FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

DESARROLLO DE GUÍA TÉCNICA PARA LA IMPLEMENTACIÓN DE SEGURIDAD DE REDES EN UNA ORGANIZACIÓN

AUTORES

ÁNGEL DANIEL SARITAMA RODRÍGUEZ

ESTEFANÍA ELIZABETH SALAZAR DUQUE

AÑO

2017

FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

DESARROLLO DE GUÍA TÉCNICA PARA LA IMPLEMENTACIÓN DE SEGURIDAD DE REDES EN UNA ORGANIZACIÓN.

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

Profesor Guía

Mg. William Eduardo Villegas Chiliquinga

Autores

Ángel Daniel Saritama Rodríguez

Estefanía Elizabeth Salazar Duque

Año

2017

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con los estudiantes, 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”.

_____

William Eduardo Villegas Chiliquinga
Magister en Redes de Comunicaciones
CI: 1715338263

DECLARACIÓN DEL PROFESOR CORRECTOR

“Declaro haber revisado este trabajo, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Ángel Gabriel Jaramillo Alcázer
Magister en Gerencia de Sistemas y Tecnologías de la Información.
CI: 1715891964

DECLARACIÓN DE AUTORÍA DE LOS ESTUDIANTES

“Declaramos que este trabajo es original, de nuestra 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”.

_____	_____
Ángel Daniel Saritama Rodríguez	Estefanía Elizabeth Salazar Duque
CI: 1104788425	CI: 1722379318

AGRADECIMIENTOS

A Dios por la fortaleza y sabiduría que me brinda día tras día y a mis padres por todo el apoyo brindado durante todo el transcurso de la carrera, gracias a ellos he logrado terminar una etapa muy importante en mi vida profesional.

Estefanía Salazar

AGRADECIMIENTOS

A todas las personas que me brindaron su apoyo durante todo este tiempo. De especial manera a mi familia por cada palabra de aliento.

Daniel Saritama

AGRADECIMIENTOS

A los Ingenieros William Villegas y Ángel Jaramillo por su ayuda, asesoramiento y disponibilidad que han tenido en todo momento.

Daniel, Estefanía

DEDICATORIA

A mis padres y hermana por apoyarme en cada momento difícil y ayudarme a seguir adelante para cumplir mis metas.

Estefanía Salazar

DEDICATORIA

A mis padres por todo el apoyo brindado desde el primer paso y a mi hermano y cuñada por estar presentes en todo momento.

Daniel Saritama

RESUMEN

La seguridad de la información es hoy en día un pilar fundamental en el mundo empresarial, las cuales día a día pueden verse vulneradas en cuanto a confidencialidad, disponibilidad e integridad de su información.

Cuando la información es confidencial las empresas siempre tiene la inquietud de que alguien pueda sustraérsela aprovechándose de las vulnerabilidades de los sistemas, con el fin de perjudicar a sus semejantes, por ello se debe contar con medidas de seguridad para prevenir estos robos de información, ya sea mediante el uso de políticas de seguridad en la organización o de herramientas de seguridad en los sistemas, también verificar que posibles vulnerabilidades pude existir y saber cómo mitigar los riesgos evitando en su totalidad la injerencia de intrusos.

La seguridad de la información muchas veces no se da en su totalidad, pero si se puede tener en su gran mayoría gracias a las nuevas técnicas y herramientas que se han ido consiguiendo con el pasar de los años.

Este trabajo de titulación toma en consideración la seguridad de redes, en donde las empresas pueden estar seguras de que su información valiosa va a estar protegida, para lo cual se elaborará una investigación de las características, parámetros y técnicas necesarias para la protección de la información.

ABSTRACT

Information security is nowadays a fundamental pillar in the business world, which from day to day may be violated as to the confidentiality, availability and integrity of its information.

When the information is confidential companies always have the concern that someone can take it away exploiting the vulnerabilities of the systems, in order to harm their fellow men, so it must have security measures to prevent these information theft, and Either through the use of security policies in the organization or security tools in the systems, also verify that possible vulnerabilities may exist and know how to mitigate the risks by completely preventing intrusion of intruders.

Information security often does not occur in its entirety, but it can be had in large part thanks to the new techniques and tools that have been achieved over the years.

This titling work takes into account network security, where companies can be assured that their valuable information will be protected, for which an investigation of the characteristics, parameters and techniques necessary for the protection of information will be developed.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. Capítulo I. Introducción

1.1. Anteproyecto

1.1.1. Alcance

Al presente trabajo de titulación estará enfocado en la elaboración de una guía técnica para la implementación de seguridad de la red en una organización, esta contará con los procedimientos a detalle necesarios para el aseguramiento de la misma.

La guía técnica a desarrollarse se basará en la identificación de los componentes, características y parámetros necesarios para brindar una respuesta a los problemas de seguridad dentro de una red empresarial.

Además, se detallarán las distintas técnicas tales como: el control de acceso a las redes (NAC), así como también el uso de herramientas de seguridad para la prevención y detección de intrusos.

Finalmente tomaremos como un caso de estudio para la implementación de la guía técnica, el datacenter académico de la UDLA.

1.1.2. Justificación

En la actualidad, la seguridad informática se ha vuelto una pieza fundamental en el entorno empresarial, y esta ha sido el incentivo del desarrollo de este trabajo de titulación. En esta investigación se elabora una propuesta sustentada en una guía viable para satisfacer las necesidades de una organización, ya que lo que se desea proyectar es una visión clara y precisa del porqué y cómo implementar seguridad en las redes.

El impacto que genera el proyecto es relevante ya que el tema abordado implica un beneficio para las organizaciones que quieren mejorar la seguridad en sus comunicaciones.

1.1.3. Objetivo General

Realizar una guía técnica para la implementación de seguridad de redes en una organización.

1.1.4. Objetivos Específicos

- Determinar las características, parámetros y técnicas necesarias para la protección de las redes de información en las organizaciones.

- Desarrollar una guía técnica con procedimientos que puedan ser utilizados con fines prácticos en una organización.

- Implementar la guía técnica en un caso de estudio enfocado al datacenter académico de la UDLA.

1.2. Introducción a la seguridad de redes

“La seguridad de redes consiste en las políticas adoptadas para prevenir y monitorear el acceso no autorizado, el mal uso, la modificación o la denegación de una red de computadoras y recursos de acceso de red”. (Cisco, 2016)

Tal y como se muestra en el Figura 1, existen varios tipos de amenazas que más adelante serán detalladas.

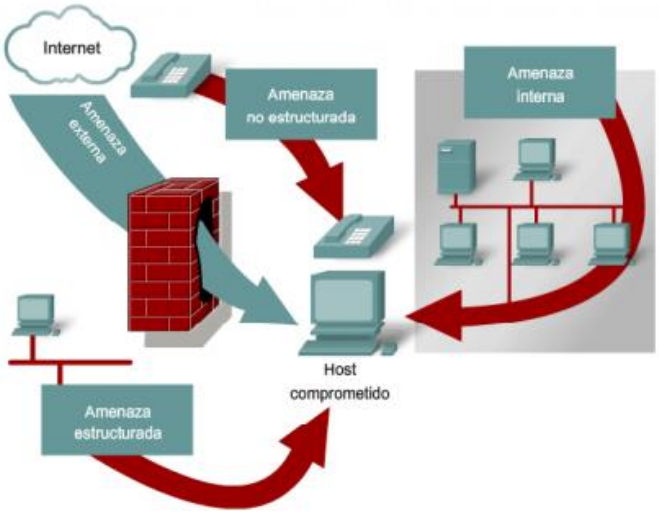

Figura 1. Amenazas más comunes en redes empresariales.

Tomado de (Cisco, 2016)

La seguridad de la información no es más que salvaguardar la información de acuerdo a cinco principios mediante procesos sustentados en políticas de seguridad mismos que faciliten el control adecuado de los datos en una organización.

1.3. Principios de la seguridad de la información

1.3.1. Confidencialidad

La confidencialidad trata de la urgencia que tienen las empresas para que su información sea privada para las personas desconocidas, el uso de protocolos de seguridad es fundamental para que los datos estén seguros. (Flores & Puppi, 2013)

1.3.2. Integridad

La integridad de la información no es más que hacer que los datos permanezcan inalterados a menos que sean controlados y modificados por personal autorizado y estos cambios sean auditados. (Flores & Puppi, 2013)

1.3.3. Disponibilidad

La disponibilidad de la información, es la capacidad para que la misma esté disponible 24 horas los 365 días al año.

1.3.4. Autenticidad

La autenticidad de la información es importante ya que obliga al usuario a proporcionar información verdadera. Uno de los métodos que permite garantizar la autenticidad es la firma electrónica. (Flores & Puppi, 2013)

1.3.5. Control

El control es el encargado de certificar que solamente las personas que tengan autorización puedan elegir cuando acceder a la información. (Flores & Puppi, 2013)

1.4. Tipos de Seguridad

Dentro de cualquier organización se ha vuelto de lo más común disponer de una red de comunicaciones para interconexión de equipos, sea cual sea el enfoque del negocio. Esta red permite brindar los distintos servicios que la empresa necesite, así esta no sea robusta. (Garzón, 2015)

Hoy en día se ha vuelto muy esencial una conexión a la red para la realización de procesos, facilitando así la manera de trabajar de sus empleadores compartiendo recursos y datos en red, así como también el proporcionar un acceso hacia el internet con el uso de varios servicios. (Garzón, 2015)

Sin embargo, al tener esta conexión local y global, se descartan muchos factores de más importancia como son los datos y su aseguramiento. Pues dependiendo la perspectiva, se puede decir que los datos son el bien más importante dentro

de una empresa. La mayor parte de las organizaciones cuentan con servidores llenos de información crucial la cual depende un 100% de los negocios que se realizan día a día. (Garzón, 2015)

La seguridad viene a ser un elemento muy importante dentro de una red de información en una organización, es por ello que se podrá clasificarla en dos tipos:

- Seguridad Física.
- Seguridad Lógica.

1.4.1. Seguridad Física

Según Richard Kissel, en su glosario de términos, define a la seguridad física como: “La aplicación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas contra las amenazas a los recursos y la información confidencial.” (Kissel, 2013)

Es decir, son todos los mecanismos de prevención y detección ante cualquier amenaza sobre todos los equipos físicos dentro de una organización que forman parte de directa o indirectamente con la red de comunicación.

Es verdad que es muy importante, no obstante, es el módulo menos implementado en distintas organizaciones. Al ser un aspecto muy vulnerable por su facilidad de acceso, en caso de estar mal implementado, es más propenso a ataques.

Existen muchos aspectos a tomar en cuenta antes de la instalación de todos y cada uno de los equipos que conforman la red, además de su futuro control y monitoreo, tal y como lo describe el “Grupo de Seguridad Corporativa” detallado en la figura 2. Es por ello que para muchas compañías es de vital importancia el control de acceso a todos estos equipos instalados en las distintas partes del

edificio, y sobre todo al centro de datos (datacenter) de la empresa. (Garzón, 2015)

Figura 2. Estudio de Seguridad Física.

Tomado de (GSC, s.f.)

Sin embargo, no necesariamente un atacante puede ser el único que pueda afectar a los equipos físicamente; existen varios factores externos, incluyendo desastres naturales, o fallas en los mismos equipos por los que estos se pueden ver perjudicados.

Debemos tener en cuenta que, aunque la organización cuente con herramientas y mecanismos de seguridad robustos, nuestra red en un momento determinado será nula si no se previene ante un desastre o ataque físico. A continuación, se detallarán algunos aspectos a tomar en cuenta con respecto a este tipo de seguridad.

1.4.1.1. Control de acceso a equipos

Entre las principales causas por las que se producen ataques físicos provocados por el hombre, es debido a la falta de control para poder acceder a los laboratorios y equipos dentro de una organización. Como se mencionó anteriormente, si un atacante puede llegar físicamente a nuestra información, la

seguridad lógica quedará incapacitada para cualquier bloqueo, logrando así modificar, destruir o simplemente leer la información de nuestros equipos. Visto desde este panorama la seguridad lógica va a depender de cierta seguridad física para mantener nuestra información a salvo. (Bustamante, 2013)

Es por ello que se implementan distintas políticas de seguridad para brindar autorización para que ciertas personas tengan acceso a las instalaciones donde se encuentra toda la información. Esto generalmente se controla con la portación de credenciales especiales de acceso y el uso de una tarjeta o llave específica para el ingreso a los laboratorios de cómputo y distintos equipos equipados en la red empresarial. (Bustamante, 2013)

1.4.1.2. Desastres naturales

El control de acceso a usuarios no restringidos no es el único motivo por lo cual implementar seguridad física en nuestro centro de datos y equipos instalados. Pues al ser muy poco comunes, dependiendo la zona, los desastres naturales se pueden presentar en un momento inesperado, y si lo haces puede causar daños muy perjudiciales si no se tiene una debida prevención de ellos. (Bustamante, 2013)

Los más comunes son:

- Terremotos.
- Inundaciones.
- Tormentas eléctricas, entre otros.

Al ser desastres que al presentarse puedan causar fallas parciales o totales de nuestros equipos, debemos realizar un estudio de las posibilidades de presentarse cualquiera de estos para su respectiva prevención.

En el caso de los terremotos, la ubicación de los laboratorios será un factor muy importante al momento de determinar si es factible montar toda una

infraestructura lo suficientemente segura para soportar este desastre, pues las vibraciones que éste forma pueden dañar cualquier elemento electrónico en los equipos causando daños y hasta pérdida de información. (Bustamante, 2013)

Por otra parte, las inundaciones al igual que las tormentas eléctricas, son factores muy peligrosos para todo equipo electrónico que se encuentre atado a la red local; dado el caso en que alguno esté en contacto con el agua o haya sido afectado por un rayo, pueden provocar desde la avería parcial del componente, hasta un cortocircuito masivo que puede apagar toda nuestra red causando un daño irreparable. (Bustamante, 2013)

1.4.1.3. Desastres del entorno

Los desastres de entorno se producen dentro de los laboratorios de informática o en el lugar donde se encuentran instalados los equipos, provocando desastres por causas externas a las acciones del hombre, o al menos indirectamente. (Bustamante, 2013)

Existen muchos desastres que se pueden presentar, pero entre los principales están:

- **Electricidad**

  Lo que se refiere a las instalaciones eléctricas comúnmente se presentan problemas con las subidas de tensión, pues, aunque sea por unos milisegundos, el cambio de voltaje entrante que un equipo recibe puede sobrepasar el mínimo soportado, causando así daños o cortocircuitos en los componentes del mismo. (Bustamante, 2013)

  La pérdida de datos en este tipo de inconvenientes no es muy común, pues la mayor parte de equipos cuentan con fusibles, reguladores de voltaje o hasta UPS’s instalados en la empresa. Sin embargo, los cortes constantes

de energía pueden causar daños en el software irrecuperables. (Bustamante, 2013)

- **Incendios**

Dentro de un centro de cómputo, los incendios vendrán usualmente relacionados con los cortocircuitos eléctricos. Por una parte, éstos pueden ser producidos por algún desastre natural, además también pueden ser ocasionados por problemas en los equipos conectados causando problemas eléctricos en el mismo y provocando este desastre. (Bustamante, 2013)

- **Ruido eléctrico**

El ruido eléctrico es un problema que se genera muy común en los equipos por la incidencia de máquinas externas que afectan a su funcionamiento. Es verdad el ruido eléctrico no lo producirán equipos pequeños, debido a que estos no generan demasiadas cantidades de ruido, sino maquinaria pesada o motores que se encuentren cerca. La ubicación correcta de esta maquinaria es fundamental para evitar los problemas con los equipos de la empresa. (Bustamante, 2013)

1.4.1.4. Prevención

Para la prevención de ataques físicos existen mecanismos como: “analizadores de retina o huella, hasta videocámaras, tarjetas inteligentes o control de llaves que abren una puerta en específico” (RedIRIS, 2002), los cuales dependiendo el grado de criticidad de su información son implementados para su seguridad.

Existen normas como la ISO 27001 que recomiendan una serie de controles para la prevención de intrusos a las instalaciones físicas donde se encuentran los equipos. Por otra parte, con un buen cableado estructurado y mantenimiento del

mismo se pueden prevenir a futuro tanto daños como accesos no autorizados es estos.

1.4.1.5. Detección

La detección es un concepto que va de la mano con la prevención, pues en caso de implementar la prevención, por cualquier motivo sea económico o humano, se debe potenciar la detección de amenazas. (Bustamante, 2013)

La detección de accesos no autorizados a los equipos es lo más crítico para la implementación de seguridad, es por ello que se opta por la instalación de cámaras de seguridad, alarmas o en casos más extremos el uso de personal de vigilancia. (Bustamante, 2013)

1.4.1.6. Protección de datos

Como se mencionó al inicio de este capítulo, una de las causas del robo de información es por medio de la intrusión física a los equipos de la red, tanto a la información guardada en los servidores, así como la que puede ser interceptada mientras se transmite por red. (Bustamante, 2013)

En esta sección se habló de algunas técnicas e implementaciones que se realizan en una empresa para la protección de equipos físicos de la red, esto conlleva implícitamente a la protección de los datos.

Tanto la detección y prevención, los controles y las políticas implementadas serán de primordial importancia para mantener los datos resguardados ante ataques naturales o humanos.

1.4.2. Seguridad Lógica

Como se ha venido mencionando anteriormente, la implementación de seguridad dentro de una red tiene como principal objetivo el resguardo y protección de los

datos. Pues, la red al ser muy vulnerable hacia distintas amenazas y ataques, es necesario la aplicación de distintos procedimientos que logren brindar un uso efectivo de la misma, así como garantizar la integridad, disponibilidad y confidencialidad de la red en sí y de la información. (Bustamante, 2013)

Una vez detallados los procedimientos necesarios para poder asegurar los equipos físicos que conforman la red organizacional, es importante puntualizar que, a pesar de tener una buena infraestructura armada, la mayoría de ataques son realizados a través de los puntos vulnerables en la red, al ser un medio más factible y rápido con las herramientas y conocimientos adecuados. (Bustamante, 2013)

Siendo así, la seguridad física solo será un punto a tomar en cuenta al momento de querer proteger nuestra red, puesto que los ataques lógicos, en su mayor parte, estarán orientados a la información almacenada en los servidores y a cómo está siendo procesada.

Debido a la gran cantidad de amenazas, no existe una solución única y eficaz que permita la protección total de nuestro sistema de red, es por ello que se han establecido el uso de algunos componentes, que al trabajar conjuntamente logren minimizar el mantenimiento y mejorar la red, entre los cuales está: (Bustamante, 2013)

- El uso de herramientas que permitan mantener la información segura ante cualquier intento de robo, garantizando la confidencialidad, integridad y disponibilidad de los datos.

- Implementación de políticas de seguridad que permitan tener un control del uso correcto de la red.

- Protocolos de control de autenticación de usuarios que necesiten tener conexión a distintos equipos.

- Medidas de detección y prevención de intrusos.
- Instalación de herramientas y mecanismos, tanto físicos como lógicos, que logren favorecer con el aseguramiento de la red.

1.4.2.1. Controles de acceso interno

A igual que en la seguridad física, el control de acceso es el proceso que se realiza dentro del sistema que permite verificar la legitimidad de los usuarios que intenten ingresar a la red de datos interna y además protegerlos ante cualquier amenaza que pretenda afectar su integridad. Estos controles podrán implementarse tanto en la red, en el sistema operativo, en la información en sí o en cualquier otro aplicativo o recurso según sea lo requerido. (Bustamante, 2013)

Con respecto a los estándares de seguridad al referirse al control de acceso, algunas instituciones como el Instituto Nacional de Estándares y Tecnología (NIST) y la Organización Internacional de Normalización (ISO), hablan sobre los requisitos mínimos que una red debe tener para aplicar control en la red interna, entre los que se puede resaltar los siguientes campos los cuales en capítulos posteriores se profundizarán más a detalle:

- Manejo de roles.
- Permisos.
- Limitación de servicios.
- Encriptación de datos.
- Etiquetas de seguridad.

Cabe recalcar que la implementación de estos estándares dependerá del grado de seguridad que necesitemos en nuestra red, ya que éstos son simplemente una guía para el diseño de seguridad a manejar.

1.4.2.2. Controles de acceso externo

Estos controles estarán enfocados a la protección lógica de la red de datos con respecto a los diferentes servicios y usuarios externos a la organización que deseen acceder al sistema. (Bustamante, 2013)

De igual manera, existen algunas técnicas que se pueden implementar en la red para brindar la protección necesaria, tal como:

- Firewalls.
- Control de accesos públicos.
- Sistemas de detección y prevención de intrusos.

