DISEÑO TÉCNICO DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC), QUE PERMITA DETERMINAR LOS REQUERIMIENTOS TECNOLÓGICOS PROPIOS DE UN EQUIPO DE RESPUESTA DE EMERGENCIAS INFORMÁTICAS (CSIRT) PARA LA EMPRESA PLATINO SISTEMAS

MADELIN FUENTES ROBAYO
CAMILO ANDRÉS VALLEJO VARGAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2021

DISEÑO TÉCNICO DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC), QUE PERMITA DETERMINAR LOS REQUERIMIENTOS TECNOLÓGICOS PROPIOS DE UN EQUIPO DE RESPUESTA DE EMERGENCIAS INFORMÁTICAS (CSIRT) PARA LA EMPRESA PLATINO SISTEMAS

MADELIN FUENTES ROBAYO
CAMILO ANDRÉS VALLEJO VARGAS

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

Tutor
ING. FREDY MONCALEANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2021

NOTA DE ACEPTACIÓN

Firma presidente del jurado

Firma del jurado

Firma del jurado

Bogotá, Cundinamarca, 18 de junio de 2021

DEDICATORIA

Primero que todo a Dios, por acompañarnos en cada paso, por fortalecer nuestro corazón e iluminar nuestra mente, por haber puesto en nuestros caminos a aquellas personas que han sido soporte y compañía en nuestra vida.

A nuestras familias por todo el apoyo incondicional y por la motivación para iniciar y culminar este proyecto, a todas las personas que nos acompañaron en esta etapa, aportando a nuestro crecimiento tanto profesional como personal.

AGRADECIMIENTOS

Al Lic. Danny Fernando León M. Sc, tutor del curso Proyecto de Grado I por sus observaciones pertinentes y guía durante el desarrollo del proyecto de grado en su primera fase.

A la Ing. Yenny Stella Nuñez, Magister en seguridad informática y directora del curso Proyecto de Grado I por sus aportes puntuales y relevantes que ayudaron a la construcción del documento proyecto aplicado.

Al Ing. Fernando Barajas, Magister en seguridad informática y tutor del curso Proyecto de Grado II por su asesoría y oportuno apoyo en el desarrollo de la fase 2 de este proyecto.

Al Ing. Fredy Moncaleano, director del trabajo de grado por su asesoría, observaciones e indicaciones durante el desarrollo del proyecto.

RESUMEN

En virtud de la creciente expansión del uso de las herramientas tecnológicas y del Internet, se han incrementado las amenazas cibernéticas tanto para las organizaciones públicas como privadas. De acuerdo con el estudio “Tendencias del Cibercrimen en Colombia 2019-2020” liderado por el programa Seguridad Aplicada al Fortalecimiento Empresarial (SAFE), del Tanque de Análisis y creatividad de las TIC (TicTac)[1], la cifra de incidentes cibernéticos reportados a la Policía Nacional durante el 2019 fue de 28.827, lo cual representa un aumento del 54% respecto al 2018.

En este contexto y conforme a las necesidades de la empresa PLATINO SISTEMAS de garantizar sus servicios para la protección, el respaldo y el aseguramiento de los activos de información de los clientes, surge la necesidad de invertir tiempo, dinero y otros recursos para definir mecanismos que permitan detectar, prevenir y solventar fallos de seguridad en los sistemas y servicios que administra la organización.

Es por esto que se diseñará un Centro de Operaciones de Seguridad (SOC por sus siglas en inglés)[2] en adelante SOC, que corresponde a “una plataforma que permite la supervisión y administración de la seguridad del sistema de información a través de herramientas de recogida, correlación de eventos e intervención remota” y de esta manera determinar los requerimientos tecnológicos propios de un Equipo de Respuesta a incidentes de Seguridad Informática (CSIRT)[3], en adelante CSIRT, el cual dispone de un equipo especializado en seguridad de las TI que tiene como propósito ayudar a mitigar y disminuir los incidentes de seguridad y de esta manera proteger el patrimonio de las organizaciones.

De acuerdo con lo anterior, en la primera fase se abordará el diseño de la estructura organizacional que permitirá definir las capacidades de las operaciones del SOC,

[1] TicTac (10-2019). Tendencias del Cibercrimen en Colombia 2019-2020. Disponible en _https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf
[2] Oracle Database Security. [Sitio web] Disponible en https://www.oracle.com/es/database/security/que-es-un-soc.html
[3] ENISA. Agencia de la Unión Europea para la seguridad Cibernética. (2019). CSIRT en Europa. Disponible en: https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network

posteriormente se realizará la formulación de las políticas, alcance y servicios propuestos. En la segunda fase se establecerán las herramientas de hardware y software que permitirán el desarrollo de las actividades en función de los servicios del CSIRT y finalmente se ejecutarán las actividades más importantes del CSIRT en un ambiente controlado y virtualizado sujeto a los recursos disponibles.

Palabras Claves: CSIRT, SOC, incidente, SGSI, vulnerabilidad, amenaza, riesgo.

ABSTRACT

Due to the growing expansion of the use of technological tools and the Internet, cyber threats have increased for both public and private organizations. According to the study "Trends in Cybercrime in Colombia 2019-2020" led by the Security Applied to Business Strengthening (SAFE) program of the ICT Analysis and Creativity Tank (TicTac), the number of cyber incidents reported to the Police National during 2019 was 28,827, which represents an increase of 54% compared to 2018.

In this context and in accordance with the needs of the company PLATINO SISTEMAS to guarantee its services for the protection, support and assurance of customer information assets, the need arises to invest time, money and other resources to define mechanisms that allow to detect, prevent and solve security failures in the systems and services managed by the organization.

That is why a Security Operations Center (SOC) will be designed hereinafter SOC, which corresponds to “a platform that allows the supervision and administration of the security of the information system through collection tools, correlation of events and remote intervention "and thus determine the technological requirements of a Computer Security Incident Response Team (CSIRT), hereinafter CSIRT, which has a specialized IT security team whose purpose is to help mitigate and reduce security incidents and thus protect the assets of organizations.

In accordance with the above, in the first phase the design of the organizational structure that will allow defining the capabilities of the SOC operations will be addressed, then the formulation of the proposed policies, scope and services will be carried out. In the second phase, the hardware and software tools that will allow the development of activities based on the services of the CSIRT will be established and finally the most important activities of the CSIRT will be executed in a controlled and virtualized environment subject to available resources.

Keywords: CSIRT, SOC, Incident, SGSI, vulnerability, threat, risk.

TABLA DE CONTENIDO

1. INTRODUCCIÓN 16
2. DEFINICIÓN DEL PROBLEMA 18
2.1 Antecedentes Del Problema 18
2.2 Formulación Del Problema 19
3. JUSTIFICACIÓN 20
4. OBJETIVOS 23
4.1 Objetivo General 23
4.2 Objetivos Específicos 23
5. MARCO REFERENCIAL 24
5.1 Marco Teórico 24
5.2. Marco Conceptual 28
5.3. Marco Legal 32
6. DISEÑO METODOLÓGICO 36
7. DESARROLLO DE LOS OBJETIVOS 37
7.1 Estructura Organizacional Y Capacidades De Las Operaciones Del Soc. 37
7.1.1 Estructura Organizacional 37
7.1.2 Áreas, Responsabilidades y Roles 38
7.1.3 Capacidades de las Operaciones del SOC 42
7.1.3.1 Organigrama SOC 42
7.1.3.2 Perfiles y Roles del SOC 42
7.2 Políticas, Alcance y Servicios Propuestos por el SOC (Centro De Operaciones De Seguridad). 47
7.2.1 Políticas de Seguridad 47
7.2.2 Alcance del SOC 49
7.2.3 Servicios Propuestos por el SOC 50
7.3 Herramientas Tecnológicas de Hardware y Software para el Desarrollo de las Actividades Propias del CSIRT. 51
7.3.1 Herramientas de Software. 51
7.3.1.1 Servidor WEB - XAMP: 51
7.3.1.2 Servicio de correo electrónico - POSTFIX: 52
7.3.1.3 Servicio de Intranet - XAMPP: 53
7.3.1.4 Servidor de Archivos - SAMBA: 54
7.3.1.5 Servicio de Copias de Seguridad - VEEAM BACKUP & REPLICATION: 54

7.3.1.6 Servidor DNS - BIND: 55
7.3.1.7 Servidor de Monitoreo - PANDORA FMS: 56
7.3.1.8 Servidor de Sandbox - FIREJAIL: 57
7.3.1.9 Correlacionador de eventos - ALIENVAULT OSSIM: 59
7.3.1.10 Servicio Registro y seguimiento de Incidentes - OSTICKET: 60
7.3.1.11 Informática forense - SANS DFIR: 61
7.3.2 Herramientas de Hardware. 62
7.3.2.1 Switch Core WS-C3560X-24 62
7.3.2.2 Switch Cisco Catalyst 2960S-48TS-S 63
7.3.2.3 Firewall - IDS/IPS 63
7.3.2.4 WAF 64
7.3.2.5 EDR 66
7.3.2.6 Diagrama Topológico de Hardware de Platino Sistemas 69
7.3.2.7 Segmentación de La Red 70
7.4 Diseño del Ambiente Controlado y Virtualizado. 70
7.4.1 Instalación y funcionamiento del servidor WEB - XAMPP 8.0.2.0 70
7.4.2 Instalación y funcionamiento del servidor de Archivos - SAMBA 73
7.4.3 Instalación y funcionamiento del servidor de Monitoreo - PANDORA 77
7.4.4 Instalación y funcionamiento del Software de Copias de Seguridad - VEEAM BACKUP. 81
7.4.5 Instalación y funcionamiento del Servidor de Sandbox - FIREJAIL. 83
7.4.6 Instalación y funcionamiento del software de Registro y Seguimiento de incidentes - OSTICKET. 87
7.4.7 Instalación y funcionamiento del Correlacionador de Eventos - ALIENT VAULT. 88
8. RESULTADO OBJETIVOS PLANTEADOS 94
Repositorio del Proyecto: 95
Video: 95
9. CONCLUSIONES 96
10. GLOSARIO 98
11. BIBLIOGRAFÍA 100

LISTA DE TABLAS

Tabla 1. Servicios del SOC.....50
Tabla 2. Herramientas de Software.....51
Tabla 3. Herramientas de Hardware.....62
Tabla 4. Segmentación de Red.....70

LISTA DE FIGURAS

Figura 1. Estructura Organizacional CSIRT.....37
Figura 2. Organigrama SOC.....42
Figura 3. Modelo típico de distribución de red por zonas. 46
Figura 4. Servidor WEB XAMPP. 52
Figura 5. Servidor Correo Electrónico Postfix.....53
Figura 6. Servicio de Archivos Samba.....54
Figura 7. Servicio de Copias de Seguridad VEEAM. 55
Figura 8. Servidor DNS BIND. 56
Figura 9. Servidor de Monitoreo PANDORA FMS. 57
Figura 10. Servidor de Sandbox Firejail. 58
Figura 11. Correlacionador de eventos Alien Vault OSSIM. 59
Figura 12. Servicio Registro y seguimiento de Incidentes OSTICKET. 60
Figura 13. Informática Forense SANS DFIR.....61
Figura 14. Switch Core WS-C3560X-24 62
Figura 15. Switch Cisco Catalyst 2960S-48TS-S 63
Figura16. Firewall Pfsense. 64
Figura17. WAF ModSecurity.....66
Figura18. Arquitectura de GRR (Google Rapid Response) 67
Figura19. Diagrama topológico de hardware Platino Sistemas 69
Figura20. Descarga Instalador de XAMPP 70
Figura21. Instalación XAMPP.....71
Figura22. Verificación de la ejecución de los servicios de XAMPP 72
Figura23. Verificación de la ejecución de los servicios de XAMPP desde Consola 73
Figura24. Sitio WEB Platino Sistemas alojado en servidor XAMPP. 73
Figura25. Activación del Servicio SMBD. 74
Figura26. Activación del Servicio NMBD 74
Figura27. Creación de usuarios con acceso a recursos compartidos 75

Figura28. Verificación de acceso a recurso compartido. 76
Figura29. Acceso a recurso compartido 76
Figura30. Inicio de sesión en Servidor de Monitoreo. 77
Figura31. Página de inicio de la plataforma de monitoreo 77
Figura32. Vista táctica de la plataforma de monitoreo últimos eventos. 78
Figura33. Vista táctica de la plataforma de monitoreo gráfico de eventos 78
Figura34. Gestión de usuarios plataforma de monitoreo. 79
Figura35. Auditoría plataforma monitoreo. 79
Figura36. Instalación de agentes en los equipos monitorizados. 80
Figura37. Instalación VEEAM BACKUP. 81
Figura38. Verificación de los componentes de la herramienta. 81
Figura39. Asignación del nombre del servidor 82
Figura40. Lista de Jobs de Backup. 83
Figura41. Instalación de FIREJAIL. 83
Figura42. Verificación de la versión instalada. 84
Figura43. Interfaz gráfica FIREJAIL. 84
Figura44. Vista de aplicaciones ejecutadas desde Interfaz gráfica. 85
Figura45. Vista de aplicaciones ejecutadas desde Consola. 85
Figura46. Configuración desde interfaz gráfica. 85
Figura47. Restricción de accesos a directorios. 86
Figura48. Verificación restricción de accesos 86
Figura49. Verificación acceso a Downloads. 87
Figura50. Instalación herramienta OsTicket 87
Figura51. Inicio de sesión ALIENVAULT OSSIM. 88
Figura52. Dashboards – Overview. 89
Figura53. Deployment Status 90
Figura54. Gestión de Alarmas 91
Figura55. Gestión de Eventos (SIEM) 92
Figura56. Gestión de Tickets 93

LISTA DE CUADROS

Cuadro 1. Marco Normativo.....32
Cuadro 2. Director de Tecnología.....38
Cuadro 3. Director SOC 38
Cuadro 4. Coordinador de formación 39
Cuadro 5. Líder Infraestructura tecnología 40
Cuadro 6. Equipo de investigación.....40
Cuadro 7. Analista financiero.....41
Cuadro 8. Abogado 41
Cuadro 9. Director SOC 42
Cuadro 10. Gestor de Incidentes.....43
Cuadro 11. Técnico L1 43
Cuadro 12. Especialista de Seguridad 43
Cuadro 13. Analista L1 44
Cuadro 14. Experto Forense 44
Cuadro 15. Técnico Forense L1 45
Cuadro 16. Políticas de Seguridad.....47
Cuadro 17. Desarrollo de los objetivos.....94

1. INTRODUCCIÓN

El evidente incremento del uso de las herramientas tecnológicas y de Internet, ha favorecido de manera importante el desarrollo operativo y comercial de las organizaciones optimizando su productividad, no obstante, este crecimiento ha venido acompañado del surgimiento de nuevas amenazas cada vez más sofisticadas que ponen en riesgo la integridad de los activos de información de cualquier entidad.

Por lo anterior se hace necesario establecer mecanismos de protección ante las vulnerabilidades relacionadas con ciberseguridad que pueden afectar a los entes tanto gubernamentales como particulares, es así que surge la necesidad de crear los equipos de respuesta a incidentes de seguridad CSIRT, los cuales proporcionan una serie de servicios con el fin de prevenir y mitigar los riesgos en caso de que se materialicen, respondiendo de manera ágil y eficiente, con el fin de garantizar el mínimo impacto y el restablecimiento de las actividades en el menor tiempo posible, así como asegurar el cumplimiento de los tres pilares de la información aplicados en el SGSI (Sistema de Gestión de Seguridad de la Información) confidencialidad, integridad y disponibilidad[4].

Este documento tiene como finalidad diseñar un Centro de Operaciones de Seguridad SOC, permitiendo además determinar los requerimientos tecnológicos propios de un Equipo de Respuesta a Incidentes Cibernéticos (CSIRT) ajustado a las necesidades de la empresa PLATINO SISTEMAS. Esta es una organización colombiana enfocada en la prestación de servicios de seguridad para la protección de la Información, la cual tiene como propósito crear y gestionar las funciones de respuesta a incidentes cibernéticos, ofreciendo servicios que permitan dar soporte a sus clientes en ciberseguridad, conforme a los acuerdos de niveles de servicio los cuales dan respuesta a los incidentes reactivos y proactivos.

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

La propuesta se fundamenta en referentes de tipo académico, empresarial y organizacional que sirven de base argumental para dar soporte al diseño del SOC del CSIRT.

Se desarrollará la estructura organizacional, capacidades del SOC y roles del equipo de trabajo alineados con la propuesta tecnológica para las operaciones y servicios brindados por el SOC.

Las operaciones del SOC estarán soportadas en herramientas Open Source y en hardware previamente evaluados de manera que permita dar cumplimiento al desarrollo de las actividades del CSIRT de acuerdo a los servicios reactivos y proactivos ofrecidos.

Se evaluará el software mediante la configuración y ejecución de pruebas de un laboratorio controlado virtualizado a través de la propuesta de un diseño lógico de las siguientes herramientas:

- Servidor de monitoreo
- Correlacionador de eventos
- Servidor de copias de Seguridad
- Servidor de Sandbox
- Registro y Seguimiento de Incidentes
- Servidor WEB
- Servidor DNS
- Servidor de Archivos

2. DEFINICIÓN DEL PROBLEMA

2.1 Antecedentes Del Problema

PLATINO SISTEMAS es una organización colombiana que presta servicios de seguridad para la protección de la Información. Garantizar la confidencialidad, integridad y disponibilidad de la información es el core de la empresa, así como la evaluación y control de amenazas y riesgos a las que están expuestas las organizaciones de sus clientes.

Según el informe generado por el Tanque de Análisis y creatividad de las TIC (TicTac)[5] en octubre de 2019 “Tendencias del Cibercrimen en Colombia 2019-2020”, en el país, lo que llevaba del año, el crecimiento de los ataques por malware fue de un 612%, por rescate de información se había pagado entre 32 a 160 millones de pesos, en este contexto, Colombia se encontraba entre los países que recibió el mayor número de ataques por ransomware en Latinoamérica con un total de 252 lo que corresponde al 30% después de Brasil y Argentina.

Aunado a lo anterior, y de acuerdo con las estadísticas de la Policía Nacional de Colombia[6], los incidentes cibernéticos reportados en lo corrido del 2020 afectan principalmente al sector ciudadano, seguido del sector financiero, el sector educativo, menores de edad, gobierno, tecnología, salud y medios de comunicación. En cuanto a las modalidades, el phishing es el método más usado, seguido por la suplantación de identidad, estafa por compras, amenazas a través de redes sociales, malware, sextorsión, injuria y/o calumnia, vishing, carta nigeriana y smishing.

En consecuencia, y con el fin de prevenir afectaciones del servicio, problemas legales, la pérdida de la imagen institucional entre otros impactos críticos, se requiere la

[5] TicTac (10-2019). Op. Cit.
[6] Policía Nacional de Colombia. Ciberincidentes. [Sitio web] Disponible en https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real/historico

implementación de una herramienta y/o metodología que permita gestionar de manera ágil y eficiente la atención a incidentes cibernéticos, en donde se brinde soporte a los clientes de acuerdo al nivel de servicio contratado, que puede ser de respuesta a incidentes o de gestión a vulnerabilidades, de esta manera garantizar la protección, el respaldo y el aseguramiento de los activos de información de los clientes.

De acuerdo con lo anterior, se considera necesario el diseño técnico de un SOC, que permita determinar los requerimientos tecnológicos propios de un CSIRT para la empresa Platino Sistemas.

2.2 Formulación Del Problema

¿Cómo puede Platino Sistemas brindar respuestas a incidentes y/o gestionar las vulnerabilidades de los posibles eventos cibernéticos, que garanticen la protección de los activos de información de sus clientes?

3. JUSTIFICACIÓN

En virtud del análisis liderado por el centro cibernético policial, donde se realiza una caracterización del cibercrimen en los últimos años, se evidencia que las víctimas más atractivas para este tipo de delitos son el ciudadano común y las grandes empresas del sector público y privado, dada la mayor rentabilidad que generan para la actividad criminal.

De acuerdo con el reporte de la IOCTA 2020[7], el ransomware continúa encabezando la lista de las principales amenazas de ciberseguridad tanto en Europa como en otros continentes, por otro lado, el malware tuvo un incremento en la afectación de las principales organizaciones durante el año 2019, y los ataques DDoS de acuerdo a las investigaciones cumplieron 20 años en las listas de amenazas cibernéticas.

El gobierno nacional ha incrementado sus esfuerzos con el fin de atender esta problemática y combatir las persistentes amenazas de seguridad de la información, para lo cual ha definido los lineamientos estableciendo leyes relacionadas con el derecho al acceso de la información pública y con la protección de los datos personales, algunas de estas leyes son; la Ley 1581 de 2012 “Ley de Protección de Datos Personales”, la Ley 1712 de 2014 “Ley de Transparencia y Acceso a la Información Pública”, la expedición del CONPES 3701 de 2011 “Lineamientos de política para ciberseguridad y ciberdefensa” y el CONPES 3854 de 2016 “Política Nacional de Seguridad Digital”, entre otros, las cuales buscan priorizar y salvaguardar la seguridad digital de la población en general y ofrecer valor público en un entorno de confianza digital.

Entre tanto, el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) formuló el Modelo de Seguridad y Privacidad de la Información (MSPI)[8] como

[7] La IOCTA es el producto estratégico insignia de Europol que destaca las amenazas dinámicas y en evolución de la ciberdelincuencia. Disponible en https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

[8] El cual se encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas. Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

estrategia para combatir la ciberdelincuencia, dicho modelo articuló las mejores prácticas en materia de seguridad de la información basándose en la ISO 27001 de 2013 y las 21 guías que propone el modelo para su implementación, permitiendo así elevar el nivel de madurez del sistema de seguridad de la información y cerrando brechas que existen entre las entidades.

De acuerdo con las previsiones del Centro para la Ciberseguridad (C4C, por sus siglas en inglés) del Foro Económico Mundial 2020 (FEM)[9], la pérdida económica debida al delito cibernético puede alcanzar los 3 billones de dólares para el año 2020, y el 74% de las empresas del mundo podrían ser hackeadas el próximo año, mientras que para 2021 se estima que los daños ocasionados por los ciberdelitos alcancen los 6 trillones de dólares.

Conforme los objetivos de la organización PLATINO SISTEMAS, es necesario implementar el diseño técnico de un SOC que realice las actividades de monitoreo, detección y análisis de incidentes previo a que se materialicen y de esta manera determinar los requerimientos tecnológicos propios de CSIRT que permita crear y gestionar las funciones de respuesta a incidentes cibernéticos, lo anterior con el propósito de ofrecer soporte a sus clientes, brindando respuesta a incidentes y/o gestión a vulnerabilidades. Con lo anterior se pretende fortalecer la protección a la información logrando confidencialidad e integridad en el tratamiento de la misma y teniendo siempre la disponibilidad de la información de los clientes.

El CSIRT deberá establecer políticas y procedimientos acordes a los objetivos de la organización para llevar a cabo el tratamiento y gestión de los eventos e incidentes de seguridad de la información, por lo anterior se deberá definir las estrategias de contención para controlar y mitigar el impacto dentro de las operaciones de la organización en caso de presentarse un incidente de seguridad.

[9] Foro Económico Mundial (2020). Shaping the Future of Cybersecurity and Digital Trust. Disponible en https://www.weforum.org/centre-for-cybersecurity/

Las ventajas del software Open Source son cada vez mayores frente a las soluciones propietarias. Un ejemplo claro de ello es el cambio de grandes empresas desarrolladoras de software como Microsoft que se ha unido a Open Source Initiative[10] para promover el software de código abierto cuyo propósito es brindar apoyo a la construcción y conocimiento colectivo lo cual representa tecnología al alcance de todos.

[10] Portal de proyectos Open Source de Microsoft. Disponible en https://opensource.microsoft.com/

4. OBJETIVOS

4.1 Objetivo General

Elaborar el diseño técnico de un Centro de Operaciones de Seguridad (SOC), que permita determinar los requerimientos tecnológicos propios de un Equipo de Respuesta de Emergencias Informáticas (CSIRT) para la empresa Platino Sistemas.

4.2 Objetivos Específicos

- Diseñar la estructura organizacional y establecer las capacidades de las operaciones del SOC (Centro de Operaciones de Seguridad)
- Formular políticas, alcance y servicios propuestos por el SOC (Centro de Operaciones de Seguridad).
- Determinar las herramientas tecnológicas de hardware y software que permitan desarrollar las actividades propias del CSIRT.
- Diseñar un ambiente controlado y virtualizado que permita ejecutar las actividades del CSIRT.

5. MARCO REFERENCIAL

A continuación, se abordan los diferentes aspectos que fundamentan el proyecto.

