UNIVERSIDAD JOSÉ ANTONIO PÁEZ

EVALUACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA EN LA RED CORPORATIVA DE MONTANA GRÁFICA C.A.

Autor:

Manuel A. Colmenares E.

Urb. Yuma II, Calle Nº 3. Municipio San Diego – EDO. Carabobo

Teléfono: (0241) 8714240 (master) – Fax: (0241) 8712394

REPÚBLICA BOLIVARIANA DE VENEZUELA

UNIVERSIDAD JOSÉ ANTONIO PÁEZ

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA EN TELECOMUNICACIONES

EVALUACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA EN LA RED CORPORATIVA DE MONTANA GRÁFICA C.A.

Informe de Pasantías presentado como requisito para optar al título

de

INGENIERO EN TELECOMUNICACIONES.

Autor: Manuel Alejandro Colmenares Estupiñan
C.I.: V-23.825.751.
Tutor: Rainier Blanco

San Diego, Octubre del 2019

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE TELECOMUNICACIONES
INGENIERÍA EN TELECOMUNICACIONES

EVALUACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA EN LA RED CORPORATIVA DE MONTANA GRÁFICA C.A.

CONSTANCIA DE APROBACION

TUTOR EMPRESARIAL

Lic. Moises Alfonzo
C.I. 7.122.690

TUTOR ACADEMICO

Ing. Rainier Blanco
C.I. 11.556.607

Autor: Manuel A. Colmenares E.
C.I. 23.825.751

San Diego, Octubre del 2019

AGRADECIMIENTOS

Primeramente, a Dios por darme vida y salud para poder llegar a este momento tan importante de mi vida.

A mi abuela María Amelia quien hoy ya no está conmigo físicamente, por demostrarme que vale más el ser persona que cualquier título académico.

A mi abuela María Margarita quien hoy ya no está conmigo físicamente, por enseñarme a luchar y no rendirme por las cosas que deseo.

A mi padre José Abel Colmenares por siempre poner en un segundo plano sus necesidades por mi futuro y por demostrarme que nunca es tarde para alcanzar lo que se desea.

A mi madre Thannia Estupiñan por siempre creer en mí en las adversidades y ver un futuro en mí que ni yo mismo veía.

A mi hermana Anggie Rivero, por ser la mejor hermana madre que pude tener y jamás poner en duda mis habilidades.

A mi hermano Abel Colmenares por enseñarme el valor del esfuerzo y exigirme siempre lo mejor para no conformarme nunca.

A mi sobrino Emilio Marquez por ser una pequeña alegría que me impulsa a nunca desistir de mis sueños para así poder ser un ejemplo para él.

A mi tía Osana Estupiñan y mi tio Carlos Vera por abrirme las puertas de su casa cuando llegue a la ciudad de Valencia a continuar mis estudios universitarios.

A Freddy Rivero y Milagro Rivero por abrirme las puertas de su casa durante 6 meses cuando no tenían ningún compromiso conmigo.

A mis compañeros de estudio por toda la ayuda prestada a lo largo de la carrera universitaria.

A todas las grandes amistades como Daniel Mora, Dhamarys Bellorin, Cesar Méndez, Martin Serrano, José Hernández, José Rafael Rivas por hacer de mi estadía en la ciudad de Valencia más amena.

A mis amigos de toda la vida Daniel Moreno, Cristhian Hernández, Williams Bustos, Yves Chacón, Isaac Ruiz, Nicolás Contreras, Walter Zambrano y Gilmer Chávez por su apoyo a la distancia.

A Corimon C.A por permitirme realizar las pasantías y a todo el departamento de TI por las enseñanzas.

A mi tutor académico Rainier Blanco por sus enseñanzas y apoyo durante el desarrollo de mi trabajo de aplicación profesional.

A la Universidad Nacional Experimental del Táchira (UNET) por abrirme las puertas en el ámbito universitarios y a la Universidad José Antonio Páez (UJAP) por recibirme y permitirme cerrar este ciclo de mi vida.

INDICE

Lista de Figuras

Lista de Tablas

INTRODUCCIÓN

El siguiente trabajo de aplicación de pasantía es un aporte académico para la escuela de ingeniería en telecomunicaciones de la Universidad José Antonio Páez, ya que se enfoca en aplicar conocimientos adquiridos durante la carrera para así por poder actualizar la seguridad en la red empresarial de Montana Grafica C.A.

Hoy en día el concepto de seguridad no solo se limita a lo tangible más bien en las últimas décadas es mucho el valor que ha tomado la seguridad de la información ya que lamentablemente esta ha ganado más protagonismo.

El concepto de seguridad de la información no es solo eliminar virus o bloquear hackers que puedan acceder a la red. La seguridad en información abarca también los procedimientos que deben seguir los empleados y la dirección de una compañía para garantizar la protección de los datos confidenciales frente a las amenazas actuales.

El desarrollo de este trabajo de aplicación profesional está estructurado en cinco capítulos, los cuales están compuestos de la siguiente manera:

En el capítulo I se refleja la información acerca de la empresa. En el capítulo II se presenta el planteamiento del problema, formulación del problema, objetivo general, objetivos específicos, justificación, limitación y alcance. En el capítulo III se plantean los fundamentos teóricos necesarios para poder ejecutar la actualización de la seguridad como son antecedentes, bases teóricas, definición de términos básicos. En el capítulo IV se aprecia la metodología planteada para realizar el trabajo de pasantía y finalmente en el capítulo V se expresan los resultados obtenidos.

CAPITULO I

LA EMPRESA

1.1 Razón social y reseña histórica

Corimon es una empresa especializada en cuatro áreas de negocios, Pinturas, Productos, Resinas y Empaques. El ámbito de actuación de Corimon es Venezuela y sus mercados de influencia regional donde busca consolidar su presencia comercial mediante una agresiva estrategia de mercado que aumente el valor del negocio para sus accionistas y les garantice a sus clientes productos competitivos en oportunidad, calidad y precio.

Pinturas Montana, C.A. (actualmente Corimon Pinturas C.A.), es una de las primeras fábricas de pinturas en Venezuela. Comenzó operaciones en 1949 con el nombre de “Montana Fábrica de Pinturas” y rápidamente se consolidó en el mercado nacional durante la década de los años 50.

En 1959 se constituyó Montana Gráfica como la segunda empresa del Grupo Corimon y posteriormente, durante ese mismo año, se creó Resimon con el fin de cubrir las necesidades de Pinturas Montana en cuanto a resinas y así reemplazar la importación de las mismas. Desde sus inicios tanto Montana Gráfica como Resimon trabajaron independientemente de Pinturas Montana.

En la figura 1 se puede apreciar los comienzos de pinturas Montana.

Figura 1. Pinturas Montana en sus inicios.

Fuente:http://www.corimon.com/

Una vez consolidada en el mercado arquitectónico, Pinturas Montana, se inició en los segmentos de mantenimiento industrial, madera, marino y automotor. En este último, elaboró fondos que sirvieran de base para la aplicación de pinturas, haciendo de Chrysler y General Motors sus primeros clientes.

El grupo comenzó a contribuir con el desarrollo del país, no sólo a través de la inversión en el sector industrial, sino haciendo constantes aportes a la educación y a la cultura, por medio de fundaciones y centros culturales, ya que la responsabilidad empresarial social es uno de sus más preciados nortes.

El primer gran proyecto de Pinturas Montana, fue durante la presidencia del General. Marcos Pérez Jiménez, y consistió en pintar los túneles de la Autopista Caracas-La Guaira. Para esta obra se elaboró un aditivo especial que evita en gran medida la adherencia de suciedad, que protegió a los túneles y mantuvo su pintura en buen estado durante muchos años. A comienzos de la década de los setenta se incorporan a las empresas existentes Grafis, Cerdex, entre otras.

En 1993 Corimon incursiona en el mercado de capitales, a través de la cotización de sus acciones comunes en la bolsa de valores de Caracas y la bolsa de valores de Maracaibo, y de sus ADR's en la bolsa de Nueva York.

En 1994, Corimon se concentró en el mercado de pinturas, beneficiado por su posición como uno de los grupos empresariales privados más grandes y respetados de Venezuela y a través de sus compañías Montana, Pinco Pittsburgh, Wantzelius, Construcentro, Cerdex, Colorín, Sissons Paints, General Paint Company y Standard Brands, inicia operaciones en México, Colombia y en la Costa Suroeste de los Estados Unidos, a la vez que afianzan sus operaciones en Venezuela, Argentina y el Caribe.

En la actualidad el Grupo Corimon se ha concentrado en el mercado nacional y es un Grupo absolutamente vanguardista en lo que respecta a su alta participación de mercado en todas las áreas en donde incursiona. A su vez, posee en sus producciones equipamiento de última tecnología, se destaca en su organización, su alto estándar de calidad y en su solidez financiera.

Al presente el Grupo Corimon está compuesto por tres divisiones, las cuales se pueden ver reflejadas en la tabla 1.

Tabla 1. Divisiones del Grupo Corimon.

División de pinturas	
· Corimon Pinturas, C.A. · Tiendas Montana, C.A. · Cerdex, C.A.	
División de Resinas	**División de Empaques**
· Resimon C.A.	· Montana Grafica C.A.

Fuente: El Autor.

Montana Gráfica es una de las empresas industriales afiliadas al Grupo Corimon. En los años 50, había una sola empresa en este grupo, Pinturas Montana, en la cual funcionaba un departamento de imprenta donde se hacían etiquetas para las latas de pintura, cartas de color y material impreso de publicidad y de promoción. Ya en el año 1959 ese departamento había crecido mucho y además tuvo tanto éxito en la presentación de sus productos que se decidió separarlo de la fábrica de pinturas y darle vida propia. Así nació Montana Grafica, Compañía Anónima.

Se seguía produciendo material impreso para Pinturas Montana, empezando a desarrollar también actividades para otros clientes, tales como impresión de almanaques artísticos, etiquetas de todo tipo, estuches para alimentos y productos de limpieza, marquillas para cigarrillos y otros trabajos de impresión litográfica, siempre de papel o de cartón.

En 1961 dos años después de su fundación como empresa separada, Montana Grafica absorbió a la Litografía Miangolarra. La empresa estaba funcionando desde el principio en Los Ruices, pero en 1964 se mudó a Boleíta donde sigue operando la Litografía.

Al mismo tiempo empezó a trabajar con materiales nuevos, llamados flexibles, tales como envoltorios de todo tipo para alimentos, cosméticos, productos farmacéuticos, entre otros. Estos materiales no se podían imprimir por el sistema litográfico, por lo que tuvo que aprender y absorber la tecnología del retrograbado, la cual es la producción de materiales flexibles, donde hay las mayores innovaciones tecnológicas, tendientes a mejorar más y más la conservación del alimento, la facilidad y el ahorro en la distribución de los productos para el consumidor, y también la belleza de la presentación.

Para finales de los años 70, la planta de Boleíta resultó demasiado pequeña para contener las actividades de la Litografía y de la conservación de los empaques flexibles. Así nació la planta de Mariara. En la actualidad, la planta de Mariara ya no es simplemente una imprenta, más bien, es una industria donde se producen materiales de empaque a base de laminaciones, revestimiento y embozado, son todas las operaciones llamadas “de conversión”, con materia prima de calidad y tecnología de punta.

En el día de hoy Montana Grafica C.A. garantiza la calidad de sus empaques desde el mismo momento de su concepción, gracias a la amplia gama de servicios que ofrece: diseño gráfico, separaciones, selecciones y pruebas de colores, montajes, grabación de cilindros para impresión en retrograbado y flexografía e investigación de materiales para el desarrollo de nuevos empaques.

Desde su arranque fue preocupación de la junta directiva y personal técnico, fabricar y comercializar un producto de calidad, por lo que, mediante la revisión periódica de los elementos estratégicos, ha identificado como elementos clave el alcanzar calidad superior a sus competidores a costos competitivos. Es por ello que se estableció como meta mantener un Sistema de Gestión de la Calidad bajo los lineamientos de la Norma Venezolana COVENIN – ISO 9001:2008.

En la figura 2 se puede apreciar la fachada de Montana Grafica C.A.

Figura 2. Montana Grafica C.A; Sector Agua Blanca Mariara, Estado Carabobo.

Fuente:http://www.corimon.com.

1.2 Misión

Proveer empaques flexibles adaptados a las necesidades y exigencias de los clientes a través de tecnología de vanguardia, el mejoramiento continuo de los procesos y prácticas, eficiencia, recurso humano motivado, rol social activo y compromiso con el medio ambiente, generando así valor a los accionistas.

1.3 Visión

Ser el empaque flexible donde todos los productos de América Latina deben estar.

1.4 Política integral de calidad e inocuidad

En Montana Grafica se trabaja con el compromiso de producir empaques flexibles de la más alta calidad, garantizando su inocuidad a través del mejoramiento continuo de sus procesos, la integración y comunicación de objetivos comunes en toda la cadena de suministro, en concordancia con la legislación vigente y superando las expectativas de sus clientes.

1.5 Política de seguridad, salud y ambiente

En Montana Grafica se fabrican y comercializan empaques flexibles, satisfaciendo las necesidades de sus clientes bajo estrictas normas de calidad, protección del ambiente, seguridad y salud laboral.

Mediante un proceso de mejora continua se compromete a:

1. Adecuar el nivel de servicio a los requerimientos del cliente
2. Prevenir accidentes y proteger la salud de los trabajadores y terceros
3. Preservar el medio ambiente y uso eficiente de los recursos naturales

4. Cumplir con las exigencias legales y lineamientos corporativos relativos a la seguridad, salud y ambiente.

1.6 Valores

1. **Integridad:** los trabajadores de Montana Grafica siempre actúan de buena fe y con los mejores propósitos. Todas sus acciones están enmarcadas dentro de más alto sentido ético y moral.
2. **Respeto y confianza:** en Montana Grafica confía en las capacidades e intenciones de los demás. Se profesa el respeto mutuo en todas las relaciones interpersonales.
3. **Excelencia:** la gestión está orientada a la creación del máximo valor posible en todo lo que se hace, en miras de aumentar constantemente la competitividad.
4. **Innovación:** Montana Grafica se adecúa a las necesidades del mercado para ser los primeros en satisfacerlas
5. **Compromiso Mutuo:** Montana Gráfica se compromete a brindar a sus trabajadores la oportunidad para que cada uno potencie su desarrollo personal y profesional, limitado solo por la habilidad y el deseo individual. Promueve a los trabajadores su capacidad y calidad de trabajo. Asimismo, Montana Grafica se compromete a ofrecer condiciones de trabajo seguras y a impulsar acciones en pro de la conservación del medio ambiente.

1.7 Mercado

Montana Gráfica produce y comercializa empaques flexibles en tres diversas estructuras: simplex, dúplex y triplex. Los productos que comercializa están dirigidos a la industria alimenticia y no alimenticia.

1.8 Productos

1. **Empaques primarios de estructuras simplex:** estructuras donde se emplea como materia prima un solo sustrato o película, la cual puede ser polipropilenos transparentes o polipropilenos metalizados.
2. **Empaques primarios de estructuras simplex con recubrimiento:** compuestas por polipropilenos metalizados, polipropilenos perlados o papel.
3. **Empaques primarios de estructuras dúplex:** son estructuras constituidas por dos sustratos, los cuales se unen a través de adhesivos base solvente o base acuosa
4. **Empaques primarios de estructuras triplex: s**on estructuras compuestas por tres sustratos, los cuales se laminan con los adhesivos usados en las laminaciones de estructuras dúplex.

En las figuras 3 y 4 se pueden apreciar los organigramas del Grupo Corimon y de Montana Grafica C.A.

1.9Estructura Organizacional

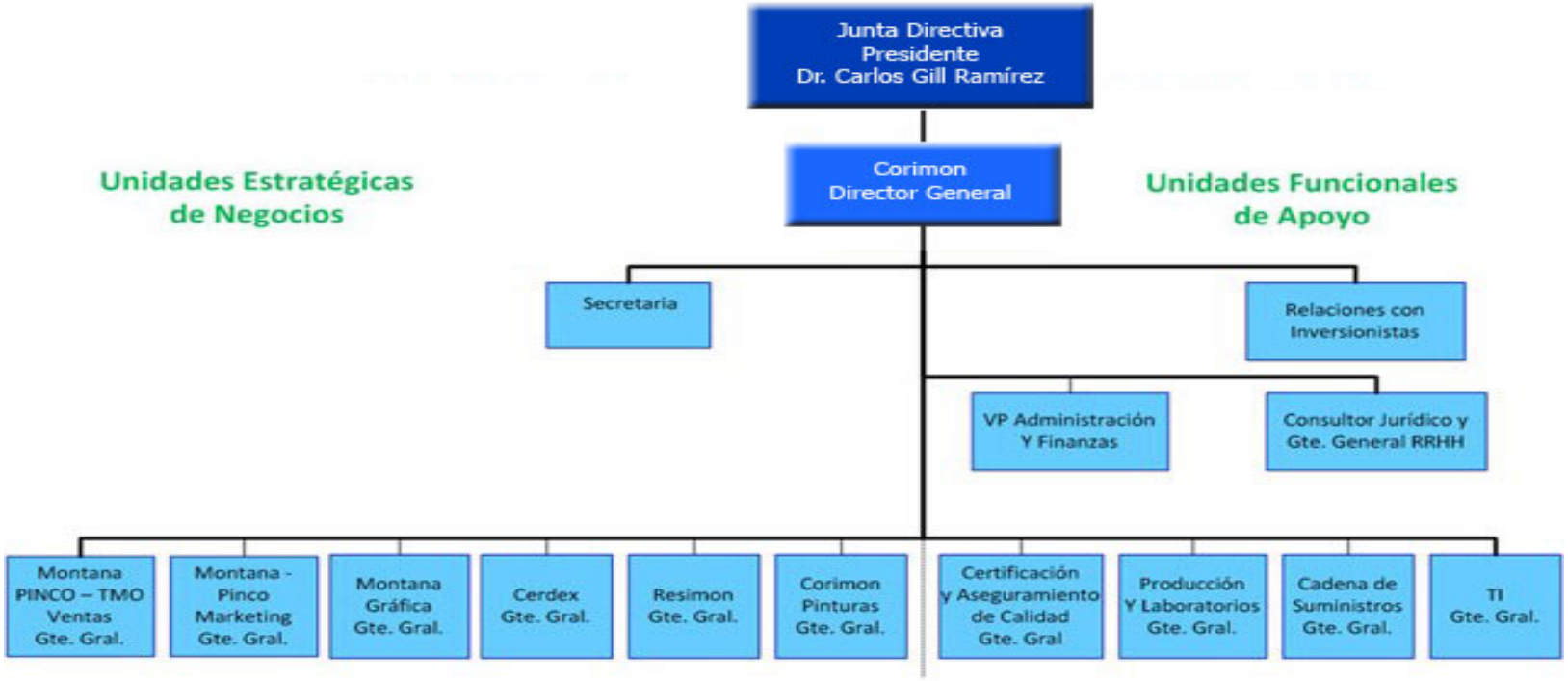

Figura 3. Estructura Organizacional del Grupo Corimon.

