FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

PROPUESTA DE UN MODELO PARA LA IMPLEMENTACIÓN DE UN SIEM EN PYMES

AUTOR

DIEGO ANDRES PANCHI PANCHI

AÑO

2020

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

PROPUESTA DE UN MODELO PARA LA IMPLEMENTACIÓN DE UN SIEM EN PYMES

Trabajo de Titulación presentado en conformidad a los requisitos establecidos para optar por el título de Ingenieros en Electrónica y Redes de Información.

Profesor Guía

Ms. Iván Patricio Ortiz Garcés

Autor

Diego Andres Panchi Panchi

Año

2020

DECLARACIÓN PROFESOR GUÍA.

"Declaro haber dirigido el trabajo, propuesta de un modelo para la implementación de un SIEM en PYMES, a través de reuniones periódicas con el estudiante Diego Andres Panchi Panchi, en el semestre 202020, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".

Iván Patricio Ortiz Garcés

Magister en Redes de Comunicaciones

C. I. 0602356776

DECLARACIÓN PROFESOR CORRECTOR.

"Declaro haber revisado este trabajo, propuesta de un modelo para la implementación de un SIEM en PYMES, del estudiante Diego Andres Panchi Panchi, en el semestre 202020 dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".

William Eduardo Villegas Chiliquinga

Magister en Redes de Comunicaciones

C. I. 1715338263

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE.

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

Diego Andres Panchi Panchi

C. I. 1724869241

AGRADECIMIENTOS

Agradezco a mis padres por su apoyo incondicional, por estar siempre presentes y por ayudarme a cumplir mis objetivos. Agradezco también a toda mi familia por creer en mí y por todos los consejos que me han dado, me han ayudado a ser cada día mejor y a siempre creer y a confiar en mí.

DEDICATORIA

Este trabajo va dedicado a mis padres y hermano, son lo mejor que tengo y son mi motivación para alcanzar mis objetivos. Se lo dedico también a mis tías Myriam y Jeanneth que ocupan un lugar especial en mi corazón pues me han ayudado desde niño y han estado presentes en los peores momentos. Espero hacerlos sentir orgullosos.

RESUMEN

Este proyecto de titulación busca diseñar una propuesta de un modelo capaz de ofrecer una alta eficiencia en el manejo de la seguridad informática para redes de empresas pequeñas y medianas. Para alcanzar ese objetivo se profundizará en temas relacionados con los riesgos, vulnerabilidades, amenazas y ataques más comunes dirigidos a esas infraestructuras de red, conceptos que ayudarán

a tener una visión y un contexto general de la problemática que rodea al entorno empresarial.

Para encontrar una solución al problema expuesto anteriormente se analizarán una serie de herramientas denominadas SIEM, las cuales cuentan con varios controles encargados de monitorear y mantener seguras las redes, esas herramientas serán estudiadas tomando en cuenta sus características y su habilidad para adaptarse al entorno de las empresas PYMES, eligiendo así, la más adecuada para cubrir con sus necesidades en cuanto a la seguridad de la información. Posteriormente se analizarán las normas ISO para encontrar el estándar que mejor se adapte al manejo de términos de seguridad informática y búsqueda de soluciones en caso de incidentes, esto con el fin de seguir sus directrices para la implementación y gestión del SIEM.

Por último, tomando en cuenta los resultados obtenidos del análisis previo, se desarrollará la propuesta del modelo para la implementación de un SIEM en PYMES que brinde seguridad en sus redes.

ABSTRACT

This degree project seeks to design a proposal for a model capable of offering high efficiency in the management of computer security for networks of small and medium-sized companies. To achieve this objective, the topics most common risks, vulnerabilities, risks and attacks directed at these network infrastructures will be explored, concepts that help to have a vision and a general context of the problems that surround the business environment.

In order to find a solution to the previously exposed problem, a series of tools called SIEM will be analyzed, which have various controls in charge of monitoring and keeping networks safe, these tools will be studied taking into account their characteristics and their ability to deal with the environment. SMEs, thus choosing the most appropriate to meet their needs in terms of information security. Subsequently, the ISO standards will be analyzed to find the standard that best suits the handling of computer security terms and search for solutions in the event of incidents, this in order to follow its guidelines for the implementation and management of the SIEM.

Finally, considering the results obtained from the previous analysis, develop the model proposal for the implementation of a SIEM in SMEs that provides security in their networks.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Introducción

En la actualidad se observa como la tecnología ha ido ganando un espacio importante en la vida diaria de las personas, estos avances tecnológicos procuran ofrece un buen vivir a la sociedad y se deben a que un gran número de científicos, empresas y demás elementos afines a estos campos se encuentran trabajando constantemente en la búsqueda de soluciones a los problemas más comunes que enfrentan las persona.

El sector que presenta una mayor evolución es el de los sistemas de información, sector cuyo desarrollo se ve claramente influenciado por la dependencia que existe por parte de las personas a encontrarse siempre conectados, intercambiar información, compartir software, hardware, etc. Esta dependencia o necesidad deriva a su vez en que la seguridad informática adquiera un rol fundamental ya que se necesita proteger todas las actividades que realizan las empresas pues el manejo de la información es catalogado como un aspecto crítico que debe estar en constante monitoreo.

La necesidad de implementar seguridad informática nace de la facilidad con la cual actualmente se accede tanto a información como a herramientas que pueden y son utilizadas para encontrar y explotar vulnerabilidades en una red. A este problema se lo denomina ataque, acción que es realizada en su mayoría por personas ajenas a la empresa atacada y que a su vez reciben el nombre de Hackers, buscan robar, modificar o eliminar información valiosa tratando de encontrar algún tipo de beneficio o simplemente tratando de causar daños a nivel de software o hardware en los equipos que conforman la red con lo cual detener el normal funcionamiento de la empresa.

Por esos problemas es fundamental contar con personal instruido en la seguridad de redes que aparte se encuentren equipados con los sistemas adecuados para prevenir ataques o minimizarlos hasta un punto en el que no representen un riesgo claro.

Los datos muestran que el 63% de empresas pequeñas y el 60% de empresas medianas a nivel global han sido víctimas de diversos tipos de malware como: virus, gusanos, troyanos, spyware, etc. Es importante destacar que dentro del rango de empresas Pymes se registra un porcentaje mínimo en lo que representan ataques de tipo Phishing, DoS y Ciber-espionaje, estos ataques en su mayoría se realizan a empresas grandes (Jiménez, 2017).

Hay que tomar en cuenta que no se puede hablar de una red que sea 100% segura (Kaspersky, 2016), que esté libre de ataques y que no pueda ser hackeada, lo que se puede hacer y se ha venido realizando es implementar un sistema gestor de eventos de seguridad informática que nos ayude a tener una mayor seguridad.

Una muestra de las bondades que aporta el implementar el sistema gestor de eventos OSSIM es lo realizado en la infraestructura de red del Gobierno Autónomo Descentralizado de la Provincia de Chimborazo donde la implementación del sistema dio a conocer varias problemáticas, como por ejemplo: un software sin soporte con una gran cantidad de puertos abiertos, navegación web en sitios potencialmente peligrosos, la red con más vulnerabilidades serias es en la que se encuentran los servidores web, DNS y mail, los puertos más utilizados en ataques son el http y https, Skype y Google Talk son las aplicaciones que más alertas generan (Morales y Guerrero, 2015).

La tabulación de los resultados obtenidos de la implementación de OSSIM en la red del Gobierno Autónomo Descentralizado de la Provincia de Chimborazo dio a conocer los porcentajes de gravedad de las vulnerabilidades donde, el 1% son serias, el 8% son altas y el 91% son bajas, demostrando que OSSIM nos permite detectar los ataques de red y por tal motivo sirviendo para conseguir el objetivo de monitorizar las redes de empresas pequeñas y medianas (Morales y Guerrero, 2015).

Otro ejemplo es lo realizado en el sistema de la Universidad tecnológica empresarial de Guayaquil (UTEG) donde el resultado obtenido del sistema termino por detectar diez riesgos que comprometían directamente a 20 procesos que eran considerados críticos en la red de datos de la Universidad, siendo la peor vulnerabilidad encontrada la alta temperatura a la que están expuestos los equipos, siendo su posible causa la falta de refrigeración e infraestructura inadecuada (Espinoza, 2015).

Como solución a los problemas encontrados con el sistema OSSIM, en la UTEG se diseñó un nuevo esquema que permita mejorar la seguridad informática en la red de datos, para esto se propuso llevar a cabo la implementación de una serie de servidores dedicados a informar sobre vulnerabilidades y amenazas (Espinoza, 2015).

Alcance

Este proyecto de titulación busca encontrar un mecanismo que permita generar un registro de los eventos afines a la seguridad informática que necesitan monitorear empresas pequeñas y medianas, implementando para esto un gestor de eventos que permita detectar vulnerabilidades y amenazas.

Para el control sobre los eventos se utilizará el sistema OSSIM ya que se ajusta a nuestras necesidades que se basan principalmente en conocer las vulnerabilidades y riesgos presentes en la red de empresas pequeñas y medianas, además, su licencia es gratuita logrando de esta forma una reducción de costo que es necesario para no causar un gran impacto en el factor económico, adicionalmente se analizaran las bondades de otros sistemas que son tanto gratuitos como de paga.

Se analizarán las normas ISO/IEC 27001 e ISO/IEC 27002, normas que se pueden utilizar para un sistema de gestión de eventos, se estudiaran sus especificaciones técnicas y resultados encontrados a través de la experiencia vivida en otros proyectos en los que han sido utilizados.

Simularemos la monitorización de los equipos y por medio de la generación de un registro de los eventos se encontrarán riesgos que es posible que ocasionen una falta de disponibilidad y confiabilidad de los servicios prestados por estas empresas.

Justificación

Hoy en día los datos de personas, información de empresas y demás activos informáticos con los cuales cuentan empresas Pymes se han convertido en parte importante en el giro de sus negocios, se han encontrado amenazas que significan un riesgo para la protección de estos datos y por ende para el buen funcionamiento del negocio, entonces, es importante contar con un sistema que sea capaz de garantizar la seguridad informática de estas empresas consiguiendo mantener la confidencialidad e integridad de las mismas.

A razón de que, en la actualidad la información de cómo realizar ataques o encontrar vulnerabilidades en una red es abundante y está a disposición de todos, los riesgos a los que la información se expone han aumentado ya que personas no autorizadas podrían ser capaces de llegar a los equipos o la base de datos, consiguiendo así robar información, añadir virus, etc.

Buscando controlar las amenazas y proteger a estas empresas de los ataques, se ha detectado que se necesita contar con un sistema que nos ayude a la gestión de eventos de seguridad informática para reducir las amenazas

llevándolas hasta un punto donde los daños realizados no signifiquen un riesgo claro para el negocio.

Objetivos

Objetivo General

- Implementar un sistema de gestión de eventos de seguridad informática en un entorno simulado para la red de pequeñas y medianas empresas.

Objetivos Específicos

- Análisis del mercado de las herramientas de gestión de eventos de seguridad informática que poseen licencia gratuita y de paga.
- Estudio de las normas que se pueden utilizar para un sistema de gestión de eventos de seguridad informática.
- Implementar el sistema de gestión de eventos de seguridad informática en un entorno simulado.

1 CAPITULO I. MARCO TEORICO

En este capítulo se plantea dar introducción a los conceptos generales relacionados a la seguridad de la información, vulnerabilidades, riesgos y ataques a infraestructuras de redes Pymes, además de dar conceptos de posibles soluciones que ayuden a mitigar estos problemas.

1.1 PYMES

También llamado pequeñas y medianas empresas. En el territorio ecuatoriano una empresa entra en este concepto al tomarse en cuenta el número total de trabajadores de los que el negocio dispone, el volumen de ventas que se registra, el número de años que se encuentra tal negocio vigente en el mercado y los niveles que se presentan en cuanto a producción, representando en otras palabras el capital del que se dispone. Es importante entender que no es una definición que sea estricta para todos los negocios pues muchos de ellos se encuentran en constante cambio dependiendo de la situación del mercado y de la situación económica del país. (Pico, 2016)

1.2 Seguridad de la información

Si se necesita una red que disponga de medidas de seguridad de la información, se debe tomar en cuenta que no solo se trata de la compra de equipos, no por adquirir los de última generación o tal vez los más costosos significa que su red se va a encontrar libre de ataques o de posibles infiltraciones por parte de terceros, si bien contar con estos equipos ayudaría de cierta forma, se necesita del compromiso por parte de todos los integrantes de la compañía para enfocar correctamente los puntos a tomar en cuenta dentro de lo que es la seguridad de la información y seguridad informática pues ambas partes se complementan.

Para entender que es seguridad de la información es importante saber que es seguridad y que se entiende por activo, la primera de ellas nos explica que se refiere a un sistema que se encuentre libre de todos los peligros que la comprometan física y virtualmente, la segunda se refiere a los activos con los que cuenta y sirven de base para el funcionamiento de la empresa. (Luzón, 2017)

El objetivo principal es ese, conseguir establecer medidas de seguridad sobre los activos informáticos que tiene la empresa, de eso nos habla la seguridad de la información, de una protección de los activos en la que no importa su estado o forma utilizando para esto protocolos que actúan sobre los riesgos existentes, las normas, las buenas prácticas y las estructuras organizaciones. Puntos que sirven como pauta para la construcción de medidas aplicables en caso de emergencia, así como para cumplir con niveles óptimos de seguridad en los procesos.

Entonces, se entiende que esta parte se enfoca en la protección de los datos que son manejados en los sistemas de la empresa pues estos son vistos como activos valiosos que en caso de ser vulnerados no solo traería consigo problemas económicos sino también afectaría a la imagen y a la seriedad que la empresa muestra a sus clientes, por ello, es necesario que la seguridad de la información se encuentre presente en los objetivos principales de cualquier negocio.

Al hablar de este tipo de seguridad nos referimos a ella como una técnica que es utilizada con el fin de realizar un estudio del entorno de la empresa, buscando consigo posibles vulnerabilidades y riesgos con el fin de implementar protocolos para el desarrollo y uso de políticas, esquemas, procedimientos a llevar a cabo en cada área en caso de ataques, control de accesos definidos dependiendo del rol de cada persona y para la protección de la red la implementación de un sistema de seguridad informática en caso de que se haya resuelto su necesidad en el análisis previo. (Luzón, 2017)

1.2.1 Principios de la seguridad de la información

Para establecer de forma óptima tanto las normas como las políticas de seguridad a seguir se han establecido tres principios, estos servirán como base para desarrollar todos los planes orientados a la seguridad de la información, estos principios son: confidencialidad, integridad y disponibilidad:

- **Confidencialidad:** asegura mantener la privacidad de toda la información que se encuentre almacenada dentro de un determinado sistema, dando acceso de forma única a aquellos usuarios que se encuentren autorizados a ingresar a tal información, protegiendo los datos de posibles infiltraciones por parte de terceros. (Morales & Guerrero, 2015)

- **Integridad:** se fundamenta en la preservación de la información almacenada asegurando con ello la veracidad, validez, exactitud, completitud, precisión y consistencia tanto de los datos como de los métodos que se van a utilizar para procesar o transformar esta información. (Morales & Guerrero, 2015)

- **Disponibilidad:** habla sobre garantizar el acceso continuo a todos los usuarios que se encuentren autorizados a interactuar con determinada información almacenada dentro del sistema, este principio adquiere mayor importancia en negocios que están orientados a la prestación de servicios de forma permanente. (Morales & Guerrero, 2015)

1.3 Seguridad informática

Nos habla de un conjunto de estrategias o procesos técnicos que se encuentran destinados a proteger las redes e infraestructura de la empresa, buscando mantener la disponibilidad, la integridad y la confidencialidad de los datos, en otras palabras se limita a proteger toda la información en formato digital junto a los equipos y los procesos informáticos que se encargan de su procesamiento y almacenamiento, entonces, la seguridad informática viene a monitorear y

conseguir evaluar el estado en tiempo real de la red, esto con el fin de llevar a las amenazas hasta un punto en el que no representen un riesgo claro. (Carpentier, 2016)

Enfocando esta necesidad hasta el escenario de empresas Pymes se ha determinado que lo que se busca es encontrar soluciones de bajo presupuesto, es decir, que no necesiten de una gran inyección de capital para la compra de hardware o software. Como respuesta apareció el análisis de riesgos, nos muestra las amenazas que son más frecuentes y reincidentes a los que se enfrenta a red para poder planificar, desarrollar e implementar procesos de controles de seguridad.

Actualmente la información de la que hemos hablado ya no se encuentra escrita sobre una hoja de papel y almacenada en anaqueles sino más bien la mayoría se guarda en equipos informáticos cuya estructura se encuentra diseñada para el ingreso, almacenamiento, transformación y entrega de esta información. De la protección de aquellos equipos y de todo lo que contiene es de lo que la seguridad informática se encarga, hace uso de firewalls, antivirus, monitoreos, IDS, correlación, etc., que, siendo bien utilizados por medio de los protocolos establecidos, van a permitir encontrar soluciones a los problemas de la empresa. (Carpentier, 2016)

Buscando una diferencia entre estos conceptos se puede decir que la seguridad informática se encuentra enfocada a medios informáticos mientras que la seguridad de la información se enfoca a diferentes medios. Para poder contar con un sistema seguro de protección de red y de su entorno hay que trabajar con estos dos términos pues es clave que ambos se encuentren interconectados.

1.3.1 Conceptos básicos en seguridad informática

Sabiendo que el concepto de seguridad informática y todos los términos que se encuentran relacionados a su definición son abundantes, se procede a explicar los más relevantes, los mismos que sirven como base y apoyo para la construcción de un sistema que proteja los datos y logre encontrar la seguridad informática idónea para los requerimientos de la empresa, dichos términos son:

- **Información:** se entiende como un conjunto de datos que ya han sido procesados, ordenados y transformados para generar nuevo conocimiento a una persona o para proporcionar un valor (activo) a una empresa. (Chanaluisa, Meza & Tasipanta, 2012)

- **Vulnerabilidad:** fragilidad que se encuentra presente dentro del sistema informático que puede ser utilizado por terceros para generar daños a los equipos, consiguiendo falta de consistencia en su funcionamiento o en su defecto logrando corromper la información causando estragos en la confidencialidad, integridad y disponibilidad de estos.

  Estas vulnerabilidades son fruto de las limitaciones que presenta la tecnología en uso, posibles fallos en hardware o software o por falla humana, por lo cual, se concluye que no existe un sistema que sea seguro en su totalidad. (Incibe, 2017)

- **Riesgo:** habla de la probabilidad que existe de que una amenaza se materialice y se transforme en un problema para el normal funcionamiento y el giro del negocio que realiza la empresa, un correcto análisis sobre los riesgos a los que la empresa se expone conllevaría la creación de un plan de contingencia que evite a una amenaza materializarse hasta un nivel en el que cause un impacto.

- **Ataque:** es un intento por parte de un tercero que no presenta las credenciales apropiadas para ingresar a determinada información, utilizando formas violentas para acceder al sistema buscando modificar,

eliminar, robar información o dañar los equipos para conseguir algún tipo de beneficio.

- **Monitoreo:** acción que permite interactuar constante al administrador de red con el sistema de vigilancia que se encarga de detectar posibles riesgos o ataques presentes dentro de la red, permite controlar observado la forma en que se van desarrollando las acciones cotidianas de la empresa dentro del sistema.

- **Protocolos:** se refiere a un conjunto de normas o de buenas prácticas que se deben seguir para el manejo de distintas situaciones que se presenten en caso de que aparezcan eventos que alteren el funcionamiento del sistema, se usan estos protocolos para regular todo lo que se refiere al manejo de los distintos recursos que cuenta el sistema, como la seguridad, la protección, etc. (Luzón, 2017)

- **Control:** se refiere a aquellas acciones que se realizan para prever o evitar que un riesgo se materialice, entre sus puntos se encuentra la autorización del acceso a la información, políticas, autenticación y demás procesos que se encuentren relacionados con la seguridad informática. (Luzón, 2017)

1.3.2 Elementos de la seguridad informática

Este tipo de seguridad tiene como base el proteger todos los elementos informáticos que son utilizado y se encuentran almacenados en el sistema, por ello, se toma en cuenta cuatro factores que se encuentran constantemente interactuando con esta información, pues son responsables directos y resultan ser la clave para contar con una seguridad informática que no presente grietas en los mecanismos de los que está compuesta, estas bases son:

- **Empresa:** principal responsable de designar tanto los recursos económicos como el personal calificado necesario para el análisis de las vulnerabilidades de la red y posterior construcción de los mecanismos de defensa que ayuden al cumplimiento de los principios anteriormente expuestos en la seguridad de la información. Se requiere de una implicación total del personal ubicado en los altos cargos de la empresa, de su implicación para ayudar y facilitar todos los procesos de investigación.

- **Usuarios:** se refiere a las personas para las cuales está diseñada la topología de red, así como el giro de negocio de la empresa. Son las únicas personas que se encuentran autorizadas a ingresar a su información, así como son las únicas que pueden hacer uso de los recursos o servicios de la empresa.

  Al brindarles acceso al sistema hay que tomar en cuenta que están autorizadas a observar su información y no la de otros usuarios, siendo necesario para esto, elaborar controles destinados al único acceso de la información autorizada, no se descarta la posibilidad de que un usuario sea responsable de un ataque o simbolice una vulnerabilidad en el sistema. (Espinoza, 2015)

- **Equipos:** es el conjunto de herramientas de Hardware y Software encargado de dar servicios y brindar recursos a los usuarios. En cuanto a los procesos que estos realizan se encargan de la recolección, procesamiento, transformación, almacenamiento, respaldo y distribución de la información a los usuarios o a los interesados que tengan autorización, es decir, dichos equipos están destinados a dar facilidades en el día a día de los usuarios pues no visualizan el proceso que se lleva a cabo sino únicamente son conscientes del resultado que se les entrega. (Luzón, 2017)

- **Administrador de red:** persona o grupo de personas que se encargan de administrar las redes informáticas, entre sus funciones se encuentra

mantener siempre operativa y optima la red de la empresa con el fin de que sus servicios se brinden correctamente. Trabaja en conjunto con los equipos y sistemas diseñados para la red pues a su vez es el encargado de su monitoreo, se muestra siempre alerta y en búsqueda de posibles vulnerabilidades para dar respuesta a ataques.

1.4 Ciberseguridad

Es vista como un conjunto de medidas que sirven como un mecanismo de protección para los activos informáticos, utilizan para ello diferentes protocolos que ayudan a disminuir el factor de riesgo a los que se expone la información en cualquiera de sus estados, estos pueden ser: información siendo procesada, transportada de un lugar a otro, interconectada mediante equipos de red o almacenada dentro de cualquier punto del sistema. (Porras & Salazar, 2016)

Se diferencia de los otros términos de seguridad anteriormente hablados en el punto en el cual la ciberseguridad no solo aplica medidas de defensa contra ataques sino también es capaz de aplicar medidas ofensivas contra estos.

1.4.1 Fases de ciberseguridad

Conociendo los peligros a los que se expone la información en todas las partes del mundo es necesario protegerse contra estos, implicando para ello procesos de ciberseguridad que estén listos para tomar acción en caso de ser necesario, estas medidas aumentaran su efectividad una vez comprendidas las tres fases en las que se debe aplicar cada una, estas son: prevención, localización y reacción.

- La primera medida en consideración es la prevención, como en la mayoría de los procesos y situaciones en la vida es conveniente prevenir un mal evento antes que afrontar sus consecuencias. Llevándolo al término de la

seguridad de la información, esta fase ayuda a disminuir el porcentaje de riesgo sobre el sistema. Esto significa actuar de forma temprana, analizando los sistemas e identificando vulnerabilidades y amenazas para la posterior construcción de protocolos que tomaran acción en caso de que una vulnerabilidad se materialice en un ataque. (Ciber, 2019)

- En caso de que la prevención no haya cumplido su objetivo, el siguiente paso es la localización del problema para su posterior erradicación. Una herramienta de uso común en este paso es el antivirus que dependiendo de sus características nos puede ayudar a detectar el problema en tiempo real, sin embargo, en caso de tratarse de un hacker intentando infiltrase, resulta complejo que un simple antivirus logre tal hazaña, por ello, es necesario tomar en consideración la utilización de un sistema para monitorear los eventos en red. (Ciber, 2019)

- Habiendo ya localizando la amenaza, el siguiente paso es la reacción, para ello se debe considerar los protocolos anteriormente establecidos en la etapa de prevención, utilizándolos para dar una respuesta técnica y efectiva que lleve dichos problemas hasta un punto en el que no representen un riesgo claro para la empresa. (Ciber, 2019)

  En caso de no haber logrado neutralizar la amenaza y llevando la situación hasta un punto crítico lo más recomendable es desconectar los equipos, cambiar las contraseñas del personal que tiene acceso al sistema, llevar a cabo una limpieza total para que no existan peligros en el futuro y en caso de encontrar pistas de que los datos hayan sido corrompidos, sustituirlos por sus copias de seguridad. Tomando en cuenta que los datos han sido vulnerados es importante dar conocimiento a los usuarios afectados y dar parte de lo ocurrido a las autoridades.

1.5 Elementos que requieren protección

La seguridad de los equipos que permiten llevar a cabo todos los procesos de gestión y almacenamiento de la información recolectada es vital, para ello, se necesita contar con seguridad física, tanto de personal que sea capaz de proteger a los equipos de robos, huelgas y desorden social, como de sistemas ya integrados en las salas de equipos que lo protejan de inundaciones, fallas del suministro eléctrico, terremotos, fallas en la refrigeración, etc. Comprendidos dichos escenarios los equipos que deben tomarse en cuenta para encontrase en dichas salas especializadas, son los siguientes:

- Servidores, Routers, Switches.
- Computadoras, laptops, hosts.
- Elementos de conexión con otros equipos.
- Data Center.
- Terminales.
- Software utilizado para la conexión de aplicaciones y redes.

Hay que considerar que al proteger estos recursos nos encontramos protegiendo a todo el sistema de la empresa y dependiendo del caso a otras redes a las cuales se tenga acceso pues todo se encuentra interconectado.

1.6 Vulnerabilidades

Son todas aquellas situaciones que ocasionan un riesgo claro contra la seguridad o la estabilidad del sistema, entendiéndose de igual forma como un punto débil que puede y tiende a ser explotado por terceros.

1.6.1 Amenazas que causan vulnerabilidades

Para entender de donde provienen las vulnerabilidades es importante tomar en cuenta las amenazas que causan dichos problemas y que directa o indirectamente se encuentran siempre latentes apuntando hacia el sistema. Las amenazas por tomar en consideración son:

- **Naturales:** se encuentran enfocadas a aquellas vulnerabilidades relacionadas con la naturaleza. El riesgo que se presente tiende a variar dependiendo del clima, de la ubicación, de la cercanía de servicios de policía, bomberos y de la infraestructura que se haya armado para proteger a los equipos de distintos contratiempos como: huracanes, incendios, terremotos, etc.

- **Hardware:** en este nivel las vulnerabilidades son causadas por defectos al momento de fabricar los equipos o al momento de configurarlos, hay que prestar especial importancia a si se les da un uso adecuado, si el ambiente en el que se encuentran es el ideal, así como a las actualizaciones que los equipos vayan necesitando. (Balarezo & Poveda, 2015)

- **Software:** vulnerabilidades causadas por la descarga de programas o información que proviene de sitios no confiables, provoca un riesgo claro pues derivaría en una infección en los procesos del sistema. Otra causa puede ser su configuración, al no ser la adecuada es posible dejar ciertos vacíos que pueden ser explotados en un ataque. Finalmente, no se descarta las instalaciones no autorizadas pues significa que no han pasado por las pruebas pertinentes de la PC y antivirus, siendo directamente instaladas del internet. (Balarezo & Poveda, 2015)

- **Almacenamiento:** se encuentra toda la información ingresada al sistema y tiende a ser víctima del deseo de personas que no se encuentran autorizadas a su acceso, es uno de los sectores marcados como objetivo por los hackers. Hay que recordar que se podrían crear vulnerabilidades

en caso de que los soportes que se encargan de almacenar la información no se encuentren siendo utilizados correctamente facilitando el ingreso a terceros e incluso llegando al caso de que este mismo proceso afecte la confidencialidad, integridad y disponibilidad de los datos. (Balarezo & Poveda, 2015)

- **Humanas:** son los tipos de vulnerabilidad producidos por fallas humanas que pueden causar daños a la información que se encuentra almacenada y a los equipos que soportan toda la estructura del sistema. Estos fallos se deben principalmente a descuidos, falta de dominio sobre las funciones que una persona es responsable de ejecutar o por falta de instrucción sobre las medidas de seguridad que se deben adoptar en caso de que aparezca una amenaza.

1.6.2 Tipos de vulnerabilidades

Los puntos que presentan una mayor debilidad en la mayoría de los sistemas son las vulnerabilidades que se refieren a:

- **Diseño:** se refiere a un mal análisis previo que serviría como causa para un deficiente desarrollo de protocolos y de políticas de seguridad que en caso extremo puede que no estén elaborados.

- **Implementación:** engloba todos los errores que se da en la etapa de desarrollo del sistema siendo parte de estos los errores de programación y de configuración que sin duda puede ser la causa de la existencia de posibles puertas traseras que afecten al sistema.

- **Uso:** falta de preparación y de conocimiento por parte de usuarios, miembros de la empresa o responsables del sector de informática. Engloba la falta de atención y de cuidado al momento de conectar un equipo a puntos de internet desconocidos, acceder al sistema en

portátiles, celulares, tables o Netbooks, falta de cuidado en lo que se conecta en los lectores USB, etc.

1.7 Amenazas informáticas

Se define como amenaza informática a todos aquellos elementos, acciones o eventos que causan problemas que atenten contra la seguridad a la cual está sujeta la información y que busquen acceso a los datos, causar daños en los equipos o interrupción en cuanto a los servicios prestados. Para encontrar una grieta en la seguridad del sistema toman como punto de partida una vulnerabilidad existente en la red, lo que quiere decir que una amenaza llega a existir si encuentra una vulnerabilidad que puede llegar a ser explotada. (Fernández, 2013)

Entonces, si bien una amenaza puede ser ocasionada por terceros que se encuentren bien instruidos sobre temas informáticos, la mayoría de las veces una amenaza nace de las limitaciones, fallos en el monitoreo o poca planificación de la seguridad. Es importante resaltar que si una amenaza logra materializarse de forma exitosa escala en cuanto al peligro que conlleva para el sistema, transformándose en un ataque y ocasionando riesgos sobre los activos informáticos. Dependiendo del área en donde las amenazas informáticas se encuentren pueden ser clasificadas en dos tipos.

1.7.1 Amenazas internas

Son aquellas que provienen del interior de la empresa siendo ocasionadas por personas que forman parte del equipo de trabajo, ocurre de forma planificada o no ya que incluso se cataloga como amenaza interna a una persona que por descuido accede a sitios poco confiables, se conecta a redes inalámbricas desconocidas, deja las credenciales, contraseñas, llaves y demás controles de seguridad bajo libre acceso de terceros, etc. (Parra & Porras, 2007)

A las amenazas internas planificadas también se lo llama sabotaje corporativo y presenta mayor riesgo, la persona en cuestión tiene libre acceso a las instalaciones facilitando su movilidad hacia los equipos, tiene contraseñas que le permiten el acceso al sistema siendo posible que deshabilite mecanismos de protección como firewalls, IPS, SIEM y sobre todo tiene el conocimiento de cómo funciona la empresa y de en donde se encuentra la información sensible. (Aguilera, 2010)

1.7.2 Amenazas externas

Son aquellas que provienen de afuera de la empresa siendo causadas por personas que no se encuentran asociadas al equipo de trabajo, sin los accesos necesarios para tener en sus dominios la información que desean, realizan investigaciones buscando vulnerabilidades que puedan utilizar para ingresar al sistema, robar información, dañar los equipos, etc. Hacen uso de virus, troyanos, gusanos, espionaje industrial y demás mecanismos que les permita encontrar una puerta de acceso. (Parra & Porras, 2007)

1.8 Ataque informático

Es causado por las acciones que realiza una o varias personas aprovechando las vulnerabilidades encontradas en los componentes del sistema de la organización (hardware, software y personal) buscando algún tipo de beneficio económico o afectar los activos de la empresa consiguiendo la desestabilización del negocio. Al realizarse estos ataques el objetivo es comprometer los principios fundamentales en los que se basa la estructura de la seguridad de la información, la confidencialidad, integridad y disponibilidad de los datos.

Una forma de controlar los ataques o disminuir su nivel de peligro, es la utilización de protocolos enfocados al control sobre las vulnerabilidades encontradas en el análisis previo, este enfoque permitirá comprender la forma de actuar tanto de posibles malwares introducidos, así como la metodología que los atacantes pueden tomar para forzar su ingreso. Si bien contar con medidas y pasos a seguir en cada problema es una respuesta acertada y coherente, no deja de ser la mejor solución la educación del personal en términos de consejos sobre precaución con el uso y exposición de los activos de la empresa.

1.8.1 Fases de un ataque informático

Conocer las fases a los que usualmente se rigen los ataques informáticos es otra manera de adquirir cierta ventaja sobre los atacantes. Toda esta información es de gran utilidad para aquellos profesionales enfocados en la seguridad, permite comprender, analizar y adelantarse a las acciones que los intrusos puedan tomar para ingresar al sistema. En la Figura 1 se muestran las fases más comunes que siguen los ataques informáticos una vez iniciados.

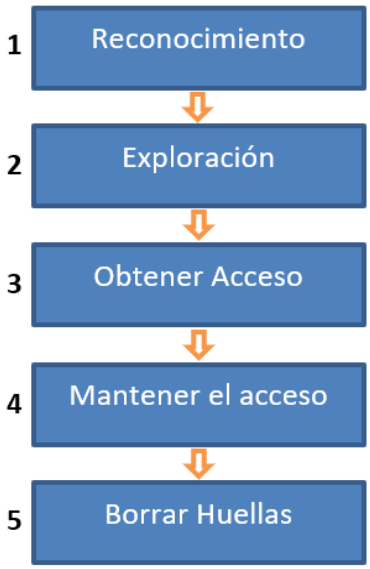

Figura 1. Fases de un ataque informático.

Tomado de (Mieres, 2019)

- La primera fase es tomada como una etapa de preparación, en esta se obtiene la información que se necesite sobre la persona o empresa marcada como objetivo del ataque informático.

  Para recolectar estos datos es común que el atacante utilice como recursos de búsqueda redes sociales, Google, Mail, Yahoo y documentos impresos para encontrar patrones que guíen a posibles contraseñas y demás información relacionada con su vida privada o el entorno de la empresa. En la fase de reconocimiento pueden aparecer técnicas de captura de datos más avanzados como son los casos de Ingeniería social, Sniffing, Dumpster Diving etc. (Mieres, 2019)

- La segunda etapa trata sobre el procesamiento y transformación de la información que fue recolectada en la primera fase, se sondea al objetivo buscando vulnerabilidades que pueden ser aprovechadas por los atacantes para tener acceso a la información. Estas vulnerabilidades pueden ser Hosts, direcciones IP, contraseñas, etc. En la fase de exploración aparece el uso de herramientas como mapeadores y escáneres de redes y de puertos, así como escáneres que buscan vulnerabilidades. (Mieres, 2019)

- En la tercera fase comienza el ataque, todos los datos obtenidos dejan de ser información procesada y comienzan a materializarse. Utilizando las vulnerabilidades del sistema que fueron encontradas en las dos fases previas, se accede al sistema y el atacante se prepara para la utilización de técnicas que le permitan robar información o causar una discontinuidad en los servicios brindados por el negocio, para ello, se apoya en la utilización de ataques de diferentes tipos como: desbordamiento de búfer, DoS, DDos, secuestro de sesiones y filtrado a nivel de contraseñas.

- En la cuarta fase el atacante se encuentra dentro del sistema, en este nivel ya tiene acceso a la información por tanto le es posible modificar, manipular y eliminar información. Lo que ahora busca es implementar herramientas que le brinden acceso de forma permanente desde

cualquier sitio donde disponga de un computador y acceso a internet, con ese fin, además de añadirle el deseo de no ser detectado para que no se tomen medidas de protección que le nieguen el acceso, recurre a utilizar troyanos, backdoors y rootkits. (Mieres, 2019)

- En la quinta fase el atacante ya logro obtener la información e implementar herramientas para mantener su acceso al sistema en el futuro, por tanto, el objetivo de esta fase es borrar todas las evidencias creadas por la intrusión forzada que realizo, esto se hace para no ser detectado por parte del personal que se encarga de brindar seguridad informática al sistema. Las evidencias que el intruso buscara eliminar son las alarmas que se hayan generado por parte del Sistema de Detección de Intrusos (IDS) y los archivos de registro. (Mieres, 2019)

1.8.2 Tipos de ataques informáticos

Conociendo el ciclo de vida común que presentan los ataques informáticos, es importante saber diferenciar sus tipos pues cada uno de ellos tienen su propia forma de actuar, su forma de infectar al sistema, su forma de atacar las vulnerabilidades y su forma de esconderse de las medidas de protección implementadas. Hay que mencionar, como bien fue hablado en los puntos 1.7.1 y 1.7.2 sobre las amenazas internas o externas, los ataques aparecen cuando estas amenazas se materializan, clasificándose en ataques pasivos y activos.

1.8.2.1 Ataques pasivos

En este tipo de ataque la comunicación y transmisión de los archivos no se ve interrumpida o alterada, el atacante se limita a monitorizar y escuchar pues la finalidad del ataque es capturar la información que es transmitida por esos canales. (Parra & Porras, 2007) En otras palabras, su objetivo es analizar el

tráfico que el blanco presente, así como interceptar los datos que transmite o recibe. La información que busca obtener es:

- El origen y destino de todas las comunicaciones que realice, utilizando para ello las lecturas de las cabeceras que se encuentran en los paquetes monitorizados.

- Las actividades que el individuo usualmente realiza, así como las que no está acostumbrada a realizar, para eso analiza el volumen del tráfico que se encuentra siendo intercambiado

- Las horas de actividad de la persona, utilizando como factor las horas habituales en las cuales se realizan los intercambios de comunicación.

Algunos ejemplos de estos tipos de ataques que se basan en escuchas o pinchazos electrónicos son los siguientes:

- **Sniffing:** es una técnica comúnmente utilizada por atacantes para monitorizar o escuchar el tráfico que se encuentra transitando por la red, para ello, se necesita de un sniffer, programa que sirve para capturar, interpretar y almacenar tramas. (Parra & Porras, 2007)

  El sniffer puede ser instalado dentro de un router, Gateway o en una estación de trabajo, sitios desde donde va a leer los mensajes que atraviesen su ubicación y va a ir recolectando toda la información que circule como contraseñas, correos electrónicos, usuarios, etc. Estos datos a su vez son grabados dentro de un fichero para su posterior obtención.