1.4.2.3. Políticas de Seguridad

Para poder implementar un sistema casi al cien por ciento seguros en una organización es necesaria la inversión de mucho dinero para costear todos los equipos y herramientas requeridas. Sin embargo, debido a la falta de interés o capital, se optan por otras opciones momentáneas y necesarias para delimitar todo el espectro de seguridad en la red. (Bustamante, 2013)

Por lo tanto, la aplicación de procedimientos y estrategias como directrices y recomendaciones en una organización podrá facilitar el uso de las distintas tecnologías y procesos implementados, evitando así el manejo inadecuado de los mismos y aprovechando de mejor manera las características que nos brindan. (Bustamante, 2013)

La mayor parte de las empresas optan por la documentación de todas estas directrices, teniendo así constancia de todo lo detallado y además tener un control sobre todos los miembros de la institución. Con esto se quiere concientizar a todos los usuarios sobre la importancia de los recursos a su disposición y la sensibilidad de la información a manejarse. (Bustamante, 2013)

1.5. Niveles de Seguridad Informática

Los niveles de seguridad informática (figura 3), “han sido la base de desarrollo de estándares europeos (ITSEC/ITSEM) y luego internacionales”. (DoD, 1985)

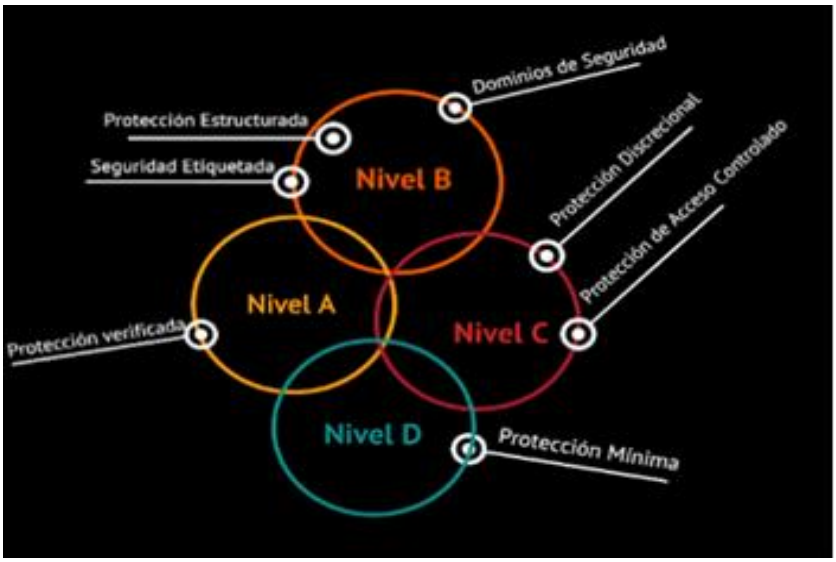

Figura 3. Niveles de Seguridad Informática.

Tomado de (TCSEC, 1985)

1.5.1. Nivel D

“Este nivel contiene solamente una división y está reservada específicamente para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad. Es decir, sistemas que no son confiables, no tienen protección para el hardware, el sistema operativo es inestable y no tiene autenticación. Los sistemas operativos que corresponden a este nivel son MS-DOS y System 7.0 macintosh”. (Pacheco, s.f.)

1.5.2. Nivel C1

“En este nivel los usuarios requieren identificación lo cual les va a permitir el acceso a diferente información, cada usuario puede tener su información reservada y se hace la distinción entre los usuarios y el administrador del sistema que es el que tiene el control total del sistema”. (Pacheco, s.f.)

1.5.3. Nivel C2

“El administrador del sistema puede autorizar que usuario ejecutará ciertos comandos o a que archivos acceder dentro del sistema. Algunos usuarios de un sistema C2 cuentan con la autorización para realizar algunas tareas administrativas, sin necesidad de ser administradores del sistema. Por lo mismo es necesario que en este nivel exista auditoria la cual es utilizada para llevar registros de cada acción que se realiza en el sistema”. (Pacheco, s.f).

1.5.4. Nivel B1

“Este nivel soporta seguridad multinivel: secreta y ultra secreta. Aquí se establece que el dueño de un archivo no podrá modificar permisos de un objeto que esté bajo el control de acceso obligatorio. Para esto a cada objeto del sistema, se le asigna una etiqueta con un nivel de seguridad jerárquico (alto, secreto, reservado etc.) y con diferentes categorías. Cada usuario que accede a un objeto debe poseer un permiso, es decir que cada uno tiene sus objetos asociados”. (Pacheco, s.f).

1.5.5. Nivel B2

En este nivel se requiere que todos los objetos del sistema estén etiquetados de manera jerárquica, los recursos como discos, archivos, terminales pueden tener asignados uno o varios niveles de seguridad. Los usuarios no solo necesitan el control de acceso discrecional obligatorio, sino también un control obligatorio según etiquetas. (Pacheco, s.f.)

Las etiquetas dependen de las políticas de seguridad determinado por el sistema administrador, que clasifica a sujetos y objetos en niveles de seguridad que deben estar basados en una documentación clara y formal. (Pacheco, s.f.)

1.5.6. Nivel B3

“Hay un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega según las políticas de acceso que estén definidas. Este nivel requiere que la terminal del usuario se conecte al sistema por medio de una conexión segura. Asimismo, cada usuario tiene asignado los lugares y objetos a los que puede acceder”. (Pacheco J, s.f.)

1.5.7. Nivel A

“Es importante saber que este nivel incluye todos los niveles de seguridad anteriores. Asimismo, es el nivel más elevado, ya que incluye el proceso de diseño, control y verificación del sistema, mediante métodos formales (matemáticos)”. (Pacheco J, s.f).

Además, añade confiabilidad con un análisis formal y demostración matemática asegurando todos los procesos que el usuario realice en el sistema.

1.6. Vulnerabilidad en Redes

Las vulnerabilidades no son más que condiciones que permiten un ataque a la seguridad dentro de las redes en una organización. (Bustamante, 2013)

1.6.1. Inseguridad en un sistema

- Uno de los más sencillos modos para acceder a la red de una organización puede ser los puntos de acceso remoto que no seguros.
- La filtración de la información puede facilitar al atacante la versión del S.O y de las aplicaciones.
- Servicios ejecutados por los usuarios como: FTP, DNS y SMTP que dejan vulnerabilidades en el sistema.

- Puede estar en peligro la seguridad de los servidores las contraseñas sencillas o reutilizadas.
- Las cuentas de usuario de prueba con excesivos privilegios pueden poner en peligro la información de la empresa.
- Los servidores de internet mal configurados.
- Las aplicaciones que no tengan parches o que se hayan dejado con configuraciones predeterminadas.
- Los servicios sin un control de acceso requerido.
- La capacidad de registro y la detección inadecuada a nivel de red y de host.

1.7. Amenazas en la información

A continuación, se detallan las amenazas que puede presentar una organización al no tener seguridad en sus datos:

1.7.1. Robo

Hoy en día, las computadoras son instrumentos valiosos de todas las empresas ya que guardan información importante y confidencial de las mismas, por esta razón es una propiedad fácilmente de robar o sustraer información que no esté protegida sin dejar ningún rastro. (Bustamante, 2013)

1.7.2. Fraude

Anualmente, miles de dólares son despojados de las organizaciones y las computadoras son utilizadas con estos fines. Al final esto provoca una mala

imagen de la empresa ya que esta se involucra en este tipo de situaciones desagradables. (Bustamante, 2013)

1.7.3. Sabotaje

Este es uno de los peligros más graves que presentan las empresas ya que a pesar de que configuran programas relacionados con la seguridad, la protección contra el saboteador es uno de los retos más grandes. (Bustamante, 2013)

1.8. Tipos de delitos informáticos

1.8.1. Delitos y modificaciones cometidos a los sistemas informáticos

1.8.1.1. Alteración de la información

Este es uno de los delitos informáticos más comunes, debido a que es sencillo de cometer y dificultoso de descubrir.

1.8.1.2. Manipulación de programas

Trata sobre la modificación de programas que ya existen o en incluir nuevos programas al sistema. Este delito es muy complicado de descubrir y frecuentemente atraviesa inadvertido ya que los infractores una persona que tiene conocimientos técnicos. (Bustamante, 2013)

1.8.1.3. Manipulación de los datos de salida

Consiste en dañar el funcionamiento del sistema, esto se lo hace mediante la falsificación de instrucciones a las computadoras para sustraer datos confidenciales. (Bustamante, 2013)

1.8.1.4. Fraude efectuado por manipulación informática

Consiste en sacar información importante del sistema en especial de cuentas bancarias, se aprovecha de las repeticiones automáticas del sistema y transfiere datos de una cuenta a otra. (Bustamante, 2013)

1.8.1.5. Sabotaje informático

Trata acerca de la modificación o eliminación de información importante y confidencial del sistema sin consentimiento, obstaculizando el funcionamiento del sistema. (Bustamante, 2013)

1.8.1.6. Acceso no autorizado a sistemas y recursos informáticos

Consiste en ingresar al servidor de políticas de la empresa y brindar accesos al sistema a personas no autorizadas. (Bustamante, 2013)

1.9. Ataques a la seguridad de redes

1.9.1. Identificación de atacantes

En todos los sistemas de red de datos, o al menos en la mayoría, existen agujeros de seguridad, en los cuales es muy probable que sean detectados por personas que, intencionalmente, desean infiltrarse en la red. (Bustamante, 2013)

Hoy en día existen un sin número de personas dedicadas a encontrar esos huecos en las distas redes organizacionales, es por eso que dependiendo sus intenciones se han llegado a clasificar en algunos tipos.

1.9.1.1. Hackers

El término Hacker alrededor del mundo es el más escuchado para las personas que no saben mucho sobre el tema ya que generalmente lo asocian como el

conjunto de todos los atacantes cibernéticos, no obstante, su definición dentro de la informática es muy distinto. (Gómez, s.f.)

Los hackers son intrusos que poseen un amplio grado de conocimientos acerca de informática y redes, los cuales los aprovechan para infiltrase dentro de los sistemas sin un fin más allá de poner a prueba sus habilidades, ya que ellos no pretenden hacer ningún tipo de daño. Por lo contrario, luchan en contra de los softwares pagados y buscan la difusión libre de todo tipo de información. (Gómez, s.f.)

Al ser un pasatiempo muy extenso debido a que ninguna red es igual, los hackers buscan siempre estar al día en nuevos métodos de infiltración discreta, pues su intención primordial es romper todas las barreras e introducirse en el sistema, es por ello que a pesar de que sea por simple curiosidad, sigue siendo ilegal y es un delito si llegan a ser detectados. (Gómez, s.f.)

1.9.1.2. Crackers

A diferencia de los Hackers, lo Crackers tienen un fin más allá de la investigación o de poner a prueba sus habilidades. Pues ellos, sea cual sea el motivo (intereses económicos, políticos, venganza, etc.), logran infiltrarse a la red de una empresa con la intención de realizar algún daño, obteniendo así beneficios de forma ilícita. (Gómez, s.f.)

1.9.1.3. Sniffers

Los Sniffers generalmente buscan el robo de la información rastreando los paquetes que circulan por medio de la red. Interceptan los datos y los decodifican para así obtener toda la información deseada. (Gómez, s.f.)

1.9.1.4. Spammers

Es un término muy conocido en estos días, ya que estas personas se dedican al envío simultáneo y masivo de solicitudes hacia un sistema en específico, provocando la sobrecarga de procesos y, como consecuencia, el colapso de los servidores. (Gómez, s.f.)

Comúnmente estas personas realizan sus ataques a los usuarios de correos electrónicos, pues en su mayoría intentan enviar códigos maliciosos (virus) o a su vez realizan intentos de estafa por internet (phishing). (Gómez, s.f.)

1.9.1.5. Piratas informáticos

Los piratas informáticos se dedican a la copia y reproducción ilícita de programas o contenido multimedia, con el fin de su distribución ilegal gratuita o a menor costo. En muchos países es un delito penado ya que infringe con la propiedad intelectual. (Gómez, s.f.)

1.9.2. Tipos de ataques

Debido a los distintos tipos de seguridades que existen dentro de una red en una organización, se he llegado a ser difícil de penetrar todas estas barreras por parte de los atacantes cibernéticos para poder obtener y robar información. Hoy en día hay un sin número de técnicas y herramientas que les permiten violar todas estas seguridades para cumplir con sus propósitos. A continuación, se detallarán los tipos de ataques más comunes. (Gómez, s.f.)

1.9.2.1. Ingeniería Social

Al estar diseñada una red con tanta impenetrabilidad vieron la necesidad de usar otros recursos para acceder a ella. Siendo así su principal enfoque hacia las

personas, al ser el recurso más vulnerable que una empresa puede tener con acceso a la información de la misma. (Gómez, s.f.)

La ingeniería social es definida como la acción de manipular a las personas para esquivar los sistemas de seguridad de una organización. Pues, los atacantes usan la persuasión y manipulación psicológica para así aprovecharse de la inocencia de cualquier usuario trabajador en una empresa, sin importar su cargo o importancia dentro de ella. (Gómez, s.f.)

Para poder realizar estos ataques se usa, como generalmente se lo conoce, un motivador, el cual será el ancla entre atacante y la víctima. (Gómez, s.f.)

En la ingeniería social se utilizará este motivador para los siguientes puntos:

- Llamar la atención de la víctima.
- Ganarse su confianza.
- Medir sus capacidades y conocimientos.
- Generar una distracción.
- Sacar información personal del usuario.

Finalmente, con toda la información obtenida del usuario, el atacante tendrá todos los recursos necesarios para proceder con el acceso, tanto físico o lógico, a la información requerida.

1.9.2.2. Ataques de día cero

El reconocido antivirus ESET denomina al ataque de día cero como: “Una nueva vulnerabilidad para la cual no se crearon parches o revisiones, y que se emplea para llevar a cabo un ataque. El nombre 0-day (día cero) se debe a que aún no existe ninguna revisión para mitigar el aprovechamiento de la vulnerabilidad.” (ESET, 2005)

Estos ataques estarán de la mano con las vulnerabilidades del sistema, pues dependerá mucho de las seguridades previamente establecidas en la red.

1.9.2.3. Análisis de tráfico

Este tipo de ataques están enfocados en todos los tipos de tráficos que circulan por una red, pues utilizan herramientas como los "*sniffers*" para poder interceptar toda la información sin que esta sea alterada de alguna manera. Estos ataques se aprovechan de la falta de control de acceso a la red, tanto de hardware como software. (Gómez, s.f.)

1.9.2.4. Ataques de denegación de servicio (DoS)

Los ataques de denegación de servicio han sido de los más letales para muchas compañías en los últimos tiempos, pues si se logra burlar las seguridades y tener acceso a la red, enviar uno de estos ataques puede causar pérdidas enormes en las compañías. Tienen como fin imposibilitar los sistemas y recursos dentro de una organización con el envío masivo de peticiones (spam) a los servidores hasta su colapso. (Gómez, s.f.)

Hay dos tipos de ataques DoS muy conocidos, estos son:

- Denegación de servicio por saturación.
- Denegación de servicio por explotación de vulnerabilidades.

Su objetivo no es el robo ni alteración de la información, simplemente es común realizarlo para causar pérdidas económicas y daño en la reputación de las empresas; pues al alterar los servidores, también afectará a todos los servicios utilizados por los usuarios interesados. (Gómez, s.f.)

2. Capítulo II. Normas y políticas de seguridad de la información

Según la ISO en la norma 27001 especifica que el objetivo de las políticas de seguridad es: “Proporcionar orientación y apoyo a la gestión de seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normas pertinentes.” (INEN-ISO/IEC, 2016)

Se tomarán algunos conceptos en cuenta para el mejor entendimiento de las normas de seguridad, entre ellos son:

- **ISO**

Según la Norma Técnica Ecuatoriana NTC-ISO 27005, define a la ISO como: “La ISO (Organización Internacional de Normalización) e IEC (la Comisión Electrotécnica Internacional) constituyen el sistema especializado para la normalización a nivel mundial.

Los organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de normas internacionales a través de comités técnicos establecidos por las organizaciones respectivas para realizar acuerdos en los campos específicos de la actividad técnica”. (INEN-ISO/IEC, 2016)

- **Generalidades**

Es necesario e importante que el sistema de gestión de seguridad de la información este integrado con todos los procesos de la empresa, así mismo con la estructura global que esta tenga. (INEN, 2006)

La norma internacional podrá ser utilizada tanto internamente como externamente para la evaluación de las capacidades de la organización para así cumplir con los requisitos de seguridad que esta tenga. (INEN, 2006)

- **Metodología de un SGSI según ISO 27001**

A continuación, se muestra en la (Figura 4) un diagrama explicativo acerca de la metodología de un SGSI según ISO 270001.

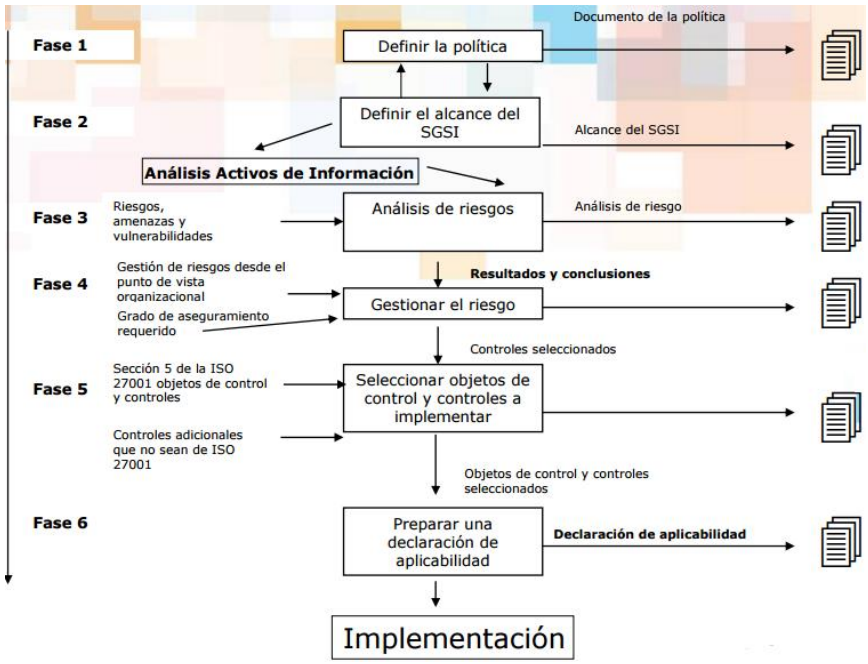

Figura 4. Metodología de un SGSI.

Tomado de (Normas ISO 27001, 2005)

A continuación, en la tabla 1, se detallan las normas establecidas por la ISO 27001 las cuales serán aplicadas para el análisis de las políticas de seguridad que se enfocan a la red.

Tabla 1.