Fuente: http://www.corimon.com/

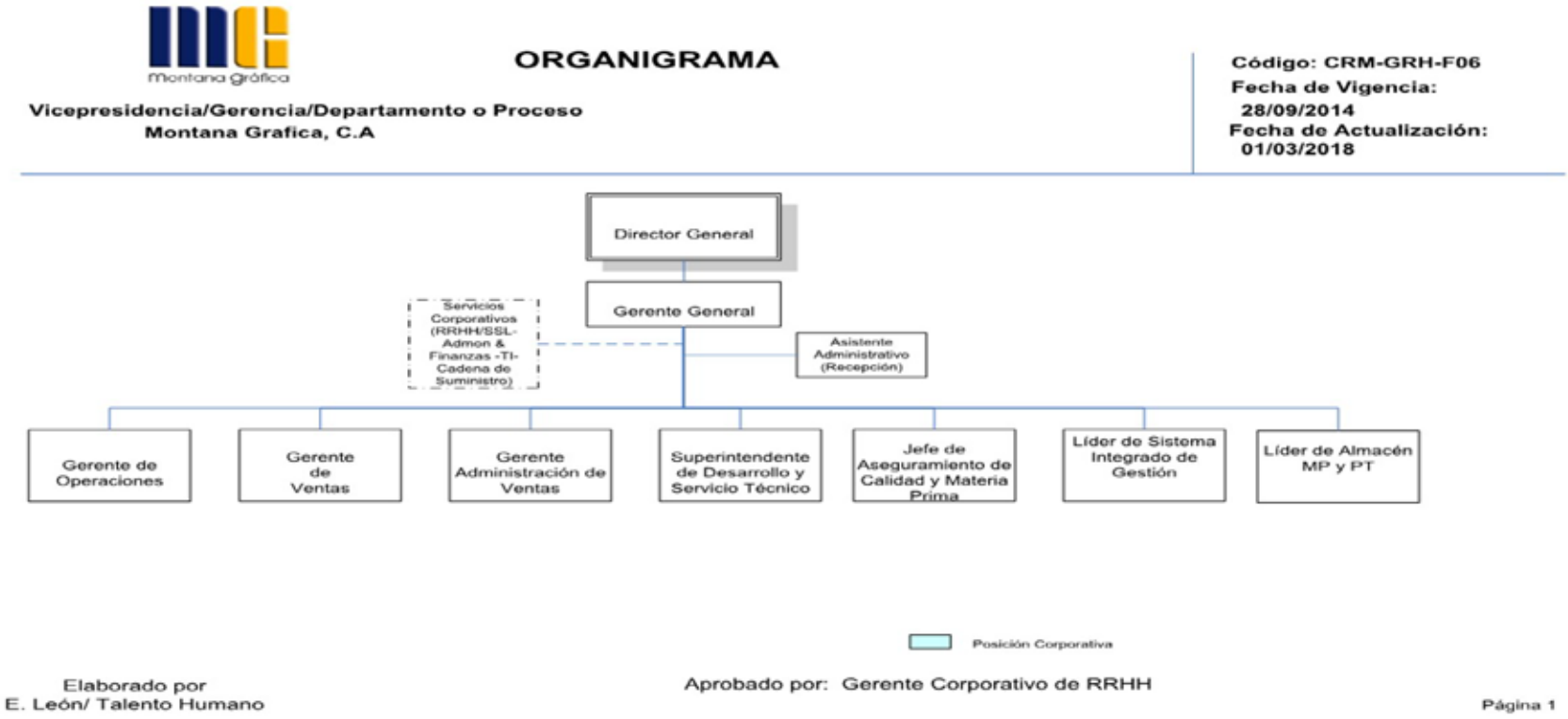

Figura 4. Estructura Organizacional de Montana Grafica C.A.

Fuente: Archivo Corimon 2018

CAPITULO II

EL PROBLEMA

2.1 Planteamiento del Problema

Desde los tiempos antiguos se ha entendido que la palabra seguridad del latín *securitas* es “la ausencia de riesgo o la confianza en algo o alguien”, si bien era muy común asociar la seguridad solo con la parte tangible, también existen cosas intangibles que deben ser seguras como lo son los datos que posteriormente al ser procesados pasaran a ser información.

De este modo al pasar de los años y debido a la constante evolución tecnológica se ha ido prestando más atención a la seguridad intangible como lo es la seguridad informática, también conocida como ciberseguridad o seguridad de tecnología de información.

Dentro de este orden ideas se puede definir la ciberseguridad como el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta, especialmente la información contenida en una computadora o circulante a través de las redes de computadoras.

En resumen, la seguridad en un ambiente de red es la habilidad de identificar y eliminar vulnerabilidades, así como también prestar atención a la necesidad de salvaguardar la ventaja organizacional, incluyendo información y equipos físicos, tales como los mismos computadores.

.

En el ámbito de la seguridad el uso de la información es una prioridad ya que es un activo con mucho valor, debido a esto se ha podido observar que en las últimas décadas tanto las empresas públicas como privadas han optado por darle un uso adecuado y una estructura organizada que permita que la información confidencial mantenga su integridad dentro de la empresa, ya sea una información de gran valor o que no tenga tanto impacto dentro de la misma.

Por consiguiente, para Montana Grafica C.A es imperativo conocer, mejorar y actualizar sus sistemas de seguridad informática debido a que en los últimos tiempos se han presentado vulnerabilidades en su red Corporativa y ha disminuido la productividad de sus trabajadores, en este sentido es fundamental disponer de un robusto sistema de seguridad el cual incluya el filtrado de páginas web para así obtener mejores resultados laborales y económicos dentro de la empresa.

Por todo lo antes expuesto la investigación plantea la siguiente interrogante:

2.2 Formulación del Problema

¿Cómo el conocimiento de las políticas de seguridad informática permitirá un uso adecuado de la red Corporativa de Montana Gráfica?

2.3 Objetivos de la investigación

2.3.1 Objetivo General

Evaluar las características de las políticas de seguridad informática usadas en la red corporativa de Montana Gráfica C.A. con el propósito de proponer e implementar protocolos de seguridad actualizados.

2.3.2 Objetivos Específicos

1. Identificar los protocolos de seguridad de red usados en las políticas de seguridad informática de Montana Gráfica C.A.
2. Describir como los protocolos de seguridad usados inciden en la vulnerabilidad de la red corporativa.
3. Formular y establecer las políticas de seguridad informática y los protocolos aplicables a redes corporativas de acuerdo a prácticas internacionales
4. Evaluar el desempeño de la seguridad de la red corporativa de Montana Gráfica de acuerdo los protocolos y políticas establecidos.

2.4 Justificación de la investigación

El siguiente trabajo se realizará debido a las vulnerabilidades presentadas en la seguridad de Montana Grafica C.A, para así poder lograr beneficios en la parte técnica y económica. En el ámbito técnico, se desea que, con una optimización de la seguridad, se logre proteger la privacidad de los usuarios y de la empresa en general, mientras que en el ámbito productivo se espera que los trabajadores aumenten su productividad dentro de la empresa.

2.5 Limitaciones

La principal limitación que se puede encontrar es el poco conocimiento de las políticas de seguridad aplicadas en años anteriores en Montana Grafica C.A.

Otra limitación no menos importante, es el factor tiempo, ya que, al existir tantas políticas de seguridad, se necesitaría mucho más tiempo para realizar un estudio detallado, que garantice el estar cien por ciento seguros que la política de seguridad aplicada sea la correcta para la empresa

2.6 Alcances

El proyecto tiene como finalidad optimizar la seguridad de la información de Montana Grafica C.A, así como también crear conciencia a sus trabajadores para poder dar un mejor uso a los recursos informáticos.

CAPITULO III

MARCO TEORICO

3.1 Antecedentes

Para la realización de cualquier investigación formal es importante la búsqueda y recopilación de estudios anteriores, relacionadas directa o indirectamente con el tema que se va a desarrollar, ya que los mismos sirven de soporte para exponer el estudio que se va a llevar a cabo. Entre los antecedentes asociados con esta investigación vale la pena destacar los siguientes:

Bajo un enfoque relacionado directamente con este trabajo, se tiene que el trabajo de grado realizado por Bermúdez y Bailon (2015) titulado "**ANALISIS EN SEGURIDAD INFORMATICA Y SEGURIDAD DE LA INFORMACION BASADO EN LA NORMA ISO/EC 27001-SISTEMAS DE GESTION DE SEGURIDAD DE LA INFORMACION DIRIGIDO A UNA EMPRESA DE SERVICIOS FINANCIEROS"** de la Universidad Politécnica Salesiana sede Guayaquil , cuyo objetivo fue el de analizar los procesos críticos de credigestión respecto a las gestiones de seguridad adecuadas para garantizar la confidencialidad, integridad y disponibilidad de la información, mediante la formulación recomendaciones de seguridad y controles basados en la norma ISO/EC 27001. El estudio se basó en una investigación de campo y bibliográfica. Dicho estudio indica un aporte de vital importancia ya que demuestra un patrón a seguir, el cual sirve de modelo para poner en práctica el proyecto.

Por otra parte, Ortega (2015) realizo un trabajo de grado bajo el nombre "**DISEÑO DE UN MODELO DE POLITICAS DE SEGURIDAD EN INFORMATICA PARA LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DE BOGOTA"** en la Universidad Libre de Colombia para optar al título de ingeniero de sistemas. El proyecto tuvo como objetivo diseñar un modelo de políticas de seguridad de la información para la protección de los datos en la superintendencia de industria y comercio de Bogotá. El trabajo fue realizado bajo un estudio de investigación de campo. Se interrelaciona mucho con el proyecto que se va a definir, debido a que realizaron consideraciones importantes a la hora de referirse en cuanto a seguridad de información, por lo que detallar el trabajo de grado a fondo daría buen pie a la hora de hablar sobre política de seguridad.

3.2 Bases Teóricas

Palella (2006) define las bases teóricas como el soporte al estudio, puesto que permite integrarla teoría con la investigación, estableciendo su interrelación. Según lo expuesto anteriormente y en pocas palabras, las bases teóricas son el sustento teórico que busca darle una idea al lector sobre la investigación.

3.2.1 Seguridad

La palabra seguridad proviene del latín *securitas*, la cual hace referencia a estar libre de cualquier peligro, por otra parte, la seguridad también es la necesidad de las personas de sentirse seguras y protegidas contra todo aquello que pueda perturbar o atentar contra su integridad física, moral, social y hasta económica.

3.2.2 Seguridad de tecnología en información o ciberseguridad

Según el estándar ISO 27001 la seguridad de información se refiere a la confidencialidad, la integridad y las disponibilidades de la información y datos importantes para la organización o empresa.

Para llevar a cabo una seguridad de información adecuada es necesario que se cumplan tres conceptos básicos los cuales son:

1. Confidencialidad: es la propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados.
2. Integridad: es la propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada.
3. Disponibilidad: es una característica, cualidad o condición de la información que se encuentra a disposición de quien tiene que acceder a esta, bien sea personas, procesos o aplicaciones.

En la figura 5 se puede observar el muy conocido triangulo de la seguridad en información.

Figura 5. Triada de la Seguridad de Información

Fuente:https://technologyincontrol2.wordpress.com/2016/01/14/perfilado-de-activos-de-informacion/

Los activos de la información son los elementos que la seguridad de información debe proteger dentro de una empresa, dichos activos son:

1. Información: es el objeto de mayor valor para la empresa.
2. Equipos: suelen ser hardware, software y la propia empresa.
3. Usuarios: son las personas que usan la tecnología de la organización.

3.2.3 Redes

Entiéndase de manera sencilla por red como el conjunto de dispositivos (nodos) conectados por enlaces de un medio físico, sin embargo este es un concepto muy general por lo que se requiere llevar el concepto de red a términos de tecnología, el cual es asociado a red de datos, que no es más que un conjunto de hardware y software conectados entre sí por medios de enlaces físicos mediante el cual reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos con la finalidad de compartir información, recursos y ofrecer servicios.

3.2.3.1 Tipos de redes según su escala

3.2.3.1.1 Red PAN

Andreu Gómez (2010) define las PAN (Personal Área Network) como una “red inalámbrica de interconexión de periféricos que se pueden encontrar tanto a unos pocos centímetros como a metros de distancia del emisor, con velocidades de transmisión inferiores al megabit por segundo. El estándar más conocido es el bluetooth.” (pág. 213).

Así mismo Tanenbaum (2003) define las redes de área personal como “Las redes que están destinadas para una sola persona. Por ejemplo, una red inalámbrica que conecta una computadora con su ratón, teclado e impresora, es una red de área personal” (pág. 15).

En la figura 6 se da un ejemplo de los accesorios que forman parte de las redes PAN.

Figura 6. Accesorios de redes PAN.

Fuente: https://sites.google.com/site/redesinalambricas3/tipos-de-redes-inalambricas/bluetooth.

3.2.3.1.2 Red MAN

A su vez Tanembaum (2003) define “Una red de área metropolitana (MAN) abarca una ciudad. El ejemplo más conocido de una MAN es la red de televisión por cable disponible en muchas ciudades” (pág. 18).

En la figura 7 se aprecia un ejemplo de una red MAN.

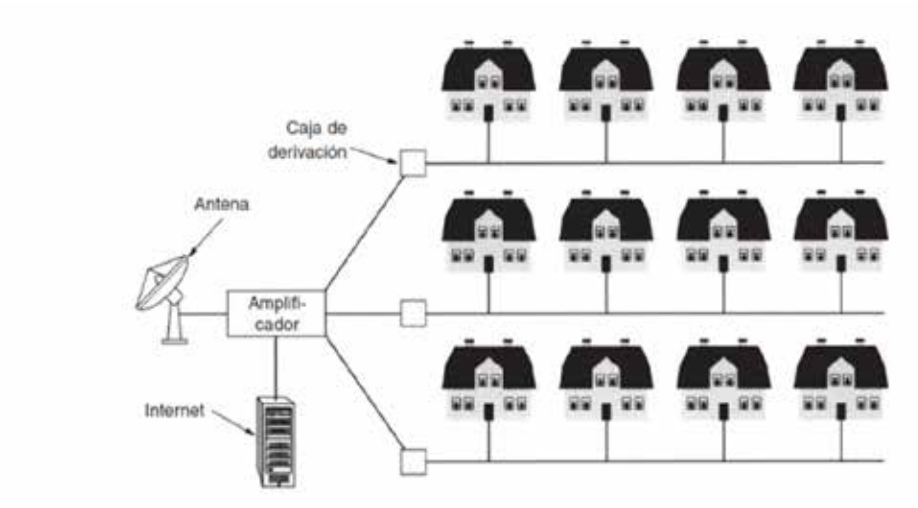

Figura 7. Una red de área metropolitana basada en TV por cable.

Fuente: Tanenbaum (2003).

3.2.3.1.3 Red LAN

Para Tanenbaum (2003) las LAN (Local Área Network)

> Son redes de propiedad privada que se encuentran en un solo edificio o en un campus de pocos kilómetros de longitud. Se utilizan ampliamente para conectar computadores personales y estaciones de trabajo en oficinas de una empresa y de fábricas para compartir recursos (por ejemplo, impresoras) e intercambiar información" (pág. 16).

Sallent y otros (2003) definen las LAN como un sistema flexible de comunicaciones que puede implementarse como una extensión o directamente como una alternativa a una red cableada en redes de pequeño tamaño. (pág. 37).

A continuación en la figura 8 se logra ver una estructura de la red LAN.

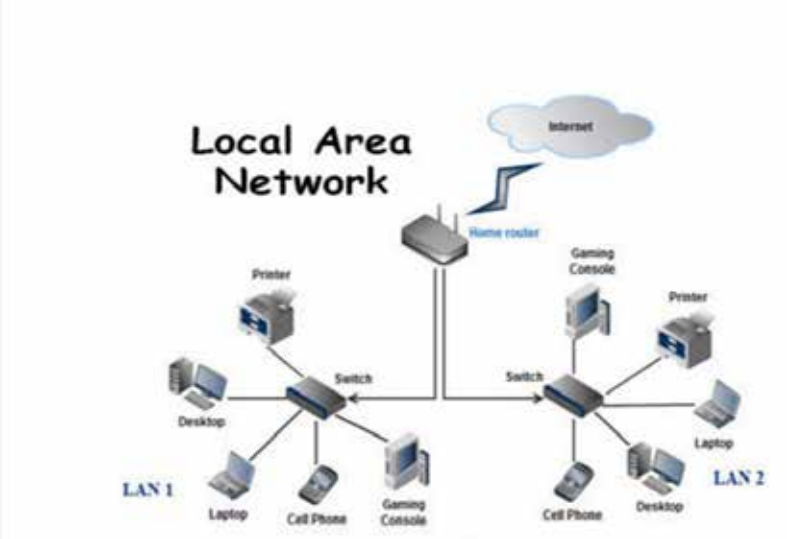

Figura 8. Estructura de una red LAN.

Fuente: https://www.indiamart.com/proddetail/lan-networking-services-17122003630.html

3.2.3.1.4 Red WAN

Conviene destacar que Tanenbaum (2003) señala que una red WAN (Wide Área Network) “Abarca una red geográfica, con frecuencia un país o un continente” (pág. 19)

Por otra parte, Stallings (2004) define “como redes amplias a todas aquellas que cubren una extensa área geográfica, requieren atravesar rutas de acceso público y utilizan, al menos parcialmente, circuitos proporcionados por una entidad proveedora de servicios de telecomunicación” (pág. 15).

En la figura 9 se puede ver la estructura de una red WAN.

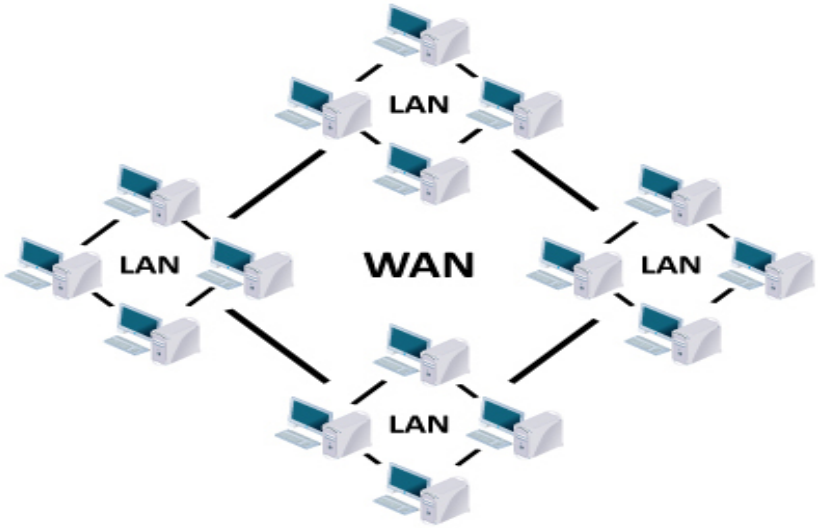

Figura 9. Estructura de una red WAN.

Fuente: http://www.knfegaming.us/wp-content/uploads/2015/10/wan1.jpg

De forma general los tipos de redes según su escala se suelen clasificar en: WAN, MAN, LAN y PAN. El alcance de cada una de ellas se expone en la Figura 10.