- **Tempest:** es la sigla de Tecnología de Vigilancia de Emisión de Pulsos Electromagnéticos Transitorios. Se basa en el principio de que todos los equipos electrónicos en funcionamiento son responsables de causar emanaciones magnéticas y eléctricas, estas emanaciones de las que se habla son posibles de captar y de transformarlas en información robando

de esta forma datos confidenciales. Por este problema hoy en día existen equipos que cuenta con filtros Anti-Tempest. (Parra & Porras, 2007)

- **Ingeniería Social:** es una técnica que se deriva de la habilidad que tienen los atacantes para tener acceso a información personal mediante manipulación y engaño. (Parra & Porras, 2007)

  Es vista como una técnica psicológica que conlleva a la otra persona a entregar voluntariamente información sensible como contraseñas o claves de acceso. Por lo general al usar este tipo de estrategia el atacante se hace pasar el administrador de red o miembros de soporte, para evitar caer en esta trampa es importante considerar educar a los usuarios pues son considerados como el eslabón débil en la cadena de todo sistema.

Estos tipos de ataques informáticos son los que resultan ser más complicados de detectar pues no dejan ninguna huella producto de que no se encuentran accediendo a los datos de forma agresiva. Para evitar estos problemas las medidas a considerar son el cifrado de la información, adquisición de equipos diseñados para la protección de datos y la educación de los usuarios.

1.8.2.2 Ataques activos

Este tipo de ataques tiene como característica modificar, eliminar o robar información, no dejando de lado su otro objetivo que se enfoca en mantener cierto control sobre los flujos de datos de tal forma que puedan crear un falso flujo y generar interrupciones o retrasos en las transmisiones de los usuarios. Resulta complicado detectarlos ya que tienden a camuflarse haciéndose pasar por eventos accidentales. Estos ataques pueden dividirse en cuatro categorías:

1.8.2.2.1 Suplantación de identidad

El atacante toma la identidad de otra persona permitiéndole ignorar controles de acceso y teniendo libre albedrio sobre secuencias de autenticación. Esta persona tendría acceso a todos los recursos y privilegios que la entidad suplantada poseía, en caso de tratarse de un usuario se lo puede comparar con el libre acceso a una cuenta ajena y en caso de hablar de un miembro que es parte y tiene un rol dentro de una organización resulta critico pues al tener los mismos privilegios y accesos de la persona que está suplantando significaría un riesgo potencial para la empresa.

1.8.2.2.2 Reactuación

Este ataque consiste en que uno o varios mensajes lícitos sean capturados para posteriormente repetirlos produciendo un efecto que no es el deseado. Se lo puede entender como ejemplo a la acción de ingresar dinero de forma repetida en una misma cuenta. (Parra & Porras, 2007)

1.8.2.2.3 Modificación de mensajes

Se lo realiza sobre mensajes lícitos que tienen tanto un emisor como uno o varios receptores, es el acto de tomar una porción de estos mensajes y alterarlos, retrasarlos o reordenarlos para dar otro tipo de razonamiento a quien se dirija él mensaje.

1.8.2.2.4 Degradación fraudulenta del servicio

Este ataque impide que se utilice de forma normal los recursos informáticos y de comunicaciones entre los usuarios o miembros de la misma organización. Se habla de que el intruso tendría la capacidad de evitar que una persona o área de

trabajo reciban mensajes causando posibles fallas como un mal desempeño o interrupción de los servicios prestados por medio del envió de una gran cantidad de mensajes basura. (Parra & Porras, 2007)

1.8.2.2.5 Ataques por códigos maliciosos

También conocido como Malware, es un software cuyo objetivo es ingresar al sistema sin la autorización del personal buscando espiar las acciones que realizan los usuarios, dañar archivos, corromper recursos o volver completamente no funcional al sistema.

A medida que la información va adquiriendo mayor importancia representa un beneficio económico para las compañías por ello los ataques por medio de códigos maliciosos se vuelven cada vez más comunes, más especializados y difíciles de tratar. Los malwares más utilizados son:

- **Virus:** software que ha sido creado con el objetivo de ocasionar fallos en el funcionamiento de equipos informáticos, perjudicando y alterando su rendimiento al remplazar archivos ejecutables que no se encuentran infectados por otros que ya tienen este código maligno. Son transparentes para los usuarios y tienen la habilidad de autorreproducirse. Se propagan por varios medios siendo los más comunes a través de dispositivos extraíbles y la red a la cual se encuentran conectados los equipos. (Parra & Porras, 2007)

- **Gusanos:** este malware tiene la característica de autorreplicarse para poder propagarse e infectar a otras computadoras, envía sus copias utilizando la red en uso causando perjuicios en la velocidad de internet pues consumen ancho de banda. A diferencia del virus los gusanos no dañan o generan cambios en los archivos de la computadora apuntada como destino y generalmente logran su ingreso a otro dispositivo disfrazándose en mensajes, archivos adjuntos o publicidad que son

enviados vía correo electrónico pidiendo ser ejecutados por él usuario. (Parra & Porras, 2007)

- **Troyanos:** es un software malicioso que se presenta al usuario como una aplicación o programa que puede ser de utilidad, genera interés en el usuario invitándolo a ejecutarlo, al hacer esto, permite inconscientemente al atacante el acceso de forma remota al equipo que se encuentra infectado dándole el poder de eliminar archivos, instalar programas con otros malwares, crear puertas traseras, etc. A diferencia de gusanos y virus los troyanos necesitan ser ejecutados ya que se encuentran en formato .exe y no tienen la habilidad de autorreproducirse. (Parra & Porras, 2007)

- **Spyware:** es un malware que se interesa en la recopilación de información que se encuentra almacenada en el ordenador infectado para enviársela a una entidad remota sin ningún tipo de consentimiento o conocimiento por parte del titular del ordenador. Muestra publicidad que no ha sido solicitada por el usuario, causan perdidas en cuanto al rendimiento del sistema, problemas de estabilidad del computador y problemas con las conexiones a internet. (Yubal, 2019)

- **Adware:** es un programa que cumple la función de ofrecer y mostrar publicidad que resulta ser engañosa o que simplemente no es del deseo del usuario. Usualmente se lo puede encontrar colgado en una página web en la que se está navegando, mostrándose con mensajes llamativos utilizando carteles, gráficos, diferentes tipos de letras, fuentes y colores con el fin de llamar la atención del usuario y generar ganancias mediante publicidad. (Yubal, 2019)

1.8.2.2.6 Ataques por denegación de servicios

El objetivo de este ataque es lograr que los recursos o servicios prestados por una empresa sean inaccesibles para los usuarios. Se llega a ese punto provocando que exista una perdida en cuanto a la conectividad con la red producto del insuficiente ancho de banda, para esto los atacantes saturan los puertos de los servidores con cientos de flujos de información que sumándole al procesamiento habitual que tienen los equipos, al momento de encontrarse con un evento poco común causa que el sistema colapse impidiendo la prestación de servicios o el acceso a los usuarios. (Luzón, 2017)

A diferencia de otros, los ataques DoS no buscan tener acceso a la información para modificarla o robarla, sino que busca afectar la imagen de la empresa dañando su credibilidad al no cumplir con el principio de disponibilidad viéndose en desventaja con sus competidores. Los ataques por DoS más utilizados son:

- **IP Flooding:** genera todo tipo de tráfico adulterado con la finalidad de ocupar un mayor ancho de banda para causar problemas en cuanto a los servicios de red producto de la lentitud en las comunicaciones. (Álvarez, s.f.) En la figura 2 se puede observar la forma de actuar de este ataque.

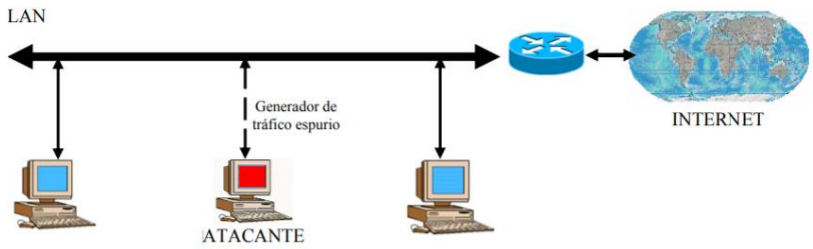

Figura 2. Ataque IP flooding.

Tomado de (Álvarez, s.f.)

- **Broadcast:** en este caso el atacante utiliza la dirección de identificación que pertenece a la red IP como el destino del paquete. Esto produce una serie de eventos en el cual el router se encuentra obligado al envío de dicho paquete a todos los computares que formen parte de la red causando tráfico y problemas en los servicios. (Álvarez, s.f.) En la figura 3 se puede observar la forma de actuar de este ataque.

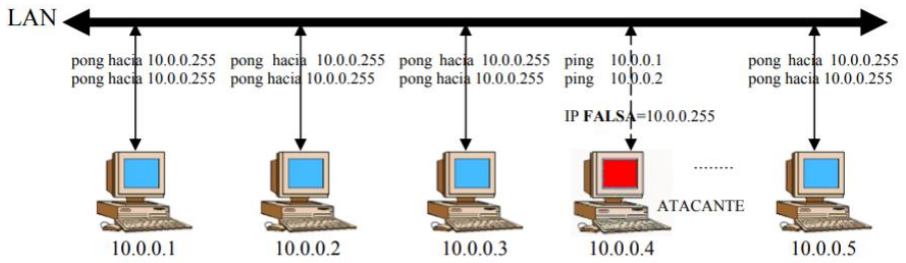

Figura 3. Ataque broadcast.

Tomado de (Alvarez, s.f.)

- **Smurf:** este ataque se dedica a crear falsificaciones de las direcciones de origen y destino procedentes de las peticiones de ICMP de ECHO. En el origen se coloca la dirección IP que pertenezca al blanco del ataque y en el destino se coloca la dirección broadcast de la red que va a ser utilizada para ocasionar el colapso del sistema en la máquina de origen. (Álvarez, s.f.) En la figura 4 se puede observar la forma de actuar de este ataque.

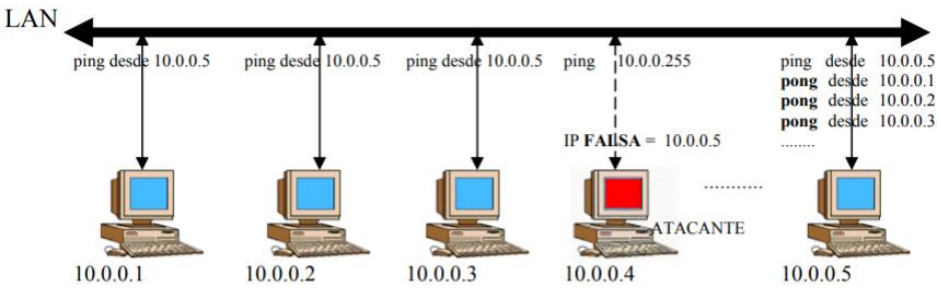

Figura 4. Ataque smurf.

Tomado de (Alvarez, s.f.)

- **LAND:** se lleva a cabo por medio de la falsificación de la dirección y del puerto de origen para que a su vez también sean utilizadas en el puerto de destino, esto va a causar que la maquina atacada se encuentre constantemente recibiendo peticiones que son enviadas por la misma máquina. (Álvarez, s.f.) En la figura 5 se puede observar la forma de actuar de este ataque.

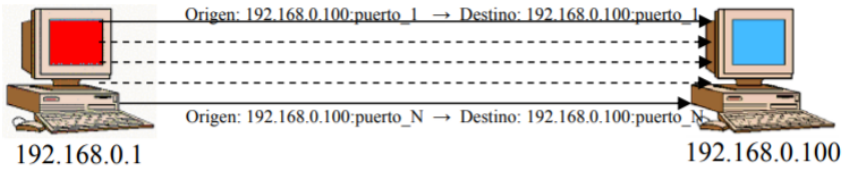

Figura 5. Ataque Land.

Tomado de (Alvarez, s.f.)

1.8.2.2.7 Ataques por denegación de servicios distribuidos

A este tipo de ataque se lo puede definir como una variante del ataque DoS, la diferencia radica en que la degeneración de servicio distribuido (DDoS) se realiza sobre varios equipos, sobrecargando los sistemas de los blancos del ataque con múltiples peticiones que son generadas por varias máquinas, para realizar estas acciones es posible que se necesiten redes gigantes de bots. (Gómez, 2019)

Analizando la estructura de red de un ataque DDoS se observa que genera más tráfico comparado a su predecesor que únicamente maneja un equipo. En la figura 6 se puede observar la forma de actuar de un ataque DDoS.

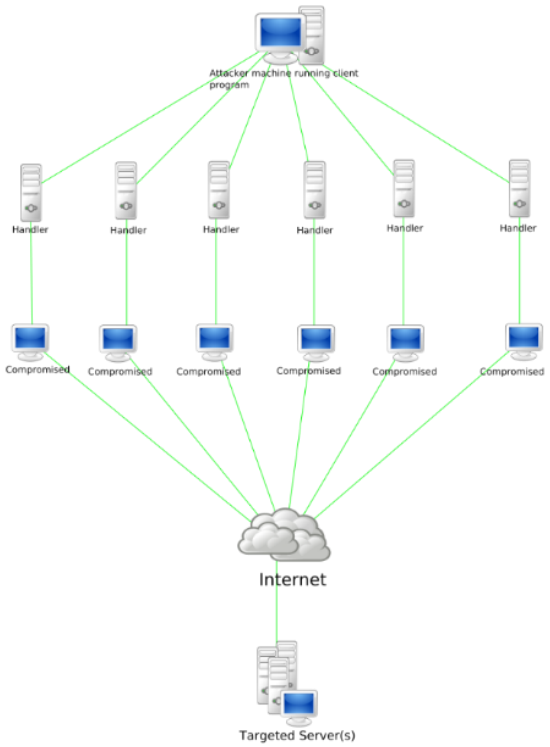

Figura 6. Ataque DDoS.

Tomado de (Alvarez, s.f.)

1.8.3 Formas de ataque a la seguridad informática

Dependiendo del tipo de método que utiliza una amenaza para realizar su ataque se lo puede dividir en cuatro categorías. En la figura 7 se observan las cuatro formas que una amenaza utiliza para atacar al sistema.

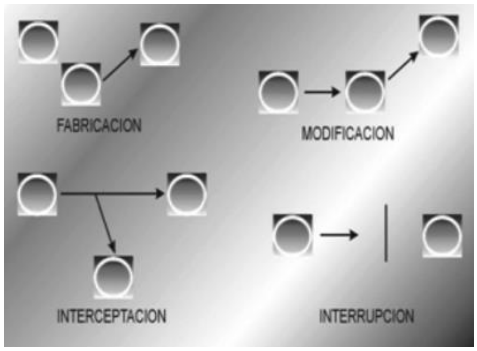

Figura 7. Formas de ataque.

Tomado de (Parra & Porras, 2007)

- **Fabricación:** se refiere a la modificación o interrupción de la información, en este método el intruso modifica o crea un contenido similar al interceptado para evitar que el destinatario sea capaz de diferenciar entre ambos, generando controversia en la autenticidad de la información que es recibida. (Parra & Porras, 2007)

- **Modificación:** en esta forma de ataque, el intruso se limita a interceptar información para modificar una trama del mensaje, consiguiendo cambiar la naturaleza de lo que fue escrito. (Parra & Porras, 2007)

- **Intercepción:** esta forma es similar a un pinchazo electrónico, el intruso se encuentra dentro de los canales de comunicación y se limita a escuchar sin alterar ni intervenir. Roba la información sin que su presencia se note. (Parra & Porras, 2007)

- **Interrupción:** las amenazas que siguen esta forma de ataque buscan impedir que los flujos de datos sean transportados hasta su destino. Este método es parecido al que utilizan los ataques de tipo DoS y DDoS pues saturan el servidor volviéndolo incapaz de dar respuesta. (Parra & Porras, 2007)

Analizando las formas de ataque a la seguridad informática, todos los tipos de ataques vistos con anterioridad siguen uno de estos caminos para causar daños en el sistema, siendo algunos más fáciles de detectar, otros más difíciles de controlar y otros los que presentan mayor riesgo.

1.9 Sistemas de gestión de la seguridad de la información (SGSI)

Es importante entender que, sin importar el estado del arte de la información, todos los datos van adquiriendo un valor, pues una vez procesados, las empresas pueden crear publicidad más asertiva, conocer tendencias de

consumo y encontrar posibles ideas para innovar. Puntos que sumándole a otros aspectos vuelven valiosa a la información, convirtiéndose ya en un factor económico y siendo víctima del deseo de terceros que buscan tener su acceso para lucrar con ella.

En vista del problema, la Organización Internacional para la Estandarización (ISO) y la Comisión Electrónica Internacional (IEC) resolvieron trabajar en equipo (ISO/IEC) y el resultado de la colaboración crearía el concepto de Sistema de Gestión de Seguridad de la Información (SGSI). Dicho concepto establece que, todos los sistemas involucrados con procesos SGSI se van a enfocar en la preservación de la información tomando como base mantener tres principios: la confidencialidad, integridad y disponibilidad, así como de la seguridad de los equipos y sistemas adicionales que se encuentren implicados en sus procesos. (Luzón, 2017)

Para brindar seguridad sobre la información y sus equipos relacionados hay que definir los controles que van a manejar los SGSI, se debe analizar los controles a utilizar tomando en cuenta las necesidades de la empresa pues esto permitirá disminuir el riesgo de ataques y la cantidad de vulnerabilidades del sistema.

Decir que una vez establecidos los controles se alcanza una seguridad total en el entorno de la empresa es imposible, ninguna red es 100% segura, por ello, estos sistemas se mueven bajo un prototipo de mejora continua que le permite supervisarse a sí mismo e ir aprendiendo de los resultados obtenidos y del porcentaje de eficiencia que presenta en cada control que realiza.

1.9.1 Modelo de procesos PDCA

Este modelo de proceso se basa en una estructura cíclica de mejora continua, la conforman cuatro etapas que deben seguirse sistemáticamente para alcanzar el

mejoramiento de los procesos, entendiendo como una mejora en la calidad al acto de controlar ataques, eliminar vulnerabilidades, solucionar problemas, elevar los porcentajes de eficiencia y generar opiniones positivas. (Orozco, 2013)

Al tener una estructura cíclica se da a entender que una vez recorrida la cuarta etapa se debe volver a la primera y repetir este ciclo constantemente de forma que tanto eventos como actividades que se hayan realizado sean reevaluadas de forma periódica buscando en cada ocasión añadir mejoras.

Este concepto es utilizado por los SGSI para que sus procesos se construyan y se rijan a un modelo de mejora continua que ayuden a crear mecanismos que solidifiquen una buena prestación de servicios, con eso se busca generar confianza con los clientes para mejorar relaciones, creciendo así la empresa como imagen y marca dentro del mercado. En la figura 8 se puede observar el ciclo que sigue el proceso PDCA el cual se encuentra formado por cuatro etapas.

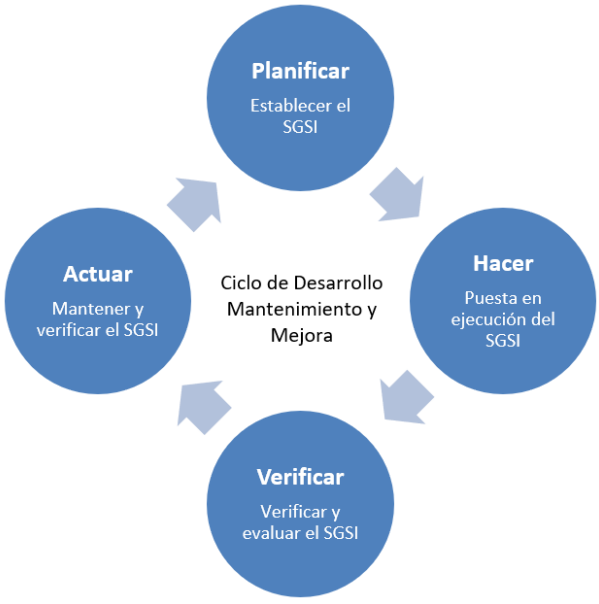

Figura 8. Esquema del ciclo PDCA.

Tomado de (Amutio, 2012)

- En la primera fase se diseña el SGSI. Se lo construye con la evaluación previa de los riesgos y vulnerabilidades de la empresa, se encuentran sus

objetivos y se selecciona los controles que van a ser instaurados para dar respuesta a estas amenazas. (Orozco, 2013)

- La segunda fase es la de implantación. Los controles que han sido seleccionados en la primera fase pasan a ser instalados y utilizados por el personal a cargo de su monitoreo. (Orozco, 2013)

- En la tercera fase se evalúa el desempeño. Se analiza, revisa y evalúa el rendimiento que el SGSI se encontraba ofreciendo en la segunda etapa hasta la fecha, está directamente relacionada con la eficiencia y eficacia que sus controles ofrecían frente a eventos inesperados. (Orozco, 2013)

- En la última fase se toman acciones que mejoren el rendimiento. Una vez que los controles hayan sido evaluados en la tercera fase, se procede a realizar los cambios o correcciones que se necesiten para impulsar al SGSI a un mejor rendimiento, es la acción de mantener lo bueno y mejorar lo malo del SGSI. (Orozco, 2013)

1.9.2 Normas para la seguridad de la información

Del trabajo que han realizado y que siguen realizando en conjunto la Organización Internacional para la Estandarización y la Comisión Electrónica Internacional se han escrito varias normas o estándares que están relacionados con los sistemas de gestión y que sirven como guías para establecer protocolos de seguridad, implementación y mantenimiento. Estos estándares son escritos para ser seguidos en todas partes del mundo, facilitando así, temas relacionados con el comercio, la adaptación de nuevas tecnologías y el intercambio de información.

Lo que se busca es que todas las empresas trabajen con normas o estándares que se encuentren avaladas a nivel mundial y que ya han mostrado su utilidad,

su otro objetivo es evitar el desarrollo de otras tecnologías que puedan causar dificultades a empresas de menor jerarquía al momento de adaptarse a las necesidades de los grandes conglomerados.

Dada la necesidad de estándares que ayuden con el análisis previo e implementación de un sistema de gestión de seguridad informativa, la familia de normas que entra en escena son las normas ISO/IEC 27000 que proporciona normativas para gestionar la seguridad y que son utilizables para implementarse en empresas grandes, medianas o pequeñas. La aplicación de las normas recomendadas por estas normativas se verá influenciada por las necesidades, objetivos, estructura y demás procesos presentes en la empresa a ser intervenida.

1.9.2.1 Norma ISO/IEC 27001

Esta norma fue desarrollada por la importancia que tiene la información que es procesada de forma electrónica, pues en la actualidad, las empresas manejan estos datos como los activos más importantes que se deben salvaguardar, incluyendo en este contexto una administración responsable que la mantenga libre de peligros, amenazas y posibles arremetidas violentas por parte de atacantes que fuerzan su acceso con el fin de robar esta información o corromper los datos.

Contra estos ataques se ha ido construyendo alrededor de la información mecanismos de defensa como procesos, medidas en caso de riesgos, consciencia en la mente de los empleados y la más importante de ellas, el tener instaurado un Sistema de Seguridad de la Información que se encuentre basada en los principios dictados por la norma internacional ISO/IEC 27001 que explicándolo a breves rasgos brinda apoyo en cuanto al análisis de riesgos, monitoreo, control e identificación sistemática de problemas que pueden surgir, todo esto, en tiempo real.

La norma ISO/IEC 27001 aparece por primera vez en octubre del año 2005 después de haber sido aprobada y publicada por el comité formado para su desarrollo (ISO/IEC). Una vez que ha sido implantada, esta norma tiene un sitio dentro del sistema de gestión general de la empresa pues viene a encargarse de los riesgos que puedan presentarse. Su objetivo es mejorar todos los canales de seguridad, creando, implementando, monitoreando, operando, controlando, manteniendo y supervisando eventos que mejoren el Sistema de Gestión de Seguridad de la Información. (Morales & Guerrero, 2015)

Al utilizar la norma ISO/IEC 27001 significa que nuestro sistema va a dejar de funcionar de forma intuitiva y tomara responsabilidades sobre los eventos que ocurren con la información que procesa la empresa.

1.9.2.2 Norma ISO/IEC 27002

La norma ISO/IEC 27002 aparecería por primera vez en escena en Julio del año 2005 bajo el nombre de ISO 17799:2005 después de que, como todas las normas publicadas fuera aprobada por el grupo de trabajo (ISO/IEC). Con el tiempo, para ser precisos el 1 de Julio del año 2007 cambiaria su nombre por el que actualmente lleva. (Villacís, 2016)

A esta norma se la conoce como Tecnologías de la información y Técnicas de seguridad ya que se basa en un conjunto de códigos, resultado de buenas prácticas que consiguieron mejorar la gestión de los elementos relacionados a la seguridad de la información, para ello, esta norma establece los principios que van a ser tomados como base, las directrices a usarse para su implementación, los métodos de mantenimiento a seguir y la mejora continua que va a regir sobre los controles, políticas, estructuras organizacionales y demás procedimientos del sistema sometidos constantemente a evaluación. (Barragán, Góngora & Martínez, 2011)

Las empresas que usualmente utilizan esta norma son aquellas que buscan conseguir los siguientes puntos:

- El desarrollo de una guía de gestión de seguridad de la información que resulte propia de la empresa
- Contar con controles en la seguridad de la información que sean aceptados a nivel mundial y hayan demostrado su valía en el control de amenazas.
- Realizar la selección correcta de los controles que se deben implementar en el sistema, tomando en cuenta tanto las necesidades de la empresa como la información brindada por la norma ISO/IEC 27001.

Los controles de seguridad de la información que maneja esta norma están estructurados de la siguiente manera: 14 dominios, 35 objetivos a controlar y 114 controles que a su vez se dividen en controles técnicos, normativos y organizaciones. En la figura 9 se puede apreciar la estructura que siguen los dominios de esta norma.

Figura 9. Dominios norma ISO/IEC 27002.

Tomado de (Barragán, Góngora & Martínez, 2011)

En el siguiente capítulo se analizará de forma más detallada las herramientas de gestión de eventos de seguridad informática.

2 CAPITULO II. HERRAMIENTAS DE GESTIÓN DE EVENTOS DE SEGURIDAD INFORMÁTICA

En este capítulo se analizarán diferentes productos SIEM gratuitos y de paga comercializados en el mercado, esto con la finalidad de conocer las características de cada uno de ellos para encontrar el sistema mejor enfocado y que ofrezca las soluciones más eficientes a las necesidades de empresas PYMES.

2.1 Que es un SIEM

Gestión de Eventos e Información de Seguridad, es un sistema desarrollado fruto de la convergencia de SIM y SEM, dos tecnologías cuyos rasgos resultaron ser complementarios para crear una estructura basada en la habilidad para monitorear, recopilar, correlacionar, agregar, gestionar eventos de red en tiempo real como proxys, logins, archivos de registro, accesos, IPS, etc., de la recopilación de esos datos realiza un análisis y los emite mediante informes que son registrados como eventos de seguridad ejecutados dependiendo de la situación en la cual se encontraba el sistema frente a una amenaza. (Fernández, Herrera & García, 2017)

De los resultados obtenidos por esos controles, se evalúa el comportamiento que ha ofrecido el sistema comprobando su efectividad y eficacia, determinando a la vez, el nivel de seguridad y en caso de ser necesario dejando la posibilidad a implantar posibles mejoras.

En breves rasgos un SIEM es un sistema que colecciona diferentes tecnologías de SIM y SEM para ofrecer protección a nivel de datos informáticos y equipos de red frente a posibles amenazas causadas por agentes externos o internos, es un sistema creado por la motivación de mantener la confidencialidad, integridad y

disponibilidades de los servicios que se prestan y de la información que siempre debe estar disponible para los usuarios.

2.1.1 Objetivos de un SIEM

Como ya se ha hablado con anterioridad al ser SIEM un sistema centralizado que parte de la colección de diferentes tecnologías de SIM y SEM también se ve en la necesidad de cumplir con sus objetivos utilizando para ello un algoritmo que se lo puede resumir en los siguientes puntos.

- Lograr una gestión centralizada de todos los medios de protección, sistemas técnicos instaurados en la red, eventos, alertas, software, sistemas operativos y demás infraestructura que se encuentre relacionada a las tecnologías de la información, este es un paso clave para evitar cuestiones que causan vulnerabilidades y futuros ataques causados por perder algún tipo de incidente ya que esto puede derivar directamente en un registro de eventos eliminado, en que el firewall o antivirus se encuentren desactivados, etc. (LAIN, 2016)

- Se enfoca en la recolección centralizada de toda la información. El sistema se va a encargar de transportar todos los registros que se encuentran en línea y que vienen de todas las fuentes del sistema de la empresa y transformarlos a un solo formato con el cual trabajar para procesar la información, de esta forma se logra un mejor entendimiento de los datos que se manejan mejorando la eficiencia y facilitando el siguiente punto que es su análisis. (LAIN, 2016)

- Analiza los datos para valorar su nivel de importancia, clasifica dicha información y coloca como primer punto a aquellos eventos marcados como críticos. Cuando ya se ha analizado la información, hay que tomar en cuenta que al tomar como muestra un solo evento no se logra observar el historial o el plano general del problema, por tanto, no da lugar a conclusiones puntuales que permitan dar soluciones inmediatas, es por

eso por lo que es imprescindible la correlación de los eventos, para encontrar posibles tendencias o problemas de seguridad frecuentes. (LAIN, 2016)

- Todo el análisis lo realiza en tiempo real mediante el monitoreo permanente de los recursos, infraestructura, etc., esto permite interpretar los eventos tan pronto como ingresan al sistema. Con ello, se dan las herramientas para gestionar la seguridad contra incidentes de forma inmediata logrando aumentar el porcentaje de probabilidad de una respuesta asertiva por parte del personal encargado de la seguridad informática en la empresa. (LAIN, 2016)

2.1.2 Funciones de un SIEM

Para que un sistema SIEM pueda cumplir con sus objetivos, su estructura debe ser fuerte, debe estar bien construida y sobre todo su mecanismo de funcionamiento tiene que estar bien analizado y bien instaurado en el sistema de la empresa, es así que un SIEM se apoya en varias funciones para alcanzar sus objetivos, estas funciones son las de recolección de información, análisis, monitoreo, alertas, reportes, etc., capacidades que permiten al sistema cumplir las políticas establecidas y gestionar las vulnerabilidades. En la figura 10 se pueden observar las funciones de un SIEM.

Figura 10. Funciones SIEM.

Tomado de (Camilleri, 2017)

- **Recolección y gestión de logs:** se encarga de recolectar los datos arrojados desde diferentes fuentes poniendo especial atención a los datos catalogados como de alto riesgo o muy importantes, de igual forma, se encarga de almacenar esa información en una base de datos que se encuentra centralizada y ahí es en donde se procede a realizar el análisis sintáctico de cada dato con el fin de normalizarlo pues al venir de diferentes destinos da paso a diferentes formatos de lenguaje. (Marquina, 2018)

  Todos los datos que se manejan en esta función son en tiempo real y esto ayuda al SIEM a conocer la salud del sistema, la seguridad de los sensores instaurados y el rendimiento de los equipos que forman parte de la infraestructura de red.

- **Cumplimiento de las regulaciones:** explica que todos los protocolos y actividades que se han ejecutado en el sistema pueden y deben ser puestos bajo análisis, deben ser puestos bajo conceptos de filtrado o reglas que brinden la oportunidad de auditar y validar las decisiones que se han tomado, teniendo como línea de visión el cumplimiento de las políticas de seguridad impuestas por la empresa en las resoluciones vigentes en la fecha expresa. (Marquina, 2018)

- **Registro forense:** brinda la posibilidad de analizar tanto los datos arrojados por los equipos como las alertas que se han emitido hasta el momento, esto con el fin de encontrar el origen de todas aquellas incidencias ocurridas en contra de la seguridad del sistema, hacerlas frente y reforzar la seguridad para que no vuelvan a ocurrir. (Marquina, 2018)

- **Correlación de eventos de seguridad:** se analizan diferentes sucesos para encontrar posibles relaciones entre ellos, en este punto se estudia su frecuencia, su rango horario, etc., para poder establecer posibles patrones, tendencias, eliminar falsos positivos, unir amenazas que puedan encontrarse relacionadas, etc., para ver una pantalla global y más

certera del problema que ayude a crear una estrategia para su tratamiento. (Marquina, 2018)

- **Retención de registro:** se encarga de mantener almacenados todos los datos históricos que se han generado para facilitar el buen desarrollo de las correlaciones de eventos realizadas en el pasado, sirve para tener una base de los datos analizados y hacer seguimiento del cumplimiento de las normas y protocolos que se tendrían de haber seguido dependiendo de cada caso. (Pedraza, 2019)

- **Alertas en tiempo real:** la tecnología de SIEM permite realizar acciones de monitoreo y de visualización en tiempo real, entonces, cuando encuentra una situación fuera de lo común este sistema presenta automáticamente una notificación o alerta que avisa inmediatamente al administrador de red o a la persona responsable de la seguridad informática de lo que está sucediendo.

- **Capacidad de respuesta:** cuando el sistema SIEM detecta alguna situación fuera de lo normal, lo cataloga como un incidente de seguridad y tras todo el proceso de correlación de eventos y demás etapas de análisis del riesgo, se avanza a la siguiente acción, la de reacción automática por parte del sistema frente a ataques, esto se lo lleva a cabo con la finalidad de disminuir riesgos y mitigar la amenaza de forma inmediata. (Pedraza, 2019)

- **Seguridad en los equipos clientes:** función desarrollada por y para los clientes, dado el caso vienen a ser los empleados de la empresa, SIEM brinda la oportunidad de monitorizar en tiempo real la situación en las que se encuentran los equipos finales que forman parte de la red, esto nos permite saber los procesos que se encuentran activos, los recursos utilizados, el estado del firewall, el estado del antivirus, etc.

- **Informes de seguridad:** capacidad de un SIEM para presentar informes con contenido técnico y ejecutivo sobre todos los eventos que se han reportado, las medidas que se han tomado y los resultados conseguidos siguiendo el lineamiento de los protocolos establecidos.

2.2 Consideraciones para elegir un SIEM

El mercado es amplio y existen muchas empresas que ofrecen distintas soluciones para las problemáticas de las empresas, por ello hay que tomar en cuenta cuales son los elementos por considerar para elegir uno de estos sistemas.

Se deben analizar la situación actual de la empresa en donde se va a implementar el SIEM, hay que realizar un análisis bastante completo pues hay que considerar todos los eventos a ser controlados, esto busca evitar que el sistema comprado o incluso ya instalado no tenga afinidad con el control que se necesite.

No se debe adquirir un SIEM sobrecargado, es decir, que posea todo tipo de funcionalidad posible. Se puede controlar la mayoría de las vulnerabilidades con un sistema genérico, no se necesita adquirir el de última generación cuando no se van a utilizar sus controles más avanzados pues están diseñados para redes de grandes empresas y el punto en cuestión son empresas PYMES, estas pueden ver comprometida su situación financiera en caso de hacer un desembolso excesivo, se debe manejar la relación calidad/precio.

En breves rasgos la elección de un SIEM debe basarse en los siguientes puntos:

- Necesidades y expectativas de la empresa.
- El costo del sistema.
- Un sistema con buscadores de registros flexible y ágil.

- La infraestructura vigente en la compañía.
- Un sistema con visualización y generación de informes en tiempo real.
- El tamaño de recursos necesarios, en cuento a rendimiento, almacenamiento, etc.
- Un sistema que maneje alertas e informes adecuados (técnicos, ejecutivos, etc.). (Merino, 2018)

2.2.1 Cuadrante mágico de Gartner

Es un aporte que realiza la empresa Gartner a la sociedad, el negocio de esta compañía gira entorno a la investigación en la industria de las TI, se dedica a realizar el análisis de las tendencias que sugiere el mercado y utilizando estos datos elabora un ranking en el que se encuentran las soluciones tecnológicas más importantes del momento. (Cabrera & Agüero, 2015)

La idea es dar una imagen real de la situación del mercado, buscando así facilitar la toma de decisiones en cuanto a la selección de soluciones y productos. Este estudio de mercado que realizan se basa en los resultados que ha tenido la implantación de su propia metodología de investigación y de la distribución de diferentes equipos humanos alrededor del mundo.

El cuadrante del cual se habla se lo utiliza para varios tipos de tecnologías, entre ellas se encuentran los SIEM y como se dijo con anterioridad, en Gartner usan su propia metodología de investigación y en caso de estos sistemas para realizar el análisis y elaborar el ranking se toman en cuenta los siguientes factores:

- Escala de implementación.
- Monitoreo en tiempo real.
- Análisis post/captura.
- Requisitos de presentación de informes de cumplimiento. (Cabrera & Agüero, 2015)

Estudiados esos detalles la empresa Gartner recomienda que se desarrollen requisitos enfocados en los controladores encargados de eventos críticos, que siempre se trate de anticipar una futura aplicación a mayor escala de las capacidades que use actualmente el SIEM y que el proyecto presente rasgos que ayuden a la adaptación del SIEM en un entorno cambiante provocado por: cambios de equipos, cambios en las necesidades de la empresa y en base a las posibles amenazas que se puedan presentar. En la figura 11 se puede observar la división que presenta el cuadrante mágico de Gartner.

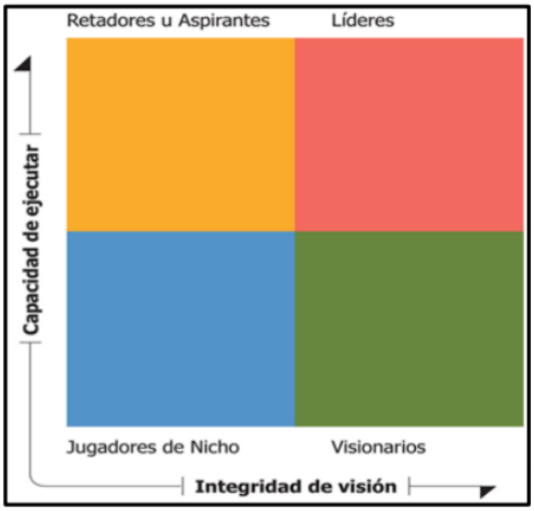

Figura 11. Cuadrante mágico de Gartner.

Tomado de (Cabrera & Agüero, 2015)

Como se puede ver en la figura 11 y como dice en su nombre, el cuadrante mágico de Gartner presenta cuatro divisiones, cada una de ellas es una sección diferente, estas son:

- **Líderes:** en esta sección se encuentran todos los productos que se pueden considerar como los mejores de sus ramas, que se encuentre en dicho sitio quiere decir que alcanzo una alta calificación en los dos ejes de los cuales se compone el cuadrante.