Identificación de Políticas de Seguridad orientadas a redes

Identificación de Políticas de Seguridad enfocadas a las redes de información según normas 27001 y 27002		
Políticas de la seguridad de la información		
• Políticas de seguridad	✓ Aplica	
• Revisión de políticas	✓ Aplica	

Organización de la seguridad de la información		
Organización interna		
• Roles y responsabilidades en seguridad de la información	✓ Aplica	
• Segregación de tareas	✓ Aplica	
• Contacto con las autoridades	✓ Aplica	
• Contacto con grupos de interés especial	✓ Aplica	
• Seguridad de la información en la gestión de proyectos	✓ Aplica	
Los dispositivos móviles y el teletrabajo		
• Política de dispositivos móviles		❖ No Aplica
• Teletrabajo	✓ Aplica	
Seguridad relativa a los recursos humanos		
Antes del empleo		
• Investigación de antecedentes		❖ No Aplica
• Términos y condiciones del empleo		❖ No Aplica
Durante el empleo		
• Responsabilidades de gestión		❖ No Aplica
• Concienciación, educación y capacitación en seguridad de la información		❖ No Aplica
• Proceso disciplinario		❖ No Aplica
Finalización del empleo o cambio en el puesto de trabajo		
• Responsabilidades ante la finalización o cambio		❖ No Aplica
Gestión de activos		
Responsabilidad sobre los activos		
• Inventario de activos	✓ Aplica	
• Propiedad de los activos		❖ No Aplica
• Uso aceptable de los activos		❖ No Aplica
• Devolución de activos		❖ No Aplica
Clasificación de la información		
• Clasificación de la información		❖ No Aplica
• Etiquetado de la información		❖ No Aplica
• Manipulado de la información	✓ Aplica	
Manipulación de los soportes		
• Gestión de soportes extraíbles		❖ No Aplica
• Eliminación de soportes		❖ No Aplica
• Soportes físicos en tránsito		❖ No Aplica
Control de acceso		
Requisitos de negocio para el control de acceso		
• Política de control de acceso	✓ Aplica	

• Acceso a las redes y a los servicios de red	✓ Aplica	
Gestión de acceso de usuario		
• Registro y baja de usuario	✓ Aplica	
• Provisión de acceso de usuario		❖ No Aplica
• Gestión de privilegios de acceso	✓ Aplica	
• Gestión de la información secreta de autenticación de los usuarios		❖ No Aplica
• Revisión de los derechos de acceso de usuario	✓ Aplica	
• Retirada o reasignación de los derechos de acceso		❖ No Aplica
Responsabilidades del usuario		
• Uso de la información secreta de autenticación	✓ Aplica	
Control de acceso a sistemas y aplicaciones		
• Restricción del acceso a la información	✓ Aplica	
• Procedimientos seguros de inicio de sesión	✓ Aplica	
• Sistema de gestión de contraseñas	✓ Aplica	
• Uso de utilidades con privilegios del sistema	✓ Aplica	
• Control de acceso al código fuente de los programas	✓ Aplica	
Criptografía		
Controles criptográficos		
• Política de uso de los controles criptográficos	✓ Aplica	
• Gestión de claves	✓ Aplica	
Seguridad física y del entorno		
Áreas seguras		
• Perímetro de seguridad física		❖ No Aplica
• Controles físicos de entrada		❖ No Aplica
• Seguridad de oficinas, despachos y recursos		❖ No Aplica
• Protección contra las amenazas externas y ambientales		❖ No Aplica
• El trabajo en áreas seguras		❖ No Aplica
• Áreas de carga y descarga		❖ No Aplica

Seguridad de los equipos		
• Emplazamiento y protección de equipos	✓ Aplica	
• Instalaciones de suministro	✓ Aplica	
• Seguridad del cableado	✓ Aplica	
• Mantenimiento de los equipos	✓ Aplica	
• Retirada de materiales propiedad de la empresa		❖ No Aplica
• Seguridad de los equipos fuera de las instalaciones		❖ No Aplica
• Reutilización o eliminación segura de equipos		❖ No Aplica
• Equipo de usuario desatendido		❖ No Aplica
• Política de puesto de trabajo despejado y pantalla limpia		❖ No Aplica
Seguridad de las operaciones		
Procedimientos y responsabilidades operacionales		
• Documentación de procedimientos operacionales		❖ No Aplica
• Gestión de cambios		❖ No Aplica
• Gestión de capacidades		❖ No Aplica
• Separación de los recursos de desarrollo, prueba y operación		❖ No Aplica
Protección contra el software malicioso (malware)		
• Controles contra el código malicioso	✓ Aplica	
Copias de seguridad		
• Copias de seguridad de la información	✓ Aplica	
Registros y supervisión		
• Registro de eventos	✓ Aplica	
• Protección de la información de registro	✓ Aplica	
• Registros de administración y operación	✓ Aplica	
• Sincronización del reloj	✓ Aplica	
Control del software en explotación		
• Instalación del software en explotación		❖ No Aplica
Gestión de la vulnerabilidad técnica		
• Gestión de las vulnerabilidades técnicas		❖ No Aplica
• Restricción en la instalación de software		❖ No Aplica

Consideraciones sobre la auditoria de sistemas de información		
• Controles de auditoría de sistemas de información		❖ No Aplica
Seguridad de las comunicaciones		
Gestión de la seguridad de redes		
• Controles de red	✓ Aplica	
• Seguridad de los servicios de red	✓ Aplica	
• Segregación en redes	✓ Aplica	
Intercambio de información		
• Políticas y procedimientos de intercambio de información	✓ Aplica	
• Acuerdos de intercambio de información	✓ Aplica	
• Mensajería electrónica	✓ Aplica	
• Acuerdos de confidencialidad o no revelación	✓ Aplica	
Adquisición, desarrollo y mantenimiento de los sistemas de información		
Requisitos de seguridad en sistemas de información		
• Análisis de requisitos y especificaciones de seguridad de la información	✓ Aplica	
• Asegurar los servicios de aplicaciones en redes públicas	✓ Aplica	
• Protección de las transacciones de servicios de aplicaciones	✓ Aplica	
Seguridad en el desarrollo y en los procesos de soporte		
• Política de desarrollo seguro		❖ No Aplica
• Procedimiento de control de cambios en sistemas		❖ No Aplica
• Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo		❖ No Aplica
• Restricciones a los cambios en los paquetes de software		❖ No Aplica
• Principios de ingeniería de sistemas seguros		❖ No Aplica
• Entorno de desarrollo seguro		❖ No Aplica
• Externalización del desarrollo de software		❖ No Aplica
• Pruebas funcionales de seguridad de sistemas		❖ No Aplica

• Pruebas de aceptación de sistemas		❖ No Aplica
Datos de prueba		
• Protección de los datos de prueba	✓ Aplica	
Relación con proveedores		
Seguridad en las relaciones con proveedores		
• Política de seguridad de la información en las relaciones con los proveedores		❖ No Aplica
• Requisitos de seguridad en contratos con terceros		❖ No Aplica
• Cadena de suministro de tecnología de la información y de las comunicaciones		❖ No Aplica
Gestión de la provisión de servicios del proveedor		
• Control y revisión de la provisión de servicios del proveedor		❖ No Aplica
• Gestión de cambios en la provisión del servicio del proveedor		❖ No Aplica
Gestión de incidentes de seguridad de la información		
Gestión de incidentes de seguridad de la información y mejoras		
• Responsabilidades y procedimientos	✓ Aplica	
• Notificación de los eventos de seguridad de la información	✓ Aplica	
• Notificación de puntos débiles de la seguridad	✓ Aplica	
• Evaluación y decisión sobre los eventos de seguridad de información	✓ Aplica	
• Respuesta a incidentes de seguridad de la información	✓ Aplica	
• Aprendizaje de los incidentes de seguridad de la información	✓ Aplica	
• Recopilación de evidencias	✓ Aplica	
Aspectos de seguridad de la información para la gestión de la continuidad del negocio		
Continuidad de la seguridad de la información		
• Planificación de la continuidad de la seguridad de la información		❖ No Aplica
• Implementar la continuidad de la seguridad de la información		❖ No Aplica

• Verificación, revisión y evaluación de la continuidad de la seguridad de la información		❖ No Aplica
Redundancias		
• Disponibilidad de los recursos de tratamiento de la información	✓ Aplica	
Cumplimiento		
Cumplimiento de los requisitos legales y contractuales		
• Identificación de la legislación aplicable y de los requisitos contractuales		❖ No aplica
• Derechos de propiedad intelectual (DPI)		❖ No aplica
• Protección de los registros de la organización		❖ No aplica
• Protección y privacidad de la información de carácter personal		❖ No aplica
Revisiones de la seguridad de la información		
• Revisión independiente de la seguridad de la información		❖ No aplica
• Cumplimiento de las políticas y normas de seguridad	✓ Aplica	
• Comprobación del cumplimiento técnico		❖ No aplica

Tomado de (INEN, 2006)

Una vez analizadas las políticas enfocadas a las redes de comunicación referentes a la seguridad de la información, se procede a realizar un análisis más detallado de cada una de estas.

2.1. Políticas de la seguridad de información

2.1.1. Políticas de seguridad

“Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas distinguidas”. (INEN-ISO/IEC, 2016)

2.1.2. Revisión de políticas

Las políticas de seguridad de la información tienen que ser evaluadas periódicamente y siempre que exista algún cambio en la institución. (INEN-ISO/IEC, 2016)

2.2. Estructura para la seguridad de información

2.2.1. Estructura interna

Para el desarrollo de un sistema de gestión de seguridad se debe contar con una estructura de gestión bien establecida previo a la implementación y control de distintas políticas de seguridad en todas las áreas competentes dentro de la organización. (INEN-ISO/IEC, 2016)

Es recomendable y conveniente, en caso de requerirlo, la intervención de personal y grupos especialistas que ayuden con la implementación de todo un sistema de seguridad, pues una buena gestión será el inicio de un buen sistema de seguridad. (INEN-ISO/IEC, 2016)

2.2.1.1. Roles y responsabilidades

Cada acción por tomarse dentro de la organización deberá ser aprobada y gestionada por la dirección competente. (INEN-ISO/IEC, 2016)

La dirección será la responsable de certificar ya apoyar la eficacia de cada política creada, asegurando cumplir con los requerimientos de seguridad con que la empresa exige. Además, están comprometidos a realizar planes y programas que ayuden a mantener y mejorar la integridad de las políticas implementadas en la institución. (INEN-ISO/IEC, 2016)

Dentro de las organizaciones se procede con la asignación de roles para el uso de funciones laborales pertinentes. Con esta actividad se procura tener un mejor manejo de todas las actividades realizadas que puedan afectar directamente a la información, con modificaciones no autorizadas o uso indebido de la misma. (INEN-ISO/IEC, 2016)

2.2.1.2. Segregación de tareas

Es necesaria la retribución de la responsabilidad del control de la seguridad, pues con la colaboración de más personas se podrá distribuir por áreas la responsabilidad, para así tener un mejor control de seguridad de todas las funciones realizadas en la empresa. (INEN-ISO/IEC, 2016)

2.2.1.3. Contacto con autoridades

Ante la sospecha del incumplimiento de las políticas de seguridad o irrupción a la seguridad de la información, se deberá contar con un plan de soporte por parte de las autoridades pertinentes (sea policía, autoridades de la empresa, proveedor de servicio de internet, entre otros), para así tomar las acciones respectivas ante algún incidente. (INEN-ISO/IEC, 2016)

2.2.2. Terceros

Es de conocimiento que muchas empresas se valen y brindan servicios hacia organizaciones externas, las cuales generalmente necesitan el acceso a la red y el manejo de la información. Es por ello que se debe mantener acuerdos de seguridad con los terceros para mantener los datos seguros. (INEN-ISO/IEC, 2016)

2.2.2.1. Identificación de riesgos

Al compartir recursos e información con empresas externas, se deben definir los riegos que esto conlleva, imponiendo los controles respectivos antes de brindar el acceso. (INEN-ISO/IEC, 2016)

En el caso de requerir acceso a los recursos de la empresa, se deberán tomar en cuenta algunos aspectos para tener un mayor control:

- El tipo de acceso, sea lógico o físico, y a qué recursos.
- Los permisos otorgados sobre ese acceso.
- La información a la que se accede.
- Los acuerdos establecidos por los terceros para el manejo de la información, entre otros.

2.2.2.2. Acuerdos con terceros

Previo a la otorgación de permisos y accesos a los recursos, se debe revisar detalladamente los contratos existentes establecidos entre los terceros y la organización, controlando: (INEN-ISO/IEC, 2016)

- El cumplimiento total de políticas.
- Protección de los activos de la empresa, especialmente la información.
- Controles en la transferencia de información.
- Responsabilidades con el uso adecuado y mantenimiento de los servicios a disponer.
- Garantizar la protección de la red ante cualquier malware.
- Respetar los derechos de propiedad intelectual, y otros.

2.3. Seguridad relativa a los recursos humanos

2.3.1. Antes del empleo

“Consiste en certificar de que los empleados y contratistas comprendan sus responsabilidades y si son apropiados para las funciones encomendadas”. (INEN-ISO/IEC, 2016)

2.3.1.1. Antecedentes

“La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debe efectuar de acuerdo con las leyes, normas y códigos éticos que sean de aplicación y debe ser proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos”. (INEN-ISO/IEC, 2016)

2.3.1.2. Términos y condiciones del empleo

“De acuerdo a las obligaciones contractuales, los empleados y contratistas deben establecer los términos y condiciones de su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización”. (INEN-ISO/IEC, 2016)

2.3.2. Durante sus funciones

“Consiste en asegurar que los empleados y contratistas sepan y cumplan con sus responsabilidades en la seguridad de la información”. (INEN-ISO/IEC, 2016)

2.3.2.1. Acuerdos

“La dirección debe exigir a los empleados y contratistas, que utilicen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la empresa”. (INEN-ISO/IEC, 2016)

2.3.2.2. Capacitación para los usuarios

“Los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización”. (INEN-ISO/IEC, 2016)

2.3.3. Finalización de contrato

“Cuidar los intereses de la empresa como parte del proceso de cambio o finalización del empleo”. (INEN-ISO/IEC, 2016)

2.3.3.1. Responsabilidades ante la finalización o cambio

“Las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo se deben definir, comunicar al empleado o contratista y se deben cumplir”. (INEN-ISO/IEC, 2016)

2.4. Administración de activos

2.4.1. Categorización de la información

Al ser el activo más importante de la empresa, la información se debe clasificar de manera correcta para darle su debida protección dependiendo el tipo y la importancia que esta tenga en la empresa, cumpliendo así con los siguientes principios de seguridad: (INEN-ISO/IEC, 2016)

- Confidencialidad.
- Integridad.
- Disponibilidad.

2.4.2. Manipulación de la información

Existen muchos tipos de procedimientos que se pueden implementar para poder etiquetar y manejar la información de manera adecuada, dependiendo de algunos parámetros, siguiendo un esquema específico designado por la institución; este variará según el tipo de información que se maneje dentro de la empresa. (INEN-ISO/IEC, 2016)

2.5. Control de acceso

2.5.1. Requerimientos para el control de acceso

2.5.1.1. Política de control de acceso

“Se deberá establecer, documentar y estudiar una política de control de acceso la cual tiene que basarse en los requerimientos de la organización y de la seguridad de la información.” (INEN-ISO/IEC, 2016)

2.5.1.2. Acceso a la red

Solamente se deberá brindar acceso a la red a usuarios específicamente autorizados. (INEN-ISO/IEC, 2016)

2.5.2. Administración del acceso para los usuarios

2.5.2.1. Acuerdos de usuario

“Se deberá establecer un procedimiento formal de registro y retirada de usuarios para hacer posible la asignación de los derechos de acceso.” (INEN-ISO/IEC, 2016)

2.5.2.2. Gestión de privilegios de acceso

Se debe mantener un control sobre el uso de privilegios con que los usuarios cuentan para el acceso a los sistemas. (INEN-ISO/IEC, 2016)

2.5.2.3. Derechos de acceso de usuario

“Los propietarios de los activos deben estudiar los derechos de acceso de usuario a intervalos regulares.” (INEN-ISO/IEC, 2016)

2.5.3. Compromisos del usuario

2.5.3.1. Manejo de contraseñas

La seguridad implementada, vendrá de la mano de la colaboración de los usuarios con el manejo adecuado de los sistemas y el uso minucioso de las contraseñas para el acceso a los mismos. (INEN-ISO/IEC, 2016)

Se deben cumplir con las políticas aplicadas sobre el manejo de las contraseñas, evitando así el acceso de personas no autorizadas, sin poner así en peligro a los recursos de la empresa. (INEN-ISO/IEC, 2016)

Existen algunos aspectos que los usuarios deberían estar conscientes sobre el manejo de las contraseñas:

- Mantener privacidad de los accesos y contraseñas asignados.
- Se recomienda el cambio periódico de la contraseña.
- Diseñar una contraseña segura.
- No se debe compartir datos de la contraseña con nadie.

La capacitación y conocimiento de los usuarios sobre las políticas de seguridad para el manejo de contraseñas, es fundamental para mantener a los sistemas

fuera del alcance de personas no autorizadas, es por ello que se debe poner énfasis dentro de la organización para concientizar a los usuarios sobre la responsabilidad que ésta influye en la seguridad. (INEN-ISO/IEC, 2016)

2.5.4. Control de acceso a la red

2.5.4.1. Manejo de servicios de red

El control de accesos a todos los servicios de red estará monitoreado por el responsable de la seguridad de la información. Cada usuario, dependiendo sus funciones, se le concederá permisos de acceso a los servicios de red, en donde las políticas deberán controlar: (INEN-ISO/IEC, 2016)

- A qué servicios de la red y en sí qué red el usuario tendrá acceso.
- La aplicación de controles respectivos para la autenticación, autorización y contabilización de todos los ingresos a la red y sus servicios.
- Tener un control sobre el tipo de ingreso a la red y el riesgo que esto abarca.

El uso inadecuado de la red puede ser el inicio de vulnerabilidades para cualquier tipo de ataque o filtración de código malicioso. Así que se debe efectuar más detalladamente un control sobre los ingresos externos a la red empresarial y además el acceso a los servicios críticos de la organización. (INEN-ISO/IEC, 2016)

2.5.4.2. Autenticación de usuarios

El uso de sesiones remotas para el ingreso a la red empresarial es un tema muy común hoy en día y además un tema muy vulnerable sin los respectivos controles y políticas. La autenticación a la red con el uso de VPNs (Red Privada Virtual), por motivos de seguridad, se la debe realizar usando técnicas de criptografía o

protocolos de autenticación que permitan el acceso seguro por usuarios remotos. (INEN-ISO/IEC, 2016)

2.5.4.3. Reconocimiento de equipos

Hoy en día existen muchas herramientas que permiten la identificación automática de todos los nodos y equipos que están estableciendo una conexión a la red, pues con esto, se debe tener un control de todos los equipos autorizados, su ubicación exacta y los servicios y aplicaciones que están consumiendo. (INEN-ISO/IEC, 2016)

2.5.4.4. Subdivisión de redes

Es esencial dentro de una empresa, sobre todo medianas y grandes empresas, la subdivisión de sus redes en dominios lógicos de red separados, para tener un mejor control de las mismas, definiendo los riegos que esto conlleva y los requerimientos de seguridad para su aplicación. (INEN-ISO/IEC, 2016)

Se debe tomar en cuenta que, dentro de estos perímetros de dominios establecidos, se implementarán las respectivas seguridades para el control de acceso. (INEN-ISO/IEC, 2016)

2.5.4.5. Control de conexión a la red

Para evitar la saturación de sesiones conectadas a la red, se debe restringir el número de usuarios dentro de ella, esto dependerá del número de usuario que requieran el acceso y la capacidad de la red para soportar un número de usuarios. (INEN-ISO/IEC, 2016)

Para mayor control de la conexión a la red, se puede restringir a través de las puertas de enlace de la red como, por ejemplo:

- Restricciones en el envío de correos electrónicos.
- Transferencia de archivos.
- Acceso a internet.
- Acceso a aplicativos

2.5.4.6. Control de enrutamiento en la red

Dentro de las normas ISO 27001, nos detalla: “Se deberían implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y flujos de información no incumplan la política de control de acceso de las aplicaciones del negocio.” (ISO, 2014)

Por lo tanto, la aplicación de estos controles se debería establecer para la validación de las direcciones origen y destino.

2.6. Criptografía

2.6.1. Controles criptográficos

“Garantizar el uso adecuado y eficaz de la criptografía para salvaguardar la confidencialidad, autenticidad e integridad de la información”. (INEN-ISO/IEC, 2016)

2.6.1.1. Uso de los controles criptográficos

“Se deberá desarrollar e implementar una política en cuanto al uso de los controles criptográficos para proteger la información”. (INEN-ISO/IEC, 2016)

2.6.1.2. Administración de los controles criptográficos

“Se deberá desarrollar e implementar una política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida”. (INEN-ISO/IEC, 2016)

2.7. Seguridad de las operaciones

Dentro de las normas 27001 de la ISO, nos especifica que: “se debe asegurar la operación correcta y segura de los servicios de procesamiento de información y comunicaciones”, pues se debe efectuar un manejo correcto y responsable para así cumplir con el resguardo de la información que se está operado. (INEN-ISO/IEC, 2016)

Dentro de las políticas a los recursos humanos, se estableció la responsabilidad que los usuarios tienen con respecto al cumplimiento de las políticas de seguridad de la información y el uso adecuada de la misma.

2.7.1. Protección contra software malicioso

Es necesario aplicar los respectivos controles ante la amenaza de los distintos códigos maliciosos que puedan afectar a la red y la información en sí. Con la detección y prevención correcta, se podrá contrarrestar el efecto negativo que estos puedan provocar. (INEN-ISO/IEC, 2016)

Los responsables del área de seguridad de la información, y sobre todo los usuarios que realizan las operaciones en la empresa, son los responsables de mantener la información segura ante cualquier amenaza de software, siempre y cuando se cumplan con las políticas de seguridad establecidas por la dirección. (INEN-ISO/IEC, 2016)

2.7.2. Copias de seguridad

Dentro de una empresa, el respaldo de la información es primordial. Estas copias se las realizarán de acuerdo a procedimientos establecidos por los responsables del área de seguridad. (INEN-ISO/IEC, 2016)

Los respaldos se los deben realizar periódicamente y se recomienda considerar algunos aspectos:

- Se debe establecer un tiempo periódico para cada respaldo a realizarse.
- La extensión y frecuencia que se realizan las copias dependerá de las necesidades de la empresa.
- Se debe establecer un cierto grado de seguridad a la información respaldada.
- Se debe controlar el sistema encargado de realizar las copias ante posibles fallas en el mismo, entre otros.