1 m	Metro cuadrado	Red de área personal
10 m	Cuarto	Red de área local
100 m	Edificio	
1 km	Campus	
10 km	Ciudad	Red de área metropolitana
100 km	País	Red de área amplia
1,000 km	Continente	
10,000 km	Planeta	Internet

Figura 10. Rango de cobertura de los tipos de redes.

Fuente: Tanenbaum (2003)

3.2.4 Topologías de red

Ahora bien, se puede definir topologías de red como las diferentes estructuras de intercomunicación en que se pueden organizar las redes de transmisión de datos entre dispositivos.

Cabe considerar que cada topología de red lleva asociada una topología física y una topología lógica, siendo la primera la que define la estructura física de la red, es decir, la manera en la que debe estar dispuesto el cable de interconexión entre los elementos de la red, mientras que la topología lógica hace referencia al conjunto de reglas normalmente asociado a la topología física, dichas reglan definen el modo en que se gestiona la transmisión de datos en la red.

Es importante señalar que la utilización de cualquier topología influye en el flujo de información, ya sea en velocidad de transmisión, tiempos de llegada, entre otras. Asimismo, influye en el control de la red, y en la forma en la que esta se puede expandir y actualizar.

3.2.4.1 Interconexión total y parcial

Es la que proporciona múltiples enlaces físicos entre los nodos de la red, de tal modo que no existen varios canales de comunicación compartidos y múltiples caminos de interconexión entre dos nodos.

La interconexión llega a ser total cuando todos los nodos están conectados de forma directa entre ellos, existiendo siempre un enlace punto a punto para su intercomunicación, sin embargo, la interconexión es parcial cuando no todos los nodos pueden conectarse mediante un enlace punto a punto con cualquier otro nodo de la red.

3.2.4.2 Interconexión en estrella

Consiste en que cada nodo se enlaza a un nodo central encargado del control de acceso a la red por el resto de nodos.

3.2.4.3 Interconexión en bus

Se define como todos los nodos que se conectan a un único medio de transmisión utilizando los transceiver, los cuales son los encargados de controlar el acceso al bus, asimismo cabe destacar que los mensajes que se envían por el bus llegan a todos nodos, sin embargo, el único nodo que procesa la información es hacia el que va dirigido el mensaje.

3.2.4.4 Interconexión en árbol

Se entiende por ella como el encadenamiento de diferentes estructuras en bus de diversas longitudes y de características diferentes, constituyendo así desiguales ramas de interconexión.

3.2.4.5 Interconexión en anillo

Consiste en la unión de los nodos en serie alrededor del anillo, lo cual es equivalente a unir los extremos de una red en bus, por otra parte, es importante indicar que en este tipo de topología no existe un nodo principal y que a su vez el control de la red queda distribuido entre todos los nodos.

Si bien es cierto que las topologías de redes mencionadas anteriormente son las más comunes, también existen aquellas topologías que son hibridas de varios tipos de interconexión.

En la figura 11 se representa mediante una imagen las distintas topologías de redes.

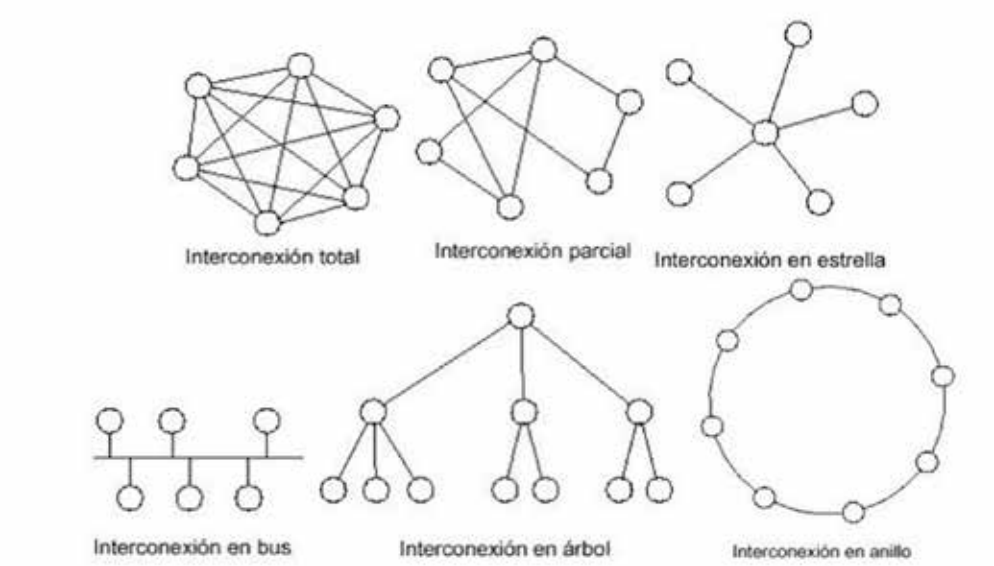

Figura 11. Topología de Redes.

Fuente: https://www.uv.es/rosado/courses/sid/Capitulo2_rev0.pdf

3.2.5 Protocolos y políticas de Seguridad en Redes

Las inseguridades en las redes de información van más allá de los virus informáticos ya conocidos, es por eso que la introducción de mecanismos de protección es una prioridad para cualquier empresa.

Los atacantes de una red de telecomunicaciones no necesitan obligatoriamente estar en contacto físico con la víctima, ya que los datos pueden ser fácilmente copiados, transmitidos, modificados o destruidos cuando son transmitidos por la red, y es por esto

que si no se dispone de los mecanismos de protección adecuados la red quedaría muy vulnerable.

3.2.6 Principales causas de los problemas de seguridad

Existen tres tipos de deficiencias esenciales que dan lugar a estos problemas:

a). Deficiencias tecnológicas: todas las tecnologías poseen deficiencias inherentes conocidas o desconocidas y vulnerabilidades que pueden ser explotadas por un atacante suficientemente motivado.

- Ø Entre las deficiencias tecnológicas se tiene:
- Ø Los protocolos de internet los cuales no fueron diseñados pensando en la seguridad de las telecomunicaciones.
- Ø Los sistemas operativos, ya que todos los sistemas operativos tienen vulnerabilidades que deben ser abordadas mediante parches, actualizaciones entre otras.
- Ø Debilidades de los accesorios y equipos de comunicación con la red.

b). Deficiencias de la política de seguridad: se da cuando se generan amenazas de seguridad en la red de forma inconsciente. Los siguientes ejemplos son algunas situaciones que pueden afectar negativamente al sistema informático de un negocio o empresa:

- Ø Inexistencia de un documento escrito donde conste la política de seguridad.
- Ø Ausencia de un plan de contingencia para la recuperación en casos de desastres.
- Ø Inexistencia de criterios para la modificación o incorporación de hardware o software.
- Ø Ausencia de un supervisor de seguridad.

- Políticas de empleo, por ejemplo, una rotación de personal con alta frecuencia o emplear a personas con falta de formación en cargos de responsabilidad pueden tener impacto de forma negativa.

c). Deficiencias de configuración: son muchos los dispositivos de red que tienen una configuración por defecto que facilita la instalación o intenta conseguir las máximas prestaciones en detrimento de aspectos de seguridad.

- Ineficacia de las listas de control de acceso al no bloquear solicitudes no autorizadas.
- Contraseñas o passwords por defecto.
- Puertos o servicios innecesarios activos.
- Intercambio de identificadores de usuario y contraseña sin cifrar.
- Acceso remoto a través de internet no debidamente protegido.

3.2.7 Clasificación de ataques

Se definen los ataques en las redes de telecomunicaciones como los diferentes tipos de actividades sistemáticas dirigidas a disminuir o corromper su seguridad. Asimismo, existen diferentes formas de ataque entre las que se destacan:

1. Ingeniera Social
2. Ataques de denegación de servicio
3. Ataques a determinados protocolos
4. Ataques a servidores
5. Adivinar contraseñas
6. Espionaje de todo tipo

3.2.8 Ataques pasivos

Se hace referencia a ataques pasivos cuando el atacante monitoriza el canal de la comunicación sin modificar ni añadir datos ya que su objetivo solo es el de obtener la información que se está transmitiendo.

Es por ello que los ataques pasivos están relacionados con el contenido del mensaje y con el análisis de tráfico, en la figura 12 se aprecia un ejemplo de un ataque pasivo.

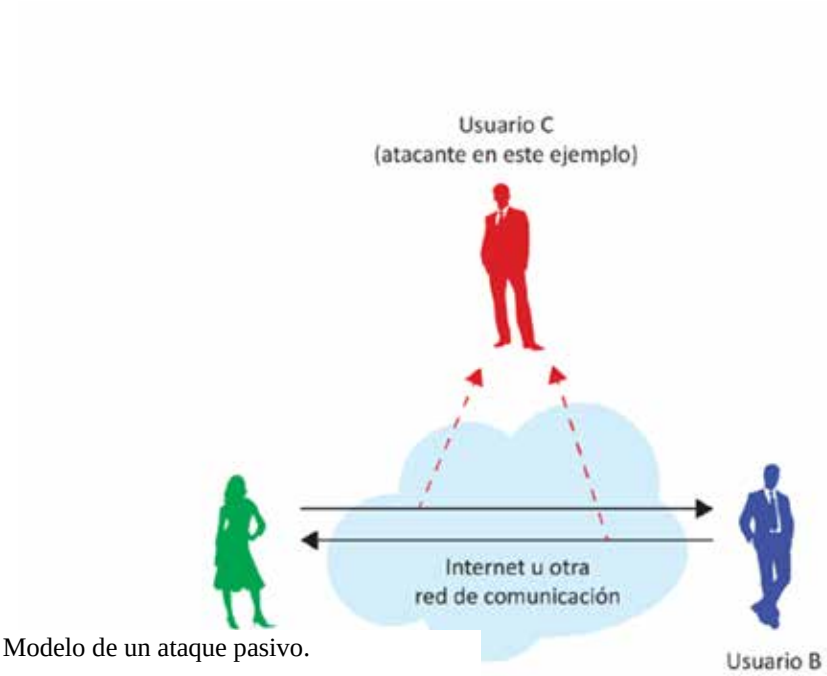

Figura 12. Modelo de un ataque pasivo.

Fuente: Soriano (2013).

3.2.9 Ataques activos

Se entiende por ataque activo como aquel que intenta alterar los recursos del sistema o afectar su funcionamiento; en este tipo de ataque el adversario intenta borrar, añadir o modificar los datos transmitidos. En la figura 13 se aprecia un ejemplo de un ataque activo.

Los ataques activos pueden dividirse en cuatro categorías:

1. Suplantación de identidad
2. Repetición
3. Modificación de mensajes
4. Hombre en el medio (Man in the middle, MitM)

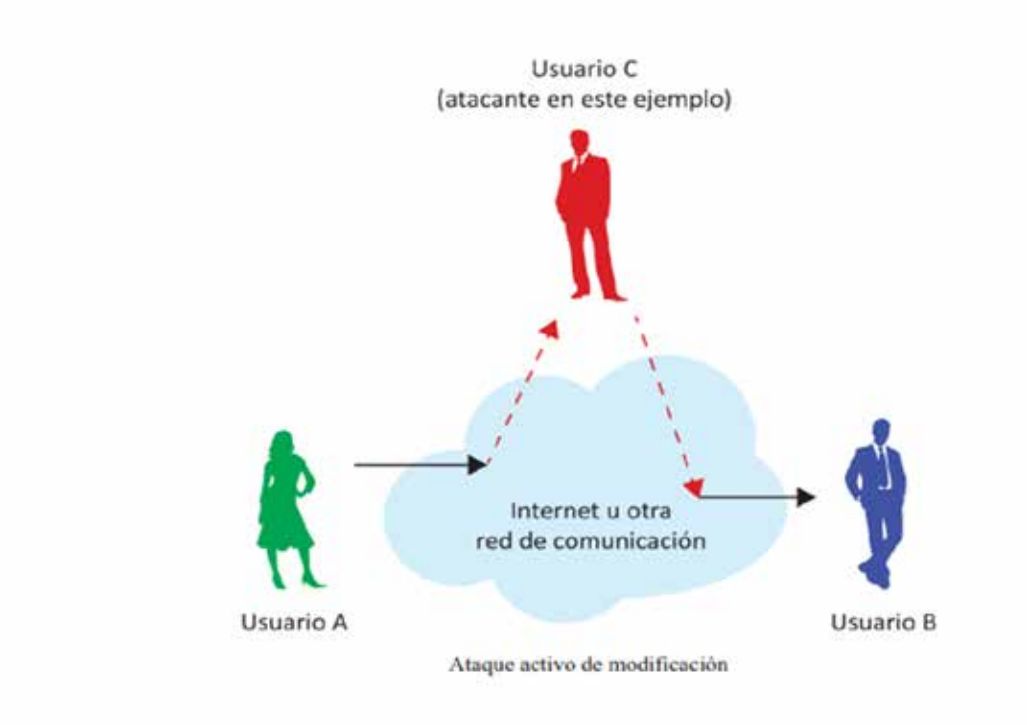

Figura 13. Modelo de un ataque activo.

Fuente: Soriano (2013)

3.2.10 Seguridad en Servicios de red

3.2.10.1 Transport Layer Security (TLS)

Se le conoce como un protocolo estándar de internet que proporciona seguridad en las comunicaciones a través de internet. El objetivo principal de este protocolo es proporcionar confidencialidad e integridad de datos entre dos entidades que se comunican.

Ahora bien, el uso más importante del TLS es proteger el tráfico de la World Wide Web permitiendo transacciones seguras de comercio electrónico, así como también proteger aplicaciones como puede ser el correo electrónico.

Es importante subrayar que el TLS se usa ampliamente en aplicaciones tales como la navegación web, correo electrónico, fax por internet, mensajería instantánea y voz sobre ip (VoIP).

Algunas de las características de la TLS es que se basa en un protocolo anterior llamado Secure Sockets Layer (SSL), de igual manera ambos protocolos utilizan algoritmos criptográficos y certificados de clave pública para verificar la identidad de las entidades que se comunican.

A su vez utilizan cifrado simétrico para ofrecer confidencialidad, y funciones de hash para la integridad del mensaje.

En la figura 14 se puede observar de una manera muy simplificada como se establece una sesión TLS para una comunicación web segura entre un usuario y un servidor web.

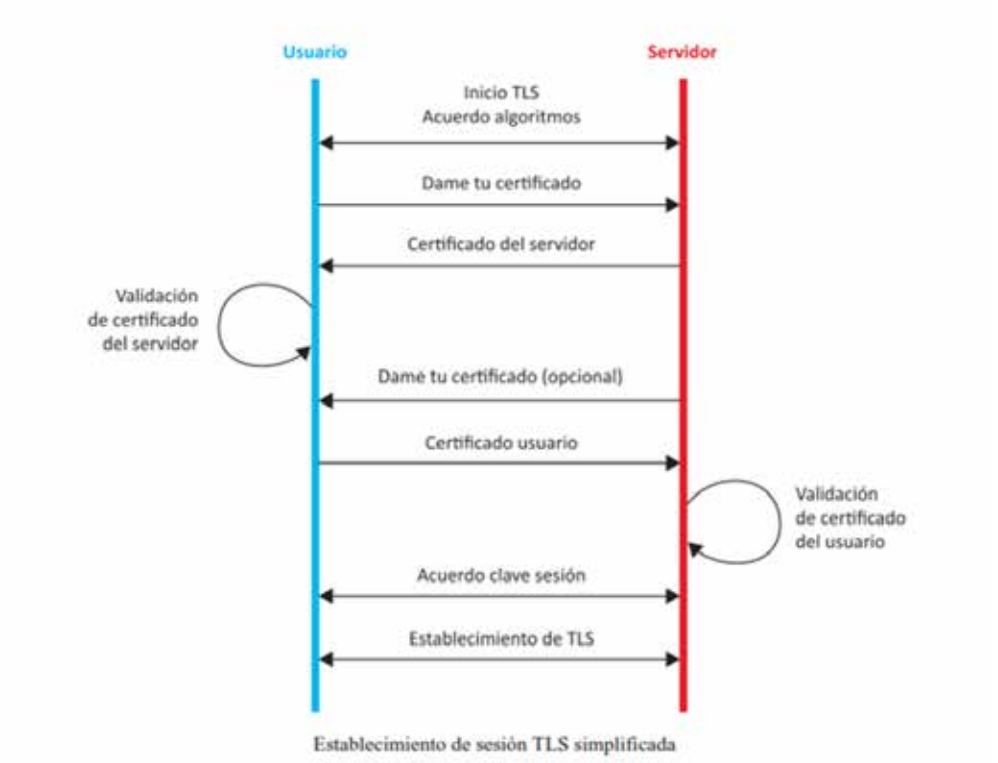

Figura 14. Sesión TLS

Fuente: Soriano (2013).

3.2.10.2 Seguridad en el correo electrónico

Los correos electrónicos son un flanco muy vulnerable ya que cualquier persona que lo intercepte puede leer su contenido, por lo que si lo que sea desea es que el contenido sea confidencial y/o autentico es necesario utilizar técnicas criptográficas.

La solución más aceptada para proporcionar seguridad al correo electrónico es el estándar S/MIME, el cual se encarga de ofrecer los siguientes servicios de seguridad: autenticación, integridad del mensaje, no repudio de origen (usando firma digital) y la confidencialidad de datos. El uso de S/MIME requiere certificados digitales.

En la figura 15 se podrá observar un ejemplo de cómo es el modelo de confidencialidad de S/MIME

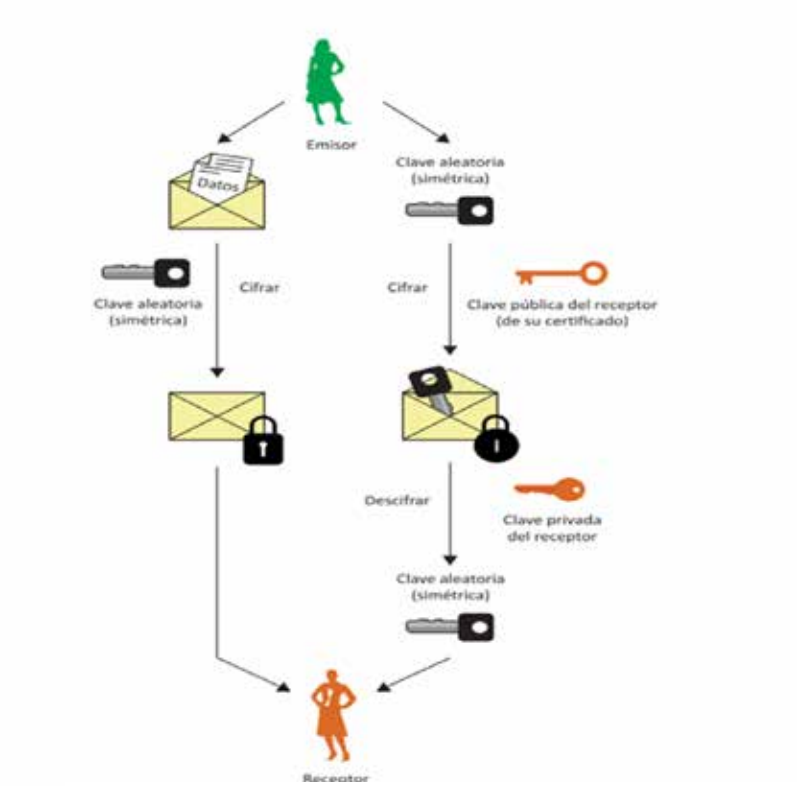

Figura 15. Esquema de confidencialidad de S/MIME.