5.1 Marco Teórico

Tal como lo indica Adeva A. y Vera J. (2020)[11], el Equipo de Respuesta Ante Incidencias de Seguridad Informática (CSIRT), tuvo sus inicios en 1988 motivado al ver comprometida la seguridad de las infraestructuras de las TICs a causa de un incidente de seguridad informático, generado por un estudiante de Harvard “Robert Tappan Morris” quien creó un gusano informático llamado “Morris” el cual afectó un 10% de los sistemas conectados a ARPANET (Advanced Research Projects Agency Network). Se calcula que este incidente tuvo un costo estimado de 15 millones de dólares lo que puso en evidencia la necesidad de coordinar el trabajo entre los administradores de TICs de una manera ágil, eficiente y oportuna.

A lo largo de los siguientes dos años fue incrementando el número de equipos de respuesta a incidentes, de acuerdo con sus requisitos de información, nacionalidad, propósito y grupo de clientes atendidos. Un incidente informático llamado “gusano Wank” generado en octubre de 1989, estableció la necesidad de crear un organismo denominado FIRST en 1990, con el fin de optimizar la comunicación entre los equipos de respuesta a incidentes de diversos sectores.

El CSIRT (Computer Security Incident Response Team)[12] tiene como objetivo principal centralizar los procesos y recursos para la gestión de incidencias, permitiendo coordinar las acciones para brindar las respuestas frente a los incidentes que se puedan presentar en la organización.

[11] Ágorasic. Centro de Conocimiento en Ciberseguridad. CSIRTs al pie del Cañon. Disponible en https://www.first.org/newsroom/releases/FIRST-Press-Release-20201118.pdf

[12] El cual establece la guía de creación de un CERT / CSIRT. Disponible en https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/520-ccn-stic-810-guia-de-creacion-de-cert-s.html

Los CSIRT los podemos encontrar en diferentes ámbitos, como los son[13].

- ✔ CSIRT Académicos: que tienen como finalidad atender y gestionar los incidentes de seguridad de las universidades, institutos y escuelas.
- ✔ CSIRT Comerciales: que se enfocan en las empresas que solicitan los servicios de gestión de incidentes realizando un pago por dicho servicio.
- ✔ CSIRT de infraestructura crítica, su objetivo es proteger los activos de información y la infraestructura crítica de la nación.
- ✔ CSIRT Gubernamentales: se centra en garantizar que la infraestructura de TI de las instituciones públicas, que ofrecen servicios a los ciudadanos proporcione un nivel de seguridad adecuado.
- ✔ CSIRT Nacionales: es el punto de contacto para la gestión de incidentes a nivel nacional e internacional, además se encarga de la coordinación a nivel nacional las respuestas a incidentes.
- ✔ CSIRT del Sector Militar: Se enfocan en la defensa de incidentes o ataques cibernéticos ofensivos de la nación, centrándose en las TIC de uso militar como sistemas de radares y armamento.
- ✔ CSIRT de Proveedores: se centran en ofrecer servicios a productos específicos de un proveedor de servicios, fabricante o desarrollador.
- ✔ CSIRT de PYME: tiene como objetivo atender las solicitudes de comunidades de pequeñas y medianas empresas.

El CSIRT, aunque no tiene un retorno de inversión para las empresas, su principal objetivo es la protección de los activos de información de la misma, los servicios que ofrece el equipo de respuesta a incidentes de una empresa cuentan con tres categorías como lo indica Martínez que son; servicios reactivos, servicios proactivos y servicios de gestión de la calidad de la seguridad como lo indica Martinez[14].

[13] Buenas prácticas para establecer un CSIRT Nacional. Disponible en https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

[14] MARTINEZ, Graciela, Introducción a la creación de un CSIRT. Lacnic CSIRT. Disponible en https://onthemove.lacnic.net/wp-content/uploads/2020/08/lotm_csirt-amparo.pdf

Los servicios reactivos de un CSIRT de acuerdo con la definición de Lanfranco y Pérez[15], hacen referencia a la reacción frente a eventos o solicitudes, como por ejemplo código malicioso, vulnerabilidades en el software, un host comprometido o detección de intrusos.

Los servicios proactivos proporcionan información sobre cómo proteger a la comunidad y su infraestructura de posibles ataques anticipando que estos llegaran a suceder y reduciendo la probabilidad de que ocurran[16].

Los servicios de gestión de la calidad de la seguridad, tiene como fin concientizar a la comunidad sobre la seguridad de la información, realizar una correcta gestión del riesgo, brindar información útil para optimizar la seguridad de la información en una organización, ofrecer consultoría y asesoría para la mejora continua de las actividades y procesos[17].

- Infraestructura e instalaciones de un CSIRT

Dada la información confidencial y sensible que posee el CSIRT, se requiere que su instalación se realice en un espacio a puertas cerradas, que garantice el acceso limitado a dicha información. "*Se debe limitar el acceso a las instalaciones del* CSIRT con el fin de evitar el acceso no autorizado a los recursos y a la información. Con el mismo fin, el edificio o el área donde se encuentran las principales instalaciones CSIRT deben contar con vigilancia 24 horas"[18].

En cuanto a la infraestructura, la sugerencia de la OEA[19] en su guía de buenas prácticas es "*Los servidores, los equipos de comunicaciones, los dispositivos de seguridad lógica y los repositorios de datos pueden permanecer en un centro de datos o en las instalaciones del CSIRT, pero en todos los casos, el acceso físico y lógico a los equipos se regirá por un estricto control de acceso que garantice que se respeten las políticas de acceso a la información. Además de asegurar la información electrónica, el CSIRT*

[15] LANFRANCO, Einar y PÉREZ, Ernesto. ¿De qué se trata?, modelos posibles, servicios y herramientas. Disponible en https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2016/15551-EC/4B%201.pdf
[16] Ibid., p. 12
[17] Ibid., p. 12
[18] Buenas Prácticas para establecer un CSIRT nacional. Op cit.
[19] Ibid., p. 75.

mantendrá un depósito de seguridad para almacenar información sensible no digital, fichas, discos duros y servidores, entre otros". En virtud de que la información será custodiada y gestionada por el CSIRT, no se requiere la subcontratación de un proveedor para esta actividad.

- Métodos de trabajo para la gestión de incidentes del CSIRT

Conforme lo establece el Enisa[20], el primer paso es conocer los sistemas de TI que tiene instalados la organización, la generación de alertas, comunicados y advertencias, siguiendo el siguiente esquema:

- Recopilación de información
- Evaluación de la información sobre la pertinencia y la fuente
- Evaluación del riesgo basada en la información recopilada
- Distribución de la información

- Gestión de incidentes de seguridad del CSIRT

Con base en lo definido en la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información de MINTIC[21] los pasos a seguir en el manejo de un incidente son:

1. *"Planificación y preparación para la gestión del Incidente*
2. *Detección y análisis*
3. *Contención, erradicación y recuperación*
4. *Actividades Post-Incidente"*

[20] ENISA. Agencia de la Unión Europea para la seguridad Cibernética. Op cit.
[21] MINTIC. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

5.2. Marco Conceptual

CERT: Computer Emergency Response Team (Equipo de Respuesta ante Emergencias Informáticas). Conjunto de personas responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información.

CSIRT: Conforme lo establece la Guía de Seguridad (CCN-Stic-810) del Ministerio de Defensa del Gobierno de España y el Centro Criptográfico Nacional[22], el CERT corresponde a "un equipo multidisciplinar de expertos que trabaja según unos procesos definidos previamente y que disponen de unos medios determinados para implantar y gestionar, de un modo centralizado, todas y cada una de las medidas necesarias para mitigar el riesgo de ataques contra los sistemas de la Comunidad a la que presta el servicio y responder de forma rápida y efectiva en caso de producirse".

De acuerdo con el FIRST CSIRT Services Framework Versión 2.1 un CSIRT correctamente implementado tiene un mandato claro, un modelo de gobernanza, un marco de servicios a medida, tecnologías y procesos para proporcionar, medir y mejorar continuamente los servicios definidos.

SOC: Centro de Operaciones de Seguridad SOC, tiene la finalidad de realizar actividades de monitoreo, detección y análisis de incidentes previo a que se materialicen. Suministran la información necesaria para detectar brechas de seguridad de manera eficiente, para posteriormente ser mitigadas por medio de la implementación de controles, agilizando los tiempos de respuesta en dichos eventos.

Equipo de respuesta a incidentes de seguridad informática: un equipo de respuesta a incidentes de seguridad informática es una unidad organizativa (que puede ser virtual) o una capacidad que proporciona servicios y apoyo a un grupo definido para prevenir, detectar, manejar y responder a incidentes de seguridad informática, de acuerdo con su misión.

[22] El cual establece la guía de creación de un CERT / CSIRT. Disponible en https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/520-ccn-stic-810-guia-de-creacion-de-cert-s.html

Gestión de eventos de seguridad de la información: La gestión de eventos de seguridad de la información tiene como objetivo identificar los incidentes de seguridad de la información basados en la correlación y el análisis de eventos de seguridad de una amplia variedad de eventos y fuentes de datos contextuales.

ISO 27001: Norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

Servicio: Conjunto de acciones coherentes y reconocibles encaminadas a un resultado determinado para los mandantes de un equipo de intervención en caso de incidentes, o en su nombre. Lista de funciones utilizadas para realizar el servicio. (Marco de servicios SIRT V 1.0).

Equipo de intervención en caso de incidentes de seguridad de productos (PSIRT) – Equipo dentro de una entidad comercial (normalmente un operador) que gestiona la recepción, investigación y la notificación interna o pública, de información de seguridad sobre vulnerabilidades relativas a productos o servicios comercializados por esa organización. (Marco de servicios SIRT V 1.0).

Gestión de incidentes: servicios relativos a la gestión de eventos de ciberseguridad destinados a incorporar a los mandantes que lanzan la alerta y las actividades de coordinación relacionadas con la respuesta, la mitigación y la recuperación en caso de incidente. La gestión de incidentes depende de las actividades de análisis que se definen en la sección "Análisis". (Marco de servicios SIRT V 1.0).

Rastreo de incidentes: documentación de información sobre acciones tomadas para resolver un incidente, por ejemplo, información crítica recopilada, análisis realizados, pasos tomados en la resolución y mitigación, y cierre y resolución. (Marco de servicios SIRT V 1.0).

Ambiente (de desarrollo, pruebas o producción): “Es la infraestructura tecnológica (hardware y software) que permite desarrollar, probar o ejecutar todos los elementos o componentes para ofrecer un servicio de Tecnologías de la Información”.

Confidencialidad: La confidencialidad es la propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados. Asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización

Control: Conjunto de políticas, procedimientos, mecanismos empleados para el procesamiento de la información que permiten dar cumplimiento a los niveles de riesgos de seguridad de la información en u grado inferior al nivel de riesgo asumido.

Control preventivo: Mecanismo empleado para anticipar la materialización de un riesgo.

Control correctivo: Procedimiento orientado a la eliminación de las causas detonantes de un riesgo materializado antes que produzca pérdidas considerables.

Disponibilidad: Propiedad de que la información y sus recursos relacionados deben estar disponibles y utilizables cuando sean requeridos. La disponibilidad es la característica de la información de encontrarse disponible para quienes deban acceder a ella. Esto contempla usuarios, procesos o aplicativos.

Estrategia TI: Es el conjunto de principios, objetivos y acciones concretas que reflejan la forma en la cual una entidad decide utilizar las Tecnologías de la Información para permitir el logro de su misión de una manera eficaz. La Estrategia TI es una parte integral de la estrategia de una entidad.

Evaluación de riesgos: Proceso global de identificación, análisis y estimación de riesgos.

Integridad: Propiedad de salvaguardar la exactitud de la información y sus métodos de procesamiento deben ser exactos. Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. La integridad es mantener con exactitud la información

tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

Mejores prácticas: Conjunto de acciones que han sido implementadas con éxito en varias organizaciones, siguiendo principios y procedimientos adecuados.

CIS CONTROL: Conjunto de acciones priorizadas que colectivamente forman un conjunto de mejores prácticas de defensa que mitigan los ataques más comunes contra sistemas y redes.

Servicios Reactivos: Surgen de la explotación de una vulnerabilidad o materialización de un incidente de seguridad relacionado con la infraestructura tecnológica.

Servicios Proactivos: Realiza las actividades necesarias para proteger la infraestructura tecnológica con el objetivo de evitar ataques o incidentes de ciberseguridad.

5.3. Marco Legal

Cuadro 1. Marco Normativo

Artículo	Descripción
Ley 1273 de 2009	
269A	Acceso abusivo a un sistema informático.
269B	Obstaculización ilegítima del sistema informático o red de telecomunicación.
269C	Interceptación de datos informáticos.
269D	Daño Informático
269E	Uso de software malicioso
269F	Violación de datos personales.
269H	Circunstancias de agravación punitiva.
269I	Hurto por medios informáticos y semejantes.
269J	Transferencia no consentida de activos.
Artículo	**Descripción**
Ley 527 de 1999	
Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.	
Ley 599 de 2000	
58	**Numeral 17**
	Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.
Ley 842 de 2003	
31	b) Custodiar y cuidar los bienes, valores, documentación e información que, por razón del ejercicio de su profesión, se le hayan encomendado o a los cuales tenga acceso; impidiendo o evitando su sustracción, destrucción, ocultamiento o utilización indebidos, de conformidad con los fines a que hayan sido destinados.
	f) Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder.
32	g) Causar, intencional o culposamente, daño o pérdida de bienes, elementos, equipos, herramientas o documentos que hayan llegado a su poder por razón del ejercicio de su profesión.

35	b) Respetar y hacer respetar todas las disposiciones legales y reglamentaras que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones.
	c) Velar por el buen prestigio de estas profesiones.
39	a) Mantener el secreto y reserva, respecto de toda circunstancia relacionada con el cliente y con los trabajos que para él se realizan, salvo obligación legal de revelarla o requerimiento del Consejo Profesional respectivo.
53	a) Derivar, de manera directa o por interpuesta persona, indebido o fraudulento provecho patrimonial en ejercicio de la profesión, con consecuencias graves para la parte afectada.
	e) Incurrir en algún delito que atente contra sus clientes, colegas o autoridades de la República, siempre y cuando la conducta punible comprenda el ejercicio de la ingeniería o de alguna de sus profesiones auxiliares.
Ley 1581 de 2012	
Por la cual se dictan disposiciones generales para la protección de datos personales.	
Decreto 0032 de 2013	
Comisión Nacional Digital y de Información Estatal	
CONPES 3701 DE 2011	
Lineamiento de Políticas de Ciberseguridad y Ciberdefensa	
CONPES 3854 DE 2016	
Política Nacional de Seguridad Digital	
CONPES 3995 DE 2020	
Política Nacional de Confianza y Seguridad Digital	

Fuente: Del Autor

Ley 1273 de 2009 Tiene como objeto crear 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.

Ley 527 de 1999 Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 599 de 2000 Por la cual se expide el Código Penal.

Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales" la cual tiene como objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Decreto 0032 de 2013 Su objeto es la coordinación y orientación superior de la ejecución de funciones y servicios públicos relacionados con el manejo de la información pública, el uso de infraestructura tecnológica de la información para la interacción con los ciudadanos y el uso efectivo de la información en el Estado Colombiano, emitir los lineamientos rectores del Grupo de Respuesta a Emergencias Cibernéticas de Colombia del Ministerio de Defensa Nacional y asesorar al Gobierno Nacional en materia de políticas para el sector de tecnologías de la información y las comunicaciones, de conformidad con la definición que de éstas hace la Ley.[23]

CONPES 3701 DE 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa. Señala los logros alcanzados con la creación del COLCERT[24] del Ministerio de Defensa, el Comando Conjunto Cibernético (CCOC) de las Fuerzas Militares y el Centro Cibernético de la Policía Nacional (CCP).

CONPES 3854 DE 2016 Política Nacional de Seguridad Digital. Señala los logros alcanzados con la creación del COLCERT del Ministerio de Defensa, el Comando Conjunto Cibernético (CCOC) de las Fuerzas Militares y el Centro Cibernético de la Policía Nacional (CCP).[25]

[23] Por el cual se crea la Comisión Nacional Digital y de Información Estatal para uso de manera efectivo de la información del país. Disponible en https://www.mintic.gov.co/portal/604/articles-3602_documento.pdf

[24] Organismo coordinador a nivel nacional en aspectos de ciberseguridad y ciberdefensa y tiene como misión la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional. Disponible en http://www.colcert.gov.co/

[25] Departamento Nacional de Planeación. Mintic. Compes 3854, pág. 13. Consejo Nacional de Política Económica y Social. Disponible https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

CONPES 3995 DE 2020: Política nacional de confianza y seguridad digital, la cual amplía el marco de acción en la formulación de políticas de seguridad cibernética, con la finalidad de permitir que los ciudadanos y los sectores económicos continúen con la adopción de estas políticas, y que se aproveche el enfoque basado en la gestión de riesgos.[26]

[26] Conpes 3995 de 2020. Política Nacional de Confianza y Seguridad Digital. Disponible en https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

6. DISEÑO METODOLÓGICO

El desarrollo de este proyecto está basado en la práctica del análisis documental mediante el uso de una revisión sistemática la cual emplea diferentes bases de datos que fueron consultadas a través del servicio de e-Biblioteca de la UNAD. Se compiló, clasificó y seleccionó documentación relacionada con el tema de estudio hallado mediante consultas en Internet lo cual arrojó información de fuentes tales como: e-libros, revistas, foros, conferencias para su posterior análisis mediante lectura crítica intertextual[27] la cual permitió interrelacionar los resultados expuestos a través de las diferentes fuentes consultadas y asociarlos al ámbito laboral actual; logrando un acercamiento con la implementación del diseño del CSIRT para la empresa Platino Sistemas.

El desarrollo de esta metodología posibilita la ejecución de un análisis comparativo de los diferentes planteamientos y posturas encontradas en las diversas consultas, así como en las definiciones de los diferentes actores del tema caso de estudio.

Lo anterior sugiere un desarrollo por etapas que contemplan las siguientes Fases:

- Fase 1: Recopilación de la Información
- Fase 2: Análisis e Interpretación de la Información
- Fase 3: Diseño de Estructura Organizacional y alcances.
- Fase 4: Definición de Servicios y propuesta de herramientas de Hardware y Software.
- Fase 5: Diseño de ambiente virtualizado con mínimos requeridos.

[27] SUAREZ, Ángela (2019). TRES NIVELES DE LECTURA [Sitio web]. Disponible en https://eclipsegrafia.blogspot.com/2019/06/tres-niveles-de-lectura.html

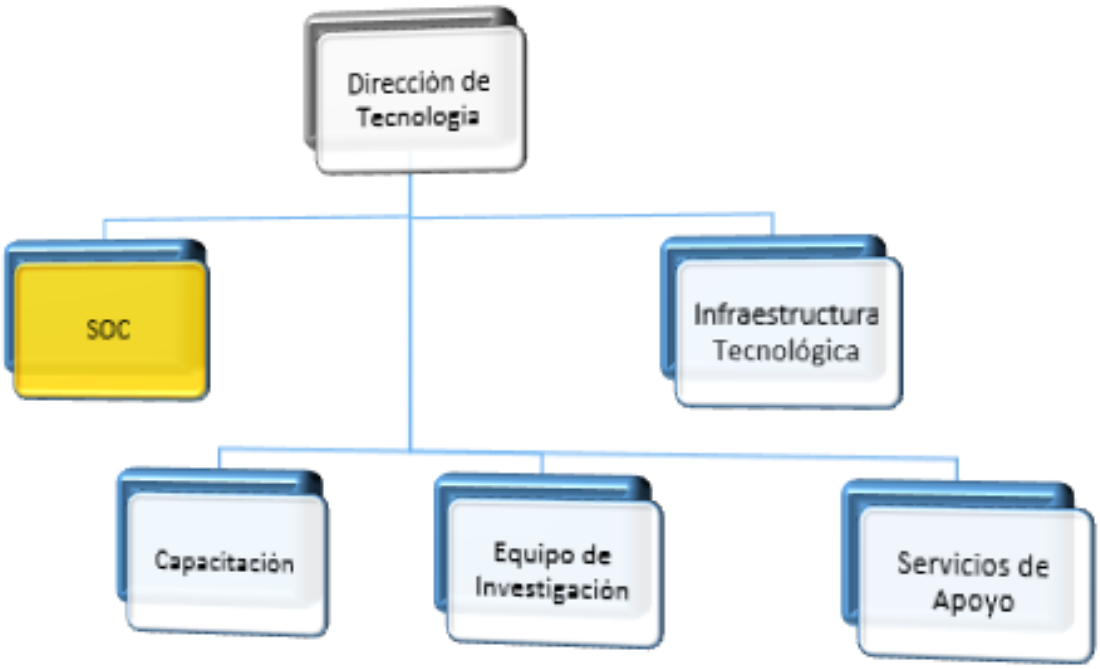
7. DESARROLLO DE LOS OBJETIVOS

7.1 Estructura Organizacional Y Capacidades De Las Operaciones Del Soc.

7.1.1 Estructura Organizacional

Teniendo en cuenta la importancia de la interacción que debe haber entre los diferentes directivos de Platino Sistemas, se considera necesario que el CSIRT este encabezado por la Dirección de Tecnología, del cual se desprenderán las áreas fundamentales para sus actividades tal como se evidencia en la Figura 1.

Figura 1. Estructura Organizacional CSIRT



Fuente: De autor

7.1.2 Áreas, Responsabilidades y Roles

Cuadro 2. Director de Tecnología

Número	1
Nombre del puesto:	Director de Tecnología
Objetivo	Controlar y organizar los procesos del laboratorio CSIRT.
Responsabilidades	- Planificar y dirigir al equipo. - Aprobar actividades del CSIRT. - Llevar el control de los avances del equipo. - Verificar el cumplimiento de las actividades programadas. - Elaborar informes y reportes periódicos - Aplicar estrategias con la aprobación de la alta gerencia. - Notificación a los directivos de otras áreas
Perfil y Capacidades	- Grado académico de Magíster en Seguridad de la Información - Capacidad de actuar autónomamente. - Tener iniciativa para aportar soluciones o alternativas novedosas. - Capacidad de comunicación efectiva. - Capacidad de relación interpersonal. - Tener motivado al equipo de trabajo. - Capacidad de razonamiento y diseño para resolución de problemas. - Demostrar conocimiento y comprensión del CSIRT

Fuente: Del Autor

Cuadro 3. Director SOC

Número	2
Nombre del puesto:	Director SOC
Objetivo	Monitorear y gestionar incidentes de seguridad informática
Responsabilidades	- Administrar y gestionar el Centro de operaciones de seguridad Monitoreo y análisis de incidente - Realizar tareas de detección de posibles incidentes de seguridad. - Establecer procedimientos operativos para garantizar una efectiva monitorización. - Coordinar, dirigir, planear y evaluar la utilización de las herramientas de monitoreo. - Administrar y resguardar información sensible de monitoreo. - Recomendar mejoras para el proceso de monitoreo. - Recopilar, investigar y analizar nuevos desarrollos técnicos, actividades de intrusos y tendencias relacionadas para ayudar a identificar futuras amenazas. - Reportar el avance de sus tareas.

	- Cumplir con las actividades programadas. - Elaborar informes y reportes periódicos.
Perfil y Capacidades	- Título universitario en TI - Especialización en seguridad Informática - Experiencia y formación en el área. - Tener iniciativa y ser resolutivo. - Capacidad de monitorización de redes. - Actuar con responsabilidad y ética profesional. - Capacidad de integrarse rápidamente. - Trabajo en equipo. - Poseer habilidades de aprendizaje. - Capacidad de razonamiento, resolución y análisis

Fuente: Del Autor

Cuadro 4. Coordinador de formación

Número	**3**
Nombre del puesto:	Coordinador de formación
Objetivo	Proveer información acerca de actividades principales de la seguridad de la información.
Responsabilidades	- Dar capacitaciones en seguridad informática. - Ejecución de talleres, cursos, tutoriales. - Transmisión de pautas para la resolución de incidentes. - Recomendar mejoras para los procesos de capacitación. - Recopilar, investigar y analizar nuevos desarrollos técnicos, actividades de intrusos y tendencias relacionadas para ayudar a identificar futuras amenazas. - Llevar un control de las capacitaciones. - Reportar el avance de sus tareas. - Cumplir con las actividades programadas. - Elaborar informes y reportes periódicos
Perfil y Capacidades	- Formación en docencia - Experiencia y formación en el área. - Tener iniciativa y ser resolutivo. - Capacidad de liderazgo. - Actuar con responsabilidad y ética profesional. - Capacidad de integrarse rápidamente. - Trabajo en equipo. - Poseer habilidades de aprendizaje. - Capacidad de comunicación efectiva. - Capacidad de relación interpersonal.

