DISEÑO DE UNA GUIA DE SEGURIDAD PERIMETRAL ESCALABLE Y EN ALTA DISPONIBILIDAD CON EQUIPOS FIREWALL TIPO NGFW

AUTOR: CARLOS MARIO BENJUMEA OSPINO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

BOGOTA SEPTIEMBRE DEL 2016

PROYECTO DE GRADO

DISEÑO DE UNA GUIA DE SEGURIDAD PERIMETRAL ESCALABLE Y EN ALTA DISPONIBILIDAD CON EQUIPOS FIREWALL TIPO NGFW

AUTOR: CARLOS MARIO BENJUMEA OSPINO

DOCTORA: IVYS ALIETH DAVILA

DIRECTORA DEL PROYECTO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

BOGOTA SEPTIEMBRE DEL 2016

PROYECTO DE GRADO

RESUMEN

Actualmente las empresas sin importar su naturaleza demandan de intercambio de información, transacciones en línea y procesos informáticos necesario para su crecimiento, funcionamiento y adaptabilidad en los mercados actuales.

De acuerdo con el Departamento de Delitos Informáticos de la Policía Nacional de Colombia, el año 2015 se recibieron 7.118 denuncias, y en promedio, el 43% de las empresas en el país no poseen planes de respuesta frente a este tipo de incidentes; desafortunadamente son las pymes las más vulnerables, ya sea en materia de capacidad instalada o recursos económicos para afrontar ataques cada vez más sofisticados. (Bdo Colombia, 2016).

En pleno 2016, las organizaciones colombianas siguen sin darle el suficiente valor a la cantidad de datos que manejan. Tanto así que, durante el 2015, se recibieron 7.118 denuncias por parte de víctimas de delitos informáticos, evidenciando un aumento del 40 % con respecto al 2014, de acuerdo con un estudio que publicó el operador Movistar.

Lo más grave es que, según el mismo diagnóstico, las pérdidas económicas derivadas por estos actos representan al país alrededor del 0,14 % del PIB Nacional, es decir, cerca de 500 millones de dólares aproximadamente. Para completar el panorama, el 43 % de las empresas en el país no poseen planes de respuesta frente a los ataques de los piratas cibernéticos. (Portafolio, 2016).

En este sentido es un gran porcentaje de las organizaciones las que carecen de sistemas informáticos seguros que garantice la confiabilidad, disponibilidad e integridad de la información. La expansión de los centros de datos, la segmentación de la red, la virtualización y las iniciativas de movilidad obligan a replantear cómo habilitar el acceso a las aplicaciones y la de proteger la red contra una clase más sofisticada de amenazas avanzadas que eluden los mecanismos de seguridad tradicionales.

Este proyecto pretende diseñar una guía aplicable que pueda adaptarse a cualquier tipo de organización mediante esquemas de seguridad y dispositivos Firewall de nueva generación que

puedan ajustarse fácilmente y que las empresas sin importar su tamaño puedan implementar de acuerdo a su necesidad.

Logrando lo anterior las organizaciones puedan tener la tranquilidad de contar con accesos seguros e intercambio de información confiables garantizando en todo instante la disponibilidad, mejora de los servicios de Infraestructura Tecnológica IT, continuidad de servicio, óptimo desempeño, gestión, fortalecimiento, y administración a la infraestructura tecnológica que soporta todos los procesos misionales y administrativos y así mismo velar por la integridad de la información y la seguridad de la plataforma tecnológica.

Palabras Clave
Firewall NGFW, Ataques Informáticos, Escalabilidad y Disponibilidad, Balanceo de Tráfico Redes.

ABSTRACT

Currently, companies regardless of their nature demand information exchange, online transactions and computer processes necessaries for their own growth, operation and adaptability in the markets of today. A large percentage of the organizations lack secure computer systems to ensure reliability, availability and integrity of information.

The expansion of data centers, network segmentation, virtualization and mobility initiatives require to rethink how to enable access to applications and how protect networks against a more sophisticated kind of advanced threats that circumvent traditional security mechanisms.

This project aims to design an applicable guide that can be adapted to any kind of organization through security schemes and New Generation Firewall devices that can be easily adjusted, and the companies can to implement this according their needs, no matter their size.

This makes organizations can be quiet expecting secure access and reliable information exchange, ensuring availability at all times, improving Technology Infrastructure IT services, continuity of service, optimal performance, management, strengthening, and managing the technology infrastructure that supports all mission processes and administrative and likewise ensure the integrity of the information and technology platform security.

Keywords
Firewall NGFW, Computer Attacks, scalability and availability, traffic balancing, Networks.

ÍNDICE DE CONTENIDO

PÁG.

ÍNDICE DE FIGURAS

PÁG.

INDICE DE TABLAS

PÁG.

INTRODUCCIÓN

Es común escuchar la frase “mi empresa es pequeña, quien va a desear mi información”, El tema tratado en el presente proyecto se refiere a la necesidad que tiene la gran mayoría de la pequeña y mediana empresa (PYMES) en nuestro país de contar con una guía práctica que les ayude a determinar los elementos requeridos para asegurar las aplicaciones tecnológicas utilizadas para el crecimiento empresarial.

Las pymes son las que se encuentran más desprotegidas y por ende más fácil de vulnerar por programas dañinos o personas mal intencionadas con los conocimientos informáticos para poner en riesgos la información y la reputación de la empresa.

Internet, denominada también la red o red de redes, se ha convertido en la última década en un fenómeno que ha revolucionado la sociedad. Con el fin de mejorar la productividad y el rendimiento de una organización competitiva, es fundamental evaluar las técnicas actuales y la tecnología disponible para desarrollar sistemas que brinden eficiencia y eficacia de la gestión de la información relevante.

La implementación de sistemas de información en una compañía, brindan la posibilidad de obtener grandes ventajas, incrementar la capacidad de organización de la empresa, y tornar de esta manera los procesos a una verdadera competitividad.

Sin embargo debemos tener en cuenta que todas estas nuevas aplicaciones tecnológicas conectadas a internet presentan amenazas y riesgos de ataques que requieren de mecanismo preventivos para su mitigación. Minimizar los riesgos de ataques informáticos a la infraestructura se logra mediante la estructuración y acoplamiento de dispositivos de seguridad capaces de detectar y prevenir las amenazas en la red.

En el 2014 expertos de Kaspersky Lab, argumentaron que los problemas a los que se enfrentan las empresas no son solo tecnológicos, también tienen su raíz en las políticas y procedimientos implementados por ellas. La cibercriminalidad es, cada vez más, una amenaza que solo podrá

ser mitigada mediante la formación y capacitación adecuada, consiguiendo así un conocimiento transversal de la problemática en todos los niveles de negocio, aprendiendo las tácticas que los atacantes utilizan para obtener la información que desean. (Kaspersky 2014).

Como podemos analizar tener una infraestructura adecuada para mitigar los ataques informáticos requiere de cierta experiencia. Los diseños, implementaciones y adquisiciones de soluciones de seguridad informática puede ser un proceso complejo que requiere de personal experto en el área, sin embargo, si se cuenta con una línea base, una guía adaptable de lo que se debe tener en cuenta a la hora de definir criterios y necesidades para tener una solución de seguridad informática, hace que el proceso sea más sencillo y de fácil socialización.

1. FORMULACIÓN DEL PROBLEMA TÉCNICO

1.1. ANTECEDENTES DEL PROBLEMA.

Un ataque informático consiste en aprovechar alguna debilidad o falla en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; para obtener un beneficio, por lo general de condición económica, causando un efecto negativo en la seguridad del sistema, que luego pasa directamente en los activos de la organización. (Alegsa 2012).

Existen diferentes tipos de ataques informáticos los cuales en diferentes escenarios pueden ocasionar daños irreversibles a los sistemas informáticos de cualquier tipo de organización.

A continuación se detallan algunos de estos ataques y las consecuencias que dejaron a las organizaciones donde se presentaron, lo anterior según información consultado del sitio web gizmodo.com (Zahumenszky, 2014).

El gran *hack* de EE.UU.: 160 millones de usuarios: No tiene nombre oficial porque no afectó a una sola compañía, sino a una larga lista de ellas que incluía el índice bursátil NASDAQ, 7-Eleven, JC. Penney, JetBlue, Dow Jones o Global Payment entre otras. El ataque se prolongó durante siete años desde 2005, y robó los datos de tarjetas bancarias de 160 millones de clientes. Cinco personas de origen ruso fueron acusadas y condenadas por el caso.

1. eBay: 145 millones de usuarios Es el último gran ataque. El asalto a la base de datos de usuarios de la página de comercio online ha obligado a cambiar sus contraseñas a 145 millones de personas. Aún no se ha podido calcular el volumen de la información filtrada.

2. Sony PlayStation Network: El ataque que robó información de las cuentas de 77 millones de usuarios de los servicios PlayStation en todo el mundo supuso un duro golpe para Sony, entre otras cosas porque tardó una semana en reconocer el problema. Tuvo que compensar a los usuarios y recibió varias sanciones en países como Reino Unido.

3. AOL: 92 millones de usuarios: Este ataque comenzó desde dentro en 2004. Un ingeniero de la compañía que había sido despedido utilizó sus conocimientos de la empresa para infiltrarse en la red interna de AOL, y robar la lista con los correos de sus 92 millones de usuarios. Después vendió la lista online a un grupo de *spammers*.

4. Veteranos de EE.UU.: 76 millones de usuarios: Un disco duro que se envió a un servicio técnico en 2009 fue el punto por el que se robaron 76 millones de fichas personales de veteranos de guerra estadounidenses, incluyendo sus números de la seguridad social.

En Colombia los ataques informáticos a diferentes empresas y organizaciones no han pasado desapercibido es así como un informe elaborado por la organización de seguridad informática estadounidense FireEye, identifica que el 98% de las empresas nacionales son objeto de ataques informáticos permanentemente. El informe recoge datos de 1.500 clientes en más de 40 países y concluye que los sectores más atacados son gobierno, servicios y consultoría, alta tecnología y finanzas cuyos datos tanto internos como los relacionados con clientes son puestos en riesgo a través de dos vectores principales: ataques vía web o e-mail.

Colombia es considerada una de las naciones más atractivas para los delincuentes informáticos en América Latina, muestra de ello es que el 25% de los ciberataques registrados en el 2015 se originaron en esta parte del mundo. Así lo explica un reciente informe de Certicámara sobre los principales retos que tendrá que asumir el país en materia de seguridad informática este año, ya que "solo el 10% de los ciudadanos tiene plena confianza en usar los medios electrónicos para sus transacciones diarias". (Certicamara 2015).

La firma especializada en seguridad informática Digiware, por su parte, pronostica que el número de ataques informáticos incrementará en los próximos años en América Latina, afectando en gran medida a sectores como el financiero, telecomunicaciones e incluso al Gobierno.

Los ataques informáticos y las técnicas de los ciberdelincuentes evolucionan conforme se desarrollan nuevas herramientas. En el informe anual realizado por Digiware integrador de

seguridad informática, se reveló que Colombia es el país de habla hispana que genera más ataques informáticos en Latinoamérica.

Andrés Galindo, director de alianzas de Digiware, afirma que los ataques provienen desde una persona común hasta grupos criminales organizados, "con diferentes entidades, especialmente la Dijin, se han detectado grupos criminales que en algunos casos son personas independientes, pero en otros casos financiados hasta por narcotráfico que están buscando otro tipo de negocios rentables". (Caracol 2014).

De acuerdo a Galindo, generar un ataque en la red es un proceso sencillo, "hoy en día atacar es solo querer, hay guías para subcontratar los servicios de ataque y google enseña en línea y uno puede encontrar desde como lanzar un ataque hasta poder adquirir servicios de spam"

Cisco por su parte reveló que las empresas colombianas han mejorado en el último año en sus estrategias de seguridad informática, gracias a la implementación de buenas prácticas para controlar y gestionar el antes, durante y la fase posterior de ataques realizados por cibercriminales, especialmente en sectores donde hay procesos avanzados como retail, banca, defensa y finanzas.