2.7.3. Registro y supervisión

2.7.3.1. Registro de eventos

Se debe tener constancia de todas las actividades realizadas dentro de los sistemas en la organización. Estas pueden ser ejecutadas por los usuarios, cambios en el sistema, fallos y distintos eventos que se producen. Estos incluyen: (INEN-ISO/IEC, 2016)

- Hora de ingreso y salida al sistema.
- Fallos y soluciones realizadas.
- Modificación en el sistema o la información.
- Accesos denegados.
- Eventos de seguridad, etc.

2.7.3.2. Protección de la información de registro

Al igual que los respaldos de información, se debe proteger todos los eventos que se realizan en el sistema ante manipulación y accesos no autorizados a esta información. (INEN-ISO/IEC, 2016)

2.7.3.3. Sincronización del reloj

Es primordial dentro de un sistema de registro de eventos la sincronización del reloj, del equipo donde se realiza la operación con los servidores a lo que se están accediendo y la hora del registro del evento. Esta información debe ser precisa y confiable, ya que la información de la hora que se realizó el evento ayudará previamente para su correcto manejo. (INEN-ISO/IEC, 2016)

2.8. Protección de las redes de comunicación

2.8.1. Administración de la seguridad de redes

“Garantizar la protección de la información en las redes y los recursos de tratamiento de la información que tenga la empresa”. (INEN-ISO/IEC, 2016)

2.8.1.1. Controles de red

“Las redes tienen que ser gestionadas y controladas para proteger la información de la organización”. (INEN-ISO/IEC, 2016)

2.8.1.2. Protección de los servicios de red

“Se deberán identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan”. (INEN-ISO/IEC, 2016)

2.8.1.3. Segregación en redes

“Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas”. (INEN-ISO/IEC, 2016)

2.8.2. Transferencia de información

“Conservar la seguridad en la información que se transfiere dentro de una organización y con cualquier entidad externa”. (INEN-ISO/IEC, 2016)

2.8.2.1. Políticas de transferencia de información

“Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación”. (INEN-ISO/IEC, 2016)

2.8.2.2. Acuerdo de transferencia de información

“Deben establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros”. (INEN-ISO/IEC, 2016)

2.8.2.3. Mensajería electrónica

“La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida”. (INEN-ISO/IEC, 2016)

2.8.2.4. Acuerdos de confidencialidad o no revelación

“Deben identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación”. (INEN-ISO/IEC, 2016)

2.9. Relación con proveedores

2.9.1. Gestión de la provisión de servicios del proveedor:

“Mantener un nivel acordado de seguridad y de provisión de servicios en línea con acuerdos con proveedores”. (INEN-ISO/IEC, 2016)

2.9.1.1. Control y revisión de la provisión de servicios del proveedor

“Las organizaciones deben controlar, revisar y auditar regularmente la provisión de servicios del proveedor”. (INEN-ISO/IEC, 2016)

2.9.1.2. Gestión de cambios en la provisión del servicio de proveedor

“Se deben gestionar los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la información existentes”. (INEN-ISO/IEC, 2016)

2.10. Aspectos de seguridad para la gestión de la información

2.10.1. Redundancia

Asegurar la disponibilidad de los recursos de tratamiento de la información.

2.10.1.1. Disponibilidad de los recursos de tratamiento de la información

“Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad”. (INEN-ISO/IEC, 2016)

2.11. Cumplimiento

2.11.1. Requisitos legales

Dentro de aspectos organizacionales, es de suma importancia el cumplimiento de toda obligación legal, reglamentos y estatutos concernientes a la seguridad de la información, siendo esta el bien más valioso de la empresa. (INEN-ISO/IEC, 2016)

2.11.1.1. Derechos de propiedad intelectual

Se deben cumplir con todos los requisitos legales y regulatorios para garantizar el respeto de la propiedad intelectual sobre el uso de cualquier sistema de control, monitoreo, entre otros, en donde puedan existir derechos de autor o sistemas patentados. (INEN-ISO/IEC, 2016)

2.11.1.2. Protección de la información

Las políticas que se aplican a nivel institucional en general, están para la protección de la información, es por eso que, con la ayuda de un SGSI, se debe certificar la protección y privacidad de la misma según lo requieran. (INEN-ISO/IEC, 2016)

2.11.1.3. Controles criptográficos

Según la ISO: “Se deben utilizar controles criptográficos que cumplan todos los acuerdos, leyes y los reglamentos pertinentes”. (INEN-ISO/IEC, 2016)

2.11.2. Revisión de la seguridad de la información

2.11.2.1. Revisión de políticas

Todos los controles y políticas dentro del sistema, deben ser revisados y controlados periódicamente para mantener el margen de seguridad adecuado para la protección de los sistemas, la red y la información. (INEN-ISO/IEC, 2016)

2.11.2.2. Cumplimiento de políticas

Dentro de una organización, los directivos y responsables de la seguridad, deben cerciorar y controlar todos los procedimientos que se llevan a cabo para mantener los sistemas de gestión de seguridad en orden y funcionando

correctamente, cumpliendo así con todas las normas y políticas aplicadas en los sistemas de la empresa. (INEN-ISO/IEC, 2016)

3. Capítulo III. Mecanismos y Herramientas de Seguridad

Los mecanismos y herramientas de seguridad son sistemas diseñados exclusivamente para ayudar a los administradores de una organización, alertándolos o realizando acciones automáticas programadas necesarias para mantener el sistema seguro. (Bustamante, 2013)

Existen 2 tipos mecanismos de seguridad:

- *Orientadas a host*: Consiste en trabajar únicamente con información disponible dentro de la máquina de cada usuario.
- *Orientadas a red*: Consiste en trabajar únicamente con información proveniente de la red (conexiones no autorizadas, puertos, etc.).

3.1. Herramientas de seguridad

Debido a que existen herramientas para el análisis de seguridad en redes, también existen herramientas para proteger al sistema contra diferentes ataques. (Bustamante, 2013)

El firewall, es una de las herramientas indispensables en la seguridad de redes, pero además existen otros sistemas de protección algunos de los cuales se detallan a continuación:

3.1.1. Firewalls

“Son sistemas localizados entre dos redes que ejercen una política de seguridad determinada. Los firewalls se encargan de proteger una red confiable de una que no lo es (internet). También permite habilitar el acceso a los usuarios y servicios autorizados.” (Bustamante, s.f.)

3.1.1.1. Tipos de firewall

- “Filtros a nivel de paquete (Packet Filters).
- Firewall a nivel de circuito (Circuit Level Firewalls).
- Firewall a nivel de aplicación (Aplication Layer Firewalls).
- Filtros dinámicos a nivel de paquete (Dynamic Packet Filters)” (Bustamante, s.f.).

3.1.1.1.1. Filtros a nivel de paquete (Packet Filters)

“Pertenecen a la primera generación de firewalls la misma que analiza el tráfico de la red. Cada paquete que ingresa o sale de la red es inspeccionado y lo acepta o rechaza basándose en las reglas definidas por el usuario.” (Bustamante, s.f.)

A continuación, se describen las reglas para rechazar o aceptar un paquete:

- “Si no se encuentra una regla que aplicar el paquete, el paquete es rechazado”. (Bustamante, s.f)

- “Si se encuentra una regla que aplicar al paquete, y la regla permite el paso, se establece la comunicación”. (Bustamante, s.f)

- “Si se encuentra una regla que aplicar al paquete y la regla rechaza el paso, el paquete es rechazado”. (Bustamante, s.f)

3.1.1.1.2. Firewall a nivel de circuito (Circuit Level Firewalls)

“Pertenece a la segunda generación de firewalls y verifica que los paquetes pertenezcan ya sea a una solicitud de conexión o a una conexión entre dos computadoras. Aplica mecanismos de seguridad cuando una conexión TCP o UDP es establecida. Cuando la conexión se establece, los paquetes pueden ir y venir entre las computadoras sin tener que ser revisados cada vez.” (Bustamante, s.f)

3.1.1.1.3. Firewall a nivel de aplicación (Aplication Layer Firewalls)

“Un firewall de nivel de aplicación representa el extremo opuesto en el diseño de un firewall. En vez de usar un mecanismo de propósito general para permitir diversos tipos de tráfico, código de propósito específico puede utilizarse para cada aplicación deseada. Estos firewalls además poseen otra característica apreciada, pueden registrar (log) y controlar todo el tráfico de entrada y salida”. (Microsoft, 1997)

3.1.1.1.4. Filtros dinámicos a nivel de paquete (Dynamic Packet Filters)

“Pertenece a la cuarta generación de firewall, permite modificaciones a las reglas de seguridad sobre la marcha. En la práctica, se utilizan dos o más técnicas para configurar un firewall”. (Bustamante, s.f)

3.1.1.2. Cuadrante mágico de Firewall para redes empresariales

Figura 5. Cuadrante mágico de Firewall para redes empresariales. Tomado de (Gartner, 2016)

Según Tecnologías de información, 2016, “el cuadrante de Gartner es una representación gráfica de la situación del mercado de un producto tecnológico en un momento determinado.” (AdvisorSecurity, s.f.)

“En el eje X, Gartner define una categoría “integridad de visión” y en el eje Y se indica la “capacidad de ejecutar”, las dos divisiones fragmentan el cuadrante en cuatro sectores en donde se encuentran las compañías en función de su tipología y la de sus productos: líderes, retadores o aspirantes y visionarios.” (AdvisorSecurity, s.f.)

A continuación, en la tabla 2, se muestran algunos productos comerciales de firewalls líderes de acuerdo al cuadrante de Gartner:

Tabla 2.

Comparación de equipos de firewalls líderes en el mercado.

Firewalls Comerciales			
Equipo	Cisco ASA 5555-X with FirePOWER	CheckPoint 4600	FortiGate 500D
Licencia	Comercial	Comercial	Comercial
Precio	Desde $11,900.00	Desde $16,300.00	Desde $10,900.00
NGFW	si	si	si
Firewall Throughput	4 Gbps	3.4 Gbps	16 Gbps
IPS (Gbps)	1.3 Gbps	630 Mps	4.7 Gbps
Switch Ports	8x 1GE Ports	Desde 4x 1GE o 2x 10GE ports	10x 1GE ports, 8x 1GE ports.

Tomado de (Fortinet, s.f.)

3.1.1.3. Análisis de equipos (Firewall, IDS, IPS, Servidor de control de acceso ACS de cisco)

En el caso de la gama de dispositivos Cisco ASA 5555-X, son equipos de próxima generación llamados (NGFW), son diseñados especialmente para protección contra amenazas y malware avanzado. Lo interesante de estos dispositivos es que ofrecen defensa contra amenazas antes, durante y después del ataque gracias a la incorporación de un sistema integrado de protección contra malware y amenazas, es decir que actúan a la vez como un IPS.

Una vez realizada la comparación de equipos en la Tabla 2, se puede observar las distintas características que estos firewalls ofrecen, para la selección de estos equipos, simplemente dependerán de las necesidades del cliente y el presupuesto con que se cuente.

3.1.1.4. Ubicación de Firewall en la red

Los firewalls al ser el punto de seguridad entre dos redes, mantienen separada la red interna de diferentes redes externas, tal y como se ilustra en la Figura 6.

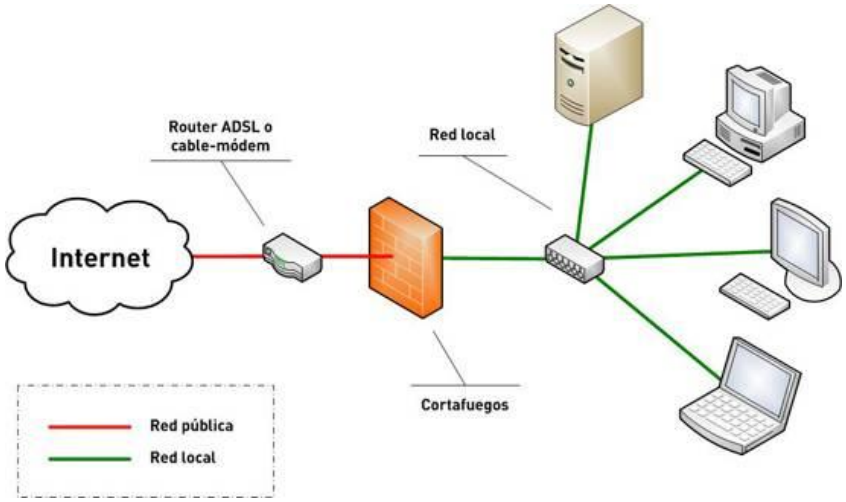

Figura 6. Ubicación Firewall dentro de la red.
Tomado de (Servinetwork, s.f.)

3.1.2. Sistema de Detección de Intrusos (IDS)

“Los IDS están compuesto por tres elementos: una fuente de información que proporciona los eventos que realiza el sistema, un motor de análisis que busca evidencias de intrusiones y un mecanismo de respuesta que actúa según los resultados de motor de análisis”. (Garzón, 2015)

Además, comparten la información de otros sistemas como los firewalls, routers y switches. También, permiten utilizar protocolos SNMP enviando notificaciones y alertas a otros equipos de la red a lo que llamamos interoperabilidad. (Garzón, 2015)

Para poder evaluar el comportamiento de un IDS hay que tener en cuenta cuando en términos de probabilidad se analice, por ejemplo: cuando se detecta un ataque en el sistema y cuando se producen falsas alarmas. Se debe analizar

y tener en cuenta el gran número de alertas generadas y las falsas alarmas que se pueden producir, al final esto puede tornarse una tarea muy tediosa para los administradores del sistema, requiriendo una constante supervisión. (Garzón, 2015)

3.1.2.1. Funciones de un IDS

A continuación, se detallan las funciones de un sistema de Detección de Intrusos:

- Cuando el ataque está sucediendo este es el encargado de detectar la intrusión.
- Gracias a las herramientas de búsqueda se puede automatizar la búsqueda de nuevos patrones de ataques.
- Mediante el análisis del tráfico y logs, se puede descubrir sistemas habilitados, los mismos que no deberían estarlo.
- “Automatiza tareas, por ejemplo: actualización de reglas, obtención y análisis de logs, configuración de cortafuegos etc”. (Garzón, 2015)

3.1.2.2. Análisis de IDS

En primer lugar, se procederá a comparar los tipos de IDS que existen para luego proceder analizar qué tipo de IDS sería mejor utilizar en nuestro caso de estudio.

3.1.2.2.1. IDS basados en red (NIDS)

En el caso de los NIDS, la red es fundamentalmente donde actúan este tipo de IDS. Estos detectan ataques a los paquetes que se transmiten por la red, escuchando y examinando un segmento. Un NIDS permite examinar y proteger a los hosts que están conectados a un fragmento de red.

Tabla 3.

Ventajas y desventajas NIDS.

NIDS	
Ventajas	**Desventajas**
Los NIDS se pueden instalar en segmentos de red, por ende, utilizando uno solo se puede detectar los ataques que están sucediendo en todos los equipos conectados a este segmento. Además, son independientes de la plataforma utilizada por los diferentes equipos de la red.	Los NIDS son ineficientes en sistemas con tráfico cifrado. En redes de alta velocidad el funcionamiento de estos se vuelve inviable, impidiendo examinar todos los paquetes rápidamente. Si se llega a producir una congestión en la red varios paquetes pueden perderse.

3.1.2.2.2. IDS basados en host (HIDS)

"Operan sobre la información obtenida desde una computadora, por ejemplo: los ficheros de auditoria del sistema operativo. Con esta información el IDS puede analizar las actividades que se producen con gran precisión, logrando determinar que procesos y usuarios exactamente están involucrados en un ataque dentro del sistema operativo". (Gómez, s.f.)

Tabla 4.

Ventajas y desventajas HIDS

HIDS	
Ventajas	**Desventajas**
Los HIDS pueden detectar de mejor manera los ataques desde adentro del equipo, es decir puede monitorear inicios de sesión, cambios de ficheros etc. Además, estos pueden comunicar sobre el estado del atacado confiablemente.	Son difíciles de implementar ya que tienen que ser instalados en varias máquinas y puede ser necesario el desarrollo en distintas plataformas. Como estos residen en host no se puede confiar en los informes ya que pueden ser manipulados.

Al analizar las ventajas y desventajas de los dos tipos de IDS (detalladas en la Tabla 3 y Tabla 4), se vio claramente que dentro de una organización será fundamental su implementación para la detección de ataques. Pues, en el caso de los NIDS, se enfocarán en detectar cualquier anomalía que se produce al momento de transmitir paquetes, por otra parte, los HIST estarán más enfocados en la detección de ataques que se produzcan dentro del host sin la necesidad de saber el estado de la red.

En la Figura 7 se muestra claramente dónde opera cada tipo de IDS:

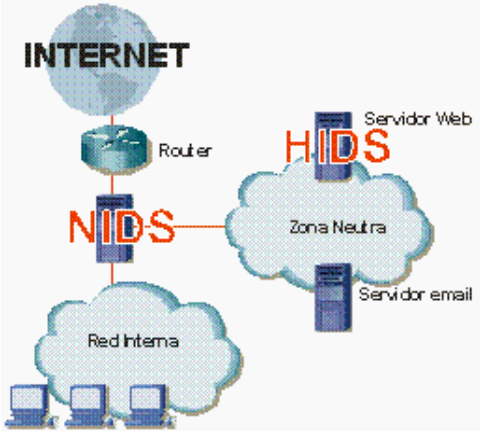

Figura 7. Utilización de IDS.

Tomado de (Gómez, 2011)

3.1.2.3. Tipos de eventos para la detección de intrusos

Existen dos tipos de eventos para la detección de intrusos:

- *Detección de abusos*: Es la más usada (Detallada en la Tabla 5).
- *Detección de anomalías*: La utilizan algunos IDS de forma limitada buscando patrones anormales (Detallada en Tabla 6).

Tabla 5.

Ventajas y Desventajas acerca de Detección de abusos o de firmas

Tipos de eventos para la detección de intrusos	
Detección de abusos o de firmas	
Ventajas	**Desventajas**
Evaden un gran número de falsas alarmas que se da por la acción efectiva de los detectores de ataques. Determinan rápida y exactamente el uso de herramientas o técnicas de un ataque particular.	Actualizaciones constantes de las firmas de los últimos ataques.

Tabla 6.

Ventajas y Desventajas acerca de Detección de anomalías

Tipos de eventos para la detección de intrusos	
Detección de anomalías	
Ventajas	**Desventajas**
“Los IDS detectan comportamientos inusuales, de esta manera poseen la capacidad de detectar ataques para los cuales no tienen un conocimiento definido”. (Garzón, 2015)	“Ocasiona un gran número de falsas alarmas, por los comportamientos inusuales de usuarios y redes”. (Garzón, 2015)

3.1.2.4. Productos comerciales

Dentro del mercado de IDS’s se ha visto importante reconocer a las siguientes marcas por su importancia y sus diversas características:

- **Dragon - Enterasys Networks:**

Este IDS consiste en la toma de información acerca de las actividades sospechosas de un sensor al cual se lo llama DragonSquire, este es el encargado de monitorear los logs de los firewalls y otros sistemas. La información recopilada será enviada a un Dragon Server para los análisis correspondientes. (Garzón, 2015)

- **NetRanger - Cisco Systems:**

"Este sistema de detección de intrusos de cisco, puede detectar, prevenir y reaccionar contra actividades no autorizadas por medio de la red. Cisco IDS Host Sensor v2.0 puede identificar ataques y prevenir accesos no autorizados a recursos que son críticos para el servidor". (Garzón, 2015)

- **Snort:**

Se puede ejecutar en UNIX y WINDOWS, cuenta con 1600 reglas para analizar diferentes tipos de alertas, además es flexible y muy pequeño, fue elaborado como prototipo cumpliendo con todas las exigencias de un IDS, con el tiempo creció y se adoptó a funciones que solamente tiene los IDS de marcas importantes. (Garzón, 2015)

En la Tabla 7 se muestran algunas herramientas de detección de intrusos que existen en el mercado:

Tabla 7.

IDS's Comerciales en el mercado.

Herramientas de detección de Intrusos		
Nombre	**Tipo**	**Licencia**
Cisco Secure Intrusion Detection System	NIDS	Comercial

Dragon	HIDS/NIDS	Comercial
NFR	HIDS/NIDS	Comercial
Snort	NIDS	Open Source
ISA Server	HIDS	Comercial

3.1.2.5. Donde colocar un IDS

Existen 3 zonas principales en las cuales se debería ubicar un sensor, como se observa en la imagen de la Figura 8.

- Zona roja: esta zona tiene un índice de riesgo elevado, por ende, el IDS deberá ser configurado de forma sensible debido a que el tráfico de entrada como de salida de la red se verá y esto genera más alarmas.
- Zona verde: la sensibilidad en esta zona es mayor que la zona roja, aquí aparecen menos falsas alarmas y los servidores se podrán acceder solo desde esta zona.
- Zona azul: esta zona es la zona confianza, si llega tráfico malicioso no se lo deja pasar.