Esta ubicación nos dice que se puede esperar una solución eficiente, bien estructurada, madura y que es capaz de adaptarse según su entorno. También da referencias en cuando a la situación en la que se encuentra la marca que provee dicho producto, sugiere que la empresa se encuentra en su plenitud, que posee recursos suficientes para enfrentar posibles problemas y que ha logrado con éxito implantar su solución en diferentes escenarios alrededor del mundo. (Gartner, 2020)

- **Visionarios:** se encuentran todos los productores que han alcanzado una muy buena puntuación en uno de los dos ejes del cuadrante, para ser específicos en el eje de “Integridad de visión”, sin embargo, no han obtenido una puntuación satisfactoria en el segundo eje “Capacidad de ejecutar”. Esto quiere decir que se encuentran todas aquellas empresas con una visión bien estructurada de las situaciones que atraviesa el mercado, pero no cuentan con la capacidad de materializar su visión. (Gartner, 2020)

- **Retadores o aspirante:** se trata de empresas que se encuentran muy bien posicionadas dentro del mercado, han logrado implementar su idea y ya se encuentran ofreciendo altas tasas de éxito cuando instalan su solución. Sin embargo, no presentan variedad en cuento a soluciones o sus productos únicamente se enfocan en resolver un determinado aspecto que se demande dentro del mercado, en este problema también pueden entrar situaciones como déficit en sus ventas o una mala posición geográfica del negocio. (Gartner, 2020)

- **Jugadores de Nicho:** en teoría es el cuadrante menos favorable, en esta sección se encuentran las soluciones con peores calificaciones. Aquí se encuentran los productos que no han sido capaces de lograr una nota aceptable en alguna categoría. Sin embargo, se encuentran y aun se sostienen en el mercado, por tanto, las soluciones que ofrecen presentan algún tipo de ventaja o calidad en algunas situaciones. (Gartner, 2020)

Entonces, el cuadrante mágico de Gartner viene a ser un gráfico que se encuentra trazado basándose en los resultados obtenidos del rendimiento que han presentado los productos de TI en el mercado y en un momento determinado. Este gráfico sirve como fuente de información, como una referencia que se debe analizar para prever comportamientos y posibles eventualidades que puedan tener los proveedores de los productos en un mercado que siempre se encuentra cambiante.

2.2.2 Cuadrante mágico de Gartner de Sistemas SIEM

Desde el enfoque de Gartner el mercado de los sistemas SIEM se mueve por la necesidad que tienen las empresas en analizar los datos que son arrojados por sus sistemas de seguridad en tiempo real, con eso buscan conseguir la detección temprana de las infracciones y ataques que amenacen la red corporativa para poder tomar medidas que impidan esta clase de eventos.

Las funciones que Gartner analizó y tomo en consideración para el desarrollo del cuadrante mágico de esta tecnología fueron las capacidades que tienen los productos de los proveedores para resolver los siguientes puntos:

- Recopilar.
- Almacenar.
- Investigar.
- Respaldar la mitigación.
- Reportar todos los datos relaciones a la seguridad.
- Respuesta a los incidentes.
- Cumplimiento de las normas.
- Análisis forense. (Gartner, 2020)

En la figura 12 se puede observar los proveedores que han sido evaluados y forman parte del cuadrante mágico de Gartner de los sistemas SIEM. Estos proveedores presentan productos que ejecutan las funciones habladas con

anterioridad y ya se dedican a comercializar y vender de forma activa sus sistemas en el área de compras de seguridad de la información.

Figura 12. Cuadrante mágico de Gartner de sistemas SIEM. Febrero 2020. Tomado de (Kavanagh, Bussa & Sadowski, 2020)

Traduciendo rápidamente, lo que la figura 12 quiere decir es lo siguiente:

- **Líderes:** Splunk, IBM, Exabeam, Securonix, Rapid7, LogRhythm, Dell Technologies (RSA).
- **Visionarios:** LogPoint.
- **Retadores:** ninguno.
- **Jugadores de nicho:** FireEye, AT&T Cybersecurity, McAfee, Fortinet, Micro Focus, Han Sight, ManageEngine, SolarWinds.

Las PYMES pueden tomar en consideración dichos productos ya que han demostrado su valía en el mercado y sus soluciones ya tienen un nivel de

aceptación por parte compañías que han implementado estas tecnologías, esta información nos sirve como fuente de información, un punto de partida para conocer cuáles son las soluciones que más se ajustan a las necesidades de PYMES.

2.3 Sistemas SIEM

Una vez se ha explicado sobre la cantidad de problemas que enfrentan las redes de empresas, la importancia de contar con niveles óptimos en la seguridad informática y en base a la investigación y a la experiencia de otras empresas en este tema, se ha llegado a la conclusión de que se necesita contar con un sistema de gestión de eventos de seguridad informática que brinde las herramientas adecuadas a los administradores de red para luchar contra estos problemas.

Hablando ya de las herramientas SIEM, se pueden encontrar una gran cantidad de sistemas que presentan diferentes tipos de características, diferentes niveles de capacidad para la recopilación, diferentes niveles de abstracción en la correlación, etc., detalles que se encuentran relacionados directamente con los costos de sus licencias y el entorno para el cual fueron desarrollados, entonces, es importante analizar las diferencias que existen entre las soluciones con el fin de encontrar la más adecuada a nivel económico, de solución ofrecida y de rendimiento demostrado para las redes de empresas pequeñas y medianas.

2.3.1 Sistemas SIEM de paga

A continuación, se presenta una lista de productos SIEM de paga, dicha lista la conforma un grupo de soluciones a las cuales se les puede considerar como las más vendidas y utilizadas en el mercado, de igual forma, todas ellas presentan características avanzadas de un SIEM y está claro el éxito de cada una en

implementaciones ya realizadas pues los comentarios de sus clientes son positivos y se recomienda su uso en entorno ya empresarial, estos productos son:

- Splunk ES
- QRadar
- McAfee ESM
- RSA

2.3.1.1 Características de los SIEMS de paga

En este punto se presenta el análisis de todos los SIEMS expuestos en el punto 2.3.1, se procede a dar información acerca del proveedor encargado de su distribución, otros tipos de productos SIEM ofrecidos por la misma marca, las licencias de sus productos en conjunto con las métricas establecidas para calcular su precio, los componentes de estas herramientas, los inconvenientes encontrados y las fortalezas de la solución puesta bajo análisis.

- **Splunk:** es un proveedor de SIEM cuya sede se encuentra en San Francisco, California. Presenta dos productos principales los cuales son el Splunk Enterprise y el Splunk Cloud, añadidos a estos existen otros tres tipos de soluciones que vienen a ser el Splunk Enterprise Security (ES), el Splunk UBA y el Splunk Phantom, todos estos elementos son independientes y por tanto se venden por separado. (Kavanagh, Bussa & Sadowski, 2020)

  Hablando del Splunk Cloud y del Splunk Enterprise, estas soluciones encuentran su fuerte en el enfoque que realizan al momento de recopilar datos, eventos, visualizaciones y búsquedas. Toda esta información es utilizada para las posteriores operaciones que realizan las Tecnologías de la Información y por los procesos que corresponden a cada caso de seguridad. (Kavanagh, Bussa & Sadowski, 2020)

En cuanto a ES, encuentra su fuerte en sus capacidades para realizar el monitoreo de los eventos de red, consultas en tiempo real, administración de casos, paneles y respuestas por incidentes encontrados. Hablando de UBA además de dominar las anteriores características agrega un análisis mucho más avanzado que es efectuado sin ser supervisado por el administrador de red y que se basa en ML. Phantom, tiene rasgos de trabajo de forma autónoma, es decir, evalúa el riesgo, lo clasifica y brinda soluciones de forma automática para reducir las amenazas de seguridad informática y también brinda servicios SOAR. (Kavanagh, Bussa & Sadowski, 2020)

El costo de las licencias de estos productos también difiere entre ellos. En primer lugar, se encuentra Splunk Cloud y Enterprise cuyos precios se basan en el número de datos que sean ingresados en su plataforma. En cuanto a ES, esta solución cuenta con licencia según su consumo. Por otro lado, el costo de UBA se basa en el número de cuentas del cual vaya a disponer la empresa en donde se va a instaurar el sistema. (Splunk, 2020)

Finalmente, Splunk Phantom presenta dos tipos de licenciamiento, el primero se basa en la cantidad de eventos en los cuales los usuarios se han visto obligados a tomar medidas de protección y la otra basa su precio por la cantidad de usuario que tienen la herramienta. (Splunk, 2020) En la tabla 1 se puede observar el cuadro comparativo de las fortalezas e inconvenientes de la herramienta Splunk ES.

Tabla 1.
Cuadro comparativo de la herramienta Splunk ES.

Fortalezas	Inconvenientes
La estrategia que sigue este sistema proporciona la recopilación y análisis de datos de forma centralizada lo cual atrae a todas aquellas empresas que buscan una solución que sea capaz de trabajar con múltiples equipos. Esta característica brinda la oportunidad a los compradores de una eventual expansión tomando en cuenta una fricción limitada.	Los precios que se manejan al momento de negociar contratos, evaluar un proyecto y contratar servicios con su soporte se encuentran muy por encima de otras soluciones. Las empresas alegan el alto coste que maneja Splunk sobre sus licencias, precios y costos.
Ha logrado comprimir el mercado, para ello ha construido un ambiente denso de socios y de alianzas tecnológicas que le han permitido crear aplicaciones diseñadas específicamente para un caso de uso específico de Splunk, consiguiendo de esa forma mejorar su nombre, aumentar sus prestaciones y elevar su valor de marcado.	Splunk presenta falencias por la falta de sensores de red y de punto final, este inconveniente obliga a los compradores de este sistema a encontrar una solución complementaria. Los obliga a buscar en el mercado productos de terceros que les permitan cumplir con los requisitos que tiene un centro de operaciones de seguridad (SOC) que en la actualidad se encuentra estructurada de la siguiente forma: (SIEM + UEBA + SOAR + EDR + NTA).
La imagen que tiene Splunk con sus clientes es positiva, los usuarios de ese sistema aprecian el producto y lo puntúan con altas calificaciones. Estas notas se deben a razón de la facilidad con la cual esta tecnología se integra, la calidad de sus soluciones, la disponibilidad del producto y a que adicional a eso realiza el trabajo de capacitación del usuario que va a hacer uso del sistema.	Como se sabe Splunk es un proveedor, de este salen varias soluciones catalogados como diferentes modelos. Uno de estos modelos es el Splunk UBA y el inconveniente con esta solución es que se la puede tratar como un elemento de tecnología que se encuentra separada del resto, es decir, no se encuentra integrada en el núcleo de Splunk y hasta la fecha es un modelo que trabaja de forma local lo cual puede causar posibles problemas a los compradores del modelo de Splunk Cloud.
La forma de trabajar de la sección de marketing de Splunk y las oportunidades de venta que presenta con otras empresas han causado que se vuelva muy visible en el mercado de SIEMS, el nombre de esta solución se toma en consideración de empresas grandes, globales y hasta multinacionales.	

- **IBM:** su sede se encuentra ubicada en Cambridge, Massachusetts y su catálogo de productos consta de una gran cantidad de servicios de seguridad y de diferentes tecnologías.

  Dentro de los servicios que ofrece en cuanto a seguridad informática se puede encontrar a QRadar, un producto SIEM cuya estructura se compone de una mezcla de elementos que tienen diferentes precios, estos son:

  a. IBM QRadar Vulnerability Manager, este componente se encarga de integrar todos los datos que serán utilizados para realizar la evaluación de las vulnerabilidades del sistema.

  b. IBM QRadar Network Insights, se encarga de realizar la inspección del contenido de cada paquete, además logra la visibilidad de la aplicación de los indicadores y señales.

  c. QRadar Risk Manager, se enfoca en la capacidad del sistema para realizar simulaciones de escenarios que amenacen la salud de la red empresarial y se encarga de monitorear las configuraciones implementadas en los dispositivos de red.

  d. IBM QRadar User Behavior Analytics (UBA), este es un módulo complementario totalmente gratuito que se encarga de dar casos de uso a las amenazas internas que se han encontrado en el sistema.

  e. IBM QRadar Incident Forensics, brinda soporte en el área de investigación forense del sistema.

  f. IBM QRadar Advisor con Watson, mediante una serie de análisis avanzados viene a identificar la fuente de la amenaza, es el motor de atribución con el cual trabaja QRadar.

g. IBM Resilient, ofrece una solución de tipo SOAR, es capaz de soportar la mutua integración entre la respuesta dada por QRadar SIEM y Resilient, ayudando de esta forma a optimizar todos los flujos de trabajo que formen parte en los procesos de la empresa. (Kavanagh, Bussa & Sadowski, 2020)

En cuanto a la forma de adquirir esta solución, QRadar presenta una característica única, esta plataforma se la puede comprar por dos modalidades, adquiriendo las licencias o mediante una suscripción perpetua. Para el tema de las licencias, los costos se encuentran sujetos a dos ideas, la primera toma en cuenta la cantidad de eventos por segundo (EPS) que se manejan en las fuentes de datos ubicados en el alcance y la segunda toma como referencia los flujos por minuto (FPM). (IBM, 2020)

Hablando de los precios que manejan los componentes adicionales que se complementan con IBM QRadar, cada uno maneja sus propias métricas, por ejemplo:

a. QRadar Network Insights, basa su costo en el número de flujos que se da a IBM.

b. QRadar Vulnerability Manager, basa su costo en el número de activos en se presentan en el alcance de IBM.

c. QRadar Risk Manager, basa su costo en el número que se tiene de los sistemas de los cuales se extrae la información. (IBM, 2020)

En la tabla 2 se puede observar el cuadro comparativo de las fortalezas e inconvenientes de la herramienta QRadar.

Tabla 2.
Cuadro comparativo de la herramienta QRadar.

Fortalezas	Inconvenientes
El plan que sigue IBM hasta la fecha le permite contar con una buena cantidad de recurso internos y un buen número de asociaciones que respaldan a la marca y lo ayudan en aspectos importantes como al momento de cerrar ventas, a la hora de implementar sus soluciones y en la parte de apoyo en cuanto al soporte de sus productos incluyendo en este aspecto a los servicios que se venden por separado.	QRadar presenta problemas al momento de definir su modelo de venta y de precios. La propuesta con la cual trabajan resulta confusa, tienen licencias perpetuas y otras que basan sus costos en situaciones como la velocidad de los datos, el número total de activos y si su implementación se la realiza de forma local o en la nube. A eso hay que añadir sus diferentes esquemas de precios con los componentes que se ofrecen adicionalmente para la plataforma de QRadar.
Esta solución ofrece a sus clientes flexibilidad en cuento a su arquitectura, brinda varias opciones al momento de implementarlo junto con una gran cantidad de posibles combinaciones que se ajustan a todo tipo de entorno. En esta parte se incluyen dispositivos virtuales y físicos que pueden formar parte en sistemas distribuidos y centralizados, así como también pueden ser adquiridos por medio de una licencia exclusiva para su implementación dentro de la nube.	Presenta dificultades al momento de recopilar datos forenses que provienen de usuarios finales, este producto se ve limitado, presenta falta de capacidad para la detección de un punto final y respuesta (EDR). Muchos de los clientes que manejan esta solución se han visto en la necesidad de contratar productos de terceros debido a este problema.
Sumándole a QRadar el componente Watson, la herramienta brinda un fuerte apoyo en todos los planos que se refieren a la investigación de incidentes ocurridos, esto lo hace mediante el análisis de diferentes contextos que provienen de fuentes externas e internas. También utiliza dicho análisis para sugerir los pasos a seguir en caso de ataques, siempre basándose en posibles acciones que puede tomar el	IBM está demostrando que sufre de una gran dependencia de sus productos ofrecidos de forma complementaria y dichos productos aparte de tener un costo adicional vienen a tratar de rellenar huecos en el funcionamiento de QRadar. Estos son los casos de Advisor y Resilient, componentes utilizados para mejor las capacidades de investigación, priorización y otras acciones que

atacante y a su vez priorizando la función de alertas por posibles inconvenientes.	buscan dar una mejor respuesta a los incidentes ocurridos.
Cuenta con una API abierta la cual permite a usuarios, socios, clientes participar de forma activa en el desarrollo de futuras integraciones a la plataforma. Este punto ayuda a QRadar a mantenerse firme dentro del mercado de aplicaciones pues siempre se encuentra realizando una nueva integración que ha sido desarrollada por IBM en colaboración con terceros.	QRadar presenta problemas de desfase en cuando al nivel de madurez de cada elemento de su plataforma y adicional presenta problemas de integración cuando se la relaciona con otros componentes.
Al momento de comprar la licencia básica de QRadar se incluye de forma gratuita el componente User Behavior Analytics (UBA).	Según la opinión de varios clientes de este producto: los análisis elaborados por QRadar, su forma de actuar y los procesos que corresponden a la contratación y venta de sus soluciones, son áreas por tomar en consideración para aplicar mejoras.

- **McAfee:** la sede de este proveedor se encuentra ubicada en Santa Clara, California y cuenta con una serie de oficinas distribuidas por todo el mundo.

  McAfee es un proveedor de diferentes tipos de tecnología y es McAfee ESM el cual responde en el campo de los sistemas SIEM. Esta herramienta trabaja de forma parecida a IBM, cuenta con componentes dedicados a mejorar el rendimiento de sus servicios prestados, estos componentes son:

  a. McAfee Direct Attached Storage (DAS), ofrece a los clientes un adicional almacenamiento de registro.

  b. McAfee Global Threat Intelligence (GTI), añade indicadores cuya finalidad es determinar las amenazas y proteger la reputación contextual (archivos, sitios web, certificados, conexiones de red).

c. McAfee Application Data Monitor (ADM), viene a reforzar el monitoreo en la capa de aplicaciones para detectar posibles amenazas ocultas.

d. McAfee MVISION Cloud, su objetivo es ofrecer seguridad a los datos al momento de acceder a la nube. (Kavanagh, Bussa & Sadowski, 2020)

Hablando de precios, se vende en el mercado para dispositivos virtuales o físicos por medio de una licencia perpetua. Su costo depende de la velocidad de eventos por segundo y los clientes tienen la oportunidad de aumentar el volumen que presentan estos eventos hasta llegar al límite de las capacidades de sus dispositivos. Por otro lado, el componente McAfee Global Threat Intelligence se vende por suscripción anual y su costo depende del modelo de hardware o en su defecto depende del recuento de núcleos de la herramienta ESM adquirida por el cliente. (McAfee, 2020)

En la tabla 3 se puede observar el cuadro comparativo de las fortalezas e inconvenientes de la herramienta ESM.

Tabla 3.
Cuadro comparativo de la herramienta ESM.

Fortalezas	Inconvenientes
Ofrece una fácil integración con otros productos dedicados a operaciones de seguridad que pertenecen al catálogo de McAfee, esto brinda la oportunidad de complementar las soluciones de su SIEM, McAfee ESM.	ESM se encuentra rezagado en comparación a sus competidores cuando busca dar respuesta a movimientos sospechosos dentro de dispositivos que se encuentran fuera del catálogo de su proveedor (McAfee).

Cuenta con un entorno fuerte y bien estructurado, formado por una serie de alianzas tecnológicas compuestas por socios activos y personas dedicadas a contribuir con contenido a la plataforma.	Al compararlo con sus competidores McAfee se queda atrás al momento de valorar el nivel de amenaza mediante el análisis de eventos sospechosos, su mapeo de eventos se ve superado ampliamente.
McAfee ESM encuentra su principal fortaleza cuando se habla de la gestión de datos y de las funciones de adquisición. El planeamiento y ejecución de dichos eventos resulta ser bastante sólido.	En comparación a otras soluciones presenta una menor capacidad al momento de automatizar eventos de seguridad.
Se encuentra muy bien posicionado en las regiones de Europa, Oriente Medio y África (EMEA). En esos sectores es especialmente fuerte pues cuenta con una gran variedad de servicios disponibles para todas aquellas empresas que necesiten gestionar servicios, realizar consultorías e implementar soluciones SIEM.	

- **DELL:** la sede de este proveedor se encuentra ubicada en Round Rock, Texas e igual a McAfee cuenta con una serie de oficinas distribuidas por todo el mundo.

  Dell es un proveedor de servicios y tecnología con un catálogo bastante amplio de productos, dentro de este catálogo se encuentra RSA NetWitness, un producto enfocado a realizar operaciones de SIEM en donde se encuentra la detección de intrusos, análisis forenses, reportes, correlación de eventos, monitoreo en tiempo real, telemetría y muchas otras funciones sujetas a la estructura de esta tecnología.

  En cuanto al plan para la venta de licencias de este servicio, se basa en la naturaleza de la herramienta de la cual se esté hablado, en algunos

casos se toma en consideración el volumen de datos que recibe y en otros casos (licencias de forma perpetua o basadas en algún termino) el costo viene a ser el valor predeterminado por ser clientes nuevos. (Dell, 2020)

Para los precios de los componentes adicionales, estos tienen su propia métrica, por ejemplo:

a. RSA NetWitness Endpoint, su costo es calculado en base al número de puntos finales.

b. RSA NetWitness UEBA su costo es calculado utilizando el número de usuarios que se encuentran siendo monitoreados.

c. Red RSA NetWitness, su costo es calculado por el volumen de datos recibidos.

d. RSA NetWitness Orchestrator, su costo es calculado por el número de analistas de seguridad. (Dell, 2020)

En la tabla 4 se puede observar el cuadro comparativo de las fortalezas e inconvenientes de la herramienta RSA.

Tabla 4.
Cuadro comparativo de la herramienta RSA.

Fortalezas	**Inconvenientes**
La arquitectura de este sistema permite la implementación de soluciones capaces de ajustarse a todo tipo de entorno debido a la posibilidad que brinda para combinar y mezclar dispositivos de software y dispositivos virtuales. Adicional presenta capacidades para una eventual escalabilidad horizontal.	El proveedor de esta herramienta no coloca a RSA como una oferta de software como servicio (Saas) y en caso de que alguna empresa desee y logre conseguir un SIEM SaaS entregado directamente por este proveedor, las características de dicho producto pueden enfrentar posibles limitaciones.

Su estructura es lo suficientemente madura como para basarse en su visión y análisis realizados en redes y puntos finales cuando se busca realizar acciones de defensa contra amenazas de un nivel avanzado.	RSA NetWitness encuentra problemas al momento de dirigir sus soluciones al mercado de empresas medianas, en dicho mercado se ve superado por sus competidores al ser una plataforma demasiado compleja de implementar y de utilizar. Con esa característica, organizaciones sin una estructura madura tendrán serios problemas al momento de operar la herramienta.
Presenta características solidas en cuanto a las funciones de análisis forenses y a la localización de amenazas.	
A diferencia de Splunk esta herramienta resulta ser adecuada cuando se busca implementar un centro de operación de seguridad (SOC).	

2.3.2 Sistemas SIEM gratuitos

A continuación se presenta una lista de productos SIEM gratuitos, esta lista está estructurada por un grupo de soluciones a las cuales se les puede considerar como las herramientas Open Source más utilizadas en el mercado, presentan las características básicas de un SIEM y está clara la efectividad de sus soluciones pues los comentarios de otros análisis, investigaciones e implementaciones son positivos en cuanto a sus formas de conseguir alcanzar los objetivos básicos para mantener la seguridad de la información, estos productos son:

- OSSIM
- Hyperic HQ
- Elastic Stack

2.3.2.1 Características de los SIEM gratuitos

En este punto se presenta el análisis de todos los SIEMS expuestos en el punto 2.3.2, se procede a dar información acerca del proveedor encargado de su distribución, otros tipos de productos SIEM ofrecidos por la misma marca, los componentes de estas herramientas, los inconvenientes encontrados y las fortalezas de la solución puesta bajo análisis.

- **AT&T:** es una multinacional, un conglomerado de empresas la cual tiene dentro de su cartera de negocios la sección de AT&T Cybersecuriry, su sede se encuentra ubicada en Dallas, Texas.

  AT&T Cybersecuriry se encarga de ofrecer diferentes tipos de soluciones SIEM, siendo su producto insignia Unified Security Management (USM) Anywhere, producto que a diferencia de RSA es entregado por el proveedor como una solución SaaS. A ese producto se le suma el Sistema de gestión de la información de seguridad Open Source (OSSIM) que a diferencia de USM es una plataforma de código abierto.

  OSSIM aparte de ser gratuito, también se dedica a gestionar la seguridad de la información transportada en una red, para ello esta plataforma integra una gran cantidad de productos enfocados a brindar seguridad informática los cuales a su vez son capaces de correlacionarse para lograr mejores resultados.

  A diferencia de los otros productos analizados anteriormente como RSA, McAfee, etc., al enfocarnos en la plataforma de AT&T Cybersecuriry-OSSIM no se puede hablar sobre los tipos de licencia y las métricas para calcular costos, al ser una herramienta Open Source su descarga, posteriores configuraciones y utilización es gratuita, eso sí, comparándolo con USM se debe tomar en cuenta las capacidades limitadas de OSSIM. En la tabla 5 se puede observar el cuadro comparativo de las fortalezas e inconvenientes de la herramienta OSSIM.

Tabla 5.
Cuadro comparativo de la herramienta OSSIM.

Fortalezas	Inconvenientes
Su plataforma integra varias herramientas enfocadas a la seguridad informática, todas ellas Open Source.	Cumple funciones básicas, se enfoca en almacenar eventos, generar reportes y alarmas. No toma ningún tipo de acción para mitigar o reducir ataques.
La correlación de eventos realizada por OSSIM ayuda a disminuir el porcentaje de falsos negativos y falsos positivos.	Presenta problemas al momento de leer los registros entregados por los equipos propietarios.
Tiene la opción de realizar análisis forenses mediante el uso de los eventos almacenados en el sistema.	En comparación con USM (versión pagada de AT&T Cybersecuriry), OSSIM tiene capacidades limitadas.
Cuenta con una amplia comunidad abierta en distribuida por todo el mundo y en constante auge, esto ayuda a realizar cuestiones de soporte.	Esta plataforma fue desarrollada enfocada en el mercado de empresas pequeñas y medianas por tanto no es de mucha utilidad para grandes organizaciones.
Es un sistema centralizado, recopila toda la información y agrupa todos los eventos que transitan la red para mostrarlos en una pantalla facilitando la detección de intrusos.	
Su licencia no tiene ningún tipo de costo.	

- **Elastic:** es una empresa Norteamérica con sede en Mountain View, California. Esta organización se adentró en el mercado de los sistemas SIEM a pesar de no tener un producto con las características o funcionalidades necesarias para acometer el control sobre eventos y mantener la seguridad de la información en la red de una empresa. Sin embargo, se encuentra de forma merecida en el mercado gracias a la combinación de tres componentes que se complementan y crean un SIEM de altas prestaciones, estos componentes son:
    a. Elasticsearch.
    b. Logstash.
    c. Kibana. (Marquina, 2018)

  La fusión de esos elementos da origen a Elastic Stack, un producto cuyo funcionamiento se basa en el trabajo mutuo del conjunto de los paquetes de la unión realizada. Estos paquetes le dan a la nueva plataforma el motor de búsqueda, agentes utilizados para endpoints, colectores de datos, todas ellas forman parte del paquete de herramientas de seguridad informática que van a desempeñar diferentes funciones de un SIEM, como: reportes, alertas, monitoreo, recolección de datos, recopilación de información, etc. (Marquina, 2018)

  Elastic Stack utiliza diferentes herramientas Open Source por ello es una solución sin ningún costo, sin embargo, se le puede añadir distintos plugin de paga. En la tabla 6 se puede observar el cuadro comparativo de las fortalezas e inconvenientes de la herramienta Elastic Stack.

Tabla 6.
Cuadro comparativo de la herramienta Elastic Stack.

Fortalezas	Inconvenientes
Las herramientas que forman la estructura del SIEM son Open Source.	Necesita de la fusión de tres componentes para llegar a ser un SIEM.

La plataforma tiene como característica ser modular, da la oportunidad de únicamente instalar las herramientas necesarias según el caso.	Algunos complementos necesarios para mejorar el rendimiento de esta plataforma no son Open Source.
Uno de sus componentes base es Elastic Search, brinda al SIEM un potente motor de búsqueda.	No se presenta ningún tipo de automatización por parte del proveedor, se debe construir desde cero por el personal de la empresa donde va a ser instalado.
En la entrega habitual del cuadrante mágico de los sistemas SIEM organizada por Gartner se nombra a Elastic Stack como una alternativa SIEM destacada por mostrarse como una alternativa frente a la complejidad y el costo de adquirir y ejecutar otros tipos de productos SIEM.	Hay mucha dificultad cuando se necesita realizar soporte, esto se evita si se logra adquirir el producto bajo algún tipo de licencia entregada por otra organización como puede ser logz.io.
Tiene agentes que pueden ser instalados en servidores o desktops.	

- **Hyperic:** esta es una empresa de origen norteamericano con sede en San Francisco, California que entró en el mercado de los sistemas SIEM al posicionar su producto Hyperic HQ.

  Su solución utiliza como punto fuerte un robusto monitoreo aplicado sobre diferentes tipos de servicios, aplicaciones, softwares y sistemas. Se encarga de verificar la disponibilidad de los servicios ofrecidos a los clientes, el rendimiento que presentan y de forma automática descubre amenazas y maneja los recursos en red sin poner mayor atención a su lugar de ubicación. (Hyperic, 2020)

Tiene la opción de personalizar alertas lo cual da lugar a crear una tonalidad o una estructura distinta de mensaje dependiendo de cada caso, con esto facilita la localización del problema debido a la posibilidad de sectorizar las alertas. A esta característica se le suma la ventaja de distinguir entre los diferentes niveles de gravedad antes de proceder a emitirlas, es decir, no emite una alerta por motivos banales, para emitir una alerta se basa en el grado en el cual podría afectar al rendimiento del sistema reduciendo de esta forma el porcentaje de falsos negativos. (Caballero, s.f.)

Esta solución se encuentra cómoda al trabajar en conjunto con varias plataformas, estas son:

a. Unix.
b. Linux.
c. Windows.
d. Solaris.
e. AIX, HPUX.
f. VMware.
g. Amazon Web Services. (Hyperic, 2020)

En la tabla 7 se puede observar el cuadro comparativo de las fortalezas e inconvenientes de la herramienta Hyperic HQ.

Tabla 7.
Cuadro comparativo de la herramienta Hyperic HQ.

Fortalezas	Inconvenientes
Los nuevos clientes o máquinas virtuales son detectados de forma automática y al instante, en un lapso menor a 60 segundos permite comenzar con la monitorización de nuevo equipo.	Se encuentran varios problemas al nivel de la documentación oficial presentada por los proveedores, no logra diferenciar de forma correcta entre las características de sus productos comerciales y Open Source.

Maneja multiplataforma en cuanto a bases de datos, soporta a Oracle, MySQL y por supuesto a PostgreSQL, esta última herramienta Hyperic HQ la instalada por defecto.	El enfoque de trabajo de su área de marketing intenta dar una visión excesivamente consumidora a los clientes.
Permite al cliente controlar de forma completa la plataforma desde la interfaz web.	No brinda soporte profesional, su modelo se basa en soporte comunitario.
Su implementación resulta rápida y sencilla. La configuración de esta herramienta tiene un nivel medio/bajo, ideal para ser manejado por personal no especializado en el área de TI.	
El formato de reportes y análisis se encuentra muy bien estructurado, presenta graficas de relevancia, líneas de tendencia y planeación tomando en cuenta las capacidades del sistema.	

2.3.3 Comparación de los sistemas

Una vez hablado sobre los factores que se deben considerar para comparar SIEMS. De forma general, todos los productos analizados en los puntos 2.3.1.1 y 2.3.2.2 son candidatos muy serios para pensar en una implementación y utilizarlos en entornos ya empresariales.

Cada uno de esos sistemas son capaces de gestionar eventos, recolectar información, cumplir políticas de seguridad, controles, etc., en este punto entra a acotación algunas diferencias, no todos presentan las mismas características pues algunos sistemas como ESM, OSSIM y Splunk no tienen agentes encargados de integrar utilizando una forma nativa a los endpoints, también

existe el caso de Elastic Stack, el único sistema del cual se habló y no posee un listado inteligente de amenazas.

En cuanto al motor de búsqueda todos los productos se encuentran sobre los estándares, aunque en este punto Elastic Stack a pesar de tener que implementarlo aparte sobresale con Elastic Search y Splunk de igual forma se encuentra por encima de sus competidores al presentar un motor más potente.

De los otros sistemas como OSSIM e Hyperic HQ tienen la ventaja de ser herramientas gratuitas, esto les abre el mercado de las empresas PYMES a pesar de contar con funcionalidades limitadas. En el caso de Hyperic HQ no cuenta con la función de exploración de redes o también se puede mencionar la falta de un NIDS dentro de su plataforma. En el caso de OSSIM, el problema es su enfoque, se concentra en las funciones básicas como: generar reportes, alarmas, etc., y a diferencia de sistemas como Splunk, ESM, RSA y QRadar no es capaz de tomar acciones contra los ataques detectados en red.

2.4 Análisis de SIEMS enfocado a empresas.

Un punto importante para elegir un SIEM y a la vez una clara diferencia entre las soluciones analizadas es el factor económico, como no puede ser de otra manera, la mayoría de las empresas PYMES no tienen un núcleo empresarial maduro y no cuentan con la estabilidad económica suficiente para basar sus decisiones en ventajas a futuro o en la implementación de mejores mecanismos de seguridad, por ello solo analizan el costo del producto y no se fijan en las características de estos sistemas.

Eso se debe principalmente a la incapacidad de los altos cargos de estas empresas al no poder visualizar las ventajas de un modelo con una alta eficiencia, se centran en la parte económica viendo y centrándose en un posible

retorno directo del monto invertido traído por la herramienta para amortizar el valor desembolsado, en este análisis lo único a encontrar es un valor negativo pues un SIEM no viene a generar ganancias de forma directa, no va a generar recursos por sí solo, un SIEM actúa y devuelve la inversión realizada al momento de proteger la red de ataques, en ese punto evita fuertes pérdidas económicas.

Otro punto para considerar es realizar un análisis previo del estado actual de la organización donde se vaya a realizar la implementación, se aconseja a todas las PYMES llevar a cabo una evaluación individual de las necesidades de su organización, en este punto se debe excluir todo lo leído referente a recomendaciones de SIEMS de fabricantes, proveedores, ventajas y desventajas leídas en este trabajo o en cualquier otro artículo leído en otro sitio.

Ese análisis se enfoca en reconocer las funciones de cada SIEM y abstraerlo a un plano en el cual se pueda imaginar su forma de actuar en el entorno de la organización en cuestión. Con eso queda claro, no existe información precisa sobre el rendimiento de un SIEM, cada una de estas soluciones se va a encontrar con diferentes entornos, toda empresa presenta diferentes fuentes de información, necesita diferentes combinaciones dependiendo de la complejidad de su infraestructura, necesita diferentes tipos de informes de cumplimiento, etc.

En conclusión, un SIEM puede ser el mejor y puede ser perfecto para algunos tipos de organizaciones, pero ese mismo SIEM puede no ser la mejor solución y no ser capaz de responder a las expectativas de otros tipos de organizaciones.

2.4.1 Análisis de SIEMS para empresas grandes

En este punto se presenta un breve análisis de la forma en la cual se adaptarían los SIEMS analizados en los puntos 2.3.1.1 y 2.3.2.2 en el entorno de empresas grandes.

- **Splunk:** una vez se han analizado las características de las soluciones de Splunk, se puede decir que estos productos resultan ser convenientes para aquellas empresas que se encuentran buscando una solución de SIEM que le permita crecer desde un uso de nivel básico a usos más avanzado que le den la posibilidad de tener un mejor manejo de la seguridad por medio de la implementación de nuevos controles. Es muy visible en el mercado ya que su proveedor se encuentra muy bien posicionado en todo el mundo y es una solución tomada en consideración de empresas grandes, globales y hasta multinacionales.

- **IBM:** analizadas las características de QRadar, se puede decir que este producto ofrece un sistema destacado por ser robusto, por permitir construir funciones dedicadas a la detección de intrusos y por brindar la oportunidad de dar respuestas a las amenazas, por tanto, este sistema tiende a llamar la atención de grandes empresas.

- **McAfee:** esta solución encaja dentro de entornos empresariales dispuestos a realizar una inversión bastante fuerte en la tecnología presente dentro del catálogo de la marca McAfee, se recomienda la incursión en este mercado de núcleos empresariales maduros y complejos.

- **Dell:** este producto encaja en el mercado donde se encuentran empresas grandes, con un núcleo empresarial maduro y bien definido, encaja en las necesidades de todas aquellas empresas que buscan una plataforma SIEM con todos los servicios y funciones (endpoint nativo, SOAR, análisis forenses, reportes, monitoreo, rastreo).

- **AT&T:** en cuanto al mercado donde se encuentran las multinacionales y grandes organizaciones tanto OSSIM como USM tienen muy poco para ofrecer. En comparación a otras soluciones estas plataformas presentan menos funciones, una cantidad menor de controles, realiza un análisis y

monitorización menos estricta, en definitiva, no resuelve de forma óptima las necesidades de entornos complejos.

- **Elastic:** como su forma básica no es un SIEM esta es una plataforma no visualizada en el entorno de las grandes empresas, su implementación en organizaciones de tal magnitud no solo no es recomendada, se encuentra fuera de discusión pues vendría a causar más inconvenientes que a resolver problemas.

- **Hyperic:** el nombre de su solución es Hyperic HQ, una muy buena opción a tomar en cuenta por sus funcionalidades relevantes y a la vez necesarias en un SIEM, sin embargo, no se encuentra muy bien alineada para una posible implementación en multinacionales debido a que no maneja una gran cantidad de usuarios, se encuentra enfocada a brindar servicio a un número limitado de personas lo cual resulta contraproducente en organizaciones masivas.

2.4.2 Análisis de SIEMS para empresas PYMES

En este punto se presenta un breve análisis de la forma en la cual se adaptarían los SIEMS analizados en los puntos 2.3.1.1 y 2.3.2.2 en el entorno de empresas PYMES.

- **Splunk:** las empresas PYMES encontrarían una solución para todas sus problemáticas en caso de instalar esta herramienta, las características de esta plataforma permiten dar respuestas solidas contra cualquier tipo de vulnerabilidad y su proveedor se encuentra muy bien posicionado en el mercado, sin embargo, el costo de las licencias de este producto es claramente un factor negativo pues comparándolo con las otras herramientas viene a ser el más costoso.

- **IBM:** en cuento a empresas PYMES, si bien esta es una solución que no encaja para el nivel de sus necesidades, se pueden ver beneficiadas por la facilidad de uso de la herramienta y por la gama de controles orientados a usos dentro de escenarios no muy avanzados.

- **McAfee:** no se recomienda la implementación de McAfee ESM para núcleos de empresas PYMES pues como se habló, se necesita de una importante inyección de capital para utilizar todas las virtudes de esta solución y un desembolso de tal magnitud es algo fuera de la planificación de dichas organizaciones, podría causar problemas financieros, afectar los niveles institucionales y causar un grave desequilibro de los recursos.

- **Dell:** no se recomienda la implementación de RSA NetWitness para empresas PYMES pues como se habló, tanto la implementación como la operación de esta plataforma es bastante compleja y no se encuentra diseñada para organizaciones con un núcleo empresarial poco maduro, esta herramienta tiene soluciones muy avanzadas que son difíciles de operar y requieren de todo un equipo de trabajo para sacar su máximo rendimiento, en otras palabras, para empresas PYMES esta sería una herramienta sobrecargada y una perdida excesiva de recursos.