Fuente: Soriano (2013)

3.2.10.3 Seguridad Perimetral

3.2.10.3.1Firewall

Un firewall o cortafuegos es un mecanismo que se utiliza para proteger la red interna de una empresa, dicha protección se lleva a cabo mediante la separación de la red interna del mundo exterior.

Cabe destacar que todos los mensajes que entran o salen de la red interna a través del firewall son examinados para verificar si cumplen las normas de seguridad especificadas en las reglas del firewall.

Es importante que antes de instalar el firewall se definan las normas o reglas que constituyen la política de seguridad, ya que sin este documento no se puede asegurar la red con un firewall.

Por otra parte, un firewall puede hacer dos cosas, puede bloquear o permitir una comunicación. Generalmente se permiten todas las comunicaciones de la red interna a la red externa, pero si la política de seguridad establece una regla impidiendo el paso de un tipo de mensajes, el firewall lo bloqueará.

Esto se observa mucho cuando se intentar acceder a sitios de internet que no son seguros o que son considerados una amenaza para la empresa

3.2.10.3.2 Sistema de detección de intrusión

En vista de que los ataques a la red son cada vez más sofisticados es necesario el uso de los sistemas de detección de intrusión, mejor conocido por sus siglas en inglés como IDS (Intrusion detection systems), los cuales aparecieron para dar respuesta al creciente número de ataques a los principales lugares de interés y redes.

Los IDS son una especie de sistema de gestión de seguridad para los ordenadores y redes, estos se encargan de recopilar y analizar la información de un ordenador o una red para identificar posibles violaciones de seguridad, incluyendo tanto el mal uso (ataques desde adentro de la empresa) así como las intrusiones (ataques fuera de la empresa).

Las funciones de un IDS son:

1. Análisis de los usuarios y actividades del sistema
2. Análisis de las configuraciones del sistema y sus vulnerabilidades
3. Evaluación de un sistema e integridad de sus archivos
4. Capacidad de reconocer patrones típicos de los ataques
5. Análisis de los patrones de las actividades normales

Un IDS se diferencia de un firewall ya que este último limita el acceso entre redes con el fin de prevenir la intrusión, mas no indican un ataque desde el interior de la red.

Los IDS se clasifican de varias maneras, entre ellas se tiene:

3.2.10.3.3 Detección de mal uso y detección de anomalías

1. Detección de mal uso: el IDS analiza la información que recopila y la compara con grandes bases de datos de firmas de ataques. Esencialmente, el IDS busca un ataque específico que ya se ha documentado.
2. Detección de anomalías: el administrador del sistema define el estado normal del tráfico de la red, protocolos y los tamaños típicos de intercambios con el fin de comparar el estado en cada momento con el estado normal y a partir de las diferencias se buscan anomalías de comportamiento que pueden ser producidas por un ataque.

3.2.10.3.4 Basados en red o basados en equipos

1. Basados en red: mejor conocidos como NIDS (Network-based system) se basa en analizar las comunicaciones que se intercambian por la red. El NIDS puede detectar mensajes maliciosos diseñados de forma que las reglas de filtrado de un firewall no lo detecten.
2. Basados en equipo: mejor conocido como HIDS (Host-based system), este analiza toda actividad en cada equipo por individual.

3.2.10.3.5 Sistemas pasivos o sistemas reactivos

1. Sistema pasivo: el IDS detecta un posible fallo de seguridad, registra la información y envía las señales de alerta
2. Sistema reactivo: el IDS responde a una actividad sospechosa cerrando la sesión de un usuario o reprogramando el firewall para bloquear el tráfico de red que tiene en su origen en una entidad sospechosa.

   En las figuras 16 y 17 se aprecian unos ejemplos de los firewall que se usan en las redes empresariales.

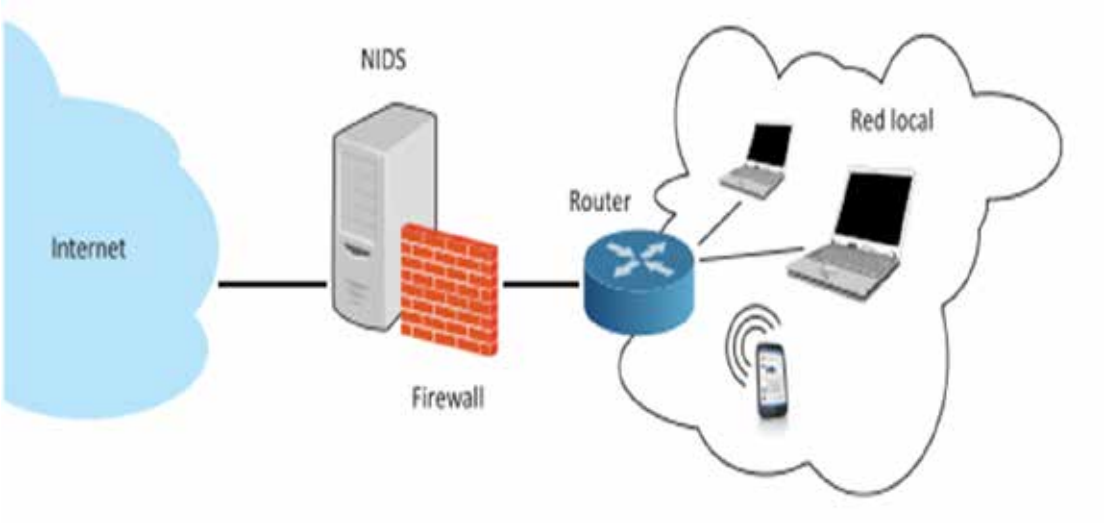

Figura 16. Diagrama con firewall e IDS.

Fuente: Soriano (2013)

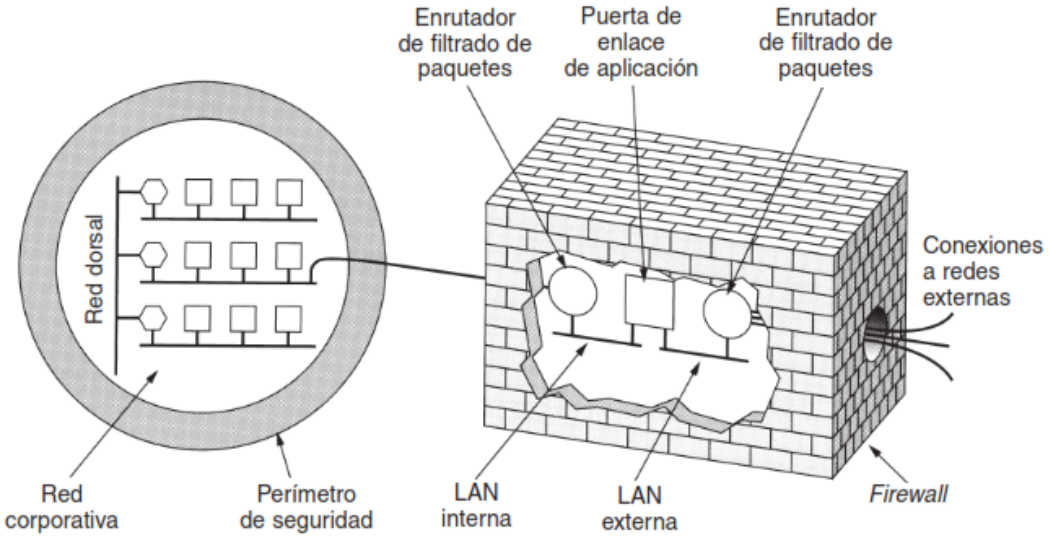

Figura 17. Un firewall que consiste en dos filtros de paquetes y en una puerta de enlace de aplicación.

Fuente: Tanenbaum (2003)

3.2.10.3.6 Virus

Entiéndase por virus como los programas informáticos que tiene el objetivo de alterar el funcionamiento del computador que el usuario lo note, generalmente infectan otros archivos del sistema con la intención de modificarlos para destruir de manera intencionada los datos almacenados.

Entre los virus más comunes se tienen:

1. Adware: se instala de forma disimulada o directamente oculta.
2. Spyware: recopila información de un equipo y la transmite a otra entidad externa sin que el usuario lo sepa y sin su consentimiento.

3. Malware: altera el funcionamiento normal de un dispositivo, ya sea corrompiéndolos o destruyendo archivos.
4. Ransomware: consiste en que el ladrón cibernético pide un rescate económico a la víctima para devolver el control del equipo.
5. Worms: se caracteriza por poder multiplicarse en cada sistema a través del envío masivo de copias de sí mismo por correo electrónico u otras vías de contacto como redes domésticas o wifi.
6. Troyano: se adueña del ordenador debido a que el mismo usuario lo instala, ya que normalmente se disfraza de un juego, un archivo de powerpoint o cualquier otro archivo que se necesita.
7. Denegación de servicio: consiste en la petición masiva de servicios a través de bots que bloquean la respuesta de la plataforma durante horas, produciendo así que el servicio sea inaccesible para los usuarios.
8. Phishing: se centra en el envió de correos electrónicos para obtener datos confidenciales del usuario haciéndose pasar por fuentes fiables.

3.2.10.3.7 Antivirus

Los antivirus no son más que programas que fueron creados con el objetivo de detectar y eliminar los virus informáticos.

3.2.10.3.8 Tipos de antivirus

1. Antivirus preventores: se caracterizan por avisar antes de que se presente la infección, por lo general ese tipo de virus se mantiene en la memoria del computador, monitoreando las acciones y funciones del sistema.
2. Antivirus identificadores: tienen como objetivo identificar programas infecciosos que pueden afectar el sistema.
3. Antivirus descontaminadores: se especializan en descontaminar un sistema que fue infectado a través de la eliminación de programas malignos

3.2.10.3.9 Filtrado web

Hace referencia a un programa diseñado para controlar que contenido se puede mostrar, se usa especialmente para restringir el acceso a ciertos materiales de la web.

Los usos comunes de un filtrado web son de padres que limitan el contenido de sus hijos, así como también de empresas que lo usan para restringir a sus empleados en el trabajo y administrar así el ancho digital de la empresa.

3.2.10.3.10 Proxy

Se entiende como proxy al programa que realiza una tarea de acceso a internet en lugar de otro ordenador, dicho de otra forma, un proxy es un punto intermedio entre un ordenador conectado a internet y el servidor al que está accediendo.

3.2.10.3.11 Tipos de proxy

1. Proxy web o proxy cache web: se trata de un proxy para una aplicación específica, la cual es el acceso a la web, aparte de la utilidad general de proxy, este proporciona un cache para las páginas web y los contenidos descargados, dichos contenidos son compartidos por toda la red, con la consiguiente mejora en los tiempos de acceso para consultas futuras.
2. Proxy transparentes: combina un servidor proxy con NAT (Network Address Translation) de una manera que las conexiones son enrutadas dentro del proxy sin configuración por parte del cliente y sin que el mismo conozca de su existencia.
3. Proxy inverso: es un servidor proxy instalado en el domicilio de uno o más servidores web, dicho de otra forma, todo el tráfico entrante de internet y con destino de uno de los servidores web pasa a través del proxy.
4. Proxy NAT: consiste en realizar un network addres translation.

5. Proxy abierto: dicho proxy ejecutará cualquier petición de cualquier ordenador que pueda conectarse a él.

3.2.10.3.12 Ancho de banda digital (bandwidth)

El ancho de banda digital o ancho de banda de red se define como la medida de recursos disponibles para transmitir datos, en otras palabras, es la forma más precisa de medir la velocidad de la conexión de internet.

Se puede usar para referirse a cantidades o consumo y su unidad de medida es en bits por segundo, kilobits por segundo, megabits por segundo o algún otro múltiplo.

3.3 Definición de términos básicos

Tamayo y Tamayo (1993), en su estudio titulado: "El proceso de la investigación científica", señalan la definición de términos básicos como "la aclaración del sentido en que se utilizan las palabras o conceptos empleados en la identificación y formulación del problema" (p. 78). Basado en la consideración anterior se procede con la definición de algunos términos, esto a fin de esclarecer interrogantes surgidas durante el proceso de lectura del proyecto investigativo, y hacer de este, uno correctamente entendible y fluido.

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

2. PAN: es una red informática que sirve para interconectar dispositivos centrados en el espacio de trabajo de una persona individual.

3. MAN: es una red de área metropolitana que posee una alta velocidad que da cobertura a un área geográfica extensa.

4. LAN: es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada, como por ejemplo una habitación, edificio o área de edificio.

5. WAN: es una red de computadoras capaz de cubrir distancias de unos 100 metros hasta 1000 kilómetros, proveyendo de servicio a un país o continente.

6. DOS: también conocido como Disk Operating System, hace referencia a una familia de sistemas operativos de ordenadores personales.

7. APT: son las siglas de advanced packaging tool y no es más que un sistema de gestión de paquetes creado por el proyecto debían.

CAPÍTULO IV

MARCO METODOLÓGICO

Arias (2006), señala que “la metodología del proyecto incluye el tipo o tipos de investigación, las técnicas y los procedimientos que serán utilizados para llevar a cabo la indagación” (p. 19). Con base en lo anterior planteado, se puede señalar, que, en todo proyecto de investigación, así como en su hecho investigativo, se requiere que el(los) investigador(es) delimiten en orden, la metodología utilizada para la realización del mismo, pues esto presenta los procedimientos, métodos y técnicas utilizados en la estructura de la investigación en forma organizada, clara y precisa para lograr así los objetivos propuestos. La metodología debe reflejar la estructura lógica y el rigor científico del proceso de investigación desde la elección de un enfoque metodológico específico hasta la forma como se van a analizar, interpretar y presentar los resultados.

4.1 Nivel y tipo de investigación:

Para Tamayo y Tamayo, (2003) “cuando se va a resolver un problema en forma científica, es muy conveniente tener un conocimiento detallado de los posibles tipos de investigación que se pueden seguir. Este conocimiento hace posible evitar equivocaciones en la elección del método adecuado para un procedimiento específico”

Arias (2006), manifiesta que “la investigación descriptiva consiste en la caracterización de un hecho, fenómeno, individuo o grupo, con el fin de establecer su estructura o comportamiento. Los resultados de este tipo de investigación se ubican en un nivel intermedio en cuanto a la profundidad de los conocimientos se refiere”. Por otro lado, señala que un proyecto factible “se trata de una propuesta de acción para

resolver un problema práctico o satisfacer una necesidad. Es indispensable que dicha propuesta se acompañe de una investigación que demuestre su factibilidad o posibilidad de realización". Además "Los estudios descriptivos miden de forma independiente las variables y aun cuando no se formulen hipótesis, tales variables aparecen enunciadas en los objetivos de investigación.

Con frecuencia, la meta del investigador consiste en describir fenómenos, situaciones, contextos y sucesos; esto es, detallar cómo son y se manifiestan. Con los estudios descriptivos se busca especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. Es decir, únicamente pretenden medir o recoger información de manera independiente o conjunta sobre los conceptos o las variables a las que se refieren, esto es, su objetivo no es indicar cómo se relacionan éstas. (Hernández Sampieri y otros. 2014).

En atención a las teorías propuestas por Arias y Hernández Sampieri se considera que la investigación es de tipo proyecto factible y descriptivo, por cuanto se busca mejorar y actualizar el sistema de seguridad en la red corporativa de Montana Grafica C.A, pues se realiza la caracterización de un hecho, con el fin de establecer su comportamiento y a su vez es un proyecto factible porque busca satisfacer la necesidad de la empresa para optimizar su seguridad.

4.2 Diseño de investigación:

Arias (2006) expresa que “el diseño de investigación es la estrategia general que adopta el investigador para responder al problema planteado”. En atención al diseño, la investigación se clasifica en documental, de campo y experimental.

De acuerdo a la clasificación expresada por Arias (2006) “la investigación de campo es aquella que consiste en la recolección de datos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos (datos primarios), sin manipular o controlar variable alguna, es decir, el investigador obtiene la información, pero no altera las condiciones existentes. De allí su carácter de investigación no experimental”. Además, en una investigación de campo también se emplean datos secundarios, sobre todo los provenientes de fuentes bibliográficas, a partir de los cuales se elabora el marco teórico. No obstante, son los datos primarios obtenidos a través del diseño de campo, los esenciales para el logro de los objetivos y la solución del problema planteado.

En atención a lo planteado por Arias, se considera que este proyecto está enmarcado bajo la modalidad de diseño de campo. Debido a que se recopilo información necesaria para la actualización del sistema de seguridad en la red corporativa de Montana Grafica C.A, directamente de la realidad donde ocurren los hechos (datos primarios), sin manipular o controlar variable alguna, es decir, sin alterar las condiciones existentes, con el fin de obtener el mejor diseño posible.

4.3 Técnicas e instrumentos de recolección de datos

Citando a Arias (2006) “las técnicas de recolección de datos son las distintas formas de obtener información”. Al aplicar una técnica de recolección de datos o información, dicha información debe ser guardada de forma que estos puedan ser analizados e interpretados luego. Este soporte se conoce con el nombre de instrumento. Para Arias (2006) “un instrumento de recolección de datos es cualquier recurso, dispositivo o formato (en papel o digital), que se utiliza para obtener, registrar o almacenar información.

Para Méndez (1999, p.143) las fuentes y técnicas para recolección de la información son los hechos o documentos a los que acude el investigador y que le permiten tener información”. Otros investigadores como Fernández C y Baptista P (2014, p.252) definen que la utilización de datos secundarios “implica la revisión de documentos, registros públicos y archivos físicos o electrónicos”. Al ser estos los métodos más utilizado para la recolección de datos en la presente investigación ya que por medio de estos se identificó la información necesaria para la realización de la misma.

4.4 Fases de la investigación

Al ejecutar cualquier proyecto de investigación es necesario seguir un camino pautado el cual hará posible la ejecución de dicho proyecto. En el mismo orden de ideas el camino pautado en esta investigación se denomina “fases de la investigación”, y se encuentran estrictamente relacionadas con los objetivos que se plantean cumplir, pudiendo de esta forma avanzar paulatinamente a través de dichos objetivos y cumplir o acercarse lo más posible al objetivo principal de la investigación.

Fase I: Identificar los protocolos de seguridad de red usados en las políticas de seguridad informática de Montana Gráfica C.A.

Durante la primera fase se identificó la situación actual de la seguridad de Montana Grafica C.A. para a conocer las políticas aplicadas de Montana grafica en su red LAN. Este conocimiento implica que tan actualizados están con los estándares existentes en seguridad. Dicho diagnostico indicará posibles mejoras de seguridad que puedan ser aplicables.

Fase II: Describir como los protocolos de seguridad usados inciden en la vulnerabilidad de la red corporativa.

Luego de haber completado con éxito la primera fase, se investigó mediante material bibliográfico o en la web, cuales son los protocoles de seguridad más recomendados a aplicar en las redes empresariales.