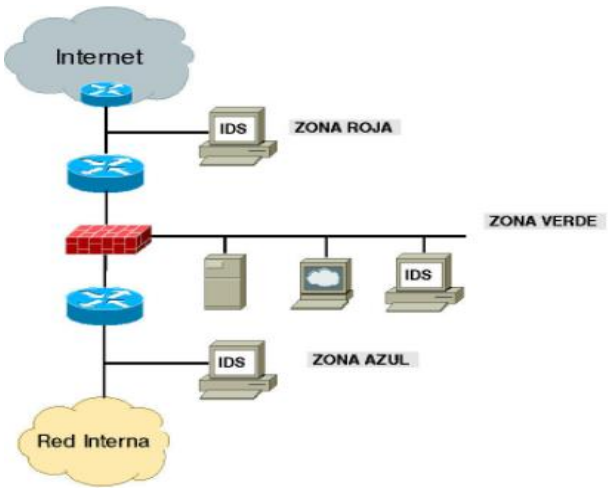

Figura 8. Donde colocar un IDS.
Tomado de (Cisco, 2016)

3.1.3. Sistema de Prevención de Intrusos (IPS)

“El sistema de prevención de intrusos (IPS) consiste en un conjunto de acciones predefinidas que tienen como objetivo prevenir actividades sospechosas que provienen tanto de las redes externas/internas como del mismo host de una manera proactiva y eficaz. Los IPS presentan una mejora importante sobre las tecnologías de cortafuegos tradicionales, al tomar decisiones de control de acceso basados en los contenidos del tráfico, en lugar de direcciones IP o puertos.” (Panda, s.f.)

La diferencia entre un IPS y un IDS está en que los IDS alertan al administrador del sistema acerca de una posible intrusión, mientras que los IPS establecen políticas de seguridad para proteger la red de un ataque, los IPS protegen al equipo proactivamente mientras que los IDS lo hacen reactivamente.

3.1.3.1. Funcionamiento de un IPS

Los IPS son equipos de seguridad de red que monitorean el tráfico de la red y lo que suceden en el sistema, buscando alguna actividad maliciosa que se presente. (Garzón, 2015)

A continuación, se enlistan las principales funciones de un IPS:

- Identificar actividades maliciosas.
- Detener actividades maliciosas.
- Establece políticas de seguridad para cuidar los equipos y la red de intrusiones.
- Los IPS protegen la red de manera proactiva ya que pueden bloquear las intrusiones de inmediato, sin importar el protocolo de transporte que se utilice y sin la reconfiguración de dispositivos externos.

- Graban información de cada actividad maliciosa y con esto pueden generar reportes.

3.1.3.2. Análisis de IPS

Existen 3 tipos de IPS detallados a continuación en la tabla 8:

Tabla 8.

Comparación entre IPS.

Comparación entre IPS		
Basados en red LAN (NIPS)	**NBA**	**Basados en Host (HIPS)**
Se encargan de monitorear la red LAN buscando tráfico dudoso y este tráfico es analizado por protocolo de comunicación.	"Se encargan de examinar el tráfico de la red e identificar amenazas que generan tráfico inusual". (Bonilla, 2016)	Consiste en instalar paquetes de software que se encargan de monitorear un host único en busaca de actividades sospechosas.

Anidada de (Bonilla, 2016)

Al analizar los tipos de IPS en la Tabla 8, se puede concluir que los NIPS y HIPS son necesarios e indispensables en una red empresarial para tener mayor seguridad en una organización. Ahora bien, es importante detallar que se puede utilizar un IPS que cumpla con las funciones de NIPS y HIPS con esto se estaría ahorrando costos a la empresa ya que solo se debería comprar un equipo que realice las dos funciones.

Al igual que los IDS, se pueden colocar en distintos puntos de la red, como se muestra en la Figura 9. Esto dependerá del grado de control que deseemos implementar en la red.

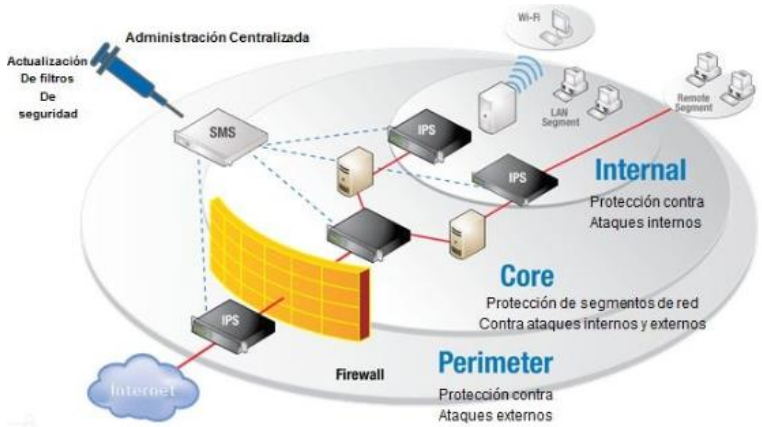

Figura 9. Donde colocar un IPS.

Tomado de (Cisco, 2016)

3.1.3.3. Tipos de detección de tráfico

Existen diferentes formas que los IPS detectan el tráfico malicioso, tal y como se muestra en la Tabla 9:

- “Detección basada en firmas.
- Detección basada en políticas.
- Detección basada en anomalías”. (Bonilla, 2016)

Tabla 9.

Formas que los IPS detectan intrusiones.

Formas que los IPS detectan intrusiones		
Detección basada en firmas	**Detección basada en políticas**	**Detección basada en anomalías**
“Tienen la capacidad de descubrir una determinada cadena de bytes en cierto contexto, y luego manda una alerta. Este tipo de detección funciona como un antivirus.”	Para este tipo de detección, se requiere que en los IPS se especifiquen las políticas de seguridad.	“Consiste en analizar el tráfico de la red por periodo de tiempo determinado creando una línea base de comparación.”

Tomado de (Bonilla, 2016)

3.1.3.4. Productos comerciales

- **Sensores Cisco IPS serie 4500**

Es un elemento fundamental de una arquitectura Cisco SecureX, ofrece inspección acelerada por hardware, rendimiento real, alta densidad de puertos y eficiencia energética en un chasis preparado para su ampliación. A continuación, en la tabla 10, se detallan las características de este equipo. (Garzón, 2015)

Tabla 10.

Sensores Cisco IPS serie 4500.

Sensores Cisco IPS serie 4500		
Nombre	**Características**	**Precio**
Cisco Secure Intrusion Detection System	Protección específica para el Data Center en servidores basados en la Web, bases de datos y almacenamiento; aplicaciones de clase empresarial Oracle y SAP, y software personalizado. Fácil implementación y gestión: la configuración de la implementación dirigida por un asistente incluye plantilla de firmas focalizada en el Data Center; gestión eficiente con Cisco IPS Manager Express o Cisco Security Manager que abarca toda la línea de productos de IPS.	Desde $19,000.00 en adelante dependiendo de las características que tengan.

Anidada de (Cisco, 2014)

3.1.4. Control de Acceso a la Red (NAC)

La adaptación de nuevas tecnologías para el acceso a los sistemas de una red empresarial ha crecido de una manera indiscutiblemente amplia. Esto conlleva al sin número de amenazas y vulnerabilidades a las que se puede estar

expuestos sin la seguridad adecuada. (Cisco, Cisco NAC Appliance (Clean Access), 2016)

La capacidad que tienen los usuarios para acceder a la red corporativa se ha visto afectada tanto positiva como negativamente. Teniendo en cuenta la facilidad de acceso desde cualquier punto geográfico con tan solo una conexión a internet por medio de VPNs, además se puede evidenciar el aprovechamiento de los recursos adoptados para el acceso y manejo de la información de la empresa por medio de la intranet. Sin embargo, al tener todas estas facilidades, se está expuesto a varios ataques antes mencionados en donde nuestra red pueda salir afectada. (Cisco, Cisco NAC Appliance (Clean Access), 2016)

Al realizar este control se han identificado al menos las siguientes fases, tal como se muestra en la Figura 10:

- *Detección*: Descubrir todas las peticiones de conexión tanto físicas o virtuales a la red.
- *Cumplimiento*: La confirmación del cumplimiento de las políticas y requisitos mínimos establecidos para el acceso a la red.
- *Aceptación*: Es la permisión de ingreso al usuario únicamente a los recursos requeridos dependiendo su rol previamente establecido.
- *Denegación*: Bloqueo a usuarios no autorizados o que no cumplan con los requerimientos de acceso.
- *Control***:** El monitoreo constante del cumplimiento de los requerimientos para evitar la violación de las políticas.

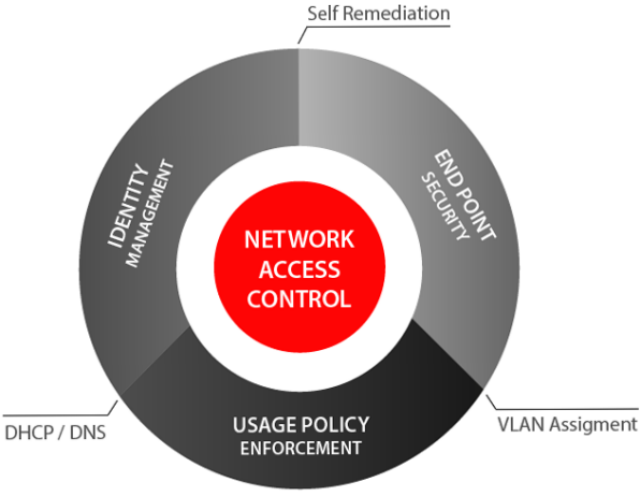

Figura 10. Control de acceso a la red.
Tomado de (Secure IT, 2016)

3.1.4.1. Funcionalidades de NAC

NAC nació como un recurso de red que permitía la administración de las políticas, identificando las operaciones que los usuarios y los distintos equipos realizaban dentro de la red. A continuación, permitió controlar el sistema operativo de los usuarios que querían acceder, verificando si cumple con ciertos parámetros de seguridad como aplicaciones instaladas, si cuenta con antivirus, parches actualizados, entre otras características. (Cisco, Cisco NAC Appliance (Clean Access), 2016)

Así pues, el mecanismo Network Access Control se enfoca en las actividades previas y durante una petición de acceso a una red, facilitando su monitoreo y administración, y además disminuyendo las amenazas e intrusiones no deseadas. (Cisco, Cisco NAC Appliance (Clean Access), 2016)

En el Diagrama 1 se muestran las principales funcionalidades del control de acceso a la red:

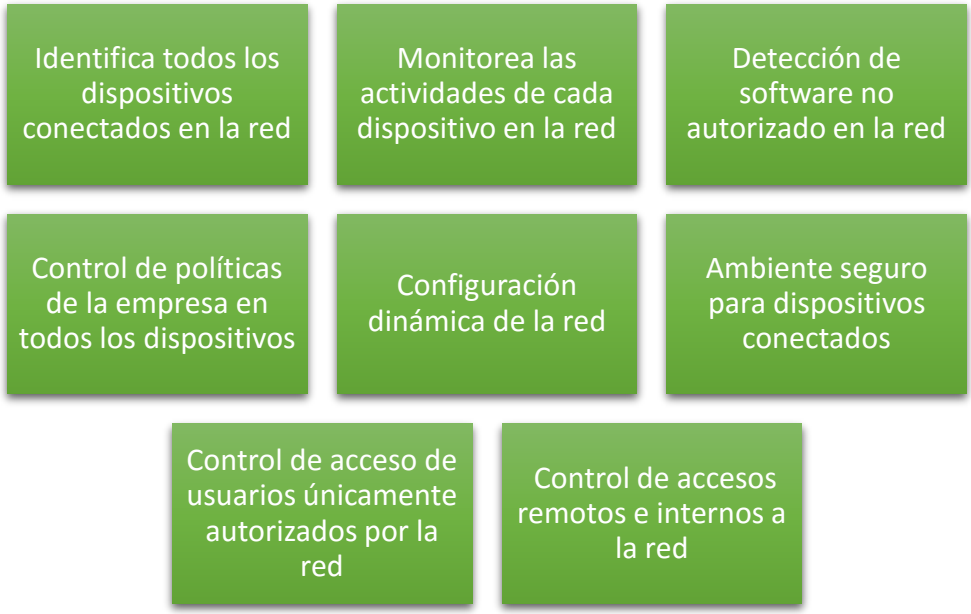

Diagrama 1. Funcionalidades de NAC.
Tomado de (Gámez, 2017)

3.1.4.2. Análisis de NAC

La implementación de Network Access Control (NAC) en una red es indispensable, al ser una tecnología que nos permitirá controlar de forma independiente todos los dispositivos que requieran de acceso a la red, cumpliendo con cierto grado de exigencias ya especificadas por medio de políticas.

Se puede evidenciar hoy en día que la infraestructura de las redes empresariales se extiende a más de un centro de negocio, los cuales están repartidos en distintos puntos geográficos; por otra parte, internamente una organización divide sus departamentos según las funciones de los usuarios dentro de ella. Al necesitar el acceso a internet y a los recursos, es necesario la implementación de varios sistemas que permitan tener el acceso correspondiente sin comprometer la integridad de los datos.

Como se señaló anteriormente, las amenazas no solo son causantes los usuarios que desean acceder a la red de manera externa, pues por más

seguridades que tengamos, como firewalls, IDS, IPS, entre otros, si el usuario que accedió a la red con un software malicioso se encuentra dentro de la empresa, estará afectando los sistemas desde un punto que no se pudo obtener un control de seguridad con estos mecanismos, así como se puede observar en la Figura 11.

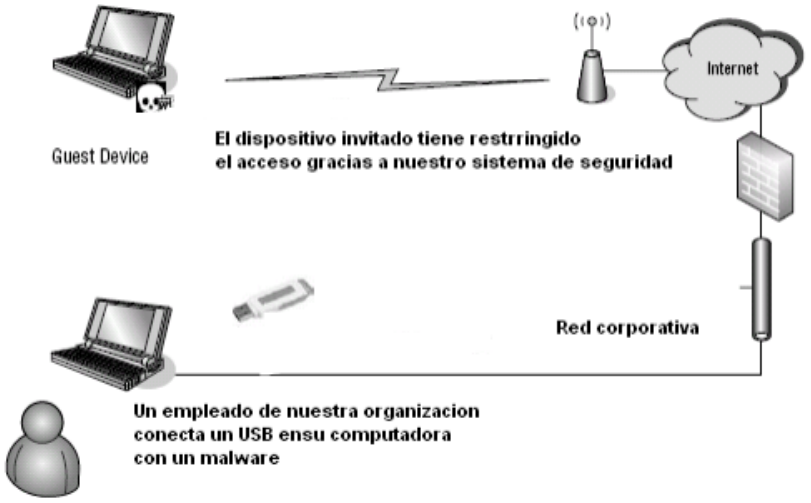

Figura 11. Amenaza interna a la red empresarial.
Tomado de (Esmoris, s.f.)

Para brindar soluciones de NAC, se han establecido dos tipos:

- *"Clienless"***:** No es necesario ningún software en los equipos de los usuarios.

- *"Client-based"***:** Es necesaria la instalación de un componente de software para asistir al proceso que realiza NAC.

3.1.4.3. Tecnologías especializadas en Control de Acceso

Una vez planteado el escenario de los distintitos controles que se deben establecer tanto perimetralmente como dentro de la red empresarial se pueden identificar algunas tecnologías que nos proporcionan este control:

3.1.4.3.1. NAC de Cisco

La tecnología Cisco es una de las más implementadas a nivel empresarial, es por eso que se analizará la solución que ellos nos brindan.

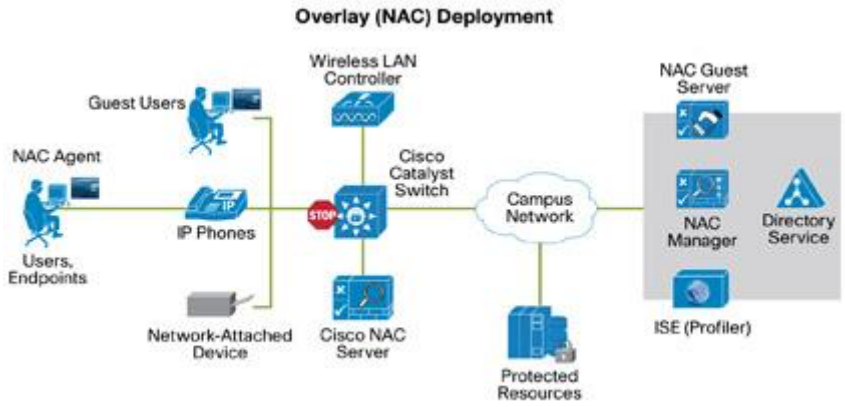

Figura 12. Escenario de control de acceso a la red con NAC.

Tomado de (Cisco, 2006)

Cisco nos plantea el escenario (Figura 12) donde muchas empresas no cuentan con la seguridad adecuada para los equipos que se conectan a la red, tanto interna como externamente.

NAC de Cisco, hará cumplir con los siguientes parámetros:

- Controlar todos los accesos de los usuarios que intenten ingresar a la red.
- Hacer cumplir con todas las políticas implementadas en la red.
- Bloquear a los usuarios que no cumplan con las políticas de seguridad.
- Eliminar las vulnerabilidades de red.

- **Arquitectura NAC de Cisco**

  Para el complemento de este software, es necesaria la aplicación de control, también recomendado una de propiedad de Cisco “Cisco Secure Access”.

Este aplicativo recopilará toda la información de los equipos en red y aplica los controles que sean configurados en el sistema. Además, estos dos sistemas cuentan con un protocolo especial “EAP”, específicamente para UDP y para 802.1x. De manera más detallada se encuentra en la figura 13.

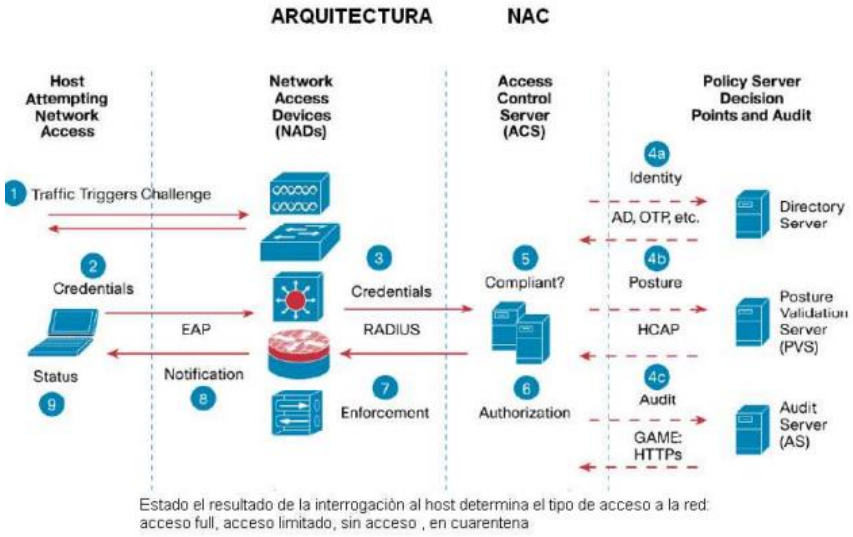

Figura 13. Arquitectura NAC de Cisco.

Tomado de (Cisco, 2016)

3.1.4.3.2. NAP de Microsoft

Por otra parte, Microsoft también plantea una solución para los controles de acceso llamada “NAP (Network Access Protection)”. Pues, NAP protege tanto a la red como a los equipos conectados en ella con la aplicación de políticas de basadas en requerimientos de seguridad que deben cumplir los dispositivos al ingresar a una red.

Al no ser Microsoft una empresa dedicada a los equipos de networking, a diferencia de Cisco, su software NAP “basa su despliegue de agentes y aplicaciones en el lado del cliente y en el uso de distinto tipo de servidores en el lado de la red tanto para la autenticación como el acceso.” (Estévez, 2007)

- **Arquitectura NAP de Microsoft**

Para poder implementar los sistemas de NAP es necesario el uso de algunos equipos que soporte el framework de control de acceso que cuente con los siguientes componentes como se muestra en la Figura 14:

- ✓ Active Directory.
- ✓ Network Policy Server.
- ✓ DHCP Server.
- ✓ NAP Administration Server.
- ✓ Health Policy.