Fuente: Del Autor

Cuadro 5. Líder Infraestructura tecnología

Número	4
Nombre del puesto:	Líder Infraestructura tecnología
Objetivo	Administración, monitoreo y aprovisionamiento de la infraestructura tecnológica
Responsabilidades	- Administrar la infraestructura de IT - Monitoreo de IT - Generación de alertas tempranas de IT - Aprovisionar infraestructura de acuerdo a requerimientos - Generar reportes de uso y capacidades de IT - Gestionar copias de seguridad de IT
Perfil y Capacidades	- Título universitario en informática o carreras afines - Experiencia y formación en el área. - Ser proactivo - Trabajo bajo presión - Tener iniciativa y ser resolutivo. - Actuar con responsabilidad y ética profesional. - Capacidad de integrarse rápidamente. - Trabajo en equipo. - Poseer habilidades de aprendizaje. - Capacidad de razonamiento, resolución y análisis

Fuente: Del Autor

Cuadro 6. Equipo de investigación

Número	5
Nombre del puesto:	Equipo de investigación
Objetivo	Realizar labores de investigación científica y tecnológica.
Responsabilidades	- Diseñar e implementar proyectos de investigación. - Fortalecer la investigación del CSIRT. - Realizar investigación para la publicación de alertas y advertencias de seguridad. - Reportar el avance de sus tareas. - Participar en evento de difusión de proyectos. - Cumplir con las actividades programadas. - Elaborar informes y reportes periódicos.
Perfil y Capacidades	- Título universitario en TI - Especialización en seguridad Informática - Experiencia y formación en el área. - Tener iniciativa y ser resolutivo. - Capacidad de investigación. - Actuar con responsabilidad y ética profesional. - Trabajo en equipo. - Poseer habilidades de aprendizaje. - Colaborar con otros grupos o investigadores.

Fuente: Del Autor

Cuadro 7. Analista financiero

Número	6
Nombre del puesto:	Analista financiero
Objetivo	Coordinar servicios administrativos y de apoyo logístico.
Responsabilidades	- Registrar plan de compras de bienes. - Planificar, organizar, dirigir y controlar presupuestos y financiamientos del CSIRT. - Proponer mejoras para optimizar recursos y servicios. - Establecer cronogramas de ejecución. - Reportar el avance de sus tareas. - Cumplir con las actividades programadas. - Elaborar informes y reportes periódicos
Perfil y Capacidades	- Analista Financiero, profesional en administración o carreras afines. - Experiencia y formación en el área. - Tener iniciativa y ser resolutivo. - Capacidad administrativa y financiera. - Actuar con responsabilidad y ética profesional. - Capacidad de integrarse rápidamente. - Trabajo en equipo. - Poseer habilidades de aprendizaje. - Tener motivación.

Fuente: Del Autor

Cuadro 8. Abogado

Número	7
Nombre del puesto:	Abogado
Objetivo	Brindar apoyo en asuntos legales.
Responsabilidades	- Redacción de políticas, procedimientos, cláusulas y el desarrollo de prácticas, para prevenir los ciberataques en la empresa. - Asesoría en la recopilación de evidencias, seguimiento y gestión en la custodia de pruebas, preparación de procesos judiciales, comunicación con los cuerpos de seguridad del Estado.
Perfil y Capacidades	- Profesional jurídico - Conocimiento en leyes y normatividad en el ámbito de seguridad informática. - Tener iniciativa y ser resolutivo. - Ayudar en la resolución de conductas antisociales a nivel de ciberseguridad. - Actuar con responsabilidad y ética profesional. - Capacidad de integrarse rápidamente. - Trabajo en equipo. - Poseer habilidades de aprendizaje. - Tener motivación.

Fuente: Del Autor

7.1.3 Capacidades de las Operaciones del SOC

7.1.3.1 Organigrama SOC

La figura 2 representa la estructura organizativa con los diferentes perfiles que componen el Centro de Operaciones de Seguridad de la empresa Platino Sistemas:

Figura 2. Organigrama SOC

Fuente: De autor

7.1.3.2 Perfiles y Roles del SOC

Cuadro 9. Director SOC

Número	1
Nombre del puesto:	Director del SOC
Responsabilidades	Será el encargado de la coordinación, planeación y toma de decisiones en la operación del SOC, debe garantizar las herramientas y recursos necesarios que permitan la atención de incidentes o eventos críticos en los que se vea afectada de forma grave la información o la infraestructura. Autoriza los procedimientos y lineamientos para el tratamiento de incidentes o actividades sospechosas.
Perfil y Capacidades	- Título universitario en TI - Especialización en seguridad Informática - Experiencia y formación en el área.

	- Tener iniciativa y ser resolutivo. - Capacidad de monitorización de redes. - Actuar con responsabilidad y ética profesional. - Capacidad de integrarse rápidamente. - Trabajo en equipo. - Poseer habilidades de aprendizaje. - Capacidad de razonamiento, resolución y análisis

Fuente: Del Autor

Cuadro 10. Gestor de Incidentes

Número	2
Nombre del puesto:	Gestor de Incidentes
Responsabilidades	Será el encargado de analizar incidentes, monitorear, registrar y proporcionar respuesta a los incidentes. Coordina respuesta a incidentes. Colabora con otros grupos de respuesta o técnicos para resolver un incidente.
Perfil y Capacidades	- Experiencia en gestión de incidentes de ciberseguridad - Experiencia en seguridad informática - Experiencia en clasificación de incidentes.

Fuente: Del Autor

Cuadro 11. Técnico L1

Número	6
Nombre del puesto:	Técnico L1
Responsabilidades	Será el encargado de realizar el monitoreo de la infraestructura tecnológica mediante el correlacionador SIEM, identifica falsos positivos y actividades sospechosas, notifica posibles incidentes de seguridad, efectúa actividades de contención ya sean reactivas o proactivas, analiza el tipo de actividad sospechosa, registra eventos de actividades sospechosas, entregará información que permita la investigación de un evento
Perfil y Capacidades	- Conocimientos en TCP/IP - Conocimientos en Seguridad Informática - Experiencia en análisis de intrusión.

Fuente: Del Autor

Cuadro 12. Especialista de Seguridad

Número	3
Nombre del puesto:	Especialista de Seguridad

Responsabilidades	- Será el encargado de realizar investigaciones específicas de ciberseguridad. - Desarrolla material técnico para el uso interno o de formación. - Supervisa ejecución de monitoreo. - Desarrolla herramientas. - Registrarse y mantener contacto con las entidades gubernamentales de seguridad, para dar gestión a los avisos de seguridad emitidos por dichas entidades.
Perfil y Capacidades	- Conocimientos en ciberseguridad. - Experiencia en análisis de intrusión. - Experiencia en gestión de eventos de ciberseguridad. - Conocimiento en el conjunto de normas de la ISO/IEC 27000 y afines.

Fuente: Del Autor

Cuadro 13. Analista L1

Número	5
Nombre del puesto:	Analista L1
Responsabilidades	Será el encargado de apoyar la gestión de interpretar actividades sospechosas, incidentes de seguridad, o falsos positivos, apoya en la definición de procedimientos para el tratamiento de incidentes de seguridad o actividades sospechosas, gestiona los eventos escalados por el operador, identifica y notifica los incidentes o actividades sospechosas de acuerdo al nivel de servicio.
Perfil y Capacidades	- Conocimientos en TCP/IP - Certificación en Seguridad de la información - Experiencia en análisis de intrusión. - Conocimiento en el conjunto de normas de la ISO/IEC 27000 y afines.

Fuente: Del Autor

Cuadro 14. Experto Forense

Número	4
Nombre del puesto:	Experto de Forense
Responsabilidades	Será responsable de investigar robos de datos y otros incidentes de seguridad, desmantelar y reconstruir sistemas dañados para recuperar información perdida, identificar sistemas o redes adicionales comprometidas en ataques cibernéticos, recopilación de evidencia útil en procesos legales, elaborar reportes técnicos sobre los casos investigados.
Perfil y Capacidades	- Conocimientos en Informática Forense - Experiencia en análisis forense. - Conocimientos en legislación informática

	- Manejo de evidencias digitales - Experiencia en procesos judiciales informáticos.

Fuente: Del Autor

Cuadro 15. Técnico Forense L1

Número	6
Nombre del puesto:	Técnico Forense L1
Responsabilidades	- Reconstrucción sistemas dañados para recuperar información perdida. - Identificar sistemas o redes adicionales comprometidas en ataques cibernéticos. - Recopilar evidencia útil en procesos legales. - Elaboración de reportes técnicos.
Perfil y Capacidades	- Conocimientos en Informática Forense - Experiencia en análisis forense.

Fuente: Del Autor

El Centro de operaciones de seguridad SOC por sus actividades de monitoreo y gestión de incidentes se considera una de las áreas más críticas y fundamentales. Este centro realiza las acciones necesarias para la gestión adecuada de los incidentes reactivos y proactivos.

Las responsabilidades del SOC estarán enfocadas en el monitoreo de la infraestructura tecnológica que soporta las aplicaciones y servicios de Platino Sistemas, lo que permitirá detectar los incidentes de seguridad mediante funciones de control, herramientas tecnológicas especializadas y la gestión de la información de la empresa, para de esta manera garantizar la confidencialidad, integridad y disponibilidad de la información de la organización.

Con el fin de que las amenazas cibernéticas puedan ser combatidas de manera óptima y oportuna, la operación se llevará a cabo las 24 horas de los 7 días de la semana.
Cuando sean reportados incidentes deberán ser clasificados y asignados conforme a los ANS suscritos con sus clientes para su posterior gestión basados en los diferentes tipos de servicios prestados por el SOC.

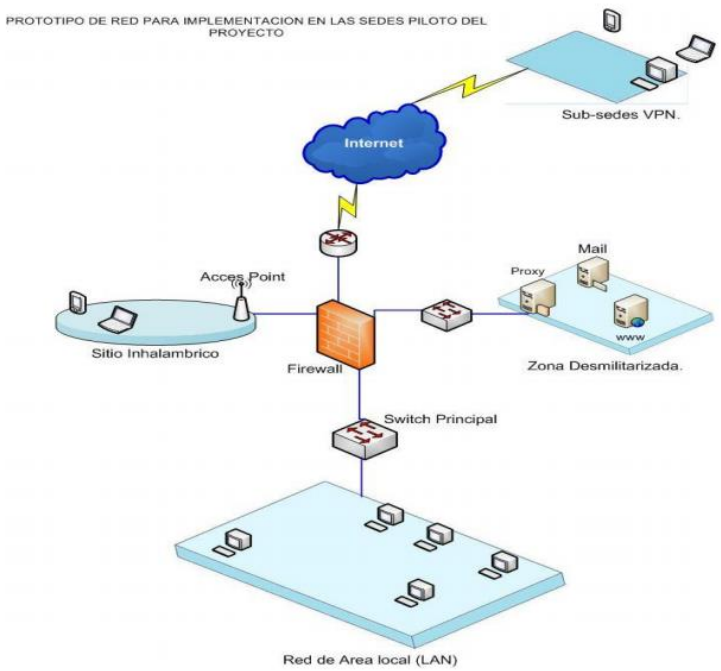
Cuando se detecten incidentes cibernéticos se contará con el apoyo del SIEM (Security Information and Event Management) para el registro y posterior reporte en caso de una auditoría.

Basados en las bondades del uso del software open source, AlienVault® OSSIM ™, es un producto de seguridad de la información y gestión de eventos (SIEM) que permite administrar eventos de seguridad. Esta solución está integrada por diferentes herramientas que posibilita la visualización de aspectos relacionados con la seguridad de la infraestructura y estado de la red.

Por lo anterior y por todas las capacidades de seguridad que ofrece está herramienta, se elige como plataforma unificada para el desarrollo de las tareas principales del SOC de la empresa Platino Sistemas.[28]

En la figura 3 se presenta la arquitectura del SOC con la herramienta AlientVault OSSIM.

Figura 3. Modelo típico de distribución de red por zonas.



Fuente: http://www.soccolombia.com/documentos/documento2.pdf

[28] AlienVault OSSIM. El SIEM de código abierto más utilizado del mundo. Disponible en https://cybersecurity.att.com/products/ossim

7.2 Políticas, Alcance y Servicios Propuestos por el SOC (Centro De Operaciones De Seguridad).

7.2.1 Políticas de Seguridad

Las siguientes políticas de seguridad de la información se encuentran alineadas a la norma ISO/IEC 27002.

Cuadro 16. Políticas de Seguridad

No.	Políticas de seguridad	Descripción de la política	Responsable
1	Política de control de acceso	Definición de los criterios de clasificación y acceso a la información.	Líder Infraestructura Tecnológica
2	Política de acceso a la información por parte de terceros	Clasificación de criterios de acceso de entes externas de la organización	Director General
3	Política de seguridad física	Lineamientos que ayudan a evitar accesos físicos no autorizados y daños contra la infraestructura tecnológica de la organización.	Director Administrativo
4	Política de seguridad de acceso a Internet	Criterios de seguridad de acceso a la red de Internet.	Líder Infraestructura Tecnológica
5	Política de gestión de vulnerabilidades	Criterios permitidos para la gestión de incidentes de seguridad.	Líder SOC
6	Política de escritorio y pantalla limpia	Lineamientos para la protección de documentos físicos, dispositivos removibles de almacenamiento, medios magnéticos y ópticos que contengan información sensible.	Líder SOC
7	Política de entrenamiento, capacitación y actualización	Establecer las directrices para el proceso de entrenamiento, capacitación y actualización del personal.	Coordinador de Formación
8	Política de selección de personal	Lineamientos de la organización para la implementación del proceso de incorporación.	Líder de Recursos Humanos
9	Política de finalización del contrato	Criterios que la organización aplica cuando se da la finalización del contrato laboral de un trabajador.	Líder de Recursos Humanos
10	Política de la seguridad del uso de equipos tecnológicos.	Criterios de aplicación de la seguridad informática sobre los dispositivos	Líder Infraestructura Tecnológica

No.	Políticas de seguridad	Descripción de la política	Responsable
		tecnológicos con los que cuenta la organización.	
11	Política de uso de correo electrónico	Lineamientos de la utilización del correo electrónico para fines exclusivos de la empresa.	Líder Infraestructura Tecnológica
12	Política de la seguridad de la red de computadoras	Lineamientos de seguridad para la protección de la información en redes informáticas de la organización.	Líder Infraestructura Tecnológica
13	Política de telecomunicación de la información	Lineamientos para el establecimiento de la comunicación por medio de equipos de telecomunicaciones entre la organización en sus diferentes sedes o con terceros.	Director de Tecnología
14	Política de uso de dispositivos móviles	Criterios de utilización de todos los dispositivos móviles que posee la organización.	Director Administrativo
15	Política de teletrabajo	Criterios de seguridad que permitan la protección de la información procesada o almacenada en los sitios en los que se lleve a cabo actividades de teletrabajo.	Líder Infraestructura Tecnológica
16	Política de la seguridad de los equipos de telecomunicaciones	Normas para la aplicación de niveles de seguridad para dispositivos de telecomunicación internos y externos.	Líder Infraestructura Tecnológica
17	Política de transferencia de información	Criterios que aseguren el intercambio de información dentro de la organización y con otras entidades.	Director de Tecnología
18	Política de la instalación de software	Criterios para prevenir explotación de vulnerabilidades de carácter técnico.	Jefe TIC
19	Política de copia de seguridad	Definir los lineamientos para el respaldo de la información que garantice la continuidad del negocio.	Líder Infraestructura Tecnológica
20	Política de protección contra software malicioso	Lineamientos que garanticen la continuidad del servicio de los sistemas de información de la organización.	Líder SOC
21	Política de controles criptográficos	Criterios enfocados a la protección de la información en caso que personal no autorizado tengo acceso a la información de la organización garantizando la confidencialidad o integridad de la misma.	Líder SOC
22	Política de privacidad y protección de la información personal identificable	Criterios de aplicabilidad que permitan asegurar la privacidad y la protección de la información de datos personales, de acuerdo a la normatividad vigente.	Líder SOC

No.	Políticas de seguridad	Descripción de la política	Responsable
23	Política de relación con los proveedores	Lineamientos que garanticen la protección de activos de la organización sujetos de acceso a los proveedores.	Director Administrativo
24	Gestión de soportes extraíbles	Directrices que garanticen la gestión, uso autorizado, control de acceso y demás relacionados con los medios extraíbles.	Líder Infraestructura Tecnológica
25	Gestión de acceso a los usuarios	Lineamientos que garanticen el acceso de los usuarios a los recursos de la organización, de acuerdo a los privilegios otorgados y que eviten el acceso a usuarios no autorizados.	Líder Infraestructura Tecnológica
26	Gestión de derechos de acceso privilegiados	Criterios que permitan la restricción y control de la asignación y uso de derechos de accesos privilegiados.	Líder Infraestructura Tecnológica
27	Sistema de gestión de contraseñas	Lineamientos que contemplen la creación, uso, protección, distribución, renovación o destrucción de las contraseñas de acceso a los recursos de la organización proporcionadas a los usuarios.	Líder Infraestructura Tecnológica
28	Acuerdos de confidencialidad	Lineamientos que permitan la protección de la información regulando los requisitos para los acuerdos de confidencialidad acordes a las necesidades de la organización.	Director General
29	Derechos de propiedad intelectual	Directrices que permitan dar cumplimiento a requisitos de orden legal, reglamentarios y contractuales relacionados con derechos de propiedad intelectual y uso de software registrado.	Director de Tecnología
30	Protección de los datos y privacidad de la información personal	Criterios que permitan garantizar el aseguramiento de la privacidad y protección de datos personales de acuerdo a lo establecido por la normatividad vigente.	Líder SOC

Fuente: Del Autor

7.2.2 Alcance del SOC

El SOC realizará el monitoreo de la infraestructura tecnológica que soporta las aplicaciones y servicios que ofrece Platino Sistemas, mediante determinados procedimientos que ayudaran a la detección de intrusiones que comprometan la seguridad de la información. Se gestionarán los incidentes y se proveerán los

mecanismos que se requieran para dar respuesta en el menor tiempo posible, garantizando la continuidad del negocio y restaurando el servicio del activo afectado ocasionando el impacto mínimo.

El SOC estará conformado el director del SOC, analistas de seguridad y operadores, los cuales tendrán las responsabilidades que se indican a continuación.

7.2.3 Servicios Propuestos por el SOC

Los servicios reactivos se focalizan en la gestión de los incidentes y en mitigar los daños que se ocasionen, en cuanto a los servicios proactivos se centran en la prevención de incidentes de ciberseguridad por medio de la implementación de herramientas para el monitoreo y la detección temprana de riesgos, además se encarga de la formación y sensibilización al personal de la empresa y sus clientes.

El SOC ofrecerá los siguientes servicios reactivos y proactivos.

Tabla 1. Servicios del SOC

Servicios Reactivos	Servicios Proactivos
Reporte y alertas de incidentes	Monitoreo
Análisis de incidentes	Escaneo de vulnerabilidades
Clasificación de incidentes	Capacitación
Tratamiento de incidentes	Análisis de riesgos
Respuesta a incidentes	Análisis forense

Fuente: Del Autor

7.3 Herramientas Tecnológicas de Hardware y Software para el Desarrollo de las Actividades Propias del CSIRT.

7.3.1 Herramientas de Software.

Tabla 2. Herramientas de Software

Nombre de servicio	Plataforma	URL
Servidor Web	XAMPP	https://www.apachefriends.org/es/index.html
Correo institucional	Postfix	http://www.postfix.org/start.html
Intranet	XAMPP	https://www.apachefriends.org/es/index.html
Servidor de Archivos	Samba	https://www.samba.org/
Copias de Seguridad	Veeam Backup	https://www.veeam.com/es/vm-backup-recovery-replication-software.html?ad=in-text-link
Servidor DNS	Bind	https://www.isc.org/bind/
Servidor de Monitoreo	Pandora FMS	https://pandorafms.com/
Servidor de Sandbox	Firejail	https://ubunlog.com/firejail-ejecuta-aplicaciones-ubuntu/
Correlacionador de eventos	Alient Vault Ossim	https://cybersecurity.att.com/products/ossim
Registro y Seguimiento de incidentes	osTicket	https://osticket.com/
Servicios especiales (Informática Forense)	Sans Dfir	https://digital-forensics.sans.org/

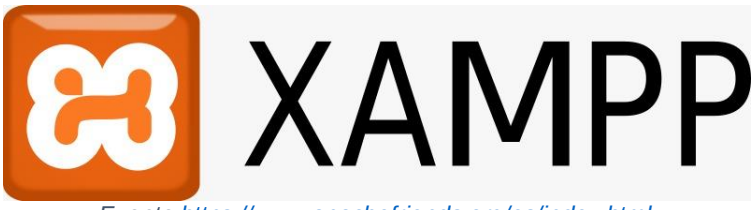
Fuente: Del Autor

7.3.1.1 Servidor WEB - XAMP:

Se realizará la publicación de alertas de seguridad con base a los reportes enviados en los boletines enviados por los principales equipos de respuesta a incidentes de seguridad informática en Colombia.

Para esto se utilizará la plataforma Xampp que es una distribución gratuita de Apache que contiene MariaDB, PHP y Perl.

Figura 4. Servidor WEB XAMPP.



Fuente https://www.apachefriends.org/es/index.html

Requerimientos de instalación:

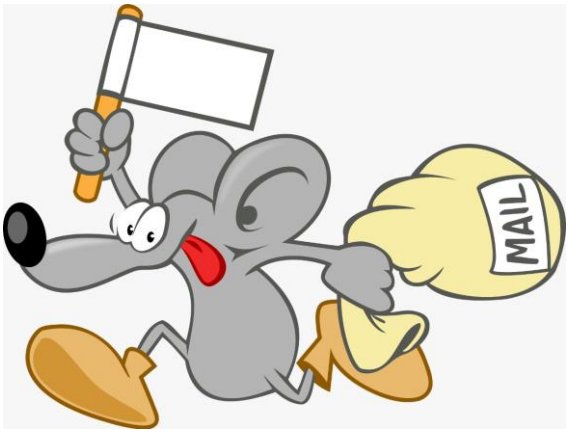
- RAM de 1 GB
- Espacio en disco de 120 GB
- CPU de 4 core
- MySQL 5.0.41
- PHP 5.2.2
- PHP 4.4.7
- phpMyAdmin 2.10.1

7.3.1.2 Servicio de correo electrónico - POSTFIX:

Se encarga de la administración de las cuentas de correo, buzones, grupos de correo y mensajes electrónicos de la empresa.

Para esto se utilizará la plataforma Postfix, el cual fue creado a partir de código fuente el cual puede ser ejecutado en sistemas similares a UNIX, incluidos AIX, BSD, HP-UX, Linux, MacOS X, Solaris y más. Postfix también se distribuye como código listo para ejecutar por proveedores de sistemas operativos, proveedores de dispositivos y otros proveedores.

Figura 5. Servidor Correo Electrónico Postfix.



Fuente http://www.postfix.org/start.html

Requerimientos de instalación:

- RAM de 4 GB
- Espacio en disco de 150 GB
- CPU de 4 core

7.3.1.3 Servicio de Intranet - XAMPP:

Se realizará la publicación de información relevante relacionada con el CSIRT, para esto se implementará la plataforma XAMPP.

Requerimientos de instalación:

- RAM de 1 GB
- Espacio en disco de 120 GB
- CPU de 4 core
- MySQL 5.0.41
- PHP 5.2.2
- PHP 4.4.7
- phpMyAdmin 2.10.1

7.3.1.4 Servidor de Archivos - SAMBA:

Permite la administracion y distribución de archivos informáticos entre los clientes de una red. Para esto se implementará Samba.

Samba es software libre con licencia GNU General Public License, el proyecto Samba es miembro de Software Freedom Conservancy. Proporciona servicios de impresión y archivo seguros, estables y rápidos para todos los clientes que utilizan SMB (Sever Message Block).

Figura 6. Servicio de Archivos Samba.

Fuente https://cutt.ly/Zj8FRPw

Requerimientos de instalación:

- RAM de 4 GB
- Espacio en disco de 100 GB
- CPU de 2 core A 2 GHz

7.3.1.5 Servicio de Copias de Seguridad - VEEAM BACKUP & REPLICATION:

Su función es restablecer los servicios y plan de continuidad del negocio, para esto se utilizará la herramienta de Veeam Backup & Replication es una aplicación de copia de seguridad desarrollado para entornos virtuales basadas en VMware vSphere, Nutanix AHV, y Microsoft Hyper-V hipervisores. El software proporciona funciones de copia de seguridad, restauración y replicación para máquinas virtuales, servidores físicos y estaciones de trabajo, así como cargas de trabajo basadas en la nube.