Sin embargo la compañía de soluciones tecnológicas, que recientemente presentó su estudio de Seguridad 2016, agrega que todavía quedan muchos retos para este año, como actualizar las políticas al interior de las organizaciones y renovar infraestructuras obsoletas que se convierten en puntos débiles que cada vez más están aprovechando los delincuentes. (Cisco 2015).

Ante el inminente incremento de ataques, robo de información y fraudes informáticos, que impacta a cualquier negocio u organización y que deja costos superiores a los 1.300 millones de dólares por año en el mundo (en Colombia llega al billón de pesos), los directivos han empezado a hacer parte activa de los problemas y soluciones de seguridad al interior de las organizaciones, señala Luis Garzón, Security Account Manager de Cisco. Según este experto, el compromiso y apoyo de los C-levels para hacer parte de las estrategias se ha dado en gran parte a la 'evangelización' y educación que han liderado las empresas del sector de las

Tecnologías de la Información (TI) para que la seguridad sea prioridad y un verdadero motor de crecimiento para las organizaciones del país.

Una investigación llamada adopción y uso de las Tecnologías de la Información y la comunicaciones TIC en las Pymes colombianas realizado por cisco en alianza con la Asociación Nacional de Micro, Pequeñas y Medianas Empresas (Acopi) revelo que el desconocimiento en tecnología y la falta de financiación son los principales obstáculos a la hora de ejecutar proyectos que permitan tener una infraestructura acorde a los avances informáticos. (Cisco 2015).

1.2. CONTEXTO DONDE SE PRESENTA EL CONFLICTO.

Las Pymes son el foco principal de esta problemática al ser estas las que no cuentan con los presupuestos adecuados para la implementación de soluciones a corto plazo que permita atenuar los riesgos sobre la infraestructura tecnológica, entendiendo que los esquemas de seguridad informática son parte estrategia y fundamental de cualquier tipo organización sin importar su tamaño, sean de carácter público a privada.

1.3. CONFLICTO (NO CONFORMIDAD) QUE DA LUGAR AL DESARROLLO DEL PROYECTO.

La falta de financiación son los principales obstáculos para escoger proyectos que permitan tener una infraestructura acorde a los avances informáticos, además que la mayoría de las Pymes no cuentan con guías o procedimientos formales que les permita contar con un diseño de seguridad adecuado.

La gran cantidad de recursos tecnológicos que ayudan al fortalecimiento empresarial también colocan en riesgo los procesos misionales de las empresas y se convierte en un problema si no se toman las medidas preventivas y proactivas adecuadas.

Los equipos de seguridad TI tradicionales de algunas organizaciones y en algunos casos la falta de compromiso y conocimiento frente a las nuevas amenazas en las redes internas, externas e

internet adecua el camino para que se puedan generar ataques informáticos que pone en riesgo la infraestructura y la información misional de las empresas.
Estas son algunas de las causas que dan lugar al desarrollo de una guía de seguridad perimetral escalable y en alta disponibilidad con equipos de seguridad de nueva generación.

Otras de las motivaciones de este proyecto resultan de la problemática cada vez mayor de ataques e incidencias de seguridad en redes, ya sean a nivel local, a nivel empresarial, u otros tipos de escenarios.

1.4. DESCRIPCIÓN DEL PROBLEMA.

Los riesgos y amenazas a la seguridad informática de las empresas son evidentes. Solo en Colombia, el año pasado se recibieron 7.118 denuncias por parte de víctimas de delitos informáticos, evidenciando un aumento del 40 % con respecto al 2014. Las pérdidas económicas derivadas por estos actos representan al país alrededor del 0,14 % del PIB Nacional. El 43 % de las empresas en el país no poseen planes de respuesta frente a este tipo de incidentes. (Portafolio, 2016).

Una encuesta publicada el 31 de agosto del 2016 por PWC y el Centro de Investigación y Desarrollo en Tecnologías de la Información y las Comunicaciones (CINTEL), revela que solo el 7% de las pymes en Colombia ha solicitado un crédito para invertir en tecnología. (Andicom, 2016)

El 46% de esa porción destinó entre $1 y $10 millones, el 12% entre $11 y $20 millones, mientras que el 6% invirtió más de $100 millones. Los recursos de estas empresas se invierten principalmente en equipos de oficina (34%), páginas web (22%), aplicaciones (18%), servidores (14%), entre otros. Con respecto a las barreras que limitan la adopción de la seguridad de la información en las pymes, el 43% expresó que el mayor obstáculo es la falta de recursos, el 19% no contaba con el personal capacitado, el 18% tiene un bajo conocimiento en ese campo, el 9% no confía en los proveedores, el 6% tuvo malas experiencias con proyectos anteriores, entre otras razones (5%). (Dinero, 2015)

Teniendo en cuenta los indicadores anteriores y la falta de guías de seguridad informática como un componente facilitador a la hora de optimizar recursos tecnológicos para resguardar la información de ataques internos y externos hace que en las Pymes estos procesos sea aún más difícil de implementar.

Los diseños, implementaciones y adquisiciones de soluciones de seguridad informática son un proceso complejo que requiere de personal experto en el área, sin embargo, si se cuenta con una línea base, una guía adaptable de lo que se debe tener en cuenta a la hora de definir criterios y necesidades para tener una solución de seguridad informática, el proceso se hace más sencillo y de fácil socialización.

La falta de mecanismo facilitadores para la estructuración de guías de seguridad ajustado al presupuesto de cada organización hace que estas dejen en segundo plano dentro de los planes de inversión la implementación de soluciones de seguridad Informática poniendo en riesgo la operatividad.

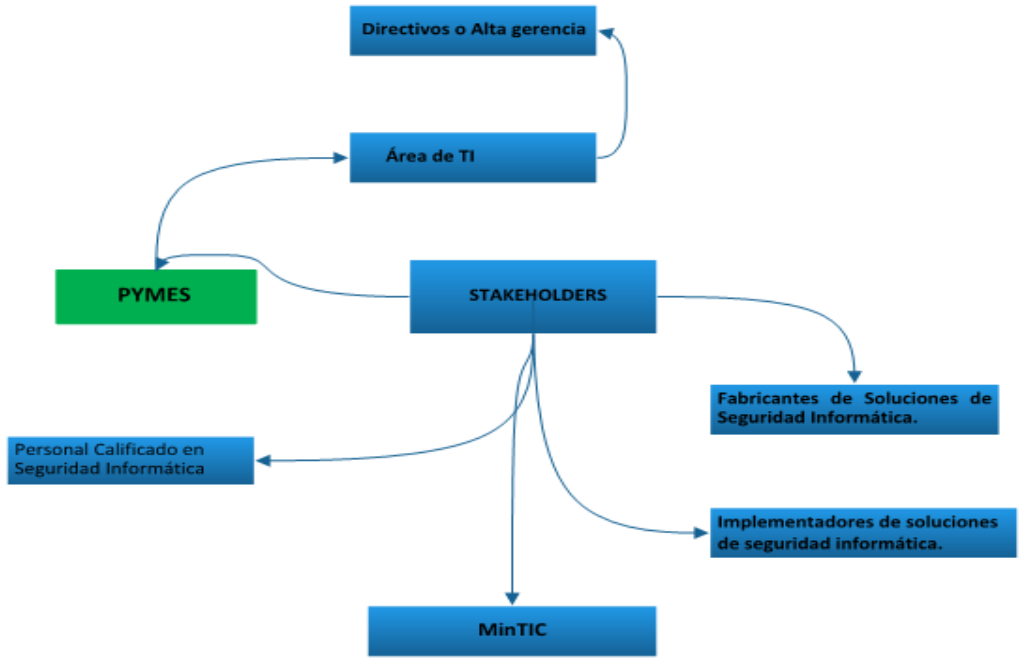
Los cambios radicales que se están produciendo en el uso de las aplicaciones, el comportamiento de los usuarios y la infraestructura de la red dan lugar a un panorama de amenazas que revela los puntos débiles de la seguridad en las organizaciones.

1.5. DEFINICIÓN DEL COMITENTE, SPONSOR DEL PROYECTO.

La persona que ofrece los recursos financieros y en especie para el desarrollo del proyecto es Carlos Mario Benjumea.

1.6. DEFINA LOS STAKEHOLDERS DEL PROYECTO.

Figura 1. Stakeholders del Proyecto.



Fuente: Propia

1.7. ESTABLEZCA LAS POSIBLES MODALIDADES DE SOLUCIÓN DEL PROBLEMA.

Una solución a esta problemática es la de contar con una guía práctica de seguridad informática, dicha guía contempla los aspectos necesarios para articular un sistema de seguridad perimetral escalable y en alta disponibilidad con equipos firewall de nueva generación, teniendo esta guía se da a las pymes la posibilidad de tener un mejor enfoque en la implementación de soluciones de seguridad informática escalables y reducidas en costos.

1.8. ESTABLEZCA LAS CONSTRICCIONES Y RESTRICCIONES DEL PROYECTO QUE USTED VA A GESTIONAR.

A continuación se presentan las constricciones y restricciones del proyecto.

CONSTRICCIONES	RESTRICCIONES
La falta de interés y apoyo de la alta gerencia para el desarrollo de proyectos de seguridad informática.	Es importante para la adaptabilidad de la guía tener apoyo de la alta gerencia que puedan entender la importancia de contar con una línea base a la hora de implementar el esquema de seguridad acorde a la necesidad que se tenga.
La guía se limita a procedimientos de buenas prácticas que se debe tener en cuenta a la hora de tomar decisiones en los procesos de implementación de los sistemas de seguridad.	Al tratarse de una guía práctica esta debe adaptarse a cada tipo de escenario ya que este pude cambiar dependiendo del tamaño y expectativa de cada organización.
No contar con personal altamente calificado para el diseño esquemas de seguridad informática.	Falta de recursos para la adquisición de elementos de seguridad.

2. JUSTIFICACIÓN

El 43% de las empresas en el país no poseen planes de respuesta frente a incidentes de seguridad informática. La falta de conocimientos en tecnología y no contar con guías o procedimientos formales que les permita tener un diseño de seguridad adecuado dificultad la mitigación de estos riesgos.

Una cifra reportada por Cisco frente a ataques cibernéticos revela que, durante el año 2015, Colombia sufrió pérdidas por alrededor de un $1 billón, lo que dejó en evidencia que para las empresas el tema de seguridad informática no es una prioridad y no existen políticas serias frente a esta materia; algo que no es exclusivo del país ya que en el mundo este fenómeno deja pérdidas por alrededor de US$1.300 millones al año. (Dinero, 2015).

Según el ministerio de las TIC (Tecnología de la información y las comunicaciones) las empresas se están vinculando a la estrategia IT para aumentar la capacidad de enfrentar las amenazas informáticas, pues en el momento presentan grandes debilidades, pese a que existen iniciativas gubernamentales, privadas y de la sociedad civil que buscan contrarrestar sus efectos no hay una coordinación interinstitucional apropiada. En 2011 en Colombia hubo más de 550 ataques exitosos a entidades del Estado. (MinTic, 2015).

Según el informe de ESET Security Report Latinoamérica 2016, los ataques de tipo pishing (suplantación de identidad se vuelven cada vez más dirigidos y mejorados y los usuarios en Colombia no tienen una cultura fuerte de seguridad cibernética, es decir que se pronostica un incremento hasta 20% para 2016-2017. (Bdo Colombia, 2016).