Se seleccionó el que más encajaba de acuerdo a la situación actual de Montana Grafica C.A, pero no sin antes haber estudiado sus ventajas y desventajas.

Fase III: Formular y establecer las políticas de seguridad informática y los protocolos aplicables a redes corporativas de acuerdo a prácticas internacionales.

En esta fase se procedió a aplicar las políticas y protocolos correspondientes a toda la empresa de Montana Grafica C.A., de haber sido necesario se pudo haber aplicado distintos softwares para optimizar la red LAN de la organización y así contar con políticas de seguridad actualizadas y confiables.

Fase IV. Evaluar el desempeño de la seguridad de la red corporativa de Montana Gráfica de acuerdo los protocolos y políticas establecidos.

Se hicieron las pruebas en los equipos correspondientes para validar que las políticas implementadas cumplían con el protocolo de seguridad que se estableció para montana grafica C.A.

CAPÍTULO V

RESULTADOS

En el capítulo de resultados se presenta la propuesta con detalle, aplicando el método de investigación planteado, en el que se incluye los resultados obtenidos en cada fase, que permitieron cumplir con los objetivos específicos para así lograr el objetivo general del estudio.

5.1 Identificar los protocolos de seguridad de red usados en las políticas de seguridad informática de Montana Gráfica C.A.

Actualmente Montana Gráfica C.A cuenta con un firewall de red llamado CISCO ASA 5510 referente a la serie Cisco ASA 5500-X Series-Firewalls y un proxy en modo de software, el cual fue desarrollado por sus antiguos trabajadores.

El firewall se encuentra ubicado exactamente en el datacenter correspondiente al departamento de TI (Tecnología de Información), en el nivel mezzanina de Montana Grafica.

En la figura 18 se puede apreciar un plano realizado en Autocad ™, donde se logra tener un punto de referencia de donde se encuentra el firewall ubicado.

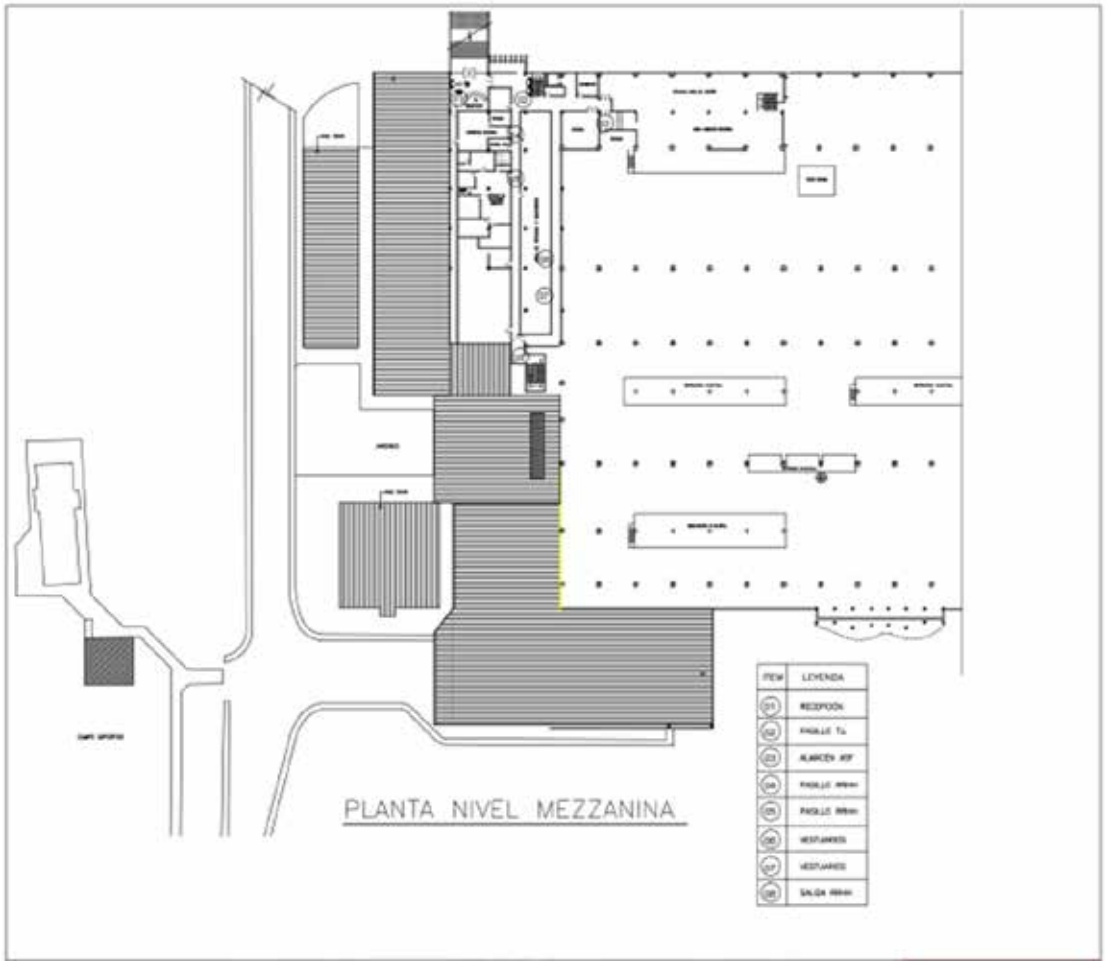

Figura 18. Plano de MGR.

Fuente: Archivo Corimon.

5.1.2 CISCO ASA (Adaptive Security Appliance) 5510

El firewall Cisco Adaptive Security Appliance (ASA) es una herramienta de seguridad que usa para proteger toda una red, del mismo modo este se encarga de preservar la integridad y estabilidad de los recursos en la red.

La función del firewall es inspeccionar el tráfico que pasa por la capa 4 del modelo OSI, mejor conocida como la capa de transporte, de modo que cualquier sesión que se esté negociando como parte de una conexión existente pueda ser admitida y rastreada.

Dicha plataforma tiene la capacidad de realizar cualquiera de las técnicas de un firewall, incluso el ASA tiene muchas características que van más allá de las técnicas básicas, dándole así una gran versatilidad.

En la figura 19 se puede aprecia una vista general del CISCO ASA 5510.

Figura 19. Firewall CISCO ASA 5510.

Fuente: https://www.cisco.com/c/en/us/support/security/asa-5510-adaptive-security-appliance/model.html#~tab-documents

Fecha de lanzamiento: 04/05/2005.

Fecha de fin de venta: 16/09/2013.

Fecha de fin de soporte: 30/09/2018.

5.1.3 Especificaciones del Cisco ASA 5510

La tabla de las especificaciones más importantes a tener en cuenta acerca del ASA 5510 se puede apreciar en el anexo 1.

La capacidad de memoria de los distintos firewalls CISCO ASA se puede apreciar en la tabla 2.

Tabla 2. Memoria de CISCO ASA.

ASA MODEL	Internal Flash Memory (Default Shipping)	DRAM (Default Shipping)	
		Before Feb. 2010	After Feb. 2010 (Required for 8.3 and higher)
5510	256 MB	256 MB	1 GB
5520	256 MB	512 MB	2 GB
5540	256 MB	1 GB	2 GB
5550	256 MB	4 GB	4 GB

Fuente: El Autor.

En la figuras 20, 21, 22 y 23 se logran ver imágenes del aspecto físico del CISCO ASA 5510 en su vista frontal, trasera, trasera con conexiones y de su módulo SSM.

5.1.4 Vista Frontal del ASA 5510

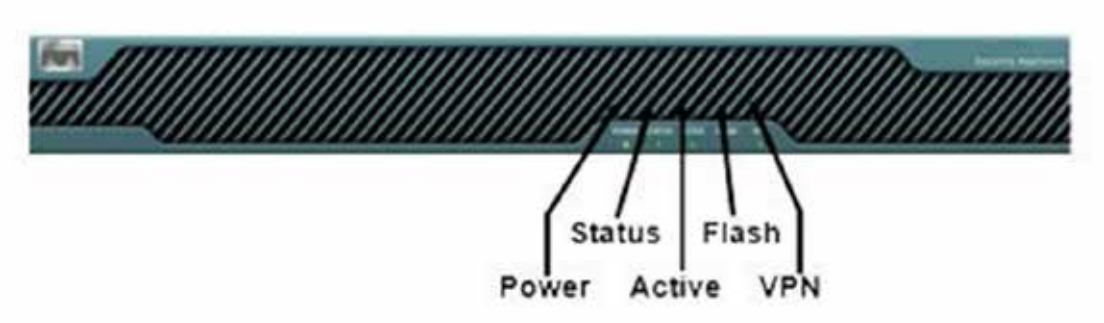

Figura 20. Vista Frontal.

Fuente: https://rumyittips.com/an-introduction-to-cisco-asa-firewall/

5.1.5 Vista Trasera del ASA 5510

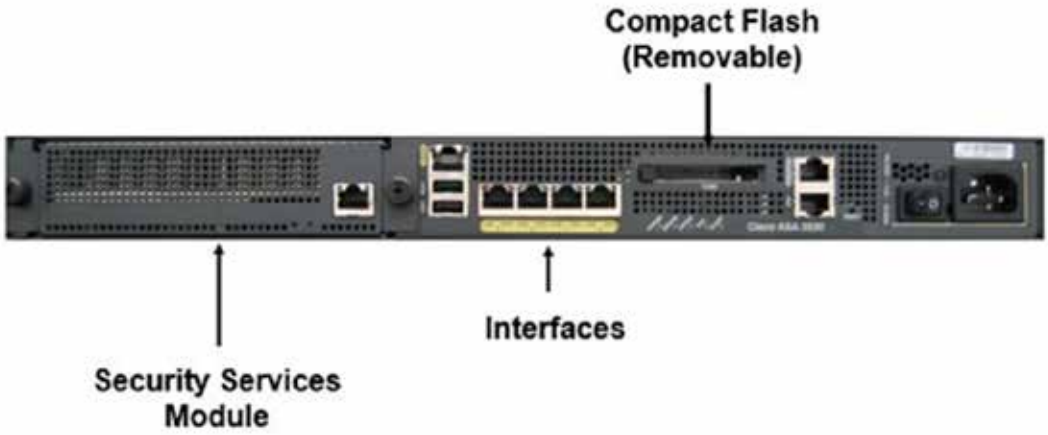

Figura 21. Vista Trasera.

Fuente: https://rumyittips.com/an-introduction-to-cisco-asa-firewall/

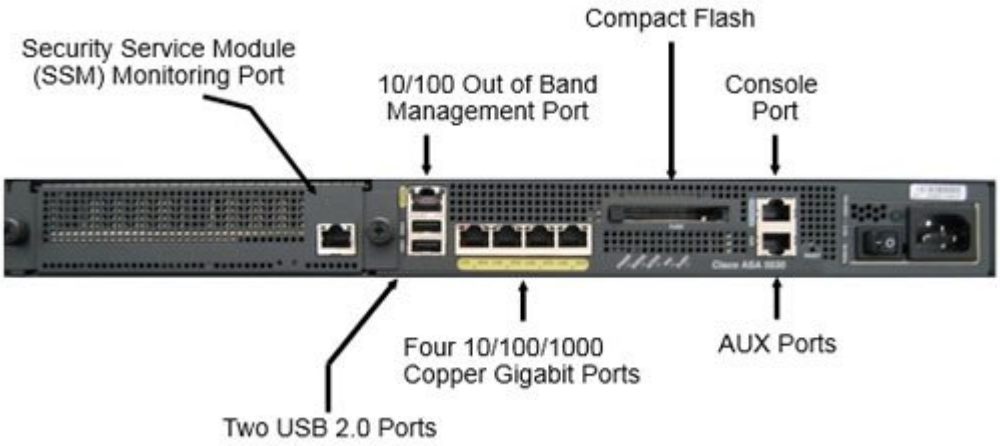

Figura 22. Vista trasera conexiones.

Fuente: https://rumyittips.com/an-introduction-to-cisco-asa-firewall/

5.1.6 Security Service Module (SSM)

Figura 23. SSM Vista interna.

Fuente:https://rumyittips.com/an-introduction-to-cisco-asa-firewall/

5.2 Describir como los protocolos de seguridad usados inciden en la vulnerabilidad de la red corporativa.

En la actualidad tanto el firewall como el proxy requieren de unas mejoras en su funcionamiento, ya que lo que se anhela es limitar el ancho de banda mediante un filtrado web para así evitar que los trabajadores accedan a sitios en la web no permitidos como lo son redes sociales o cualquier página de streaming.

El firewall CISCO ASA 5510 que se encuentra en las instalaciones de Montana Grafica C.A., es muy ambiguo y esto puede llegar a hacer más difícil sus configuraciones, ya que son muy tediosas, sin embargo, posee una forma de filtrar el trafico web mediante su interfaz gráfica, la cual deberá activarse mediante su CLI (Command Line Interface) para así poder acceder a ella.

En la figura 24 se aprecia la evolución de los modelos CISCO ASA.

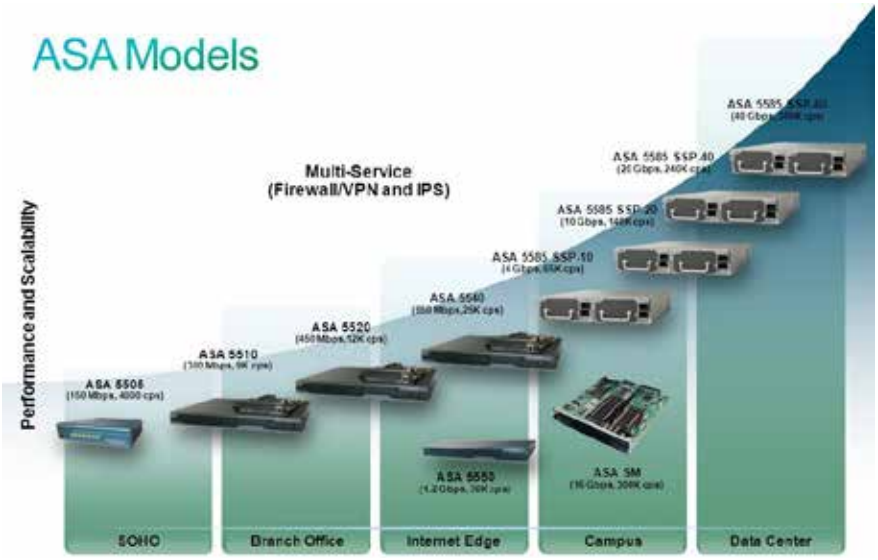

Figura 24. Evolución de los firewalls CISCO ASA.

Fuente: https://sclabs.blogspot.com/2013/01/chapter-10-implementing-cisco-adaptive.html

La interfaz gráfica denominada CISCO ASDM (Cisco Adaptive Security Device Manager) permite ver el tráfico de datos de las interfaces internas, así como también filtrar el tráfico web, pero de una manera muy compleja.

5.2.1 Activación de la interfaz gráfica del Cisco ASA 5510

Primeramente, para poder trabajar con la interfaz gráfica es necesario que el firewall tenga cargado el archivo.bin del software, además de tener habilitado el servicio HTTP para poder acceder a él.

Consiguiente a eso, se configurará el nombre y las contraseñas enable y el usuario de login:

```
ciscoasa(config)# hostname MGR-ASA

MGR-ASA(config)# enable password Cisco123

MGR-ASA(config)# username admin password Cisco123 privilege 15
```

Luego se procederá a configura la interfaz de management:

```
MGR-ASA(config)# interface management 0/0

MGR-ASA(config-if)# nameif management

INFO: Security level for "management" set to 0 by default.

MGR-ASA(config-if)# security-level 100

MGR-ASA(config-if)# management-only

MGR-ASA(config-if)# ip add 192.168.16.129 255.255.255.0

MGR-ASA(config-if)# no shutdown
```

Ahora se habilitará el servicio HTTP y se indicará que sea desea acceder a él a través de la red 192.168.16.0/24:

```
MGR-ASA(config)# http server enable

MGR-ASA(config)# http 192.168.16.0 255.255.255.0 management
```

Ahora bien, se procederá a cargar la imagen del ASDM al firewall, luego se seleccionará para que sea utilizada y se indicará para que trabaje con el logging en nivel 7 en la GUI, luego se guardara la configuración para no perder los cambios realizados en el firewall:

```
MGR-ASA(config)# copy tftp://192.168.16.1/asdm-792.bin disk0:/asdm-792.bin

Address or name of remote host [192.168.16.1]?

Source filename [asdm-792.bin]?

Destination filename [asdm-792.bin]?

Accessing tftp://192.168.16.1/asdm-792.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Verifying file disk0:/asdm-792.bin...

!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Writing file disk0:/asdm-792.bin...

32738292 bytes copied in 56.250 secs (584612 bytes/sec)

MGR-ASA(config)# asdm image disk0:/asdm-792.bin

MGR-ASA(config)# logging asdm 7

MGR-ASA(config)# write
```

```
Building configuration...

Cryptochecksum: 6a6c4aa1 19f10818 b5b7ce50 83d54555

6565 bytes copied in 0.250 secs

[OK]

MGR-ASA(config)#
```

Una vez cargado el ASDM en el firewall, es posible descargar el instalador accediendo a la siguiente ruta: https://<asa_ip_address>/admin , así como se observa en la figura 25.

Figura 25. Accediendo a la dirección 192.168.16.129

Fuente: El Autor.

En el momento en el que el instalador sea descargado, se procederá a ingresar con el usuario y contraseña previamente configurada en la línea de comandos, así como aprecia en a figura 26.

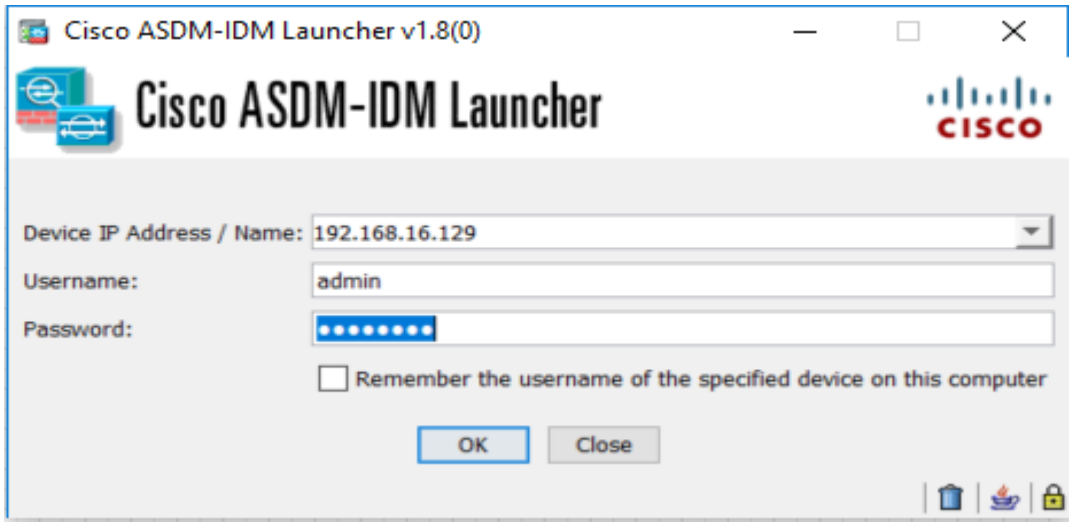

Figura 26. Cisco ASDM Launcher.

