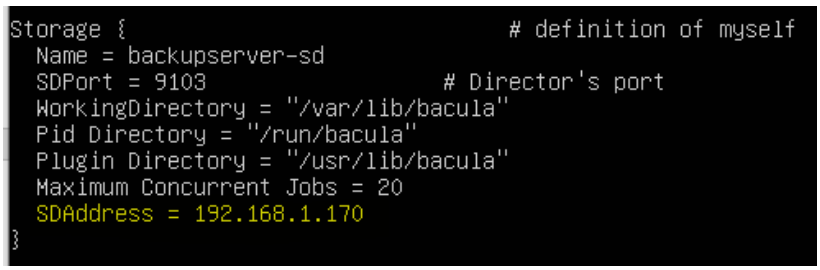
Figura 127. Asignación de nueva contraseña de acceso.




Fuente: Propia del autor.

2. Seguido de ésto realizar el cambio de IP de identificación a los siguientes archivos del servidor por la IP de este (192.168.1.170) sudo nano ***/etc/bacula/bacula-dir.conf***.

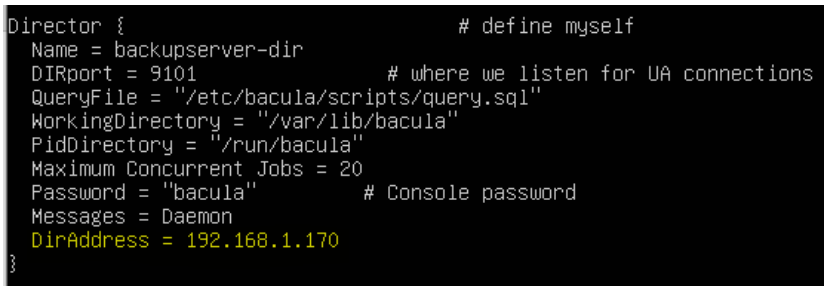
Figura 128. Cambio IP - bacula-dir.conf




Fuente: Propia del autor.

*sudo nano /etc/bacula/bacula-ds.conf*

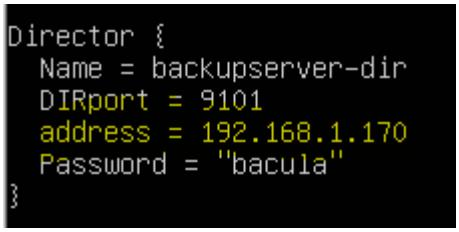
Figura 129. Figura 123. Cambio IP - bacula-sd.conf




Fuente: Propia del autor.

*sudo nano /etc/bacula/bconsole.conf*

Figura 130. Figura 123. Cambio IP - bconsole.conf




Fuente: Propia del autor

Seguido de ésto realizar el cambio de IP de identificación a los siguientes archivos del servidor por la IP de este (192.168.1.170) ***sudo nano /etc/bacula/bacula-dir.conf***

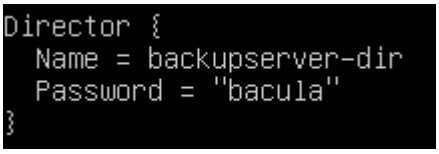
Ya realizado la anterior, se reinician los servicios y el servidor con los comandos y se reinicia el servidor:

- ***/etc/init.d/bacula-director restart***
- ***/etc/init.d/bacula-fd restart***
- ***/etc/init.d/bacula-sd restart***
- ***sudo shutdown .now -r***

Realizado lo anterior, se procede a realizar la configuración del archivo interno de cliente del servidor que se pretende enlazar con el servidor de Backup, para esto se utiliza el comando ***sudo nano /etc/bacula/bacula-fd.conf*** y se realizan las siguientes modificaciones.

1. Esta modificación permite el enlace del archivo director del servidor de Backup con el cliente que se está modificando.

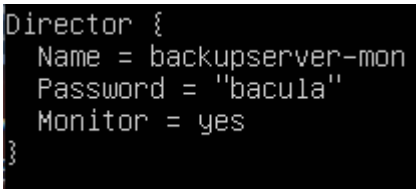
Figura 131. Enlace director - Servidor Backup.



Fuente: Propia del autor

2. Este archivo permite realizar la conexión del modo monitor del servidor con el cliente que se está modificando.

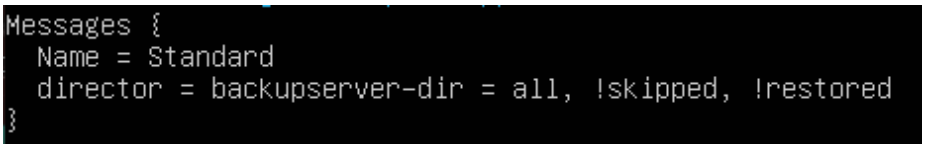
Figura 132. Enlace Monitor - Servidor Backup.




Fuente: Propia del autor

3. Este archivo permite la conexión de mensajes entre servidor y cliente.

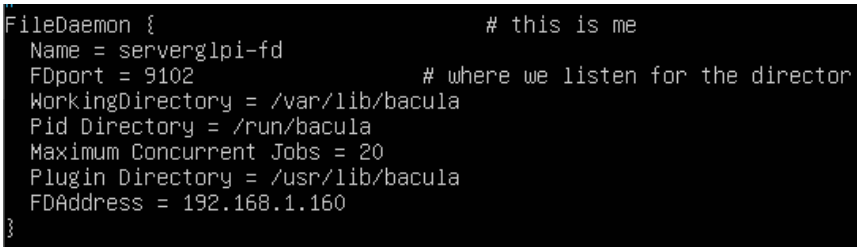
Figura 133. Enlace mensajes - Servidor Backup.




Fuente: Propia del autor

4. Este es el archivo identificador del demonio (cliente a modificar).

Figura 134. Identificador cliente.




Fuente: Propia del autor

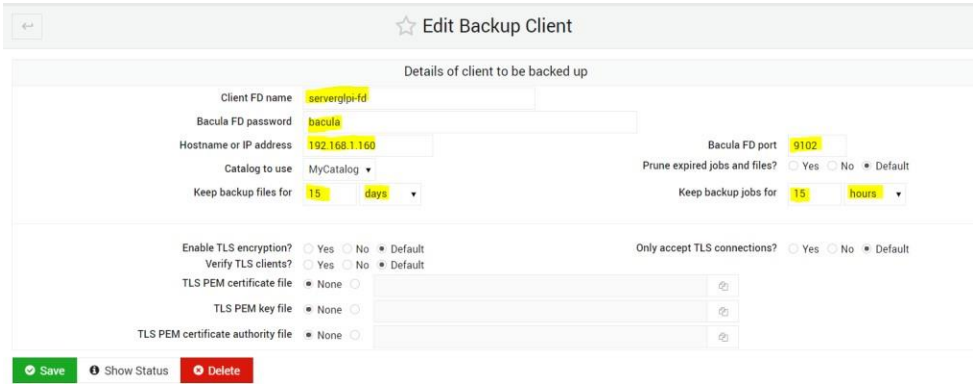
Después de realizado todos los pasos anteriores, se procede a realizar el reinicio del servidor y queda efectuada la configuración adecuada del cliente bacula para ser conocida y tener conexión entre cliente y servidor de Backup.

6.6.3. Creación de un Backup con Bacula. Ya realizado el proceso de enlace entre servidor y cliente bacula mostrado en el apartado anterior, ahora se mostrará el procedimiento de generación de copias de seguridad. Para esto se accede al WEBMIN de gestión de Bacula (192.168.1.170) y se siguen los siguientes pasos:

1. ***Creación del usuario.***

Para esta fase se accede a la parte izquierda del panel de bacula y se selecciona ***system -> Bacula Backup System***. Luego de esto se selecciona la opción ***Backup client*** *y* ***add a new backup client***. Se llenan los datos de la siguiente forma:

Figura 135. Creación de cliente en servidor bacula.




Fuente: Propia del autor.

Los datos marcados a continuación tienen el siguiente significado:

- **Cliente FD name:** Nombre del cliente encontrado en el archivo del cliente usando el comando Sudo nano /etc/bacula/bacula-fd.conf (Sección FileDaemon)
- **Bacula FD password:** Contraseña asignada en la configuración general de las contraseñas (bacula.)
- **Hostname or IP Address:** Ip del servidor cliente.

- **Bacula FD port:** 9102.