- **AT&T:** en el mercado de las empresas PYMES, las dos soluciones encuentran muchas oportunidades, para estructuras de ese tamaño fueron desarrolladas. En el caso de USM es ideal cuando se busca integrar controles de seguridad que no realizan un análisis o monitoreo profundo, además, la compra de su licencia es muy fácil de entender y su costo es menor si se lo compara con sus competidores. En el caso de OSSIM a pesar de tener una capacidad limitada es gratuita y resulta perfecta para organizaciones donde la parte económica no es estable.

- **Elastic:** para el entorno de las empresas PYMES se lo podría considerar tomando en cuenta las ventajas de ser un SIEM Open Source y la modularidad de sus componentes, sin embargo, no es la más adecuada

viéndolo desde el punto de vista de los recursos humanos que consumiría el armar el SIEM y el realizar las automatizaciones necesarias. Para esta plataforma se debe tomar en cuenta el desembolso a realizar en los técnicos necesarios para poner en funcionamiento esta solución.

- **Hyperic:** hablando de Hyperic HQ para empresas PYMES, esta es una solución que merece la pena darle una oportunidad, sus características, su modelo de negocio y sus funcionalidades se encuentran orientados para resolver problemas en organizaciones de ese tamaño, el único inconveniente seria su soporte, podría traer problemas en el futuro.

2.4.2.1 Comparación de productos SIEM para PYMES

A continuación se van a comparar algunos elementos presentes en cuatro productos SIEM, dos productos de paga y dos productos gratuitos, estas cuatro soluciones fueron seleccionadas tomando en consideración el análisis realizado en los puntos 2.4.1 y 2.4.2 enfocando dicho análisis en cuales son las herramientas que podrían tener un mejor manejo y adaptación en el entorno de empresas PYMES, por tanto, cuando se analizaron todas las soluciones se determinó que Splunk ES, QRadar, OSSIM e Hyperic HQ son las mejores opciones SIEM de paga y gratuitas para empresas pequeñas y medianas.

En la tabla 8 se puede observar un cuadro comparativo de cuatro productos SIEM.

Tabla 8.
Cuadro comparativo de productos SIEM.

Características	**Splunk Splunk ES**	**IBM QRadar**	**AT&T OSSIM**	**Hyperic Hyperic HQ**
Costo	Muy Alto	Alto	Sin Costo	Sin Costo
IDS	✓	✓	✓	✓
NIDS	✓	✓	✓	✗
Detección de vulnerabilidades	✓	✓	✓	✗
Monitorización de Host	✓	✗	✓	✓
Exploración de redes	✓	✓	✓	✗
Notificaciones o alertas automáticas	✓	✓	✓	✓
Complementos gratuitos	✗	✗	✓	✓
Retención de registros	✓	✓	✓	✗
Interfaz web	✓	✓	✓	✓

Número de usuario	Múltiples	Múltiples	Uno	Uno
Soporte	Profesional	Profesional	Comunitario	Comunitario

2.4.2.2 Elección del mejor SIEM enfocado a PYMES

De la lista inicial en la cual se encontraban los sistemas SIEM gratuitos y de paga más utilizados en el mercado se seleccionaron cuatro herramientas que no eran las mejores en cuanto a sus características y funcionamiento, pero si eran las mejores al ajustarse a las necesidades y limitaciones de las empresas PYMES, estas soluciones fueron Splunk ES de Splunk, QRadar de IBM, OSSIM de AT&T Cybersecurity e Hyperic HQ de Hyperic.

Como se puede ver en la tabla 8, en la segunda lista se realizó un análisis más profundo, se tomaron en cuenta las funciones más solicitadas por empresas PYMES y las amenazas más comunes que rodean a estas organizaciones. Con esa premisa se colocaron doce características importantes que debían ser cubiertas y analizando la información de cada plataforma se seleccionó a la herramienta OSSIM como la mejor solución, al final fue la herramienta con más puntos positivos cubriendo todos los aspectos críticos solicitados por las empresas pequeñas y medianas.

Se eligió a OSSIM como la mejor solución enfocada a cubrir con las necesidades y a resolver los problemas de empresas PYMES debido a que cumple con los siguientes puntos:

- No tiene costo.
- Tiene un sistema de detección de intrusos.
- Tiene un sistema de detección de intrusos en una red.

- Se encarga de la detección de vulnerabilidades.
- Realiza monitorizaciones de host.
- Lleva a cabo exploraciones de redes.
- Emite alertas automáticas en caso de encontrar un evento sospechoso.
- Los complementos manejados por esa plataforma son gratuitos.
- Realiza retenciones de registros.
- Su interfaz web es amigable con el usuario.
- Tiene un soporte comunitario.

2.5 OSSIM

Hablando de OSSIM, a esta plataforma se la puede definir de forma básica como una herramienta de gestión de eventos y seguridad informática de código abierto integrada por varios componentes dedicados a proteger la información. Estos componentes funcionan como un conjunto, trabajan de forma centralizada para lograr altas prestaciones al momento de recolectar información, monitorear eventos, dar prioridad al manejo de información completa, gestionar de mejor forma la masiva cantidad de reportes y detectar situaciones de seguridad. (Luzón, 2017)

Esta plataforma también utiliza alertas para informar lo más pronto posible al administrador de red o a la persona responsable de administrar la seguridad informática de la empresa sobre la situación que origino dicha alerta, con la notificación en manos del personal calificado, este se encargará de analizarlo, interpretarlo y dar respuesta al evento con el fin de mitigarlo o reducirlo hasta un punto en el cual no signifique un riesgo claro para la empresa.

Las características de OSSIM que vuelven a esta herramienta la más indicada para implementarse en empresas PYMES son las siguientes:

- No tiene costo.

- Maneja de forma eficiente el tráfico de los eventos de red.
- Su monitoreo es centralizado.
- Realiza pruebas de vulnerabilidad.
- Su interfaz web es fácil de entender y muy simple de manejar.
- Se encarga de recolectar los registros sin importar su lugar de origen.
- Utiliza alertas como medio de comunicación en caso de encontrar alguna anomalía en la red.
- Realiza el análisis de las situaciones fuera de lo común y de los posibles riesgos que amenacen la empresa. (Luzón, 2017)

2.6 OSSIM vs USM

AT&T Cybersecuriry tiene dos versiones de productos SIEM en el mercado, el primero de ellos es OSSIM del cual se habló con anterioridad y el segundo es USM, una plataforma cuyas cualidades son superiores a OSSIM, algo coherente tomando en cuenta el detalle de ser la versión pagada de ese proveedor lo cual va a causar un mayor interés al momento de realizar su diseño.

USM al ser una versión premium tiene mejores capacidades de monitoreo y un mayor número de controles para gestionar eventos de seguridad, por ello, sumándole el hecho de haber sido diseñada para entornos de empresas PYMES es una buena opción por considerar para una eventual implementación. En la tabla 9 se pueden observar las diferencias entre OSSIM y USM, ambas distribuidas por AT&T Cybersecuriry.

Tabla 9.
Cuadro comparativo, OSSIM vs USM.

Características	OSSIM	USM
Disponibilidad de producto	Software Open Source	Servicio localizado en la nube

Costo	Sin costo	Suscripción anual
Monitoreo de seguridad	Entornos virtuales locales y físicos	Entornos virtuales locales y físicos Aplicaciones en la nube
Arquitectura de implementación	Solo servidor	Entrega SaaS implementado con sensores para cada entorno monitoreado
Descubrimiento de inventario y activos	✓	✓
Evaluación de vulneravilidades	✓	✓
IDS	✓	✓
Monitoreo de comportamieto sospechoso	✓	✓
Correlación de eventos	✓	✓
Gestión de registros	✗	✓
Monitoreo en la nube	✗	✓
Monitoreo de aplicaciones	✗	✓

Tomado de (AT&T Cybersecuriry, 2020)

Como se observó en la tabla 11, USM es una plataforma con una mejor preparación en comparación a OSSIM, la diferencia y el motivo por el cual se seleccionó a la otra solución radica en el costo de las licencias, es mucho más fácil trabajar con una herramienta gratuita para el tipo de entornos empresariales de empresas PYMES.

En el cuadrante mágico de Gartner de los SIEM, AT&T Cybersecuriry se encuentra ubicado en la parte de jugadores de nicho, la solución analizada por Gartner para posicionar en ese lugar al proveedor fue USM por tanto todas las referencias dadas por esa empresa pertenecen a la versión de paga y no hacen referencia de su versión gratuita.

De forma breve Gartner habla de USM de la siguiente forma: es una plataforma diseñada para empresas medianas y pequeñas, su precio se encuentra por debajo del de sus competidores y ofrece un alto nivel de compatibilidad al momento de integrar los productos de su catálogo.

En el siguiente capítulo se analizarán las normas a las cuales se ajustan los productos SIEM analizados anteriormente.

3 CAPITULO III. ANÁLISIS DE LAS NORMAS ISO/IEC 27001:13 E ISO/IEC 27002:13

En este capítulo se analizarán las normas ISO orientadas al desarrollo de sistemas de gestión de la seguridad de la información aplicando un mayor énfasis en las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013, normas de las cuales se estudiará su estructura, especificaciones técnicas y la importancia de su uso para alcanzar óptimos niveles de seguridad en las redes de empresas pequeñas y medianas.

3.1 Normas ISO

Son una serie de estándares establecidos por la Organización Internacional para la Estandarización (ISO) enfocados a gestionar el orden en las distintas áreas de una empresa para alcanzar una calidad deseada.

Pese a ser un conjunto de reglas opcionales en la actualidad han ganado una alta reputación debido a los excelentes resultados de su uso lo cual a transformado ese grado opcional a uno casi obligatorio si lo que se busca es mantener una alta competencia con otras empresas y encontrarse dentro de los procesos globalizados ya que la mayoría de organizaciones alrededor del mundo trabajan utilizando las normativas dictadas por estas normas, de ahí estos estándares han recibido la aceptación internacional y el reconocimiento de todo el mundo. (ISOTools, 2020)

3.1.1 Objetivos de las normas ISO

Los objetivos sobre los cuales fueron creadas las normas ISO y que en la actualidad sirven para ir dibujando la trayectoria del desarrollo de nuevos o adaptación de antiguos estándares son los siguientes:

- Orientación.
- Simplificación.
- Coordinación.
- Unificación de criterios, se busca estandarizar las normas de servicios y productos. (ISOTools, 2020)

Perseguir dichas metas han llevado a estas normas hasta la cima, se han adoptado por una gran cantidad de empresas distribuidas por todo el mundo debido a que responden a diferentes necesidades como:

- Características de los productos.
- Seguridad ofrecida de los servicios y productos.
- Estandarizar las variables a considerar para presentar términos de calidad. (ISOTools, 2020)

3.1.2 Ventajas de las normas ISO para las empresas

Como sus objetivos se encuentran directamente enfocados a resolver las problemáticas de las empresas, está claro que utilizar dichas normas trae beneficios a todas las organizaciones independientemente del tamaño, las ventajas planteadas a alcanzar son las siguientes:

- Brinda herramientas a las empresas para llegar a tener y lograr mantener mejores niveles de calidad en la prestación de servicios o productos.
- Da pautas para alcanzar a satisfacer las exigentes demandas de los clientes.
- Las empresas reducen sus gastos, consiguen una mejor rentabilidad y logran elevar el nivel de productividad, contempla un mejor nivel de ventas.
- Utilizar estas normas mejora tu imagen con el cliente, logra aumentar la competitividad de la empresa.

- Ayuda a mitigar posibles incidencias ocurridas en el normal transcurso de la prestación o producción de servicios.
- Mediante datos con información específica permite instaurar un modelo robusto de mejora continua en los procesos del negocio.
- Ayuda a entrar en mercados internaciones, permite a la empresa ser vista por clientes con una mejor jerarquía. (ISOTools, 2020)

Si bien brinda a las empresas de varias herramientas para lograr una mejor funcionalidad y entregar un mejor servicio a los clientes, las ventajas de las normas ISO sobrepasan ese margen a un punto en el cual hasta los gobiernos se ven favorecidos pues se apoyan en ellas para controlar el comercio exterior y establecer varios requisitos sujetos a controles como: un mínimo de calidad en los servicios, un nivel apropiado de seguridad, diversas cuestiones del medio ambiente, etc.

3.1.3 Familias de las normas ISO

Al ser las normas ISO una serie de estándares dedicados a diferentes tipos de empresas para alcanzar una calidad deseada estamos hablando de estándares enfocados a varios sectores de la producción, por ello, a todas estas normas se las agrupan en varias familias con una nomenclatura especifica tomando en cuenta su naturaleza, importancia y aplicabilidad.

Cada una de estas familias tienen un diferente propósito a certificar dependiendo de su área. En la tabla 10 se puede observar las familias en las cuales se dividen las normas ISO más importantes, las nomenclaturas utilizadas para identificarlas y sus áreas de trabajo o de implementación.

Tabla 10.
Familias de las normas ISO.

Sectores	Familias	Descripción
Gestión de calidad	ISO 9001:2015, ISO 900 4:2018, ISO/IEC 17025:2017, ISSO TS 6949:2016	Se encuentran todas las normas dedicadas a regularizar los estándares enfocados a la calidad de los servicios prestados y productos en el mercado de todas las organizaciones, sin importar su sector de actividad, tamaño, propiedad capital, ámbito de actuación, forma jurídica, etc.
Gestión del medio ambiente	ISO 14001:2015, ISO 50001:2018	Estas normas ayudan a las organizaciones a colocar todas sus actividades dentro de las regularizaciones establecidas para respetar el medio ambiente. Permiten cumplir con las legislaciones de protección ambientales, ayuda a concientizar y vienen a exigir un buen trato al entorno.
Gestión de riesgos y seguridad	ISO 45001:2018, ISO 22000:2005, ISO 22301:2019, ISO 27001:2013, ISO 28000:2007, ISO 31000:2009, ISO 39001:2013, ISO 19600:2014	En esta área se encuentran aquellos estándares enfocados a evitar, impedir o mitigar todos los riesgos relacionados con las amenazas que enfrentan las empresas debido a sus negocios.
Gestión de responsabilidad social	SA 8000:2014, ISO 26000:2010	Las normas de esta sección hablan sobre el comportamiento ético y moral. Su objetivo principal es lograr implantar un comportamiento ético y transparente dentro del modelo de negocio de todas las empresas.

Tomado de (ISOTools, 2020).

3.2 Familia ISO/IEC 27000

Esta familia se encuentra en el área de gestión de riesgos y seguridad dada la naturaleza de su trabajo, se encarga de brindar normas técnicas de Seguridad de la Información que certifiquen la integridad informática de las empresas utilizando una serie de normas previamente integradas a su familia.

Estas normas a pesar de tener su propia nomenclatura pertenecen a la serie 27000, debido a su área de aplicación todas ellas se dedican a dar respuestas o en su defecto a dar apoyo para mantener la seguridad de la información en todas las áreas de la empresa en donde se maneje información, estas normas trabajan siempre en conjunto pues sus integrantes se complementan para brindar una especie de soporte que es ofrecido a través de la recopilación de las funciones principales de sus normas, de forma general estas establecen que:

- Implantan controles
- Manejan la gestión de riesgos
- Establecen modelos de auditoria
- Desarrollan buenas prácticas.
- Trabajan con recomendaciones. (ISO 27000, 2015)

3.2.1 Objetivos de la norma

En las normas de la familia ISO/IEC 27000 siempre se han presentado modificaciones cada cierto tiempo y para enfocar correctamente estos cambios, en general destinados a responder las nuevas exigencias de los clientes, verifican si al aplicar sus normas se cumplen con los siguientes objetivos:

- Aportar con recomendaciones relevantes y de utilidad a nivel administrativo o técnico para el administrador de red o la persona encargada de gestionar la seguridad informática de la empresa.

- Preservar todos los niveles de seguridad manejados en el sistema siempre manteniendo en vista posibles mejoras que puedan ser llevadas a cabo mediante controles de análisis con el fin de blindar a la red empresarial, la infraestructura y la información almacenada de posibles ataques.

- Generar protocolos orientados a ofrecerse como fuente de apoyo en caso de una posible amenaza y en caso de comprobarse el peligro ayudar a dar respuesta en el menor tiempo posible.

- Educar al personal de la empresa en términos de seguridad de la información para concientizar el rol que ocupan, la importancia de sus datos personales, el peligro al cual se expone la información manejada por la organización, el buen uso de sus credenciales y como utilizar de forma correcta los demás elementos de seguridad manejados por ellos.

- Realizar monitoreos de forma periódica para comprobar la utilización de las normas, revisar el desarrollo de las recomendaciones planteadas sobre las actividades de la empresa y en caso de ser necesario sugerir mejoras.

- Mantener siempre lista y al alcance de la persona autorizada la documentación con la información de todos los procesos manejados por el SCSI. (ISO 27000, 2015)

3.2.2 Ventajas de la norma ISO/IEC 27000 en las empresas

Implementar las normas integradas en la familia ISO/IEC 27000 ofrece una mayor garantía en el nivel de seguridad ya que las normativas manejadas por esta serie se enfocan en la mejora continua de los procesos para la protección de la información, sin embargo, al realizar la implementación aparte de esa característica también deben sumársele las siguientes ventajas:

- Ayuda a cumplir con los principios de la seguridad de la información (confidencialidad, integridad y disponibilidad) disminuyendo el riesgo de posibles amenazas que puedan modificar, eliminar, robar o tener acceso a los datos de los usuarios.

- Mejora el entendimiento y la ejecución de los procesos del sistema, se diseñan protocolos con buenas soluciones y permite una administración más clara de los recursos.

- En caso de ser necesario es posible acoplar otro tipo de normas ISO, una empresa puede manejar varias normativas distintas sin que estas interfieran en el trabajo de la otra.

- Usar estas normativas generan una cierta ventaja competitiva en relación con sus otros competidores pues la hace ver como una empresa mejor preparada.

- Mejora la imagen de la organización con los clientes y con sus mismos empleados, una empresa con un mejor nivel de seguridad genera confianza provocando un buen ambiente laboral y una serie de comentarios positivos. (Villacis, 2016)

3.2.3 Evolución a través del tiempo

Estas normas tienden a ir cambiando con el transcurso del tiempo, se ajustan a las nuevas necesidades de las empresas y van respondiendo a las más exigentes demandas del mercado. Para ir actualizándose toman en cuenta la creación de nuevas normas que aparecen para remplazar a otras ya obsoletas o simplemente ajustan los parámetros de una norma ya existente y se crea una nueva versión mejorada de la misma, por esas fluctuaciones la familia 27000 presenta varias versiones en cada uno de sus estándares.

Estas continuas actualizaciones se las realizan de forma periódica, usualmente cada 4 o 5 años, por esta razón cada una cuanta con una nomenclatura distinta, sus números de identificación se encuentran reservados y van desde las normas ISO/IEC 27000 hasta llegar a la norma ISO/IEC 27019, en ese punto tienen un salto para comenzar de nuevo con la norma ISO/IEC 27030 topando como fondo la norma ISO/IEC 27044, en esta última sección se incluye a la norma ISO/IEC 27799. (Columba, 2017)

En la figura 13 se puede observar la evolución de la familia ISO 27000, para el gráfico se tomaron en cuenta las normas más importantes y la última actualización presentada para realizar el diseño de un SGSI.

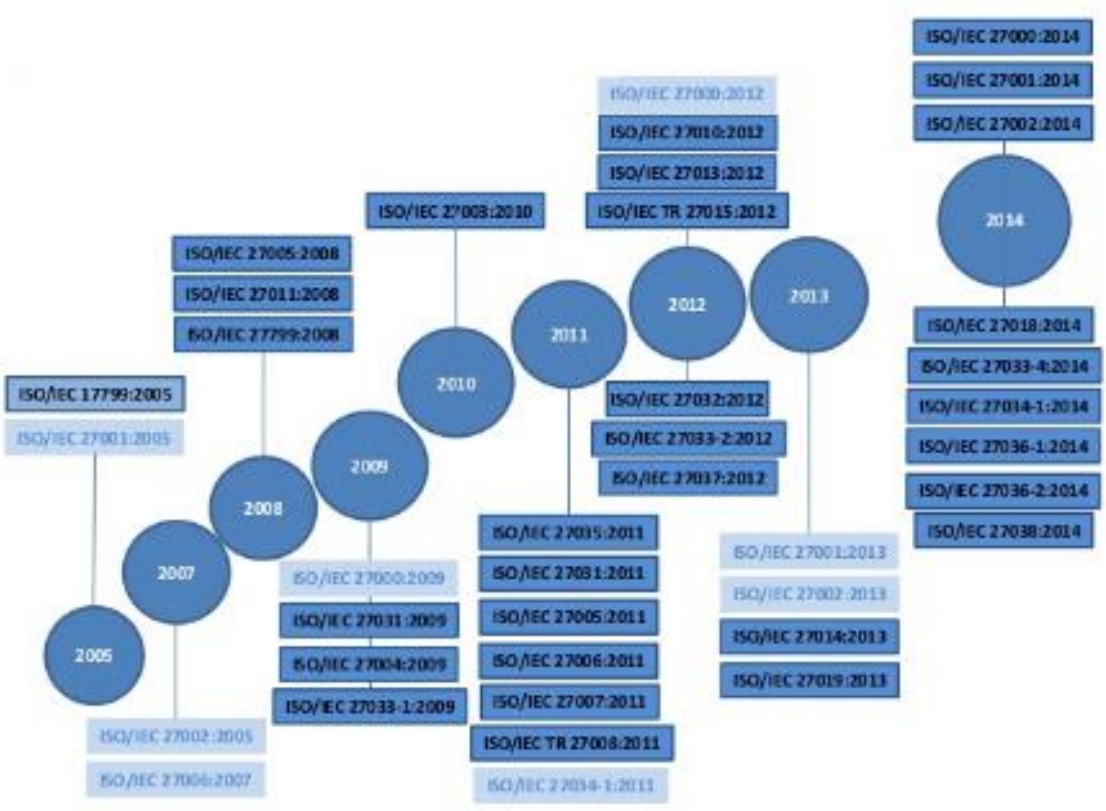

Figura 13. línea de tiempo de la familia ISO/IEC 27000.

Tomado de (Urbina, 2019)

3.3 Estándares ISO/IEC 27000

En esta familia se encuentran varias normas con un objetivo similar, las cualidades de estos estándares muchas veces se complementan y causan un mejor rendimiento por medio de mejores soluciones, sin embargo, se debe tomar en cuenta que al realizarse una implementación varios factores entran en escena, dependiendo de estos inconvenientes existe la posibilidad de no poder aplicar todas las normas de esta serie pues en muchos casos al tener un objetivo similar puede darse la circunstancia de colocar una norma por encima de otra e incluso hay normas aun en etapa de desarrollo o experimentación. (Villacis, 2016)

Debido a esos problemas y añadiendo los factores de que la norma ISO 27001 es la encargada de colocar los principios a seguir en la gestión de la seguridad de la información, tiene un carácter internacional, se la puede utilizar para cualquier tipo de organización y principalmente a que es la única opción certificable, es el estándar por utilizar para la implementación de un SIEM en PYMES.

3.3.1 Estándar ISO/IEC 27000:2014

Apareció por primera vez en 2009, posteriormente seria actualizada en el año 2012 y finalmente mantendría la versión de 2014 hasta la actualidad. Se enfoca en dar una visión global de las maneras de actuar y los objetivos que siguen las normas integradas en esa familia, instruyendo a las empresas sobre las metodologías seguidas y el alcance máximo en el cual actúan. (Ramírez & Moreira, 2017)

También tiene el objetivo de presentar un conjunto de términos y definiciones relacionados a las normas de esta serie, da una breve introducción de los sistemas SGSI y termina explicando de forma básica las reglas a seguir para

establecer, monitorizar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información.

3.3.2 Estándar ISO/IEC 27001:2013

Su primera versión fue publicada en el año de 2005, pasaría a ser modificada en 2013 y mantendría esa versión hasta la fecha. Esta norma es la más importante de toda la familia, llega al punto de haber sido reconocida como su estándar principal y dicho reconocimiento está bien fundamentado pues las reglas que propone albergan todos los requisitos para la gestión de un sistema SGSI.

Esta norma da varias ventajas, se la puede implementar en todo tipo de entorno, puede ser utilizada por cualquier tipo de persona instruida en el tema, etc., independientemente de los factores siempre se encarga de entregar una estrategia de trabajo a implementar. A lo anterior se le añade, esta norma da lugar a certificación, esto quiere decir que una entidad externa dedicada a seguir esos procesos se encargara de confirmar la presencia de la seguridad de la información en dicha compañía en cumplimiento con los parámetros dictados por la norma ISO/IEC 27001. (Ramírez & Moreira, 2017)

En la figura 15 se puede ver de forma clara el aumento en el número de empresas a nivel mundial que se certifican en el estándar ISO/IEC 27001.

Figura 14. Diagrama de barras de las empresas certificadas bajo la norma 27001. Tomado de (ISO 27001, s.f.)

3.3.3 Estándar ISO/IEC 27002:2013

Su primera aparición la tuvo bajo el nombre de ISO 17799:2005 y seria en el año 2007 cuando tomaría el nombre de ISO/IEC 27002 el cual mantiene hasta la actualidad. El enfoque del estándar es el de una guía de buenas prácticas, es decir, se encarga de establecer las directrices y los principios que servirán de base en todas las etapas de la gestión de la seguridad de la información implementada dentro de una empresa.

En términos generales, esta norma es un catálogo cuyo contenido ha sido escrito a partir de la experiencia vivida de otras personas en este campo y mediante diversos tipos de colaboraciones, la recopilación de toda esa información ha hecho posible diseñar una estrategia y encontrar los objetivos comúnmente aceptados en torno a la gestión de la seguridad de la información. Alberga varios objetivos de control que a su vez manejan diferentes tipos de controles que buscan ayudar a los usuarios en el desarrollo de reglas de seguridad y practicas eficientes relacionadas a gestionar los parámetros de seguridad.

Por esa razón, esta norma es un punto clave dentro de su serie, los controles que ofrece deben ser cuidadosamente seleccionados y es por ello por lo que su elección se encuentra sujeta a los resultados encontrados en un análisis de riesgos realizado con anterioridad y el nivel de su implementación se determinara tomando en cuenta los requisitos de seguridad de la empresa y los recursos disponibles, buscando siempre un buen balance entre seguridad y precio. (Gómez & Álvarez, 2015)

3.3.4 Estándar ISO/IEC 27003:2010

Es un estándar sin opción a ser certificable el cual fue publicado en 2010 y se centra en la implementación de la norma ISO/IEC 27001. Sirve como una guía

enfocada en los puntos críticos que se necesitan resolver para alcanzar un nivel de diseño y una posterior implementación exitosa de un SGSI.

Esta guía se caracteriza por su nivel de detalle, habla de la implementación desde la primera fase definida como el momento de concepción, hasta ser finalmente puesta en marcha adentrándose a la fase de implementación. Adicionalmente, describe el proceso a seguir para obtener la aprobación de implementación del SGSI. (Ramírez & Moreira, 2017)

3.3.5 Estándar ISO/IEC 27004:2009

Es una norma publicada en 2009 sin opción a ser certificable. Sirve como guía para determinar los niveles de eficacia en los cuales se encuentran trabajando los controles implementados por el estándar ISO/IEC 27001 y el SGSI, para llegar a determinar esos parámetros esta norma específica el desarrollo y utilización de un conjunto de métodos y métricas orientadas a calificar el desempeño mostrado hasta una fecha específica. (Ramírez & Moreira, 2017)

3.3.6 Estándar ISO/IEC 27005:2011

La primera edición apareció en el año 2008 y en 2011 se anunció al público su segunda edición. Cumple la función de proporcionar distintas directrices enfocadas al manejo de la gestión de riesgos, apoya el enfoque de los conceptos manejados por la serie a la cual pertenece y está diseñada para ayudar con la seguridad de la información basándose para ello en un nuevo enfoque, viéndolo desde el punto de la gestión de riesgos. (Ramírez & Moreira, 2017)

3.3.7 Estándar ISO/IEC 27006:2015

Esta norma fue publicada en el año 2007. Aporta a esta serie con la descripción de los requisitos necesarios para realizar la certificación de los SGSI y ayuda con las acciones de acreditación de entidades relacionadas con auditoria, sin embargo, a este estándar no se le atribuye la acción de acreditar, es más bien visto como una herramienta que facilita la interpretación de la norma ISO/IEC 17021 la verdadera norma enfocada a realizar la acreditación. (Ramírez & Moreira, 2017)

3.3.8 Estándar ISO/IEC 27007:2020

Fue publicada en el año 2011 y es una norma utilizada como una herramienta de guía para realizar auditorías de un SGSI, viene a dar apoyo a lo establecido por la norma ISO 19011. (Ramírez & Moreira, 2017)

3.3.9 Estándar ISO/IEC 27011:2016

Apareció por primera vez en 2008 y esta es una guía enfocada a gestionar la seguridad de la información dentro del sector de las telecomunicaciones, tiene la peculiaridad de haber sido desarrollada con la colaboración de la ITU. (Columba, 2017)

3.3.10 Estándar ISO/IEC 27014:2013

En términos generales es un estándar creado como un medio de gobernanza sobre la seguridad de la información, facilita el trabajo de las empresas al momento de evaluar, dirigir, controlar y comunicar. (SGSI, 2014)

3.3.11 Estándar ISO/IEC 27031:2011

Es una norma publicada en 2011 y utilizada como un mecanismo de guía para brindar soporte al momento de realizar adecuaciones dentro del sector de las comunicaciones o de las tecnologías de la información para adaptar nuevas tecnologías buscando mejorar la continuidad del negocio. (Ramírez & Moreira, 2017)

3.3.12 Estándar ISO/IEC 27032:2012

Publicada en 2012. De forma general esta es una guía desarrollada para dar apoyo a la seguridad cibernética, mejorando con ello el margen de seguridad al momento de realizar intercambios de información. (Ramírez & Moreira, 2017)

3.3.13 Estándar ISO/IEC 27033:2009

Proporciona una vista de forma general de la seguridad en la red, para realizar esta actividad el estándar maneja siete componentes los cuales son:

- **27033-1:** Manejo de conceptos generales.
- **27033-2:** Diseño de la seguridad e implementación en la red.
- **27033-3:** Manejo de los escenarios de referencia de redes
- **27033-4:** Mantener seguras las comunicaciones que se realicen entre distintas redes
- **27033-5:** Asegurar las comunicaciones utilizando para ello VPNs
- **27033-6:** Convergencia IP
- **27033-7:** Conexiones inalámbricas. (Columba, 2017)

3.3.14 Estándar ISO/IEC 27034:2011

Esta guía se desarrolló buscando alcanzar niveles óptimos de seguridad en las aplicaciones informáticas, para ello se establecieron los siguientes componentes:

- **27034-1:** Manejar los conceptos generales.
- **27034-2:** Revisar el marco normativo de la empresa.
- **27034-3:** Analizar el proceso que sigue la gestión de la seguridad con las aplicaciones.
- **27034-4:** Validar el nivel de seguridad en las aplicaciones.
- **27034-5:** Monitorizar la distribución de los datos, los protocolos establecidos y los controles de las aplicaciones instaurados.
- **27034-6:** Crear una guía enfocada para la seguridad de las aplicaciones de un uso definido. (Columba, 2017)

3.3.15 Estándar ISO/IEC 27035:2011

Esta norma se dedica a resolver los problemas en la seguridad causadas por posibles incidentes como fallos, controles de seguridad ausentes o soluciones incompletas. Cuando eso ocurre las amenazas pasan sin problemas y es el deber de esta norma gestionar estos incidentes aplicando controles correctivos. (SGSI, 2014)

3.3.16 Estándar ISO/IEC 27037:2012

Tiene un mayor enfoque a los dispositivos electrónicos móviles como celulares, cámaras, tarjetas de memoria, etc., esta norma sirve como guía para identificar, recopilar, consolidar y preservar toda la información almacenada en esos dispositivos para después ser utilizada como una evidencia digital en las situaciones que lo ameriten. (Columba, 2017)

3.4 Estructura general de los estándares ISO/IEC 27000

Las normas de la serie 27000 son estándares relacionados con la seguridad de la información, debido a esa naturaleza todas buscan fortalecer los métodos de protección de la empresa y para lograr ese fin muchas veces tienen que implementarse varios estándares de esta familia pues sus características al complementarse ofrecen un mejor funcionamiento mediante su apoyo mutuo y la mejora continua del proceso que realizan.

En la figura 14 se puede observar la estructura de las normas de esta familia. En la figura se encuentran las ramificaciones más importantes, destacando la presencia de guías específicas para ciertos sectores como es el caso del área de telecomunicaciones.

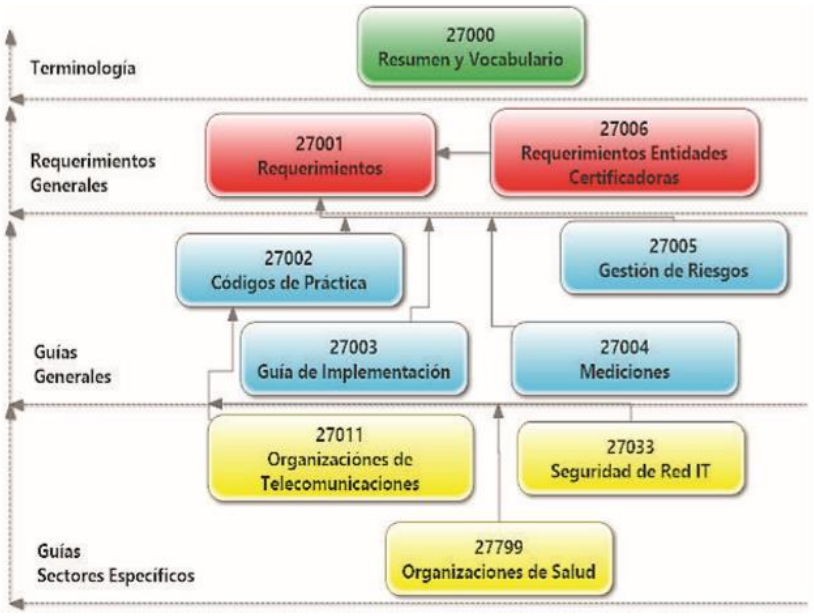

Figura 15. Estructura general de la familia ISO/IEC 27000.

Tomado de (Columba, 2017)

3.5 Norma ISO/IEC 27001:2005

Esta es la versión anterior de la norma seleccionada como la ideal para implementar en entornos de empresas PYMES.

En su tiempo esta norma era tomada como un estándar internacional el cual establecía parámetros para mantener en óptimas condiciones de trabajo a los sistemas de gestión de la seguridad de la información, para conseguir esa meta se apoyaba en el ciclo de mejora continua (PDCA) y en una alianza formada con las normas ISO 14001 e ISO 9001. (Audea, 2007)

Los puntos tratados por esta norma para conseguir mejorar el rendimiento del sistema de gestión eran los siguientes:

- Revisaba los riesgos.
- Realizaba auditorías internas del sistema de gestión de la seguridad de la información.
- Seleccionaba los controles en base al nivel de aceptación de los riesgos de la empresa.
- Orientaba la evaluación de los riesgos buscando posibles resultados comparables entre sí.
- Manejaba mediciones para controlar el grado de efectividad del SGSI.
- Actualizaba controles, procedimientos y demás medidas de seguridad ya establecidas.
- Manejaba un documento de aplicabilidad de todas las medidas de seguridad. (Audea, 2007)

3.6 Evolución de la norma ISO/IEC 27001

El encontrarse en un medio siempre cambiante obliga a cambios, eso sucedió con la norma ISO/IEC 27001, se vio sometida a continuas actualizaciones que

comenzaron en los años 90, para ser más específicos en 1998, fecha en la cual aparecería por primera vez bajo el nombre de BS 7799-2 especificando las condiciones para la certificación de los sistemas SGSI, no sería hasta el año 2005 donde cambiaria completamente su nomenclatura para comenzar a ser llamada 27001:2005 y en el año 2013 pasaría a ser reconocida como 27001:2013, la versión que se mantiene hasta la fecha. (Villacís, 2016) En la figura 13 se puede observar la evolución de la familia ISO/IEC 27001.

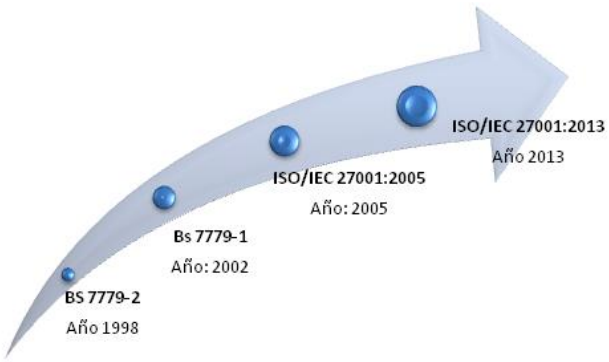

Figura 16. Evolución de la norma ISO/IEC 27001.

Tomado de (Giudice, 2014)

3.7 Norma ISO/27001:2013

Esta es la norma más importante de la serie 27000, destaca entre las otras por ser un estándar internacional diseñado para generar juicios que evalúen, revisen, mejoren, establezcan, implementen, operen y monitoreen un SGSI.

Como ya es completamente necesario contar con un sistema SGSI pues es considerado como una decisión estratégica de negocio para mantener la competitividad en el mercado, es muy importante saber orientar a esta herramienta para resolver los problemas de seguridad en la red, esta norma se encarga de eso, alinea las necesidades, requisitos de seguridad, los objetivos y protocolos de la empresa con las soluciones que ofrece el SGSI.

Todas las empresas necesitan de un estudio previo antes de llevar a cabo una implementación de cualquier tipo y esta no es la excepción. Se necesita saber identificar y como administrar de forma correcta las actividades realizadas por la empresa, por ello, es completamente necesario contar con un sistema de procesos el cual contenga información ya almacenada sobre las actividades, la correlación de los procesos y la gestión a considerar dependiendo del caso encontrado. (Robalino, 2018)

El funcionamiento y los objetivos de esta norma internacional llevan al usuario a comprender la importancia de los siguientes puntos:

- Comprender cuales son las necesidades de la empresa en cuestiones de seguridad de la información y la necesidad de colocar políticas sobre estas con el fin de proteger los datos de posibles amenazas.

- Instalar nuevos controles que permitan manejar las vulnerabilidades a las cuales aún no se les ha dado respuesta.

- Controlar mediante un monitoreo periódico el grado de efectividad presentado por el SGSI

- Lograr implementar un ciclo de mejora continua tomando como base los objetivos de la empresa.