Fuente: El Autor.

Finalmente se ingresa a la interfaz gráfica del CISCO ASA 5510, allí se aprecia su ventana de inicio, como se puede observar en la figura 27.

Figura 27. Ventana de Inicio de la interfaz gráfica.

Fuente: El Autor.

Seguidamente, se seleccionará la pestaña configuración ubicada en lado superior de la ventana, para luego poder seleccionar la pestaña del firewall, y de allí seleccionar donde dice reglas de filtrado para poder aplicar el filtrado correspondiente como logra en la figura 28.

Figura 28. Configuración del Firewall.

Fuente: El Autor.

5.3 Formular y establecer las políticas de seguridad informática y los protocolos aplicables a redes corporativas.

El protocolo de seguridad que se va a aplicar en la red de Montana Grafica C.A. será Sophos Central, cabe destacar que sophos se sincroniza con el Active Directory (AD), la cual es una herramienta de microsoft que proporciona servicios de directorio normalmente en una red LAN.

El active directory es el que le exporta la base de datos de los usuarios e ip privadas de la empresa a sophos.

Las configuraciones a aplicar se deben realizar desde la página web https://central.sophos.com/manage/login, allí se debe ingresar con el usuario correspondiente.

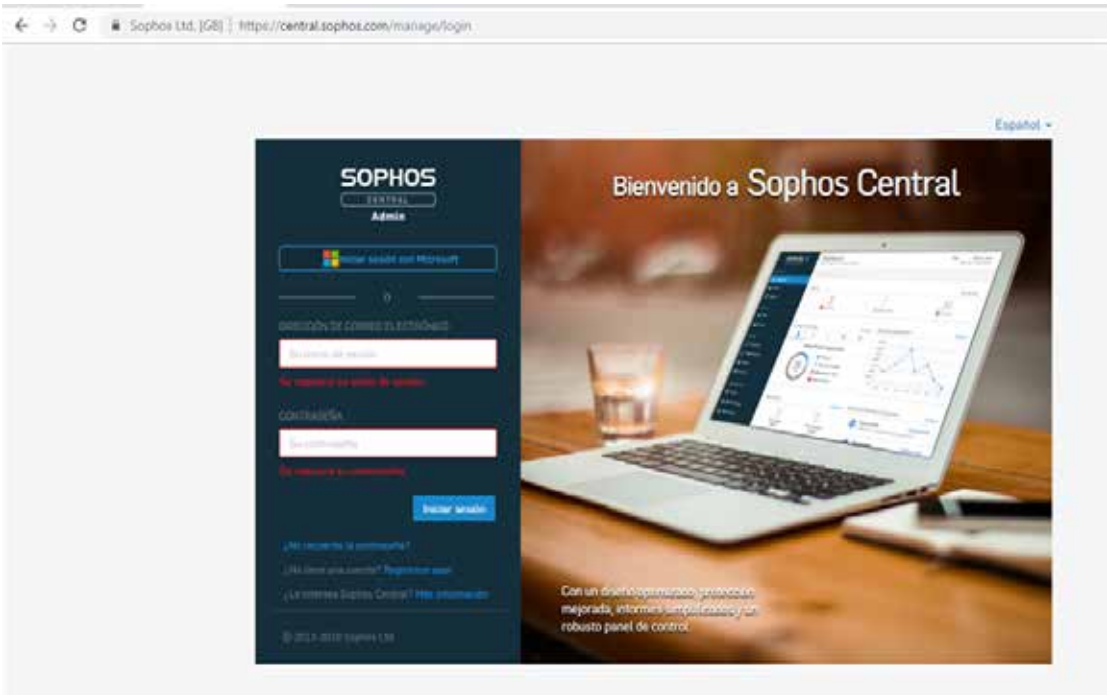

Figura 29. Inicio de sesión en Sophos.

Fuente: El Autor.

Una vez adentro se situará la página de inicio de sophos central, tal y como se puede apreciar en la figura 30.

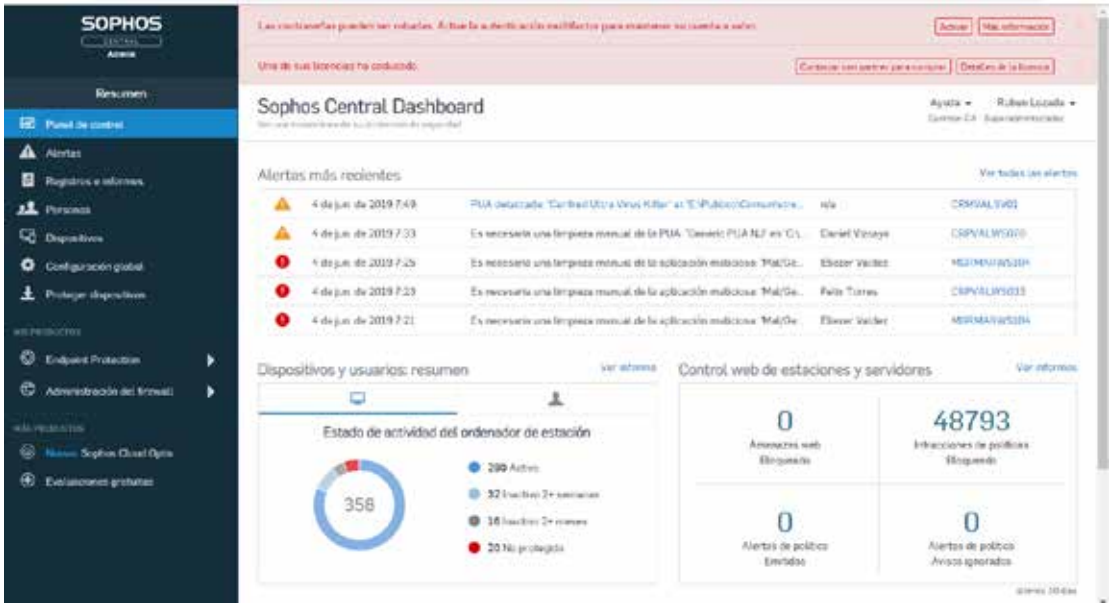

Figura 30. Página de inicio de Sophos Central.

Fuente: El Autor.

Allí se puede observar en el panel izquierdo los productos adquiridos, se seleccionará Endpoint protection, la cual es la herramienta aplicativa que se empleara para realizar el filtrado de navegación como se puede ver en la figura 31.

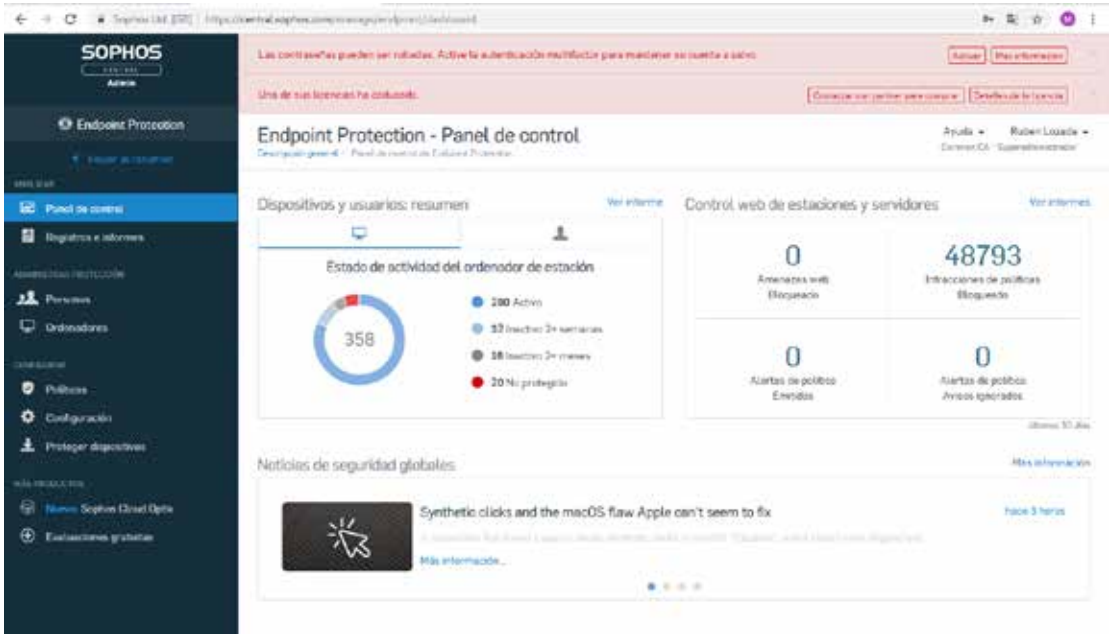

Figura 31. Endpoint Protection.

Fuente: El Autor.

En el área de control web, esta impuesta una política de nombre “Política base control web”, la cual es una política aplicada por defecto cuando no existen otras políticas creadas. Ver figura 32.

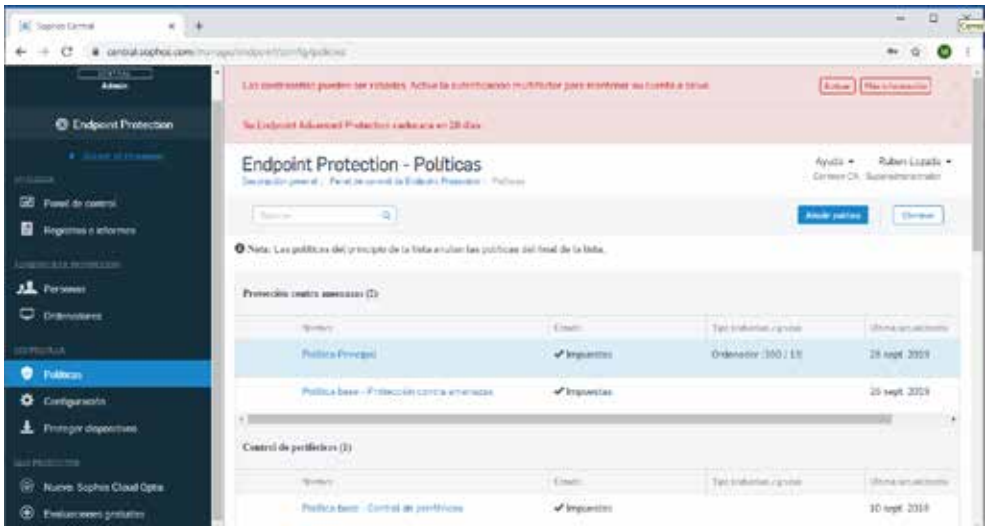

Figura 32. Políticas.

Fuente: El Autor.

Ahora bien, se creará una nueva política de seguridad referente al control web, para esto se seleccionará la opción añadir política. Ver figura 33.

Figura 33. Añadir Política.

Fuente: El Autor.

Procedente a esto, se desplegará el listado que allí se observa, el cual mostrará varias opciones de políticas a crear que contiene el producto, se seleccionara la que interesa la cual es control web.

La política ha sido creada tal cual como se observa en la figura 34, ahora se le pondrá el nombre que se desea, lo recomendable es que el nombre indique el lugar de referencia o departamento donde se aplique.

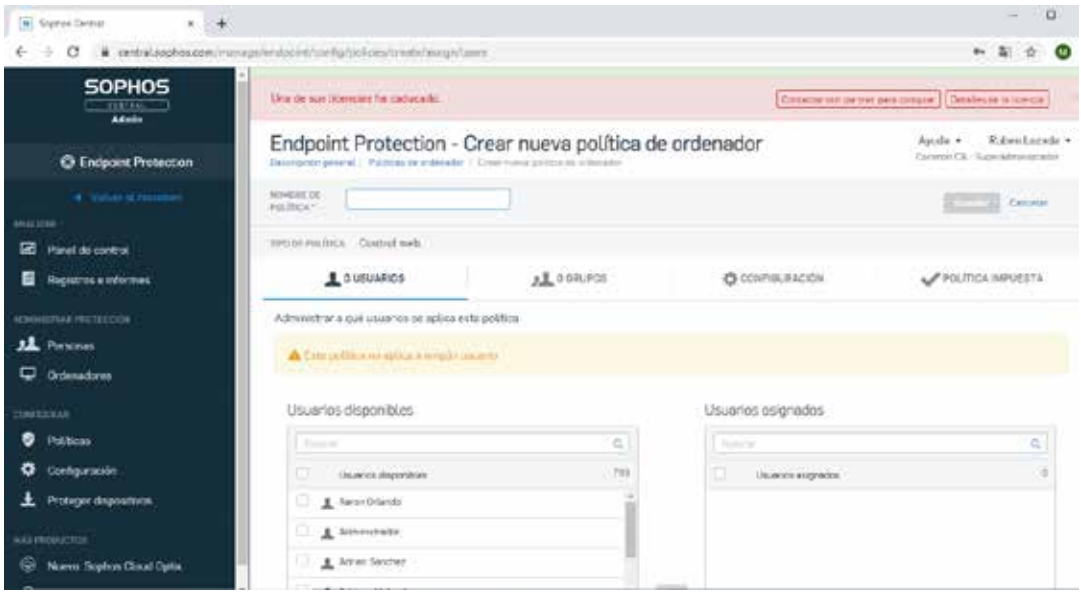

Figura 34. Política Creada.

Fuente: El Autor.

Procedente a este paso, se seleccionará la pestaña configuración para aplicar las restricciones necesarias. Ver figura 35.

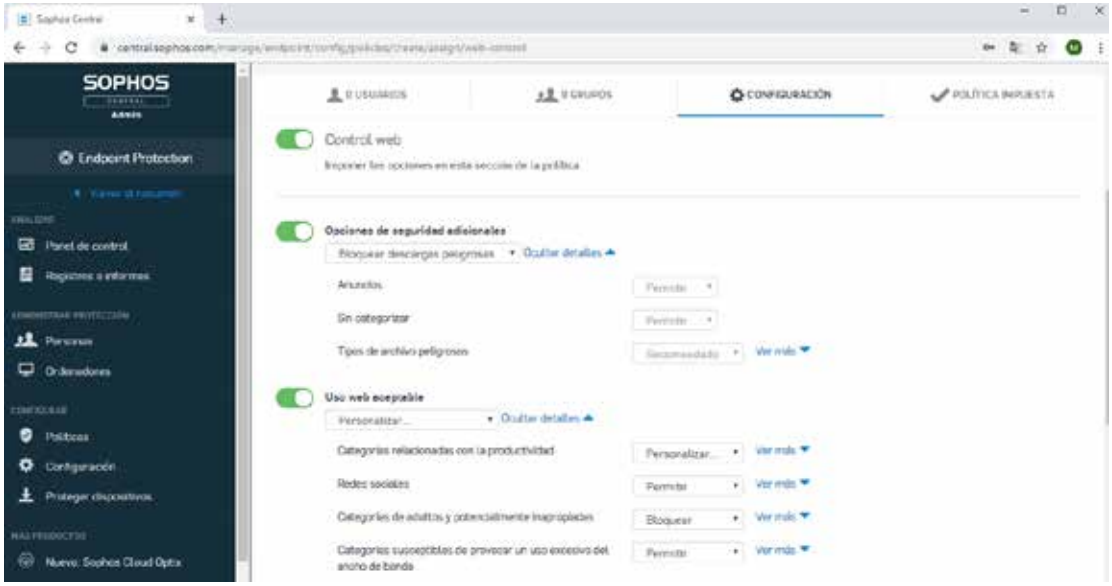

Figura 35. Pestaña Configuración.

Fuente: El Autor.

Como se observa, se pueden aplicar muchas configuraciones que ofrece endpoint protection, por ahora la que es de interés es la se titula como “Uso de web aceptable”, se dará click allí para desplegar el menú. Ver figura 36.

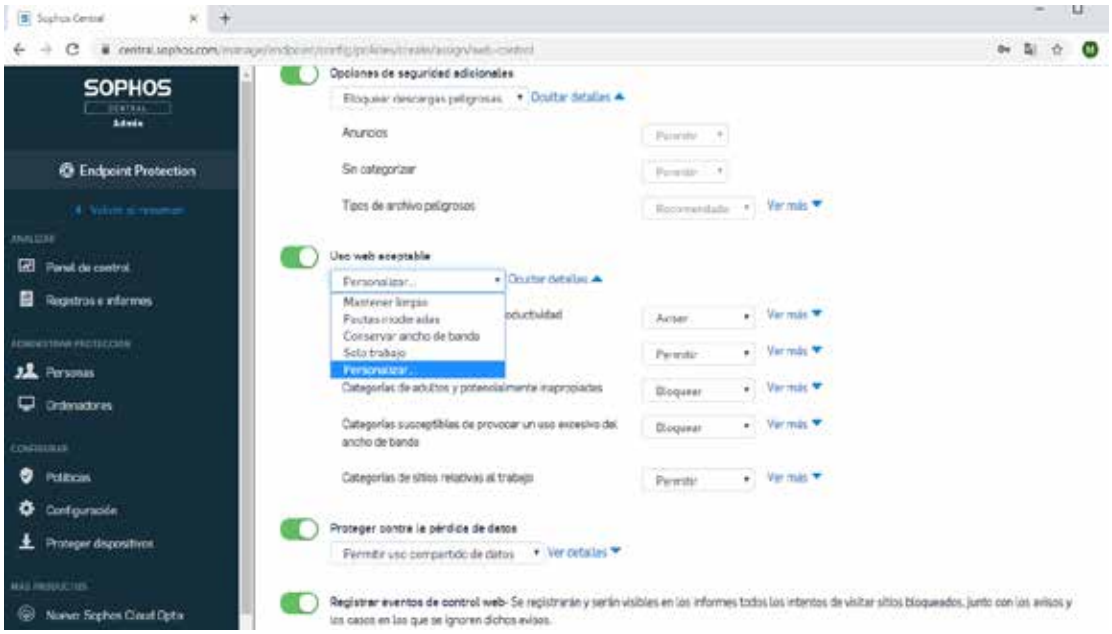

Figura 36. Uso web aceptable.

Fuente: El Autor.

Allí se seleccionará la opción personalizar, la cual es la que permitirá ejecutar de forman manual y a nuestros intereses las sub categorías del control web. Ver figura 37.

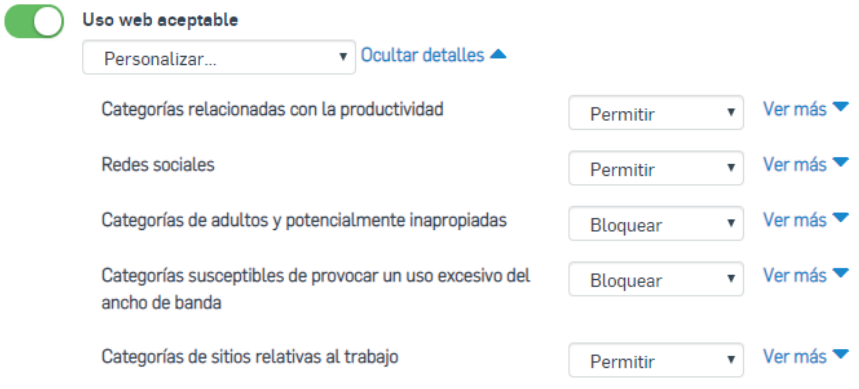

Figura 37.Uso web aceptable (personalizar).