Despues de realizados los pasos mencionados, se procede a revisar el estado de conexión del cliente, para lo cual antes de presionar el boton save, se presiona ***show status*** para lo cual se debe presentar un resultado como el siguiente.

Figura 136. Creación de file name.

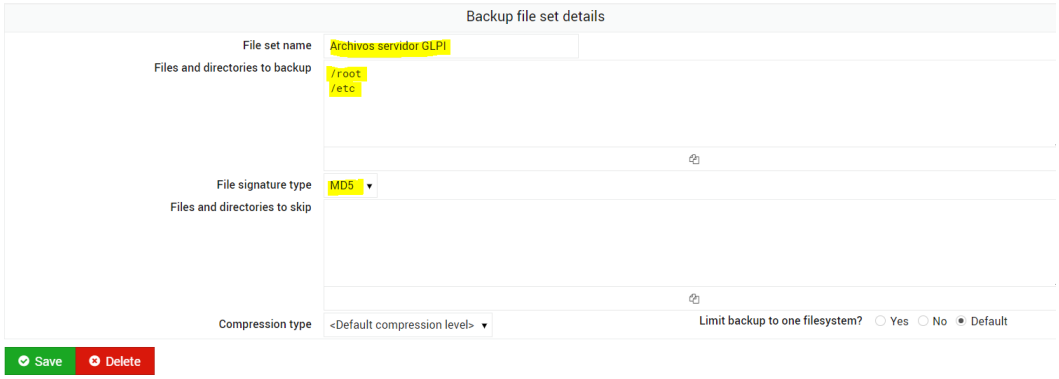

Fuente: Propia del autor.

Seguido de ésto se reinicia el servidor por medio del entorno gráfico.
**Nota:** No olvidar reiniciar el servidor al terminar de crear al usuario.

## 2. *Creación de lo que se va a respaldar.*

Para esta fase se accede a la parte izquierda del panel de bacula y se selecciona ***system -> Bacula Backup System***. Luego de ésto se selecciona la opción ***File Sets*** *y* ***add a new backup file set***. Se llenan los datos de la siguiente forma:

Figura 137. Creación dl file set.




Fuente: Propia del autor.

Los datos marcados a continuación tienen el siguiente significado:

- **File set name:** El nombre del file set que se creara.
- **File and directories to backup:** las rutas que se van a respaldar del cliente.
- **File signature type:** MD5.

Despues de realizados los pasos mencionados, se procede a guardar los cambios y se reinicia el servidor por medio del entorno gráfico.

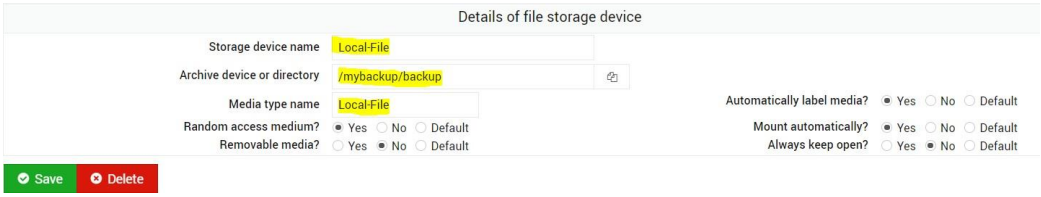
**Nota:** No olvidar reiniciar el servidor al terminar de crear el file set.

A continuación de lo anteior, se procede a crear los archivos de **almacenamiento del servidor de backup**.

### *3. Creación del storage device*

Para esta fase se accede a la parte izquierda del panel de bacula y se selecciona ***system -> Bacula Backup System***. Luego de esto se selecciona la opción ***Storage device*** *y* ***add a new storage device*** se llenan los datos de la siguiente forma:

Figura 138. Creación del Storage device




Fuente: Propia del autor.

Los datos marcados a continuación tienen el siguiente significado:

- **Storage device name:** El nombre del almacenamiento.
- **Archive device or directory:** Lugar donde se van a guardar los backups.
- **Media type name:** Local-File.

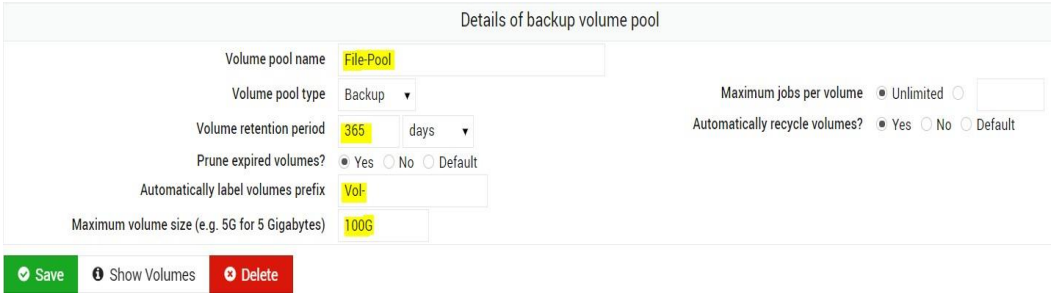
Despues de realizados los pasos mencionados, se procede a guardar los cambios y se reinicia el servidor por medio del entorno gráfico.

**Nota:** No olvidar reiniciar el servidor al terminar de crear el storage device.

### *4. Creación del volumen pool*

Para esta fase se accede a la parte izquierda del panel de bacula y se selecciona ***system -> Bacula Backup System***. Luego de esto se selecciona la opción ***Volumen pool*** *y* ***add a new volumen pool*** se llenan los datos de la siguiente forma:

Figura 139. Creación del volumen pool.




Fuente: Propia del autor.

Los datos marcados a continuación tienen el siguiente significado:

- **Volumen pool name:** El nombre del pool de volumen.
- **Volumen retention period:** La retencion que tendrán lo backup.
- **Automatically label volumen prefix:** El prefijo automático que tendrán los backups al ser creados.
- **Maximun volumen size:** El tamaño máximo que tendrán las copias de seguridad.

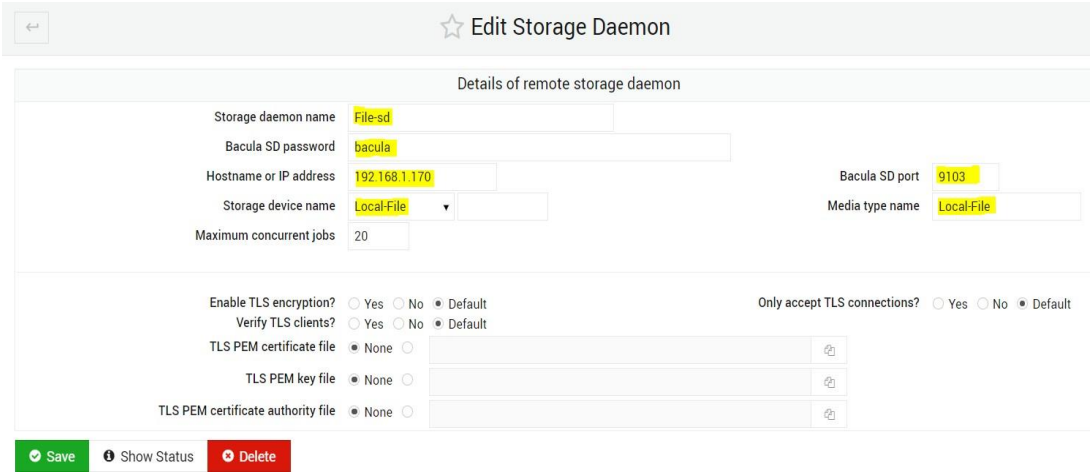
Despues de realizados los pasos mencionados, se procede a guardar los cambios y se reinicia el servidor por medio del entorno gráfico.

**Nota:** No olvidar reiniciar el servidor al terminar de crear el volumen pool.

### 5. *Creación de Storage deamon*

Para esta fase se accede a la parte izquierda del panel de bacula y se selecciona ***system -> Bacula Backup System***. Luego de esto se selecciona la opción ***Storage daemon*** *y* ***add a new storage daemon*** se llenan los datos de la siguiente forma, como se muestra en la Figura siguiente:

Figura 140. Creación del storage deamon.




Fuente: Propia del autor.

Los datos marcados a continuación tienen el siguiente significado:

- **Storage daemon name:** Nombre del daemon de comunicación.
- **Bacula SD password:** Contraseña por defecto establecida.
- **Hostname or IP address:** Ip del servidor.
- **Bacula SD port:** Puerto de escucha del daemon.
- **Storage device name:** Se selecciona el storage device que se creo para verificar que se le realizara backup.
- **Media type name:** Local-File.