Figura 7. Servicio de Copias de Seguridad VEEAM.

Fuente https://n9.cl/rfozl

Requerimientos de instalación:

- RAM de 4 GB
- Espacio en disco
    - 120 GB Sistema Operativo
    - 1 TB para Backup de VM
- CPU de 4 core
- Conexión de Red de 1 Gbps

7.3.1.6 Servidor DNS - BIND:

Se encarga de la administracion y asignación de nombres para poder validar continuamente las comunicaciones a través de red interna con la externa.

Para este servicio se utilizará la plataforma BIND la cual ofrece un sistema DNS muy flexible y de gran capacidad.

Figura 8. Servidor DNS BIND.

Fuente https://n9.cl/agm5

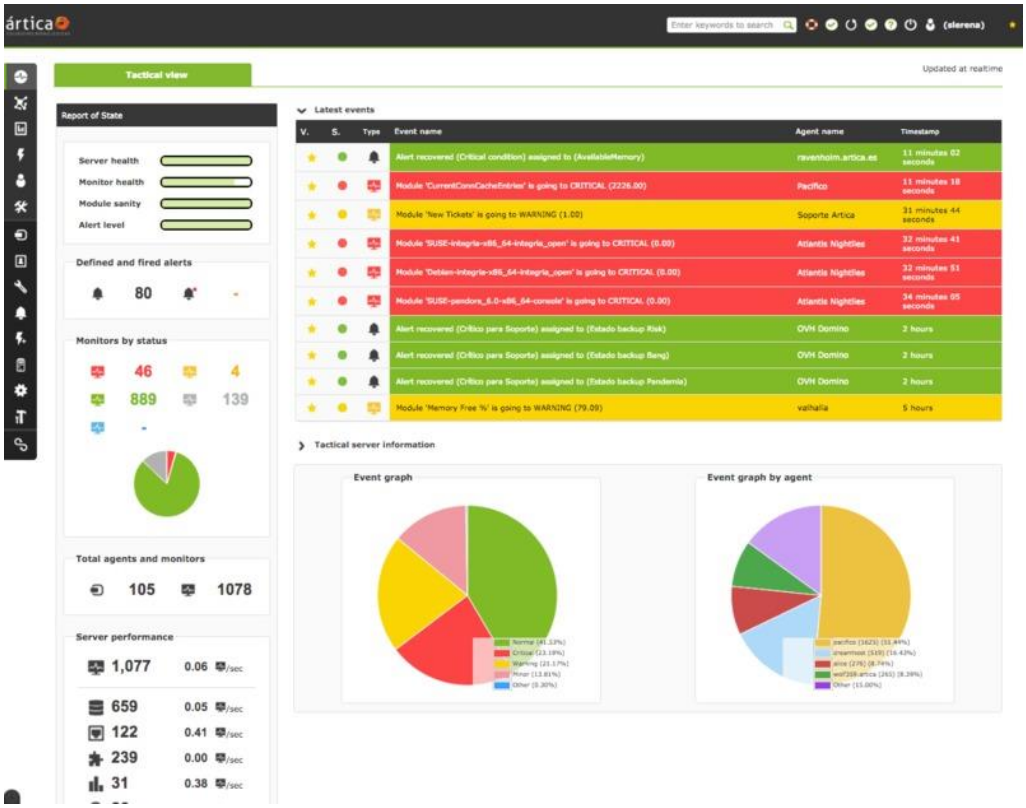
Requerimientos de instalación:

- RAM de 1 GB
- Espacio en disco de 100 GB
- CPU de 2 core

7.3.1.7 Servidor de Monitoreo - PANDORA FMS:

Almacena los incidentes de seguridad reactivos y proactivos, lo cual permite gestionar y dar respuesta de manera oportuna. Para esto se implementará la herramienta Pandora FMS la cual proporciona monitoreo a aplicaciones, sistemas o dispositivos de red, así mismo dispone de histórico de datos y eventos lo cual permite conocer el estado de los sistemas a lo largo del tiempo.

Figura 9. Servidor de Monitoreo PANDORA FMS.



Fuente https://upload.wikimedia.org/wikipedia/commons/3/34/Pandora6.0sp3-tactical-view.png

Requerimientos de instalación:

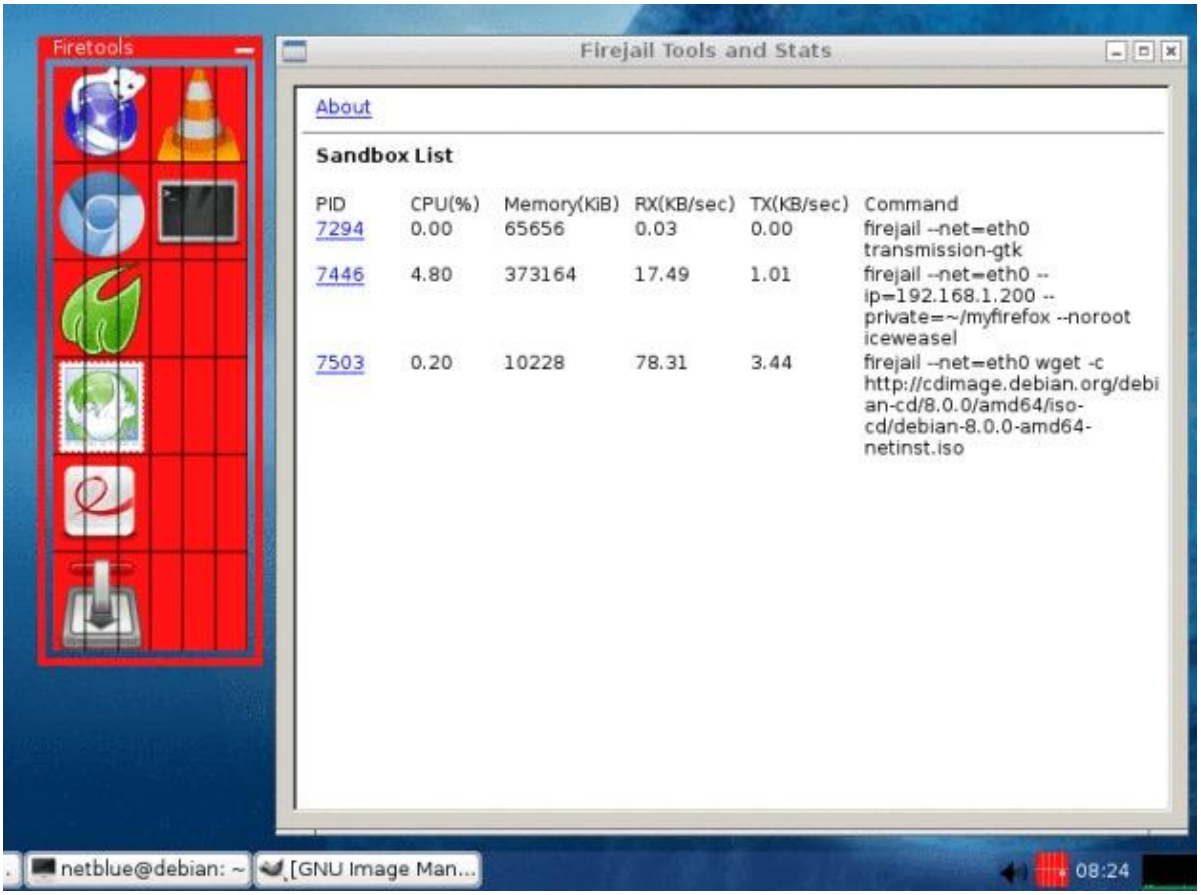
- RAM de 4 GB
- Espacio en disco de 100 GB
- CPU de 2 core a 2 GHz

7.3.1.8 Servidor de Sandbox - FIREJAIL:

Es un mecanismo de seguridad para disponer de un entorno aislado al de la red de producción, permite ejecutar desarrollo de software o programas de terceros para verificar el impacto que este tendrá en el entorno de producción.

Firejail es un programa SUID que reduce el riesgo de violaciones de seguridad al restringir el entorno de ejecución de aplicaciones no confiables que usan espacios de nombres y seccomp-bpf. Permite que un proceso y todos sus descendientes tengan su propia vista privada de los recursos del kernel compartidos globalmente, como la pila de red, la tabla de procesos, la tabla de montaje, etc.

Figura 10. Servidor de Sandbox Firejail.



Fuente https://n9.cl/40wl3

Requerimientos de instalación:

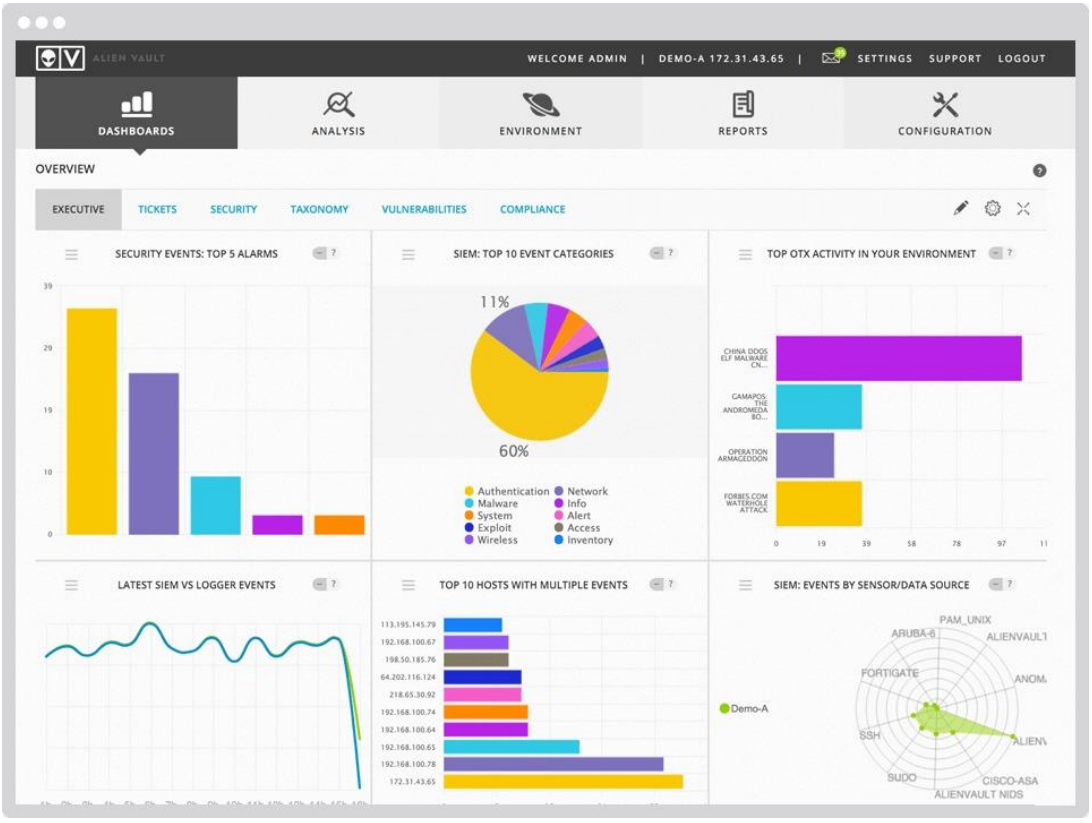
- RAM de 2 GB
- Espacio en disco de 100 GB
- CPU de 2 core a 2 GHz

7.3.1.9 Correlacionador de eventos - ALIENVAULT OSSIM:

Su principal función es administrar y analizar los eventos de los dispositivos de la red para buscar patrones, similitudes, para la detección de vulnerabilidades y ataques, también descarta los falsos positivos para ir optimizando el análisis de estos. Se realizará por medio de la herramienta de software AlienVault OSSIM.

AlienVault® OSSIM™, es un producto de seguridad de la información y gestión de eventos (SIEM) de código abierto de la empresa AlienVault, el cual proporciona un SIEM completo con recolección de eventos. Por lo anterior y por todas las capacidades de seguridad que ofrece está herramienta, se elige como plataforma unificada para el desarrollo de las tareas principales del SOC de la empresa Platino Sistemas.

Figura 11. Correlacionador de eventos Alien Vault OSSIM.



Fuente https://n9.cl/ozgvu

Requerimientos de instalación:

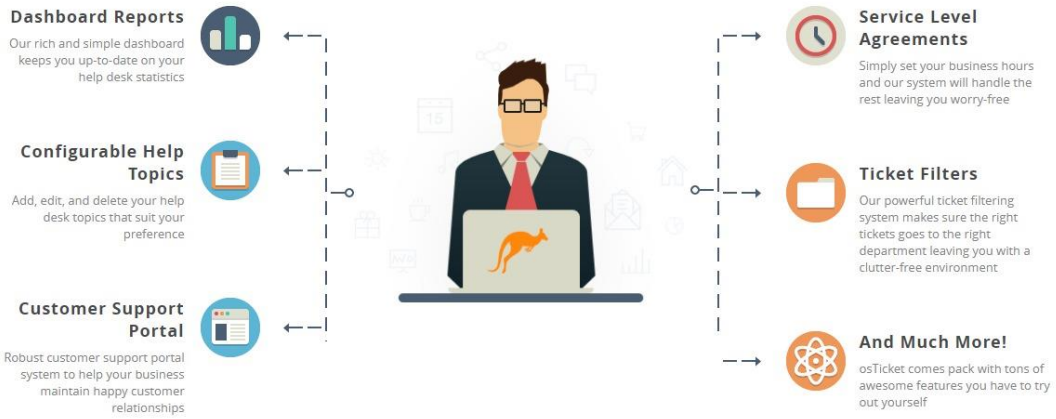
- RAM de 8 GB
- Espacio en disco de 100 GB
- CPU de 4 core a 2 GHz

7.3.1.10 Servicio Registro y seguimiento de Incidentes - OSTICKET:

Su principal función es brindar respuesta rápida y oportuna a sus incidentes reactivos y proactivos para llevar a cabo de una manera eficiente la gestión de casos, tener trazabilidad y seguimiento de estos se utilizará osTicket.

osTicket es un sistema de tickets de asistencia de código abierto. Dirige las consultas creadas a través de correo electrónico, formularios web y llamadas telefónicas hacia una plataforma de asistencia al cliente.

Figura 12. Servicio Registro y seguimiento de Incidentes OSTICKET.



Fuente https://osticket.com/

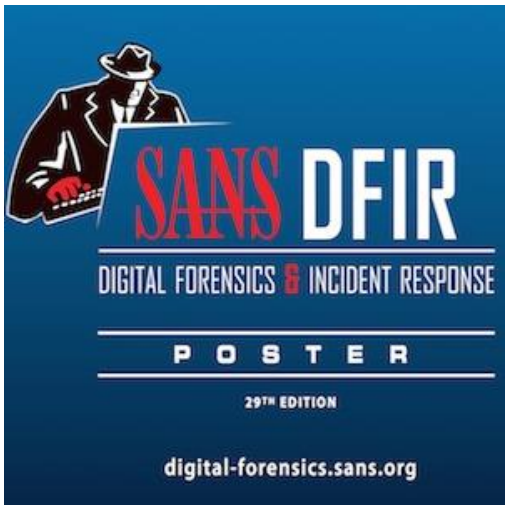
Requerimientos de instalación:

- RAM de 2 GB
- Espacio en disco de 100 GB
- CPU de 2 core a 2 GHz
- PHP 5.6
- MySQL 5.0

7.3.1.11 Informática forense - SANS DFIR:

Permite a través de análisis de los diferentes dispositivos electrónicos utilizados o que estén relacionados o involucrados en un ciberataque extraer evidencias contundentes para resolver estos y así conocer el origen de un ataque informático, para presentarlos como pruebas ante un juez y de esta manera por la parte judicial se tomen las medidas y castigos a los ciberdelincuentes, para esto se utilizará la herramienta de software Sans Dfir.

Figura 13. Informática Forense SANS DFIR



Fuente https://www.sans.org/images/posters/poster_evil_2014.png

Requerimientos de instalación:

- RAM de 8 GB
- Espacio en disco de 300 GB
- CPU de 2 core a 2 GHz. Intel Core i5 o superior.
- Puertos USB 3.0

7.3.2 Herramientas de Hardware.

Tabla 3. Herramientas de Hardware

Nombre dispositivo	Referencia	URL
Switch Core	Cisco WS-C3560X-24	https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3560-x-series-switches/data_sheet_c78-584733.html
Switch Misional 1	Cisco Catalyst 2960S-48TS-S	https://www.cisco.com/c/en/us/support/switches/catalyst-2960s-48ts-s-switch/model.html
Switch Misional 2	Cisco Catalyst 2960S-48TS-S	https://www.cisco.com/c/en/us/support/switches/catalyst-2960s-48ts-s-switch/model.html
Switch Misional 3	Cisco Catalyst 2960S-48TS-S	https://www.cisco.com/c/en/us/support/switches/catalyst-2960s-48ts-s-switch/model.html
Switch Misional 4	Cisco Catalyst 2960S-48TS-S	https://www.cisco.com/c/en/us/support/switches/catalyst-2960s-48ts-s-switch/model.html
Firewall	PFSENSE - XG-1541 1U HA	https://www.netgate.com/solutions/pfsense/xg-1541-1u-dual.html
IDS/IPS	PFSENSE - XG-1541 1U HA	https://www.netgate.com/solutions/pfsense/xg-1541-1u-dual.html
WAF	ModSecurity 3.0	https://modsecurity.org/about.html
EDR	GRR Rapid Response	https://grr-doc.readthedocs.io/en/latest/

Fuente: Del Autor

7.3.2.1 Switch Core WS-C3560X-24

Este dispositivo activo interconecta los switches de borde de red para la conexión de los equipos de los departamentos que conforman la organización.

Figura 14. Switch Core WS-C3560X-24

Fuente: https://www.tonitrus.com/es/redes/cisco/switch/cisco-catalyst-3560-x-switch/10105382-003-cisco-ws-c3560x-24t-s-catalyst-3560x-24-port-data-ip-base/

7.3.2.2 Switch Cisco Catalyst 2960S-48TS-S

Este dispositivo se encarga de interconectar los dispositivos de cada una de las áreas de Platino Sistemas, se sugieren 48 puertos contemplando la posibilidad de escalabilidad sin generar traumatismos al momento de la implementación de la infraestructura.

Figura 15. Switch Cisco Catalyst 2960S-48TS-S

Fuente: https://www.tonitrus.com/es/redes/cisco/switch/cisco-catalyst-2960-switch/10102602-003-cisco-ws-c2960-48tt-l-catalyst-2960-48-10/100-ports-2-1000bt-lan-base-image/

7.3.2.3 Firewall - IDS/IPS

PFSENSE - XG-1541 1U HA

Fue diseñado para grandes y medianas empresas, con el fin de brindar facilidades en la configuración y soporte para múltiples WAN, VPN, alta disponibilidad, balanceo de carga, generar informes, realizar monitoreo, entre otras[29].

Se puede configurar como firewall, dispositivo VPN, enrutador LAN o WAN, servidor DHCP, servidor DNS e IDS/IPS.

El dispositivo viene precargado con el software Pfsense, por lo que estaría listo para usar, cuenta con dos sistemas de 1U que brinda conmutación por error y redundancia, utiliza un espacio mínimo en rack, la configuración se realiza de manera fácil a través de la interfaz gráfica de usuario basada en web, además ofrece un bajo costo ya que no requiere complementos adicionales para su correcto y completo funcionamiento.

[29] XG-1541 1U HA Dispositivo de firewall. Disponible en https://www.netgate.com/solutions/pfsense/xg-1541-1u-dual.html

Permite la conexión entre oficinas a través de VPN cifradas, permitiendo que los empleados se conecten a su sitio de trabajo de manera segura, cuenta con un servicio integrado para facilitar las conexiones por VPN con instancia en la nube de Amazon Elastic Compute Cloud EC2.

Características:

- *“Redes de tamaño mediano a grande con gabinetes de montaje en rack de 1U*
- *Sucursal de tamaño mediano a grande con cargas pesadas.*
- *Proveedores de servicios administrados (MSP) / Proveedor de servicios de seguridad administrados (MSSP) Dispositivo local*
- *Conexiones de 10 Gigabit de alta velocidad*
- *Varias conexiones VPN*
- *Conexiones de alta velocidad con funcionalidad IDS / IPS”*

Figura16. Firewall Pfsense.

Fuente https://www.netgate.com/solutions/pfsense/xg-1541-1u-dual.html

7.3.2.4 WAF

ModSecurity 3.0

Este firewall de aplicaciones web de código abierto ofrece una cantidad importante de funciones para la protección de las aplicaciones Web, entre las cuales podemos encontrar registro, control de acceso y monitoreo en tiempo real, permite el acceso al

código fuente, tiene la capacidad de ampliar y personalizar la herramienta de acuerdo a las necesidades[30].

Opciones de Implementación

Incrustado:

ModSecurity puede ser agregado a una versión de Apache, esta opción es recomendada para una arquitectura ya diseñada y que no requiere cambio, y en caso de que se necesite proteger una cantidad importante de servidores web. Sin embargo, para estos casos no es practico construir una capa de seguridad independiente basada en proxy, además los recursos del servidor se comparten entre el servidor web y ModSecurity.

Proxy inverso

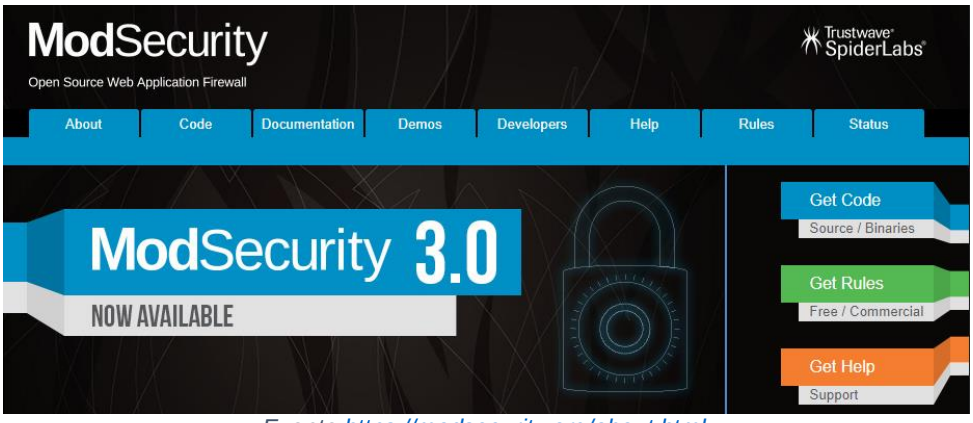
Los proxys inversos son enrutadores HTTP, que se interponen entre los servidores web y sus clientes. Al agregar ModSecuruty a un proxy inverso dedicado se obtiene un apropiado WAF de red, lo que permite la protección de los servidores web de la misma red. La capa de seguridad independiente proporciona un completo aislamiento de los sistemas a proteger con las reglas de seguridad que estos requieran.

Características:

- Monitoreo de seguridad de aplicaciones en tiempo real y control de acceso
- Registro de tráfico HTTP completo
- Evaluación de seguridad pasiva continua
- Fortalecimiento de aplicaciones web
- Documentación sólida

[30] ModSecurity Open Source Application Firewall. Disponible en https://modsecurity.org/about.html

Figura17. WAF ModSecurity.



Fuente https://modsecurity.org/about.html

7.3.2.5 EDR

GRR Rapid Response

Este es un sistema de Google el cual se accede a través de una interfaz web que garantiza una visibilidad a nivel gráfico de los Endpoints el cual permite ejecutar tareas de monitoreo[31].

Google Rapid Response GRR es un marco de trabajo completo enfocado en la conducción de procesos de respuesta a incidentes e investigación de manera remota. Su objetivo principal se centra en apoyar investigaciones y labores forenses de una manera rápida y escalable que cubra conjuntos completos de Endpoints que se encuentren integrados y monitoreados por el sistema.

Su arquitectura a alto nivel consiste en dos partes, los clientes y el servidor de gestión.

Componentes

Cliente GRR: Es desplegado a los sistemas que pueden ser sujetos de investigación o que pueden convertirse en parte de una investigación a demanda.

[31] Soluciones Endpoint Detection and Response Open-Source. Disponible en http://openaccess.uoc.edu/webapps/o2/bitstream/10609/107609/6/jbellovTFG1219memoria.pdf

GRR en versión cliente se encuentra disponible para sistemas Linux, OS X y Windows.