Fuente: El Autor.

Cada subcategoría posee un menú desplegable con las opciones: permitir, avisar, bloquear y personalizar. Se seleccionará la opción personalizar en la sub categoría de redes sociales, tal cual como se observa en la figura 38.

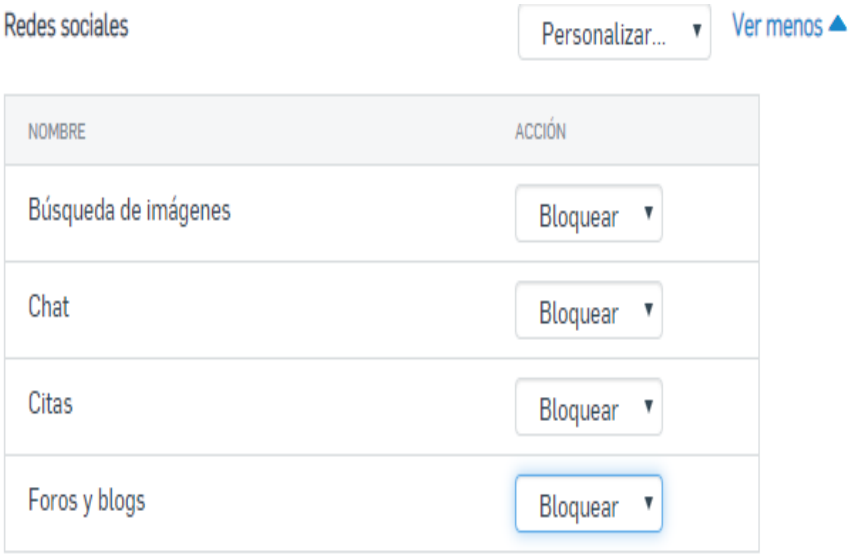

Figura 38. Subcategorías redes sociales.

Fuente: El Autor.

Y seguidamente al anterior paso, se seleccionará la opción bloquear a todas las subcategorías, lo cual impedirá el acceso a redes sociales.

Es importante señalar que se puede bloquear páginas web específicas, mediante la creación de unas etiquetas como se señala en la figura 39.

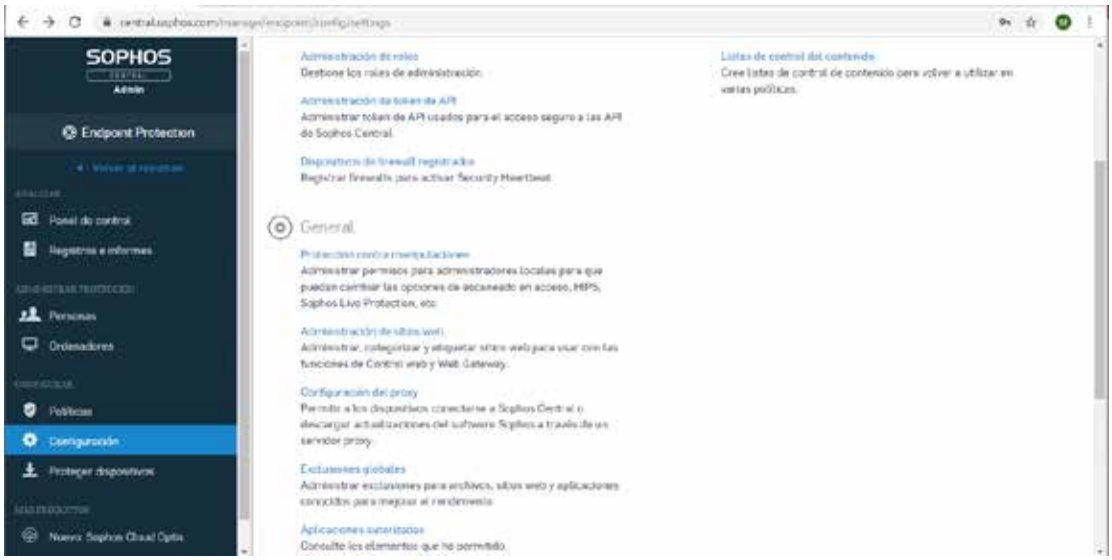

Figura 39. Configuración para crear etiquetas.

Fuente: El Autor.

En el costado izquierdo, se puede apreciar que existe una pestaña llamada configuración, se accederá a ella y procedente a esto se buscará donde diga administración de sitios web, una vez encontrado se accede a él.

A primera vista, se encontrará las etiquetas que fueron creadas anteriormente, pero como se trata de un ejemplo, se seleccionara donde dice añadir para crear una.

Ver figura 40 y 41 para tener una mejor idea.

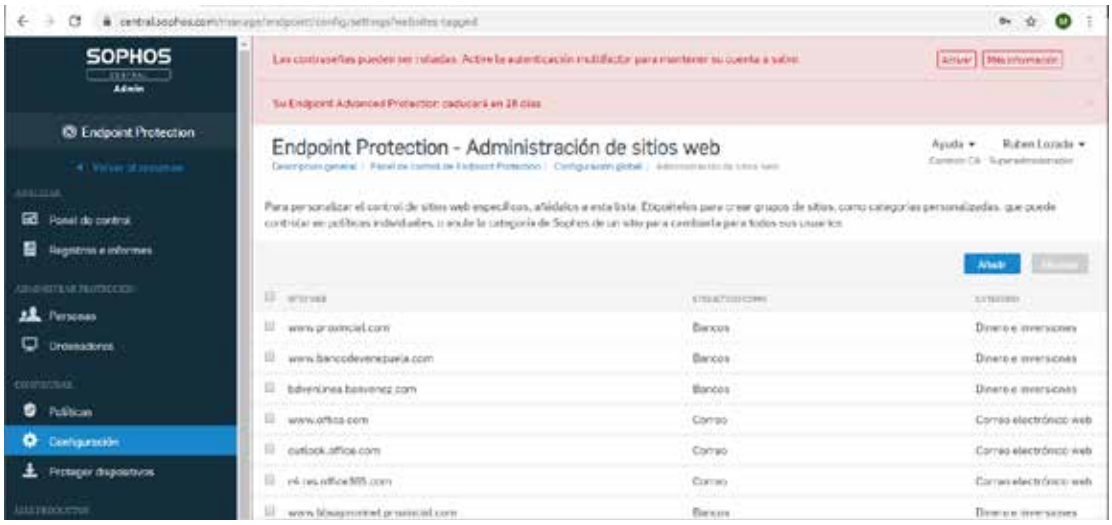

Figura 40. Lista de etiquetas.

Fuente: El Autor.

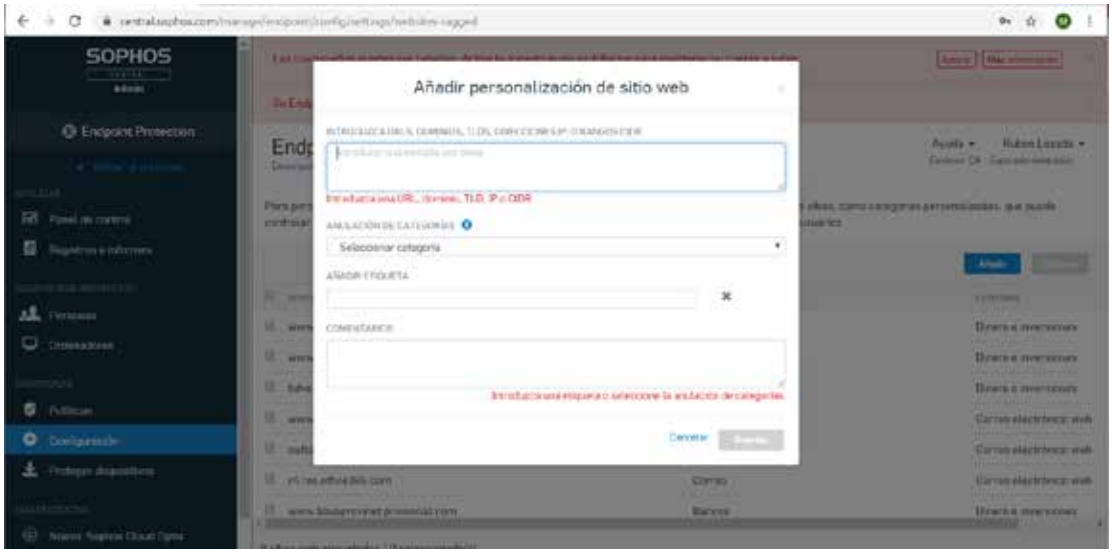

Figura 41. Añadir personalización de sitio web.

Fuente: El Autor.

Ahora bien, se podrá agregar la dirección web que se desea y ubicarla en la categoría que corresponda, así como también crear la etiqueta. Ver figura 42.

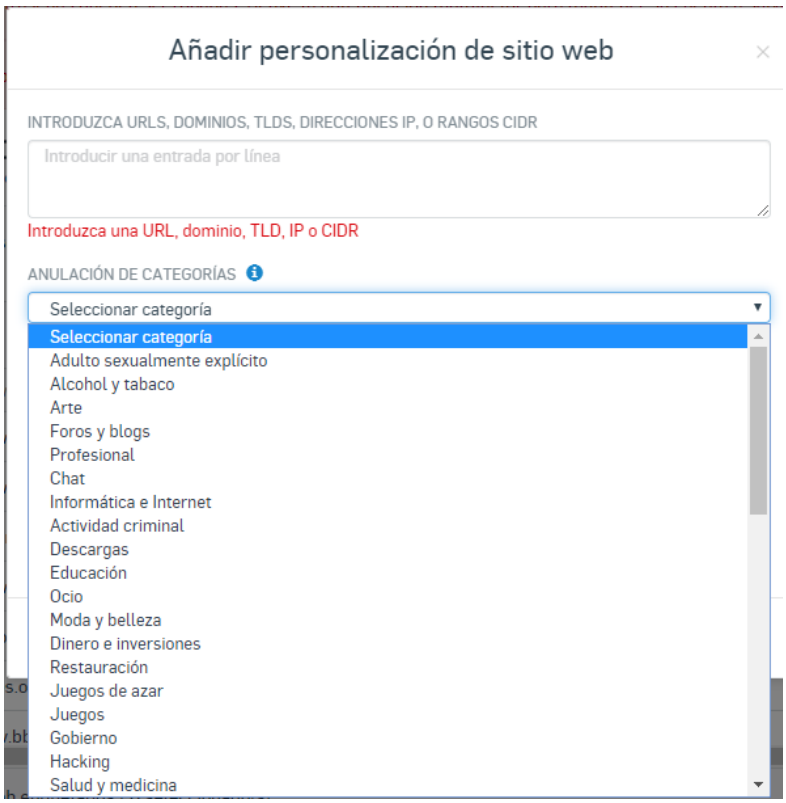

Figura 42. Categorías de etiquetas.

Fuente: El Autor.

Ahora solo dar click en guardar, se creará la etiqueta, con esto se podrá ubicar una política web creada y aplicar la etiqueta creada anteriormente tal y como se muestra en la figura 43, para luego seleccionar en el menú desplegable si es permitida o bloqueada.

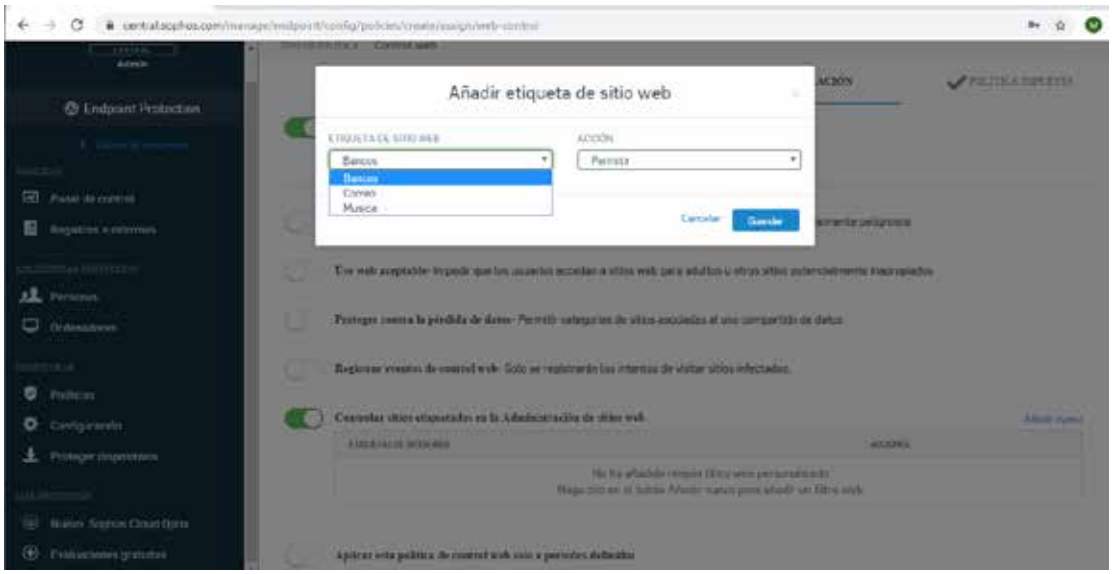

Figura 43. Etiqueta creada.

Fuente: El Autor.

La política ya está creada, ahora falta asignarla a los usuarios correspondientes; se puede realizar de dos maneras, ya sea usuario por usuario o creando un grupo para meter a los usuarios en él.

En este caso se optó por crear un grupo para llevar un mejor orden, el grupo se creó como se observa en la figura 44.

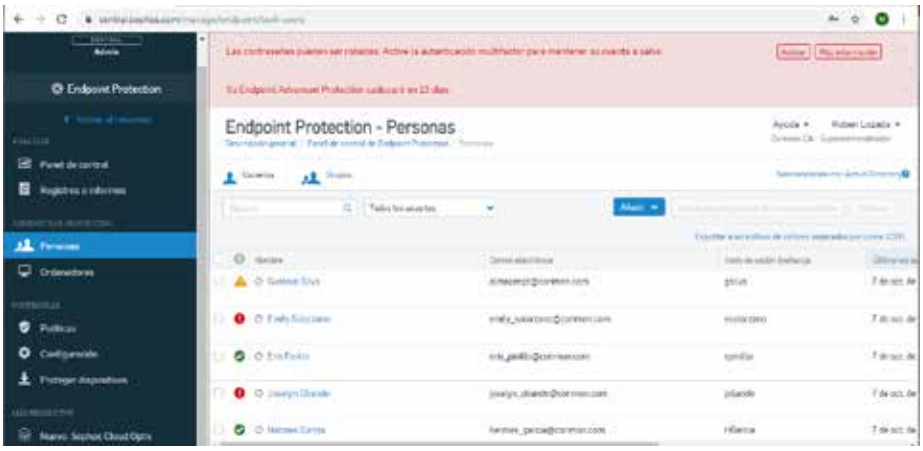

Figura 44. Crear grupo.

Fuente: El Autor.

Se seleccionará la pestaña personas en el lado izquierdo y luego se procederá a seleccionar la pestaña grupos, allí se dará click en añadir. Ver figura 45.

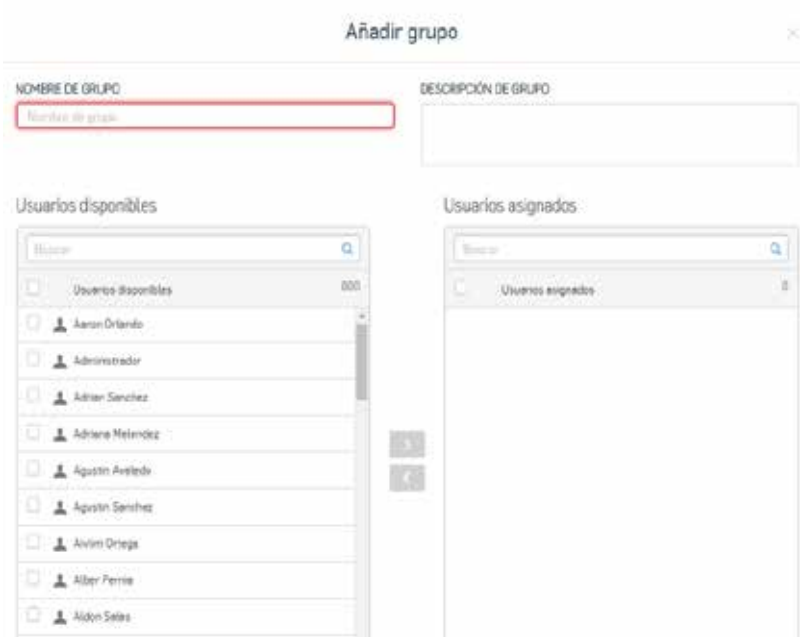

Figura 45. Añadir grupo.

Fuente: El Autor.

El grupo fue creado con éxito, ahora solo falta ir a la política que se crea y seleccionar el grupo para que así las configuraciones se apliquen sobre los usuarios que conforman ese grupo.

Figura 46. Aplicando la política al grupo.

Fuente: El Autor.

En la figura 46, se puede observar que se ha añadido el grupo “MGR Filtrado Web Redes Sociales”, el cual fue el grupo creado con los usuarios correspondientes a aplicar la política web de filtrado. Finalmente, dar click en guardar.

Listo, el filtrado web ya fue creado con éxito, los cambios tardaran en hacer efecto entre 8-10 min, mientras la información se carga en la nube.

5.3.1 Como funciona Sophos Endpoint Protection en el área de Filtrado Web.

Sophos Endpoint Protection realiza un filtrado mediante el DPI (Deep Packet Inspection) o mejor conocido en español como Inspección Profunda de Paquetes, haciendo referencia a paquetes como la unidad de datos de protocolo (PDU) de la capa 3 del modelo OSI.

Los firewalls convencionales trabajan sobre la capa 3 del modelo OSI, por lo que la inspección del paquete está relacionada al header o encabezado del mismo, este tipo de filtrado se le conoce como Stateful Packet Inspection, por lo cual solo pueden filtrar el tipo de tráfico, pero por el encabezado IP

La inspección solamente del encabezado no es confiable, dado que muchas aplicaciones usan puertos dinámicos o reutilizan puertos que anteriormente eran utilizados por otras aplicaciones, haciendo así posible saltar el filtrado de este tipo de firewall.

DPI, inspecciona desde la capa 2 a la capa 7 del modelo OSI, directamente sobre la capa 7, de aplicación, por lo cual un equipo con DPI, podría filtrar tipos de tráfico más precisos, como virus, P2P, y diferentes tipos de ataques, siendo así más preciso. Al trabajar sobre directamente la capa 7, podemos filtrar por aplicaciones, como por ejemplo YouTube, Skype y cualquier tipo de aplicación, esto resulta ideal para un administrador de red, porque podrá analizar de manera más efectiva el tráfico que está pasando por la misma.