Para lograr ese modelo de mejora continua la norma ISO/IEC 27001:2013 utiliza el modelo PDCA cuya estructura se basa en un ciclo repetitivo formado por 4 fases (Planear, Hacer, Chequear, Actuar) las cuales se van autoalimentando con los resultados obtenidos en la fase anterior. Este modelo es utilizado por esta norma en todos los procesos del SGSI. (Robalino, 2018)

3.7.1 Estructura de la norma 27001:2013

La norma ISO/IEC 27001:2013 presenta una estructura dividida en once secciones y a estas se le suma el anexo A. Las secciones comprendidas en el rango del 0 al 3 vienen a ser introductorias por tanto su implementación no es obligatoria, las secciones comprendidas en el rango del 4 al 10 son obligatorias pues básicamente contienen la estructura completa de la norma y con respecto a los controles del Anexo A solo se llegan implementar en caso de que corresponda en la declaración de aplicabilidad.

3.7.1.1 Introducción

En esta parte se explica cuál es el objetivo de la norma 27001 y habla sobre la compatibilidad existente con otras normas de gestión.

Explica que el objetivo de la norma es dotar de herramientas para lograr establecer, implementar, mantener y mejorar de forma continua los sistemas SGSI. Para ello es capaz de aplicar técnicas de alto nivel como texto idéntico, términos comunes, etc.

3.7.1.2 Ámbito

Aparte de brindar apoyo para mejorar el rendimiento de los sistemas SGSI también maneja requerimientos estrictos para valorar el trabajo realizado por estos y por el tratamiento de riesgos dados de la seguridad de la información dentro de cualquier tipo de organización.

3.7.1.3 Referencias Normativas

En esta parte se realiza una ligera acotación a la norma ISO/IEC 27000 debido a ser el estándar en el cual se encuentran comprendidos todos los términos y definiciones tratados dentro de toda la serie 27000.

3.7.1.4 Términos y definiciones

Se procede a realizar una referencia de la norma ISO/IEC 27000 por ser quien contiene la versión completa sobre términos y definiciones, esa información será utilizada para propósitos especificados en el documento, dependerá de cada caso.

3.7.1.5 Contexto de la organización

En esta área se manejan diferentes aspectos relacionados con el conocimiento de las cuestiones internas y externas relacionados con la empresa, busca comprender las necesidades y sobre todo las expectativas que mantienen las partes interesadas, a esto hay que sumarle la medición del alcance del SGSI. Esta área viene a ser parte del ciclo PDCA, para ser más específicos, pertenece a la fase de planificación. (Columba, 2017)

3.7.1.6 Liderazgo

En esta parte se mide el grado de responsabilidad de las personas situadas en la alta dirección de las empresas, se debe demostrar capacidad de liderazgo, pero sobre todo compromiso con todos los aspectos del SGSI, se necesita de su apoyo para asegurar puntos clave como: integración de requisitos en el sistema, establecimiento de políticas, utilización de recursos empresariales y verse predispuesto a brindar recursos faltantes.

Estas personas de igual forma tienen la obligación de asegurarse de que todas las responsabilidades relacionadas con la seguridad de la información se encuentren bien cubiertas. Igual al contexto de la organización, esta sección forma parte de la misma fase del ciclo PDCA.

3.7.1.7 Planificación

En esta sección se definen los elementos necesarios para realizar la evaluación de riesgos, la declaración de aplicabilidad, la determinación de objetivos y el tratamiento de posibles riesgos. Para lograr cumplir con todos estos puntos las organizaciones deben considerar los siguientes aspectos:

- Determinar un proceso de valoración de riesgos que se ajuste a las necesidades de la empresa, posteriormente aplicarlo y junto a los niveles de aceptación de riesgos trabajar en conjunto para armar criterios de valoraciones de riesgos.

- Se debe identificar todos los riesgos asociados a crear vulnerabilidades en los principios de la seguridad de la información dentro del alcance del SGSI.

- Rastrear el origen de las amenazas es muy importante, con ello se puede identificar posibles puertas traseras en el sistema.

- Se deben realizar estimaciones para poder valor correctamente las posibles consecuencias de vulnerabilidades que aún no se han materializado.

- Un punto clave es la valoración de la probabilidad de que se materialicen riesgos ya identificados, se debe determinar el nivel riesgo. Para controlar esas situaciones la empresa debe tener bien definido un proceso de tratamiento de riesgos, eso se logra cuando se está bien preparado, cuando se han definido correctamente los controles que se necesitan.

- Contar con la declaración de aplicabilidad es de gran importancia, este archivo permite mantener el control de las medidas de seguridad aplicadas.

- En caso de encontrar al dueño de un riesgo obtener su aprobación del plan de tratamiento para mitigar las amenazas ayuda a crear un ambiente más seguro, da la sensación de una mejor preparación.

Todo lo expuesto debe encontrarse sintonizado con la política de seguridad de la empresa y es este ente el cual va a decir los recursos a utilizar, los responsables de tales proyectos y el mecanismo para ser evaluados. (Columba, 2017)

3.7.1.8 Soporte

En esta sección la empresa debe definir asuntos como:

- Calcular un estimado de los recursos necesarios para garantizar el éxito de una posible implementación y mantenimiento de un SGSI.

- Comprobar el nivel de aptitud de las personas que laboran en todas las áreas de la organización, se debe generar conciencia orientada a mantener la seguridad de la información, se puede dictar un curso para educar a los empleados sobre términos como ingeniería social.

- Trabajar con información bien documentada, esto ayuda a conocer cuales acciones han sido tomadas sobre un determinado documento o proceso.

Realizar un análisis para saber las necesidades reales de comunicaciones externas e internas al SGSI. (Columba, 2017)

3.7.1.9 Operación

En esta área la empresa debe definir asuntos como:

- Tomar en cuenta los requisitos para lograr seguridad en un entorno empresarial, se debe trabajar en la planificación, implementación y control de los procesos pertinentes.

- Realizar valoraciones de riesgo de forma periódica y adicionalmente documentar todos estos datos ya que pueden servir para ser puestos bajo análisis en caso de algún inconveniente.

- Llevar acabo el plan para tratar riesgos conservando siempre documentación sobre todos estos procesos. (Columba, 2017)

3.7.1.10 Evaluación de desempeño

En esta área la empresa debe definir asuntos como:

- Utilizar el método más eficaz para evaluar el rendimiento del SGSI y de la seguridad informática.

- Mantener bien documentada toda la información relacionada con los resultados arrojados en monitoreos y mediciones, estos servirán como evidencia en caso de existir algún problema.

- Realizar auditorías de forma periódica basadas en las especificaciones sujetas en esta norma y añadiéndole el alcance presentado.

- Mantener toda la información bien documentada de los resultados alcanzados y de todos los asuntos relacionados con auditoria para conservar siempre una evidencia de los hechos. (Columba, 2017)

En este punto es importante recalcar que tanto el personal encargado de forma directa de manipular y supervisar el SGSI como los altos cargos de la empresa comparten la responsabilidad de encontrarse pendientes del rendimiento, eficacia y conveniencia ofrecida por el sistema.

3.7.1.11 Mejora

En esta sección se manejan las no conformidades, en caso de suceder este evento la empresa debe inmediatamente encargarse de ello por medio de medidas correctivas e inmediatamente pasar a hacer frente a las consecuencias de este problema mostrándose siempre preparado con la información documentada de los hechos que generaron esa no conformidad. (Pico, 2016)

En este punto también se maneja la mejora continua, después de resolver el problema se deben tomar acciones para convertir esa debilidad en fortaleza.

3.7.1.12 Anexo A

Hace referencia a los dominios y controles que se obtienen de la norma ISO/IEC 27002:2013, un total de 114 controles y 14 dominios (secciones A.5-A.18), se encuentran alineados con dicha norma.

3.8 Comparación entre los estándares ISO/IEC 27001:2005 e ISO/IEC 27001:2013

El actualizar una norma siempre significa realizar cambios en su estructura que dependiendo del caso pueden ser añadir, eliminar o modificar las reglas de su anterior versión para lograr un cambio positivo en los resultados ofrecidos al implementar el nuevo estándar, estos cambios se ven sujetos por varios factores

siendo el principal el desarrollo de la tecnología que obliga a crear mejores normas a seguir para garantizar la seguridad de la información.

En la figura 17 se pueden observar los cambios realizados en la última versión de esta norma, su estructura cambia, algunos campos desaparecen y a otros cuantos se los ve reorganizados.

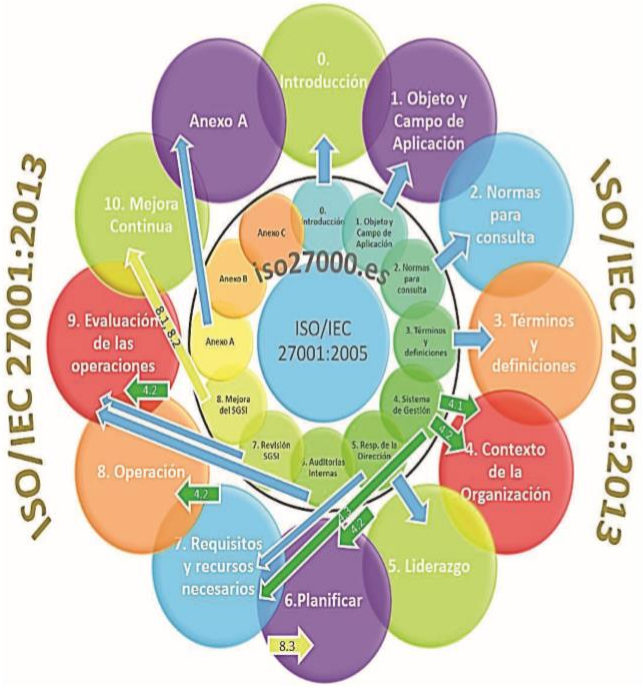

Figura 17. Diagrama de reorganización de las cláusulas de la norma ISO 27001. Tomado de (Columba, 2017)

Algunos de los cambios más importantes entre estas dos versiones de normas son las siguientes:

- El estándar actualizado tiene la característica de ser menos prescriptivo y descriptivo, eso permite dar una mayor libertad al momento de implementarse.

- En el modelo desarrollado en el 2013 no se hace una referencia manifiesta sobre el modelo PDCA, sin embargo, se encuentra presente, lo único que ha cambiado es su distribución, se reparte dentro de su misma estructura.

- En la nueva versión se da comienzo al proceso para estandarizar los requisitos fundamentales y las terminologías de los sistemas SGSI.

- La norma ISO/IEC 27002 deja de ser un estándar utilizado como una normativa de referencia.

- En la nueva versión los requisitos que se necesitan para realizar la evaluación de riesgos son más generales debido a su alineación con la norma ISO 31000, esto se debe al manejo de dicha norma sobre los conceptos de riesgos.

- Los términos y definiciones fueron removidos a la norma ISO/IEC 27000. (Columba, 2017)

3.9 Norma ISO/IEC 27002:2005

Es la anterior versión de la norma ISO/IEC 27002:13 y se puede decir que es la primera de sus evoluciones en entrar a la serie 27000 pues la anterior versión de esta llevaba otro tipo de nomenclatura.

Esta norma seguía las funciones que ha tenido desde su primera aparición, se encontraba enfocada en la seguridad de la información y servía como una guía de buenas prácticas la cual contenía información muy importante para ayudar a las organizaciones en la selección de controles.

Destacaba por el cumplimiento de los controles descritos en su guía y tenía como característica única el presentar una estructura formada por 11 dominios, 39 objetivos de control y 133 controladores.

3.10 Evolución de la norma ISO/IEC 27002

Durante su historia, la norma ISO/IEC 27002 se vio sometida a varias actualizaciones. Apareció por primera vez en 1995 bajo el nombre de BS 7799-1 la cual brindaba a todas las empresas buenas prácticas enfocadas a la seguridad de la información, entrando en el año 2000 la Organización internacional de normalización (ISO) adopto a esta norma y le fue cambiado el nombre a ISO 17799 y en el año 2007 pasaría a ser finalmente conocida como ISO 27002, nomenclatura utilizada aun hasta la fecha. (Villacís, 2016)

En la figura 18 se puede observar la evolución de la familia ISO/IEC 27002

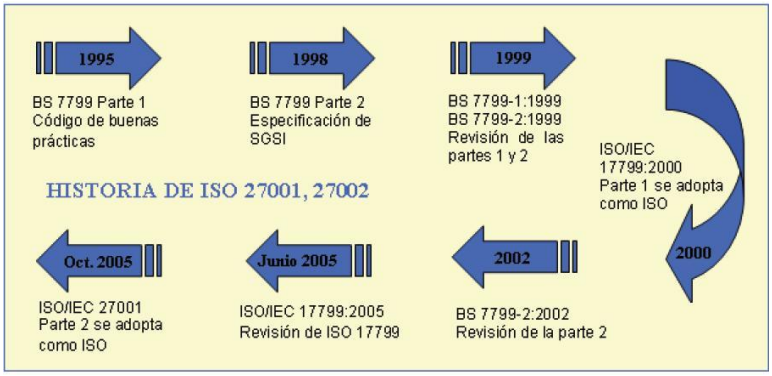

Figura 18. Evolución de la norma ISO/IEC 27002.

Tomado de (ISO 27000, 2015)

3.11 Norma ISO/IEC 27002:2013

Esta es la última versión de la nomenclatura ISO/IEC 27002, pertenece a la serie 27000 por tanto se trata de una norma enfocada en brindar respaldo a empresas para la toma de decisiones relacionadas con la seguridad de la información y al

igual que su antecesora esta norma trabaja como una guía de buenas prácticas escritas por la experiencia de varias personas en el manejo de esta tecnología.

Esta norma trabaja en conjunto con la norma ISO/IEC 27001 (perfecciona su aporte) utilizando para ello su estructura compuesta por 14 dominios entre los cuales se distribuyen según la naturaleza de sus acciones 114 controles que ayudaran a la norma 27001 a cumplir con los objetivos planteados por las empresas en cuanto a los estándares de seguridad que deben ser manejados, para ello la norma 27001 se apoya en una larga lista de controles y objetos de control que pertenecen a la norma 27002 con la finalidad de eliminar o tratar los riesgos. (Robalino, 2018)

3.11.1 Estructura de la norma

La norma ISO/IEC 27002:2013 tiene una estructura que difiere en varios aspectos si se la compara con su antigua versión, esta cuanta con 14 dominios, 114 controles y 130 requisitos de gestión, en donde cada dominio puede tener uno o varios controles.

3.11.1.1 Introducción

La norma ISO/IEC 27002 fue desarrollada con el fin de ayudar a las empresas con una serie de referencias para elegir correctamente los controles que van a ser instalados durante el proceso de implementación del SGSI. Se elaboro una norma dedicada para este aspecto debido a la importancia de la selección de controles, estos deben basarse en los requerimientos de seguridad presentados por cada organización. Las tres principales bases para la selección de controles son:

- Por medio de la valoración previamente realizada de los riesgos que usualmente amenazan la empresa.

- Utilizando regulaciones especificadas por otra organización, funciona como una especie de estándar a la cual regirse.

- Por los requerimientos y necesidades de cada negocio como objetivos propuestos, principios, etc.

Los controles también pueden ser diseñados de forma personalizada para que se ajusten a las necesidades específicas de una determinada empresa. (Columba, 2017)

3.11.1.2 Ámbito

Se encarga de ayudar a las empresas en la selección de controles adecuados para implementarse en conjunto con el SGSI. De igual forma se encuentra diseñado para llevar a cabo implementaciones de controles aceptados y brinda apoyo en la elaboración de controles propios, ajustados a necesidades seleccionadas y utilizando para ello guías de administración enfocadas a la seguridad de la información.

3.11.1.3 Referencias Normativas

Esta norma pertenece a la familia ISO/IEC 27000 la cual viene a ser un conjunto de buenas prácticas que sirven para lograr establecer e implementar para posteriormente mantener y mejorar los SGSI.

3.11.1.4 Términos y definiciones

Se procede a realizar una referencia de la norma ISO/IEC 27000 por ser quien contiene la versión completa sobre términos y definiciones, esa información será utilizada para propósitos especificados en el documento, dependerá de cada caso.

3.11.1.5 Políticas de la seguridad de la información

Esta sección tiene como objetivo crear un documento enfocado en la política de la seguridad de la información, dicho documento será de utilidad para la empresa pues permite crear una estructura basada en conceptos para mantener un buen nivel de seguridad y de igual forma se busca generar un mayor compromiso e interés de las personas ubicadas en los altos cargos de la empresa con las medidas de seguridad de la información presentes en la red. (Pandini, s.f.)

3.11.1.6 Organización de la seguridad de la información

Al buscar implementar diferentes mecanismos de seguridad de la información en una organización es clave trabajar con una estructura la cual sea capaz de sostener y gestionar a la idea para que esta vaya creciendo y adquiriendo fuerza. Esto se logra a través de la coordinación con los representantes de la empresa. (Pandini, s.f.)

3.11.1.7 Seguridad de los recursos humanos

En esta sección se analiza las contrataciones de empleados e incluso los tratos o negocios realizados con proveedores, se debe tener precaución pues tendrán acceso a la empresa, adicionalmente, se debe poner mayor énfasis en aquellas contrataciones que van a tener acceso a información confidencial para prevenir

posibles fraudes, robos mal uso de los recursos de la empresa, etc. Esta sección busca también que los proveedores y empleados:

- Sean consientes de la responsabilidad que asumen y respondan de forma eficiente en su rol designado.

- Comprendan las responsabilidades adquiridas con la seguridad de la información manejada por la empresa.

- En procesos de terminación de contrato o cambio de proveedor, protejan los intereses de la organización. (Columba, 2017)

3.11.1.8 Gestión de activos

Un activo es todo aquello con un valor para la empresa y por tanto viene a ser un elemento que necesita ser protegido de terceros. Para ello dichos activos deben ser previamente identificados, clasificados dependiendo de su naturaleza, organizados y protegidos. Los objetivos de esta sección son los siguientes:

- Identificar los activos y posteriormente darles la protección pertinente.

- Garantizar un constante nivel de protección adecuado tomando en cuenta el grado de importancia de la información siendo resguardada. (Columba, 2017)

3.11.1.9 Control de acceso

Se debe controlar el acceso a todo tipo de información o recurso de la empresa por parte de personas no autorizadas. Esta sección tiene como objetivos los siguientes puntos:

- Se encarga de controlar el acceso a los datos y a las instalaciones de la empresa en donde se encuentra siendo procesada o almacenada la información.

- Garantizar el acceso a la información y a los servicios prestados a todas aquellas personas con la autorización necesaria.

Evitar todo tipo de acceso no autorizado a servicio, información, aplicación, etc. (Columba, 2017)

3.11.1.10 Criptografía

Su objetivo principal es asegurar un uso eficaz y apropiado del cifrado para de esa forma proteger los principios fundamentales de la seguridad de la información (Confidencialidad, Autenticidad e Integridad). (Ramírez & Moreira, 2017)

3.11.1.11 Seguridad física del entorno

Esta sección nos habla sobre la prevención que se debe tener con el lugar en donde se van a ubicar las instalaciones o los equipos de red. Se debe analizar todo el entorno, desde posibles amenazas físicas como robos, huelgas, desorden social hasta considerar posibles amenazas ambientales como huracanes, deslaves, temblores, etc. Todos esos factores se deben tomar en cuenta para encontrar una ubicación ideal en donde todo el negocio se encuentre lo más seguro posible. (Columba, 2017)

3.11.1.12 Seguridad de las operaciones

En esta área es muy importante que se encuentren correctamente definidos tanto las responsabilidades por sus gestiones y operaciones como los procedimientos seguidos por la empresa, su correcta asignación permite cumplir con los objetivos de esta sección los cuales son:

- Mantener seguras a todas las operaciones dedicadas a procesar información.

- Proteger a las operaciones de procesamiento de información y a toda la información en si de una posible irrupción protagonizada por malware u otro ataque.

- Trabajar con mecanismos para la prevención de perdida de datos y registro de eventos.

- Garantizar la integridad a nivel físico y virtual de los sistemas operacionales.

- Evitar que se exploten posibles vulnerabilidades adscritas a errores técnicos.

- Reducir el impacto causado por ejecutar procesos de auditoria en los S.O. (Columba, 2017)

3.11.1.13 Seguridad de las comunicaciones

Esta sección tiene como objetivos los siguientes puntos:

- Garantizar tanto la protección de los estudios en donde se encuentran procesando toda la información de soporte como la protección de la información colgada en la red.

- Manejar herramientas para conservar la seguridad al momento de transferir la información a cualquier tipo de entidad sea esta externa o interna. (Columba, 2017)

3.11.1.14 Adquisición, desarrollo y mantenimiento de sistemas

Esta sección tiene como objetivos los siguientes puntos:

- Garantizar que la seguridad de la información va a tener un espacio adecuado en los sistemas de información en todas las fases del ciclo de vida.

- Garantizar que la seguridad de la información se encuentre siempre implementada y sea un punto clave en el ciclo de vida de los sistemas de información

- Garantizar la seguridad de todos los datos que han sido de una u otra forma utilizados para realizar pruebas. (Columba, 2017)

3.11.1.15 Relación con los proveedores

Esta sección tiene como objetivos los siguientes puntos:

- Garantizar la seguridad de todos los activos informáticos de la empresa de modo que los proveedores puedan acceder a ellos.

- Lograr cumplir con los acuerdos previamente realizados con los proveedores en cuanto al nivel de seguridad de la información y a los servicios prestados en línea. (Columba, 2017)

3.11.1.16 Gestión de incidentes de seguridad de la información

Se deben establecer procedimientos de carácter formal para establecer registros y crear un escalonamiento para la información. Todas las personas relacionadas con la empresa deben tener bien incrustada esa idea para agilizar las notificaciones de los eventos y dar una rápida respuesta frente a amenazas. (Pandini, s.f.)

3.11.1.17 Continuidad del negocio

En esta sección se deben tomar en cuenta los planes trazados con respecto a la continuidad del negocio, deben ser puestos en marcha e implementados, esto se realiza con la finalidad de prevenir una posible interrupción en el giro del negocio de la empresa para evitar parar con las actividades normales y en caso de suceder asegurar de cualquier forma que los procesos marcados como críticos logren ser recuperados en el menor tiempo posible. (Pandini, s.f.)

3.11.1.18 Cumplimiento

Esta sección tiene como objetivos los siguientes puntos:

- Evitar todos los escenarios posibles en el cual se incumpla con cualquier tipo de obligación contraída legalmente sea esta estatuaria, contractual o de reglamentación, con el fin de no recibir sanciones administrativas que puedan incurrir a una responsabilidad penal.

- Busca garantizar que la seguridad de la información haya sido implementada y se encuentre operando según los procedimientos estipulados por la empresa y en conformidad con las políticas establecidas. (Columba, 2017)

3.12 Comparación entre los estándares ISO/IEC 27002:2005 e ISO/IEC 27002:2013

Cuando una versión aparece quiere decir que la anterior ya no cumplía con las expectativas o por lo menos le costaba alcanzar un rendimiento óptimo, eso paso entre estas dos normas, la versión del 2005 necesitaba cambios que permitan explotar las capacidades de los cada vez más potentes sistemas SGSI, por ello, en 2013 se presentó a la norma ISO/IEC 27002:2013 la cual tiene la misma base de su antigua versión pero a la vez posee ciertos cambios que responden de forma eficaz a las nuevas necesidades. En la tabla 11 se pueden observar los cambios generales entre los estándares ISO/IEC 27002:2005 e ISO/IEC 27002:2013.

Tabla 11.
Cuadro comparativo de reorganización estructural de la norma 27002.

Descripción	**ISO/IEC 27002: 2005**	**ISO/IEC 27002: 2013**	**Cambios**
Controles	133	114	94 se mantienen 20 nuevos 39 eliminados
Dominios	11	14	3 nuevos
Requisitos de gestión	102	130	18 nuevos

Algunos de los cambios más importantes en esta actualización que dio paso a una nueva versión son los siguientes:

- La estructura es diferente, la versión del 2005 presenta 11 dominios y otro lado la nueva versión maneja 14 dominios.

- La nueva versión es más comprimida, a pesar de tener más secciones es más corto y está mejor centrado en comparación con su anterior versión.

- La nueva versión trajo consigo cambios en la terminología de algunas palabras de su diccionario.

3.13 Controles excluidos en la versión del año 2013

Como la versión del año 2005 ya no era capaz de lograr el máximo rendimiento y en ciertos casos sus soluciones se quedaban cortas o muy limitadas al momento de resolver problemas, en 2013 se lanzó una nueva versión con modificaciones en todos los niveles de su estructura, varios de esos cambios se encontraban orientados en los controles manejados por la versión anterior ya que estos eran obsoletos y necesitaban ser excluidos de la nueva versión.

En la tabla 12 se pueden observarlos los controles excluidos de la versión lanzada en 2013

Tabla 12.
Controles excluidos de la versión 2013.

Control	**Descripción**	**Se cambia por**	**Controles ISO 27001:2005 que se incluyen**
A.6.1.1	Comité de Gestión para la seguridad de la Información	Roles de la seguridad de la información y sus responsabilidades	A.6.1.3 y A.8.1.1
A.6.1.2	Coordinación de seguridad de la información	Contacto con autoridades	A.6.1.6

A.6.1.4	Procesos de autorización para instalaciones para procesamiento de información	Seguridad de la información en la gestión de proyectos	
A.6.2.1	Identificación de riesgos relacionados con agentes externos	Política de dispositivo móvil	A.11.7.1
A.6.2.2	Direccionamiento de seguridad al tratar con clientes	Trabajo a distancia	A.11.7.2
A.10.2.1	Entrega del servicio		
A.10.7.4	Seguridad del sistema de documentos		
A.10.8.5	Sistema de información de negocios		
A.10.10.2	Seguimiento al uso de sistema		
A.10.10.5	Falla en el registro		
A.11.4.2	Autenticación de usuarios para conexiones externas		
A.11.4.3	Identificación de equipos		
A.11.4.4	Puerto remoto de diagnóstico y configuración de protección		
A.11.4.6	Control para la conexión de redes		
A.11.6.2	Aislamiento del sistema sensible		
A.12.2.1	Validación de datos de entrada		
A.12.2.2	Control de procesamiento interno		
A.12.2.3	Integridad de mensaje		
A.12.2.4	Validación de datos de salida		
A.12.5.4	Filtración de información		
A.15.1.5	Prevención del uso indebido de las instalaciones para el procesamiento de información		
A.15.3.2	Protección de las herramientas de auditoria de sistemas de información		

Tomado de (Columba, 2017)

3.14 Nuevos controles en la versión del año 2013

Como la versión del 2005 tenía controles que ya no cumplían con su función o simplemente quedaron obsoletos debido a los altos niveles de exigencias. La versión del año 2013 daba respuesta a la problemática excluyendo a aquellos controles defectuosos y añadiendo en su lugar otros con mejores soluciones y con una mejor eficiencia frente a amenazas.

En la tabla 13 se pueden observarlos los controles agregados de la versión lanzada en 2013

Tabla 13.
Controles incorporados en la versión 2013.

Control	**Descripción**	**Controles que se absorbe de la ISO 27001:2005**
A.6.1.4	Seguridad de la información en la gestión de proyectos	
A.12.6.2	Restricciones en la instalación de software	
A.14.2.1	Política de desarrollo de seguridad	
A.14.2.5	Desarrollo de procedimientos para el sistema	
A.14.2.6	Desarrollo de un entorno seguro	
A.14.2.8	Sistema de prueba de seguridad	
A.15.1.1	Información de seguridad para las relaciones de proveedores	A.6.2.3
A.15.1.3	Cadena de suministro tecnología de información y comunicación	

A.16.1.4	Evaluación y decisión de los eventos de seguridad de la información	
A.16.1.5	Respuestas incidentes de la seguridad de la información	
A.17.1.2	Implementación de la continuidad de la seguridad de la información	
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	

Tomado de (Columba, 2017)

3.15 Comparación de los dominios

A nivel de los dominios, en las versiones 2005 y 2013 existieron varios cambios, se añadieron tres nuevos en la última versión y se realizaron varias modificaciones en los otros. Esto se debe al progreso de la tecnología, la versión antigua se encontraba enfocada en resolver las amenazas de aquella época y como progresivamente aparecían nuevas formas de ataque, creció la necesidad de realizar modificaciones para mantener un control más estricto y personalizado sobre las amenazas.

En la tabla 14 se puede observar los dominios de la norma ISO/IEC 27002:2005 e ISO/IEC 27002:2013.

Tabla 14.
Cuadro comparativo de los dominios de 2005 y 2013.

Objetivos de control ISO/IEC 27002:2005	**Objetivos de control ISO/IEC 27002:2013**
A.5 Política de seguridad	**A.5** Política de seguridad
A.6 Organización de la seguridad de la información	**A.6** Organización de la información

A.7 Gestión de activos	**A.7** Seguridad en recursos humanos
A.8 Seguridad de los recursos humanos	**A.8** Gestión de activos
A.9 Seguridad física y del entorno	**A.9** Control de acceso
A.10 Gestión de comunicaciones y operaciones	**A.10** Criptografía
A.11 Control de acceso	**A.11** Seguridad física y ambiental
A.12 Adquisición, desarrollo y mantenimiento de sistemas de información	**A.12** Seguridad en las operaciones
A.13 Gestión de los incidentes de la seguridad de la información	**A.13** Transferencia de información
A.14 Gestión de la continuidad del negocio	**A.14** Adquisición de sistemas, desarrollo y mantenimiento
A.15 Cumplimiento	**A.15** Relación con proveedores
	A.16 Gestión de los incidentes de seguridad
	A.17 Continuidad del negocio
	A.18 Cumplimiento con requerimientos legales y contractuales

Tomado de (Villacis, 2016)

3.16 Normas ISO y su relación con SIEM

Como se había dicho, SIEM es una herramienta desarrollada para implementar controles de seguridad en todo tipo de redes. Para su implementación se han estudiado varios tipos de soluciones diseñadas para organizaciones de todo tamaño, desde conglomerados hasta empresas pequeñas. Por otro lado, las normas ISO son un conjunto de estándares elaborados para la gestión de diferentes sectores entre los cuales se encuentra el de la seguridad de la información por medio de las normas de la familia 27000.

Entendiendo que, ambas definiciones se encuentran relacionadas de forma directa con la seguridad de la información, se puede comenzar a entender su relación, las herramientas SIEM son los mecanismos encargados de plasmar, de ejecutar o de llevar a cabo las acciones que han sido antes planificadas y colocadas dentro de protocolos o controles por las normas ISO.

De ese trabajo en conjunto es el tema a tratar en este punto, de dar a entender la relación que los dominios y controles del Anexo A tienen con la forma de funcionar y de actuar del SIEM.

3.16.1 Normas ISO 27001:13 y SIEM

Uno de los componentes de esta norma es el Anexo A, dicho documento le ha permitido tomar una participación en el manejo de los controles encargados de gestionar la seguridad de la información que, al concordar con todos los requerimientos de gestión presentados por la empresa, encuentra el nivel de seguridad deseado, permitiendo garantizar la sostenibilidad de los procesos del negocio y la practica normal de su funcionamiento. Esto se logra realizando un análisis correcto de los controles detallados por esta norma y aplicándolos en la herramienta SIEM. En la tabla 15 se puede observar la influencia de los controles expuestos por la norma 27001:13 en las acciones de los SIEM.

Tabla 15.
ISO/IEC 27001:13 y SIEM

Dominio	Control	Descripción	Relación con SIEM
		Todas las actividades realizadas por el usuario deben mantenerse y ser	En cuanto a su afinidad con SIEM, se relacionan en cuanto

A.12 Seguridad en las operaciones	A.12.4.1 Registro y gestión de eventos	revisadas de forma adecuada cada cierto tiempo, estas actividades sujetas a revisión son: los fallos, las excepciones y cualquier evento relacionado con la seguridad de la información.	a la política encargada de recoger los registros de aquellos eventos relacionados con la seguridad.
	A.12.4.2. Protección de los registros de información	Los activos de la empresa deben encontrarse protegidos de posibles accesos no autorizados y de otras amenazas que presenten una vulnerabilidad a su integridad.	Toda la información debe encontrarse centralizada en un sector con máximas prestaciones de seguridad
	A.12.4.3. Registro de actividad del administrador y operador del sistema	Todas las actividades realizadas por el administrador y operador del sistema deben mantenerse y ser revisadas de forma periódica.	Se encuentra relacionado con la política encargada de recoger los registros de aquellos eventos relacionados con la seguridad.
13. Seguridad en las Telecomunicaciones	A.13.1.2 Mecanismos de seguridad asociados a servicios en red	Las características que correspondan a niveles de servicio, requisitos hábiles para gestión de los servicios prestados en red y los protocolos de seguridad deben ser identificados e inmediatamente incluidos dentro de los acuerdos de red.	Esta herramienta asegura la protección de toda la información, gestionando para ello sus protocolos de seguridad.

	A.13.1.3 Segregación de redes	Todos aquellos grupos de servicios existentes van a ser segregados en redes.	Se encuentra relacionado con la política que analiza la arquitectura de red donde se realizara la implementación de la herramienta.
	A.13.2.2 Acuerdos de intercambio	Todo acuerdo al cual se llegue con la parte externa debe darse por medio de transferencias comerciales de información segura.	Se relaciona en cuanto a la política relacionada a la conectividad de personas ajenas a la empresa.

Tomado de (Robalino, 2018)

3.16.2 Normas ISO 27002:13 y SIEM

La principal característica de esta norma es su contenido, profundiza en la información relacionada con los controles y orienta o logra dar algún tipo de idea sobre cuales se deben tomar en consideración para ser implementados por parte de la empresa consultora en cuestión. Por tener esa información, esta norma tiene un gran peso sobre las SIEM, pues sus consideraciones son tomadas como un conjunto de buenas prácticas establecidas por experiencias de personas en la utilización de ese producto, de igual forma, se complementa con la norma 27001 con la cual comparte el Anexo A.

Tabla 16.
ISO/IEC 27002:13 y SIEM

Dominio	Control	Descripción	Relación con SIEM
13. Seguridad en las Telecomunicaciones	13.1.1 Controles de red	Se gestionarán y controlarán las redes. Eso busca ofrecer la máxima seguridad posible a la información	El SIEM realiza la recolección de datos de los eventos de seguridad para mediante análisis utilizarlos como

		presente en aplicaciones y sistemas	herramientas que ofrezcan mejores rasgos de protección.
16. Gestión de los incidentes de seguridad	16.1.1 Responsabilidades y procedimientos	Se asignan responsabilidades y se establecen procedimientos con el fin de ofrecer respuestas frente amenazas más eficientes y con mayor velocidad.	Todos estos puntos son un proceso realizado por el SIEM. En primera instancia se colocan responsabilidades y se establecen los procedimientos adecuados. Utilizando esos mecanismos la herramienta adquiere visibilidad de posibles amenazas. Al momento de encontrar una vulnerabilidad genera alertas y por medio de notificaciones las envía a quien corresponda para que ejecute las medidas correspondientes. Este evento genera nuevos datos, de los cuales el SIEM se alimenta y aprende, fortaleciendo así el manejo de incidentes.
	16.1.2. Notificación de los eventos de seguridad de la información	Se encarga de notificar eventos sospechosos lo más pronto posible al administrador de red o persona encargada de la seguridad informática.	
	16.1.5. Respuesta a Incidentes de seguridad	Tomando como base los procedimientos establecidos y documentados, se da respuesta a los incidentes de seguridad.	
	16.1.6. Aprendizaje de los incidentes de seguridad de la información	Se utilizarán todos los incidentes experimentados con el fin de aprender sobre ellos para reducir el nivel de amenaza e impacto de futuros eventos similares.	

	16.1.7. Recopilación de evidencia	Se definirán y aplicarán procesos que permitan la recolección y almacenamiento de toda la información sujeta a evidencia.	La información recolectada y almacenada será utilizada en los procesos forenses que correspondan dependiendo del caso.

Tomado de (Robalino, 2018)

3.16.3 Norma ISO/IEC 27001:13 y el ciclo PDCA.

La norma ISO/IEC 27001:13 establece varios parámetros para implementar correctamente y mantener un eficaz rendimiento de un SGSI. Entre las ventajas que aporta se encuentra la documentación necesaria para, en caso de cumplir con todos los requerimientos dictados en ella, obtener el derecho a certificarse, con ese detalle promueve la imagen de la empresa y afirma contar con medidas de seguridad de la información avaladas a nivel internacional.

Sin embargo, dichas directrices solo vienen a realizar una breve sugerencia sobre el enfoque a cumplir para obtener la certificación, no da ningún tipo de solución, proceso, flujo de trabajo o metodología a la cual adherirse para lograr ese objetivo, por ello, la solución a la cual se llegó fue realizar un mapeo en el cual consten todas las etapas del ciclo PDCA junto a los puntos a cumplir por la norma en cada uno de sus ciclos. En la tabla 17 se puede observar el mapeo realizado de la norma 27001:2013 sobre el ciclo PDCA.

Tabla 17.
ISO/IEC 27001 y el ciclo PDCA

Ciclo PDCA	**Procesos**
	Determinar el alcance y los limites
	Determinar la política a usarse en el SGSI

Planificar	
	Determinar el enfoque a usarse para la evaluación de riesgos
	Identificar los posibles riesgos sobre los activos
	Realizar el análisis y la evaluación de los riesgos, el impacto que estos causarían sobre el negocio.
	Valorar alternativas para el tratamiento de riesgos.
	Realizar la elección de los controles para el tratamiento de riesgos.
	Conseguir la aprobación para realizar la implementación del SGSI
	Elaborar la declaración de aplicabilidad.
Hacer	Realizar la implementación del plan de tratamiento de riesgos
	Realizar la implementación de los controles que hayan sido seleccionados
	Gestionar el desarrollo de curso de capacitación orientados a la seguridad de la información
	Gestionar las operaciones del sistema de gestión de la seguridad de la información.
	Gestionar los recursos que hayan sido asignados al SGSI.
	Realizar la implementación de controles para una rápida detección de amenazas.
Verificar	Llevar a cabo los procesos de revisión y monitoreo del SGSI
	Mantener controles periódicos sobre el SGSI
	Medir el grado de efectividad conseguido por los controles para determinar si cumplieron su rol dentro del sistema.
	Controlar constantemente el estado de la evaluación de riesgos.
	Llevar a cabo controles internos.
	Actualizar constantemente los protocolos de seguridad
	Almacenar la información de todos los eventos de seguridad ocurridos, pueden existir acciones con repercusiones en la eficiencia del SGSI.
	Realizar la implementación de las mejores que necesita el SGSI
	Realizar la implementación de todas las medidas preventivas y correctivas necesarias para corregir posibles puntos débiles.

Actuar	
	Notificar los cambios y mejoras realizadas del SGSI a todas las partes interesadas
	Confirmar que los cambios realizados se encuentren cumpliendo con sus objetivos.

Tomado de (Solarte, Enríquez, Benavides, 2015)

3.17 Estudios realizados referente a la implementación de las normas en SIEM

Actualmente se puede encontrar información de cómo realizar ataques, encontrar las vulnerabilidades de una red, manejar virus, hackear y muchas otras cuestiones que afectan el buen desarrollo de las empresas Pymes en cualquier sitio en internet, de modo que están en constante peligro.