La falta de recursos provoca, a veces, que muchas PYMES cuenten con una seguridad insuficiente o no sepan exactamente cuáles son las medidas que tienen que adaptar para estar protegidos. Con frecuencia, el uso de la tecnología de información para la globalización y la reingeniería de procesos empresariales da como resultado el desarrollo de sistemas de información que ayudan a una empresa a darle ventaja competitiva en el mercado, utilizándolos para desarrollar productos, servicios, procesos y capacidades que dan a una empresa una ventaja

estratégica sobre las fuerzas competitivas que enfrenta una empresa.

La multiplicación de prácticas de extorsión, el perfeccionamiento de los ataques por correo electrónico o la pérdida del control de los aparatos conectados a internet serán las mayores amenazas para 2016. Para el Círculo Europeo de Seguridad de Sistemas de Información, que agrupa a las organizaciones del sector, las mayores amenazas son el cibersabotaje y el ciberterrorismo. (El Universal 2015).

Normalmente cuando se habla de ataques informáticos nos enfocamos en gobiernos, en grandes corporaciones o en ataques de denegación de servicio a páginas web. Sin embargo, las Pymes se están convirtiendo en un blanco muy atractivo para los ladrones digitales, que están aprovechando la poca seguridad de estas empresas para adquirir secretos industriales y demorar los planes de la competencia.

La revista ENTER.CO entrevisto a Diego Gómez Sevilla, gerente de territorio para Pymes en la región norte de Latinoamérica de McAfee, para conocer cómo se está comportando este mercado en temas de seguridad. Lo más evidente, según Gómez, es que las empresas no invierten en seguridad sino que reaccionan a un ataque. En otras palabras, las Pymes le echan candado al negocio después de que se metieron los ladrones. Según McAfee, solo el 8% del gasto en IT de las pequeñas y medianas empresas está destinado a la seguridad informática. Teniendo en cuenta que el 73% de las Pymes colombianas sufrieron por lo menos un ataque informático, y que estas compañías mueven el 96% de la economía del país, es preocupante la falta de aseguramiento informático. (Santos s.f.).

La situación de las Pymes es complicada. Obviamente tienen recursos limitados y la seguridad en TI no está entre las prioridades. Sin embargo, las empresas deberían entender que la realidad es diferente. Los piratas informáticos son lo suficientemente inteligentes para saber dónde hay menos resistencia, y por ahí atacan.

Teniendo en cuenta lo anterior, y que no todas las pequeñas y medianas empresas tienen la experiencia necesaria para la gestación de sistema de seguridad informática de nueva

generación, es necesario facilitarles guías prácticas adaptables a cada necesidad que les ayude a tener una línea base para el aseguramiento de sus herramientas tecnológicas, de forma ágil, reduciendo costos y minimizando los riesgos de sufrir ataques informáticos. La gran variedad de aplicaciones que se utilizan en las organizaciones y los diferentes métodos de acceso hace necesario replantearse la forma como se va a garantizar la integridad y confiabilidad de la información misional.

Las áreas de tecnología de la información se han convertido en elementos de apoyo fundamentales a nivel estratégico, táctico y operativo, lo cual indica que las organizaciones dependen cada día más de éstas para alcanzar sus objetivos, generando una necesidad creciente de servicios informáticos que deben contar con equipos de seguridad de nueva generación que estén en capacidad de prevenir y detectar los diferentes tipos de ataques informáticos.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

- Desarrollar una guía práctica que sirva como insumo y permita tener una línea base facilitando la identificación de las necesidades y los recursos informáticos requeridos para asegurar la información de las PYMES utilizando equipos de firewall de última generación.

3.2. OBJETIVOS ESPECIFICOS

- Identificar los diferentes métodos y controles tanto internos como externos para el aseguramiento de la información en las Pymes.
- Determinar los aspectos fundamentales que deben tener en cuenta las pymes a la hora de implementar la seguridad informática.
- Identificar los diferentes fabricantes de firewall UTMs (Gestión Unificada de Amenazas) de última generación y las recomendaciones que estos realizan para la protección de la información en las Pymes.
- Desarrollar y describir los pasos requeridos para el aseguramiento de la información desde la parte física y los aspectos de configuración a nivel lógico en los equipos que hacen parte de la infraestructura.

4. MARCO REFERENCIAL

4.1. MARCO TEÓRICO.

La infraestructura de redes y las aplicaciones web que se utilizan en ellas están expuesta a diferentes tipos de ataques que ponen en riesgo su funcionalidad, detrás de estos ataques se encuentran los hacker.

La cultura informática del MIT parece ser la primera en adoptar el término hacker. los hackers del Club de Modelos de Trenes se convirtieron en el núcleo del Laboratorio de Inteligencia Artificial (IA) del MIT, el centro líder mundial en investigaciones sobre IA a principios delos ‘80. Su influencia se extendió sobre todo a partir de 1969, el primer año de la Agencia de Proyectos de Investigación Avanzada (ARPA).

Figura 2. Hacker

Fuente: http://www.sactop.com/los-hacker.

La red ARPA fue la primera red de computadoras transcontinental de alta velocidad fue creada por el Departamento de Defensa como un experimento sobre comunicaciones digitales, pero fue creciendo hasta conectar a cientos de universidades, laboratorios de investigación e industrias armamentísticas. Permitió a los investigadores de todas partes intercambiar información a una velocidad y flexibilidad sin precedentes, dándole un impulso enorme a los trabajos en colaboración e incrementando tremendamente el ritmo y la intensidad del avance tecnológico. El año del nacimiento de la red ARPA fue también el año en que un hacker de los laboratorios Labs llamado Ken Thompson inventó el sistema operativo UNIX.

Figura 3. Red ARPA

Fuente: https://dianeilyolivo.wordpress.com/2014/03/24/nacimiento-de-a-r-p-a-1958/

Los hackers podrían llevar consigo sus herramientas entre diferentes máquinas, en lugar de tener que reinventar el fuego y la rueda en cada ocasión. Además de la portabilidad, Unix y C tenían otros aspectos ventajosos. Un programador podía manejar en la cabeza toda la estructura lógica del C (a diferencia de la mayoría de los lenguajes anteriores) en vez de tener que consultar los manuales todo el tiempo; y UNIX se estructuraba como un kit de programas simples diseñados para combinarse entre sí de maneras productivas. (Gradin 2014).

A lo largo del tiempo, el avance de los medios tecnológicos y de comunicación ha provocado el surgimiento de nuevos vectores de ataques y de nuevas modalidades delictivas que han transformado a Internet y las tecnologías informáticas en aspectos sumamente hostiles para cualquier tipo de organización, y persona, que tenga equipos conectados a la World Wide Web.

Cada día se descubren nuevos puntos débiles y por lo general son pocos los responsables de IT que comprenden en su justa medida la importancia que tiene la seguridad y cómo pueden abordar el grave problema que existe detrás de vulnerabilidades que permiten a un atacante, violar la seguridad de un entorno y cometer delitos en función de los datos robados. Bajo esta escenografía donde los principales actores son las organizaciones de cualquier magnitud y rubro, los sistemas de información, el dinero y delincuentes informáticos; se torna realmente necesario y fundamental idear estrategias de seguridad que permitan establecer barreras defensivas orientadas a mitigar efectivamente ataques tanto externos como internos. Pero para lograr mitigar de manera eficaz el impacto provocado por los ataques informáticos, es

importante conocer de qué manera atacan y cuáles son los puntos débiles de un sistema comúnmente explotado en los que se deben enfocar los esfuerzos de seguridad tendientes a la prevención de los mismos.

Comprender cuáles son las debilidades más comunes que pueden ser aprovechadas y cuáles son sus riesgos asociados, permitirá conocer de qué manera se ataca un sistema informático ayudando a identificar las debilidades y riesgos para luego desplegar de manera inteligente estrategias de seguridad efectivas. (Mieres 2010).

Cuando analizamos fallos de seguridad en las pequeñas empresas, solemos encontrar que hay errores que suelen repetirse en muchos negocios. Estos suelen ser la causa de mayor número de incidencias informáticas en la empresa y consecuencia de una mala previsión en el departamento de informática, si lo hay.

Hay empresarios que piensan que los hackers sólo se dedican a tratar de buscar agujeros de seguridad en los servidores y sistemas de grandes multinacionales. Pero no suele ser así. De hecho, las Pymes suelen ser más vulnerables porque invierten menos en la seguridad de su negocio y suele ser más fácil perjudicarlas, aunque no salga en los periódicos.

Las empresas deben mantener el máximo de confidencialidad a nivel interno. Una cláusula que debe integrarse en los contratos, siempre que se trabaja con personal externo a la empresa, pero también con empleados, es la confidencialidad.

Regularmente la infraestructura de red de las Pymes contiene componentes o elementos básicos, por un lado tenemos los dispositivos o elementos físicos de la red como son los computadores, router, puntos de acceso, estos se interconectan mediante un componente físico o inalámbrico en algunos casos. Los componentes de red se utilizan para proporcionar servicios y procesos, que son los programas de comunicación, denominados “software”, que se ejecutan en los dispositivos conectados en red.

Un servicio de red proporciona información en respuesta a una solicitud. Los servicios incluyen

muchas de las aplicaciones de red comunes que utilizan las personas a diario, como los servicios de hosting de correo electrónico y web hosting. Los procesos proporcionan la funcionalidad que direcciona y traslada mensajes a través de la red. Los procesos son menos obvios para nosotros, pero son críticos para el funcionamiento de las redes.

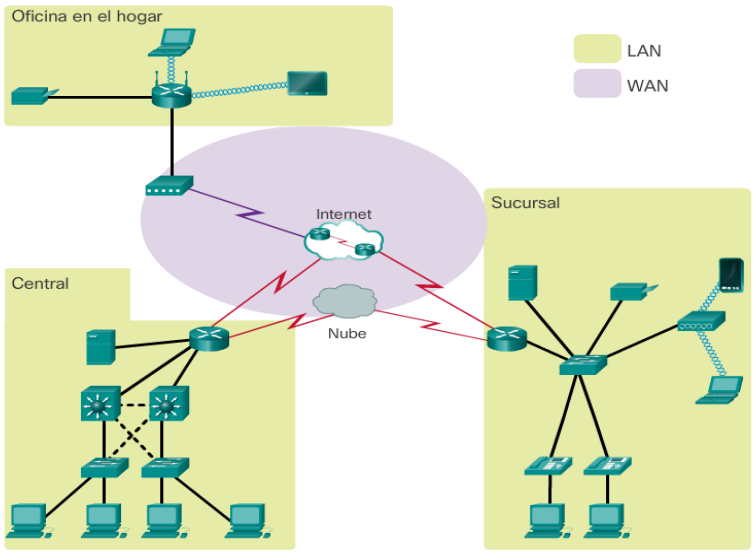
Los usuarios que utilizan los recursos o servicios informáticos lo hacen mediante dispositivos finales tales como Computadoras (estaciones de trabajo, computadoras portátiles, servidores de archivos, servidores web, dispositivos portátiles móviles como smartphones, tablet PC, PDA.

Dentro de la infraestructura tecnológica podemos encontrar diferentes tipos de redes, cisco define dos redes básicas, las redes de área local y las redes de área extensa. Las redes de área local (LAN, Local Area Networks) son infraestructuras de red que abarcan un área geográfica pequeña. Las características específicas de las LAN incluyen lo siguiente: Las LAN interconectan dispositivos finales en un área limitada, como una casa, un lugar de estudios, un edificio de oficinas o un campus. Por lo general, la administración de las LAN está a cargo de una única organización o persona.

El control administrativo que rige las políticas de seguridad y control de acceso está implementado en el nivel de red. Las LAN proporcionan un ancho de banda de alta velocidad a los dispositivos finales internos y a los dispositivos intermediarios.