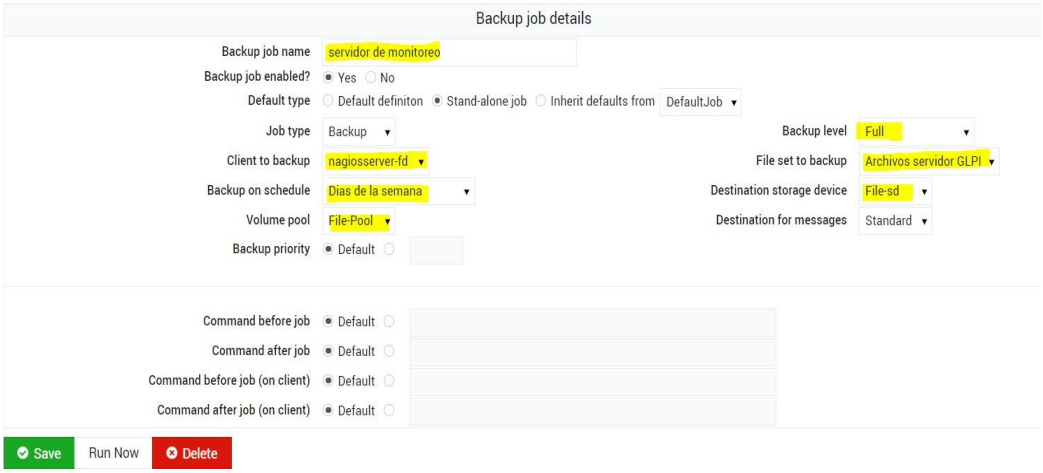
Despues de realizados los pasos mencionados, se procede a guardar los cambios y se reinicia el servidor por medio del entorno gráfico.

**Nota:** No olvidar reiniciar el servidor al terminar de crear el storage deamon.

## 6. *Creación de Backup Job*

Para esta fase se accede a la parte izquierda del panel de bacula y se selecciona ***system -> Bacula Backup System***. Luego de esto se selecciona la opción ***Backup job*** *y* ***add a new backup job*** se llenan los datos de la siguiente forma, como se muestra en la Figura:

Figura 141. Creación del Backup job.




Fuente: Propia del autor.

Los datos marcados a continuación tienen el siguiente significado:

- **Backup job name:** Nombre del job.
- **Client to backup:** Cliente a quien se le realizará el backup.
- **Backup level:** Nivel de backup a realizar.
- **File set to backup:** A que se le va a realizar backup.
- **Backup on schedule:** Como se realizará el proceso de backup en tiempo.
- **Destination storage device:** Donde se va a realizar el backup.

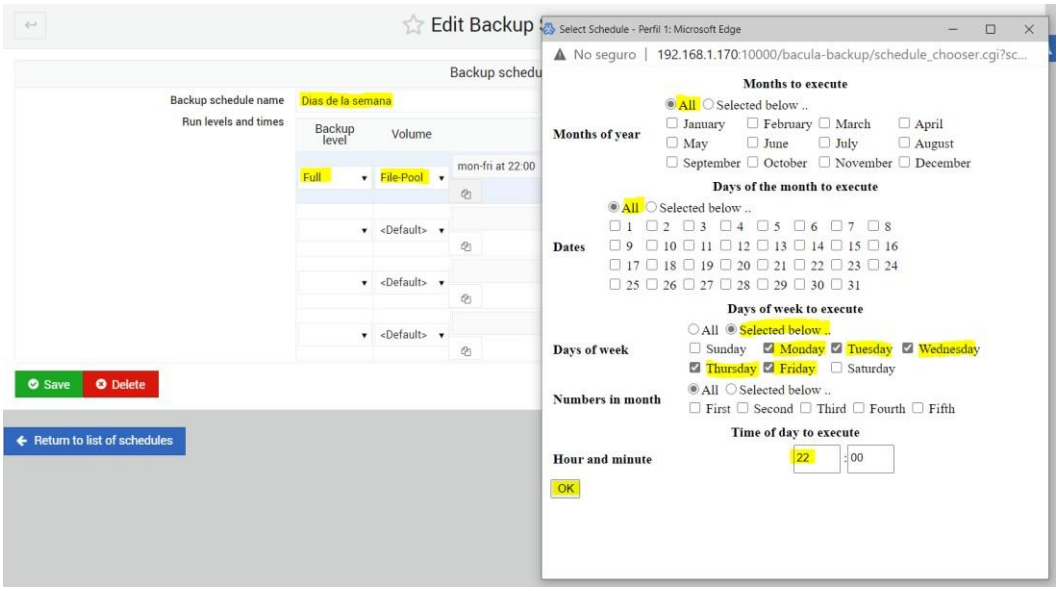
Despues de realizados los pasos mencionados, se procede a guardar los cambios y se reinicia el servidor por medio del entorno gráfico.

**Nota:** No olvidar reiniciar el servidor al terminar de crear el backup job.

## 7. *Cuando se va a arespaldar*

Para esta fase se accede a la parte izquierda del panel de bacula y se selecciona ***system -> Bacula Backup System***. Luego de esto se selecciona la opción ***Backup Schedules*** *y* ***add a new backup schedule*** se llenan los datos de la siguiente forma, como se muestra en la Figura:

Figura 142. Creación del Backup Schedule.




Fuente: Propia del autor.

Los datos marcados a continuación tienen el siguiente significado:

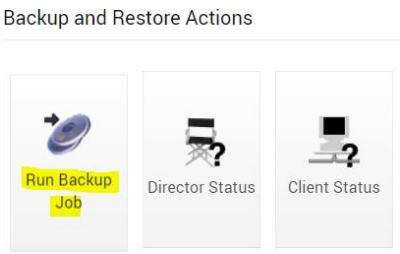
- **Backup Schedule:** El nombre.
- **Backup level:** Tipo de backup que se va a realizar.
- **Volumen:** El volumen que se va a utilizar, en este caso es el File-Pool creado.

Despues de realizados los pasos mencionados, se procede a guardar los cambios y se reinicia el servidor por medio del entorno gráfico.

**Nota:** No olvidar reiniciar el servidor al terminar de crear el backup schedules.

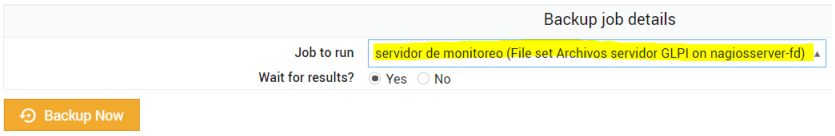
Despues de realizar el proceso anteriormente mencionado, se procede a realizar el reinicio del servidor y nuevamente se ingresa al WEBMIN para realizar el backup. Esto accediendo a la parte izquierda del panel de bacula y se selecciona ***system -> Bacula Backup System*** y luego se presiona el botón situado al final del panel ***Run Backup Job*** el cual nos permitirá seleccionar el Job a correr en base a los atributos antes creado. Se selecciona el job elegido y se procede a ejecutar el backup con el botón ***Backup Now***. El resultado positivo y el proceso se ejecución se verá a continuación en las siguientes ilustraciones.

Figura 143. Ingreso a la ejecución del backup.