Por todos esos problemas aparecieron los SIEM, herramientas de gestión de eventos de seguridad informática cuya función principal es la protección de la red empresarial de posibles intrusos, sin embargo, como los ataques han ido progresivamente empeorando se vieron en la necesidad de contar con normas que regularicen el uso de estas herramientas. Con estas normas lo que se busca es estandarizar los protocolos de seguridad, les da a las empresas una herramienta para realizar mejores decisiones en la elección de controles y lo guía en el camino de una buena implementación y mantenimiento de un SGSI.

Este trabajo en conjunto entre las normas ISO y las SIEM dieron lugar a varios estudios, análisis e implementaciones que causaron criticas positivas y recomendaciones de uso. Algunas investigaciones y resultados obtenidos por medio de su implementación son los siguientes:

- **Ecuatronix**: Al realizarse en esta compañía la propuesta de diseño de un SGSI basándose en la norma 27001:2013, se encontraron valores

de riesgos en un rango de 12 a 80 lo cual permitió a la empresa tratar el riesgo utilizando para ello dos modalidades, aceptar el riesgo para las amenazas con un bajo nivel y aplicar controles para todas las amenazas consideradas como riesgosas. (Villacis, 2016)

- **ISSFA:** En el área de procesos de los seguros previsionales del ISSFA la evaluación de la seguridad basada en la norma ISO 27001 dio lugar a conocer varias vulnerabilidades como, el personal no cuenta con talleres de capacitación sobre seguridad de la información, los datos se encuentran expuestos y usualmente son manipulados por personas sin la debida autorización y dicha área no es capaz de garantizar la continuidad de sus operaciones, fallando en el principio de disponibilidad. (Porras & Salazar, 2016)

- **Comando de la Armada Nacional de Colombia:** La implementación de un SIEM les permitió contar con un dashbord el cual presenta de forma gráfica todos los eventos que sucedan en la red para el subsiguiente proceso de análisis y toma de decisiones al momento de encontrar algún tipo de amenaza informática, adicionalmente se les fue entregado un manual de usuario. (Fernández, Herrera & García, 2017)

- **Agencia Nacional de la Superación de la Pobreza Extrema ANSPE:** se desarrolló una guía para implementar de forma correcta un sistema SIEM utilizando para ello la norma 27000. Con ello se espera conseguir que en una futura implementación guiada por el procedimiento expuesto en ese trabajo sea capaz de administrar de manera correcta los logs, aumentar el nivel de protección frente a amenazas informáticas y sobre todo lograr una implementación exitosa de cualquier solución SIEM. (Peña, 2015)

- **Cooperativa de ahorro y crédito Chibuleo LTDA.:** en esta institución se realizó el diseño de una política de seguridad la cual se encontraba basada en la norma ISO/IEC27002:2013, los resultados obtenidos de esa investigación permitieron identificar los incidentes de seguridad y

clasificarlos para posteriormente desarrollar una matriz de riesgo la cual dio paso a diferentes entregables como, eventos de riesgo, las amenazas frecuentes y vulnerabilidades del sistema. (Pilla, 2019)

Al final de dicho análisis y por medio del apoyo del jefe de tecnología de esa institución, el resultado de esa investigación fue una política de seguridad con controles capaces de responder a las necesidades de la cooperativa y alineados a sus requisitos de seguridad. (Pilla, 2019)

- **Ministerio del Interior:** se elaboró una política dirigida para el sistema encargado de sus botones de seguridad, utilizando como base para su diseño a la norma ISO/IEC 27002:2013. El problema por resolver era el resultado visto en su matriz de riesgos, ahí se evidenciaban vulnerabilidades sobre los activos y la presencia de varias amenazas. (Contero, 2019)

  La respuesta a esa problemática fue la política propuesta, al finalizarse esta se encontraba compuesta por 25 controles cuidadosamente seleccionados que buscaban reducir el impacto que pueda causar la materialización de las amenazas. Hoy en día dicha política se encuentra siendo utilizada dentro de todos los procesos que se encargan del manejo de los servicios ofrecidos por la plataforma tecnológica. (Contero, 2019)

En el siguiente capítulo se realizará la implementación de la propuesta desarrollada de un SIEM en PYMES.

4 CAPITULO IV. IMPLEMENTACIÓN Y SIMULACIÓN DEL GESTOR DE EVENTOS OSSIM

En este capítulo se tomarán en cuenta los resultados obtenidos del análisis previo para presentar la propuesta de un modelo para la implementación de una herramienta SIEM en la infraestructura de red de empresas PYMES.

4.1 Análisis de riesgos

La preocupación de las empresas por gestionar de mejor forma la seguridad de la información cada día resulta más evidente ya que se encuentran envueltos en un escenario en el cual la sociedad es cada vez más dependiente de los sistemas de información y la competencia cada vez es más agresiva al tratar de ofrecer mejores servicios.

Como varias empresas trabajan con procesos guiados y protocolos ya establecidos, mantener un escenario libre de riesgos es crucial ya que en caso de materializarse un riesgo la continuidad del servicio puede verse afectada, con ello, se resalta la necesidad de realizar con anterioridad un buen análisis de los posibles riesgos a los que se expone la empresa ya que dicho análisis será parte fundamental al crear protocolos y metodologías más asertivas, con mayor porcentaje de éxito. En la figura 19 se puede observar los elementos que toman lugar para determinar los riesgos presentes en el sistema.

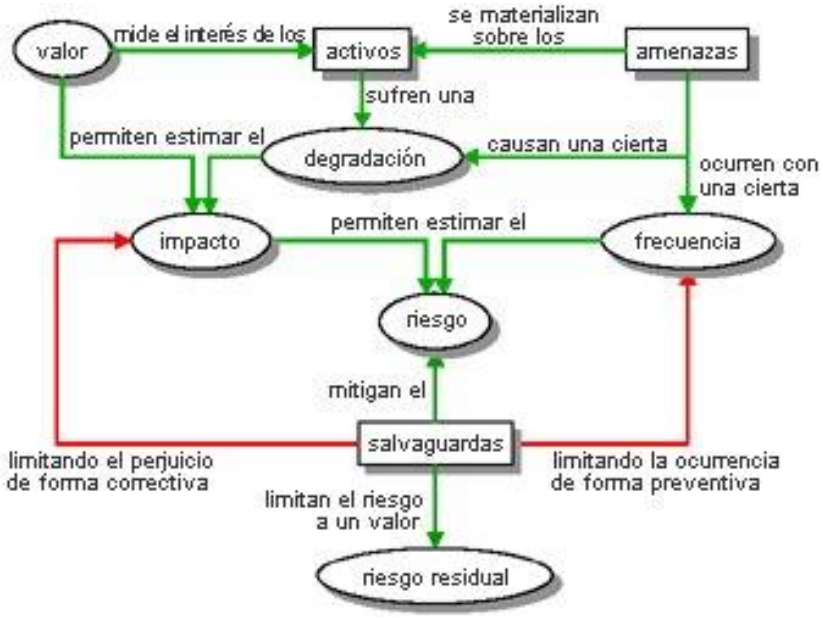

Figura 19. Ciclo del análisis de riegos.

Tomado de (Morales, 2018)

4.1.1 Definir el alcance

Al realizarse el análisis de un riesgo, la primera fase a considerar es el definir el alcance del estudio que se va a realizar, este puede verse limitado a una determinada área, así como puede encontrarse dirigido a la totalidad de la empresa. Se recalca que mientras más espacio abarque el estudio menos se va a poder profundizar pues dependiendo del tiempo y recursos asignados pueden omitirse aspectos considerados poco relevantes.

4.1.2 Identificar los activos

Entendiendo como activos a todos aquellos elementos que aportan un valor económico a la empresa, es importante comprender que todo este análisis gira entorno a estos pues lo que se busca es mantenerlos seguros. En caso de realizarse un análisis de riesgo enfocado a un departamento, únicamente se tomará en cuenta los activos disponibles en dicha área.

4.1.3 Identificar amenazas

Es un paso fundamental tomando en cuenta que cuando una amenaza llega a materializarse es capaz de causar daños y volver completamente inutilizable a los equipos o a la información almacenada, provocando perdidas y una mala imagen de la empresa. Estas amenazas pueden tener diferente origen, pueden ser causados por la naturaleza, causados por la mano humana, punto a investigar pues puede ser voluntaria o involuntariamente además de que la persona en cuestión puede pertenecer o no a la institución.

4.1.4 Identificar vulnerabilidades y salvaguardias

En este punto se debe analizar las características que presenta el sistema de la empresa, investigar su estado, para que actividades fueron desarrolladas, si se les da un buen uso a los equipos que se utilizan, controlar que el personal cuente con los conocimientos de los protocolos a seguir y con el cuidado que deben tener al dar información de los controles de acceso. Hay que considerar estos puntos débiles pues en el futuro pueden ser la cusa de vulnerabilidades.

En la parte de salvaguardias hay que analizar los controles que han sido establecidos para evitar ataques y controlar amenazas. Se recomienda verificar que dichos controles se mantengan operativos y funcionen correctamente.

4.1.5 Evaluar el riesgo

Para evaluar el riesgo que presenta una amenaza hay que tomar en cuenta varios detalles, uno de ellos son los objetivos y a que se dedica la empresa, la opinión de las partes interesadas, la reacción que puede tener sobre los usuarios, los activos que se encuentran involucrados, similares incidentes sucedidos con anterioridad, el grado de crecimiento que se puede presentar y

muchos otros factores que pueden variar dependiendo del caso. (Sotelo, Torres & Rivera, 2012)

La evaluación de riesgos a su vez tiene una matriz para reconocer el nivel en el cual se encuentra un riesgo, esta matriz tiene dos aristas, una de ellas es el nivel de probabilidad y la otra el nivel de impacto, el cálculo del riesgo se lo obtiene de la multiplicación entre los valores de esos dos puntos. En los niveles bajos las amenazas son consideradas comunes y se pueden despreciar, los niveles medios indican que se debe tomar acción sobre las amenazas pues son considerados potenciales ataques y en los niveles altos y muy altos se deben tomar acciones inmediatamente pues afectan directamente al sistema.

En la tabla 18 se puede observar el cuadro de la probabilidad que siguen los riesgos, mientras más frecuente sea, su grado y valor tienden a aumentar.

Tabla 18.
Valoración de la probabilidad.

Probabilidad		
Valor	**Grado**	**Descripción**
1	Raro	Puede ocurrir una vez cada 2 años
2	Muy baja	Al año
3	Baja	En 6 meses
4	Media	Al mes
5	Alta	A la semana

Tomado de (Sotelo, Torres & Rivera, 2012)

En la tabla 19 se puede observar el cuadro del impacto que causa un riesgo, mientras peores consecuencias presente, su nivel y valor tienden a aumentar.

Tabla 19.
Valoración del impacto.

Impacto		
Valor	**Nivel**	**Descripción**
1	Insignificante	Impacta levemente en la operatividad del proceso
2	Menor	Impacta en la operatividad del proceso
3	Moderado	Impacta en la operatividad del macroproceso
5	Mayor	Impacta en la operatividad de los procesos
8	Desastroso	Impacta fuertemente en la operatividad de los procesos

Tomado de (Sotelo, Torres & Rivera, 2012)

En la tabla 20 se puede observar la matriz para determinar el nivel de riesgo, como se ve, utiliza tanto el impacto como la probabilidad de los que se habló anteriormente.

Tabla 20.
Mapa de riesgos.

		PROBABILIDADES				
		Raro	**Poco probable**	**Posible**	**Muy probable**	**Casi seguro**
CONSECUENCIAS	**Despreciable**	Bajo	Bajo	Bajo	Medio	Medio
	Menores	Bajo	Bajo	Medio	Medio	Medio
	Moderadas	Medio	Medio	Medio	Alto	Alto
	Mayores	Medio	Medio	Alto	Alto	Muy alto
	Catastróficas	Medio	Alto	Alto	Muy alto	Muy alto

Tomado de (Sotelo, Torres & Rivera, 2012)

4.1.6 Tratar el riesgo

En esta fase se toma en consideración la evaluación realizada anteriormente, se toman aquellos riesgos que sean o puedan ser una potencial amenaza para el normal funcionamiento del sistema y son tratados dependiendo de cual estrategia pueda tener un mejor resultado. Las estrategias por considerar para el tratamiento de riesgos son:

- **Transferencia:** se busca tratar el problema transfiriéndolo del lugar en donde se encuentra a otro en el cual se encuentre aislado o que disponga de los recursos necesarios para eliminar el problema. Hay que considerar que al transferirlo se corre el riesgo de que este sea capaz de infectar otras áreas, extendiendo el problema y volviéndolo más crítico. (Sotelo, Torres & Rivera, 2012)

- **Reducción:** este método hace alusión a dos tipos de soluciones, o bien busca reducir el porcentaje de probabilidad de que ocurra un riesgo o bien busca reducir las consecuencias que este podría causar. En el primer caso intervienen protocolos de control sobre amenazas y demás análisis realizados sobre las vulnerabilidades más recurrentes. En el segundo caso intervienen los controles instaurados y demás infraestructura armada para el control sobre las vulnerabilidades. (Sotelo, Torres & Rivera, 2012)

- **Eliminar:** si en su evaluación un riesgo es considerado muy elevado o en caso de no contar con los recursos suficientes para poder mitigarlo, se puede tomar la decisión de eliminarlo, entendiendo en esta parte que junto con el riesgo se eliminarían las actividades o procesos del sistema que hayan sido infectados. (Sotelo, Torres & Rivera, 2012)

- **Asumir:** siguiendo la tabla 12, cuando un riesgo se encuentra dentro del rango de aceptación bajo el criterio de la empresa, estos pueden ser considerados comunes y se los puede asumir sin necesidad de poner mayor énfasis en mitigarlos. (Sotelo, Torres & Rivera, 2012)

4.2 Niveles de aceptación o tolerancia al riesgo

Toda persona o empresa maneja su propio criterio en cuanto a los niveles de aceptación o tolerancia que tiene sobre los riesgos. Manejando sus propios criterios se recomienda trabajar en planes de tratamiento de riesgos que se ajusten a sus necesidades y que lleven a aquellos ataques que sobrepasan dicho rango hasta un punto en el cual sean aceptables.

En la tabla 21 se puede observar los niveles de aceptación o tolerancia que se recomienda tomar en cuenta. Dicha figura toma como base los resultados obtenidos del análisis de riesgo y recomienda lo siguiente:

- Los riesgos con niveles de extremo e intolerable deben ser tratados hasta llegar al nivel de tolerable.
- Los activos críticos que se encuentren en el nivel de tolerable deben ser tratados hasta llegar al nivel de aceptable.

Tabla 21.
Valoración del nivel de aceptación/tolerancia.

Aceptación/Tolerancia		
Valor	**Nivel**	**Descripción**
1	Aceptable	Retenido
2	Tolerable	Para activos no críticos, intolerable para críticos
3	Intolerable	Atención inmediata y monitoreo permanente
4	Extremo	Tratado como intolerable, a nivel de Gerencia General

Tomado de (Sotelo, Torres & Rivera, 2012)

4.3 Control de riesgos

Una vez que se ha concluido con el análisis de riesgo, el siguiente paso es analizar las medidas de protección que ya han sido instauradas, esto con el fin de determinar si su funcionamiento sigue siendo eficaz y efectivo frente a las amenazas que se presenten, en caso de presentar defectos o un rendimiento por debajo del esperado se procede al ajuste de sus deficiencias.

Si el análisis de riesgo arroja un resultado negativo que no se ha contemplado dentro del plan operativo con el que cuenta la empresa, se deben establecer nuevos controles o medidas que se van a adoptar para estabilizar al sistema, tratar la amenaza y de ser posible añadir mejoras en la prestación de servicios. Siguiendo el ciclo que sigue el proceso PDCA el cual se basa en la mejora continua, el control de riesgos es la última fase del ciclo y los resultados que salgan serán utilizados como fuente de información para volver a comenzar el ciclo. (Sotelo, Torres & Rivera, 2012)

Los servicios que son considerados críticos para todas las empresas y por ende están sujetos a procesos de control para su protección son los siguientes:

- Integridad.
- Confidencialidad.
- Autenticación.
- No repudio.
- Control de acceso. (Sotelo, Torres & Rivera, 2012)

Con el fin de asegurar que los puntos anteriormente expuestos se encuentren libres de riesgos se debe dotar al sistema con los mecanismos considerados necesarios y oportunos.

4.4 Mecanismos de seguridad

Son herramientas de protección físicas o lógicas que se encuentran orientados al manejo de las vulnerabilidades y al trabajo sobre los riesgos del sistema, en su forma física se refiere al hardware, mientras más avanzado sea va a ofrecer mejores opciones de seguridad y mejores respuestas frente a amenazas, en su forma lógica se refiere al software que me permite establecer controles y protocolos a seguir en caso de amenaza. (Romero & Figueroa, 2018) El fin de esos mecanismos es el mismo, proteger los activos de la empresa asegurando que todos ellos, principalmente la información, mantenga su estructura original.

Se pueden encontrar varios mecanismos de seguridad informática que son capaces de brindar diferentes tipos de soluciones y que han sido desarrollados para diferentes propósitos, para su selección se recomienda llevar a cabo un análisis en el plano personal en el cual se debe considerar los riesgos que amenazan la empresa, el tipo de sistema con el que se trabaja y la función que dicho mecanismo desempañaría. Estos mecanismos de seguridad informática se dividen en diferentes grupos, los cuatro más utilizados son los mecanismos preventivos, detectores, correctores y disuasivos.

4.4.1 Mecanismos preventivos

Es el primer mecanismo de defensa contra una posible amenaza, se encarga de prevenir los ataques informáticos que puedan llegar a materializarse sirviéndose para ello de recursos como el monitoreo de los activos de la empresa, las personas que han ingresado al sistema y el registro de las actividades realizadas por parte del personal.

Al tratarse de la primera puerta contra ataques, es el mecanismo que más se toma en consideración por parte de las empresas pues su implementación no requiere de una mayor inyección de capital. Un mecanismo preventivo puede ir

desde la seguridad física como la instalación de una red de cámaras, la puerta de ingreso a la compañía, contratar personal de seguridad hasta contar con equipos más avanzados que realicen monitoreo en tiempo real, cifrado de datos, etc. (Moreno, 2018)

Los mecanismos preventivos más utilizados a nivel mundial por personas naturales y jurídicas son los siguientes:

- **Antivirus:** es un programa informático que se encarga de analizar el sistema en el cual fue instalado, se encarga de detectar posibles códigos maliciosos que se encuentren presentes en los equipos o que intenten forzar su acceso, una vez identificados se trata al problema eliminándolo o impidiendo su acceso al sistema. Dependiendo del tipo de antivirus del que se hable puede tener diferentes tipos de funciones, puede servir como un programa de defensa pro-activa, anti-spam o anti-hacker. (Moreno, 2018)

- **Firewall:** se encarga de protegernos de posibles amenazas mediante el filtrado de tráfico, examina todos los intercambios que realiza un equipo con otro, analiza cada paquete que entra y sale de la red buscando aquellos que según los criterios de seguridad se determinan como mensajes que no cumplen los requisitos establecidos, impidiendo su ingreso al sistema. Así como se encarga de bloquear mensajes no seguros también permite aquellas comunicaciones que se encuentran dentro de los estándares de seguridad establecidos. (Moreno, 2018)

4.4.2 Mecanismos detectores

La segunda línea para el control de riesgos son los mecanismos detectores, cuando un riesgo sobrepasa el nivel de defensa preventivo es de vital importancia ejecutar las medidas o sistemas que se encuentran en la segunda línea, para así, localizar los riesgos que amenazan los activos de la empresa e intervenir en ellos antes de que se conviertan en un ataque y comprometan al

sistema. (Villacis, 2016) Estas medidas deben desplegarse en búsqueda de comportamientos sospechosos donde la más común son las exploraciones de red por parte de intrusos.

En esta etapa los mecanismos más utilizados son los Sistemas de Detección de Intrusos, estos permiten monitorear la red, analizar el tráfico y analizar las actividades que se realizan en el sistema, siempre teniendo en cuenta cuales acciones pueden pertenecer a intrusos. Una buena práctica en este punto es registrar los acontecimientos de los eventos que se han detectado para poder crear planes de contingencia y fortalecer los mecanismos preventivos. (Moreno, 2018) Los Sistemas de detección de intrusos más utilizados son los siguientes:

- **N-IDS:** se trata de un Sistema de Detección de Intrusos que se encuentra basado en la red, ofrece mantenerla permanentemente bajo revisión ayudando a detectar movimientos sospechosos que puedan transformarse en posibles ataques. Tiene un modo promiscuo que carece de dirección IP y de asignación de protocolos, esto le permite analizar los paquetes que se mueven en la red sin ser detectado. (Chanaluisa, Meza & Tasipanta, 2012)

- **H-IDS:** se trata de un Sistema de Detección de Intrusos que se encuentra dentro del host que monitoriza. Su función es la de capturar los paquetes que se mueven por el host, buscar posibles amenazas, analizar la información que se encuentra en los registros, revisar configuración realizadas, etc., mediante este análisis se pretende encontrar huellas dejadas o modificaciones realizadas por los intrusos para reportarlos. (Chanaluisa, Meza & Tasipanta, 2012)

4.4.3 Mecanismos correctores

Estos mecanismos entran en acción cuando el ataque ha concluido, se ha modificado el sistema y los daños ya se han materializados. Toman la

responsabilidad de corregir los daños y errores causados por el ataque volviendo al sistema a un estado óptimo. (Moreno, 2018)

4.4.4 Mecanismos disuasivos

Se busca proteger los activos de la empresa mediante mecanismos que buscan desalentar a los intrusos de efectuar el ataque. Se las pueden ver como barreras que se encuentran instaladas para mostrar que tanto el sistema como la organización tienen un nivel de seguridad robusto, dando a entender, que la dificultad para infiltrase o realizar un ataque es sumamente complicada y que en caso de tomar dicha decisión van a necesitar de tiempo y recursos que no poseen o no entran en sus planes. Algunos ejemplos de mecanismos disuasivos son:

- Circuito cerrado de cámaras de vigilancia.
- Cifrado de datos.
- Personal de seguridad.
- Biometría.
- Contraseñas.
- Tarjetas de identificación. (Moreno, 2018)

4.5 Mecanismos de gestión

El entorno que rodea a las empresas cada vez presenta un mayor número de amenazas, conociendo esto, la mayoría de estas han tomado medidas para su protección que dependiendo de sus ingresos destinan una mayor cantidad de recursos a dicha causa, sin embargo, existen casos en los cuales a pesar de tener los equipos, protocolos, controles y soluciones pertinentes para mitigar toda amenaza siguen presentando vulnerabilidades y siguen siendo el blanco de ataques.

Esos casos se deben a una falta de procesamiento de la información de ataques previos y a la falta de administración pues a pesar de contar con todo lo necesario se desperdicia tales recursos al no crear un proceso de mejora continua, provocando, que cada área trabaje de forma individual, no sirve de nada contar con varios procesos de seguridad que no se comuniquen entre ellos. Cuando aparece este problema, la solución es implementar un sistema de gestión centralizado, con esto se gana mayor eficiencia, derivando en mejores soluciones frente a ataques, vulnerabilidades y sobre todo una mayor velocidad para dar respuesta a posibles filtraciones en el sistema. (Luzón, 2017)

En la figura 20 se puede ver un claro ejemplo de un sistema de gestión centralizado, se observa el Sistema de Gestión de Eventos de Seguridad Informática (SIEM) cuya estructura contempla la Gestión de Eventos (SEM) y la Gestión de la Seguridad de la Información (SIM).

Figura 20. Estructura del Sistema de Gestión de Eventos de Seguridad Informática.

Tomado de (TCI, s.f.)

4.5.1 SIM

Sistema de Gestión de la Seguridad de la Información, se enfoca en recolectar información de forma masiva para comprimirla y almacenarla utilizando el menor espacio posible. No analiza los datos en tiempo real y permite centralizar el almacenamiento de todos los archivos, análisis de eventos y toda la información que ha recolectado para poder administrarla y presentarla mediante informes. (Robalino, 2018)

4.5.2 SEM

Sistema de Gestión de Eventos, su modelo toma como base el seguimiento de los eventos de red que son producidos por alertas generadas del análisis de un dispositivo de seguridad como pueden ser firewalls o algún tipo de IDS instaurado en el sistema, este seguimiento se lo hace en tiempo real permitiendo monitorear y gestionar los eventos del sistema en vivo registrando anomalías que son inmediatamente reportadas y tratadas en el menor tiempo posible. (Robalino, 2018)

4.5.3 SIEM

Sistema de Gestión de la Seguridad de la Información y Gestión de Eventos, este término nace de dos tecnologías que son independientes pero que a la vez pueden ser complementarias, en otras palabras, SIEM es un hibrido formado por los elementos de los sistemas SIM y SEM.

Siendo SIEM un hibrido de SIM y SEM tiene varios atributos de ambos, permite ver las situaciones desde un punto de vista diferente, es un sistema más completo, es capaz de detectar posibles tendencias, de encontrar patrones seguidos por los intrusos y de identificar comportamientos anormales. Esto se

logra gracias a que maneja virtudes como el monitoreo, análisis, y entrega de informes con los datos de los eventos que se han generado por medio de dispositivos de seguridad como firewalls, IDS, Antivirus, etc., que se encuentran situados en la red y que se utilizan como medidas de protección contra intrusos. (Luzón, 2017)

Todo ese análisis se lo realiza en tiempo real, los mecanismos de protección de los que se habló anteriormente generan alarmas al instante que permiten acortar los tiempos para dar respuesta a las amenazas. (Luzón, 2017) Con todas estas medidas y confiando en todos los análisis previos realizados de las vulnerabilidades, análisis de riesgos, controles instaurados, etc., se puede hablar de un sistema que se encuentra preparado contra posibles amenazas, recordando siempre que no existe una red que sea 100% segura.

4.6 Propuesta para la implementación de un SIEM en Pymes

En este punto se presenta la propuesta para lograr una óptima implementación de cualquier herramienta SIEM seleccionada para utilizarse con el fin de fortalecer la seguridad informática en las redes de empresas pequeñas y medianas.

Para construir dicha metodología se tomaron en cuenta una serie de subprocesos los cuales se encargan de realizar varias actividades relacionadas al proceso de implementación que se han determinado se deben seguir cuando se trabaja en el entorno de empresas PYMES. En la tabla 22 se pueden observar los subprocesos junto a las actividades que realizan.

Tabla 22.
Actividades de los subprocesos

Metodología	
Subprocesos	**Actividades**
Requerimientos	Análisis de documentación
	Definición de las necesidades y expectativas de la empresa
	Establecer los activos a monitorear
	Selección de los controles de seguridad informática a instaurar
	Análisis del número de eventos por minuto con los cuales se trabaja
Planificación	Estudio de la infraestructura de red vigente
	Diseño de la arquitectura del SIEM
	Desarrollo de los protocolos de seguridad informática a seguir en cada caso
Selección de la tecnología	Análisis de las soluciones que cuentan con controles sobre los activos a monitorear
	Análisis de la relación calidad/precio
	Compatibilidad de los eventos y capacidad de correlación
Pruebas	Pruebas del diseño propuesto
	Optimización
Implementación de la arquitectura del SIEM	Implementación del hardware del SIEM
	Implementación del software del SIEM
Implementación de los agentes de seguridad informática	Implementación de los agentes de seguridad
	Conexión del SIEM con los agentes
Monitoreo	Verificar la procedencia de los eventos de seguridad que ocurran
	Realizar pruebas de integración
	Realizar pruebas de rendimiento del SIEM
	Correlación entre los incidentes de seguridad

Cada uno de los subprocesos se encargan de realizar diferentes acciones, se explican a continuación:

- **Requerimientos:** La primera etapa se encarga de analizar la documentación histórica de la empresa, se dedica a revisar el inventario para definir los activos con los cuales se cuenta y a la vez los clasifica dependiendo de su grado de importancia en el giro del negocio. Eso se hace para seleccionar los controles que se necesitan utilizar en el SIEM para equipar a dichos activos con el nivel de seguridad pertinente, siempre se busca conseguir su monitorización en tiempo real para prevenir posibles ataques.

- **Planificación:** La segunda etapa se encuentra enfocada en el análisis de la infraestructura de red, entra a un proceso para determinar las vulnerabilidades y puntos fuertes de la red vigente hasta la fecha realizando una especie de mapeado, facilitando de esta forma el encaje del SIEM ya que toma en cuenta sus resultados para construir la arquitectura del SIEM a ser implementada y los protocolos a seguir en casos de emergencia.

- **Selección de la tecnología:** En el tercer apartado entran en escena todas las herramientas enfocadas a brindar seguridad de la información que se ofrecen en el mercado, sin embargo, del análisis previo realizado se recomienda utilizar la herramienta OSSIM pues se la puede ver como una herramienta ideal para trabajarse en el entorno de empresas PYMES a razón de responder todas sus necesidades y exigencias.

- **Pruebas:** en el cuarto subproceso se encuentra el periodo de pruebas, se lo realiza por medio de la simulación de la propuesta planteada en un entorno virtualizado con el fin de evidenciar el funcionamiento del plan a seguir para la implementación del SIEM.

  Una vez comprobada su forma de actuar se analizan los resultados obtenidos y comparándolos con las necesidades de la empresa se procede a verificar el cumplimiento de las exigencias con las cuales se

trabaja, esto da paso a encontrar posibles inconvenientes, corregir posibles fallos o de igual forma da la oportunidad de optimizar el diseño para presentar mejores resultados y un funcionamiento más efectivo.

- **Implementación de la arquitectura del SIEM:** Una vez se han depurado los errores y se ha optimizado la solución por medio de la simulación realizada se procede a implementar la arquitectura del SIEM, para ello se deben considerar dos componentes, el hardware y el software.

  El hardware viene a ser los componentes físicos, estos elementos deben contar con la capacidad necesaria para dar respuesta a lo demandado por el software, que viene a ser la parte virtual, entonces, el hardware debe dar cabida a todas las exigencias del SIEM en cuanto a procesador, memoria, disco duro, tarjeta de red, interfaces, etc.

- **Implementación de los agentes de seguridad informática:** en la sexta etapa se habla sobre la implementación de los agentes que se encargan de ejecutar las acciones para conseguir mantener la seguridad de la información, cada uno de estos agentes tiene un área de acción y ya se les han asignado el cumplir con un determinado rol para proteger los activos de la empresa y el recopilar los datos de los eventos para realizar acciones de alertas, almacenamiento y correlación de incidencias. (Robalino, 2018)

- **Monitoreo:** el ultimo subproceso corresponde al monitoreo de la solución, una vez que todos los procesos de implementación han culminado se procede a ejecutar acciones para comprobar el óptimo funcionamiento de todos los procesos establecidos en la propuesta, es decir, en este punto se realizan las pruebas de integración mediante un rápido análisis de vulnerabilidades, se comprueba el nivel de conexión entre los agentes instalados en la red y la herramienta SIEM, se analizan los resultados del análisis de vulnerabilidades para indicar el rendimiento de la solución y finalmente, la recopilación de todos estos datos da una idea general del estado del SIEM una vez culminada su implementación.

4.7 Insumos y resultados de los subprocesos

Para que cada subproceso sea ejecutado de forma eficiente necesita abastecerse de información que pueden ser vistos como recursos o insumos los cuales va a procesar, transformándolos una y otra vez para arrojar un resultado que a su vez puede servir como insumo de otro subproceso.

En este punto se va a hablar de ese ciclo, se especificarán los insumos de entrada necesarios para que cada subproceso funcione correctamente y se indicaran los resultados entregados, para este proceso se utilizara como base a las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013.

En la Tabla 23 se pueden observar los subprocesos junto a los insumos que necesita para funcionar y los resultados conseguidos con la intervención de las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013.

Tabla 23.
Insumos y resultados de los subprocesos

Subprocesos	**Insumos**	**Resultados**
Requerimientos	Inventario	Definición de los activos que necesitan protección y selección de los controles a instaurar para mantenerlos seguros
	Análisis de riesgos	
	Reportes de incidentes	
Planificación	Activos de la empresa	Diseño de la arquitectura del SIEM y el desarrollo de los protocolos de seguridad
	Mecanismos de seguridad vigentes	
	Topología de la red	

Selección de la tecnología	Activos de la empresa	Solución SIEM a utilizar
	Mecanismos de seguridad vigentes	
	Diseño de la arquitectura del SIEM	
	Controles y protocolos por utilizar en el SIEM	
Pruebas	Activos de la empresa	Resultado de las pruebas y corrección de posibles fallas o falencias
	Mecanismos de seguridad vigentes	
	Diseño de la arquitectura del SIEM	
	Solución SIEM a utilizar	
Implementación de la arquitectura del SIEM	Resultado de las pruebas y correcciones realizadas	Implementación y configuración adecuada de la arquitectura del SIEM
	Topología de la red	
	Mecanismos de seguridad vigentes	
	Diseño de la arquitectura del SIEM	
	Solución SIEM a utilizar	
Implementación de los agentes de seguridad informática	Mecanismos de seguridad vigentes	Implementación de los agentes de seguridad informática
	Arquitectura y configuración del SIEM	
Monitoreo	Topología de la red	SIEM
	Activos de la empresa	Generar alarmas, reportes de eventos, correlación de incidentes y evaluación de efectividad.
	Mecanismos de seguridad vigentes	
	Arquitectura y configuración del SIEM	
	Agentes de seguridad instalados	

4.8 Metodología para la implementación de un SIEM

Es importante contar con un orden lógico a seguir para implementar un SIEM, este punto explica de forma básica la metodología, el funcionamiento a seguir que se ha explicado en la propuesta inicial, por medio de un diagrama de flujo se busca dar a entender el proceso completo, en este ciclo se encuentran conectados todos los subprocesos siguiendo un orden cronológico y una relación causa/efecto que en caso de no cumplirse está diseñada a convertirse en un bucle pues el objetivo principal de la propuesta es asegurar una óptima implementación del SIEM.

En la figura 21 se puede observar el diagrama de flujo de la metodología de Implementación de un SIEM

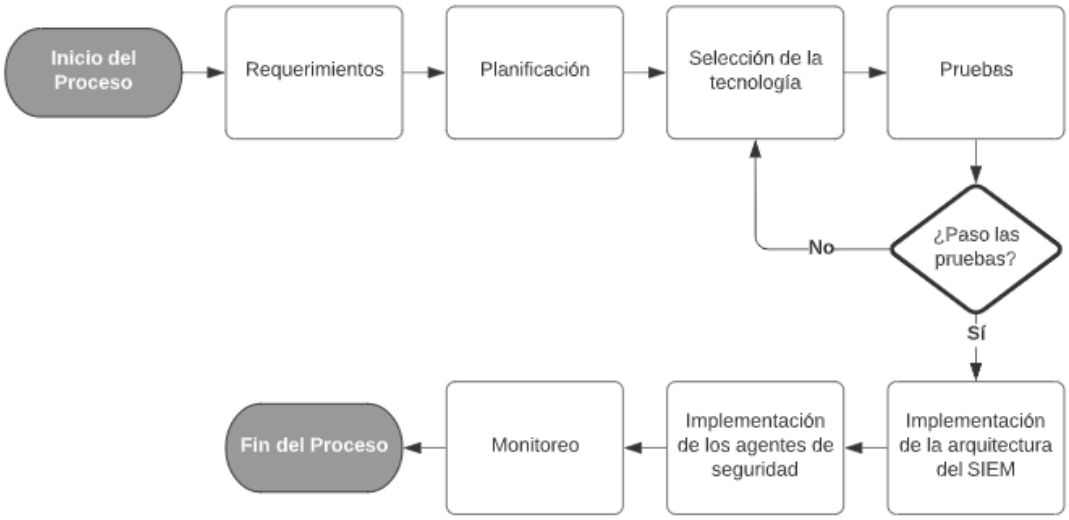

Figura 21. Flujo de la metodología de Implementación de un SIEM.

El proceso debe realizarse en el siguiente orden:

Inicio del Proceso

1. Requerimientos

2. Planificación
3. Selección de la tecnología
4. Pruebas
5. ¿Paso las pruebas?
    a) En caso de una respuesta negativa se debe volver a seleccionar una mejor solución revisando las necesidades de la empresa y los análisis realizados.
    b) En caso de una respuesta positiva se pasa a la siguiente etapa
6. Implementación de la arquitectura del SIEM
7. Implementación de los agentes de seguridad
8. Monitoreo

Fin del proceso

4.9 Proceso para la implementación de un SIEM

Comprendida la metodología a seguir se procede a explicar de forma detallada el funcionamiento de todos los subprocesos y actividades que componen la estructura de la propuesta planteada, especificando para ello la influencia causada por los insumos de entrada en el proceso de actividades para finalmente convertir esos datos en resultados.

En la tabla 24 se puede observar el diagrama general a utilizar para explicar el funcionamiento de los subprocesos.

Tabla 24.
Diagrama general de los subprocesos

<table>
<tr><th colspan="3">Subproceso</th></tr>
<tr><td>Insumos</td><td>Actividades</td><td>Resultados</td></tr>
<tr><td rowspan="2">Información de entrada necesaria para el subproceso</td><td>Acciones por realizar de cada subproceso</td><td rowspan="2">Producto de salida fruto de las acciones realizadas por el subproceso</td></tr>
<tr><td>Controles propuestos por las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013 en apoyo al subproceso</td></tr>
</table>

- **Insumos:** se refiere a todos los datos de entrada que necesita el subproceso para iniciar sus funciones.
- **Actividades:** es el conjunto de acciones que cada subproceso va a realizar para brindar seguridad informática dependiendo de su rol a cumplir.
- **Resultados:** es el elemento de salida, el producto que nace del resultado de haber llevado a cabo las actividades del subproceso
- **Controles propuestos por las normas ISO:** tomando en consideración las buenas prácticas de estas normas, sus recomendaciones serán utilizadas en aquellos subprocesos en los cuales su solución aplique o mejore la solución inicial.

4.9.1 Requerimientos

En esta etapa se van a analizar todos los datos históricos relacionados con eventos de seguridad informática de la empresa en donde se va a realizar la implementación del SIEM, este estudio permitirá conocer el entorno que rodea a la compañía y a la vez aumentar el nivel de efectividad de las soluciones que se puedan ofrecer. En la figura 22 se puede observar el diagrama de flujo con el cual el subproceso de requerimientos trabaja.