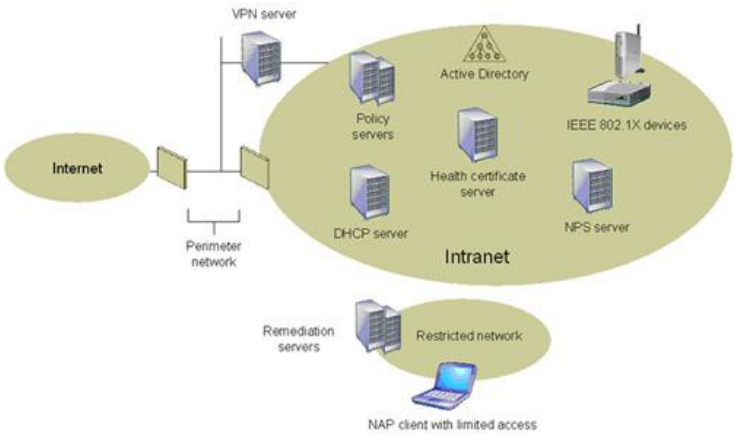

Figura 14. Arquitectura NAP de Microsoft.

Tomado de (Microsoft, 2007)

3.1.4.3.3. TNC (Trusted Network Connect)

Actualmente con la estandarización de tecnologías ha nacido TNC, una arquitectura abierta desarrollada por Trusted Computing Group, que pretende acabar con los sistemas propietarios de control de acceso.

Según Trusted Computing Group, “su propósito principal es posibilitar que cualquier organización pueda implementar políticas de integridad y control de acceso en todas sus redes y conexiones. Por lo tanto, se trata de una iniciativa para ofrecer un estándar a todos los fabricantes y organizaciones que deseen

acogerse a ella que les permita crear productos de control de acceso a la red compatibles unos con otros, y compatibles con las tecnologías y entornos ya existentes". (Trusted Computing Group, 2011)

Algunas compañías ya han anunciado su compatibilidad con el estándar TNC o al menos que pretenden hacerlo en un futuro, estas son:

- Microsoft
- Juniper
- Sygate
- Symantec

3.1.4.3.4. Comparación de tecnologías

Como se mencionó anteriormente, Cisco es una marca que abarca gran cantidad del mercado con sus equipos de networking, es por ello que en caso de una implementación Cisco, se recomienda el control de acceso con todos los componentes que esta nos provee (ACS).

Por otra parte, Microsoft plantea otra arquitectura enfocada al control para los equipos del usuario final. Y finalmente otra de las opciones es optar por TNC, el cual ya cumple con estándares y compatibilidad con muchos sistemas.

Es por ello que el uso de estos dependerá de factores de infraestructura de la red, equipos implementados en la empresa y hasta de temas económicos.

3.1.5. Mecanismo para el acceso seguro a la red

El acceso seguro a la red se realiza por medio de ciertos equipos como son el autenticador, el servidor AAA y la base de datos, los mismos están asociados entre sí para la ejecución de procesos que hayan sido configurados para permitir

el control de acceso a la red y una utilización correcta de sus recursos. (Cicenia & Vásconez, 2011)

En la figura 15 se ilustra y explica el proceso de autenticación AAA.

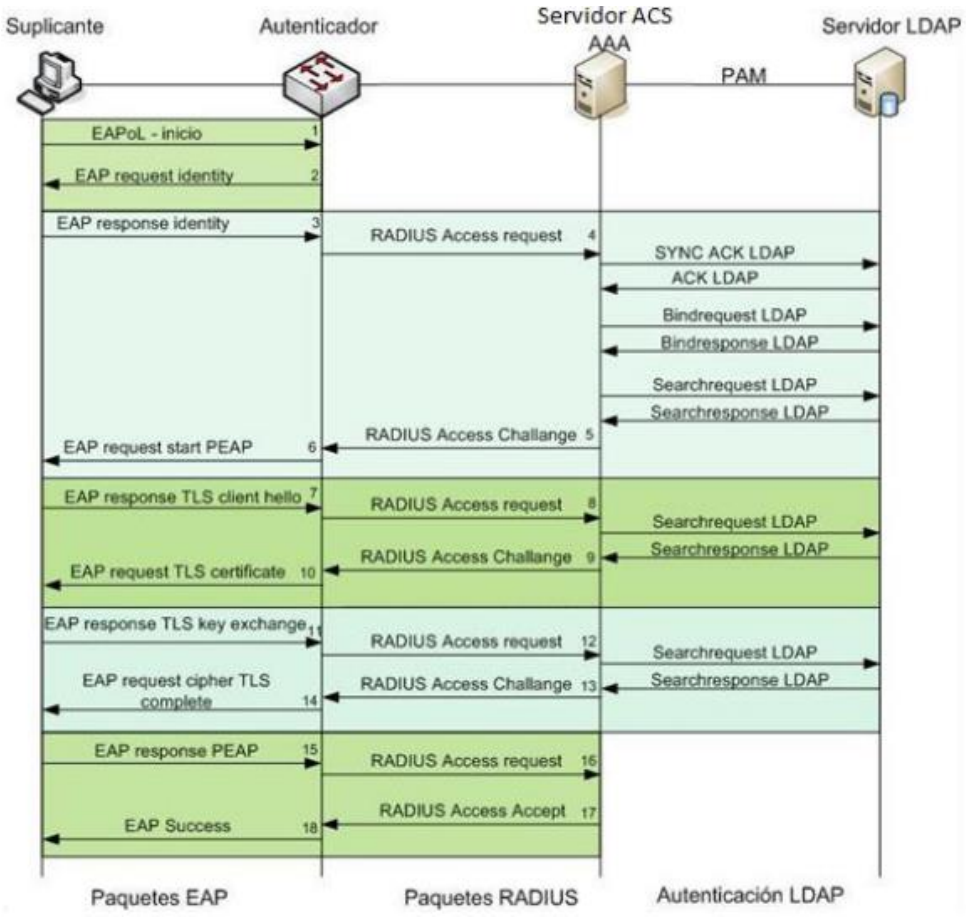

Figura 15. Procedimiento del sistema de autenticación AAA.

Tomado de (Plascencia Bedón, 2012)

3.1.5.1. ACS de Cisco

“El servidor de control de acceso Cisco (ACS) provee servicios AAA a los dispositivos que estén conectados a la red como Routers, servidores de acceso etc.” (Cicenia & Vásconez, 2011)

“El ACS utiliza los protocolos de RADIUS, TACACS+ y su antecesor, utiliza un nivel de seguridad básica que es Password Authentication Protocol (PAP), con el que los usuarios se autentican una sola vez. Además, combina la autenticación, el acceso de usuario o administrador y el control de políticas para mayor flexibilidad y movilidad del usuario.” (Cicenia & Vásconez, 2011)

En la figura 16, se muestra un diagrama de red en el cual se indican los conmutadores de red, los cortafuegos y routers que admite el protocolo AAA y tacas+ trabajando con la solución Cisco ACS.

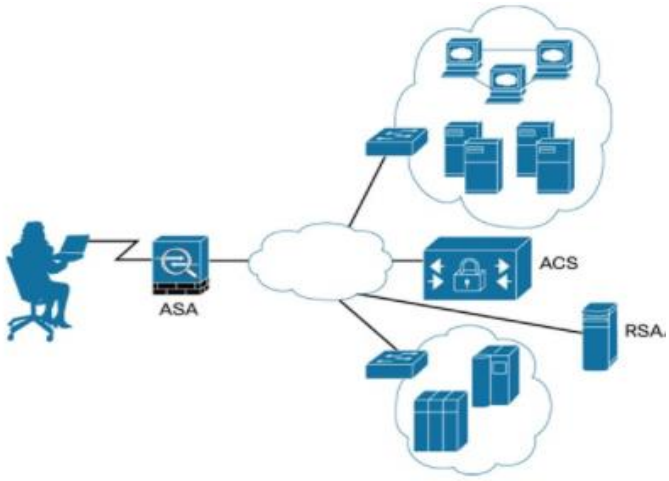

Figura 16. Autenticación, Autorización y Contabilidad (AAA)
Tomado de (Cisco Security, 2016)

En la tabla 11 se detallan los costos de los equipos ACS de Cisco.

Tabla 11.
Costos de ACS de Cisco.

ACS de Cisco		
Nombre	**Descripción**	**Costo**
CSACS-3.0	Cisco Secure ACS 3.0 for Windows	$5,995

Tomado de (Cisco, 2016)

3.2. Herramientas de Monitoreo de la red

Uno de las principales necesidades que una empresa debe contar para brindar sus servicios es el correcto funcionamiento de su red. Con el constante monitoreo de la misma se evitará la total inactividad o fallas en la red empresarial, afectando así tanto a sus usuarios, como a sus clientes. (Bustamante, 2013)

Al monitorear la red, se podrán evaluar y estar al tanto de su estado, en donde podremos tomar las medidas respectivas para solucionar los inconvenientes. Es por ello que al igual que muchas herramientas de red, dependerá mucho de nuestras necesidades y recursos para poder escoger cuál utilizar. (Bustamante, 2013)

Para la implementación de una herramienta de monitoreo se deben tomar en cuenta ciertos parámetros antes de hacerlo:

- Saber si la red requiere de la disponibilidad total de la red para brindar los servicios.
- El número de equipos es suficientemente grande para requerir de una herramienta de monitoreo.
- El tráfico en la organización es muy elevado y no puede ser controlado.

Una vez, comprobada el requerimiento de este componente, debemos saber que una herramienta de monitoreo nos podrá brindar muchas soluciones en el comportamiento de la red. (Bustamante, 2013)

Entre los principales beneficios que esta herramienta provee están:

- Optimizar los recursos y componentes que operan en la red.
- Determinar tráfico en todos los puntos de la red.
- Detección de tráfico ajeno a la red.

- Generación de logs y posterior análisis de la red, entre otros.

A continuación, se realizará el análisis de algunas herramientas, que se ha visto necesario nombrarlas debido a su importancia en el mercado empresarial y a las características que nos ofrecen.

3.2.1. Herramienta PRTG (Paessler)

Es un software que sirve para monitorear la red continuamente, diseñada para actuar 24/7 (24 horas y los 7 días de la semana). Esta herramienta fue diseñada para monitorear redes de todo tamaño, además gracias a su potente motor de monitorización y su rápida base de datos permite monitorear miles de sensores al mismo tiempo. Los datos de monitorización son guardados en una BDD para poder generar reportes históricos. (Paessler, Monitoree todo con PRTG, 2017)

PRTG se ejecuta en máquinas con sistema operativo Windows que se encuentran dentro de la red, recolecta varias características de los equipos, software y actividades realice la red etc. Un ejemplo de su funcionamiento se observa en la Figura 17.

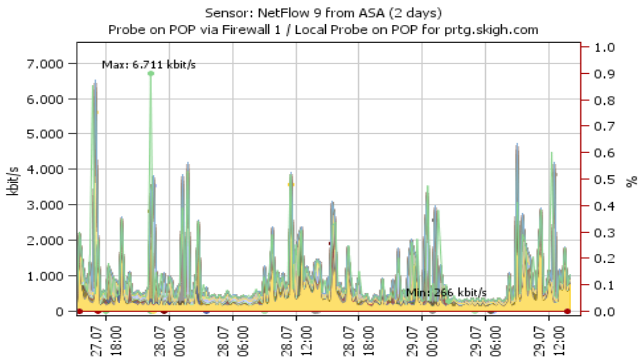

Figura 17. Análisis de red en PRTG.
Tomado de (PRTG, 2017)

PRTG cuenta con más de 200 tipos de sensores, tal y como se muestra en la Figura 18, los cuales tienen capacidades para la monitorización de ancho de banda y servidores como:

- “Monitorización del tiempo de actividad.
- Monitorización de memoria y procesador.
- Monitorización de espacio de disco y estado del disco.
- Monitorización de Firewall.
- Monitorización de Cisco.
- Sensores para monitorización de servidores SQL.
- Sensores para la monitorización de servidores virtuales.
- WMI, captura de paquetes, NetFlow y sensores SNMP para monitorización de ancho de banda de la red.” (Paessler, 2017)

Figura 18. Sensores dentro de PRTG.

Tomado de (PRTG, 2017)

La manera más sencilla de saber cómo trabajan los sensores es mediante el uso de colores, los mismos que indican el estado en el que se encuentra cada uno.

Lo interesante de esta herramienta es que se la puede utilizar para uso personal (de manera gratuita para determinado número de equipos) y comercial (pagada dependiendo de las características que se necesiten), además de ser fácil y rápido de instalar. Es una de las herramientas más usadas al rededor del mundo.

3.2.2. Herramienta *OCS Inventory*

Es un software libre que permite al personal de TI gestionar el inventario de sus activos de TI. Esta herramienta recoge información sobre hardware y software de equipos que están conectados a la red. A través de una interfaz web se puede visualizar el inventario. (OCSInventory, 2017)
OCS está compuesto por ejecutables:

- OCS Inventory Server: A través de esta herramienta se instalará el servidor que será el responsable de recopilar y administrar la información.

- OCS Inventory Agent: Esta aplicación será la que se deba instalar en los clientes que se desea inventariar. Es la responsable de brindar información al servidor.

Esta herramienta utiliza un servidor Apache, MySQL y Perl. OCS es multiplataforma, el rendimiento del lado del servidor es muy bueno. Un equipo con pocas características podrá realizar el inventario de varias máquinas sin ningún problema. El servidor pude ser instalado en sistemas operativos Linux, Windows, Mac OS X y Sun Solarias. (OCSInventory, 2017)

Es una herramienta de fácil instalación y configuración, gracias a la interfaz web (Figura 19) ofrece varios servicios entre ellos consultas de inventario, gestión de derechos de usuario, monitoreo de la red etc. Al ser una interfaz amigable con el usuario muchos lo usan como herramienta para HelpDesk. (OCSInventory, 2017)

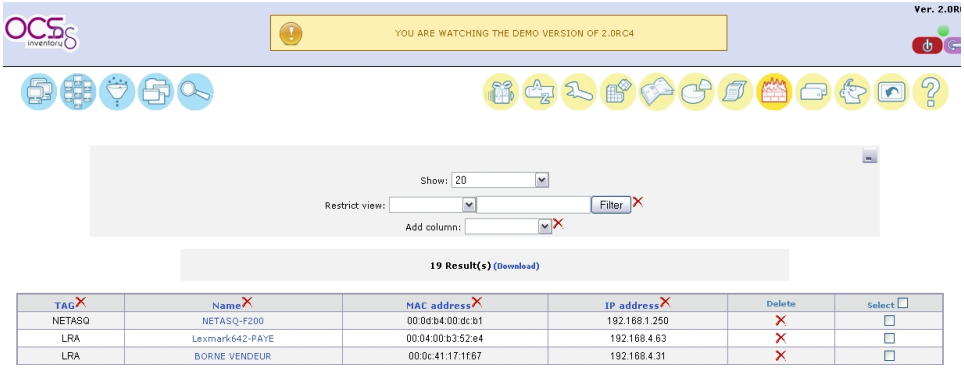

Figura 19. Análisis de red en *OCS Inventory*.
Tomado de (OCS, 2017)

3.2.3. Herramienta *WhatsUp Gold*

Al igual que PRTG, es una de las herramientas más utilizadas a nivel mundial, hoy en día con una nueva actualización: “WhatsUp Gold 2017”. Pues ofrece una nueva forma de interactuar y visualizar con todos los componentes que se encuentran conectados a la red empresarial, como se observa en la Figura 20.

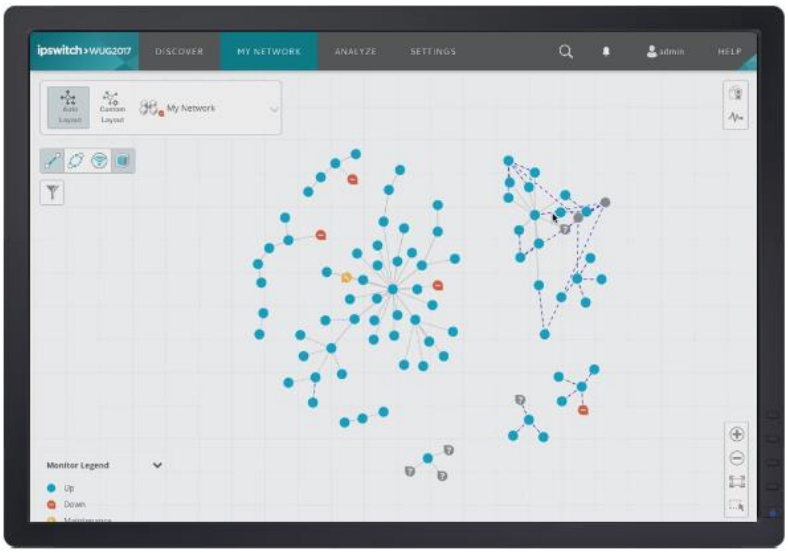

Figura 20. Monitoreo de red con *WhatsUp Gold.*
Tomado de (*WhatsUp*, 2017)

Las principales características que esta herramienta nos ofrece se detallan a continuación en el Diagrama 2:

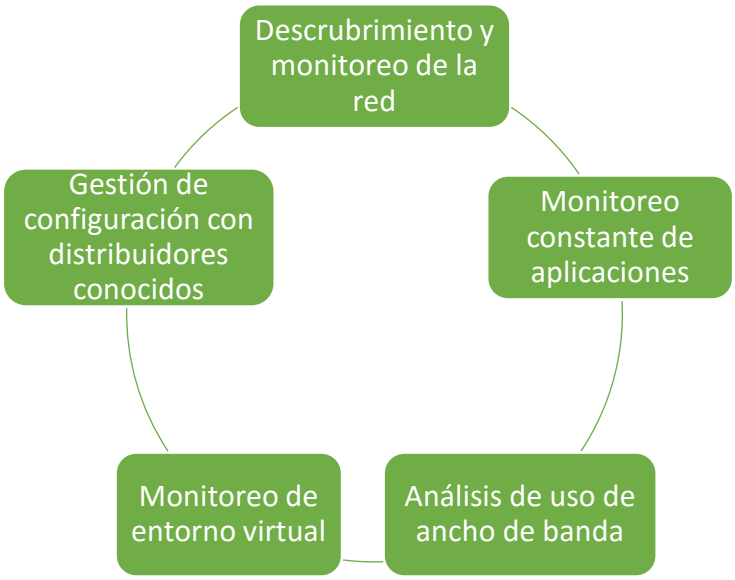

Diagrama 2. Características de *WhatsUp Gold*.
Tomado de (*WhatsUp*, 2017)

3.2.4. Análisis de costos de herramientas de monitoreo

Hay que destacar que la mayoría de estas herramientas de monitoreo son pagadas, esto se debe a que muchas de ellas cuentan con servicios complementarios que ayudan a mejorar los sistemas de control y monitoreo de la red.

A continuación, en la tabla 12 se muestra una comparación de las tres herramientas antes mencionadas, con respecto a costos.

Tabla 12.
Análisis de costos de herramientas de monitoreo

Análisis de costos de herramientas de monitoreo	
Nombre	**Precio**
PRTG	Desde $1,600.00
OCS Inventory	Gratis
WhatsUp Gold	Desde $5,500.00

Tomado de (*WhatsUp* Gold, PRTG, OCS Inventory, 2017)

3.2.5. Análisis de Herramientas para monitoreo de red

Al analizar las características de las dos herramientas de monitoreo de red como lo son PRTG y OCS, se ve claramente que PRTG es una herramienta que se enfoca más en el análisis de la red en una organización, en cambio OCS obtiene información acerca de los dispositivos que se encuentran conectados como se mencionó anteriormente, es más para inventario de equipos, sin embargo, también monitorea la red como tal.

PRTG es una de las herramientas de monitoreo de red más usada a nivel organizacional ya que ofrece muchas funcionalidades para mantener la red empresarial segura de cualquier actividad peligrosa, tomando en cuenta que los precios van acordes según los requerimientos que la empresa tenga.

Por otra parte, la nueva actualización de WhatsUp Gold es muy eficiente debido a la interfaz amigable y a la variedad de servicios que esta ofrece; a nivel empresarial es muy usado por lo antes mencionado, es por ello que sus costos son mayores comparado con otras herramientas de monitoreo.

4. Capítulo IV. Guía Técnica para la Implementación de Seguridad en una organización

En el presente proyecto de titulación se propuso la elaboración de una guía técnica para la implementación de un sistema de seguridad eficiente y funcional en una organizacional. Una vez analizadas algunas herramientas y componentes necesarios para establecer un ambiente de seguridad de red, se procede a determinar los pasos necesarios que una organización debe seguir para la implementación del sistema.

A continuación, se presenta un diagrama el cual muestra los pasos que se deben seguir para la implementación de seguridad en una organización:

Diagrama 3. Pasos a seguir para implementar seguridad de red.

4.1. Paso 1. Determinar la Situación actual de la organización

Antes de comenzar con la implementación de un sistema de seguridad se deberá analizar la situación actual de la empresa verificando con que equipos cuenta la red empresarial, así como también el número de usuarios que trabajan en la empresa. Esto será la base para la selección de un método de seguridad adecuado según sea el caso.

4.1.1. Componentes

Una red de comunicación empresarial básica al menos cuenta con los equipos que establecen las conexiones internas en la organización, es por ello que todos los equipos que conforman la red deberán ser tomados en cuenta para el análisis posterior de selección de equipos.