Las redes de área extensa (WAN, Wide Area Networks) son infraestructuras de red que abarcan un área geográfica extensa. Normalmente, la administración de las WAN está a cargo de proveedores de servicios (SP) o proveedores de servicios de Internet (ISP). Las características específicas de las WAN incluyen lo siguiente: Las WAN interconectan LAN a través de áreas geográficas extensas, por ejemplo, entre ciudades, estados, provincias, países o continentes. Por lo general, la administración de las WAN está a cargo de varios proveedores de servicios. Normalmente, las WAN proporcionan enlaces de velocidad más lenta entre redes LAN. (Cisco 2015).

Figura 4. Redes Lan y Wan



Fuente: https://static-course-assets.s3.amazonaws.com/ITN51/es/index.html#1.2.2.1

La mayor parte de los servicios o aplicaciones que consumen las Pymes son del tipo cliente servidor y aplicaciones web.

Las aplicaciones Web son populares debido a lo práctico de usar un navegador Web como cliente ligero. La facilidad para actualizar y mantener aplicaciones Web sin distribuir e instalar software a miles de usuarios potenciales es una razón de peso para su popularidad.

En ingeniería de software una aplicación Web es una "aplicación a la cual se tiene acceso vía un navegador Web sobre una red, como Internet o una intranet. Además, es una aplicación de software codificada en un lenguaje soportado por un browser o navegador Web como HTML, JavaScript, Java, en la que se confía la ejecución al navegador. (Pc Magazine 2014).

Es importante mencionar que una página Web puede contener elementos que permiten una comunicación activa entre el usuario y la información. Esto permite que el usuario acceda a los datos de modo interactivo, gracias a que la página responde a cada una de sus acciones, como por ejemplo; rellenar y enviar formularios, participar en juegos diversos y acceder a gestores de base de datos de todo tipo.

Figura 5. Consulta Web.

Fuente: https://static-course-assets.s3.amazonaws.com/ITN51/es/index.html#10.2.1.2

Un recurso importante para el intercambio de información en línea en cualquier tipo de empresas es internet. Este recurso muchas veces en las Pymes no tiene asociado un dispositivo que deniegue cierto tipo de transacciones que pueden comprometer la infraestructura de red.

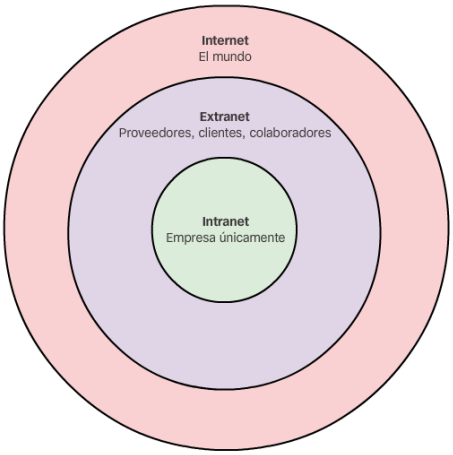
Como toda gran revolución, internet augura una nueva era de diferentes métodos de resolución de problemas. Internet produce algo que todos han sentido alguna vez; produce la esperanza que es necesaria cuando se quiere conseguir algo. Es un despertar de intenciones que jamás antes la tecnología había logrado en la población mundial. Para algunos usuarios, Internet genera una sensación de cercanía, empatía, comprensión y, a la vez, de confusión, discusión, lucha y conflictos que los mismos usuarios pueden considerar como la vida misma.

Para el intercambio de información en las aplicaciones internas las pequeñas y medianas empresas hacen uso de la intranet.

El término intranet se suele utilizar para hacer referencia a una conexión privada de redes LAN y WAN que pertenece a una organización y que está diseñada para que solo accedan a ella los miembros y los empleados de la organización u otras personas autorizadas. Básicamente, las intranets son internets a la que solamente se puede acceder desde dentro de la organización. Las

organizaciones pueden publicar en una intranet páginas Web sobre eventos internos, políticas de higiene y seguridad, boletines de personal y directorios telefónicos del personal. Por ejemplo, los lugares de estudios pueden tener intranets que incluyan información sobre los programas de clases, currículos en línea y foros de discusión. Generalmente, las intranets ayudan a eliminar el papeleo y aceleran los flujos de trabajo. El personal que trabaja fuera de la organización puede tener acceso a la intranet mediante conexiones seguras a la red interna. (Cisco 2015).

Figura 6. Intranet, Extranet



Fuente: https://static-course-assets.s3.amazonaws.com/ITN51/es/index.html#1.2.3.2

Es posible que una organización utilice una extranet para proporcionar acceso seguro a las personas que trabajan para otra organización, pero requieren datos de la compañía.

Internet ha evolucionado y ha pasado de ser una internetwork de organizaciones educativas y gubernamentales fuertemente controlada a ser un medio accesible para todos para la transmisión de comunicaciones comerciales y personales. Como resultado, cambiaron los requerimientos de seguridad de la red. La infraestructura de red, los servicios y los datos contenidos en los dispositivos conectados a la red son activos comerciales y personales muy importantes. Existen dos tipos de problemas de seguridad de red que se deben tratar: la seguridad de la infraestructura de red y la seguridad de la información.

La seguridad de una infraestructura de red incluye el aseguramiento físico de los dispositivos

que proporcionan conectividad de red y prevenir el acceso no autorizado al software de administración que reside en ellos.

La seguridad de la información se refiere a proteger la información que contienen los paquetes que se transmiten por la red y la información almacenada en los dispositivos conectados a la red. Para alcanzar los objetivos de seguridad de red, hay tres requisitos fundamentales:

Asegurar la confidencialidad: la confidencialidad de los datos se refiere a que solamente los destinatarios deseados y autorizados (personas, procesos o dispositivos) pueden acceder a los datos y leerlos. Esto se logra mediante la implementación de un sistema sólido de autenticación de usuarios, el establecimiento de contraseñas que sean difíciles de adivinar y la solicitud a los usuarios de que las cambien con frecuencia. La encriptación de datos con el fin de que solamente el destinatario deseado pueda leerlos también forma parte de la confidencialidad.

Mantener la integridad de la comunicación: la integridad de los datos se relaciona con tener la seguridad de que la información no se alteró durante la transmisión desde el origen hasta el destino. La integridad de los datos se puede poner en riesgo si se daña la información, ya sea voluntaria o accidentalmente. Se puede asegurar la integridad de los datos mediante la solicitud de validación del emisor así como por medio del uso de mecanismos para validar que el paquete no se modificó durante la transmisión.

Asegurar la disponibilidad: la disponibilidad se relaciona con tener la seguridad de que los usuarios autorizados contarán con acceso a los servicios de datos en forma confiable y oportuna. Los dispositivos de firewall de red, junto con el software antivirus de los equipos de escritorio y de los servidores pueden asegurar la confiabilidad y la solidez del sistema para detectar, repeler y resolver esos ataques. Crear infraestructuras de red totalmente redundantes, con pocos puntos de error únicos, puede reducir el impacto de estas amenazas.

Figura 7. Seguridad de la Red

Fuente: https://static-course-assets.s3.amazonaws.com/ITN503/es/index.html#1.3.2.6

Figura 8. Seguridad de la Red

Fuente: http://www.uprm.edu/cde/public_main/slider/files_slider/presentaciones_foro/seguridad_informatica.pdf

Si se pone en peligro la integridad de esos recursos, esto podría traer consecuencias graves, como las siguientes:

- Incidentes de la red que impidan la comunicación y la realización de transacciones, lo que puede provocar pérdidas de negocios.
- Robo de propiedad intelectual (ideas de investigación, patentes y diseños) y uso por parte de la competencia.
- Información personal o privada que se pone en riesgo o se hace pública sin el consentimiento de los usuarios.

- Mala orientación y pérdida de recursos personales y comerciales.
- Pérdida de datos importantes cuyo reemplazo requiere un gran trabajo o que son irreemplazables.

Para ayudar a mitigar los incidentes y las consecuencias anteriormente mencionadas existen estándares como ITIL el cual se ha convertido en el estándar mundial en la Gestión de Servicios Informáticos, la estructura base ha demostrado ser útil para las organizaciones en todos los sectores a través de su adopción por innumerables compañías como base para consulta, educación y soporte de herramientas de software. Hoy, ITIL es conocido y utilizado mundialmente. (Megazcitum, 2010).

En ITIL se establece que la correcta gestión de la seguridad no es responsabilidad exclusiva de expertos en seguridad que desconocen los otros procesos de negocio. Si caemos en la tentación de establecer la seguridad como una prioridad en sí misma limitaremos las oportunidades de negocio que nos ofrece el flujo de información entre los diferentes agentes implicados y la apertura de nuevas redes y canales de comunicación. (Itil, 2013).

Los principales beneficios de una correcta Gestión de la Seguridad son:

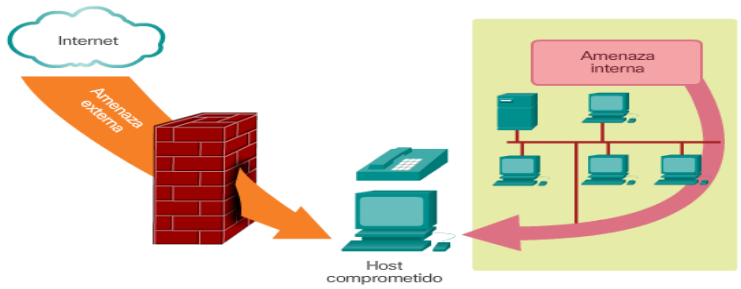
- Se evitan interrupciones del servicio causadas por virus, ataques informáticos, etcétera.
- Se minimiza el número de incidentes.
- Se tiene acceso a la información cuando se necesita y se preserva la integridad de los datos.
- Se preserva la confidencialidad de los datos y la privacidad de clientes y usuarios.
- Se cumplen los reglamentos sobre protección de datos.
- Mejora la percepción y confianza de clientes y usuarios en lo que respecta a la calidad del servicio.

Las principales dificultades a la hora de implementar la Gestión de la Seguridad se resumen en:

- No existe el suficiente compromiso de todos los miembros de la organización TI con el proceso.
- Se establecen políticas de seguridad excesivamente restrictivas que afectan negativamente al negocio.
- No se dispone de las herramientas necesarias para monitorizar y garantizar la seguridad del servicio (firewalls, antivirus).
- El personal no recibe una formación adecuada para la aplicación de los protocolos de seguridad.
- Falta de coordinación entre los diferentes procesos lo que impide una correcta evaluación de los riesgos.

4.2. MARCO CONCEPTUAL.

Figura 9. Tipos de Amenazas en la Red.



Fuente: https://static-course-assets.s3.amazonaws.com/ITN503/es/index.html#1.3.2.6

La seguridad de redes es una parte integral de las redes de computadoras, independientemente de si la red está limitada a un entorno doméstico con una única conexión a Internet o si es tan extensa como una empresa con miles de usuarios. La seguridad de red implementada debe tomar en cuenta el entorno, así como las herramientas y los requisitos de la red. Debe poder proteger los datos y, al mismo tiempo, mantener la calidad de servicio que se espera de la red. La protección de la red incluye protocolos, tecnologías, dispositivos, herramientas y técnicas para proteger los datos y mitigar amenazas. En la actualidad, muchas amenazas de seguridad de red externas se expanden por internet. Las amenazas externas más comunes a las redes

incluyen las siguientes:

Virus, gusanos y caballos de Troya: se trata de softwares malintencionados y códigos arbitrarios que se ejecutan en un dispositivo de usuario.

spyware y adware: software instalado en un dispositivo de usuario que recopila información sobre el usuario de forma secreta.

Ataques de día cero, también llamados "ataques de hora cero": ataque que ocurre el mismo día en que se hace pública una vulnerabilidad.

Ataques de piratas informáticos: ataque de una persona experta a los dispositivos de usuario o recursos de red.