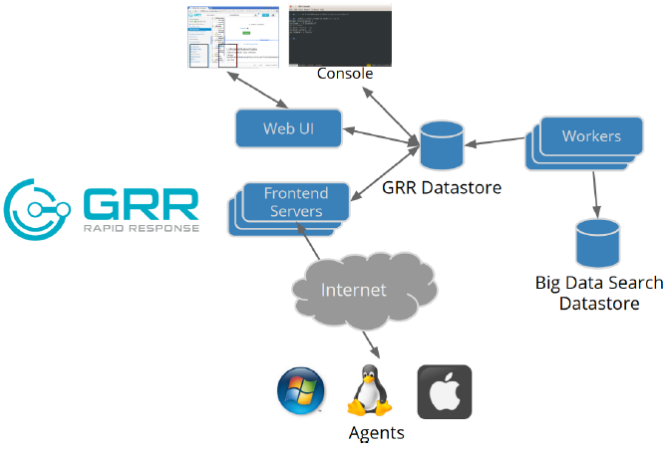
Cuenta con habilidades de análisis de memoria y reglas YARA (Yet Another Ridiculous Acronym).

Recolecta información detallada de la CPU, memoria, entre otros factores del estado del equipo.

Servidor: En este se centralizan e integran los componentes que hacen posible la operación de la herramienta, además de la interfaz gráfica web de usuario para ver los datos recibidos de los Endpoints y su procesamiento.

En detalle, integra los siguientes elementos:

Figura18. Arquitectura de GRR (Google Rapid Response)



Fuente. https://storage.googleapis.com/docs.grr-response.com/ACSC%202015-%20Defending%20the%20Gibson%20in%202015.pdf

Datastore: Es un almacén de datos en el cual se almacena la información de manera centralizada en donde se administra la comunicación de todos los componentes del servidor GRR.

Frontend servers: Estos se encargan de descifrar las solicitudes POST (se utiliza para enviar una entidad a un recurso en específico, causando a menudo un cambio en el

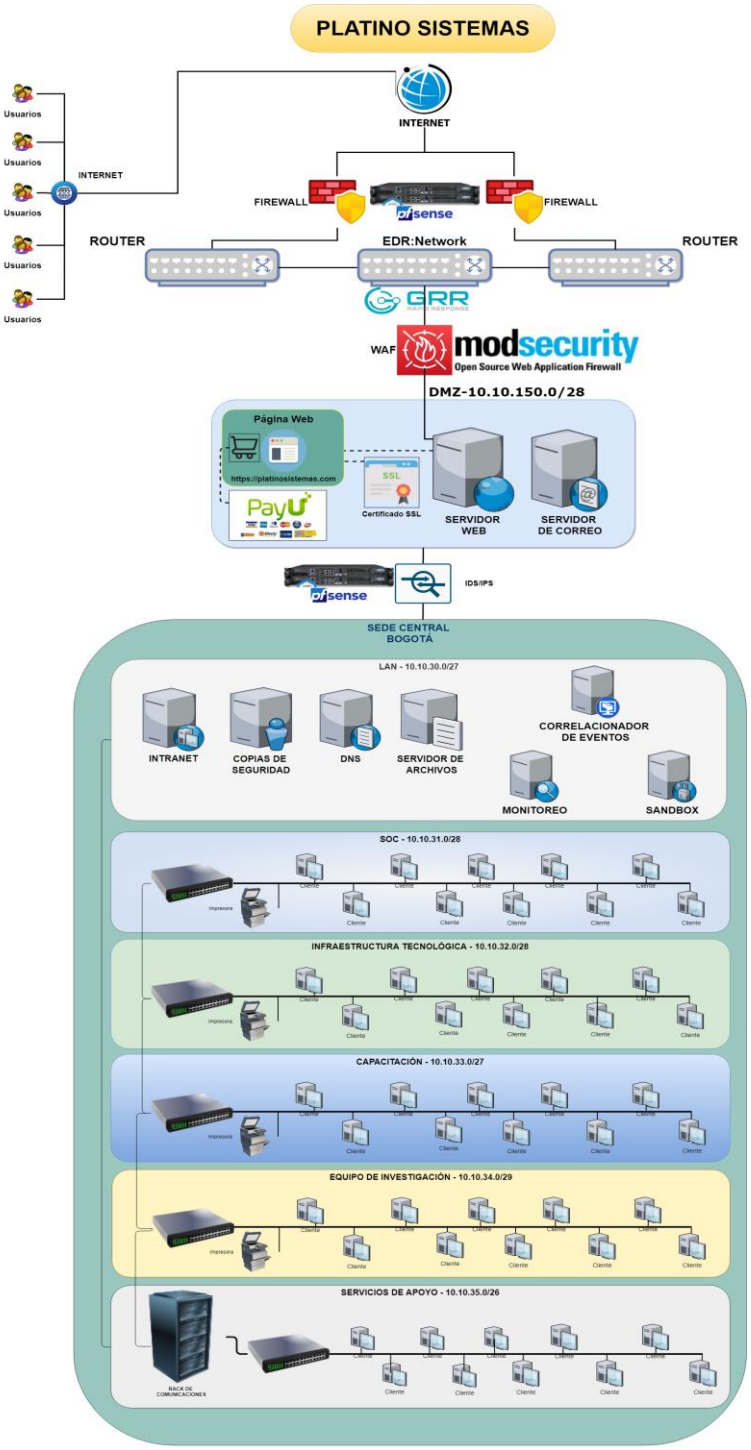
estado o efectos secundarios en el servidor) de los clientes, desagrupar los mensajes contenidos y ponerlos en la cola de espera del Datastore.

Workers: Los workers verifican las colas del almacén de datos para obtener respuestas del cliente, procesan nuevas solicitudes y flujos de comunicación. Este componente fue creado con el fin de eliminar tareas de procesamiento de datos.

Web UI: Esta interfaz de usuario Web permite al encargado de responder ante los incidentes reportados interactuar con el GRR facilitando la conexión con la API de desarrollo, utilizada para labores de automatización e integración con otros sistemas.

7.3.2.6 Diagrama Topológico de Hardware de Platino Sistemas

Figura19. Diagrama topológico de hardware Platino Sistemas



Fuente: Del autor. Disponible en https://drive.google.com/file/d/1ZP7YfQJimFR3_9xhYyARM-msO-_HN8Ku/view?usp=sharing

7.3.2.7 Segmentación de La Red

Tabla 4. Segmentación de Red

Grupo	Dirección de red	Mascara de Subred
DMZ	10.10.150.0/26	255.255.255.192
SEDE CENTRAL BOGOTÁ	10.10.30.0/27	255.255.255.224
SOC	10.10.31.0/28	255.255.255.240
INFRAESTRUCTURA	10.10.32.0/28	255.255.255.240
CAPACITACIÓN	10.10.33.0/27	255.255.255.224
EQUIPO DE INVESTIGACIÓN	10.10.34.0/29	255.255.255.248
SERVICIOS DE APOYO	10.10.35.0/26	255.255.255.192

Fuente: Del Autor

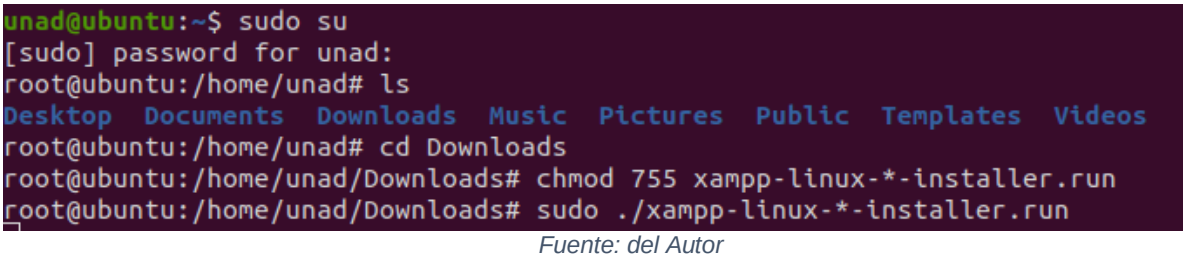
7.4 Diseño del Ambiente Controlado y Virtualizado.

7.4.1 Instalación y funcionamiento del servidor WEB - XAMPP 8.0.2.0

La instalacion de XAMPP se realiza en una maquina virtual con Sistema Operativo Ubuntu 20.04.

Se realiza la descarga de XAMPP desde la pagina https://www.apachefriends.org/es/index.html.

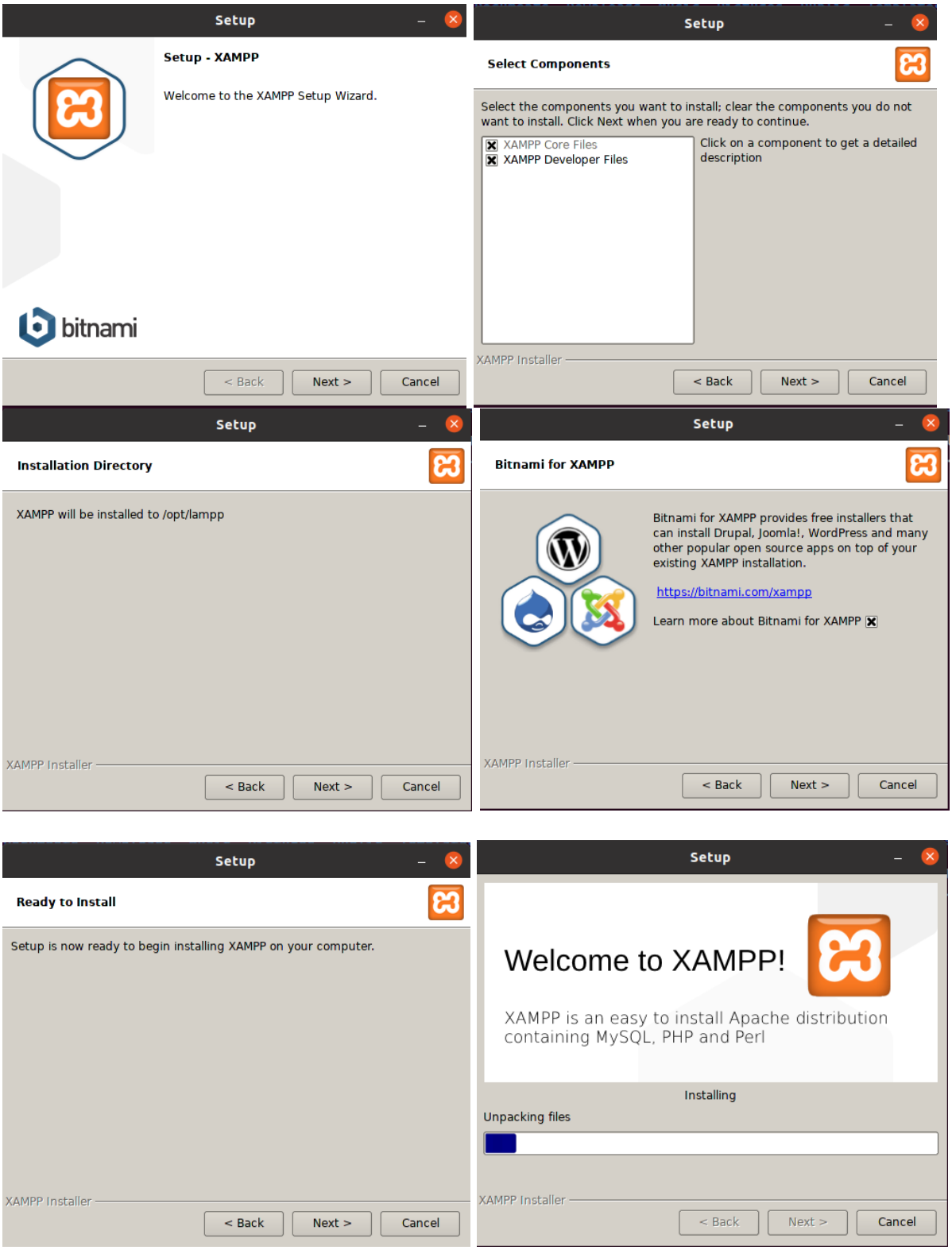
Figura20. Descarga Instalador de XAMPP

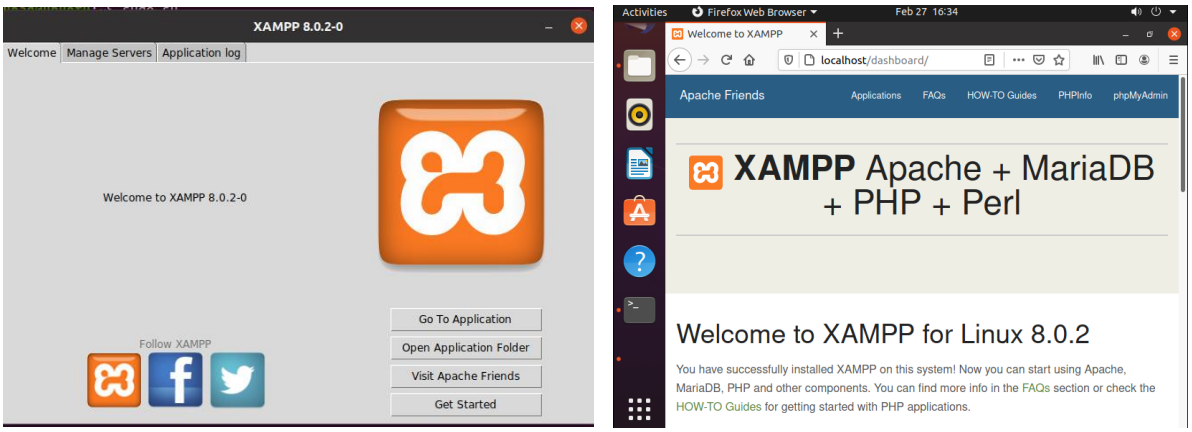


Fuente: del Autor

Ahora se abre la ventana de XAMPP para completar la instalación.

Figura21. Instalación XAMPP

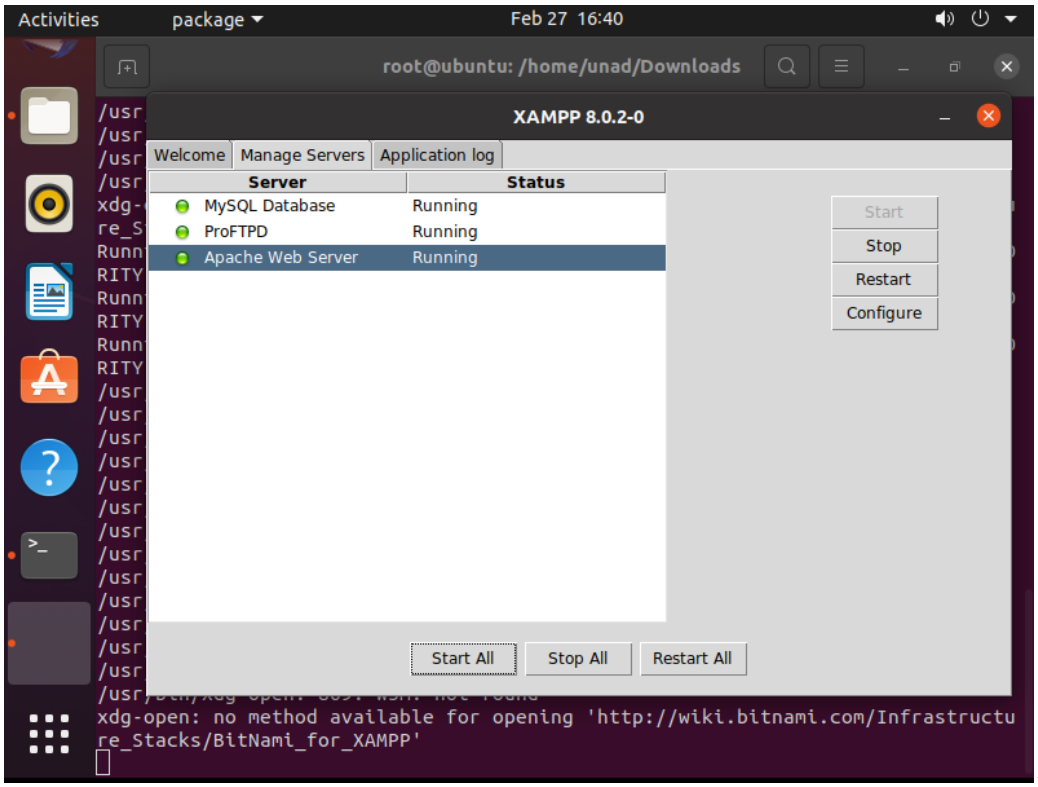




Fuente: del Autor

En la última imagen se puede observar el funcionamiento de XAMPP desde el Localhost, y en la siguiente imagen se observa la interfaz gráfica de la aplicación en la cual se evidencia que se está ejecutando la base de datos MySQL, el servidor FTP y el Apache Web Server.

Figura22. Verificación de la ejecución de los servicios de XAMPP



Fuente: Del Autor

Lo cual tambien se puede evidenciar desde la consola:

Figura23. Verificación de la ejecución de los servicios de XAMPP desde Consola

```
unad@ubuntu:~/Downloads$ sudo /opt/lampp/lampp start
Starting XAMPP for Linux 8.0.2-0...
XAMPP: Starting Apache...already running.
XAMPP: Starting MySQL...already running.
XAMPP: Starting ProFTPD...already running.
unad@ubuntu:~/Downloads$
```

Fuente: Del Autor

Alojamos el Sitio Web de PLATINO SISTEMAS en el Servidor Web XAMPP.

Figura24. Sitio WEB Platino Sistemas alojado en servidor XAMPP.

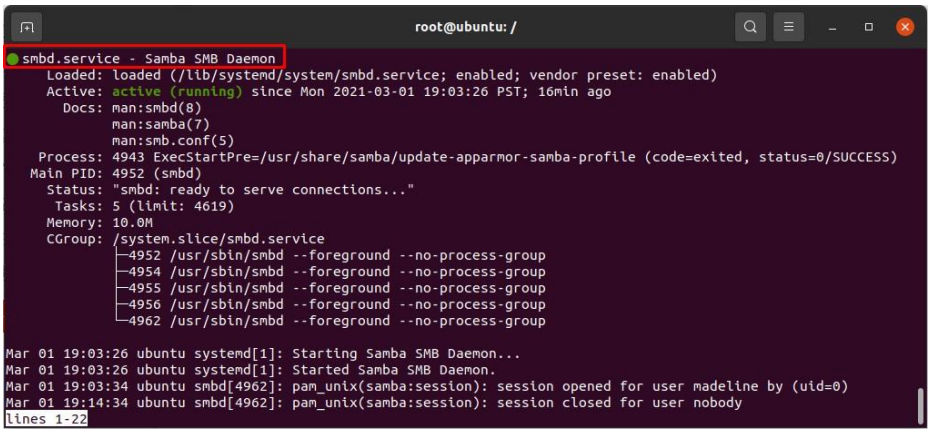
Fuente: Del Autor

7.4.2 Instalación y funcionamiento del servidor de Archivos - SAMBA

La instalación de SAMBA se realiza en una máquina virtual con Sistema Operativo UBUNTU 20.04.

Una vez instalada la herramienta se realiza la activación del servicio SMBD

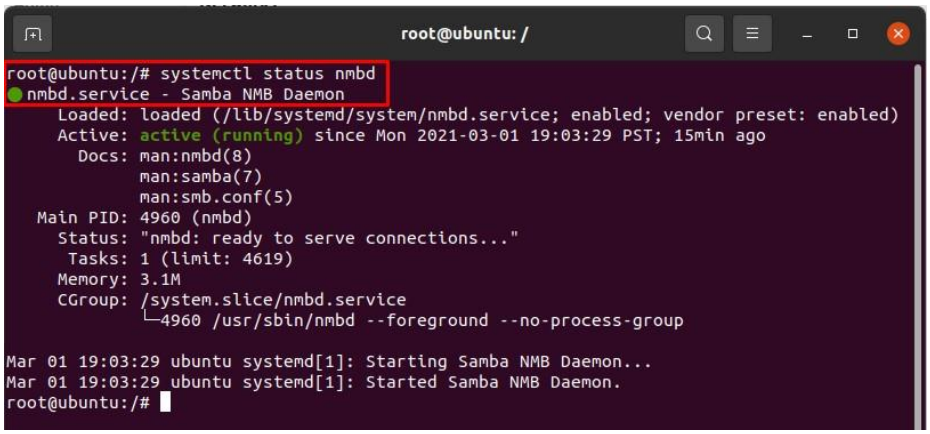
Figura25. Activación del Servicio SMBD.



Fuente: Del Autor

Y la activación del servicio NMBD

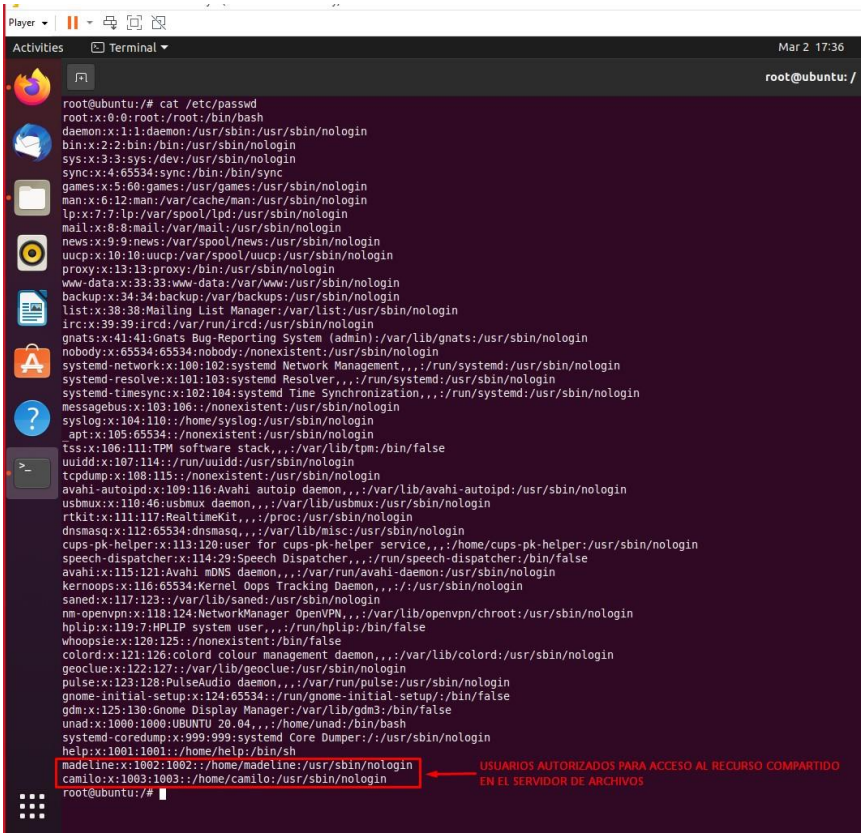
Figura26. Activación del Servicio NMBD



Fuente: Del Autor

Se crean los usuarios autorizados desde la consola.

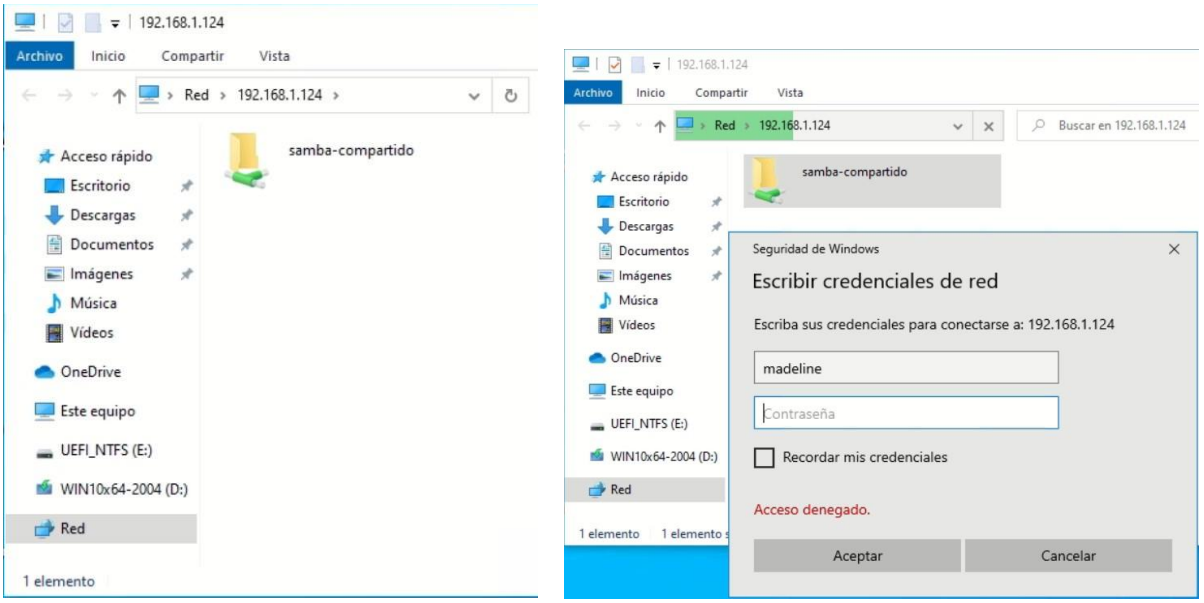
Figura27. Creación de usuarios con acceso a recursos compartidos



Fuente: Del Autor

Se ingresa al recurso compartido desde otra maquina con Windows. Como se observa a continuacion el sistema solicita las credenciales para poder acceder al recurso.