4.1.1.1. Equipos

El número de equipos en la red es muy importante al momento del análisis, pues equipos como: routers, servidores, switches, entre otros, determinarán los requerimientos iniciales de los sistemas de seguridad. Además de establecer un grado de seguridad y establecer un diseño específico para la implementación del sistema.

4.1.1.2. Herramientas y Sistemas

Una organización puede contar con sistemas y herramientas que ya estén trabajando actualmente. Al trabajar con cualquier tipo de software, se debe se realizar un análisis de compatibilidad de las herramientas al momento de adquirir los nuevos sistemas de seguridad.

4.1.1.3. Usuarios

Otro de los factores importantes al momento de adquirir un nuevo sistema, es identificar el número de usuarios con que la empresa cuenta y, sobre todo, los que utilizan los servicios de red. El número de terminales determinará la capacidad de control que se deberá establecer con respecto al control de acceso, cumplimiento de políticas, escaneo a la red, entre otros sistemas de seguridad, los cuales permitan mantener la red al margen con lo que se refiere a amenazas. (Injupemp, 2013)

4.2. Paso 2. Herramientas y mecanismos de seguridad de la red

Para la implementación de las distintas herramientas de seguridad, se deben especificar los puntos elementales donde la red pueda verse afectada ante posibles amenazas. En la tabla 13 se especifican algunos de estos puntos.

Tabla 13.

Puntos elementales para el análisis de la red

Puntos elementales para el análisis de la red	
RED	"Ausencia de pruebas de envío y recepción de mensajes.
	Líneas de comunicación sin protección.
	Tráfico sensible sin protección.
	Conexión deficiente de los cables.
	Punto único de fallas.
	Ausencia de identificación y autentificación de emisor y receptor.
	Transferencia de contraseñas "espionaje remoto".
	Gestión inadecuada de la red (tolerancia a fallas en enrutamiento).
	Conexiones de red pública sin protección."

Tomado de (Mintic, s.f.)

4.2.1. Seguridad Perimetral

La seguridad perimetral dentro de un sistema de red es un método de defensa lógico a nivel perimetral entre la red externa y la red interna. Es por ello que, se debe tener en cuenta este punto para que exista seguridad en este nivel de la red.

4.2.1.1. Firewall

Los principales componentes a nivel del perímetro son los firewalls. En este apartado se especificarán muchos aspectos para la selección del firewall como:

- *"Usuarios:* El número de usuarios activos que usan recursos de red.

- *Cantidad de Sesiones:* Un aproximado de las peticiones que un usuario realiza a redes externas (Internet).
- *VPN:* El uso de accesos remotos a la red.
- *Throughput:* Volumen de información que manejará el equipo.
- *Puertos:* El número de puertos necesarios según se requieran.
- *Nivel de Seguridad:* Tener en cuenta las funcionalidades y aplicativos para que un firewall pueda proveer de seguridad.” (GMTech, 2016)

Con los resultados realizados en el análisis de la situación actual, podremos proceder a escoger las características y marcas de productos que se van a adquirir. En anteriores capítulos se realizó una comparación de marcas y equipos que podrían servir de mayor ayuda.

4.2.1.2. Sistema de Detección y Prevención de Intrusos

La detección y prevención de intrusos será fundamental dentro de un ambiente organizacional, pues con equipos como estos podremos identificar las amenazas y contrarrestar el ataque antes que se realice.

La selección de este equipo dependerá netamente de las necesidades con que la empresa requiera. De igual manera en el capítulo 3 se describieron estos componentes y se realizó una comparación de tecnologías, lo cual puede ser útil al momento de elegir la herramienta.

Sin embargo, hoy en día se cuenta con un Firewall de siguiente generación, el cual a su vez realiza las funciones de prevención de intrusos y protector ante malware.

4.2.1.3. Control de Acceso a la red

El firewall realiza un control sobre todo el tráfico que ingresa a la red. Sin embargo, se recomienda establecer un sistema de control para los usuarios que soliciten acceso de ingreso lógico, permitiendo o negando el paso según las normas establecidas.

La implementación de un servidor de autenticación (AAA) puede ser muy útil para tener un mayor control sobre las peticiones de conexión al sistema. Es por ello que en el apartado de “Control de acceso a la red” y “Mecanismo de acceso seguro”, en el capítulo 3, se identificaron algunas tecnologías que pueden ser implementadas como complemento de un sistema de seguridad de red.

De igual manera se tomarán en cuenta aspectos como:

- Compatibilidad entre sistemas
- Soporte
- Funcionabilidad

4.3. Paso 3. Políticas de seguridad

Dentro de un sistema de gestión de seguridad, es primordial la creación y posterior implementación de políticas. Para el establecimiento de estas normas y políticas de seguridad, ha sido preciso basarse en la norma internacional de la ISO.

A continuación, en la tabla 14 se propone implementar las siguientes políticas de seguridad las cuales están determinadas en el documento de la ISO 27001. Esta tabla servirá de base para la creación de políticas según los requerimientos y el grado de seguridad que se desea implementar en la organización.

Tabla 14.

Políticas de Seguridad recomendadas para una organización.

Políticas de Seguridad necesarias en una empresa según normas 27001 y 27002	
Políticas de la seguridad de la información	
• Políticas de seguridad	✓
• Revisión de políticas	✓
Organización de la seguridad de la información	
Organización interna	
• Roles y responsabilidades en seguridad de la información	✓
• Contacto con las autoridades	✓
• Contacto con grupos de interés especial	✓
Los dispositivos móviles y el teletrabajo	
• Teletrabajo	✓
Gestión de activos	
Responsabilidad sobre los activos	
• Inventario de activos	✓
• Uso aceptable de los activos	✓
• Devolución de activos	✓
Clasificación de la información	
• Manipulado de la información	✓
Control de acceso	
Requisitos de negocio para el control de acceso	
• Política de control de acceso	✓
• Acceso a las redes y a los servicios de red	✓
Gestión de acceso de usuario	
• Registro y baja de usuario	✓
• Gestión de privilegios de acceso	✓
• Revisión de los derechos de acceso de usuario	✓
• Retirada o reasignación de los derechos de acceso	✓
Responsabilidades del usuario	
• Uso de la información secreta de autenticación	✓
Control de acceso a sistemas y aplicaciones	
• Restricción del acceso a la información	✓
• Procedimientos seguros de inicio de sesión	✓
• Sistema de gestión de contraseñas	✓
Seguridad de las operaciones	
Protección contra el software malicioso (malware)	
• Controles contra el código malicioso	✓
Copias de seguridad	
• Copias de seguridad de la información	✓

Registros y supervisión	
• Registro de eventos	✓
• Protección de la información de registro	✓
• Registros de administración y operación	✓
• Sincronización del reloj	✓
Seguridad de las comunicaciones	
Gestión de la seguridad de redes	
• Controles de red	✓
• Seguridad de los servicios de red	✓
• Segregación en redes	✓
Intercambio de información	
• Políticas y procedimientos de intercambio de información	✓
• Acuerdos de intercambio de información	✓
• Acuerdos de confidencialidad o no revelación	✓
Adquisición, desarrollo y mantenimiento de los sistemas de información	
Requisitos de seguridad en sistemas de información	
• Asegurar los servicios de aplicaciones en redes públicas	✓
• Protección de las transacciones de servicios de aplicaciones	✓
Gestión de incidentes de seguridad de la información	
Gestión de incidentes de seguridad de la información y mejoras	
• Responsabilidades y procedimientos	✓
• Notificación de los eventos de seguridad de la información	✓
• Evaluación y decisión sobre los eventos de seguridad de información	✓
• Respuesta a incidentes de seguridad de la información	✓
• Aprendizaje de los incidentes de seguridad de la información	✓
• Recopilación de evidencias	✓
Redundancias	
• Disponibilidad de los recursos de tratamiento de la información	✓
Cumplimiento	
Revisiones de la seguridad de la información	
• Cumplimiento de las políticas y normas de seguridad	✓

Tomado de (INEN-ISO, 2016)

4.4. Paso 4. Herramienta de Monitoreo

Finalmente, como último componente de seguridad, se ve la necesidad de recomendar un sistema de monitoreo de red. Detallados en el capítulo 3, los sistemas de monitoreo ayudarán a tener un control total de todos los elementos conectados a la red, y su implementación dependerá de:

- *"Manejabilidad*: Facilidad de uso y administración de la herramienta.
- *Funcionabilidad*: Variedad de funcionalidades que la herramienta de seguridad pueda ofrecer para mantener la red segura.
- *Desempeño*: Correcto funcionamiento de la herramienta ante ambientes pequeños o grandes dependiendo sus características." (GMTECH, 2016)

5. Capítulo V. Aplicación de la guía técnica en un caso de estudio enfocado al datacenter académico de la UDLA sede "Queri".

Dentro del presente proyecto de titulación se planteó el desarrollo de una guía técnica para la implementación de seguridad de red dentro de una organización, es por eso que se tomará como caso de estudio el datacenter académico de la Universidad de las Américas (UDLA) situado en el campus "Queri".

Esta guía técnica especificará detalladamente los procedimientos para implementar las seguridades necesarias según los requerimientos que se demanden y los componentes instalados con los que ya cuenta el centro de datos o la organización, analizando cada aspecto según lo mencionado en capítulos anteriores.

5.1. Situación actual

El centro de datos académico de la UDLA sede “Queri” cuenta actualmente con los siguientes equipos:

- Almacenamiento VNX3200-DC-QUERI.
- Chassis CISCO UCS MINI.
- CISCO NEXUS 3000.

El diseño efectuado por el Ing. Luis Pérez para el datacenter implementado en la UDLA campus Queri, detalla dentro de la tabla 15 las características de todos los componentes que conforman la red mencionada.

Tabla 15.

Equipos involucrados instalados en el datacenter.

Subsistema Networking				
Centro de datos: UDLA - Campus Queri				
No. de parte	Descripción	Cantidad	Detalle	Observaciones
N3K-C3524P-10GX	Cisco Nexus 3524	2	Switch Licenciamiento LAN Basic 24 puertos licenciados SFP+ Sistema Operativo NX-OS	Fuente de poder (2) y ventiladores redundantes, cables de poder C13-C14
Subsistema Computo				
Centro de datos: Campus Queri				
No. de parte	Descripción	Cantidad	Detalle	Observaciones

UCS-SPL-5108-AC2	Cisco UCS Chassis 5108	1	Chassis: 2 Fabric interconnect 6324	Fuente de poder (4) y ventiladores redundantes, cables de poder C19-C20. UCS Manager Embebido.
UCSB-B200-M4-U	Cisco UCS B200M4	12	Servidor Blade: 64GB RAM (4x16GB) 2 CPU (6 cores, 1.9GHz) Tarjeta VIC 1340	La tarjeta VIC puede virtualizar interfaces NIC y HBA según lo requerido.
Subsistema almacenamiento				
Centro de datos: Campus Queri				
No. de parte	Descripción	Cantidad	Detalle	Observaciones
V32D12-AN5PS6	VNXe 3200	1	Almacenamiento Controladoras redundantes 3 discos SD de 100GB para Fast Cache 6 discos SAS de 300GB 6 discos SAS de 1.2TB	Fuente de poder y ventiladores redundantes, cables de poder C13-C14

Tomado de (Pérez, 2016, p.10-11)

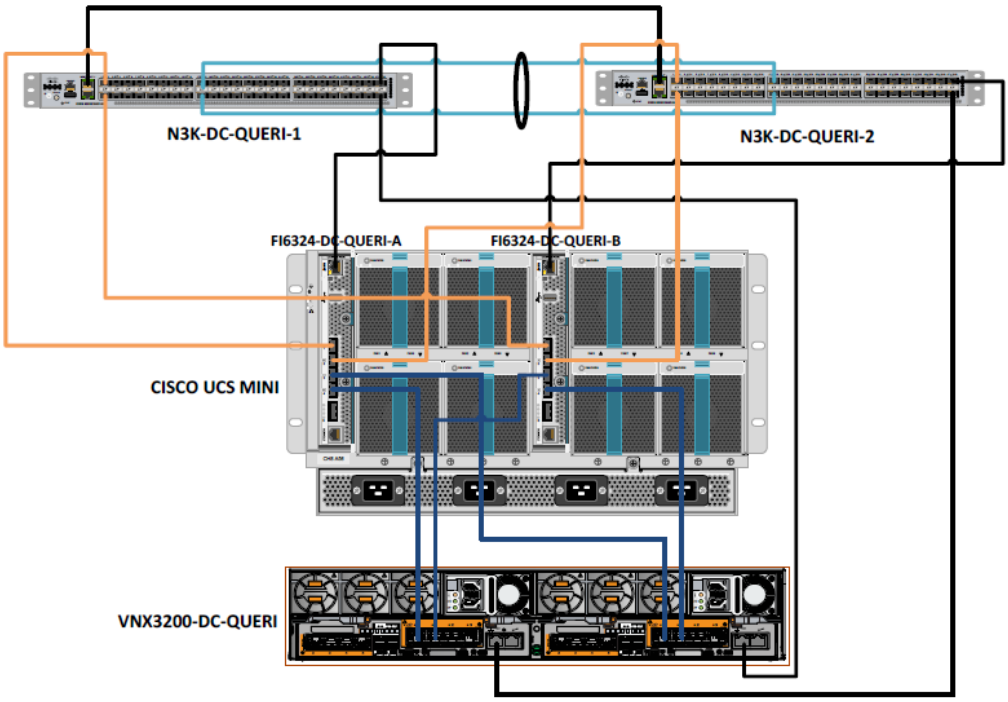

Figura 21. Diagrama topológico UDLA – Campus Queri*.*

Tomado de (Pérez, 2016)

Como se muestra en la figura 21, se cuenta con dos switchs capa 3 encargados de la conexión LAN redundante; posteriormente se encuentra instalado un equipo UCS que gestiona todos los componentes de red, cómputo y almacenamiento dentro del mismo equipo; finalmente el datacenter posee una solución de almacenamiento compartido.

5.2. Herramientas y mecanismos de seguridad de la red

La presente guía presentará un plan de seguridad a nivel de red, lo cual permitirá interconectar de manera segura la infraestructura implementada en el datacenter hacia la red general de la UDLA.

5.2.1. Seguridad perimetral

Hoy en día, una de las soluciones más convenientes que las organizaciones buscan al implementar un sistema de seguridad perimetral es el firewall de última

generación (NGFW) Cisco FirePOWER, al ser una marca reconocida según se evidenció en el cuadrante de Gartner (Figura 5).

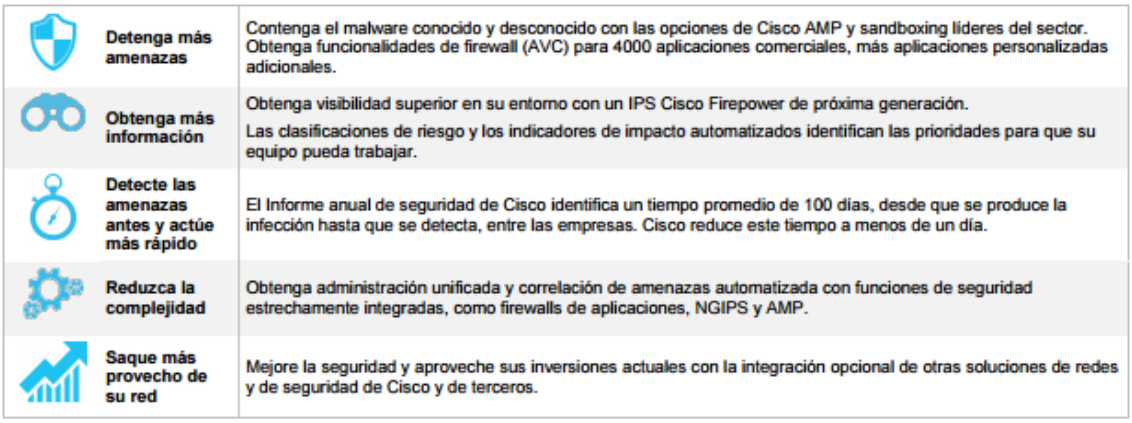

Figura 22. Funciones del Firewall NGGW.

Tomado de (Cisco, 2016)

5.2.1.1. Firewall y Sistema de Prevención de Intrusos

Teniendo en cuenta la situación actual de la red del datacenter académico de la UDLA sede Queri y al evidenciar que no cuenta con seguridad de red, se propone implementar un Firewall NGFW Cisco FirePOWER modelo ASA 5555-X como medida de prevención contra intrusiones ya que este equipo combina firewall de red con el IPS de última generación, brindando una protección contra malware avanzado. En la tabla 16 se muestran las características de este equipo.

Tabla 16.

Características del Firewall a implementar.

Subsistema Networking			
Centro de datos: Campus Queri			
No. de parte	**Descripción**	**Cantidad**	**Detalle**
ASA 5555-X FirePOWER Services	Cisco ASA 5555-X	1	FW de 4 Gbps. Multiservicio. 8 x 1 GE.

Tomado de (Cisco, 2016)

5.2.1.2. Dónde colocar el Firewall

El firewall se colocará en el punto donde la red interna se conecta hacia Internet o red externa como se puede observar en la figura 23. De esta manera el firewall podrá comprobar que el tráfico de la red es conforme a las políticas de seguridad del sistema.

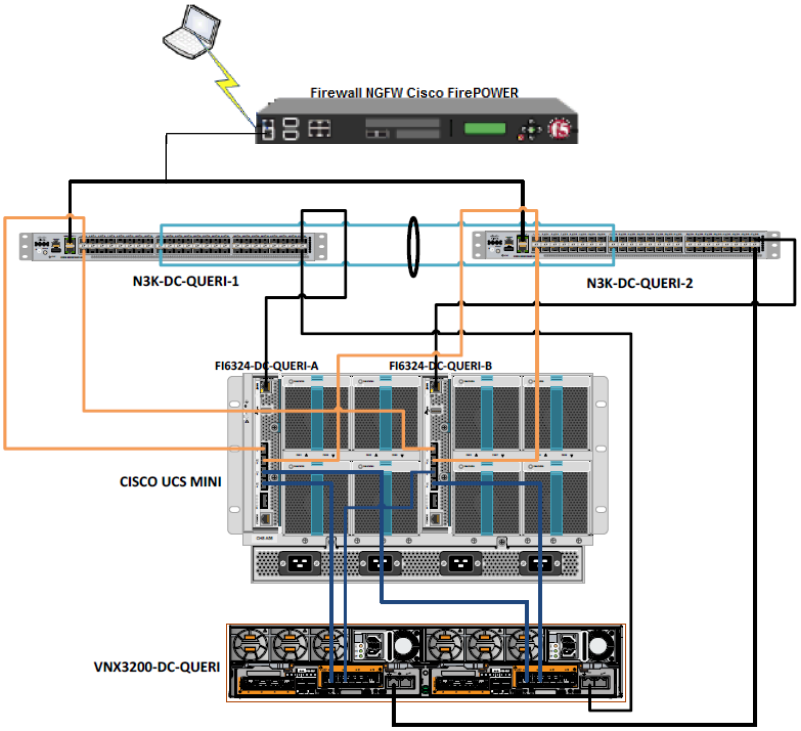

Figura 23. Ubicación de firewall en red del datacenter académico. Adaptado de (Pérez, 2016)

5.2.1.3. Costos y complejidad reducidos

“Cisco ASA con servicios FirePOWER incorpora un enfoque integrado de la defensa contra amenazas, que reduce los costos operativos y de capital, y la complejidad administrativa. Se integra sin inconvenientes con el entorno de TI, el flujo de trabajo y la estructura de red existentes. La familia de dispositivos es altamente escalable, funciona a velocidades hasta de multigigabits y ofrece seguridad sólida y uniforme en sucursales, el perímetro de Internet y los centros de datos de entornos físicos y virtuales”. (Cisco, 2016)

5.2.2. Control de acceso a la red

Se propone implementar un servidor de control de acceso Cisco (ACS) el cual provee servicio AAA (autenticación, autorización y contabilidad) a los dispositivos que estén conectados a la red como routers, servidores, conectores VPN etc.

5.3. Políticas de Seguridad

Puesto que los ataques lógicos, en su mayor parte, estarán orientados a la información almacenada en los servidores y a cómo está siendo procesada, se recomienda la implementación de las siguientes normas específicamente para el datacenter de la UDLA.

Tabla 17.

Normas generales de seguridad.