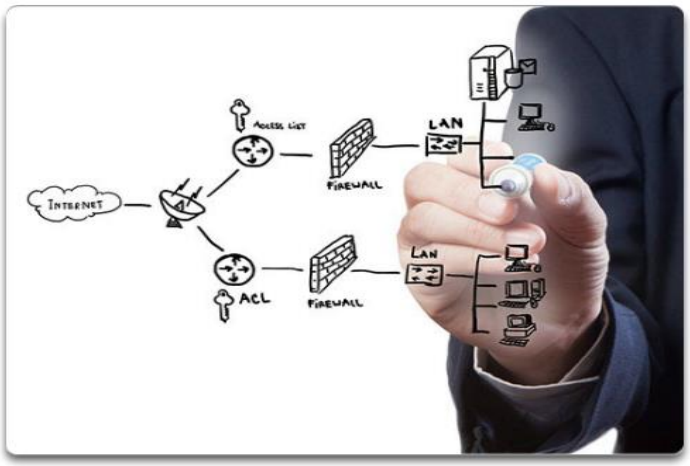
Ataques por denegación de servicio: ataques diseñados para reducir o para bloquear aplicaciones y procesos en un dispositivo de red.

Interceptación y robo de datos: ataque para capturar información privada en la red de una organización.

Robo de identidad: ataque para robar las credenciales de inicio de sesión de un usuario a fin de acceder a datos privados.

También es importante tener en cuenta las amenazas internas. Se llevaron a cabo numerosos estudios que muestran que las infracciones de seguridad de datos más comunes suceden a causa de los usuarios internos de la red. Esto se puede atribuir a dispositivos perdidos o robados o al mal uso accidental por parte de los empleados, y dentro del entorno empresarial, incluso a empleados malintencionados. Con las estrategias de BYOD en desarrollo, los datos corporativos son mucho más vulnerables. Por lo tanto, cuando se desarrolla una política de seguridad, es importante abordar tanto las amenazas de seguridad externas como las internas.

Figura 10. Soluciones de Seguridad



Fuente: https://static-course-assets.s3.amazonaws.com/ITN503/es/index.html#1.3.2.6

No hay una solución única que pueda proteger una red contra la variedad de amenazas que existen. Por este motivo, la seguridad debe implementarse en varias capas, y debe utilizarse más de una solución de seguridad. Si un componente de seguridad no puede identificar ni proteger la red, hay otros que pueden hacerlo. La implementación de seguridad en redes domésticas generalmente es muy básica. Por lo general, se implementa en los dispositivos host de conexión así como en el punto de conexión a Internet e incluso puede depender de servicios contratados al ISP. Por otra parte, la implementación de seguridad de red en redes corporativas normalmente consiste en la integración de numerosos componentes a la red para controlar y filtrar el tráfico. Lo ideal es que todos los componentes funcionen juntos, lo que minimiza la necesidad de mantenimiento y aumenta la seguridad. Los componentes de seguridad de red para redes domésticas o de oficinas pequeñas deben incluir, como mínimo, lo siguiente:

Software antivirus y antispyware: para proteger los dispositivos de usuario contra software malintencionado.

Filtrado de firewall: para bloquear accesos no autorizados a la red. Esto puede incluir un sistema de firewall basado en host que se implemente para impedir el acceso no autorizado al dispositivo host o un servicio de filtrado básico en el router doméstico para impedir el acceso no autorizado del mundo exterior a la red.

Además de lo anterior, las redes más grandes y las redes corporativas generalmente tienen otros requisitos de seguridad:

Sistemas de firewall dedicados: para proporcionar capacidades de firewall más avanzadas que puedan filtrar una gran cantidad de tráfico con mayor granularidad.

Listas de control de acceso: las listas de control de acceso (ACL, Access control list) filtran el acceso y el reenvío de tráfico.

Sistemas de prevención de intrusión: los sistemas de prevención de intrusión (IPS) identifican amenazas de rápida expansión, como ataques de día cero o de hora cero

Redes privadas virtuales: las redes privadas virtuales (VPN, Virtual private networks) proporcionan un acceso seguro a los trabajadores remotos.
Los requisitos de seguridad de la red deben tomar en cuenta el entorno de red, así como las diversas aplicaciones y los requisitos informáticos. Tanto los entornos domésticos como las empresas deben poder proteger sus datos y, al mismo tiempo, mantener la calidad de servicio que se espera de cada tecnología. Además, la solución de seguridad implementada debe poder adaptarse a las crecientes tendencias de red, en constante cambio.

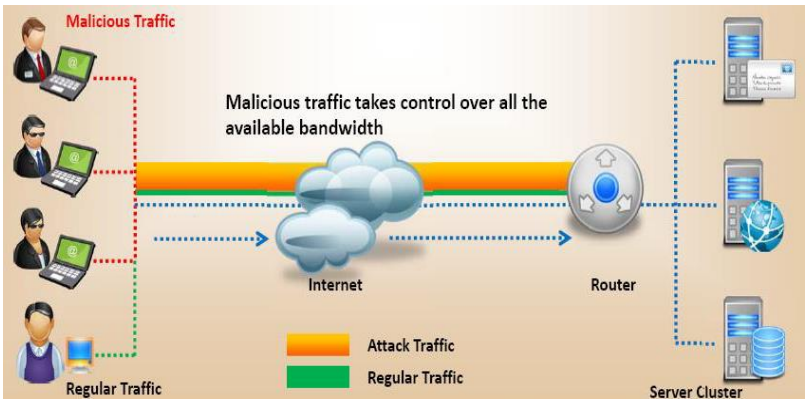
El estudio de las amenazas de seguridad de red y de las técnicas de mitigación comienza con una comprensión clara de la infraestructura de conmutación y enrutamiento subyacente utilizada para organizar los servicios de red. A continuación se presentan diferentes tipos de ataques.

Denegación de Servicio: El objetivo del ataque de denegación de servicios también conocido como ataque DoS (Denial of Service), es interrumpir el funcionamiento normal de un servicio y por lo tanto este se vuelve inaccesible para los usuarios legítimos del sistema o de la red. Este tipo de ataque se efectúa mediante la saturación de los puertos con flujo de información, lo cual

provoca que el servidor se sobrecargue y debido a esto ya no pueda continuar dado servicios. Por lo general, las denegaciones de servicio se dividen de la siguiente manera:

- Explotación de las debilidades del protocolo TCP/IP
- Explotación de las vulnerabilidades del software del servidor

Figura 11. Ataque Denegación de Servicio



Fuente:https://www.google.com.co/search?q=ataques+de+denegación+de+servicio

Intrusiones: Elevación de Privilegios: Este tipo de ataque consiste en aprovechar una vulnerabilidad en una aplicación al enviar una solicitud específica (no planeada por su diseñador). En ciertos casos esto genera comportamientos atípicos que permiten acceder al sistema con derechos de aplicación. Los ataques de desbordamiento de la memoria intermedia (búfer) usan este principio. (Owasp s.f.).

Code Injection: La inyección de código o code injection en ingles hace uso de los errores al procesar información errónea, esto puede ser usado por un atacante al introducir condigo en un programa para cambiar la ejecución normal; incluso esta vulnerabilidad en algunos programas puede ser usada para la propagación de gusanos informáticos. (Kioskea 2014)

Tipos de Inyeccion de Datos: La inyección de datos es común entre los individuos que gustan por atacar las páginas Web, generalmente usan esta técnica para obtener otra información que les ayude a atacar en mayor grado los sistemas. Algunos de los tipos de inyección de datos

buscan modificar los datos de la base de datos, este tipo de inyección se llama SQL Injection. El impacto de este tipo de inyección puede ser desde atacar el sistema Web hasta la perdida de información sensible a la empresa.

Remote Code-Inclusion: De acuerdo al portal de seguridad HoneyNet, Remote Code Inclusion "es un ataque, que explota algún agujero de seguridad en la interfaz Web de una aplicación y con ello logran un ataque del sistema operativo subyacente, y la ejecución de código arbitrario. (Kioskea 2014).

Sql Injection: La definición de SQL (Structured Query Language) es un lenguaje de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en éstas como consultas, modificaciones, inserciones eliminaciones de datos. La inyección de SQL consiste en insertar código SQL invasor dentro de otra sentencia SQL con la finalidad de alterar su funcionamiento normal y hacer que se ejecute el código invasor dentro de la base de datos. La inyección de SQL es comúnmente un problema de programación ya que consiste en ejecutar una sentencia concatenando parámetros que se reciben de lado del cliente. La solución principal es el uso de bindings.

Cross-Site Scripting: El Cross-Site scripting conocido también como XSS "HTML Injection" es un tipo de inseguridad informática que consiste en realizar una serie de ataques por secuencia de comando entre aplicaciones Web, esto es ejecutar código scripting como VBScript o JavaScript. La definición que se propone en el artículo "Cross Site Scripting" el Instituto de Seguridad de Internet menciona que "es una vulnerabilidad que afecta no tanto a los servidores como a los usuarios que navegan a páginas de Internet. La causa de la vulnerabilidad radica en la pobre verificación por parte de los sitios Web de las cadenas de entrada enviadas por los usuarios a través de formularios, o directamente a través del URL.

Estas cadenas, en el caso de ser maliciosas, podrían llegar a contener scripts completos. Cuando esta entrada se le muestra dinámicamente a un usuario dentro de una página Web, en caso de contener un script, éste se ejecuta en el navegador del usuario dentro del contexto de seguridad de la página Web visitada. Como consecuencia en el ordenador del usuario se realizan todas las

acciones que le sean permitidas a ese sitio Web, como por ejemplo interceptar entradas del usuario víctima o leer sus cookies.” En el mismo artículo se explica que el funcionamiento este tipo de ataque comienza en cuanto el usuario ingresa a alguna aplicación solicitando para esto un usuario y password, entonces la aplicación realiza una supuesta “validación”, y se redirecciona a una página HTML la cual incluye el código por parte del atacante, una vez que se ejecutó el código este tiene los mismo privilegios de cualquier otro código legitimo en el mismo sitio Web.

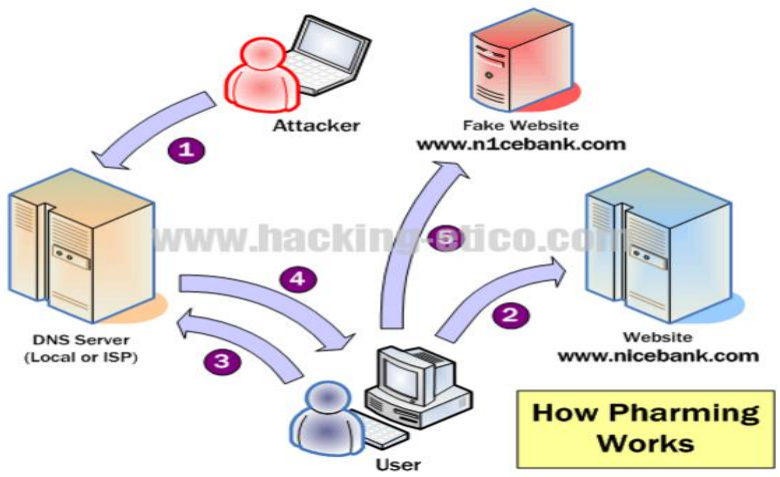
En el libro Seth Fogie, Cross Site Scripting Attacks: Xss Exploits and Defense. 2007 se mencionan dos tipos de vulnerabilidad que pueden presentar:

Directa (Persistente): Este tipo de ataque es poco común y su forma de actuar es identificando los puntos débiles dentro de la programación y de esta forma realizar inserciones de tags como pueden ser <iframe>, o <script>.

Indirecta (Reflejada): Esta es un tipo de vulnerabilidad muy común, consiste en modificar valores que la aplicación Web utiliza para pasar variables entre dos páginas, sin usar sesiones y sucede cuando hay un mensaje o una ruta en la URL del navegador o en una cookie.