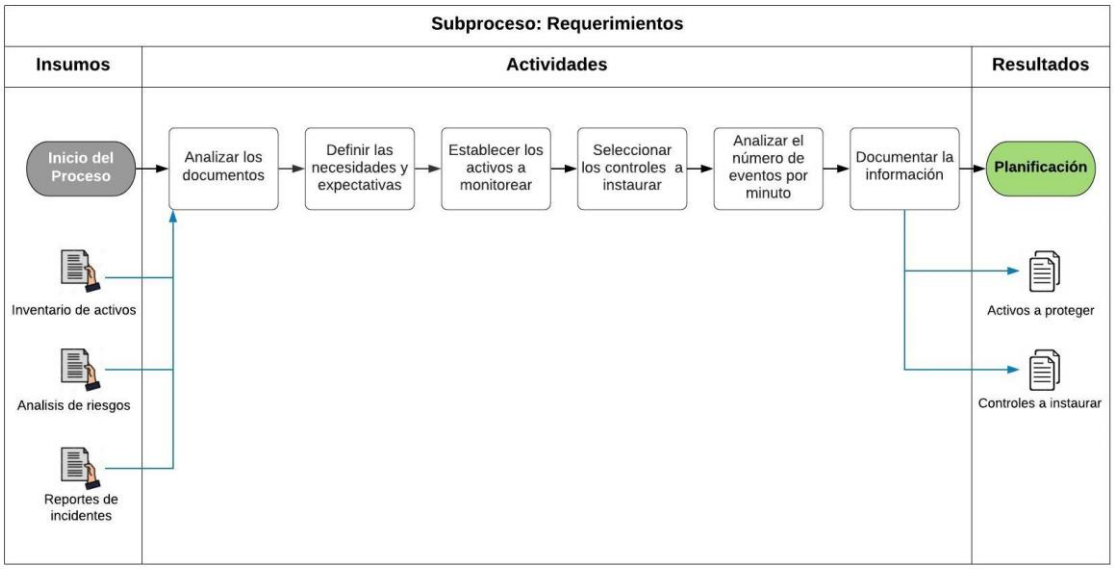

Figura 22. Flujo del subproceso de requerimientos.

Objetivo:

- La finalidad de este subproceso es analizar los activos de la empresa y tomando en cuenta el giro del negocio clasificarlos según su nivel de importancia e implicación para el normal funcionamiento de la compañía, por medio de esta información también se busca establecer controles de seguridad informática para mantener a los activos catalogados con un riesgo alto y muy algo seguros de posibles amenazas.

Insumos:

- Inventario de activos.
- Análisis de riesgo.
- Reportes de incidentes

Actividades:

- **Analizar los documentos:** en esta actividad se analiza la información de los insumos de entrada del subproceso de requerimientos, esto se lleva a cabo con el fin de tener evidencias en las cuales basarse para armar un eficiente sistema de seguridad informática, conocer los activos de la empresa y clasificarlos dependiendo del nivel de riesgo al cual se expone.

- **Definir las necesidades y expectativas:** se refiere al hecho de visualizar los problemas de la compañía para darles una pronta solución, a esto se le añade que dicha propuesta sea suficientemente eficiente para cumplir con el nivel de aceptación de riesgos.

- **Establecer los activos a monitorear:** una vez conocidas las necesidades es clave programar una reunión con los ejecutivos de alto rango y con todos los empleados relacionados con el departamento de seguridad informática en la empresa pues es importante definir los siguientes puntos:

    a) Determinar el giro principal del negocio y encontrar las actividades con mayor importancia dentro de ese núcleo.

    b) Clasificar los activos según su relevancia e influencia en el normal funcionamiento de la empresa.

    c) Elegir los activos que van a ser objeto de monitorización.

- **Seleccionar los controles a instaurar:** tomando en cuenta los activos a monitorizar se procede a elegir los controles mejor diseñados y con las

características más potentes que trabajen en esa área ofreciendo un entorno libre de amenazas.

- **Analizar el número de eventos por minuto:** se toma una cantidad referencial como muestra del número de eventos con los cuales trabaja la empresa en un minuto, esto se hace con el objetivo de conocer sus capacidades de procesamiento promedio.

- **Documentar la información:** se refiere al acto de almacenar toda la información utilizada en este subproceso pues servirá como insumo para la siguiente fase.

Resultados:

- Definición de los activos que necesitan protección.
- Selección de los controles a instaurar para fortalecer la seguridad de la información.

4.9.2 Planificación

Este subproceso toma en cuenta el resultado de la fase de requerimientos y recolecta en el camino información relacionada con el estado de la red empresarial para poder armar la arquitectura del SIEM a implementar.

En la figura 23 se puede observar el diagrama de flujo con el cual el subproceso de planificación trabaja.

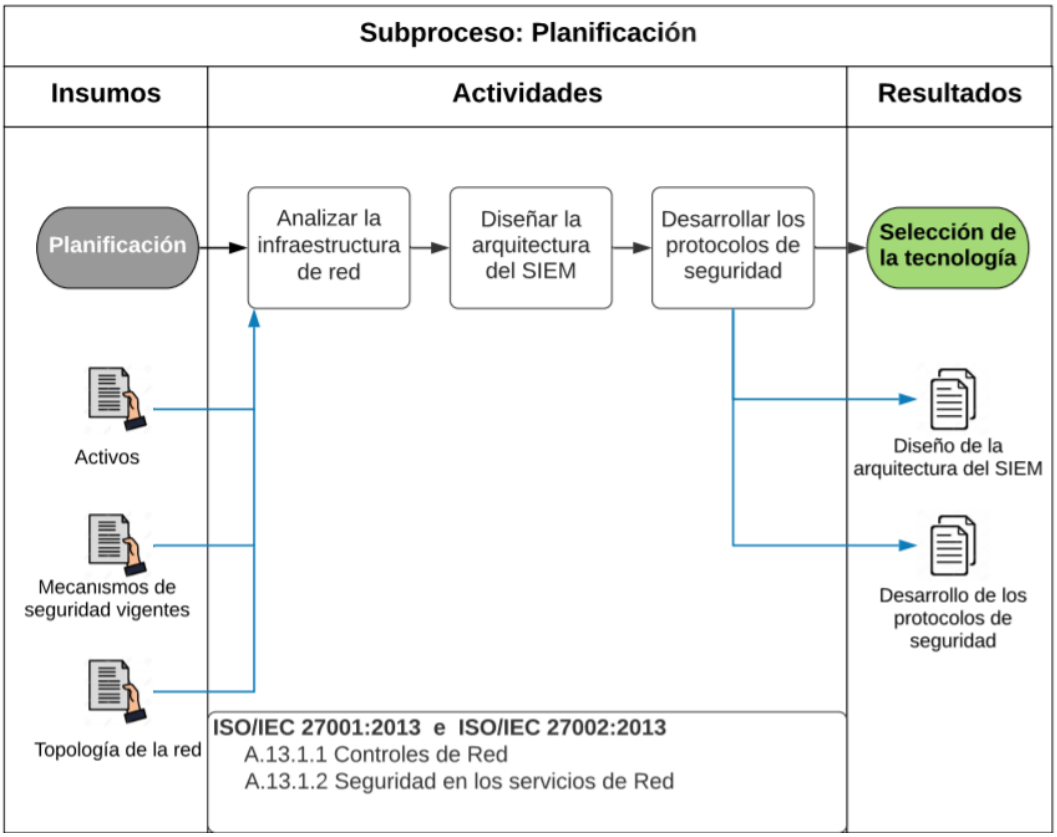

Figura 23. Flujo del subproceso de planificación.

Objetivo:

- Conseguir el diseño de la arquitectura del SIEM que se va a implementar en la red empresarial en conjunto con protocolos básicos de seguridad que apoyen a esa propuesta en cuanto a mantener ciertos niveles de seguridad.

Insumos:

- Activos de información.
- Mecanismos de seguridad vigentes
- Topología de la red

Actividades:

- **Analizar la infraestructura de red:** en este punto se analizará la topología de red con la cual se encuentra trabajando la empresa en donde se va a implementar el SIEM, se busca principalmente obtener información que facilite la implementación como: protocolos de red, direccionamiento, etc.

- **Diseñar la arquitectura del SIEM:** tomando en cuenta la topología de red y el entorno de la empresa, se elaboran los primeros diagramas de cómo se va a instalar el SIEM.

- **Desarrollar los protocolos de seguridad:** para armar estos protocolos se toma en consideración las buenas prácticas expuestas en la norma ISO/IEC 27002:2013, esto busca realizar el levantamiento de la arquitectura del SIEM sobre un entorno seguro disminuyendo riesgos potenciales.

Resultados:

- Diseño de la arquitectura del SIEM
- Desarrollo de los protocolos de seguridad

4.9.3 Selección de la tecnología

Este subproceso toma en cuenta el resultado de la fase de planificación, con lo cual, si se le añade otros insumos y las actividades que ejecuta, facilitara la elección del SIEM a implementar.

En la figura 24 se puede observar el diagrama de flujo del subproceso de selección de la tecnología.

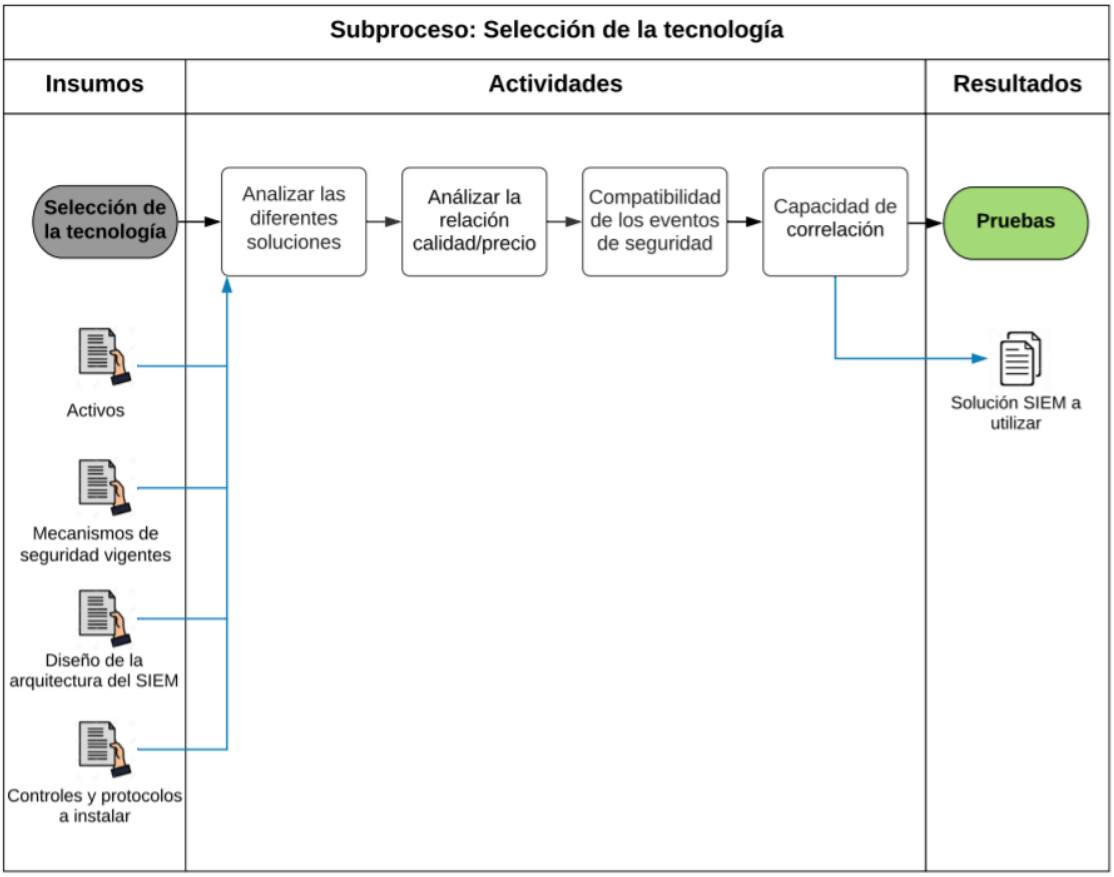

Figura 24. Flujo del subproceso de selección de la tecnología.

Objetivo:

- Tomando en consideración los insumos de entrada de este subproceso se busca encontrar la mejor herramienta SIEM a implementar para la infraestructura de red de la empresa.

Insumos:

- Activos de información.
- Mecanismos de seguridad vigentes
- Diseño de la arquitectura del SIEM
- Controles y protocolos por utilizar en el SIEM

Actividades:

- **Analizar las diferentes soluciones:** para la elección del SIEM se debe tomar en cuenta la gran variedad de herramientas presentes en el mercado, es importante tomar en consideración los análisis realizados con anterioridad en donde se habla de los controles a utilizar, los protocolos a tomar en consideración y las necesidades de la empresa pues se recomienda elegir una herramienta que de respuesta a esas premisas.

- **Analizar la relación calidad /precio:** un punto importante es encontrar el equilibrio entre la calidad y el precio de la solución, en el mercado existen varias herramientas tanto libres como de paga, cada una de ellas tienen diferentes características y se encuentran diseñadas a resolver problemas de diferentes indoles pues la complejidad de sus soluciones varían, se recomienda implementar un SIEM equilibrado, que responda a todas las necesidades de la empresa y su precio sea asequible tomando en cuenta la situación financiera de la compañía.

- **Compatibilidad de los eventos de seguridad:** otro filtrado para seleccionar un SIEM es la compatibilidad de las soluciones con los formatos de eventos de seguridad de los activos de la empresa, siempre se debe buscar una alta compatibilidad entre estos elementos pues lo que se busca es trabajar en conjunto para lograr una mejor comunicación y apoyo mutuo para brindar mejor eficiencia contra amenazas.

- **Capacidad de correlación:** Dependiendo del número de eventos por minuto, se debe seleccionar una herramienta que presente una mayor capacidad de procesamiento ya que resulta de gran importancia poder correlacionar toda esa información de forma simultánea y al instante.

Resultado:

- Solución SIEM a utilizar

4.9.4 Pruebas

Una vez se ha seleccionado la tecnología a utilizar, se monta el ambiente que se considere más prudente para realizar las pruebas de la propuesta tentativa a implementar en la red de la empresa, de forma puntual se espera analizar los resultados en cuento a respuestas en tiempo real, funcionamiento del SIEM y el grado de eficiencia de sus características.

En la figura 25 se puede observar el diagrama de flujo del subproceso de pruebas.

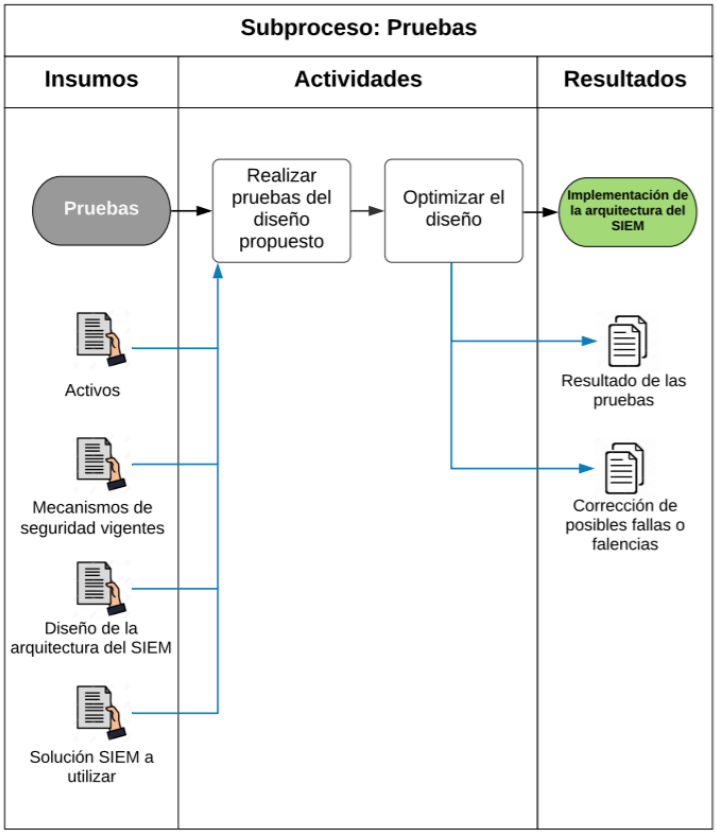

Figura 25. Flujo del subproceso de pruebas.

Objetivo

- Evidenciar por medio de una simulación el funcionamiento de la propuesta de implementación del SIEM para encontrar posibles fallas o puntos de optimización.

Insumos:

- Activos de información.
- Mecanismos de seguridad vigentes.
- Diseño de la arquitectura del SIEM.
- Solución SIEM a utilizar.

Actividades:

- **Realizar pruebas del diseño propuesto:** para desarrollar esta actividad se debe montar con anterioridad un ambiente simulado en el cual se pueda ejecutar la solución seleccionada, en este ambiente se va a poner a prueba las características de la herramienta, sus ventajas y desventajas, así como de la propuesta de implementación a seguir.

  Se recomienda realizar estas pruebas de funcionamiento lo más semejantes posibles al entorno que va a enfrentar una vez implementada pues servirá para observar su comportamiento en un ambiente parecido al real. (Robalino, 2018)

- **Optimizar el diseño:** una vez realizadas las pruebas se deben analizar los resultados para encontrar posibles fallas o inconvenientes mostrados por la solución previamente seleccionada, en caso de encontrar falencias se deben considerar posibles soluciones para optimizar su diseño.

  De no cumplir con las exigencias presentadas por la empresa se recomienda seleccionar otra herramienta SIEM.

Resultados:

- Resultados de las Pruebas.
- Corrección de posibles fallas o falencias encontradas.

4.9.5 Implementación de la arquitectura del SIEM

Conociendo los resultados de las pruebas realizadas de la herramienta SIEM a implementar y dependiendo del caso, habiendo ya corregido cualquier tipo de falla o inconveniente con la propuesta de implementación, se procede a implementar la arquitectura del SIEM en la infraestructura de la empresa en cuestión, se recuerda que sin importar del éxito en el periodo de pruebas únicamente se procede con la implementación teniendo la autorización de las personas responsables de aprobar el proyecto.

En la figura 26 se puede observar el diagrama de flujo del subproceso encargado de implementar la arquitectura del SIEM.

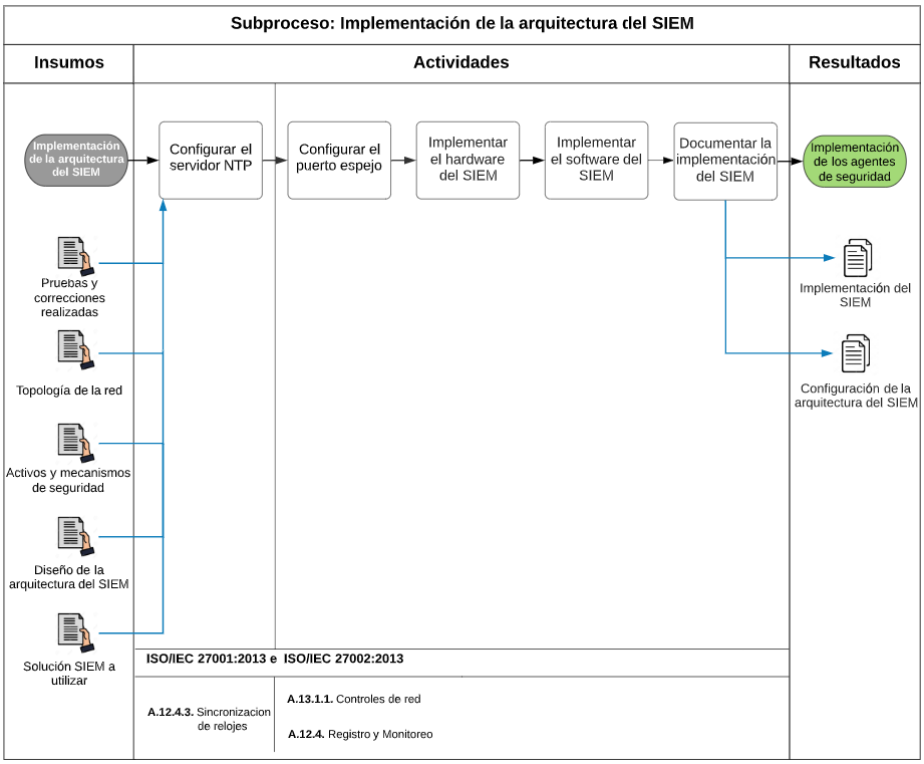

Figura 26. Flujo del subproceso de implementación de la arquitectura del SIEM.

Objetivo

- Llevar a cabo la implementación de la parte física (hardware) y virtual (software) de la herramienta SIEM seleccionada en la infraestructura de la empresa.

Insumos:

- Pruebas y correcciones realizadas
- Topología de la red
- Activos de información y mecanismos de seguridad vigentes
- Diseño de la arquitectura del SIEM
- Solución SIEM a utilizar

Actividades:

- **Configurar el servidor NTP:** se realiza esta actividad con el fin de sincronizar los periodos de tiempo manejados por la herramienta SIEM con los tiempos manejados por los activos de información que posteriormente serán objeto de monitorización, con este movimiento se consigue que los eventos de seguridad sean generados utilizando como fuente una misma hora. (Robalino, 2018)

- **Configurar el puerto espejo:** para configurar este puerto se toma en consideración la topología de la red pues se debe seleccionar aquel equipo con la conectividad más importante, ya que se trata de empresas Pymes usualmente viene a ser el switch core pues por medio de este se moviliza la mayor parte del tráfico de la empresa a lo cual se debe añadir que dicho tráfico posee los paquetes correspondientes a los activos de información que se han seleccionado con anterioridad. (Robalino, 2018)

- **Implementar el hardware del SIEM:** al hablar de hardware se refiere a todos los componentes físicos que forman parte del equipo en donde se va a implementar el SIEM, sus características deben responder a los

requisitos mínimos demandados por la herramienta a ser implementada poniendo especial énfasis en los siguientes puntos:

a) **Puerto de red de administración:** este puerto se encuentra configurado para conectarse con un equipo de tal forma que cuando se encuentre dentro de una red aislada de propiedad de la misma empresa sea capaz de darle la posibilidad al usuario de administrar el SIEM desde esa ubicación. (Robalino, 2018)

b) **Puerto de red de monitoreo de agentes:** este puerto funciona como un punto de conexión con los activos de información que se han seleccionado para implementar seguridad, esta es la ubicación exacta en donde se va a llevar a cabo la implementación de los agentes HIDS y de igual forma se procede a configurar a estos elementos para que sean capaces de enviar sus respectivos eventos de seguridad hasta el SIEM. (Robalino, 2018)

c) **Puerto de red para el análisis del tráfico:** este puerto presenta una conexión de forma directa con el puerto espejo, dado el caso viene a conectarse con el Switch Core el cual ya ha sido configurado previamente. (Robalino, 2018)

- **Implementar el Software del SIEM:** al hablarse de software se hace referencia de todos los elementos lógicos que trabajan en conjunto para lograr cumplir con las funciones de las herramientas SIEM, antes de proceder a su implementación se deben cumplir las siguientes condiciones:

a) Se debe instalar el software de la herramienta SIEM seleccionada sobre el hardware que previamente ya ha sido configurado

b) **Puerto de red de administración:** a este puerto se lo debe configurar utilizando la dirección IP, con este movimiento se consolida la conexión entre el equipo de administración ubicado en una red aislada de la misma empresa con la herramienta SIEM.

c) **Puerto de monitoreo de los agentes:** en este puerto se lleva a cabo la configuración de los activos de información seleccionados con anterioridad para que logren conectarse con el puerto de red. Es importante recalcar que en este lugar se reciben todos aquellos eventos de seguridad generados por los activos de información con el fin de ser puestos bajo monitoreo. (Robalino, 2018)

d) **Puerto de análisis de red:** en este puerto converge todo el tráfico que transita por el Switch Core, se encuentra configurado en modalidad promiscua por lo cual no posee una dirección IP.

e) **Cliente NTP:** se encarga de la gestionar el sincronismo entre la zona horaria local y el cliente en la herramienta SIEM.

f) **Equipo de administración del SIEM:** utilizando el privilegio de conectarse al puerto de red dedicado para administrar la herramienta SIEM, este equipo se encuentra ubicado dentro de una red aislada que pertenece a la misma empresa.

- **Documentar la implementación del SIEM:** se refiere al acto de almacenar toda la información relacionada con el proceso que se ha seguido para implementar la herramienta SIEM en la infraestructura de la empresa, esos detalles servirán como insumo para la siguiente fase y para posibles auditorias u otros tipos de acciones a desarrollar en el futuro.

Resultados:

- Implementación de la herramienta SIEM.
- Configuración de la arquitectura de la herramienta SIEM

4.9.6 Implementación de los agentes de seguridad informática

Como los incidentes de seguridad son causados por diferentes fuentes estos tienen varios tipos que pueden ser servidores, dispositivos de seguridad, elementos de conexión, etc., dependiendo de su naturaleza van a ser configurados por un agente HIDS, SNMP o SYSLOG.

En la figura 27 se puede observar el diagrama de flujo de la implementación de los agentes de seguridad informática

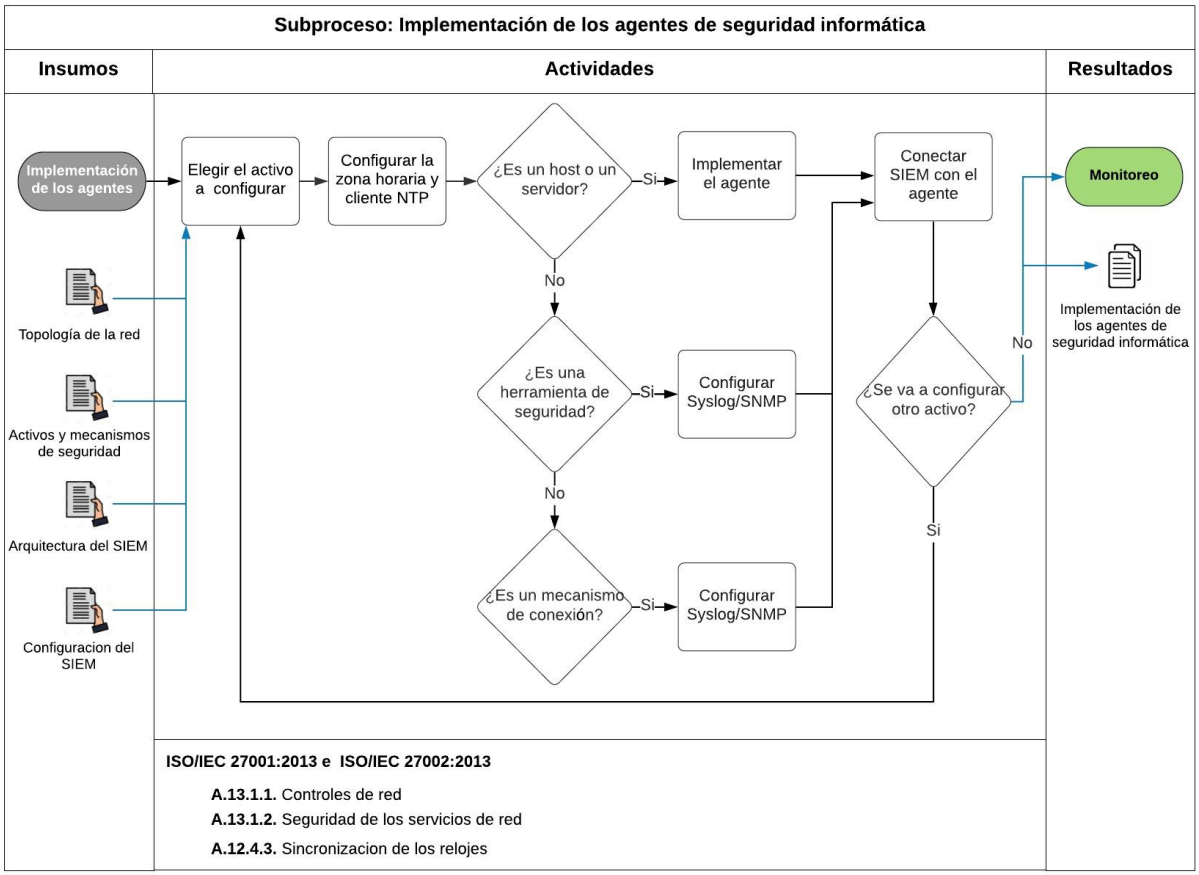

Figura 27. Flujo del subproceso de implementación de agentes.

Objetivo:

- Este subproceso busca implementar los agentes de seguridad informática en la red empresarial

Insumos:

- Topología de la red
- Mecanismos de seguridad vigentes
- Arquitectura del SIEM
- Configuración del SIEM

Actividades:

- **Elegir el activo a configurar:** dependiendo de las necesidades se procede a seleccionar el activo que necesita ser monitoreado por el SIEM.

- **Configurar la zona horaria y cliente NTP:** esta actividad es de gran importancia pues se encarga de mantener en sincronía al cliente y a la zona horario con los activos de información manejados por la empresa.

- **Configurar el activo de información:** dependiendo de las características del activo de información seleccionado, la persona encargada define el siguiente orden de preguntas para proceder con su configuración:

    a) **¿Es un host o un servidor?:** en caso de que el activo de información sea un host o un servidor se implementa el agente, en caso de no serlo se considera el literal b.

    b) **¿Es una herramienta de seguridad?:** en caso de que el activo de información sea una herramienta de seguridad como puede ser firewall se configura Syslog o SNMP los cuales se encargaran de enviar los eventos de seguridad de forma directa al SIEM, en caso de no ser una herramienta de seguridad se considera el literal c.

c) **¿Es un mecanismo de conexión?:** en caso de que el activo de información sea un mecanismo de conexión como puede ser un router o un switch se configura Syslog o SNMP los cuales se encargaran de enviar los eventos de seguridad de forma directa al SIEM.

- **Conectar SIEM con el agente:** una vez que se a configurado el agente, el siguiente paso a realizar es establecer una comunicación robusta con el SIEM, esto se hace para lograr un rápido intercambio de información para cuando el agente genere eventos de seguridad, es crucial dar parte de este hecho al SIEM.

- **¿Se va a configurar otro activo?:** en caso de que se vaya a configurar otro activo el proceso regresa hasta el punto en el cual se realiza la elección del activo de información a configurar, en caso de que no se vaya a configurar otro activo finaliza el subproceso.

Resultado:

- Implementación de los agentes de seguridad informática

4.9.7 Monitoreo

Es el ultimo subproceso que compone la propuesta para la implementación del SIEM y utiliza las características de los dispositivos instalados para realizar el proceso de monitorización de la red empresarial, con esto busca detectar posibles incidentes de seguridad que amenacen el normal funcionamiento de la empresa. Este subproceso también se apoya en la información de los controles expuestos por las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013 para confirmar que los activos de información utilizados entienden cómo funcionan los eventos de seguridad y proceden a enviarse en dirección al SIEM.

De forma general el monitoreo es el encargado de generar los informes de eventos de seguridad informática. En la figura 28 se puede observar el diagrama de flujo que sigue el subproceso encargado del monitoreo.

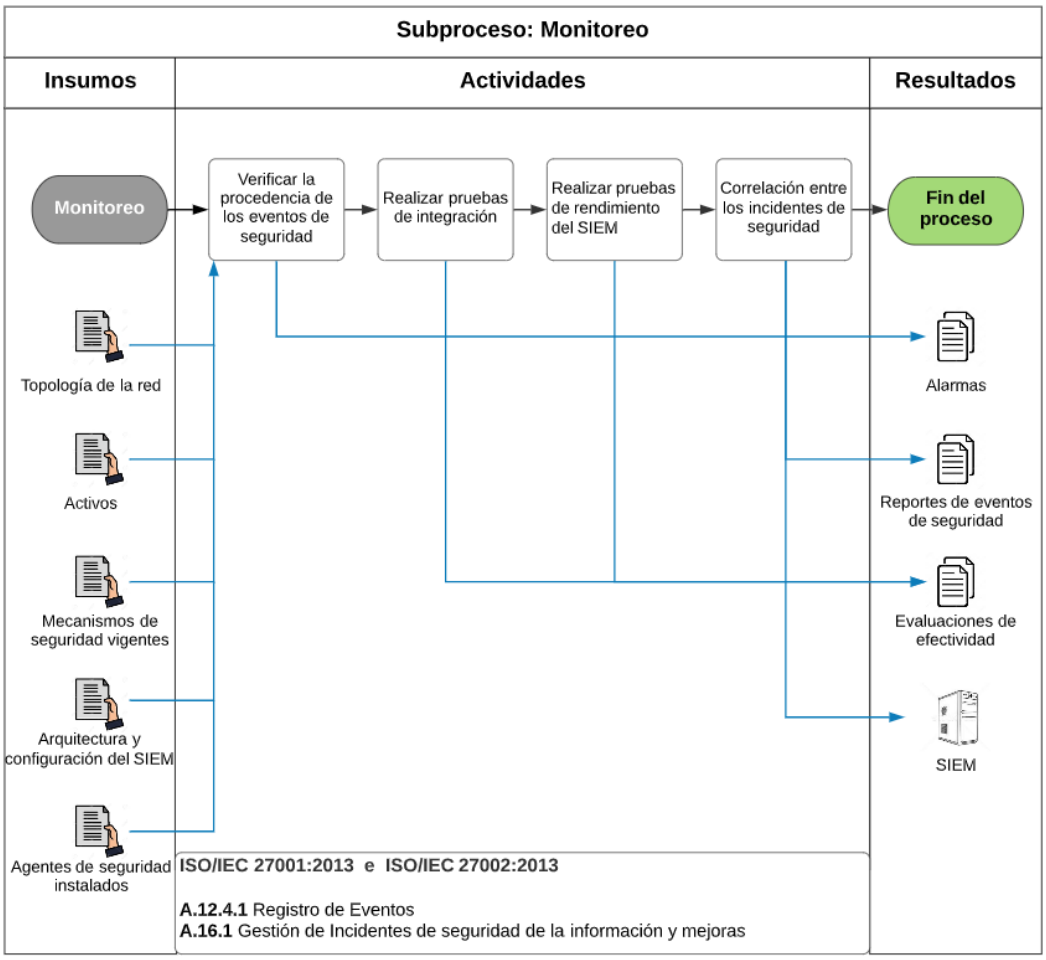

Figura 28. Flujo del subproceso de monitoreo.

Objetivo:

- Se encarga de la monitorización de las redes por medio del registro y análisis de las actividades que se encuentren siendo desarrollados en el sistema, detecta las vulnerabilidades que amenacen los activos de información.

Insumos:

- Topología de la red.
- Activos de información
- Mecanismos de seguridad vigentes
- Arquitectura y documentación del SIEM
- Agentes de seguridad instalados

Actividades:

- **Verificar la procedencia de los eventos de seguridad:** se encarga de que los eventos de seguridad se encuentren activos y listos para enfrentar las amenazas, en caso de encontrase desactivados es crucial activarlos pues de no hacerlo se convertirían inmediatamente en una vulnerabilidad.

- **Realizar pruebas de integración:** se refiere al trabajo en conjunto del SIEM con los agentes que han sido instalados, para comprobar que ambas partes están conectadas e intercambiando información de los eventos de seguridad que suceden en la red, se recomienda ejecutar un análisis de vulnerabilidades y en caso de visualizar el evento generado en el SIEM se confirmaría su óptimo funcionamiento pues se estarían comunicando correctamente. (Robalino, 2018)

- **Realizar pruebas de rendimiento del SIEM:** tomando en cuenta los resultados mostrados por los controles, protocolos y demás eventos de seguridad instalados para brindar seguridad de la información se procede a analizar las soluciones ejecutadas frente a las amenazas tomando siempre en cuenta el nivel de riesgo aceptado por la empresa. Este punto es de gran importancia ya que permite la mejora continua del SIEM

- **Correlación entre los incidentes de seguridad:** es una de las funciones más importantes del SIEM, se encarga de recopilar los datos históricos relacionados con los incidentes de seguridad que se han presentado en el sistema, los correlaciona para establecer posibles asociaciones lógicas entre ellas y con eso logra mejorar en la toma de decisiones pues adquiere

una visión más amplia de los sucesos que ocurren entorno a los activos de la empresa.

Resultados:

- SIEM en estado optimo
- Reporte de ataques y alarmas
- Reportes de eventos de seguridad
- Evaluaciones de efectividad
- Acta de entrega del SIEM.

Una vez realizadas todas las actividades expuestas en los subprocesos que conforman la propuesta para la implementación de un SIEM en infraestructuras de empresas PYMES, la compañía cuenta con una herramienta con los recursos y con la capacidad necesaria para monitorear la red constantemente en búsqueda de vulnerabilidades, amenazas o actividades sospechosas consiguiendo de esta forma mejorar la seguridad de los activos informáticos y equipos de red.

En el Anexo I (pág. 201) se puede evidenciar la implementación de la herramienta OSSIM en un entorno virtualizado.

CONCLUSIONES

Una vez culminada la investigación se llegó a la conclusión de que a diario las redes de empresas PYMES son objetivos de ataques, aproximadamente el 63% de empresas pequeñas y el 60% de empresas medianas a nivel global han sido víctimas de diversos tipos de programas malignos. Esos porcentajes son claros indicativos de una problemática en cuestiones de seguridad.

Hasta el día de hoy varias empresas tienen que soportar las consecuencias de ataques informáticos y solventar de una u otra forma los problemas ocasionados por este hecho, por ello, se detectó la necesidad de contar con un sistema de gestión de eventos de seguridad informática que evite estos hechos, proteja la información con la cual trabaja la compañía y garantice el normal funcionamiento de todos sus procesos y servicios.

Comparando a las empresas que no cuentan con planes o medidas de seguridad previamente establecidas contra posibles incidentes, las compañías que se encuentran trabajando en conjunto con estas herramientas de gestión de eventos de seguridad informática presentan un menor número de vulnerabilidades, ataques, amenazas, robos de información, etc., con eso se demuestra el grado de relevancia e influencia de las soluciones SIEM en entornos empresariales.

Se llegó a la conclusión de que a la hora de resolver los problemas de seguridad en las redes de empresas pequeñas y medianas, a pesar de presentar desventajas y un peor rendimiento en comparación con una herramienta de paga las soluciones SIEM con licencia gratuita son la mejor opción para la implementación en entornos de empresas PYMES, el motivo de esta conclusión se basa en que a pesar de sus limitadas soluciones la mayoría de estos problemas de seguridad pueden ser solventados con los controles que estas herramientas poseen.

De todas las herramientas de gestión de eventos y seguridad informática comercializadas en el mercado, para implementarse en entornos de empresas

PYMES se llegó a la conclusión de que la mejor solución a utilizarse es OSSIM de AlienVault, esto dadas sus características pues apoyan el desenvolvimiento de controles y protocolos orientados a detectar las vulnerabilidades más comunes que estas empresas registran en su mayoría.

Se llega a la conclusión de que al utilizar la norma ISO/IEC 27001:2013 para realizar los procesos de implementación, manejo y soporte de la herramienta SIEM se alcanzan mejores resultados y una mejor utilización de los recursos ofrecidos por esa solución pues este estándar ayuda a explotar sus capacidades consiguiendo un máximo y eficaz rendimiento.

Se ha detectado que el mercado en el cual se enfocan las herramientas SIEM pagadas es el de empresas grandes, eso se debe a sus soluciones, tienen un mayor número de controles y complementos que permiten tener un monitoreo más estricto sobre las redes, por otro lado, las SIEM de licencia gratuita se enfocan en el mercado de empresas PYMES pues sus soluciones son limitadas, no presentan suficientes controles para mitigar amenazas avanzadas y los complementos ofrecidos por su proveedor no se encuentran muy bien adecuados para funcionar con su estructura, es por ello que estas se deben utilizar en entornos donde la probabilidad de ataques fuertes sea menor.