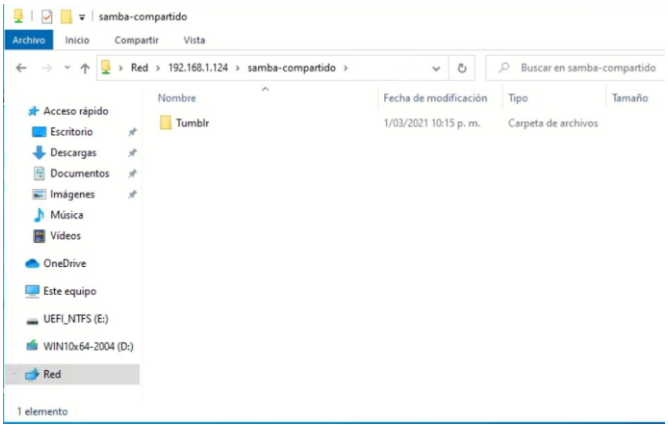
Figura28. Verificación de acceso a recurso compartido.



Fuente: Del Autor

Una vez ingresadas las credenciales podemos obtener acceso al recurso compartido.

Figura29. Acceso a recurso compartido



Fuente: Del Autor

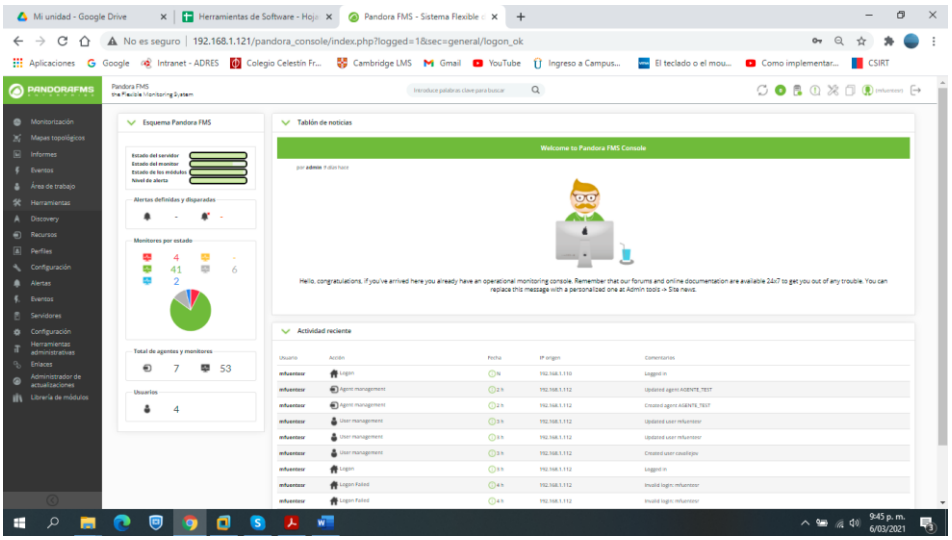
7.4.3 Instalación y funcionamiento del servidor de Monitoreo - PANDORA

La instalación del Servidor de Monitoreo - PANDORA se realiza en una máquina virtual con Sistema Operativo Centos 7. El servicio está dispuesto en el servidor 192.168.1.121 al cual podemos acceder desde cualquier equipo que se encuentre en el mismo segmento de red.

Figura30. Inicio de sesión en Servidor de Monitoreo.

Fuente: Del Autor

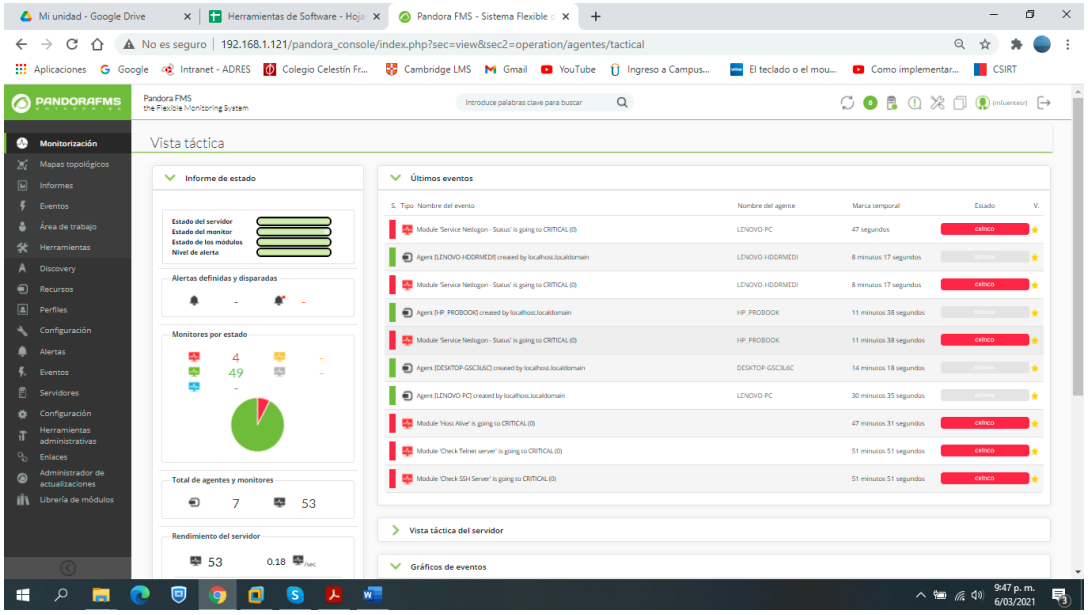
Figura31. Página de inicio de la plataforma de monitoreo



Fuente: Del Autor

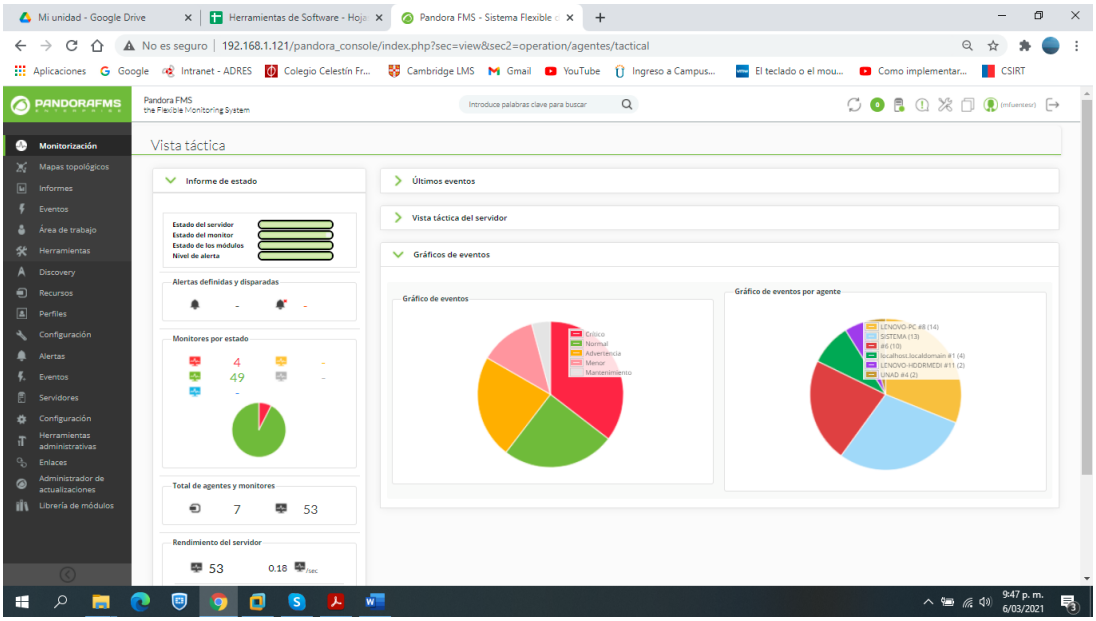
A continuación se observa la vista táctica de los eventos en la sección de monitorización, en la cual se evidencian los ultimos eventos, estado del servidor, gráficos de eventos por agente, alertas definidas y disparadas, entre otros.

Figura32. Vista táctica de la plataforma de monitoreo últimos eventos.



Fuente: Del Autor

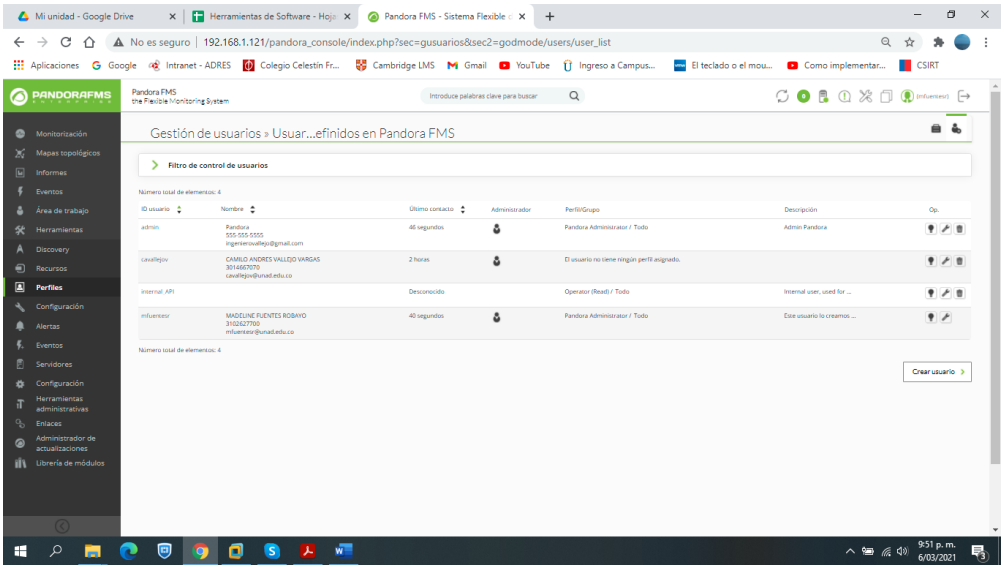
Figura33. Vista táctica de la plataforma de monitoreo gráfico de eventos



Fuente: Del Autor

En este apartado podemos crear usuarios, ingreso de datos de contacto y definición de perfiles, de los usuarios autorizados para operar la plataforma de monitoreo.

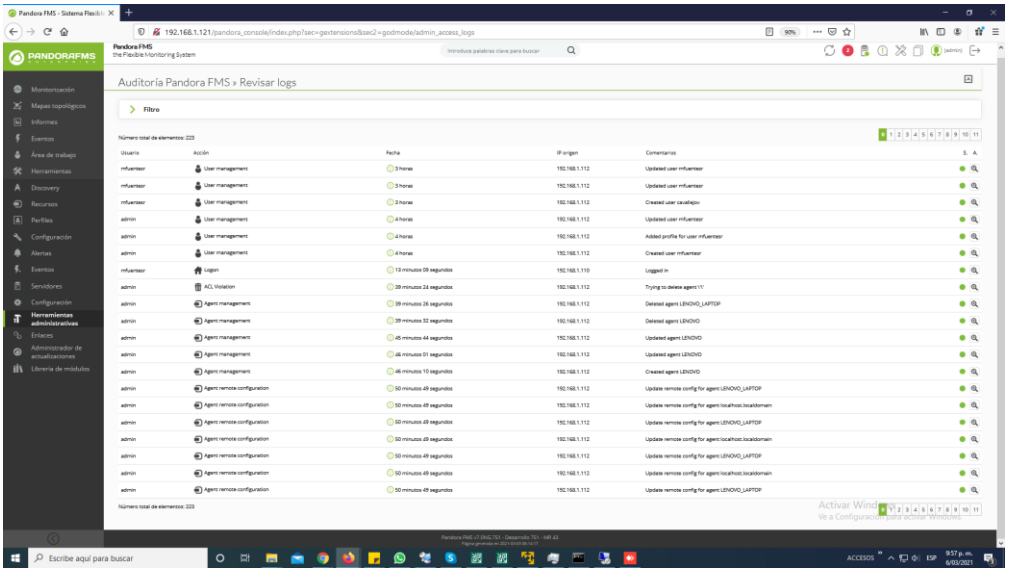
Figura34. Gestión de usuarios plataforma de monitoreo.



Fuente: Del Autor

Como herramientas administrativas contamos con Logs de auditoría del sistema, para evidenciar información de usuarios, fecha de conexión, IP de origen, entre otras.

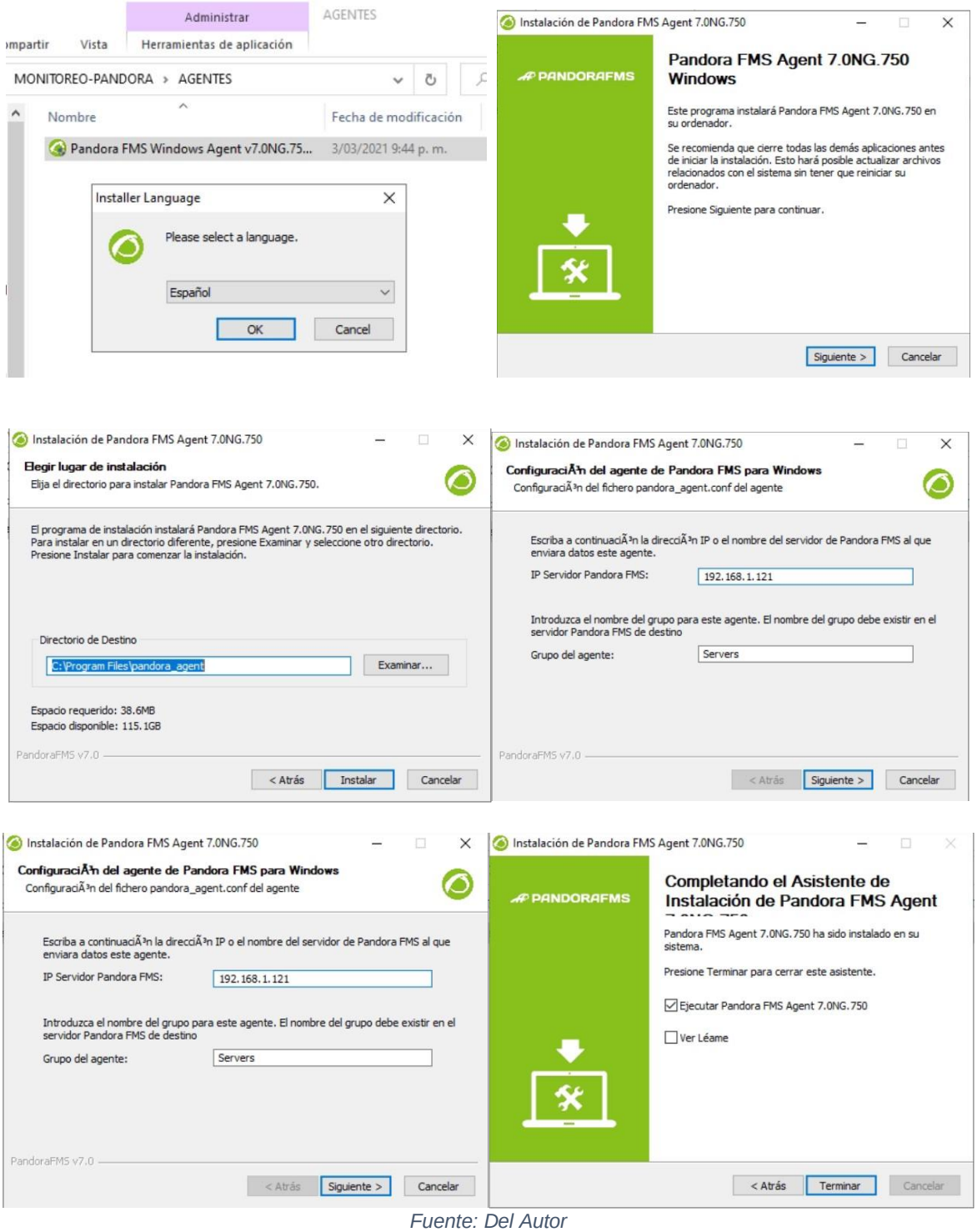
Figura35. Auditoría plataforma monitoreo.



Fuente: Del Autor

Se realiza la instalación de los agentes de Pandora en los equipos objeto de monitorización en ambiente virtualizado.

Figura36. Instalación de agentes en los equipos monitorizados.

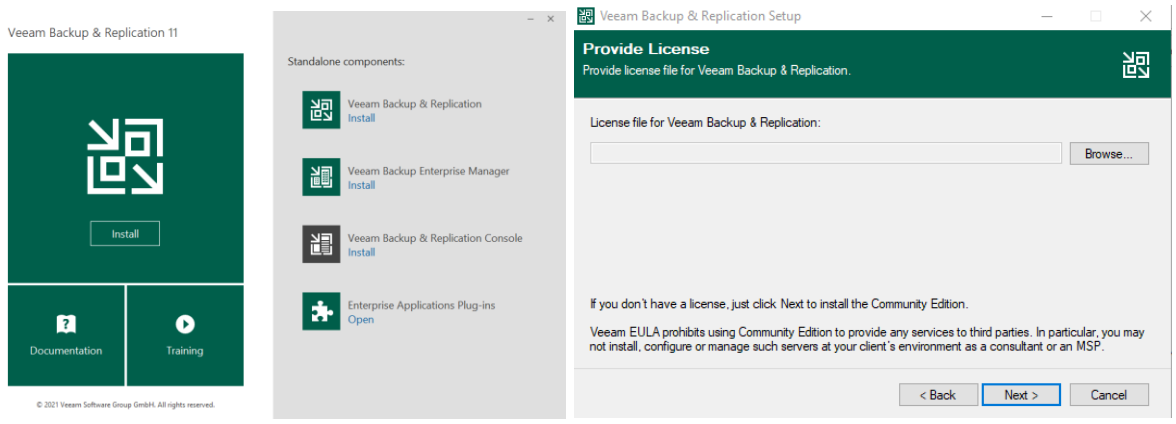


Fuente: Del Autor

7.4.4 Instalación y funcionamiento del Software de Copias de Seguridad - VEEAM BACKUP.

Iniciamos la instalación desde un equipo Windows (Físico) y aceptamos la licencia.

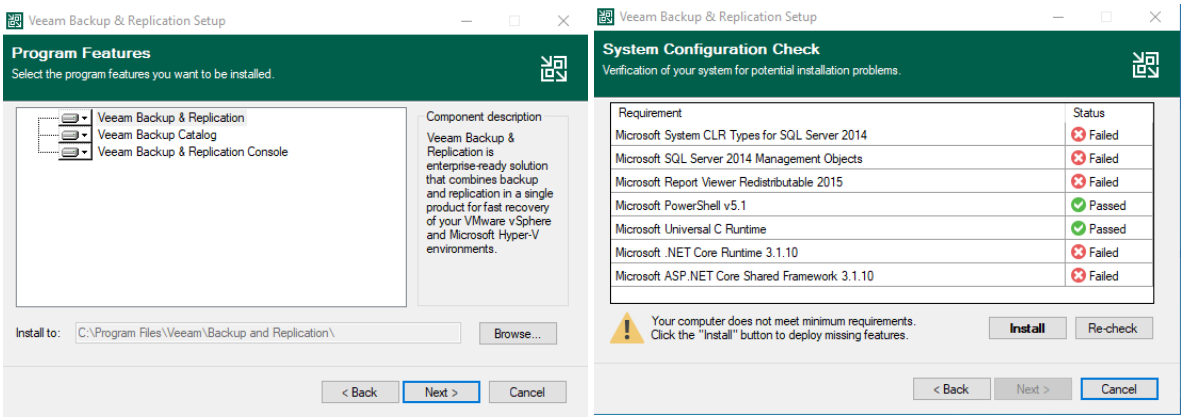
Figura37. Instalación VEEAM BACKUP.

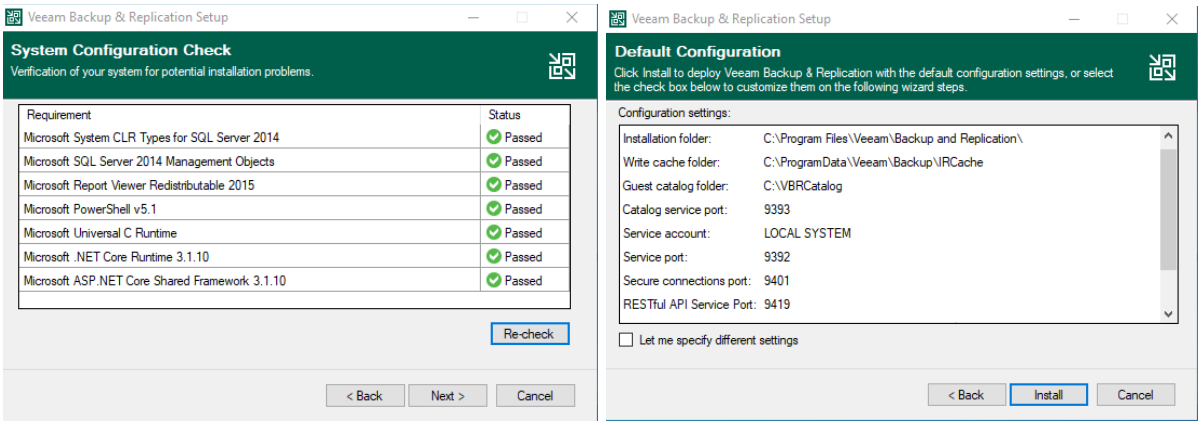


Fuente: Del Autor

Se realiza la verificación de los componentes que instalará el asistente de configuración en la máquina.

Figura38. Verificación de los componentes de la herramienta.

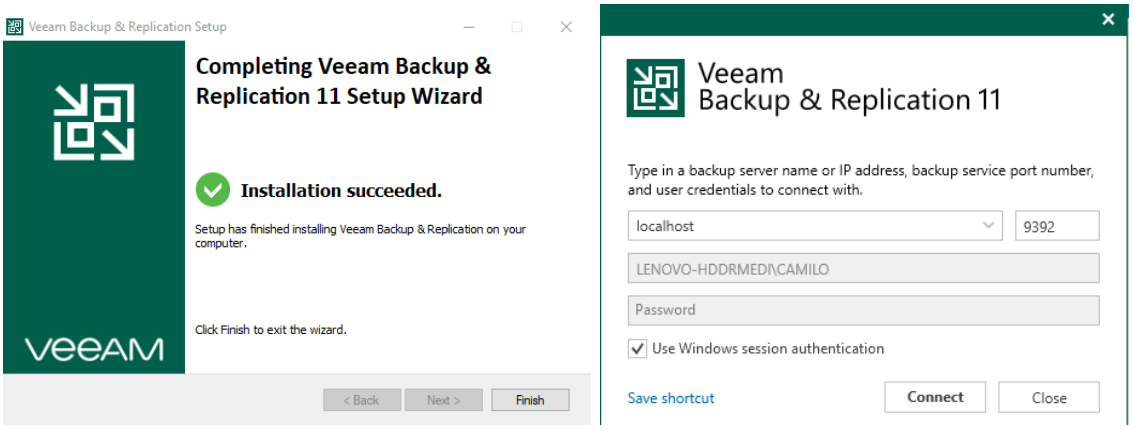




Fuente: Del Autor

Una vez finalizada la instalación del Veeam Backup se asigna el nombre del servidor, el puerto y se habilita la opción de autenticación con la sesión de Windows.