Directrices para normas de seguridad de la información		
Políticas para la seguridad de la información	Una vez definida cada política, estas deben ser aprobadas por los directivos y administradores de seguridad, posteriormente deberá ser documentado y notificado a cada uno de los usuarios involucrados.	✓
Revisión de políticas de seguridad	Las políticas deberán ser examinadas cada cierto intervalo de tiempo (6 meses, 1 año, más) o cada que se realicen cambios en los componentes del sistema.	✓
Seguridad relativa a recursos humanos		
Términos y condiciones	Los responsables de la administración y uso de los equipos y sistemas que conforman la red, deberán estar al tanto y de acuerdo con todas las políticas de seguridad implementadas.	✓

Finalización de empleo o cambio de funciones	Se debe especificar claramente dentro de los términos y condiciones la no divulgación de contraseñas o de información una vez terminadas sus funciones dentro del área.	✓
Seguridad de las operaciones		
Protección contra software malicioso	Se deben implementar las seguridades necesarias para la prevención y tratamiento de códigos maliciosos que afecten la red.	✓
Copias de seguridad	Se deben realizar respaldos de información y del sistema constantemente ante fallo o pérdida de los mismos.	✓
Registro de eventos	Se deben realizar registros de cada actividad realizada por los usuarios, alertas y eventos que correspondan con la seguridad de la red.	✓
Sincronización de reloj	Los relojes de todos los equipos que conforman la red deberán estar sincronizados con una fuente segura.	✓
Cumplimiento de políticas		
Cumplimiento de las normas y políticas de seguridad	Los directivos deben asegurar que todos los procesos se estén realizando de acuerdo a las políticas y normas planteadas para garantizar el aseguramiento de la red y de la información.	✓

Tabla 18.

Políticas de seguridad de la red

SEGURIDAD DE LAS COMUNICACIONES	
Políticas de la red	
La información que se almacena en los servidores o transita por la red, no puede ser eliminada, alterada o copiada sin consentimiento previo del responsable del recurso.	✓
Los datos generados a través de la red son responsabilidad del usuario que esté utilizando los recursos de la misma, no del Área de Sistemas.	✓

Los recursos y sistemas de red deberán ser únicamente utilizados para labores de la institución.	✓
Las cuentas de acceso correspondientes a los sistemas y recursos de la red son pertenencia de la institución, por lo tanto, no pueden ser transferidas ni usadas fuera de la misma.	✓
El uso de las herramientas de red deberá ser exclusivo para las funciones para las que fueron configurados y manejado por personal autorizado.	✓
Se deben identificar y documentar todas las herramientas y mecanismos de seguridad de red implementados dentro del datacenter para brindar una gestión más adecuada de todos los recursos de red en proceso.	✓
Accesos remotos	
El acceso a la red por medio de equipos remotos será permitido con previa autorización del administrador del área de sistemas y por medio de VPN's con las seguridades necesarias para el caso.	✓
Antivirus	
Los servidores y equipos que se conecten a la red deberán contar con un software de antivirus (adquirido por la Universidad) para su protección ante malware.	✓
El antivirus deberá estar activo las 24 horas le día, debidamente actualizado y en constante escaneo de software malicioso.	✓
La desinstalación y desactivación del antivirus estará restringida por una contraseña, administrada únicamente por el administrador del área de sistemas.	✓
RELACIÓN CON PROVEEDORES	
Políticas de seguridad en relaciones con proveedores	
El responsable del área de redes será el encargado de establecer los requisitos necesarios de seguridad para el acceso y manipulación de los sistemas y la información.	✓

Se debe mantener un monitoreo constante del enlace de comunicación y controlar todas las actividades que se realicen por medio de logs.	✓
Se debe garantizar el acceso a la red por medio de mecanismos de seguridad lógica (Firewall) y se debe validar la autentificación del usuario que desea hacerlo.	✓
Debe existir una revisión constante de los acuerdos entre terceros para garantizar el cumplimiento y correcta aplicación de las mismas.	✓
GESTIÓN DE ACTIVOS	
Políticas de usos de servicios de red	
Los administradores de red serán los encargados de gestionar los servicios de red que se ofrecen tanto a los usuarios internos como para terceros, dependiendo su rol en la institución.	✓
La gestión de perfiles y contraseñas a los servicios de red son responsabilidad de los administradores de red. Deberá ser confidencial y se prohíbe la divulgación de las mismas sin previa autorización.	✓
El administrador de la red del datacenter deberá realizar el monitoreo constante, con las herramientas de seguridad implementadas, revisar logs procesados y reportar cualquier anomalía en la red.	✓
Los administradores de red son el único personal autorizado para el manejo de los sistemas y mecanismos de seguridad de red en el datacenter.	✓
Los administradores podrán detener o realizar cambios en los servicios de algún componente de red en el caso de presentarse alguna anomalía en los mismos, con el permiso previo de los directivos según lo requiera.	✓
Cada usuario recibirá credenciales de acceso a la red y a sus distintas aplicaciones, dependiendo sus funciones de administradores de red. Estas credenciales serán administradas por el encargado del área.	✓
El jefe del área de sistemas podrá cancelar, con previa notificación a directivos, la cuenta de un usuario si este viola las normas y políticas de seguridad.	✓

Políticas de seguridad de equipos de comunicación	
Las configuraciones e información de los equipos de red deberá ser propiedad de la Institución y es prohibida su divulgación.	✓
Se debe proveer de la respectiva seguridad física para los equipos de red y acceso a los mismos para complementar con la seguridad lógica implementada.	✓
Se debe tener documentación detallada de la topología de red instalada, conjuntamente con los parámetros de configuración de los equipos.	✓
Políticas de seguridad de servidores	
Configuración e instalación	
Los administradores del área de tecnología son responsables de todas las instalaciones, configuraciones e implementación de seguridad en los servidores pertenecientes a la red de la institución.	✓
Es responsabilidad de los administradores de sistemas el control del funcionamiento adecuado y el respectivo mantenimiento sobre los servidores.	✓
Cada cambio que se realice en el servidor deberá ser reportado y autorizado por el jefe del área.	✓
El monitoreo constante debe ser realizado para garantizar la seguridad correspondiente a los servicios del servidor.	✓
Respaldos	
Se debe realizar el respaldo de los servidores diaria, semanal o mensualmente, según la criticidad de la información.	✓
Los logs de todos los procesos realizados deben ser constantemente revisados para garantizar la seguridad de los dispositivos.	✓
El resguardo de respaldos y logs deben tener el control de acceso pertinente y la seguridad necesaria.	✓

A continuación, se detallan las políticas de control de acceso a equipos que se deberán configurar en el servidor AAA:

Tabla 19.

Políticas de control de acceso a la red.

Control de acceso a la red	
“Es responsabilidad de cada administrador del sistema, que todos los servidores tengan estándares de configuración de seguridad de acuerdo al rol del servidor en la empresa.” (Injupemp, 2013)	✓
Solamente el usuario administrador tendrá acceso al ingreso de las interfaces del router y modificación de su configuración, a los demás usuarios se les negará este acceso y se deberá configurar los roles respectivos según los requerimientos de la organización.	✓
Es responsabilidad del administrador, “que las actualizaciones más recientes de seguridad sean instaladas en los servidores lo más pronto posible, validando previamente en ambientes de prueba para no afectar la continuidad del negocio.” (Injupemp, 2013)	✓
Es responsabilidad del administrador el bloqueo puertos de los servidores.	✓
Es responsabilidad del administrador realizar el monitoreo sobre el uso de centro de datos.	✓
Es responsabilidad del administrador guardar los logs de intentos no autorizados, logs de fallas de firewall y logs de intentos fallidos.	✓
Usuarios y Contraseñas	
“Es responsabilidad del área de TI la administración de usuarios, asignar un nombre único de usuario, la contraseña deberá ser robusta reservada en cada sistema informático, además, deben ser confidenciales e intransferibles.” (Injupemp, 2013)	✓
Se recomienda NO asignar códigos de identificación de usuarios genérico o universal, por ejemplo: udla1, udla2, udla3 etc.	✓
“Ningún usuario o programa debe utilizar contraseñas de administradores de sistemas, salvo personal autorizado.” (Injupemp, 2013)	✓
Los códigos de usuarios que cumplan un periodo de tres meses en estado inactivos serán desactivados por el departamento correspondiente.	✓
El usuario deberá cambiar su contraseña al menos una vez al mes.	✓

“Se limita a 3 el número de intentos infructuosos para introducir la contraseña de usuario, después del tercer y último intento la cuenta involucrada será bloqueada y se deberá notificar al área correspondiente para el desbloqueo de la misma.” (Injupemp, 2013)	✓
No se recomienda tener múltiples sesiones de usuario abiertas en diferentes máquinas.	✓

5.4. Herramienta de monitoreo de red

Finalmente, se ha visto la necesidad de recomendar una herramienta de monitoreo de red que permita tener un control total de todos los elementos conectados dentro de la misma.

Una vez analizado algunos motores de monitoreo de red en capítulos anteriores, una de las soluciones más convenientes para el caso de estudio es la herramienta “PRTG”. Pues las varias funciones que ofrece y su dinámica interfaz de administración puede ser una de las mejores opciones para su implementación dentro del centro de datos académico, tal como se observa en la figura 24.

Figura 24. Funciones de herramienta “PRTG”.
Tomado de (PRTG, 2017)

A pesar de ser una herramienta con licenciamiento, sus costos no son tan elevados como “WhatsUp Gold”, además incluye muchas funciones que hace de esta herramienta muy robusta y eficiente.

6. CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

Una vez finalizado el presente trabajo de titulación se puede concluir lo siguiente:

A lo largo del desarrollo de la guía técnica se realizó un análisis de los distintos mecanismos y herramientas de seguridad de red que serán útiles al momento de implementar seguridad dentro de una empresa.

Debido a las vulnerabilidades que presentan hoy en día las redes empresariales y las amenazas que afectan a la misma, es necesaria la implementación de seguridad tanto física como lógica; sin embargo, esto no asegura tener un sistema totalmente confiable pues dependerá también de una correcta administración de la red.

Se determinó la importancia de implementar políticas de seguridad en una empresa, ya que de esta manera se está brindando una solución que busca no solamente cuidar y administrar eficazmente la información, sino también busca prevenir las amenazas que puedan perjudicar a la red, por ello se debe contar con equipos y herramientas de seguridad, acopladas a un sistema de gestión de las mismas por medio de normas y políticas.

Es necesario que todos los usuarios que conforman la organización tengan conocimiento de las políticas de seguridad implementadas, pues de esta manera se asegurará el cumplimiento de las normas, con el fin de que se tenga un uso adecuado de los recursos de la empresa.

Se identificaron las distintas políticas de seguridad para la realización del modelo de solución para la implementación de seguridad en la red, según lo detalla las normas ISO 27000-1.

Una vez realizado el análisis de tres herramientas de monitoreo tales como: PRTG, WhatsUp y OCS Inventroy, se determinó que PRTG es la herramienta más aconsejable debido a que sus características y funcionalidades van de acuerdo a los requerimientos para el datacenter académico.

Tras un análisis de herramientas para seguridad de red se determinó que los NGFW son hoy en día una de las mejores soluciones que las empresas pueden implementar debido a que este equipo combina firewall de red con el IPS de última generación, brindando una protección contra malware avanzado.

Finalmente, en el caso de estudio enfocado al datacenter académico de la UDLA sede Queri, se realizó un análisis de los componentes y herramientas de seguridad que este sistema necesita, aplicando los requerimientos establecidos acorde a la guía técnica.

6.2. Recomendaciones

Se consultaron diferentes productos de uso comercial relacionados con los sistemas de protección para la red y se recomienda el uso del ASA 5555-X with FirePOWER Services para el datacenter académico de la UDLA, puesto que este equipo tiene incluido IPS y cumple con varias características y funciones para protección contra amenazas.

A pesar de tener equipos de seguridad, se recomienda el uso de la herramienta de monitoreo de red PRTG, la cual es capaz de analizar y mantener un control constante de todos los equipos conectados en la red del datacenter de la UDLA.

Para el control de acceso a la red, se recomienda la implementación del servidor de control de acceso Cisco (ACS) que permita la autenticación autorización y contabilidad de los equipos que requieran conexión a la red.

Para la implementación de seguridad de red en una empresa, es necesario realizar un análisis previo de la situación actual de la red. Los equipos y mecanismos a instalarse dependerán de los requerimientos de la empresa y los recursos con los que dispongan.

Se recomienda implementar políticas de seguridad que abarquen otras perspectivas, ya que las planteadas en el presente proyecto de titulación fueron enfocadas únicamente a la red.

Al momento de escoger un equipo o herramienta de seguridad, se debe tomar en cuenta un crecimiento lógico o físico de la red, teniendo así cuenta un sistema escalable ante un futuro aumento de usuarios y componentes.

Finalmente, se recomienda el uso de esta guía técnica como base para establecer un sistema de seguridad dentro de una organización.

REFERENCIAS

AdvisorSecurity. (s.f.). Cuadrante mágico de firewall para redes empresariales. Recuperado el 20 de Abril de 2017, de http://www.sadvisor.com/2015/07/14/cuadrante-magico-de-firewall-para-redes-empresariales-2/

Bonilla, M. (2016). ANÁLISIS Y DISEÑO DE UN SISTEMA DE SEGURIDAD DE RED PERIMETRAL. Recuperado el 13 de Abril de 2017, de http://repositorio.puce.edu.ec/bitstream/handle/22000/11158/BonillaAlejandra_SeguridadPerimetralADS.pdf?sequence=1

Bustamante, R. (2013). Seguridad de Redes. Recuperado el 28 de Abril de 2017, de https://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Seguridad%20en%20redes.pdf

Cicenia, K., & Vásconez, V. (2011). Análisis de la tecnología IBNS como solución AAA para el Control de Acceso. Riobamba.

Cisco. (2005). Servicios cisco para sistema de prevención de intrusiones. Recuperado el 6 de Abril de 2017, de http://www.cisco.com/c/dam/global/es_mx/products/servicios/docs/IPS_external_qa_clients_Spanish.pdf

Cisco. (2007). Soluciones de Cisco para la prevención de intrusiones. Recuperado el 20 de Abril de 2017, de http://www.cisco.com/c/dam/global/es_es/assets/publicaciones/07-08-cisco-IPS.pdf

Cisco. (2016). Basic Intrusion Prevention System (IPS) Concepts and Configuration. Recuperado el 15 de Marzo de 2017, de http://www.ciscopress.com/articles/article.asp?p=1722559

Cisco. (2016). CCNP Security - sitics. Recuperado el 13 de Mayo de 2017, de https://networkfaculty.com/es/courses/coursedetail/33-curso-ccnp-security---sitcs

Cisco. (2016). Cisco ASA with FirePOWER Services. Recuperado el 25 de Abril de 2017, de http://www.cisco.com/c/es_mx/products/security/asa-firepower-services/index.html

Cisco. (2016). Cisco NAC Appliance (Clean Access). Recuperado el 10 de Abril de 2017, de http://www.cisco.com/c/en/us/products/security/nac-appliance-clean-access/index.html

Cisco. (2016). Firewall de próxima generación Cisco Firepower. Recuperado el 8 de Mayo de 2017, de http://www.cisco.com/c/dam/global/es_mx/assets/pdfs/c78-736661-00_cisco_firepower_next-generation_firewall_ds_v4a_es-xl.pdf

Cisco. (2017). Cisco ASA 5555-X. Recuperado el 20 de Abril de 2017, de http://www.cisco.com/c/en/us/support/security/asa-5555-x-adaptive-security-appliance/model.html

DoD. (1985). Trusted Computer System Evaluation Criteria. Recuperado el 5 de Abril de 2017, de http://csrc.nist.gov/publications/history/dod85.pdf

ESET. (2005). ¿Qué es un 0-day? Recuperado el 8 de Marzo de 2017, de https://www.welivesecurity.com/la-es/2015/02/25/que-es-un-0-day/

Estévez, E. (2007). Conociendo Microsoft Network Access Protection (NAP). Recuperado el 18 de Abril de 2017, de https://www.microsoft.com/latam/technet/articulos/tn/2007/abr-17.mspx

Flores, J., & Puppi, G. (2013). Gestión de la seguridad física y lógica para un centro de datos. Recuperado el 28 de Marzo de 2017, de http://repositorioacademico.upc.edu.pe/upc/bitstream/10757/301540/2/flores_ej-pub-delfos.pdf

FORTINET. (2017). FortiGate Next Generation Firewalls. Recuperado el 13 de Mayo de 2017, de https://www.fortinet.com/products/firewalls/firewall.html

Fortinet. (s.f.). Mid-Range NGFW Comparison Guide. Recuperado el 20 de Mayo de 2017, de http://wit.co.th/fortinet/resources/Mighty_Guides_Mid-Range_NGFW_Comparison.pdf

Garzón, G. (2015). PROPUESTA PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE DETECCIÓN DE INTRUSOS. Recuperado el 8 de Abril de 2017, de http://repository.unad.edu.co/bitstream/10596/3494/3/86057594.pdf

GMTECH. (2016). Firewall: 10 tips prácticos para escoger el correcto. Recuperado el 5 de Mayo de 2017, de https://www.gmtech.es/firewall-tips-escoger-correcto/

Gómez, A. (s.f.). Tipos de ataques e intrusos en las Redes informáticas. Recuperado el Marzo de 15 de 2017, de http://www.edisa.com/wp-content/uploads/2014/08/Ponencia_-_Tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf

GroupTrustedComputing. (2011). Trusted Network Connect (TNC). Recuperado el 6 de Abril de 2017, de https://www.trustedcomputinggroup.org/wp-content/uploads/TNC_OpenStandards_April2011.pdf

INEN. (2006). Normalización y actividades conexas - Vocabulario general. Recuperado el 14 de Abril de 2017, de http://www.normalizacion.gob.ec/wp-content/uploads/downloads/2013/11/gpe_iso_iec_2_2.pdf

INEN-ISO/IEC. (2016). NTE INEN-ISO/IEC 27001. Recuperado el 24 de Marzo de 2017, de http://www.normalizacion.gob.ec/wp-content/uploads/downloads/2016/05/nte_inen_iso_iec_27001.pdf

Injupemp. (2013). Políticas de seguridad de las tecnologías de información y comunicaciones. Recuperado el 5 de Mayo de 2017, de http://www.injupemp.gob.hn/images/Politicas_Seguridad__Informacion.pdf

ITSecure. (s.f.). Network Access Control NAC. Recuperado el 3 de Abril de 2017, de https://www.secureit.es/sistemas-de-seguridad-it/network-access-control-nac/

Kissel, R. (2013). Glossary of Key Information Security Terms. Recuperado el 20 de Marzo de 2017, de http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Microsoft. (1997). ¿Cómo podemos definir un Firewall? Recuperado el 19 de Marzo de 2017, de https://support.microsoft.com/es-es/help/550606

MINTIC. (2016). Seguridad y Privacidad de la Información. Recuperado el 24 de Marzo de 2017, de https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Mintic. (s.f.). Seguridad y Privacidad de la información. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

OCSInventory. (2017). OCS Inventory NG. Recuperado el 6 de Mayo de 2017, de https://www.ocsinventory-ng.org/en/

Omar, D. (s.f.). Control de Acceso a Redes. Recuperado el 13 de Abril de 2017, de http://postgrado.info.unlp.edu.ar/Carreras/Especializaciones/Redes_y_Seguridad/Trabajos_Finales/Esmoris.pdf

Pacheco, J. (s.f.). Niveles de seguridad informática. Recuperado el 18 de Marzo de 2017, de http://masdejava.blogspot.com/2016/04/niveles-de-seguridad-informatica-orange.html#.WSsmF2g1_IU

Paessler. (2017). Monitoree todo con PRTG. Recuperado el 6 de Mayo de 2017, de https://www.es.paessler.com/monitoring-topics

Paessler. (s.f.). Herramienta de análisis de red. Recuperado el 25 de Abril de 2017, de https://www.es.paessler.com/network_analyzer_tool

Panda. (2017). ¿A qué se denomina Sistema de Prevención de Intrusos o IPS? Recuperado el 15 de Mayo de 2017, de http://www.pandasecurity.com/elsalvador/support/card?id=31452&IdIdioma=1

Pérez, L. (2016). Proyecto Data Center Laboratorio Queri. Universidad de las Américas, Quito.

RedIRIS. (2002). Seguridad física de los sistemas. Recuperado el 24 de Marzo de 2017, de https://www.rediris.es/cert/doc/unixsec/node7.html

UNAM. (s.f.). Mecanismos de seguridad de red. Recuperado el 5 de Mayo de 2017, de http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/174/A6.pdf?sequence=6

UTA. (2016). Políticas Generales de Seguridad de la Información. Recuperado el 21 de Marzo de 2017, de http://ditic.uta.edu.ec/wp-content/uploads/2016/10/POLITICAS-GENERALES-DE-SEGURIDAD-DE-LA-INFORMACI%C3%93N.pdf

WhatsUp. (2017). WhatsUp® Gold Network Monitoring. Recuperado el 13 de Mayo de 2017, de https://www.ipswitch.com/application-and-network-monitoring/whatsup-gold