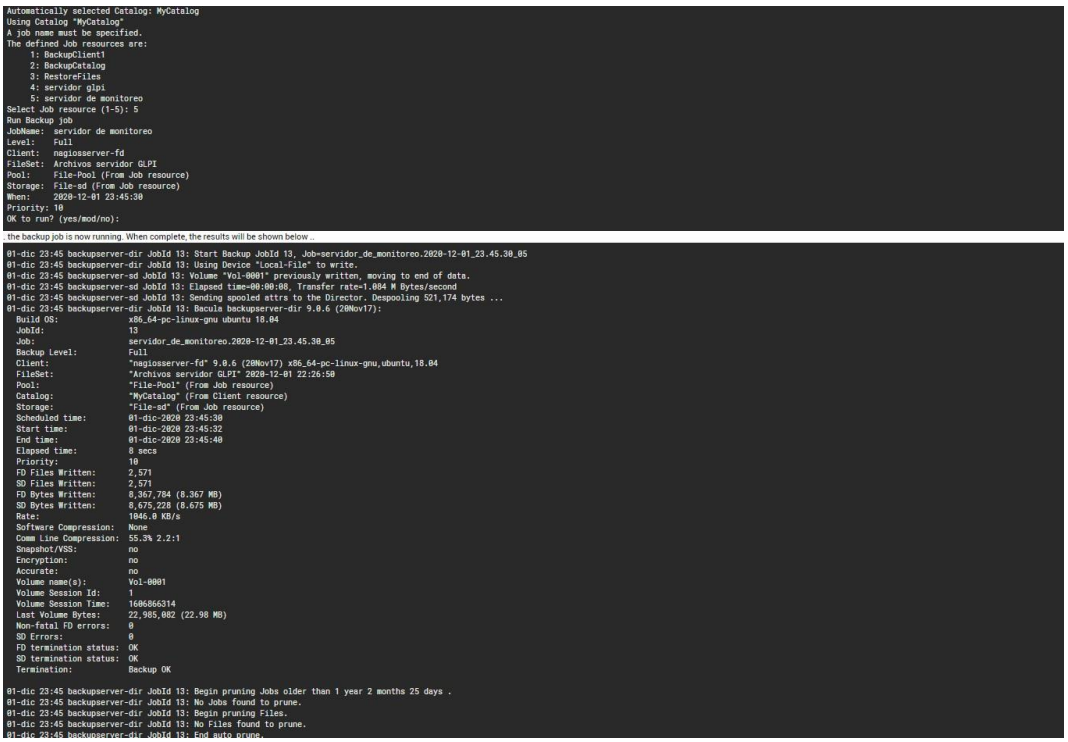

Fuente: Propia del autor.

Figura 144. Selección del job a ejecutar.




Fuente: Propia del autor.

Figura 145. Solución adecuada de la ejecución del backup.

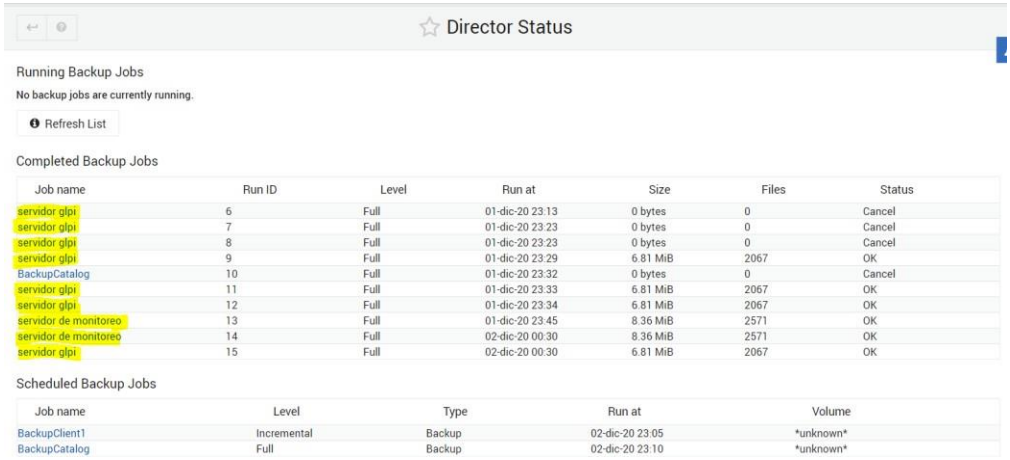



Fuente: Propia del autor.

Con los resutlados presentados en la Figura anterior, se puede evidenciar la realización correcta de un backup en un servidor BACULA.

En caso especial de que el usuario quiera verificar todos los procesos de backup que se realizarón en el sistema tanto los realizados a satisfacción como los cancelados, se debe ingresar al WEBMIN accede a la parte izquierda del panel de bacula y se selecciona ***system -> Bacula Backup System***. Seguido de esto ubicar en la parte inferior de los paneles de opciones ***Director status*** por consiguiente mostrará un resutlado general de todos los procesos realizados en el servidor (Procesos de backup), como se evidencia en la siguiente Figura.

Figura 146. Historial de backup




Fuente: Propia del autor.

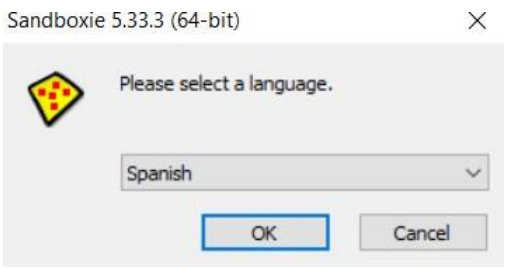
## 6.7. SERVICIO SANBOXIE.

6.7.1. Manual de instalación del servicio Sanboxie. Este apartado presenta el proceso de instalación del aplicativo Sanboxie para ejecutar aplicaciones seguras en entorno Windows. Para esto el primer paso a realizar es Dirigirse a la página de Sanboxie y descargar el aplicativo. Ya descargado este se procede a seguir los siguientes pasos de instalación.

**Link de descargar:** https://secure2.sophos.com/en-us/pages/downloadredirect.aspx?downloadKey=%7B47BAB8DC-BB6C-4D23-AD62-FC30C6796636%7D

### *1. Selección del idioma del aplicativo.*

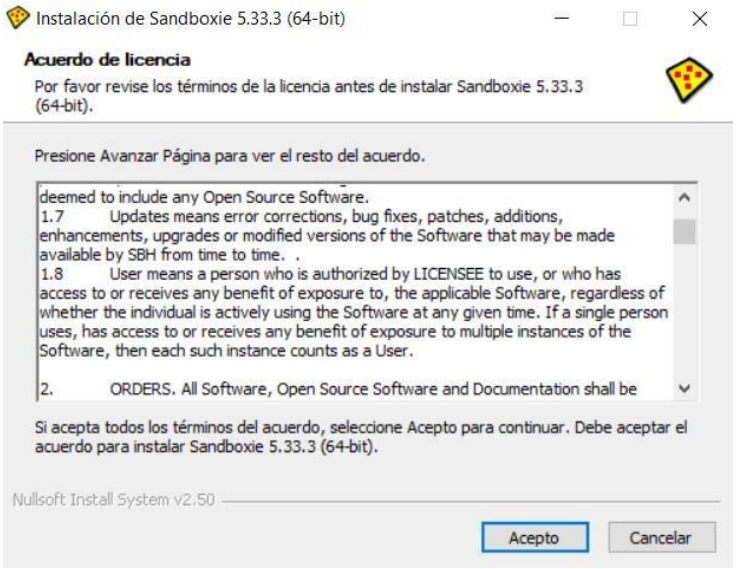
Figura 147. Lenguaje Sanboxie.



Fuente: Propia del autor.

## 2. *Aceptación de licencia del programa.*

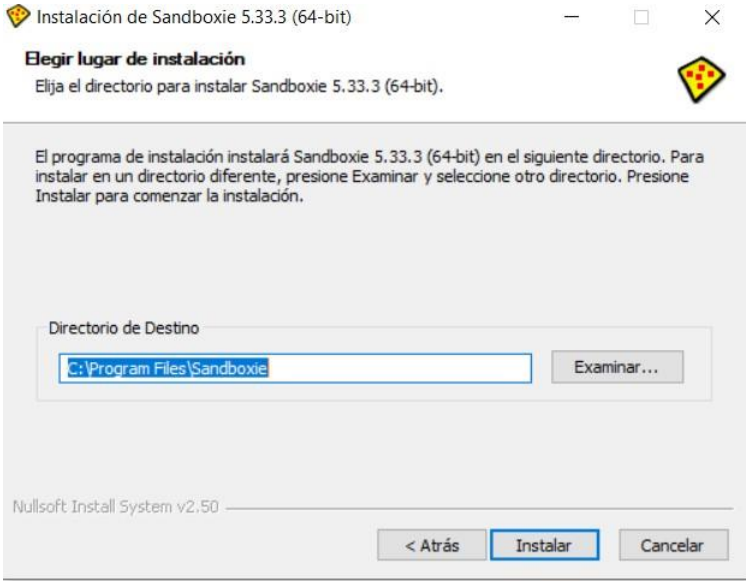
Figura 148. Licencia Sanboxie.




Fuente: Propia del autor.