Ahora bien, lo que realiza sophos es un DPI que permite tener una lista de contenido para restringir las palabras claves o cualquier otro tipo de información, es por ello que cualquier palabra o término asociado con redes sociales que encuentre en el paquete, este lo bloqueará. En las figuras 47 y 48 se muestra como se dividen las capas del modelo OSI.

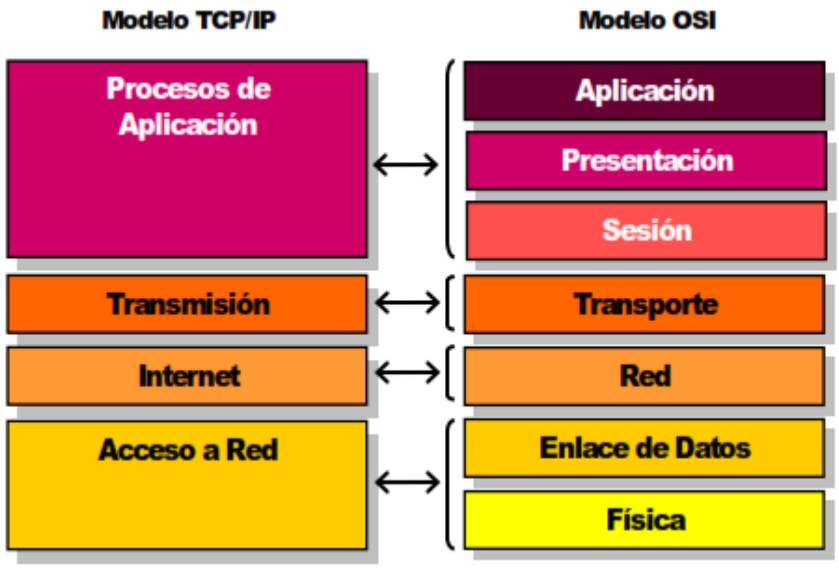

Figura 47. Modelo TCP/IP y Modelo OSI.

Fuente: Gerometta (2013).

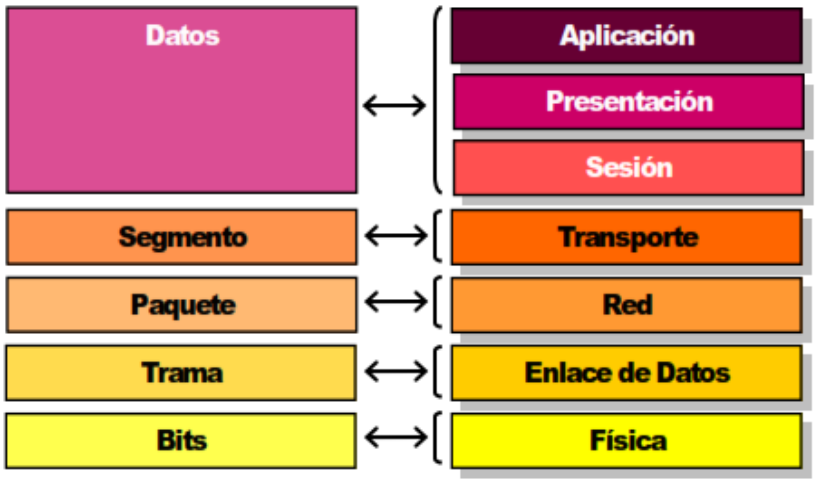

Figura 48. PDU de cada capa.

Fuente: Gerometta (2013).

5.4 Evaluar el desempeño de la seguridad de la red corporativa de Montana Grafica C.A, de acuerdo a las políticas establecidas.

Para evaluar que las políticas establecidas estaban teniendo efecto, se accedió a ir a Montana Grafica C.A. y desde varios usuarios, se intentó acceder a páginas web que están restringidas por el filtrado web, específicamente las catalogadas como redes sociales.

El resultado se puede apreciar en las figuras 49, 50, 51, 52 y 53.

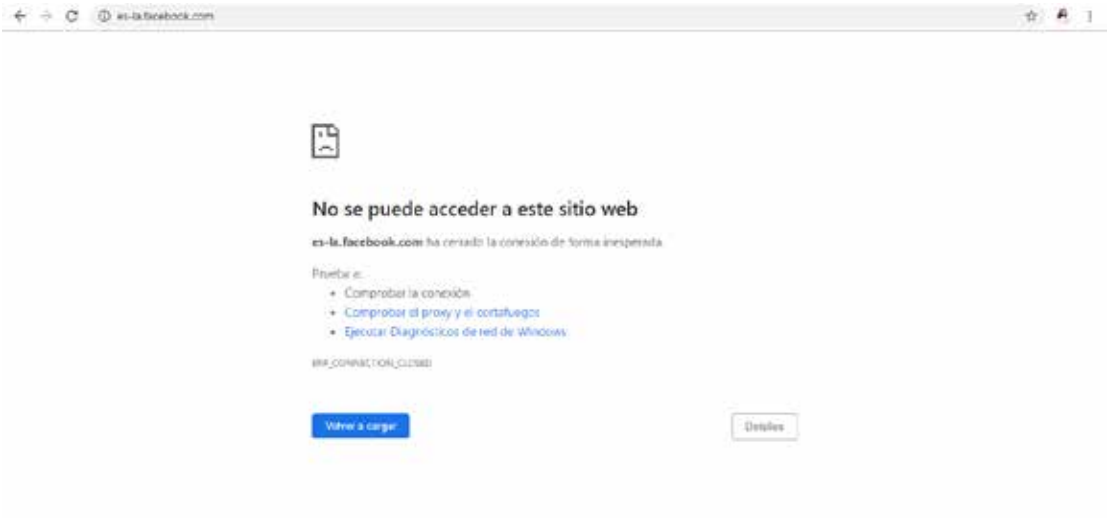

Figura 49. Facebook.

Fuente: El Autor.

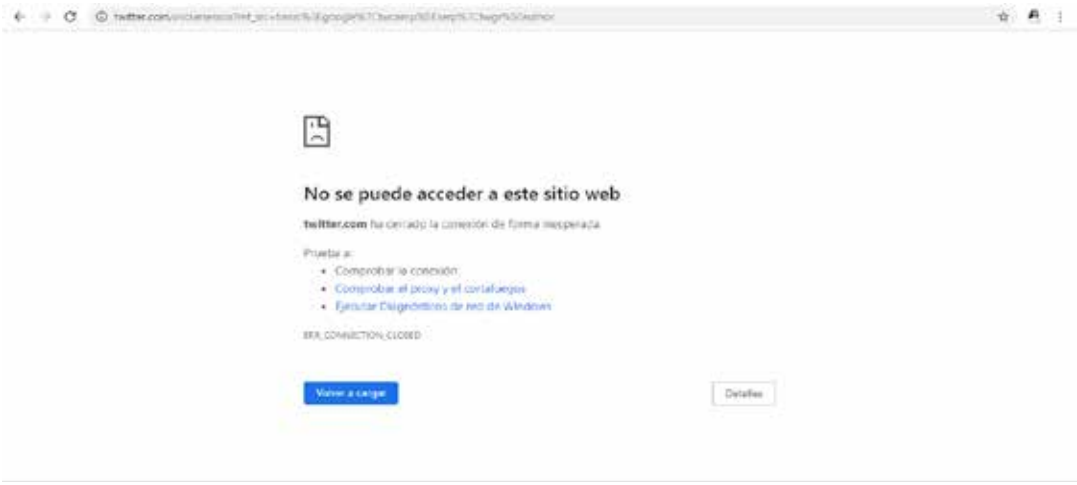

Figura 50. Twitter.

Fuente: El Autor.

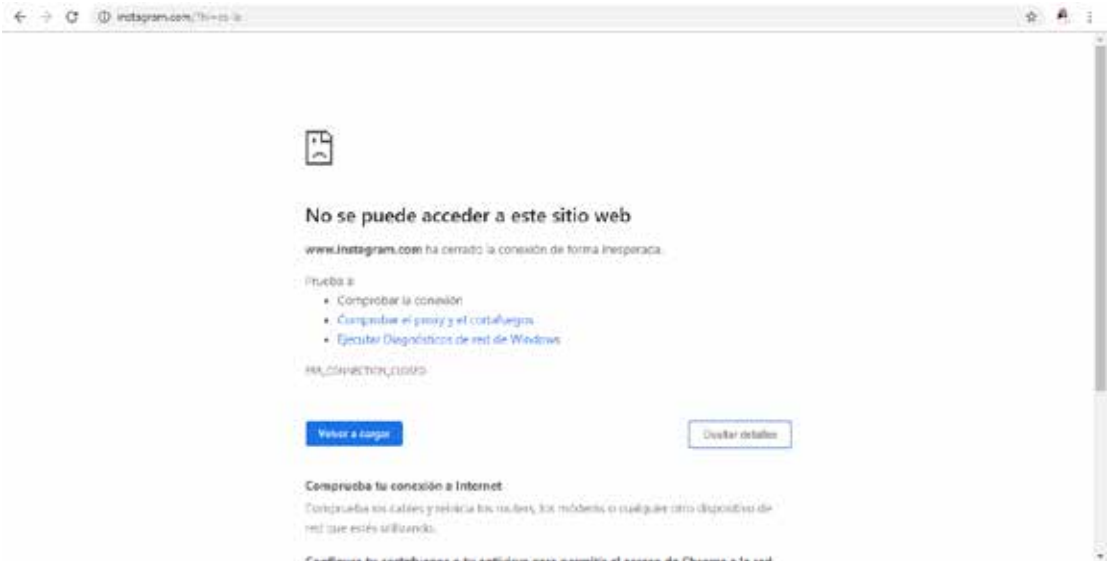

Figura 51. Instagram.

Fuente: El Autor.

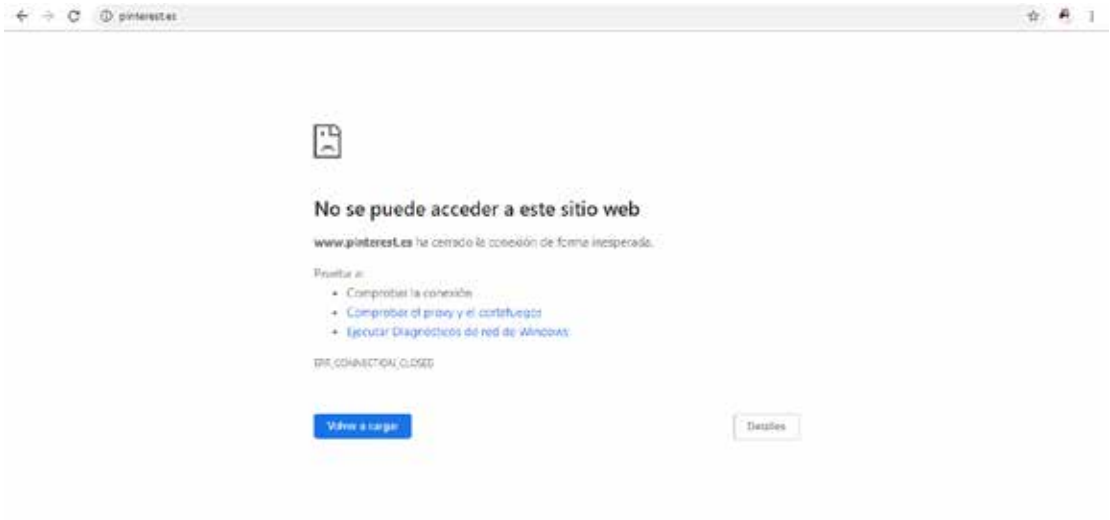

Figura 52. Pinterest.

Fuente: El Autor.

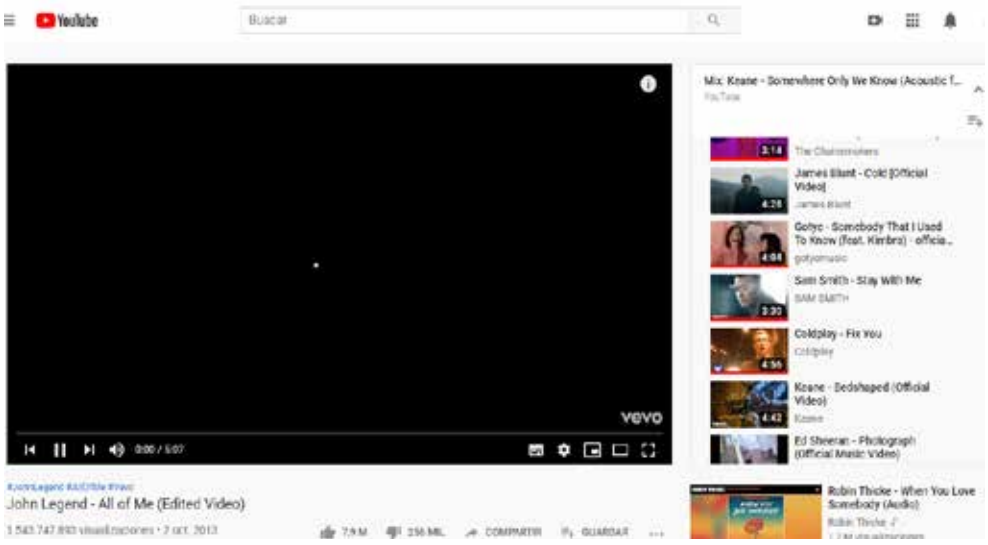

Figura 53. YouTube

Fuente: El Autor.

En el caso de youtube, el usuario puede entrar a la página y buscar distintos videos, pero sophos no le dejara reproducir ninguno, por lo que siempre quedará en un permanente buffering.

Como se puede apreciar el usuario no puede acceder a páginas que estén relacionadas con redes sociales ni streaming, el mensaje que se aprecia dice que se ha cerrado la conexión, por ende, el filtrado web está trabajando correctamente.

CONCLUSIONES

En este trabajo de aplicación profesional se evaluó las características de las políticas de seguridad informática usadas en la red corporativa de Montana Grafica C.A., con el propósito de proponer e implementar protocolos de seguridad actualizados.

Por otra parte, se logró identificar el tipo de seguridad de información que empleaba Montana Grafica C.A, en su red corporativa, así como también conocer las especificaciones del firewall CISCO ASA 5510 y que mejoras se le pueden aplicar para así llevar un mejor control del acceso a la web por parte de los usuarios.

Se formuló y se estudió a profundidad la herramienta de seguridad conocida como sophos para poder tener un mejor control web en la empresa Montana Grafica, así como también se indicó paso a paso como ejecutar un filtrado web adecuado.

Seguidamente se realizaron pruebas al intentar acceder a páginas catalogadas como redes sociales y streaming como lo son: Facebook, twitter, Instagram, Pinterest y youtube, entre otras, el resultado fue un total éxito ya que no se pudo acceder.

Para finalizar se puede agregar que no solo se logró un filtrado web correcto, sino que también se logró reducir el consumo del ancho de banda, ya que las redes sociales consumen una alta cantidad.

RECOMENDACIONES

1- Mantener una constante revisión de la seguridad de información para así estar actualizados a las nuevas amenazan que nacen día a día en el mundo de las redes.
2- Si está en la capacidad adquisitiva de la empresa obtener una herramienta de ayuda que permita controlar y saber con exactitud en donde se gasta el ancho de banda.
3- No abandonar por completo el CISCO ASA 5510, ya que este posee algunas funciones que sophos no, y juntos pueden lograr una mejor seguridad.
4- Apoyándose en este trabajo de aplicación profesional realizar un manual de usuario de cómo usar sophos para el departamento de TI, y así quien pueda llegar en un futuro pueda tener un conocimiento adecuado.

REFERENCIAS

(2003). Contexto general de las comunicaciones móviles. En O. Sallent Roig, J. L. Valenzuela Gonzales, & R. Agustí Comes, *Principios de comunicaciones móviles* (pág. 14). Barcelona.

Arias, F. (2006). “El Proyecto de Investigación. Introducción a la metodología científica”. (5ª. ed.). Caracas, Venezuela: Episteme.

Gómez A. (2010). “Servicios en red e informática” Editorial EDITEX. 1era edición.

Méndez, C (1999). “Metodología, diseño y desarrollo del proceso de investigación” Editorial Mc Graw-Hill. 4ta edición.

Palella, S. (2006). “Metodología de la investigación cuantitativa”. 2da edición. Caracas, Venezuela.

Soriano, M (2013). “Seguridad en redes y seguridad de la información”. 1era edición. Republica Checa

.

Stallings, W (2004). “Comunicaciones y redes de computadores”. Editorial Prentice Hall-Pearson. 7ma Edición. México.

Tamayo y Tamayo, M (2003). El Proceso de la Investigación Científica. (4ª. ed.) México: Limusa.

Taneambaum, A (2003). “Redes de computadoras”. Editorial Prentice Hall-Pearson. 4ta Edición. Holanda.

ANEXOS

Anexo 1

Dimensions (H x W x D):	1.75 x 17.5 x 13.2 inches
Non-Operating Relative Humidity:	5 to 95 percent noncondensing
System Bus:	Multibus architecture
Memory:	256 MB
Operating Relative Humidity:	5 to 95 percent noncondensing
Input (per power supply) Normal line voltage:	100 to 240 VAC
Non-Operating Altitude:	0 to 15,000 ft (4570 m)
SerialPorts:	2 RJ-45, console and auxiliary
SSM Expansion Slot:	1
Virtual interfaces (VLANs):	10; 25
Non-Operating Vibration:	0.41 Grms2 (3 to 500 Hz) random input
Operating Shock:	1.14 m/sec (45 in./sec) 1/2 sine input
Operating Acoustic Noise:	60 dBa max
Integrated ports:	5-10/100; 2-10/100/1000; 3-10/100; +4-10/100/1000; 4 SFP (with 4GE SSM)
Firewall Throughput :	Up to 300 Mbps
Input (per power supply) Current:	3A
Operating Altitude:	0 to 9840 ft (3000 m)
Concurrent Threat Mitigation Throughput (firewall + IPS services) :	Up to 150 Mbps with AIP-SSM-10
New sessions/second:	6000
Form factor:	1 RU, 19-in. rack-mountable
Non-Operating Temperature:	-13 to 158 F (-25 to 70 C)
Output Steady State:	150W
High Availability:	Not supported; Active/Standby
SSL VPN Peer License Levels:	10, 25, 50, 100, or 250
Minimum System Flash:	64 MB
Input (per power supply) Range line voltage:	100 to 240 VAC

Weight (with power supply):	20.0 lb (9.07 kg)
Security Contexts :	Not supported
Operating Vibration:	0.41 Grms2 (3 to 500 Hz) random input
IPSec VPN Peers:	250
Weight:	20.0 lb (9.07 kg) with power supply
Interfaces:	3 Fast Ethernet + 1 management port; 5 Fast Ethernet ports
Operating Temperature :	32 to 104 F (0 to 40 C)
Output Maximum Peak:	190W
Input (per power supply) Frequency:	47 to 63 Hz, single-phase
Users/Nodes:	Unlimited
USB 2.0 Ports:	2
Concurrent Sessions :	50,000/130,000
User-accessible flash slot:	1
Non-Operating Shock:	30 G
VPN Throughput:	Up to 170 Mbps
Output heat dissipation:	648 BTU/hr