Web Spoofing: En el departamento de ciencias de la Computación de la Universidad de Princeton en el año de 1996 se publicó el artículo “Web Spoofing: and Internet Game” en el cual se menciona que el Spoofing es un ataque que consiste en la suplantación de identidad y el cual consiste en la creación de tramas TCP/IP utilizando una dirección falseada, para poder llevar a cabo este ataque es necesario contar con tres; el atacante, atacado y un sistema suplantado.” La idea de este ataque al menos la idea es muy sencilla: desde su equipo, un pirata simula la identidad de otra máquina de la red para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del Host suplantado. El ataque antes mencionado es quizás el más conocido, IP Spoofing, pero existen diferentes tipos de ataques dependiendo de la tecnología a la que se refiera, por ejemplo existe el DNS Spoofing, ARP Spoofing, Web Spoofing.

Figura 12. DNS Spoofin



Fuente: http://hacking-etico.com/2010/08/26/hablemos-de-spoofing/

Dns Spoofing: En el libro de seguridad en UNIX y redes se hace mención a este tipo de ataque, consiste en el falseamiento de "Nombre de dominio-IP", esto se puede conseguir de diferentes formas, "desde modificando las entradas del servidor encargado de resolver una cierta petición para falsear las relaciones nombre-dirección, hasta comprometiendo un servidor que infecte la caché de otro. (Huerta 2012).

Teniendo en cuenta las definiciones anteriores y la forma como los diferentes tipos de ataques informáticos han ido evolucionando, se hace necesario implementar soluciones a nivel de seguridad que estén en la capacidad de controlar estas nuevas amenazas, acá juega un papel importantes los equipos firewall de nueva generación,

Los firewalls de nueva generación, Next-Generation Firewall (NGFW), surgieron para revolucionar la seguridad de la red tal y como la conocíamos hasta ahora. Los firewalls tradicionales se limitan a la inspección de paquetes por estado y a reglas de control de acceso, pero a medida que los hackers se hacen más sofisticados, las amenazas son más avanzadas y este sistema ha dejado de ser eficaz. Con el fin de proteger un negocio de amenazas en constante

evolución, el Firewall de Nueva Generación debe ser capaz de ofrecer un nivel más profundo de seguridad de red. (López 2014).

Un NGFW en esencia es un dispositivo cuya función es gestionar la seguridad entre redes LAN permitiendo o denegando las conexiones, pero va más allá con funcionalidades avanzadas que se pueden activar o desactivar de forma modular, tales como:

- Detección de Intrusos (IPS).
- Prevención de Intrusos (IDS).
- Control de Aplicaciones.
- Prevención de pérdida de datos (DLP)
- Autenticación de Usuarios.
- Concentrador VPN.
- Antivirus.
- Filtrado Web.

Requisitos clave que deben cumplir los firewalls de nueva generación. (PaloAlto 2011).

- Identificación de aplicaciones, no de puertos. Identificación de las aplicaciones, independientemente del protocolo, la codificación o la táctica evasiva y uso de la identidad como base para todas las políticas de seguridad.

- Identificación de usuarios y no de direcciones IP. Aprovechar la información de usuarios y grupos almacenada en los directorios de empresa para la visibilidad, creación de políticas, generación de informes e investigación forense, con independencia de dónde se encuentre el usuario.

- Bloqueo de las amenazas en tiempo real. Protección del ciclo de vida completo frente a ataques, incluyendo aplicaciones peligrosas, vulnerabilidades, software malicioso, URL de alto riesgo y una amplia gama de archivos y contenidos maliciosos.

- Simplificar la gestión de políticas. Habilitación segura de las aplicaciones con herramientas gráficas fáciles de usar y un editor de políticas unificado.

- Habilitación de un perímetro lógico. Garantizar a todos los usuarios, incluidos los que viajan y los teletrabajadores, una seguridad constante que se extienda del perímetro físico al perímetro lógico.

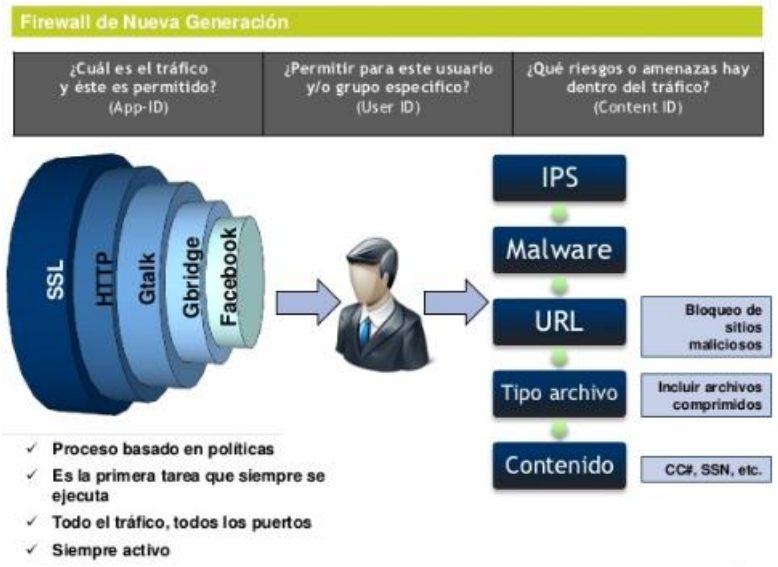
- Proporcionar un rendimiento multi-gigabit. Combinar hardware y software creados especialmente para permitir un rendimiento multi-gigabit de baja latencia con todos los servicios activados.

Los recientes cambios en el comportamiento de las aplicaciones y en los patrones de uso han ido mermando de manera continua la protección que antes proporcionaba el firewall tradicional. Los usuarios acceden a cualquier aplicación, desde cualquier ubicación, en muchas ocasiones, para hacer su trabajo. Muchas de estas aplicaciones utilizan puertos no estándar, puertos intermedios, o utilizan codificación para simplificar y facilitar el acceso del usuario y evitar el firewall. Los ciberdelincuentes aprovechan al máximo este uso sin restricciones de las aplicaciones para difundir una nueva clase de moderno software malicioso con objetivos muy específicos. El resultado es que el firewall tradicional, que se apoyaba en puertos y protocolos, ya no puede identificar ni controlar las aplicaciones y las amenazas que circulan por la red.

Figura 13. Características Firewall de Nueva Generación

Fuente: http://domotes.com/nueva-generacion-de-firewall/

Figura 14. Firewall de Nueva Generación



Fuente: http://es.slideshare.net/GrupoSmartekhAdmin/webinar-firewall-de-nueva-generacin

Los firewall de nueva generación son indispensables para tener una arquitectura de red segura sin embargo deben estar complementados con técnicas de segmentación dentro de la red LAN además de un conjunto de buenas prácticas aplicables. En este sentido es importante mencionar las Vlan o redes LAN Virtuales al igual que La Biblioteca de Infraestructura de Tecnologías de Información (o ITIL, por sus siglas en inglés).

Una VLAN crea un dominio de difusión lógico que puede abarcar varios segmentos LAN físicos. Las VLAN mejoran el rendimiento de la red mediante la división de grandes dominios de difusión en otros más pequeños. Si un dispositivo en una VLAN envía una trama de Ethernet de difusión, todos los dispositivos en la VLAN reciben la trama, pero los dispositivos en otras VLAN no la reciben. Las VLAN habilitan la implementación de las políticas de acceso y de seguridad según grupos específicos de usuarios. Cada puerto de switch se puede asignar a una sola VLAN (a excepción de un puerto conectado a un teléfono IP o a otro switch). (Cisco 2014).

4.3. MARCO LEGAL.

La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos, la protección de la información y de los datos con penas de prisión de hasta 120 meses con multas de hasta 1500 salarios mínimos legales mensuales vigentes. El Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado, denominado de la Protección de la información y de los datos, y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”. En esta ley se tipifica como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que las organizaciones deben blindarse jurídicamente para evitar incurrir en alguno de estos delitos. (UNAD 2013).

En dicha ley se recuerda los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios, transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, como conductas penalizadas y cada vez más usuales en todas partes del mundo.

La importancia de esta ley es que adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos" que divide en dos capítulos, el “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y el “De los atentados informáticos y otras infracciones”.

El capítulo primero adiciona el siguiente articulado:

- **Artículo 269A - Acceso Abusivo a un Sistema Informático:** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269B – Obstaculización Ilegítima de Ssistema Informático o Red de Telecomunicación:** El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

- **Artículo 269C – Interceptación de datos Informáticos:** El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

- **Artículo 269D – Daño Informático:** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269E – Uso de Software Malicioso:** El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del

territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269F – Violación de Datos Personales:** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269G – Suplantación de Sitios Web para Capturar datos Personales:** El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

Es primordial mencionar que este artículo tipifica lo que comúnmente se denomina “phishing”, modalidad de estafa que usualmente utiliza como medio el correo electrónico pero que cada vez con más frecuencia utilizan otros medios de propagación como por ejemplo la mensajería instantánea o las redes sociales.

Un punto importante a considerar es que el Artículo 269H agrega como circunstancias de agravación punitiva de los tipos penales descritos anteriormente el aumento de la pena de la mitad a las tres cuartas partes si la conducta se cometiere:

Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

- Por servidor público en ejercicio de sus funciones aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
- Revelando o dando a conocer el contenido de la información en perjuicio de otro. Obteniendo provecho para sí o para un tercero.
- Con fines terroristas o generando riesgo para la seguridad o defensa nacional. Utilizando como instrumento a un tercero de buena fe.
- Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Es de anotar que estos tipos penales obligan tanto a empresas como a personas naturales a prestar especial atención al tratamiento de equipos informáticos así como al tratamiento de los datos personales más teniendo en cuenta la circunstancia de agravación del inciso 3 del artículo 269H que señala "por quien tuviere un vínculo contractual con el poseedor de la información".

Por lo tanto, se hace necesario tener unas condiciones de contratación, tanto con empleados como con contratistas, claras y precisas para evitar incurrir en la tipificación penal. (Informatica Juridica 2015).

La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.
Así mismo, la Ley 1273 agrega como circunstancia de mayor punibilidad en el artículo 58 del Código Penal el hecho de realizar las conductas punibles utilizando medios informáticos, electrónicos ó telemáticos.

Como se puede apreciar, la Ley 1273 es un paso importante en la lucha contra los delitos informáticos en Colombia, por lo que es necesario que se esté preparado legalmente para enfrentar los retos que plantea. La nueva ley pone de presente la necesidad para los empleadores

de crear mecanismos idóneos para la protección del activo más valioso como lo es la información.

Las empresas deben aprovechar la expedición de esta ley para adecuar sus contratos de trabajo, establecer deberes y sanciones a los trabajadores en los reglamentos internos de trabajo, celebrar acuerdos de confidencialidad con los mismos y crear puestos de trabajo encargados de velar por la seguridad de la información. Por otra parte, es necesario regular aspectos de las nuevas modalidades laborales tales como el teletrabajo o los trabajos desde la residencia de los trabajadores los cuales exigen un nivel más alto de supervisión al manejo de la información.

Con la promulgación de esta ley se obtiene una herramienta importante para denunciar los hechos delictivos a los que se pueda ver afectado, un cambio importante si se tiene en cuenta que anteriormente las organizaciones no denunciaban dichos hechos no sólo para evitar daños en su reputación sino por no tener herramientas especiales.

Algunas normas internacionales para seguridad informática propuestas por la Organización Internacional de Normalización (ISO) son:

- ISO/IEC 27001.
- ISO/IEC 27002.
- ISO/IEC 27821.
- ISO/IEC 27000.

A continuación se presenta algunos aspectos interesantes en la legislación informática y de seguridad en algunos países que han adoptado legislaciones sobre este aspecto tan importante para las organizaciones.

Legislación en Estados Unidos.

Este país adoptó en 1994 el Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030) que edificó el Acta de Fraude y abuso Computacional de 1986, cuya finalidad es eliminar los argumentos técnicos acerca de qué es y qué no es un virus, un gusano, un troyano y en qué difieren de los virus, en la nueva acta proscribe la transmisión de un programa, información,

códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas.