De las experiencias relacionadas con la herramienta OSSIM en implementaciones realizadas en varias empresas tanto públicas como privadas, se afirma que esta plataforma muestra una buena capacidad al momento de detectar problemas de seguridad informática como vulnerabilidades en el acceso a los datos, áreas de trabajo sin bases para ofrecer disponibilidad continua en los servicios, software sin ningún tipo de soporte con una gran cantidad de puertos abiertos, navegación web en sitios potencialmente peligrosos y amenazas que comprometen directamente procesos críticos, hechos que demuestran la valía de esta plataforma en el control de vulnerabilidades.

Utilizando la investigación realizada sobre las experiencia de varias empresas en la implementación y uso de las diferentes normas ISO relacionadas con la seguridad de la información, se concluye que al utilizar estos estándares se

consigue una mejor eficiencia al momento de encontrar valores de riesgos, entregar manuales de usuario, lograr una implementación exitosa de cualquier solución SIEM, crear matrices de riesgos, elaborar eventos contra amenazas, encontrar tendencias en ataques y en la elaboración de políticas.

En empresas PYMES con un SIEM implementado en su infraestructura de red, los niveles de vulnerabilidades que presentan sus sistemas son del 1% para problemas serios, el 8% para problemas de nivel alto, el 7% para problemas de nivel intermedio y el 84% para problemas de nivel bajo.

Finalmente, se concluye que el 57% de empresas con capacidad para detectar ataques en tiempo real han sufrido diez ataques o menos en un año calendario. De ese porcentaje, el 78% de compañías había implementado una herramienta SIEM para garantizar la seguridad de la información lo cual es un claro indicador de que los hackers informáticos encuentran problemas o evitan el lidiar con redes de empresas con integraciones de soluciones de seguridad SIEM.

RECOMENDACIONES

Si mantener un bajo presupuesto es un factor prioritario para la empresa a la hora de implementar herramientas dedicadas a la protección de la información, se recomienda utilizar soluciones Open Source pues significaría una reducción en el desembolso a realizar para implementar un SIEM en una PYMES.

Previo a la adquisición de alguna plataforma de seguridad informática se recomienda realizar un análisis de las necesidades y de la verdadera situación en la cual se encuentra la compañía en lo relacionado a la seguridad de sus procesos, esto ayuda a seleccionar de forma correcta el SIEM evitando adquirir soluciones muy avanzadas o costosas las cuales ofrecerían un buen rendimiento, pero dificultarían su manejo y sería una inversión innecesaria.

Para la selección de los controles a instaurar en el sistema encargado de la seguridad de la información, se recomienda tomar en consideración la norma ISO/IEC 27002:2013 ya que este es un estándar basado en buenas prácticas las cuales sirven como referencia para la selección de controles.

Como estándar a utilizar en los procesos de seguridad de la empresa se recomienda tomar en cuenta a la norma ISO/IEC 27001: 2013 ya que permite certificación y este hecho es muy importante pues vuelve a la compañía más competitiva y mejora su imagen con los clientes al mandar un claro mensaje de que la seguridad de sus datos es de máxima importancia para la compañía y por ello siempre se encuentran en la vanguardia tecnológica.

Al momento de analizar los valores de riesgos para clasificarlos por su importancia dependiendo de los niveles aceptados por la empresa, se recomienda tener un enfoque en el cual los peligros con niveles de extremo e intolerables deban ser tratados hasta llegar al nivel de tolerable y los activos críticos que se encuentren en el nivel de tolerable deban ser tratados hasta llegar al nivel de aceptable.

Para la selección de los controles a implementar en la herramienta SIEM se recomienda tomar en cuenta los 35 objetivos de control de los cuales se conforma la norma ISO/IEC 27002:2013, estos objetivos indican el área de trabajo de los 114 controles, funciona como un tipo de clasificación y ayuda a comprender la función para la cual fueron diseñadas.

Para tratar una posible amenaza, vulnerabilidad o riesgo, se recomienda eliminarla desde su raíz, esto se fundamenta en las posibles consecuencias que se puedan presentar en el futuro si se utiliza otros mecanismos de tratamiento como la transferencia, donde existe un riesgo de infectar otras áreas, la reducción de las amenazas, la cual es una opción temporal puesto que sigue existiendo y aún se encuentra en el sistema y asumir el riesgo, donde independientemente de su nivel de gravedad es un error no tomar acciones puesto que se puede llegar a convertir en un ataque.

En relación con los empleados y personas del entorno de la empresa, se recomienda socializar temas afines a la seguridad de la información ya que con frecuencia son víctimas de terceros para obtener datos de relevancia como contraseñas o claves de acceso, por ello, estas personas son vistas como el eslabón más débil en la cadena de seguridad del sistema, al no tener un cuidado adecuado de los activos entregados por la compañía se convierten en un riesgo potencial.

REFERENCIAS

Morales, R. & Guerrero, C. (2015). Implementación del Sistema de Gestión de Eventos de Seguridad de la Información (OSSIM) en la Infraestructura de Red del GAD de la Provincia de Chimborazo. Recuperado el 26 de enero 2020, de Escuela Superior Politécnica de Chimborazo Sitio web: http://dspace.espoch.edu.ec/handle/123456789/5058

Chosgo, A. (2017). Soluciones OPEN SOURCE para seguridad perimetral de empresas PYMES. *Universidad y Cambio*, *2*(2), pp. 1-14

Patiño, R. (2017). Afectación del cibercrimen en las pymes. En Universidad Remington (1ª Ed.), Memorias: Segundo Congreso Internacional: Crimen económico y fraude financiero y contable (pp. 59-66). Medellín, Colombia: Fondo Editorial Remington.

Kaspersky. (2016) Midiendo el impacto financiero de la seguridad informática en los negocios. Recuperado de: https://latam.kaspersky.com/blog/reporte-midiendo-elimpacto-financiero-de-la-seguridad-informatica-en-losnegocios/7711/

Jiménez, W. (2017). Seguridad informática o de la información en pymes. Recuperado el 26 de enero 2020, de Universidad Piloto de Colombia Sitio web: http://repository.unipiloto.edu.co/handle/20.500.12277/4929

Espinoza, D. (2015). Estudio de la herramienta de seguridad Open Source Security Information management (Ossim) en la Universidad Tecnológica Empresarial de Guayaquil (UTEG). Recuperado el 26 de enero 2020, de Universidad de Guayaquil Sitio web: http://repositorio.ug.edu.ec/handle/redug/10185

Parra, C. & Porras, H. (2007). Las amenazas informáticas: peligro latente para las organizaciones actuales. Recuperado de https://revistas.uis.edu.co/index.php/revistagti/article/view/1259/1656

Verdejo, G. (2013). Seguridad en Redes IP. *Denegación de servicio: DOS/DDOS* (pp. 34-49). Recuperado de https://issuu.com/awalther_bm/docs/seguridadip

Barragán, I., Góngora, I. & Martínez, E. (2013). Implementación de políticas de seguridad informática para la m.i. municipalidad de Guayaquil aplicando la norma iso/iec 27002. Recuperado el 12 de abril 2020, de Escuela Superior Politécnica del Litoral Sitio web: http://www.dspace.espol.edu.ec/xmlui/handle/123456789/21546

Sotelo, M., Torres, J. & Rivera, J. (2012). Un Proceso Práctico de Análisis de Riesgos de Activos de Información. Abril 12, 2020. Recuperado el 12 de abril 2020 de: http://www.comtel.pe/comtel2012/callforpaper2012/P26C.pdf

Morales, D. (2018). Tipos de mecanismos para la protección de los servicios informáticos y sus modelos de seguridad. Recuperado el 21 de marzo 2020, de Universidad Piloto de Colombia Sitio web: http://repository.unipiloto.edu.co/handle/20.500.12277/4928

García, J. (2018). Ventajas e implementación de un sistema SIEM. Recuperado el 21 de marzo 2020, de Universitat Oberta de Catalunya Sitio web: http://hdl.handle.net/10609/81425

AT&T Cybersecurity. (2020). AlienVault OSSIM. Recuperado el 21 de marzo 2020 de https://cybersecurity.att.com/products/ossim

Kavanagh, K., Bussa, T. & Sadowski, G. (2020). Magic Quadrant for Security Information and Event Management. Recuperado el 22 de marzo 2020 de https://www.gartner.com/doc/reprints?id=1-1YE69EYM&ct=200218&st=sb

Marquina, L. (2018). Ventajas e implementación de un sistema SIEM. Recuperado el 23 de marzo 2020, de Universitat Oberta de Catalunya Sitio web: http://hdl.handle.net/10609/81267

Chanaluisa, D., Meza, A. & Tasipanta, J. (2012). Implementación del sistema de gestión y administración de seguridad para la dirección de tecnologías de la Universidad Central del Ecuador (DTIC). Recuperado el 23 de marzo 2020, de Universidad Central del Ecuador Sitio web: http://www.dspace.uce.edu.ec/handle/25000/365

Solarte, F., Enriquez, E. & Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista tecnológica – ESPOL, Vol. 28* (5). Recuperado desde: http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321

Robalino, J. (2018). Propuesta Metodológica y Simulación de la Implementación de un SIEM basado en la Norma ISO 27001 y/o 27002. Recuperado el 23 de marzo 2020, de Escuela Politécnica Nacional Sitio web: http://bibdigital.epn.edu.ec/handle/15000/19672

Audea. (2007). Conoce la ISO 27001:2005 de mano de Áudea. Recuperado el 24 de marzo 2020 de https://www.audea.com/conoce-la-iso-270012005-de-mano-de-audea/

ISOTools. (2020). Software ISO 27001. Recuperado el 24 de marzo 2020 de https://www.isotools.org/software/riesgos-y-seguridad/iso-27001

Lain. (2016). SIEM: Gestión de eventos e información de seguridad. Recuperado el 24 de marzo 2020 de https://lainholding.com/searchinform-siem/

Columba, B. (2017). Diseño de un sistema de gestión de seguridad de la información, basado en la norma ISO/IEC 27001:2013 para la compañía Aronem Air Cargo S.A. Recuperado el 24 de marzo 2020, de Escuela Politécnica Nacional Sitio web: http://bibdigital.epn.edu.ec/handle/15000/16997

Pico, F. (2016). Siem bajo software libre para la seguridad operacional en las pymes de la ciudad de Pelileo. Recuperado el 27 de marzo 2020, de Universidad Regional Autónoma de los Andes Sitio web: http://dspace.uniandes.edu.ec/handle/123456789/4691

Andres, A. & Gómez, L. (2012). Guía de aplicación de la Norma UNE ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. Recuperado de http://www.varios.cen7dias.es/documentos/documentos/90/iso.pdf

Lema, R. & Donoso, D. (2018). Implementación de un sistema de gestión de seguridad de información basado en la Norma ISO 27001:2013 para el control físico y digital de documentos aplicado a la empresa LOCKERS S.A. Recuperado el 27 de marzo 2020, de Universidad de las Fuerzas Armadas (ESPE) Sitio web: http://repositorio.espe.edu.ec/handle/21000/14397

Ramírez, C. & Moreira, R. (2017). Diseño para la implementación de los dominios de cifrado y seguridad física y ambiental basados en la norma ISO27001 e ISO27002, para el área de TI de la procesadora nacional de alimentos “PRONACA”. Recuperado el 27 de marzo 2020, de Universidad de las Fuerzas Armadas (ESPE) Sitio web: http://repositorio.espe.edu.ec/handle/21000/13182

Porras, P. & Salazar, J. (2016). Evaluación de seguridad de información en el proceso de seguros previsionales del ISSFA basado en Normas ISO: 27001. Recuperado el 27 de marzo 2020, de Universidad de las Fuerzas Armadas (ESPE) Sitio web: http://repositorio.espe.edu.ec/handle/21000/12561

Villacis, M. & Soria, V. (2016). Diseño de un sistema de gestión de la seguridad de la información (SGSI) basado en la norma ISO 27001:2013 para la red corporativa de la empresa Ecuatronix. Recuperado el 03 de abril 2020, de Universidad Politécnica Salesiana Sitio web: http://dspace.ups.edu.ec/handle/123456789/12406

Ladino, M., Villa, P. & López, A. (2011). Fundamentos de ISO 27001 y su aplicación en las empresas. *Scientia et Technica, Vol. 17* (47). Recuperado desde: https://www.redalyc.org/pdf/849/84921327061.pdf

Pazmiño, C. & Contero, W. (2019). Diseño de una política de seguridad de la información basada en la norma ISO 27002:2013, para el sistema de botones de seguridad del Ministerio del Interior. Recuperado el 07 de abril 2020, de Universidad Internacional SEK (Ecuador) Sitio web: http://repositorio.uisek.edu.ec/handle/123456789/3345

Pallas, G. (2009). Metodología de Implantación de un SGSI en un grupo empresarial jerárquico. Recuperado el 07 de abril 2020, de Universidad de la República (Uruguay) Sitio web: https://hdl.handle.net/20.500.12008/2954

ISO27001. (2020). Norma ISO 27001. Recuperado el 07 de abril 2020 de https://normaiso27001.es/

CEUPE. (s.f.). Estructura de la norma ISO 27001:2013. Recuperado el 07 de abril 2020 de https://www.ceupe.com/blog/estructura-de-la-norma-iso-27001-2013.html

INNOVA-T. (s.f.). Estructura de la Norma ISO 27001. Recuperado el 07 de abril 2020 de http://innova-t.co/topic/estructura-de-la-norma-iso-27001/

Pilla, J. (2019). Diseño de una política de seguridad de la información para el área de tecnología de la información de la Cooperativa de Ahorro y Crédito Chibuleo LTDA., basado en la norma ISO/IEC 27002:2013. Recuperado el 08 de abril 2020, de Universidad Internacional SEK (Ecuador) Sitio web: http://repositorio.uisek.edu.ec/handle/123456789/3601

Splunk. (2020). Security Information and Event Management. Recuperado el 08 de abril 2020 de https://www.splunk.com/en_us/siem-security-information-and-event-management.html

SourceForge. (2020). Hyperic Application & System Monitoring. Recuperado el 08 de abril 2020 de https://sourceforge.net/projects/hyperic-hq/

Cabrera, R. & Agüero, L. (2015). Planificación de un SIEM para la red de la UACJ y desarrollo virtual de un IDS. Recuperado el 12 de abril 2020, de Universidad Autónoma de Ciudad Juárez Sitio web: http://hdl.handle.net/20.500.11961/2915

Romero, M. & Figueroa, G. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. doi: http://dx.doi.org/10.17993/IngyTec.2018.46

Arias, L. & Bustamante, J. (2013). Procedimiento para la implementación de una herramienta SIEM en empresas que cuenten con un sistema de gestión de SGSI. Recuperado el 12 de abril 2020, de Universidad Piloto de Colombia Sitio web: http://repository.unipiloto.edu.co/handle/20.500.12277/2586

Arias, L. & Bustamante, J. (2013). Procedimiento para la implementación de una herramienta SIEM en empresas que cuenten con un sistema de gestión de SGSI. Recuperado el 12 de abril 2020, de Universidad Piloto de Colombia Sitio web: http://repository.unipiloto.edu.co/handle/20.500.12277/2586

Peña, J. (2015). Instructivo para la implementación efectiva de sistemas de información de seguridad y administración de eventos SIEM para la Agencia Nacional de la Superación de la Pobreza Extrema ANSPE. Recuperado el 21 de abril 2020, de Universidad Piloto de Colombia Sitio web: http://repository.unipiloto.edu.co/handle/20.500.12277/2866

Murillo, C., Bonilla, D. & Buitrago, J. (2012). diseño de una metodología para la implementación del sistema de gestión de seguridad de la información - sgsi, en el sector de laboratorios de análisis microbiológicos, basado en ISO 27001. Recuperado el 21 de abril 2020, de Universidad EAN Sitio web: https://repository.ean.edu.co/handle/10882/2692

StudyLib. (s.f.). Estudio de alternativas de código abierto. Recuperado el 21 de abril 2020 de https://studylib.es/doc/542038/-documento---aplicaciones-de-monitoreo-v5.0.09092103-

Areitio, J. (2008). *Seguridad de la información*, Madrid, España: Fondo Editorial Paraninfo.

Colegio Oficial de Ingenieros de Telecomunicaciones. (s.f.). Guía de Iniciación a Actividad Profesional Implantación de Sistemas de Gestión de la Seguridad de la Información (SGSI) según la norma ISO 27001. Recuperado el 24 de abril 2020 de https://www.coit.es/sites/default/files/informes/pdf/implantacion_de_sistemas_de_gestion_de_la_seguridad_de_la_informacion_sgsi_segun_la_norma_iso_27001.pdf

Herrera, J., Fernández, J. & García, J. (2017). Implementación de un security information and event management Siem, en el comando de la Armada Nacional dirección de tecnologías de la información y las comunicaciones. Recuperado el 24 de abril 2020, de Universidad Piloto de Colombia Sitio web: http://repository.unipiloto.edu.co/handle/20.500.12277/2657

Orozco, A. (2013). Sistema de gestión de seguridad de la información SGSI. Recuperado el 24 de abril 2020, de Universidad Piloto de Colombia Sitio web: http://repository.unipiloto.edu.co/handle/20.500.12277/2606

Aguilera, P. (2010). Seguridad informática. *Editex*, *1*(2), pp. 8-19

Areitio, J. (2008). Seguridad de la información redes, informática y sistemas de información. *Universidad de Deusto*, *1*(2), pp. 21-25

Moreno, P. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management). Recuperado el 26 de abril 2020, de Universidad San Francisco de Quito Sitio web: http://repositorio.usfq.edu.ec/handle/23000/4911

Villafuerte, A. & Bravo, A. (2015). Implantación De Una Herramienta Ossim Para El Monitoreo Y Gestión De La Seguridad De La Red Y Plataformas Windows Y Linux Aplicado A Empresas Medianas. Recuperado el 26 de abril 2020, de Escuela Superior Politécnica del Litoral (ESPOL) Sitio web: http://www.dspace.espol.edu.ec/xmlui/handle/123456789/29939

Balarezo, A. & Poveda, D. (2015). Propuesta de mejoramiento de la herramienta OSSIM SIEM (Open Source), para obtener los niveles óptimos de gestión en la administración de la seguridad, en una red implementada en Cloud Computing. Recuperado el 27 de abril 2020, de Universidad Politécnica Salesiana Sitio web: http://dspace.ups.edu.ec/handle/123456789/10101

ANEXOS

Anexo I

Con el fin de simular el funcionamiento de la herramienta OSSIM se procede a crear una máquina virtual utilizando para ello Oracle VM VirtualBox. En la figura 29 se puede observar las características que posee la máquina virtual.

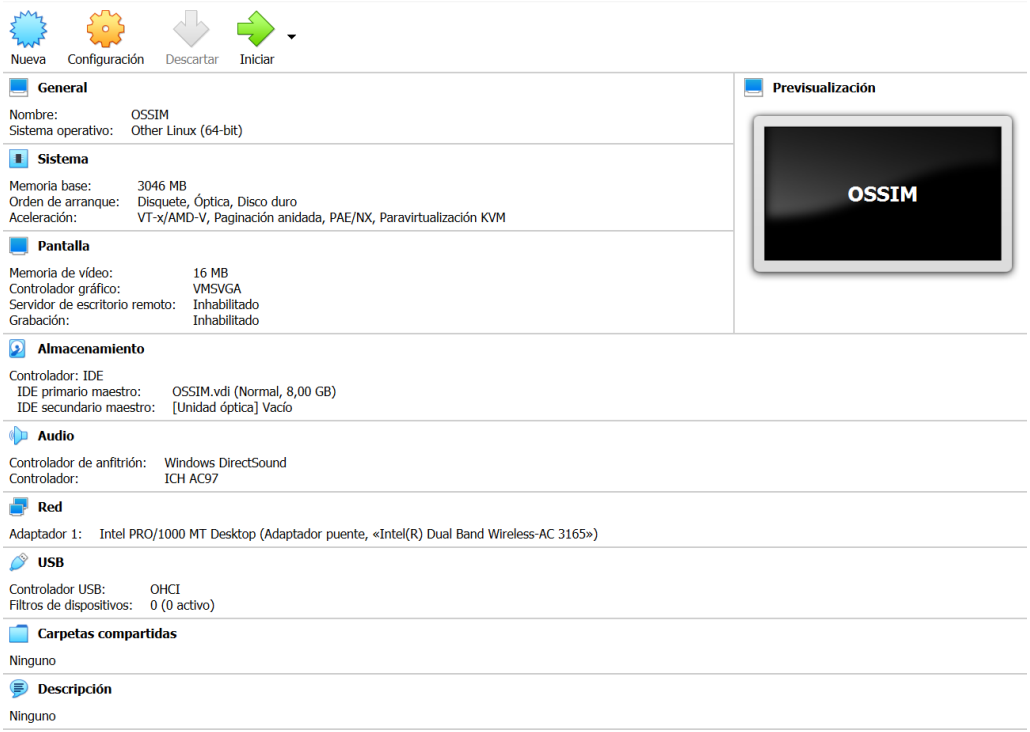

Figura 29. Características de la máquina virtual.

Iniciamos la instalación de OSSIM utilizando para ello su imagen ISO con la última versión disponible en disponible en https://cybersecurity.att.com/products/ossim la cual es la 5.8.1

En la figura 30 se puede observar una ventana donde se procede a realizar la selección del tipo de instalación que se va a ser uso.

Figura 30. Selección del tipo de Alienvault.

En la figura 31 se observan las opciones de idioma que se encuentran disponibles, para el caso se seleccionara español.

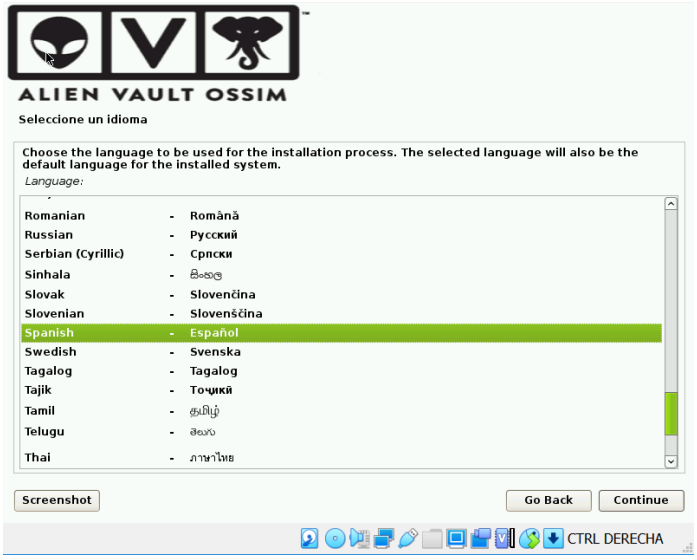

Figura 31. Selección del idioma.

En la figura 32 se observan varios países, se procede a seleccionar el país territorio o área en donde estamos ubicados, esto se hace para poder fijar la zona horaria así como para seleccionar la ubicación del sistema.

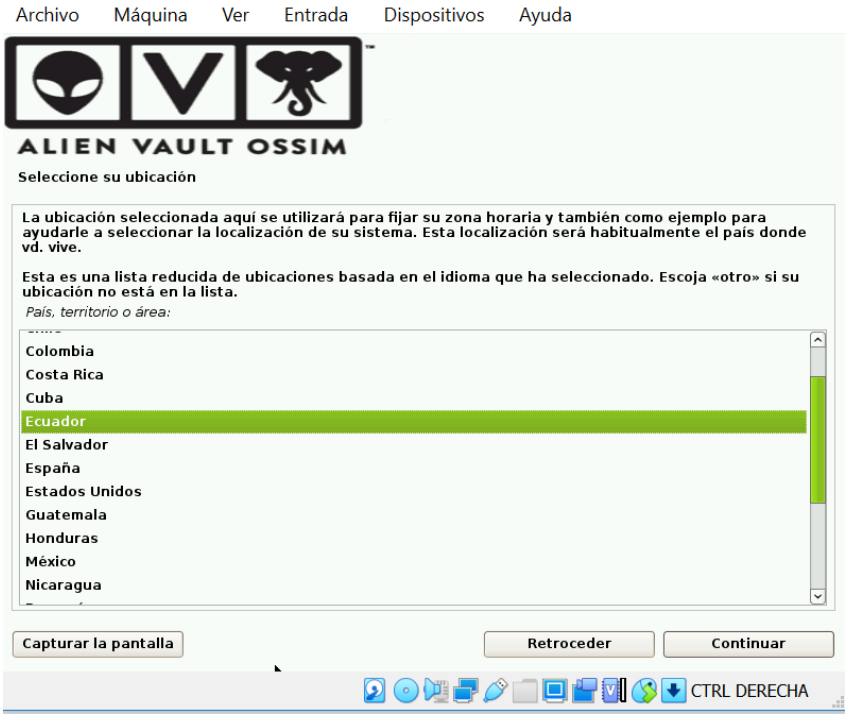

Figura 32. Selección de país.

En la figura 33 seleccionamos el tipo de teclado.

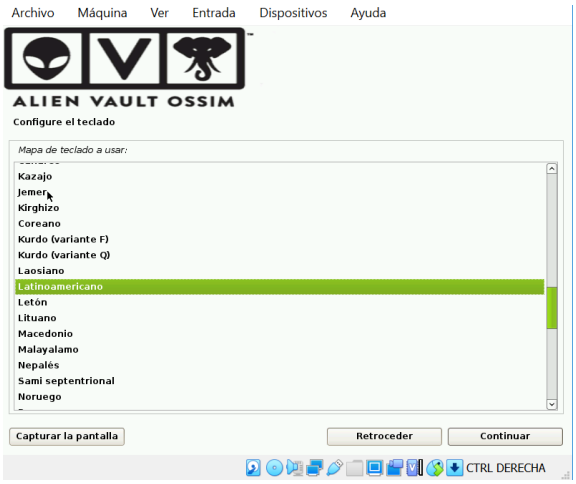

Figura 33. Selección del tipo de teclado.

En la figura 34 se observa la dirección IP que va a tener el servidor OSSIM la cual se utilizara para configurar la red.

Figura 34. Dirección IP del servidor OSSIM.

En la figura 35 se observa la máscara de red.

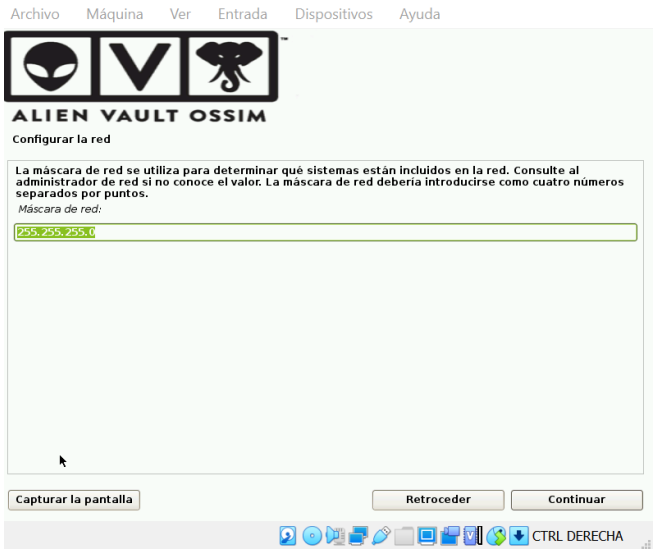

Figura 35. Mascara de red.

En la figura 36 se puede visualizar la clave que va a tener el root el cual se va a encargar de administrar todo el sistema hay que recordar que dicha contraseña debe ser robusta para prevenir el acceso de terceros.

Figura 36. Contraseña del servidor.

En la figura 37 se observa la zona horaria seleccionada para el sistema

Figura 37. Zona horaria.

En la figura 38 se observa que el sistema a comenzado con su instalación, el tiempo puede durar varios minutos dependiendo de las características del ordenador.

Figura 38. Instalación del sistema.

En la figura 39 se observa una ventana en donde se debe introducir la contraseña asignada para el root.

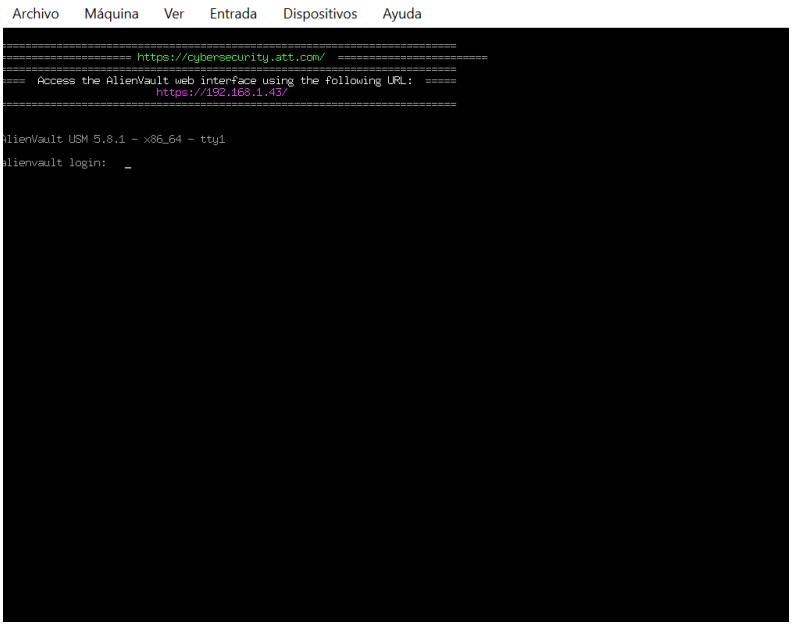

Figura 39. Pantalla de ingreso del root.

En la figura 40 se observa el modo consola, aquí se puede configurar el sistema o de igual forma también se cuenta con un acceso vía web en donde este procedimiento resulta ser más fácil.

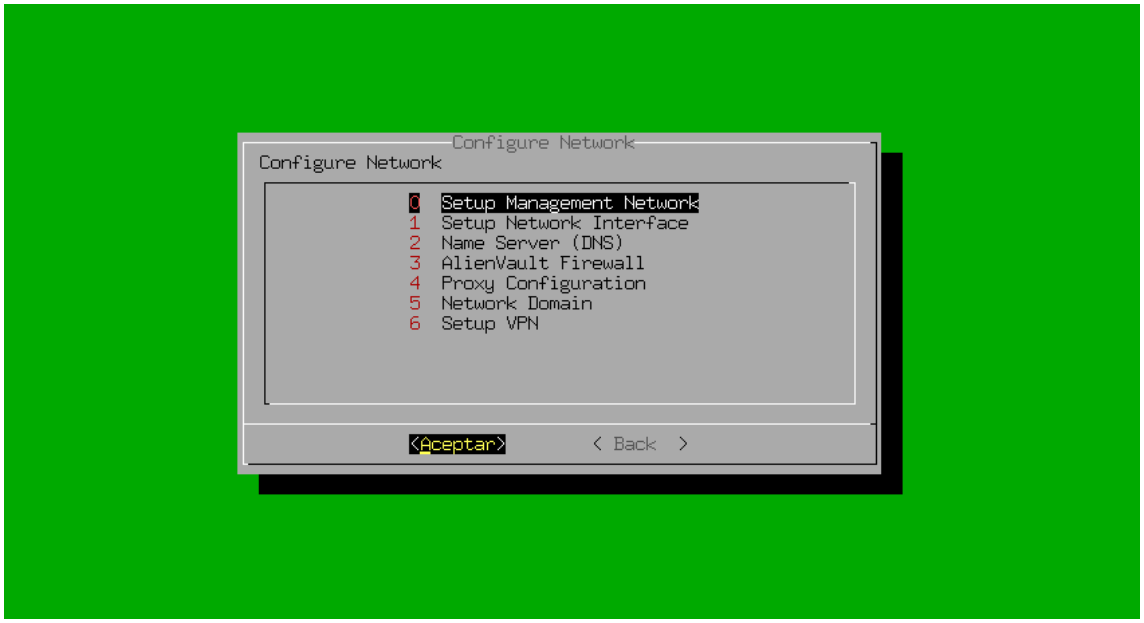

Figura 40. Interfaz modo consola.

En la figura 41 se observa el acceso vía web, para acceder a esta opción se debe ingresar la dirección IP e introducir las credenciales establecidas en la instalación del sistema.

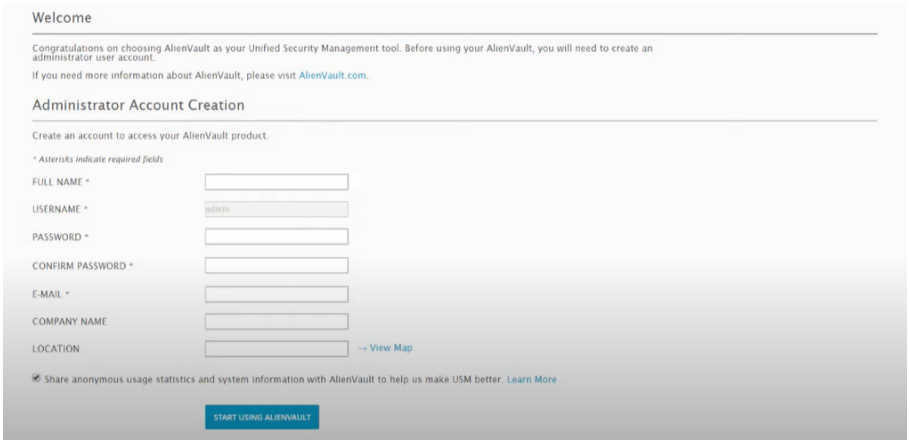

Figura 41. Creación de la cuenta de administración del SIEM.

En la figura 42 se observa la pantalla de inicio de Wizard el cual va a permitir al administrador configurar las capacidades de seguridad, para esto la herramienta permite establecer redes, analizar, descubrir activos e implementar agentes HIDS.

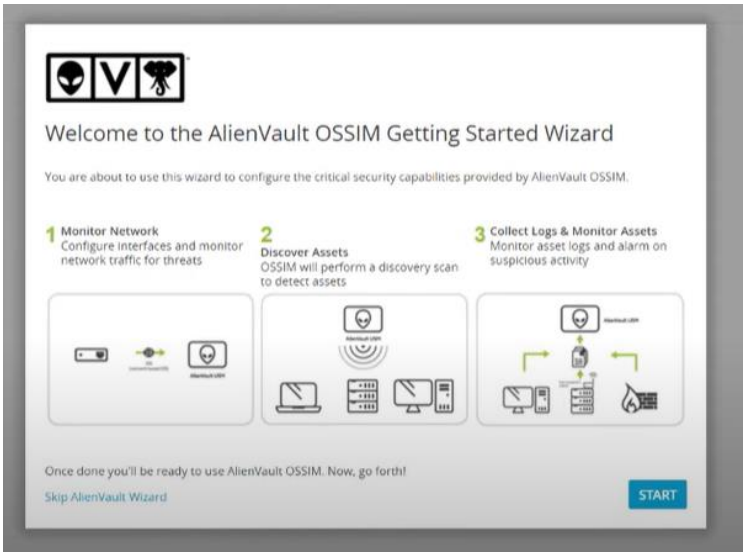

Figura 42. Configuración de Wizard.

En la figura 43 se observa que se encuentra instalado Metasploitable, esta herramienta va a entregar información de las vulnerabilidades que enfrenta la red.

```
root@metasploitable:/home/msfadmin/ossec-hids-2.9.1/doc# /var/ossec/bin/ossec-co
ntrol status
ossec-logcollector is running...
ossec-syscheckd is running...
ossec-agentd is running...
ossec-execd is running...
root@metasploitable:/home/msfadmin/ossec-hids-2.9.1/doc# _
```

Figura 43. Metasploitable instalado.

En la figura 44 se observa la pantalla de configuración de Sophos, esta herramienta va a permitir administrar los dispositivos y ofrecer seguridad a la red.

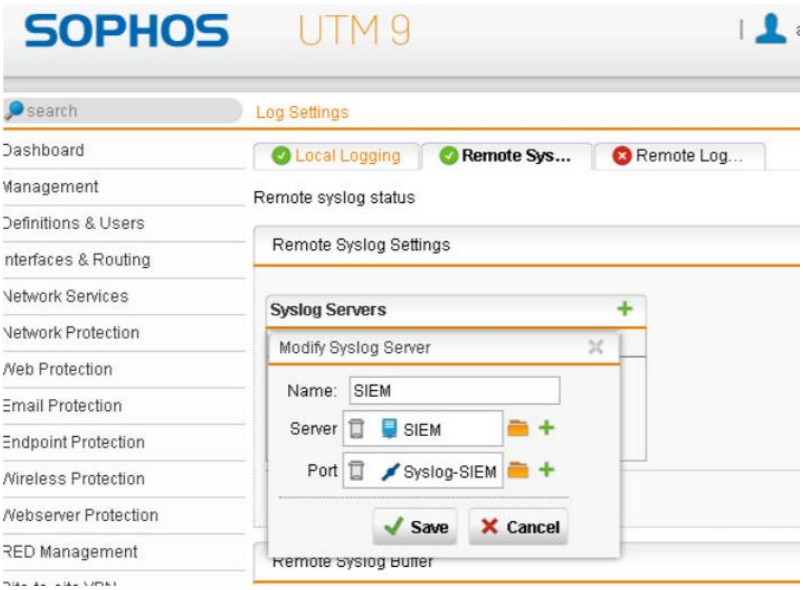

Figura 44. Firewall Sophos, servidor de logs.

En la figura 45 se observa la correlación de los eventos tomando en cuenta el modelo establecido, se puede ver que se ha llevado a cabo un ataque hacia los activos de la empresa.

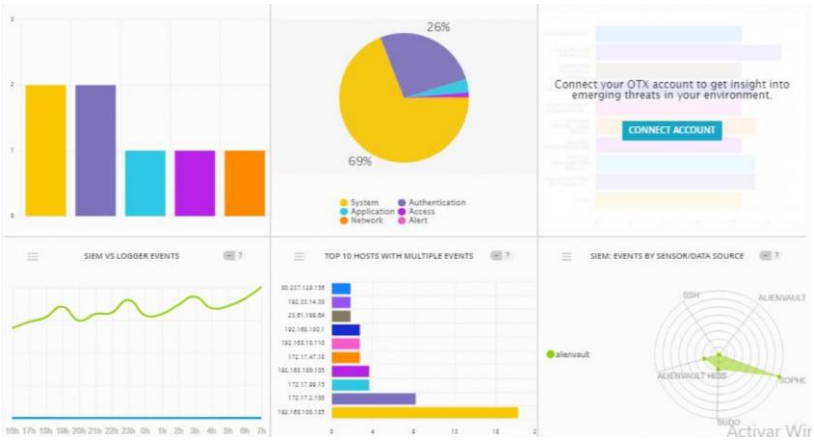

Figura 45. Correlación de eventos