## 3. *Selección de la ubicación del programa.*

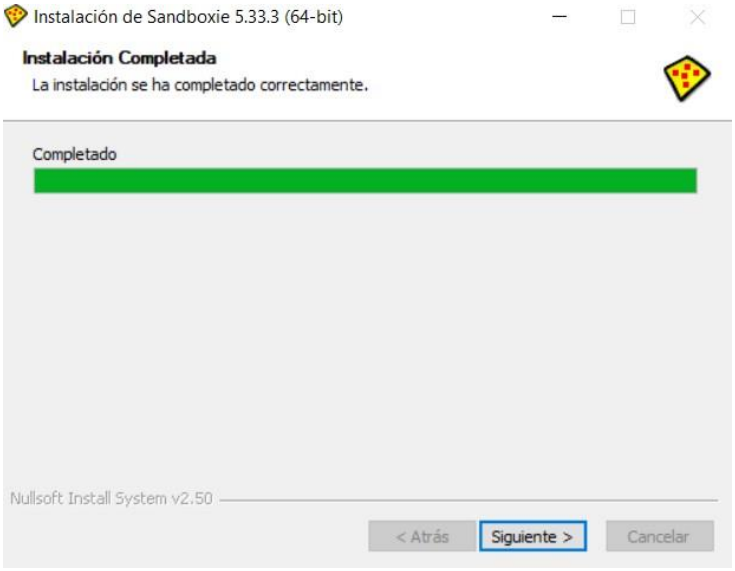
Figura 149. Carpeta Raíz Sanboxie.




Fuente: Propia del autor.

## 4. *Finalización de instalación*

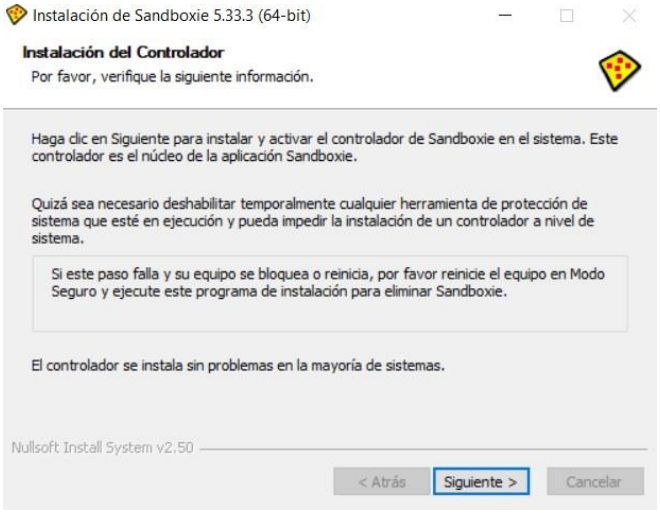
Figura 150. Finalización de instalación.




Fuente: Propia del autor.

## 5. *Solicitud de instalación de controladores.*

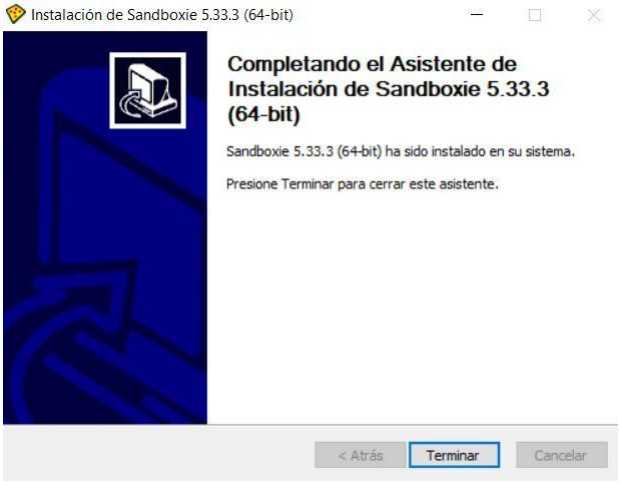
Figura 151. Instalación controladores Sanboxie.




Fuente: Propia del autor.

## 6. *Instalación completada.*

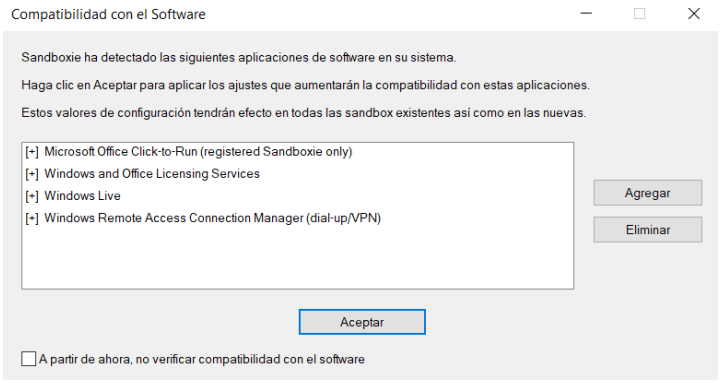
Figura 152. Instalación exitosa.




Fuente: Propia del autor.

## 7. *Detección de compatibilidad de programas con Sandboxie.*

Figura 153. Compatibilidad Sanboxie.




Fuente: Propia del autor.

**Nota:** Esta pantalla de compatibilidad es un identificador de programas que tiene la función de relacionar sus funciones con las funciones primarias del Sandboxie, y luego de esta identificación aplicar ajustes necesarios para aumentar la compatibilidad actual que tiene el software con estas.

## 8. *Tutorial de Sanboxie*

Figura 154. Tutorial. Sanboxie.


Fuente: Propia del autor.

## 9. *Ejecución del aplicativo*

Figura 155. Inicio Sanboxie.

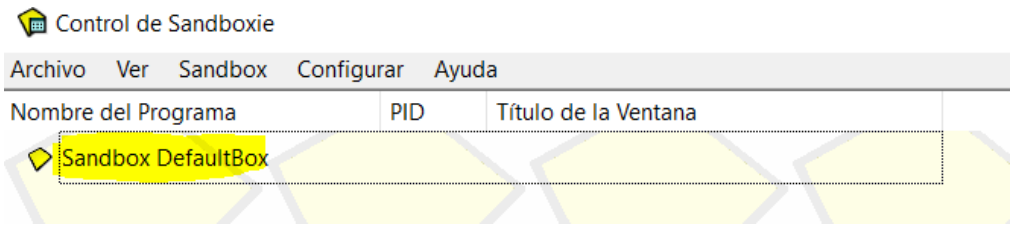

Fuente: Propia del autor.

Cabe recalcar que el proceso de instalación de este sandbox es bastante sencillo y no conlleva ningún inconveniente a la hora de su instalación.

### 6.7.2. Aplicación de Sanboxie en pruebas del explorador de Windows.

Este apartado presenta el proceso ejecución del aplicativo Sanboxie al momento de realizar navegación por el navegador de Windows y se procederá a crear cambios para verificar si también fueron efectuados por fuera del Sandbox creado para realizar la prueba. Para realizar lo antes mencionado se ingresa al aplicativo y se ubica el entorno de ejecución seguro.

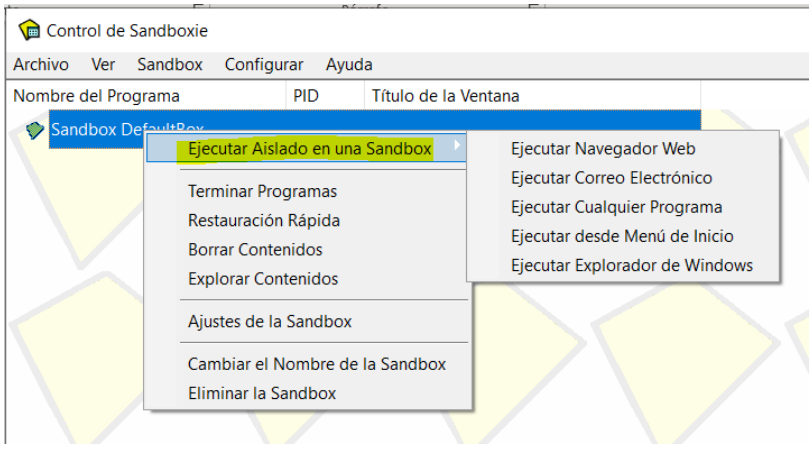
Figura 156. Entorno de prueba por defecto.




Fuente: Propia del autor.