La ley de 1994 diferencia el tratamiento de los que de manera temeraria lanzan ataques de virus a aquellos que lo realizan con la intención de hacer estragos, para eso se ha definido dos niveles para el tratamiento de quienes crean virus: a) para los que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa, y b) para los que lo transmiten sólo de manera imprudencial, la sanción fluctúa entre una multa y un año en prisión.

La nueva ley constituye un acercamiento al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen, al diferenciar los niveles de delitos la ley contempla lo que debe entenderse como acto delictivo. Lo mismo sucede en materia de estafas electrónicas, fraudes y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa a la persona que defraude a otro mediante el uso de una computadora o red informática.

Legislación en Alemania.

Este país aprobó en 1986 la Ley contra la Criminalidad Económica, que contempla los siguientes delitos: a) espionaje de datos; b) fraude informático; c) alteración de datos, y d) sabotaje informático.

Legislación en Holanda.

En marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza el hacking, el phreaking (uso de servicios de telecomunicaciones para evitar el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría), y la distribución de virus. La distribución de

virus está penada de distinta forma si se escaparon por error o si fueron liberados para causar daño. Si se demuestra que el virus se escapó por error, la pena no superará el mes de prisión; pero si se comprueba que fueron liberados con la intención de causar daño, la pena puede llegar hasta los cuatro años de prisión.

Legislación en España.

El artículo 264-2 del Nuevo Código Penal de España, establece que se aplicará la pena de prisión de uno a tres años y multa a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

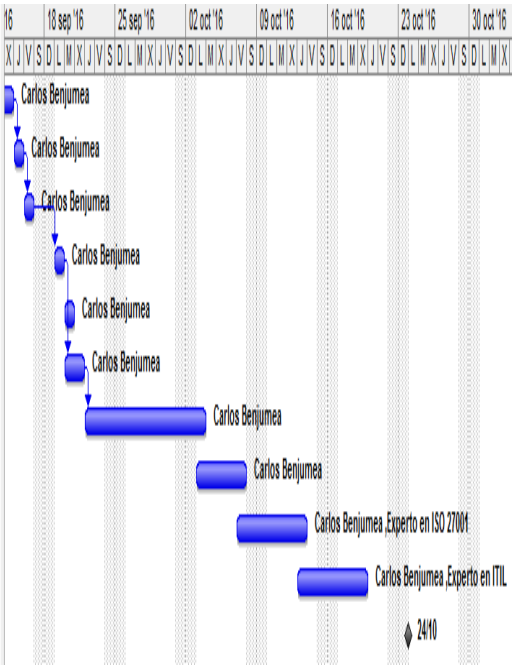
Este código sanciona en forma detallada esta categoría delictiva (violación de secretos/espionaje/divulgación), aplicando pena de prisión y multa, agravándolas cuando existe intención dolosa y cuando el hecho es cometido por parte de funcionarios públicos se penaliza con inhabilitación. (UNAD 2013).

5. ASPECTOS ADMINISTRATIVOS

5.1. CRONOGRAMA DE ACTIVIDADES.

Figura 15. Cronograma de Actividades

	Nombre de tarea	Duración	Comienzo	Fin	Pred	Nombres de los recursos
1	Analizar y Diseñar el Plan de Diagnostico	3 días	lun 12/09/16	mié 14/09/16		Carlos Benjumea
2	Identificar Topologias Estandar de Red en las Pymes	1 día?	jue 15/09/16	jue 15/09/16	1	Carlos Benjumea
3	Analizar los diferentes métodos de ataque y la forma de contrarrestarlos.	1 día?	vie 16/09/16	vie 16/09/16	2	Carlos Benjumea
4	Establecer la Politica de Seguridad para Pyme	1 día?	lun 19/09/16	lun 19/09/16	3	Carlos Benjumea
5	Identificacion de Protocolos de Red de Uso Comun en las Pymes	1 día?	mar 20/09/16	mar 20/09/16		Carlos Benjumea
6	Identificación de Recuros Informaticos	2 días	mar 20/09/16	mié 21/09/16	4	Carlos Benjumea
7	Diseño Guia de Seguridad a Nivel LAN	8 días	jue 22/09/16	lun 03/10/16	6	Carlos Benjumea
8	Diseño Guia Seguridad a Nivel Wan	5 días	lun 03/10/16	vie 07/10/16		Carlos Benjumea
9	Diseño Guia de Politicas de Seguridad	5 días	vie 07/10/16	jue 13/10/16		Carlos Benjumea ,Experto
10	Diseño Guia de Buenas Practicas ITIL	5 días	jue 13/10/16	mié 19/10/16		Carlos Benjumea ,Experto
11	Entrega Final Guia de Seguridad	0 días	lun 24/10/16	lun 24/10/16		Carlos Benjumea



Fuente: propia

5.2. PRESUPUESTO DEL PROYECTO.

Figura 16. Presupuesto del Proyecto

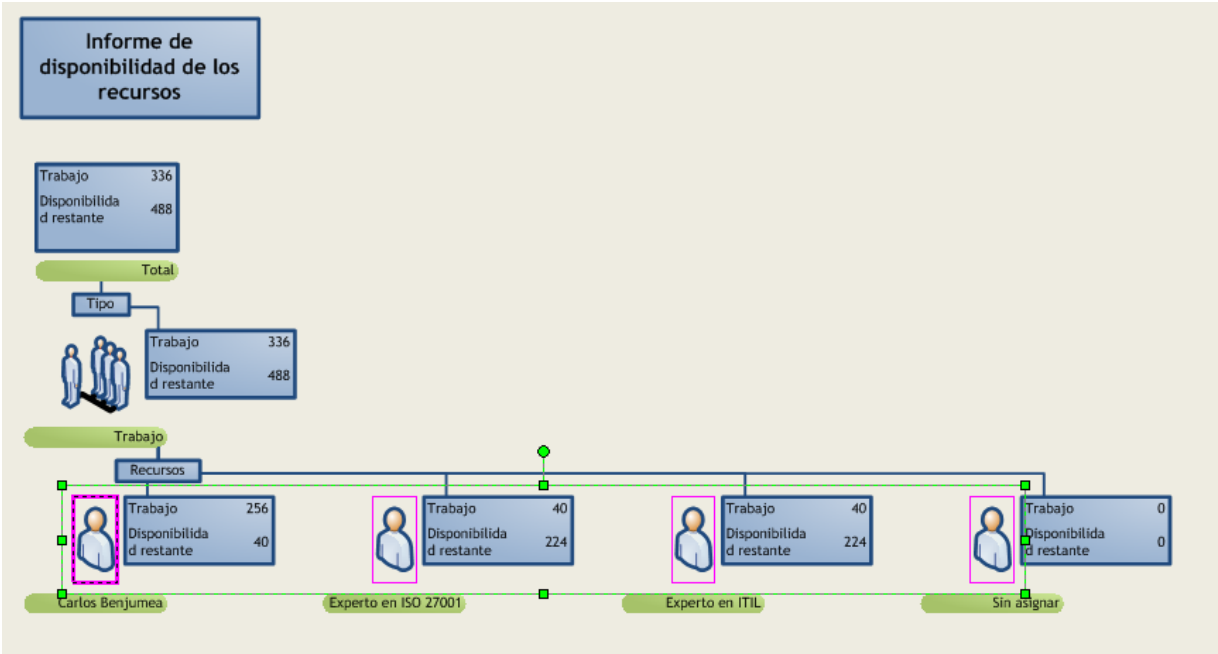
Informe presupuestario el vie 09/09/16
Proyecto_Guia_Seguridad

Id	Nombre de tarea	Costo fijo	Acumulación de costos fijos	Costo total	Previsto	Variación
9	Diseño Guia de Politicas de Seguridad	$ 0,00	Prorrateo	$ 3.200.000,00	$ 0,00	$ 3.200.000,00
10	Dieseño Guia de Buenas Practicas ITI	$ 0,00	Prorrateo	$ 3.200.000,00	$ 0,00	$ 3.200.000,00
1	Analizar y Diseñar el Plan de Diagnos	$ 0,00	Prorrateo	$ 1.800.000,00	$ 0,00	$ 1.800.000,00
2	Identificar Topologias Estandar de Red	$ 0,00	Prorrateo	$ 1.800.000,00	$ 0,00	$ 1.800.000,00
3	Analizar los diferentes métodos de ata	$ 0,00	Prorrateo	$ 1.800.000,00	$ 0,00	$ 1.800.000,00
4	Establecer la Politica de Seguridad pa	$ 0,00	Prorrateo	$ 1.800.000,00	$ 0,00	$ 1.800.000,00
5	Identificacion de Protocolos de Red de	$ 0,00	Prorrateo	$ 1.800.000,00	$ 0,00	$ 1.800.000,00
6	Identificación de Recuros Informaticos	$ 0,00	Prorrateo	$ 1.800.000,00	$ 0,00	$ 1.800.000,00
7	Diseño Guia de Seguridad a Nivel LAN	$ 0,00	Prorrateo	$ 1.800.000,00	$ 0,00	$ 1.800.000,00
8	Diseño Guia Seguridad a Nivel Wan	$ 0,00	Prorrateo	$ 1.800.000,00	$ 0,00	$ 1.800.000,00
11	Entrega Final Guia de Seguridad	$ 0,00	Prorrateo	$ 1.800.000,00	$ 0,00	$ 1.800.000,00
		$ 0,00		**$ 22.600.000,00**	**$ 0,00**	**$ 22.600.000,00**

Fuente: propia

5.3. RECURSOS DEL PROYECTO.

Figura 17. Recursos del Proyecto



Fuente: propia

Tabla 1. Roles de los recursos

Nombre	Rol	Descripción
Experto 1	Experto en ISO 27002	Asesorar la implementación de las políticas de seguridad
Experto 2	Experto en ITIL	Asesorar el manejo de los incidentes de seguridad
Carlos Benjumea	Carlos Benjumea	Encargado de estructurar la Guía de seguridad.

Figura 18. Uso de Recursos del Proyecto.