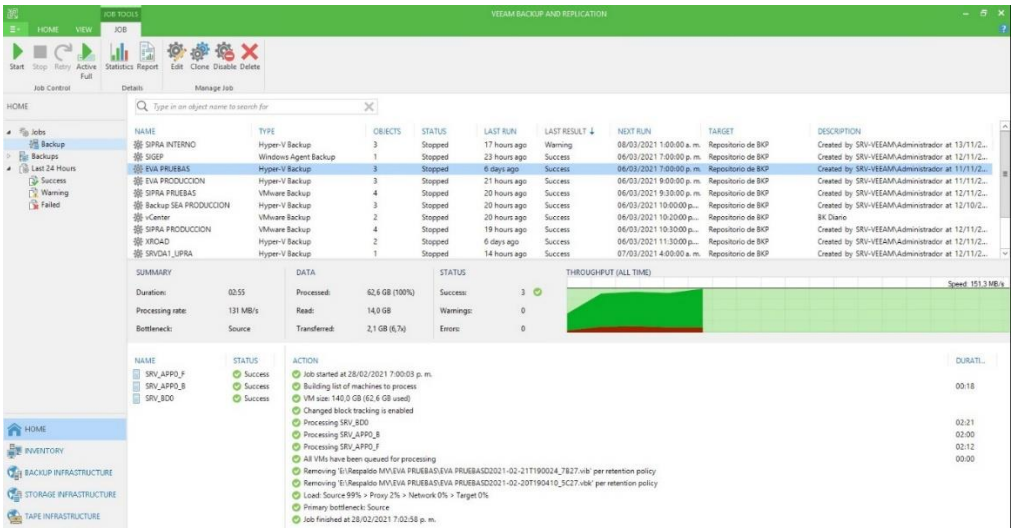
Figura39. Asignación del nombre del servidor



Fuente: Del Autor

A continuación, se observa los trabajos de Backup creados en el ambiente virtualizado como muestra de los servicios que ofrece el SOC de Platino Sistemas.

Figura40. Lista de Jobs de Backup.



Fuente: Del Autor

7.4.5 Instalación y funcionamiento del Servidor de Sandbox - FIREJAIL.

Se realiza la instalación del Servidor de Sandbox FIREJAIL en una máquina virtual con Sistema Operativo Ubuntu 20.04.

Figura41. Instalación de FIREJAIL.

```
unad@ubuntu:/$ sudo apt install firejail
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  firejail-profiles
The following NEW packages will be installed:
  firejail firejail-profiles
0 upgraded, 2 newly installed, 0 to remove and 8 not upgraded.
Need to get 383 kB of archives.
After this operation, 2,245 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 firejail amd64 0
.9.62-3 [309 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 firejail-profile
s all 0.9.62-3 [73.8 kB]
Fetched 383 kB in 1s (401 kB/s)
Selecting previously unselected package firejail.
(Reading database ... 190690 files and directories currently installed.)
Preparing to unpack .../firejail_0.9.62-3_amd64.deb ...
Unpacking firejail (0.9.62-3) ...
Selecting previously unselected package firejail-profiles.
Preparing to unpack .../firejail-profiles_0.9.62-3_all.deb ...
Unpacking firejail-profiles (0.9.62-3) ...
Setting up firejail (0.9.62-3) ...
Setting up firejail-profiles (0.9.62-3) ...
Processing triggers for man-db (2.9.1-1) ...
unad@ubuntu:/$
```

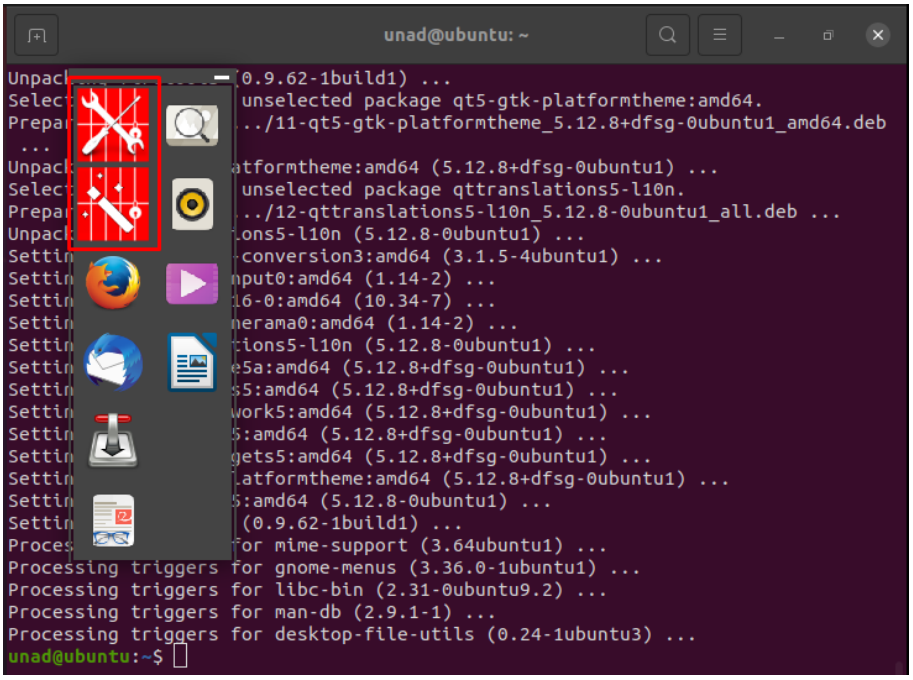
Fuente: Del Autor

Figura42. Verificación de la versión instalada.

Fuente: Del Autor

Como se observa a continuacion ya se encuentra instalada la interfaz gráfica la cual se realizo con el comando sudo apt install firetools, en la imagen se observan algunas aplicaciones que ya vienen preconfiguradas para ser utilizadas en el Sandbox:

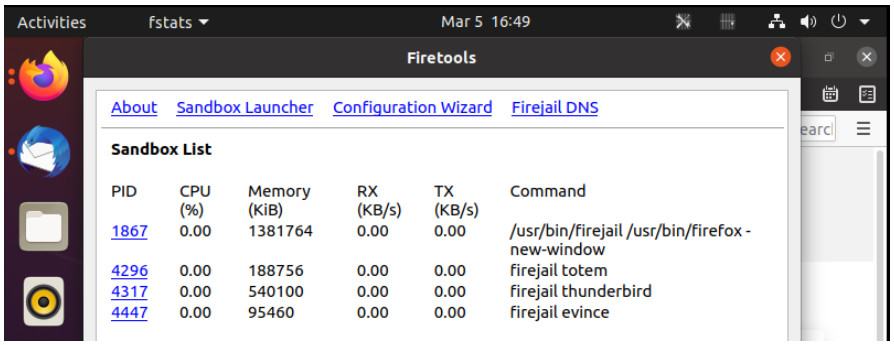
Figura43. Interfaz gráfica FIREJAIL.



Fuente: Del Autor

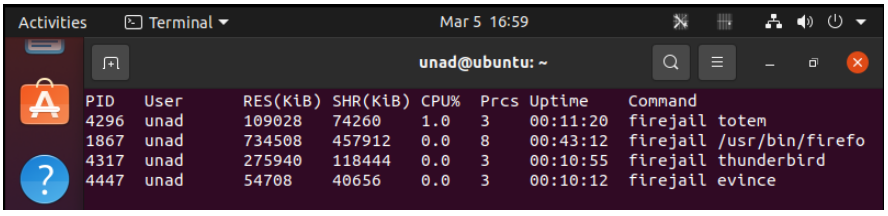
Dichas aplicaciones predeterminadas fueron iniciadas con el fin de observar si estaban corriendo en el Sandbox, lo cual se puede observar a continuación:

Figura44. Vista de aplicaciones ejecutadas desde Interfaz gráfica.



Fuente: Del Autor

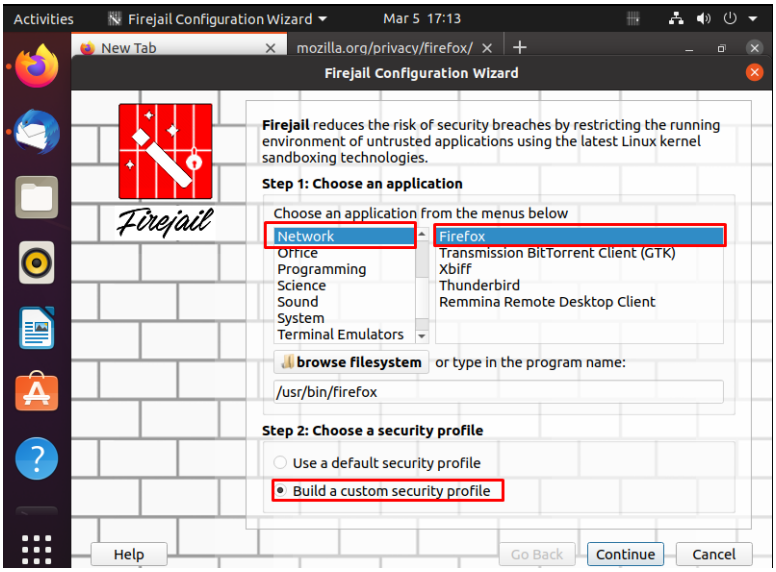
Figura45. Vista de aplicaciones ejecutadas desde Consola.



Fuente: Del Autor

Podemos realizar las configuraciones requeridas desde la interfaz gráfica, en la siguiente imagen realizaremos la restricción al ingreso a Firefox:

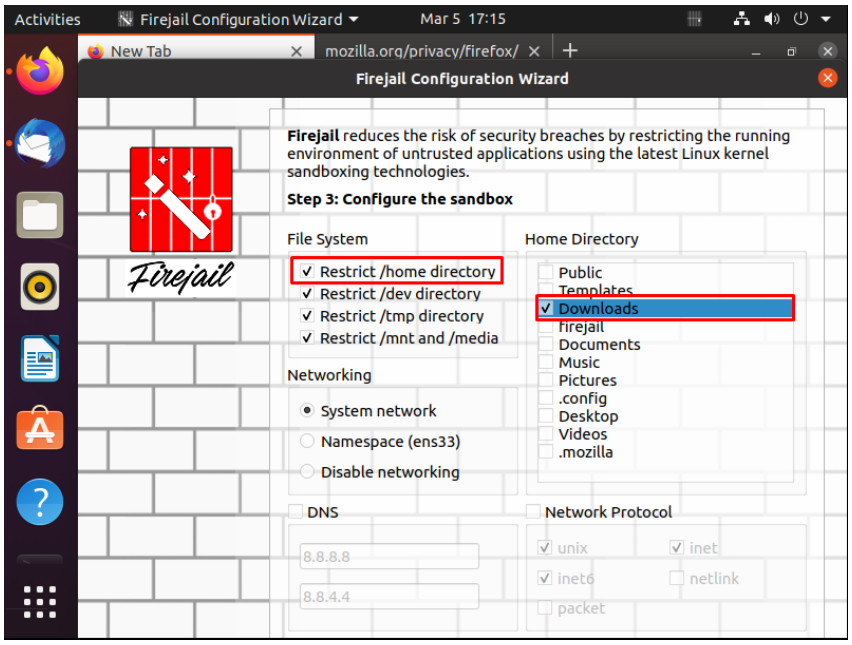
Figura46. Configuración desde interfaz gráfica.



Fuente: Del Autor

Y se restringe el acceso a los directorios, excepto el de descargas.

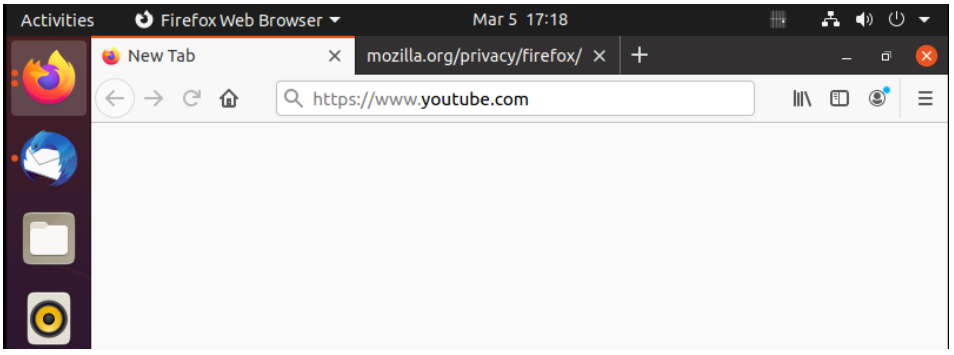
Figura47. Restricción de accesos a directorios.



Fuente: Del Autor

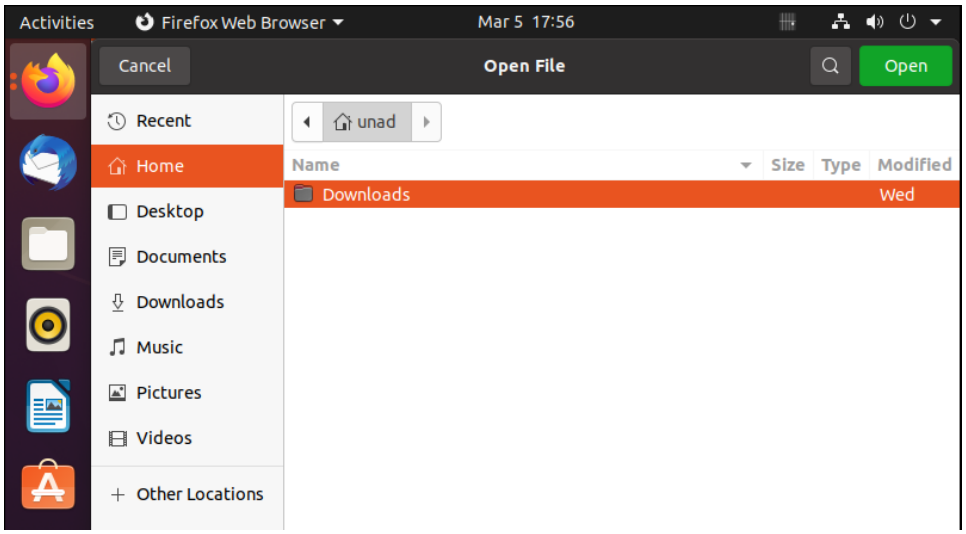
Como se observa a continuación, no se tiene acceso al Firefox y solo permite abrir archivos desde el directorio Descargas.

Figura48. Verificación restricción de accesos.



Fuente: Del Autor

Figura49. Verificación acceso a Downloads.

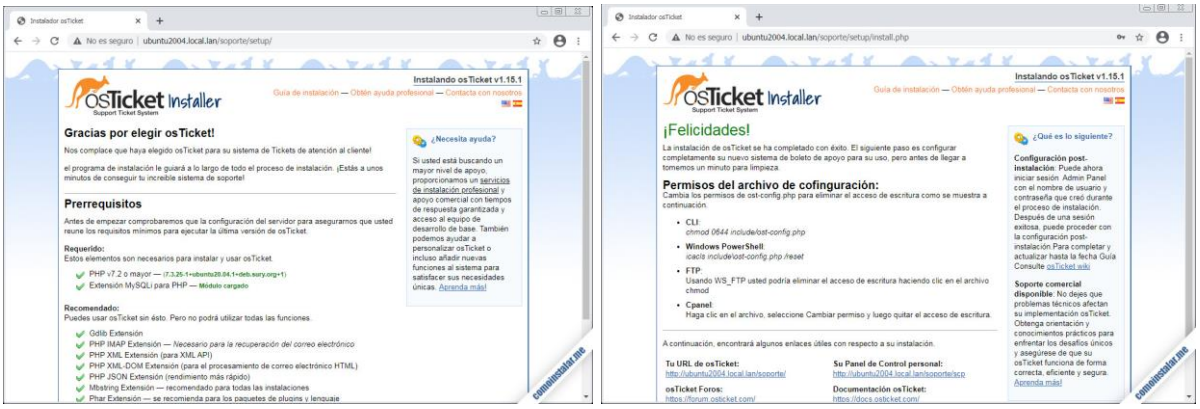


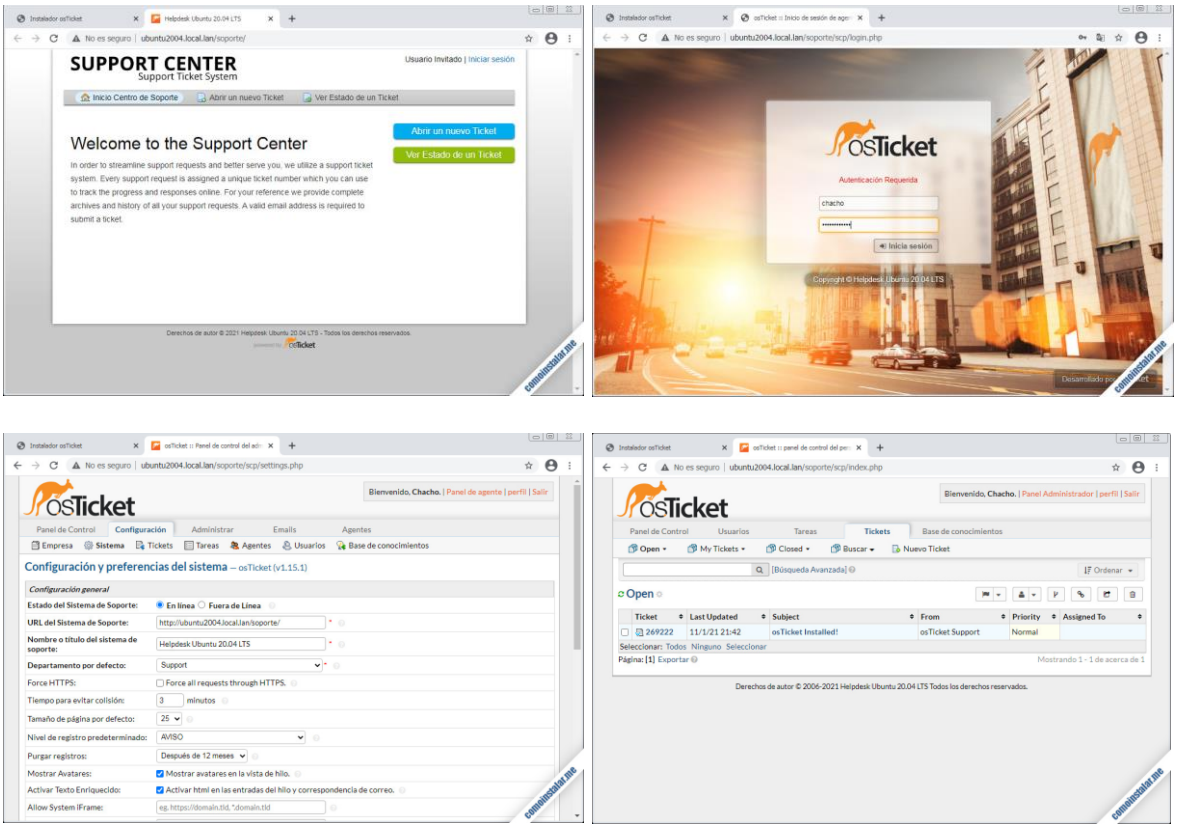
Fuente: Del Autor

7.4.6 Instalación y funcionamiento del software de Registro y Seguimiento de incidentes - OSTICKET.

La instalación de OsTicket se realiza en una máquina virtual con Sistema Operativo Ubuntu 20.04.

Figura50. Instalación herramienta OsTicket



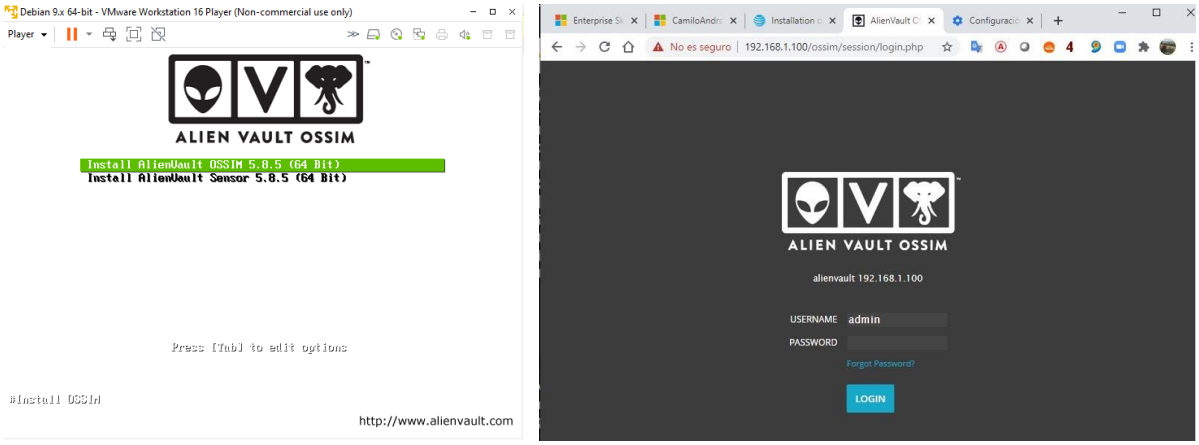


Fuente: Del Autor

7.4.7 Instalación y funcionamiento del Correlacionador de Eventos - ALIENT VAULT.

La instalación de ALIEN VAULT OSSIM se realiza en una máquina virtual con Sistema Operativo CentOS 09.

Figura51. Inicio de sesión ALIENVAULT OSSIM.

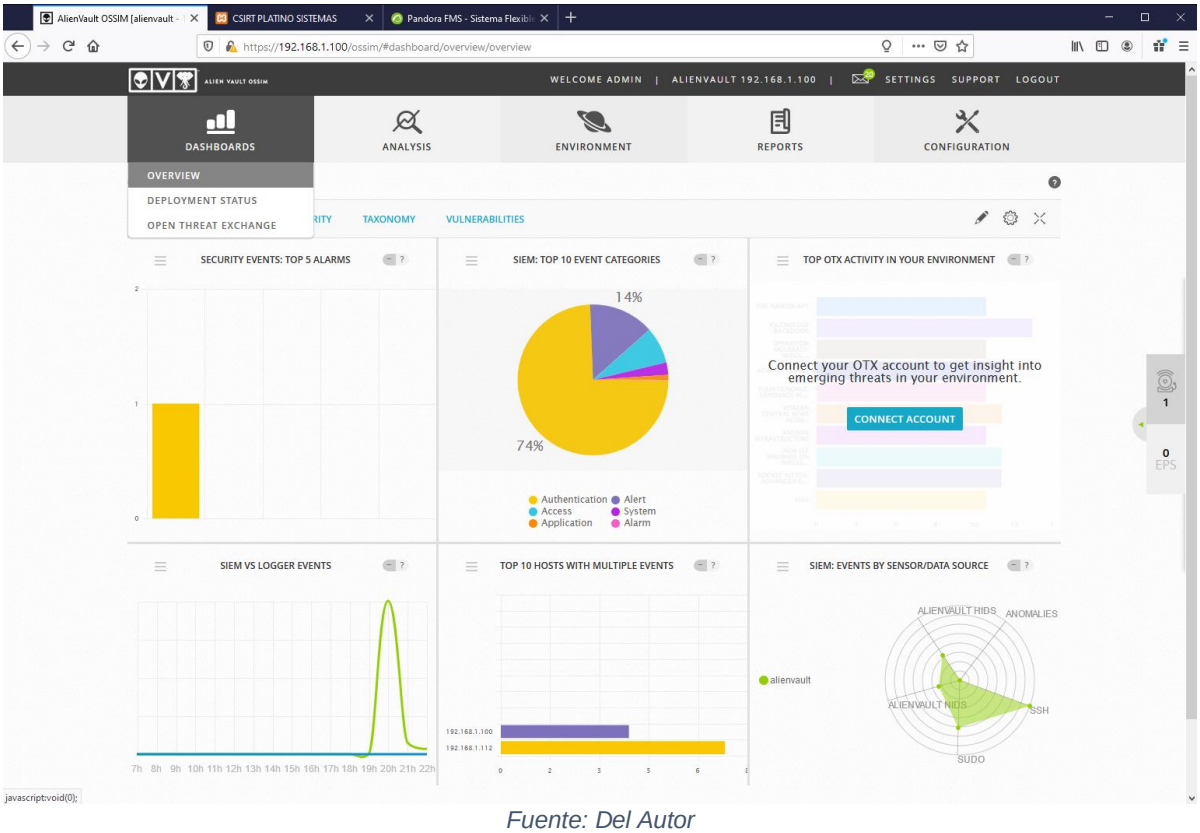


Fuente: Del Autor

En el siguiente apartado se observa el panel de información general del Correlacionador de Eventos, el cual contiene las siguentes secciones:

- Seccion SIEM: correlaciona registros y datos para detectar patrones maliciosos dentro de la actividad del host y en el tráfico de la red.
- Sección de descubrimiento de activos: detecta activos en su entorno, identifica cambios en estos y detecta activos maliciosos en la red.
- Sección de evaluación de vulnerabilidades: Detecta vulnerabilidades comparando el software de los activos con una base de datos de que contiene vulnerabilidades conocidas.