Siguiendo con el proceso de ejecución, se expande la barra de opciones del entorno seguro con click derecho, se selecciona la opción ***ejecutar aislado en un sandbox*** y se desplegará el meno de ejecución seguro del Sandboxie como se muestra a continuación:

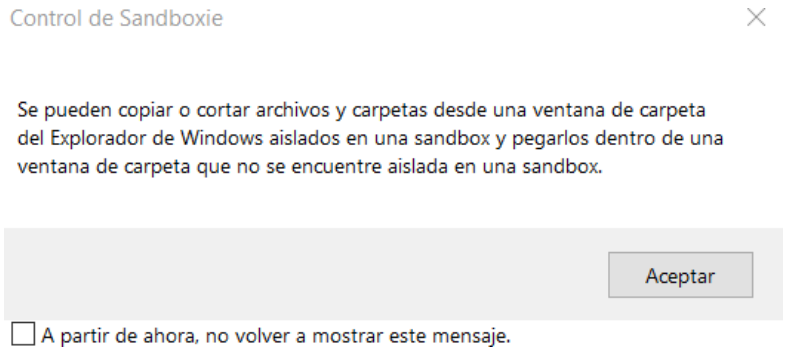
Figura 157. Meno de ejecuciones sandbox.




Fuente: Propia del autor.

El menú desplegable permitirá ejecutar en que sección se quiere ejecutar el sandbox. Para el caso particular de la resolución de este ejercicio, se seleccionará ***Ejecutar explorador de windows.***

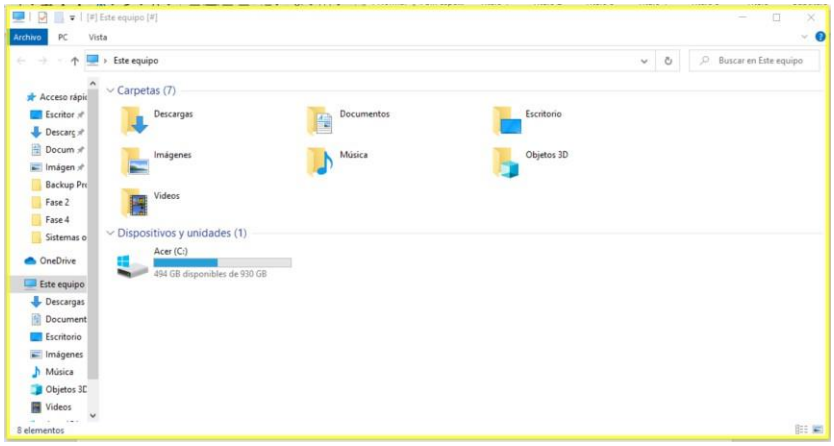
Figura 158. Aviso de creación.




Fuente: Propia del autor.

Al presionar aceptar, se desplegará el explorador de windows de la siguiente forma:

Figura 159. Entorno Sanboxie en explorador de archivos.

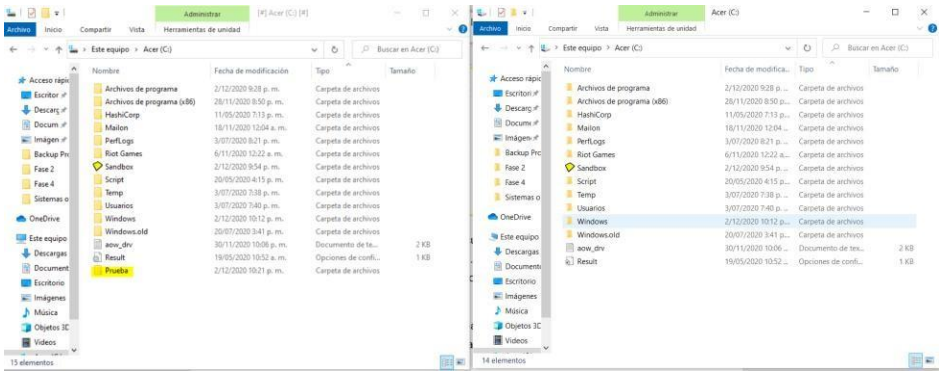



Fuente: Propia del autor.

Esta ejecución, consta de 2 particulares que permitirán identificar que se está ejecutando bajo un entorno Sandbox. La primera es la línea amarilla que rodea al explorador y la segunda es el identificador del explorador que tiene un nombre película como ***[#] Este Equipo [#]***.

Luego de esto se procederá a crear una carpeta dentro del disco C y se validará la existencia del archivo creado.

Figura 160. Prueba Sanboxie de creación de archivos.



Fuente: Propia del autor.

Como se denota en la Figura, la creación del archivo solo se hizo en el entorno seguro y no en el entorno real del equipo.

Finalmente se puede establecer que la aplicación de la herramienta Nagios para el monitoreo, Bacula para la gestión de copias de seguridad, GLPÏ como correlacionador de eventos y Sandboxie como servicio de Sandbox, permite suplir la necesidad de aplicación de un SOC que satisface las necesidades objetivas de la empresa PLATINO SISTEMAS.

Por lo mencionado, se puede evidenciar en los apartados anteriores donde se realizan pruebas de instalación y configuración de cada una de las herramientas, así como también pruebas desde el servidor de monitoreo para validar el estado de los demás servidores, pruebas de ejecución de Backups desde el servidor Bacula a los servidores de Nagios y GLPI y finalmente las pruebas de ejecución del servicio de Sandboxie para la ejecución en ambientes de pruebas de programas y otros servicios que necesiten de previa valoración.

# 7. CONCLUSIONES

Se obtiene primeramente como conclusión que, el SOC que se adecúa teniendo en cuenta a los tipos de SOC especificados (SOC pequeño, mediano y grande), es un SOC de pequeña escala, puesto que, son cuatro los servicios establecidos por la empresa PLATINO SISTEMS (Servicio de monitoreo, servicio de correlacionador de eventos, servicio de Backups y servicio de Sandboxie), la operación se podría distribuir perfectamente entre tres frentes de gestión como lo plantea el SOC de pequeña escala.

Seguido de lo anterior también se puede concluir que, la propuesta de operación antes mencionada (ver apartado **6.2**) es la ideal para que un SOC en base a su modelo de operación pueda ejecutar sus diferentes procesos de manera correcta, contemplado desde la identificación de programas, seguido del análisis de la Instrumentación utilizada en el centro, el análisis y detección por medio de herramientas utilizadas en el centro de operaciones, el monitoreo de sistemas a nivel general, la evaluación de amenazas a nivel general, la escalada, respuesta e informes generados por el mismo centro, la conciencia situacional enfocada en las soluciones de ciberseguridad y finalmente ese proceso de prevención enfocado a los incidentes cibernéticos que regula el SOC.

Otra de las conclusiones que se puede evidenciar es que, las herramientas Open-Source que permiten suplir las necesidades de implementación de servicios de SOC en la empresa platino sistema de forma adecuada, son las de GLPI por parte de la solución correlacionador de eventos, Nagios por parte de la solución para el monitoreo de las redes, Bacula por parte de la solución para la creación de Backups y por último el servicio de Sandboxie para suplir la necesidad del Sandox.

# 8. RECOMENDACIONES

Antes de finalizar, se establecen algunas recomendaciones con base a los resultados y las conclusiones a que se llegó luego del presente desarrollo investigativo:

1. Para una empresa de pequeña escala como PLATINO SISTEMAS o de infraestructura tecnológica parecida, es viable aplicar SOC de pequeña escala, puesto que no requieren de demasiados servicios tecnológicos y la administración de estos en cabeza de los tres lideres que sugiere este tipo de SOC'S es viable para satisfacer las necesidades de seguridad en la infraestructura tecnológica de la organización.

2. La aplicación de tecnológicas Open-Source pueden ser una solución viable para la aplicación de servicios que suplan las necesidades de gestión y seguridad que requiera el SOC, aunque tiene una pequeña desventaja, que para la aplicación de estas, algunas herramientas no tienen soporte ni remoto, ni en sitio, haciendo que errores materializados en el aplicativo puedan ser tanto fácil de solventar como difíciles.

3. En base a las recomendación técnicas, se puede establecer que tanto Nagios como Bacula y GLPI son herramientas de configuración estándar, esto infiere a que el proceso de configuración no es tan extensivo y relativamente amigable con la experiencia del usuario, pero se debe tener en cuenta que la aplicación de este tipo de servidores al almacenar y monitorear cantidades de información, requieren de una alta capacidad de RAM y a su vez un almacenamiento considerable para poder realizar las copias de seguridad y el monitoreo de la red de manera eficiente.

4. Como recomendación final a empresas u organizaciones, la aplicación de un SOC acarrea más beneficios que puntos negativos, puesto que a través de la implementación de estos, se establecen muchas medidas de seguridad utilizando herramientas ya sean comerciales o libres que apoyen a la aplicación de controles técnicos que van desde la disponibilidad de la información y los sistemas de información como a la integridad y confidencialidad de estos.

5. Como una recomendación adicionar a futuros desarrollos de proyectos con enfoque técnicos relacionados directamente con SOC, se deben tener en cuenta los diferentes servicios generales que presta un SOC como Detección y análisis de amenazas, Cerrar brechas de seguridad, Contención, erradicación y recuperación de eventos, Gestión de vulnerabilidades, investigación forense, entre otros; Y no solamente servicios específicos como gestión de Backups, correlacionador de eventos y servicio de monitoreo, que a la final no dejan ver toda la gestión de un SOC en su plenitud.

# 9. BIBLIOGRAFÍA


ABREU, José Luis. Análisis al Método de la Investigación. [En línea]. Nuevo León. International Journal of Good Conscience. 2015. [Consulta: 20 de marzo 2022]. Disponible: http://www.spentamexico.org/v10-n1/A14.10(1)205-214.pdf

ATLASSIAN CONFLUENCE 7.5.0. realizado a Apache Software Foundation [En línea]. 2019. Confluence. Internet community. (Consulta: 12 de octubre de 2020) Disponible en https://cwiki.apache.org/confluence/display/httpd/FAQ#FAQ-WhatisApache?

BACULA. What is Bacula?. Documentation. [En línea]. 2009. (Consulta: 12 de octubre de 2020) Disponible: https://www.bacula.org/what-is-bacula/

BONILLA, Billy y ROJAS, Anthony. Diseño y planificación de un centro de operaciones de seguridad informática aplicado como servicio por la organización A3SEC bajo marcos de trabajo propuestos por Sans, ISACA y NIST. [En línea]. Trabajo especialidad. Bogotá, Universidad Piloto de Colombia. 2019. [Consulta: 20 de marzo 2022]. Disponible: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/5814/00005153.pdf?sequence=1&isAllowed=y

CAVALLI, Enrico, *et a*l. Information security concepts and practices: the case of a provincial multi-specialty hospital. Elsevier. [Consulta: 20 de marzo 2022]. Disponible: https://www.sciencedirect.com/science/article/abs/pii/S1386505603002132#!

CISCO. Backing Up and Restoring Data. [Sitio web]. EE.UU. [Consulta: 20 de marzo 2022]. Disponible: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/unity_exp/rel3_1/administra

tion/guide/voicemail/11bkrst.html

CICHONSKI P, MILLAR T, at ep. Computer Security Incident Handling Guide. National Institute of Standards and Technology. 2012. [Consulta: 30 de mayo de 2022]. Disponible: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 1273. (5, enero, 2009). por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". (Diario Oficial No. 51945 - 11 de febrero de 2022).

COMPES 3995. POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL. Consejo Nacional De Política Económica Y Social República De Colombia Departamento Nacional De Planeación. [En Línea]. Departamento nacional de Planeación. 2020. [Consulta: 30 de mayo de 2022]. Disponible: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

DAVIES Nahla. AlienVault OSSIM. The world’s most widely used open source SIEM. [En línea]. 2020. AT&T Alien Labs. (Consulta: 13 de octubre de 2020) Disponible: https://cybersecurity.att.com/products/ossim

DELL. Servidor blade PowerEdge M630. [En línea]. 2018. (Consulta: 13 de octubre de 2020) Disponible: https://www.dell.com/co/empresas/p/poweredge-m630/pd

FREDERICK P. Brooks, Jr. The Postfix Home Page [En línea]. 2018. Carolina del Norte. POSTFIX (Consulta: 12 de octubre de 2020) Disponible en: http://www.postfix.org/documentation.html

GLPI. GLPI Network Cloud. Paris, Île-de-France. [Consulta: 20 de marzo 2022]. Disponible: https://glpi-project.org/es/recursos/

GLPI TECLIB. Características de GLPI. Gestión de TI basado en tecnologías de código abierto. [En línea]. 2020. (Consulta: 13 de octubre de 2020). Disponible: https://glpi-project.org/es/caracteristicas/

GOBIERNO DIGITAL. [Sitio web]; Bogotá: Ministerio de Tecnologías de la Información y las Comunicaciones. [Consulta: 20 de marzo 2022]. Disponible: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/CSIRT-Gobierno/

HERTEL, Chris. Samba: An Introduction. [En línea]. 2001. The Samba Team. (Consulta: 12 de octubre de 2020) Disponible: https://www.samba.org/samba/docs/SambaIntro.html

IBM. What is threat hunting?. [En línea]. Corporación. [Consulta: 30 de mayo 2022]. Disponible: https://www.ibm.com/topics/threat-hunting

INTERNET SYSTEMS CONSORTIUM. BIND 9. Why use BIND 9?. [En línea]. Nwemarket. NH. 2020. (Consulta el 12 de octubre de 2020). Disponible: https://www.isc.org/bind/

INCIBE. CEO, CISO, CIO ¿Roles en ciberseguridad?. Instituto nacional de ciberseguridad. [En línea]. 2016. [Consulta: 30 de mayo de 2022]. Disponible: https://www.incibe.es/protege-tu-empresa/blog/ceo-ciso-cio-roles-ciberseguridad

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Sistemas de Gestión de Seguridad de la información. NTC-ISO/IEC 27000:2016.

Bogotá D.C., Colombia. [Consulta: 20 de marzo 2022]. Disponible: https://www.iso27000.es/glosario.html

KASPERSKY. ¿Qué es una brecha de seguridad?. [En línea]. Corporación. [Consulta: 30 de mayo 2022]. Disponible: https://www.kaspersky.es/resource-center/threats/what-is-a-security-breach

MANAGEENGINE, ¿Qué es la gestión de incidentes ITIL?. SERVICEDESK PLUS. [En línea]. Proveedor de productos comerciales. 2020. [Consulta: 30 de mayo de 2022]. Disponible: https://www.manageengine.com/latam/service-desk/itil-incident-management/que-es-la-gestion-de-incidentes-itil.html#:~:text=La%20gesti%C3%B3n%20de%20incidentes%20es,de%20servicio%20(SLA)%20acordados.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Guía 5 para la Gestión y Clasificación de Activos de Información. [Sitio web]. Bogotá. [Consulta: 20 de marzo 2022]. Disponible: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

MORALES, Carlos, *et al*. PROPUESTA DE UN MODELO DE CENTRO DE OPERACIONES DE SEGURIDAD (SOC) PARA FUERZA AEREA COLOMBIANA. [En línea]. Trabajo especialidad. Bogotá. Universidad Piloto de Colombia. 2014. [Consulta: 20 de marzo 2022]. Disponible: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2786/trabajo%20de%20grado1627.pdf?sequence=1&isAllowed=y

NAGIOS. The Industry Standard In IT Infrastructure Monitoring. Nagios Features and Capabilities. [En línea]. 2020. (Consulta: 12 de octubre de 2020) Disponible: https://www.nagios.org/about/features/

NORTH NETWORKS. ¿Qué es Nagios?. Ciudad de México. [Consulta: 20 de marzo 2022]. Disponible: https://www.north-networks.com/que-es-nagios/

ORACLE. [Sitio web]. Redwood Shores, CA. Oracle Corporation. [Consulta: 20 de marzo 2022]. Disponible: https://www.oracle.com/es/database/security/que-es-un-soc.html

PRENDES MORENO, Michelle Ivette. “DEFINICIÓN DEL PROCESO DE CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN PARA EL CENTRO DE OPERACIONES DE SEGURIDAD INFORMÁTICA SECUINFOR S.A. [En línea]. Trabajo magister. Escuela Superior Politécnica Del Litoral. 2016. [Consulta: 20 de marzo 2022]. Disponible: http://www.dspace.espol.edu.ec/xmlui/bitstream/handle/123456789/37400/D-103388.pdf?sequence=-1&isAllowed=y

ROSENCRANCE, Linda. Sandbox (software testing and security). [Consulta: 20 de marzo 2022]. Disponible: https://www.techtarget.com/searchsecurity/definition/sandbox