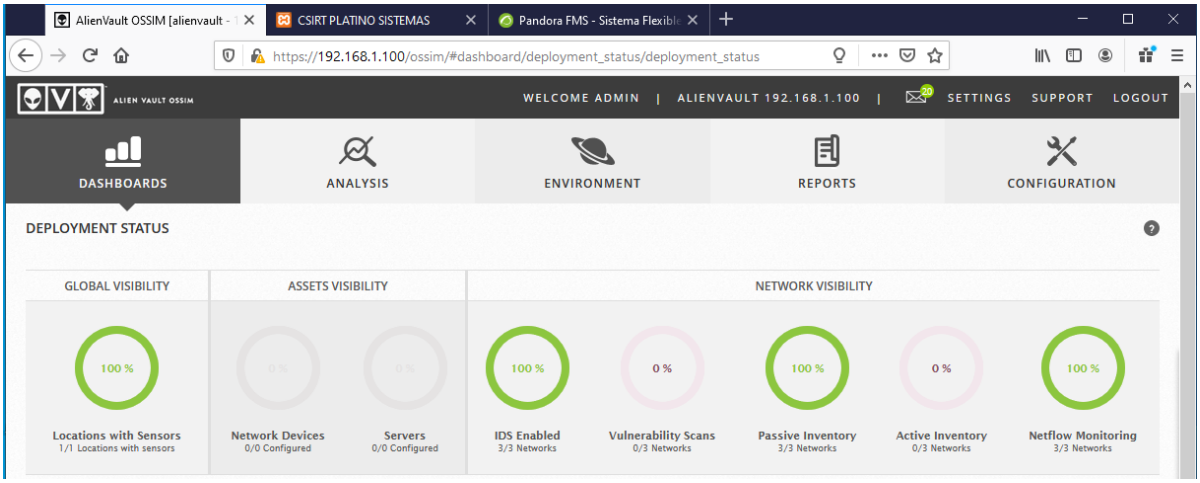
Figura52. Dashboards – Overview.



Fuente: Del Autor

El módulo Deployment Status permite visualizar información sobre el estado de la red, vulnerabilidades escaneadas, activos y servidores, entre otras.

Figura53. Deployment Status



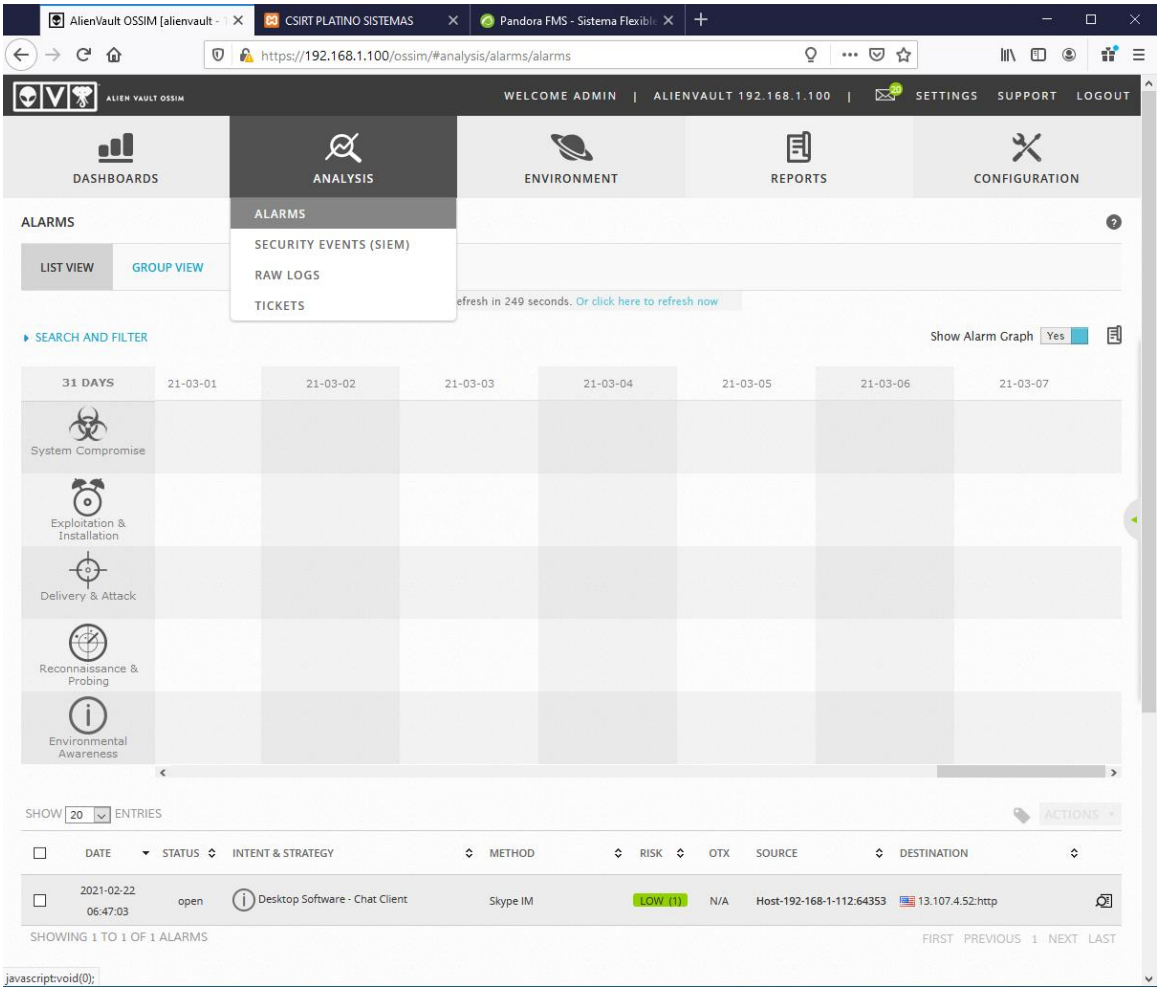
Fuente: Del Autor

En la sección Gestión de Alarmas permite visualizar las alarmas en orden cronológico inverso, como se observa en la Figura No. 51 la tabla muestra las alarmas que se presentaron en los ultimos 30 días, cada dia se representa en una columna diferente.

Existen cinco categorías diferentes en las que estan clasificadas las alarmas:

- Compromiso del sistema
- Explotación e instalación
- Entrega y ataque
- Reconocimiento y sondeo
- Conciencia ambiental

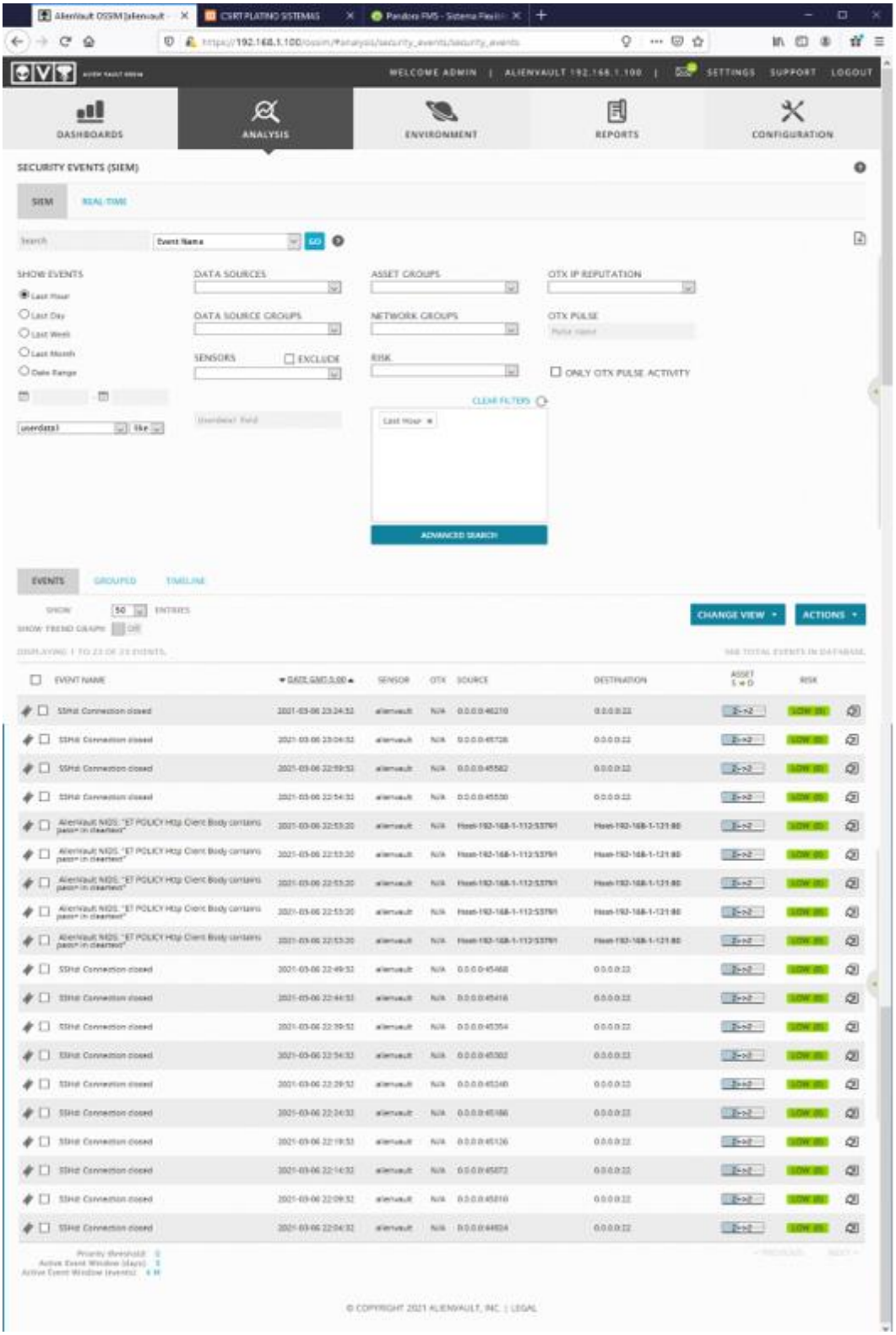
Figura54. Gestión de Alarmas



Fuente: Del Autor

La sección Gestión de Eventos - Security Events (SIEM) muestra una lista de eventos los cuales son correlacionados y priorizados en todos los activos, esta sección permite consultar cada evento para conocer información más detallada.

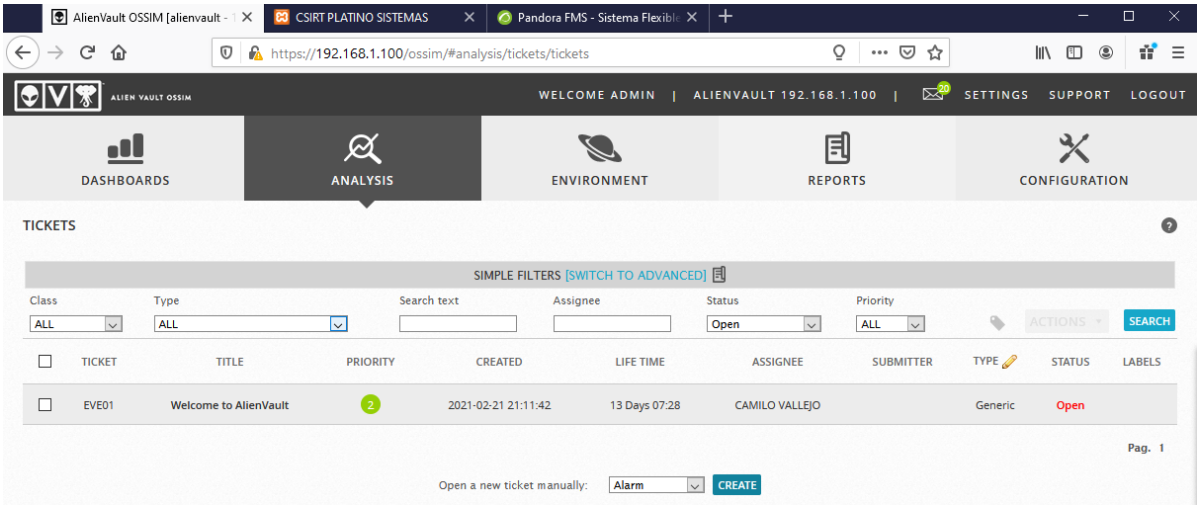
Figura55. Gestión de Eventos (SIEM)



Fuente: Del Autor

La sección de Gestión de Tickets permite realizar seguimiento a las alarmas detectadas o eventos ocurridos, la creación del ticket ayuda a conocer el progreso y la solución del problema, así como a crear una auditoria para hacer seguimiento a la situación presentada.

Figura56. Gestión de Tickets



Fuente: Del Autor

8. RESULTADO OBJETIVOS PLANTEADOS

Cuadro 17. Desarrollo de los objetivos

Objetivos	Desarrollo de los objetivos	
Diseñar la estructura organizacional y establecer las capacidades de las operaciones del SOC (Centro de Operaciones de Seguridad)	Ítem de consulta: **6.1.1. Estructura Organizacional:** Organigrama donde se propone la estructura del área de tecnología de la empresa Platino Sistemas. **6.1.2. Áreas, Responsabilidades y Roles:** Se define el objetivo, responsabilidades, perfil y capacidades de cada una de cargos que conforman el área de tecnología. **6.1.3. Capacidades de las Operaciones del SOC:** Se determinan las condiciones de funcionamiento del SOC que permiten desarrollar las actividades propias de este.	
Formular políticas, alcance y servicios propuestos por el SOC (Centro de Operaciones de Seguridad).	Ítem de consulta: **6.2.1. Políticas de Seguridad**: Se definen las políticas de Seguridad de la empresa Platino Sistemas alineadas a la ISO/IEC 27002 con los respectivos responsables de su cumplimiento. **6.2.2. Alcance del SOC:** Se definen las actividades que realizará el Centro de Operaciones de Seguridad de Platino Sistemas para la gestión de incidentes de seguridad, se señala como estará conformado y las responsabilidades de cada cargo. **6.2.3. Servicios Propuestos por el SOC**: Se listan los servicios que ofrecerá el Centro de Operaciones de Seguridad de Platino Sistemas.	
Determinar las herramientas tecnológicas de hardware y software que permitan desarrollar las actividades propias del CSIRT.	Ítem de consulta: **6.3.1 Herramientas de Software:** Se determinan las herramientas de software Open Source que serán implementadas en el diseño del SOC de la empresa Platino Sistemas. **6.3.2 Herramientas de Hardware**: Se proponen las herramientas de hardware con su descripción y características para a implementación del SOC de la empresa Platino Sistemas	
Diseñar un ambiente controlado y virtualizado que permita ejecutar las actividades del CSIRT.	Ítem de consulta: **6.4.1** Instalación y funcionamiento del servidor WEB – XAMPP 8.0.2.0	http://192.168.1.123/PLATINO1/platino.html
	6.4.2 instalación y funcionamiento del servidor de Archivos – SAMBA	192.168.1.124
	6.4.3 Instalación y funcionamiento del servidor de Monitoreo – PANDORA	http://192.168.1.120/index
	6.4.4 instalación y funcionamiento del Software de Copias de Seguridad - VEEAM BACKUP	192.168.1.112
	6.4.5 instalación y funcionamiento del Servidor de Sandbox – FIREJAIL	192.168.1.123

	6.4.6 instalación y funcionamiento del software de Registro y Seguimiento de incidentes - OSTICKET	192.168.1.123
	6.4.7 instalación y funcionamiento del Correlacionador de Eventos – ALIENVAULT	https://192.168.1.100

Fuente: Del Autor

Repositorio del Proyecto:

https://docs.google.com/document/d/1LD1gmZSPWgQ3qwEBnGChZQiHAYnfkZKg/edit?usp=sharing&ouid=100939403321447178545&rtpof=true&sd=true

Video:

https://youtu.be/v70EqC6wklE

9. CONCLUSIONES

El listado obtenido de las referencias documentales obtenidas a través del análisis y evaluación por medio de la revisión sistemática efectuada a las fuentes documentales investigadas nos da como resultado un denominador común en relación a las herramientas principales que apuntan al uso de software Open Source como resultado de las ventajas que esto conlleva.

La definición de herramientas a implementar garantiza el desarrollo de las operaciones de un SOC como parte del equipo de respuesta a incidentes de ciberseguridad que dentro de sus servicios tanto reactivos como proactivos cumplen con el desarrollo de las actividades de un CSIRT.

El diseño de la estructura organizacional se conformó con base al SOC y a la infraestructura tecnológica propuesta teniendo en cuenta las áreas transversales como la de capacitación, el equipo de investigación y los servicios de apoyo constituidos por financiera y oficina jurídica, para los cuales se contempla la posibilidad de contratar de manera externa.

Basados en el estándar de la norma ISO-IEC 27002 se formularon las políticas de seguridad las cuales deben ser acatadas por todos los integrantes del CSIRT para garantizar los tres pilares de información y asegurar así la calidad de los servicios prestados por el equipo de respuesta a incidentes.

El uso de software Open Source permiten una flexibilidad en la elección de herramientas, pero a su vez requiere de un nivel importante de conocimiento en la instalación, configuración e implementación lo cual se debe considerar al momento de elegir la solución a implementar.

La implementación de un escenario virtualizado que opere las herramientas que se consideren necesarias para la ejecución de actividades de un SOC, requiere de una infraestructura robusta para lograr establecer un ambiente óptimo que permita ejecutar las tareas propuestas en el diseño del SOC.

10. GLOSARIO

Ciberataque: es una acción maliciosa por parte de un individuo u organización de violar el sistema de información de otro comprometiendo la disponibilidad, integridad y confidencialidad de la información mediante acceso no autorizado.

Core: hace referencia a la actividad principal de una empresa que le permite generar valor y obtener ventaja competitiva.

DDoS: por sus siglas Distributed Denial of Service, es un tipo de ataque que sobrepasa las capacidades de un sistema de información o infraestructura tecnológica lo cual representa indisponibilidad del servicio.

Dirección IP: es una dirección única que identifica un dispositivo en Internet o una red local. IP hace referencia a “Protocolo de Internet", que es el conjunto de reglas que rigen el formato de los datos enviados a través de Internet o la red local.

EDR: por sus siglas Endpoint Detection and Response, es una solución integrada de seguridad de endpoints que realiza el monitoreo en tiempo real y recopila datos de endpoints, tiene la capacidad de analizar y dar respuesta automatizadas basadas en reglas.

Malware: corresponde a software malicioso que tiene como objetivo dañar un dispositivo una vez entra al sistema, este ataque realiza el robo de información, encripta o elimina datos, y puede cambiar funciones del ordenador.

Open-Source: el termino hace referencia a software de código abierto que permite su implementación, modificación y distribución.

Ransomware: hace referencia a software malicioso el cual le permite al ciberdelincuente bloquear de manera remota un dispositivo encriptando los archivos, lo cual implica que se pierda el control de los datos almacenados. El ataque solicita el pago por el rescate de la información.

Sandbox: es un espacio aislado en un entorno seguro que replica un entorno operativo de usuario final, en el cual se puede ejecutar, observar y analizar archivos ejecutables, contenido de trafico de red, entre otros, sin comprometer la aplicación, sistema o plataforma en la que se ejecute.

11. BIBLIOGRAFÍA

ADEVA, Ana y VERA, José Manuel. Ágorasic. Centro de Conocimiento en Ciberseguridad. CSIRTs al pie del Cañón, 2020.

ALIENVAULT OSSIM. El SIEM de código abierto más utilizado del mundo. [Sitio web] Dallas [Consulta: 13 de marzo 2021] Disponible en https://cybersecurity.att.com/products/ossim

AUSCERT. Forming an Incident Response Team. White Paper, SEI, 2017. [Sitio web] Pittsburgh [Consulta: 13 de marzo 2021] Disponible en. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485693

BELLO VIEDA, Jaime Andres, GARCIA FONT, Víctor y MENDOZA FLOREZ, Manuel Jesús. Soluciones Endpoint Detection and Response Open-Source, 2019. p. 14-20.

COLOMBIA, CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL 3854. POLÍTICA NACIONAL DE SEGURIDAD DIGITAL. 2016, p. 10-68

COLOMBIA, CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL 3995. POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL, 2020. p. 8-40.

COLOMBIA, MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES. Decreto 0032 de 2013. Por la cual se crea la Comisión Nacional Digital y de Información Estatal.

ENISA. Agencia de la Unión Europea para la seguridad Cibernética. [Sitio web] CSIRT en Europa. [Consulta: 19 de noviembre de 2020] Disponible en: https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network

ESQUEMA NACIONAL DE SEGURIDAD. GUÍA DE CREACIÓN DE UN CERT / CSIRT. [Sitio web] España [Consulta: 19 de noviembre de 2020] Disponible en https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/520-ccn-stic-810-guia-de-creacion-de-cert-s.html

EUROPOL. Internet Organised Crime Treath Assesment (IOCTA), European Union Agency for Law Enforcement Cooperation 2020. p. 12-59.

FORO ECONÓMICO MUNDIAL. Shaping the Future of Cybersecurity and Digital Trust. [Sitio web] Ginebra [Consulta: 19 de noviembre de 2020]. Disponible en https://www.weforum.org/centre-for-cybersecurity/

HUERTAS, Leonardo. Computer Emergency Response Team (CERT) [Video]. Colombia: YouTube, ElevenPaths Talks, 2016. 51:14 minutos. [Consulta: 21 de noviembre de 2020] Disponible en: https://youtu.be/S0KrUxj62zA

ISOTOOLS.ISO 27001.Pilares fundamentales de un SGSI. [Sitio web]. España [Consulta: 21 de noviembre de 2020]. Disponible https://www.isotools.org/2015/01/13/iso-27001-pilares-fundamentales-sgsi/

LANFRANCO, Einar y PÉREZ, Ernesto. ¿De qué se trata?, modelos posibles, servicios y herramientas. Argentina. CERT Universidad Nacional La Plata. p. 5-18

MARTINEZ, Graciela, Introducción a la creación de un CSIRT. Argentina. Lacnic CSIRT. p. 24-43.

MINDEFENSA. COLCERT Grupo de Respuestas a Emergencias Cibernéticas de Colombia. [Sitio web]. Colombia. [Consulta: 21 de noviembre de 2020]. Disponible en http://www.colcert.gov.co/

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. Colombia: MINTIC, 2016. p. 8-29.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. La nueva política de Gobierno Digital promueve la proactividad y la innovación ciudadana. [sitio web] Colombia, 2018. [Consulta: 17 de octubre de 2020] Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/75180:La-nueva-politica-de-Gobierno-Digital-promueve-la-proactividad-y-la-innovacion-ciudadana

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES. Modelo de Seguridad y Privacidad de la Información. Colombia: MINTIC, 2016. p. 20-58.

MODSECURITY Open-Source Application Firewall. [Sitio web] EcuRed [Consulta: 28 de octubre de 2020] Disponible en https://modsecurity.org/about.html

MOYLE. Ed. CERT vs. CSIRT vs. SOC: ¿Cuál es la diferencia? [Sitio web]. TechTarget, 2019. [Consulta: 21 de noviembre de 2020] Disponible en: https://searchdatacenter.techtarget.com/es/consejo/CERT-vs-CSIRT-vs-SOC-Cual-es-la-diferencia

NETGATE XG-1541 1U HA Dispositivo de firewall. [Sitio web] Netgate [Consulta: 21 de noviembre de 2020] Disponible en https://www.netgate.com/solutions/pfsense/xg-1541-1u-dual.html

ORACLE. ¿Qué es un SOC? [Sitio web] Oracle Database Security [Consulta: 10 de octubre de 2020] Disponible en https://www.oracle.com/es/database/security/que-es-un-soc.html

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS OEA. Buenas prácticas para establecer un CSIRT nacional. Estados Americanos, 2016. p. 13-81.

POLICÍA NACIONAL DE COLOMBIA. Ciberincidentes. [Sitio web] Colombia [Consulta: 10 de octubre de 2020] Disponible en https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real/historico

PROCTER, Sam y BOYDSTON, Alex. Integrating Safety and Security Engineering for Mission-Critical Systems [Video]. YouTube, SEI, 2019. 59:56 minutos [Consulta: 10 de octubre de 2020] Disponible en: https://youtu.be/5-nZG4pPEr4

SOC COLOMBIA. Security Operation Center. [Sitio web]. Colombia, 2019. [Consulta: 10 de octubre de 2020] Disponible en. http://www.soccolombia.com/documentos.php

SOFTWARE ENGINEERING INSTITUTE. Create a CSIRT [Sitio web]. Pittsburgh, USA. White Paper, SEI, 2017. [Consulta: 21 de noviembre de 2020] Disponible en: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485693

SUAREZ, Ángela. TRES NIVELES DE LECTURA [Sitio web]. Colombia, 2019 [Consulta: 6 de marzo de 2021] Disponible en https://eclipsegrafia.blogspot.com/2019/06/tres-niveles-de-lectura.html

TICTAC. Tendencias del Cibercrimen en Colombia 2019-2020. Bogotá, 2019. p. 7-36.