SHEIKH, Shah. Building a Ciber Security Operations Center [En línea]. 2018. Confluence. Internet community. (Consulta: 15 de abril de 2020) Disponible en: https://es.slideshare.net/ShahSheikh/dts-solution-building-a-soc-security-operations-center

TORRES, Román y María José. Proceso para Definir y Establecer un Centro de Operaciones de Seguridad (SOC) en una Organización Financiera. [En línea]. Trabajo Master. Guayaquil. Universidad internacional de la roja. 2019. [Consulta: 20 de marzo 2022]. Disponible: https://reunir.unir.net/bitstream/handle/123456789/8169/ROMAN%20TORRES%2c

%20MARIA%20JOSE.pdf?sequence=1&isAllowed=y

VILCAR ROMERO, Ladi y VILCHEZ, Evit. Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones. [En línea]. Trabajo Magister. Lima. Universidad peruana de ciencias aplicadas. 2018. [Consulta: 20 de marzo 2022]. Disponible: https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/624832/VilcarromeroZ_L.pdf?sequence=11&isAllowed=y

## 10. RAE

| | |
|---|---|
| **Fecha de Realización:** | 05/07/2022 |
| **Programa:** | Especialización En Seguridad Informática |
| **Línea de Investigación:** | Gestión de sistemas |
| **Título:** | DISEÑO DE UN CENTRO DE OPERACIÓN DE SEGURIDAD (SOC) PARA LA EMPRESA PLATINO SISTEMA |
| **Autor(es):** | Mailon Pérez Fernández |
| **Palabras Claves:** | SOC, Centro de Respuesta a Incidentes Cibernéticos, Backups, Correlacionador de eventos, Servidor de monitoreo. |
| **Descripción:** | Platino sistemas es una organización colombiana posicionada a nivel nacional, la cual tienen como modelo de negocios la prestación de servicios de seguridad para la protección de la información de diferentes tipos de organización. Siendo este su principal fundamento en su modelo de negocios, la necesidad de automatizar, gestionar y controlar la seguridad de la información y los datos en una organización se hace vital para todos los procesos que la constituyen, evaluación de riesgos, respuestas a incidentes, gestión de vulnerabilidades, entre otros temas que precisan de unos niveles de operatividad y transparencia importantes.<br>Con base en lo anterior, el presente proyecto tiene como finalidad la creación de un centro de respuesta a incidentes cibernéticos en el ámbito CSIRT, sobre el cual se fundamentará el desarrollo de un centro de operaciones de seguridad SOC partiendo desde la creación del diseño técnico del CSIRT y seguido por una etapa de desarrollo hardware-software que dé cumplimiento a las actividades propias de CSIRT |

**Fuentes bibliográficas destacadas:**

SHEIKH, Shah. Building a Ciber Security Operations Center [En línea]. 2018. Confluence. Internet community. (Consulta: 15 de abril de 2020) Disponible en: https://es.slideshare.net/ShahSheikh/dts-solution-building-a-soc-security-operations-center

MORALES, Carlos, et al. PROPUESTA DE UN MODELO DE CENTRO DE OPERACIONES DE SEGURIDAD (SOC) PARA FUERZA AEREA COLOMBIANA. [En línea]. Trabajo especialidad. Bogotá. Universidad Piloto de Colombia. 2014. [Consulta: 20 de marzo 2022]. Disponible:

<table>
<tr><td colspan="2">http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2786/trabajo%20de%20grado1627.pdf?sequence=1&isAllowed=y<br><br>TORRES, Román y María José. Proceso para Definir y Establecer un Centro de Operaciones de Seguridad (SOC) en una Organización Financiera. [En línea]. Trabajo Master. Guayaquil. Universidad internacional de la roja. 2019. [Consulta: 20 de marzo 2022]. Disponible: https://reunir.unir.net/bitstream/handle/123456789/8169/ROMAN%20TORRES%2c%20MARIA%20JOSE.pdf?sequence=1&isAllowed=y<br><br>CICHONSKI P, MILLAR T, at ep. Computer Security Incident Handling Guide. National Institute of Standards and Technology. 2012. [Consulta: 30 de mayo de 2022]. Disponible: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf<br><br>BONILLA, Billy y ROJAS, Anthony. Diseño y planificación de un centro de operaciones de seguridad informática aplicado como servicio por la organización A3SEC bajo marcos de trabajo propuestos por Sans, ISACA y NIST. [En línea]. Trabajo especialidad. Bogotá, Universidad Piloto de Colombia. 2019. [Consulta: 20 de marzo 2022]. Disponible: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/5814/00005153.pdf?sequence=1&isAllowed=y</td></tr>
<tr><td>Contenido del documento:</td><td>El contenido del documento se estructura de la siguiente forma:<br>1. Se presenta la definición del problema asociado a la ejecución y el desarrollo del proyecto en un enfoque técnico.<br>2. La justificación de la creación del centro de operaciones de seguridad que solventará la necesidad de la empresa Platino sistemas.<br>3. El establecimiento del objetivo general y los objetivos específicos que apoyarán a la resolución del problema planteado.<br>4. Un marco referencial que sustenta toda la estructuración y soporte para el desarrollo de los objetivos planteados.<br>5. El diseño metodológico que permitió el desarrollo de los objetivos, partiendo desde un ámbito investigativo hasta la aplicación de este en escenarios organizacionales.<br>6. Desarrollo de los objetivos planteados, partiendo desde la propuesta de roles del equipo de trabajo del SOC, siguiendo con la</td></tr>
</table>

| | |
|---|---|
| | propuesta de tecnología para la aplicación del SOC, continuando con la identificación de herramientas de hardware y software libre para el desarrollo de las actividades del SOC y finalizando con el diseño y virtualización de servicios específicos que estructuran las diferentes funcionalidades del SOC, acopladas a las actividades generales y especificas en los CSIRT.<br>7. Conclusiones encontradas en base al desarrollo de los diferentes objetivos establecidos según la línea base del problema de la empresa Platino Sistemas.<br>8. Recomendaciones realizadas en relación al desarrollo de los objetivos y a la misma aplicación del SOC, en sus diferentes ejes de ejecución.<br>9. Marco bibliográfico que sustentó el desarrollo de los objetivos propuestos para la resolución de la problemática que enmarca la empresa Platino Sistemas. |
| **Marco Metodológico:** | La metodología empleada para el desarrollo del proyecto es la cualitativa utilizando métodos inductivos. Este busca establecer tendencias narrativas causales dentro de los diferentes hechos correlacionados con la solución al objetivo general plasmado, para luego de esto realizar análisis en base a las soluciones y establecer patrones de soluciones que puedan solventar la necesidad de la empresa en cuestión. |
| **Conceptos adquiridos:** | SOC, Centro de Respuesta a Incidentes Cibernéticos, Backups, Correlacionador de eventos, Servidor de monitoreo. |
| **Conclusiones:** | 1. Se obtiene primeramente como conclusión que, el SOC que se adecúa teniendo en cuenta a los tipos de SOC especificados (SOC pequeño, mediano y grande), es un SOC de pequeña escala, puesto que, son cuatro los servicios establecidos por la empresa PLATINO SISTEMS (Servicio de monitoreo, servicio de correlacionador de eventos, servicio de Backups y servicio de |

| | |
|---|---|
| | Sandboxie), la operación se podría distribuir perfectamente entre tres frentes de gestión como lo plantea el SOC de pequeña escala.<br>2. Seguido de lo anterior también se puede concluir que, la propuesta de operación antes mencionada (ver apartado 6.2) es la ideal para que un SOC en base a su modelo de operación pueda ejecutar sus diferentes procesos de manera correcta, contemplado desde la identificación de programas, seguido del análisis de la Instrumentación utilizada en el centro, el análisis y detección por medio de herramientas utilizadas en el centro de operaciones, el monitoreo de sistemas a nivel general, la evaluación de amenazas a nivel general, la escalada, respuesta e informes generados por el mismo centro, la conciencia situacional enfocada en las soluciones de ciberseguridad y finalmente ese proceso de prevención enfocado a los incidentes cibernéticos que regula el SOC.<br>3. Otra de las conclusiones que se puede evidenciar es que, las herramientas Open-Source que permiten suplir las necesidades de implementación de servicios de SOC en la empresa platino sistema de forma adecuada, son las de GLPI por parte de la solución correlacionador de eventos, Nagios por parte de la solución para el monitoreo de las redes, Bacula por parte de la solución para la creación de Backups y por último el servicio de Sandboxie para suplir la necesidad del Sandox. |