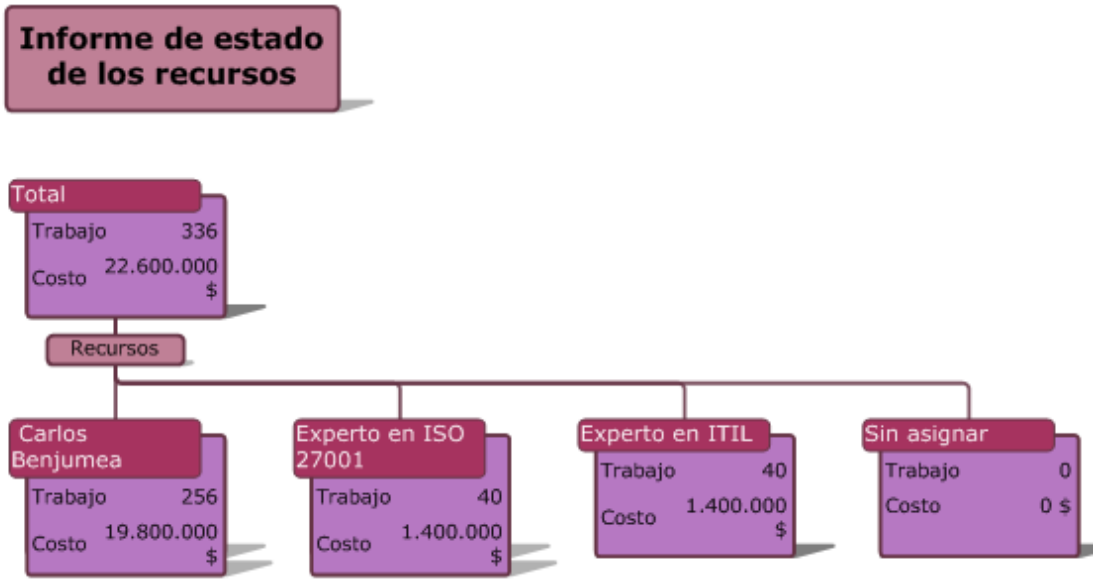
Uso de recursos el vie 09/09/16
Proyecto_Guia_Seguridad

	04/09/16	11/09/16	18/09/16	25/09/16	02/10/16	09/10/16	16/10/16	23/10/16
Carlos Benjumea		40 horas	48 horas	40 horas	56 horas	48 horas	24 horas	
Analizar y Diseñar el Plan de Diagnostico		24 horas						
Identificar Topologias Estandar de Red en las Pymes		8 horas						
Analizar los diferentes métodos de ataque y la forma de contrarrestarlos.		8 horas						
Establecer la Politica de Seguridad para Pyme			8 horas					
Identificacion de Protocolos de Red de Uso Comun en las Pymes			8 horas					
Identificación de Recuros Informaticos			16 horas					
Diseño Guia de Seguridad a Nivel LAN			16 horas	40 horas	8 horas			
Diseño Guia Seguridad a Nivel Wan					40 horas			
Diseño Guia de Politicas de Seguridad					8 horas	32 horas		
Dieseño Guia de Buenas Practicas ITIL						16 horas	24 horas	
Entrega Final Guia de Seguridad								
Experto en ISO 27001					8 horas	32 horas		
Diseño Guia de Politicas de Seguridad					8 horas	32 horas		
Experto en ITIL						16 horas	24 horas	
Dieseño Guia de Buenas Practicas ITIL						16 horas	24 horas	
Total		40 horas	48 horas	40 horas	64 horas	96 horas	48 horas	

Fuente: propia

5.4. ESTADO DE LOS RECURSOS DEL PROYECTO.

Figura 19. Uso de Recursos del Proyecto



Fuente: propia

6. RECOMENDACIONES DE LOS FABRICANTES DE FIREWALL DE NUEVA GENERACIÓN PARA LA SEGURIDAD EN LAS PYMES.

Las empresas, especialmente las PYMES, deben mantenerse a la vanguardia sobre el correcto uso de las tecnologías, de cómo mantener a salvo su integridad digital, de cómo protegerse y todas las cosas que consigo trae este tema. La verdad es que a esto muchas veces no se le suele prestar la debida atención, y por ello es que son tan frecuentes esos casos de pérdidas de información, de espionaje informático, sabotaje, etc.

Figura 20. Principales Fabricantes de Firewall de Nueva Generación. (Cuadrante mágico de Gartner)

Fuente: https://www.tecnozero.com/blog/gartner-2016-para-firewall/

Teniendo en cuenta el cuadrante mágico de Gartner para los firewall de redes empresariales del 2016, a continuación se presentan algunas recomendaciones de estos grandes líderes del sector de la seguridad informática, de igual forma se presenta un costo aproximada de un dispositivo firewall de nueva generación por fabricante teniendo en cuenta la cantidad de usuarios y el tamaño de la infraestructura tecnológica.

Tabla 2. Recomendaciones de los diferentes fabricantes firewall.

Fabricante	Recomendaciones seguridad Para Pymes	Costo de un Solución Básica
Barracuda Network	Políticas potentes y personalizables, que puedan realizar una mayor aplicación de requisitos detallados que controlan los mensajes de correo electrónico entrantes. La Solución implementada debe incorporar las siguientes características, protección typosquatting, Protección Antivirus, Prevención contra DDo	$ 15.000.000
Fortinet	Al implementar esquemas de seguridad de última generación se debe tener la capacidad de reforzar sus políticas añadiendo las identidades de "usuario" y fuente. Identificar un usuario a través de distintos métodos de autenticación, como la de identificación única. El motor de políticas debe tomar decisiones de seguridad más granulares basados en el comportamiento del usuario y el dispositivo. La detección avanzada de amenazas, basada en el comportamiento en conjunción con el sistema de reputación basado en cloud que rastrea botnets y elementos del ciclo de vida de la amenaza, pueden habilitarse y configurarse con gran facilidad.	$ 25.000.000

CheckPoint	Identificación de usuarios y no de direcciones IP. Aprovechar la información de usuarios y grupos almacenada en los directorios de empresa para la visibilidad, creación de políticas, generación de informes e investigación forense, con independencia de dónde se encuentre el usuario. Bloqueo de las amenazas en tiempo real. Protección del ciclo de vida completo frente a ataques, incluyendo aplicaciones peligrosas, vulnerabilidades, software malicioso, URL de alto riesgo y una amplia gama de archivos y contenidos maliciosos.	$ 40.000.000
Palo Alto	Implementar un modelo de seguridad completamente positivo, en el cual solo lo legítimo y autorizado es permitido, bloqueando todo lo demás. Capacidades de prevención de amenazas más amplias y exhaustivas, incluida la inspección completa de datos SSL y cifrados, sin sacrificar el rendimiento de las redes. La Solución Implementada incorpora un firewall totalmente integrado, prevención contra intrusiones (IPS), anti-bot, antivirus, control de aplicaciones, filtrado URL y la tecnología Sandboxing de Check Point con Zero-day Protection.	$ 60.000.000

7. DESARROLLO DE LA GUIA DE SEGURIDAD PERIMETRAL

La guía se basa en dos aspectos fundamentales que deben tener en cuenta las pymes a la hora de implementar la seguridad informática. Estos aspectos son los siguientes:

1. Seguridad Física.
2. Seguridad Lógica.

7.1. PASO 1: SEGURIDAD FÍSICA

La seguridad física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. En este sentido se puede optar por soluciones que controlan e identifican el acceso de personas basándose en atributos físicos como las huellas digitales. Esta tecnología discreta y fácil de utilizar simplemente escanea los atributos físicos de la persona para restringir el acceso de forma fiable a sus instalaciones y áreas operativas confidenciales.

La identificación por huellas digitales, identificación por el iris, identificación facial y otras tecnologías también se deben considerar como parte de una estrategia para el control de acceso físico.

Las siguientes son las actividades a tener en cuenta en este primer paso.

Perímetro de seguridad física.

Se deben utilizar perímetros de seguridad barreras tales como paredes, puertas de acceso controlado con tarjeta o mostradores de recepción atendidos para proteger las áreas que contienen información y servicios de procesamiento de información.

Control de acceso físico.

Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.

Seguridad de oficinas, recintos e instalaciones.

Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.

Protección contra amenazas externas y ambientales.

Se deben diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.

Seguridad de los equipos Informáticos.

Evitar pérdida, daño, robo o puesta en peligro de los activos y la interrupción de las actividades de la organización.

Ubicación y protección de los equipos Informáticos.

Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno, y las oportunidades de acceso no autorizado.

Suministro de energía.

Los equipos deben estar protegidos contra fallas en el suministro de energía y otras anomalías Causadas por fallas en los servicios de suministro.

Seguridad del cableado.

El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información debe estar protegidos contra interceptaciones o daños.

Mantenimiento de los equipos.

Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e Integridad.

Seguridad de los equipos Informáticos Fuera de las instalaciones.

Se deben suministrar seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.

Seguridad en la reutilización o eliminación de equipos.

Se deben verificar todos los elementos del equipo que contenga medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se haya sobrescrito de forma segura, antes de la eliminación.

Retiro de activos.

Ningún equipo, información ni software se deben retirar sin autorización previa.

Tabla 3. Actividades Paso 1.

Paso I	Actividades Generales	
Seguridad Física	Perímetro de seguridad física	
	Control de acceso físico	
	Seguridad de oficinas, recintos e instalaciones	
	Protección contra amenazas externas y ambientales	
	Seguridad de los equipos Informáticos.	
	Ubicación y protección de los equipos Informáticos	
	Suministro de energía	
	Seguridad del cableado	
	Mantenimiento de los equipos	
	Seguridad de los equipos Informáticos Fuera de las instalaciones	
	Seguridad en la reutilización o eliminación de equipos	
	Retiro de Activos	

7.2. PASO 2: SEGURIDAD LÓGICA

Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo. Este paso es el más importante a tener en cuenta, se debe desarrollar por fases, las cuales se describen a continuación:

Fases:

1. Planeación.
2. Implementación.

FASE I. PLANEACIÓN:

La fase de planeación representa una etapa crítica e importante por cuanto comienza con el plan de diagnóstico de la infraestructura tecnológica de las Pymes. Las siguientes son las actividades a tener en cuenta en esta fase:

- ➢ Elaborar y validar el inventario de activos de información de servicios tecnológicos, para esta actividad se requiere desarrollar y mantener el inventario de hardware y software, identificando claramente cuáles equipos están actualizados cuales requieren actualizarse dejando la respectiva documentación.
- ➢ Identificar la topología actual de la red y su funcionamiento dentro de la organización.
- ➢ Analizar, diseñar y desarrollar el plan de diagnóstico del proceso de mejoramiento de seguridad en la red.
- ➢ Revisar los esquemas de segmentación de la red de tal manera que el tráfico generado internamente este plenamente controlado a través de equipos de seguridad firewall de nueva generación. En caso de no tener esquema de red segmentado se debe realizar un diseño del mismo.
- ➢ Identificar la configuración de los equipos activos que hacen parte de la infraestructura de conectividad y seguridad de la red.
- ➢ Analizar e identificar el tipo de tráfico que circula en la red para poder determinar cuál

se debe permitir o denegar.

- ➢ Identificar las aplicaciones de uso misional dentro la organización y en base a su nivel de criticidad generar una estrategia de aseguramiento teniendo en cuenta el tipo de conectividad que utilizan.
- ➢ Validar el estado actual de los sistemas de información, los sistemas de comunicaciones y evaluar la interacción entre ellos y cuando se adopte el esquema de seguridad.
- ➢ Realizar un diseño de seguridad perimetral e interno ajustado a las características y funcionalidades de la red.
- ➢ Realizar un análisis del mercado con el fin de determinar la mejor opción costo beneficio para la adquisición de los elementos o dispositivos requeridos para el aseguramiento de la información.
- ➢ Establecer los acuerdos de confidencialidad que sean necesarios sobre el tratamiento de la información ante terceros.
- ➢ Capacitar a funcionarios de las áreas de sistemas de conformidad con los planes de capacitación establecidos en seguridad informática y establecer la sensibilización a las personas de toda la organización a fin de dar a conocer el nivel de impacto de los nuevos avances tecnológicos en aspectos de seguridad de la información.

Tabla 4. Actividades Fase I Paso 2

Fase I Paso 2	Actividades Generales	
Diagnóstico de la Situación Actual	Construcción del plan Diagnóstico	
	Inventario de TI (Hardware, software)	
	Identificar la topología actual de la red.	
	Revisar los esquemas de segmentación de la red.	
	Identificar la configuración de los equipos activos	
	Analizar e identificar el tipo de tráfico que circula en la red	

	Identificar las aplicaciones de uso misional	
	Validar el estado actual de los sistemas de información.	
	Realizar un diseño de seguridad perimetral e interno.	
	Realizar un análisis del mercado.	
	Establecer los acuerdos de confidencialidad	
	Capacitación	

7.3. FASE II. IMPLEMENTACION

La fase de implementación debe cubrir las siguientes actividades:

- Implementar un esquema de segmentación de la red separando los diferentes servicios, protocolo y aplicaciones.
- Implementar y configurar los equipos de conectividad y seguridad acorde a un esquema de topología donde el firewall de nueva generación, controle el tráfico entre los diferentes segmentos de la red.
- Implementar un sistema que permita la identificación de usuarios y no de direcciones IP. Aprovechar la información de usuarios y grupos almacenada en los directorios de empresa para la visibilidad, creación de políticas, generación de informes e investigación forense, con independencia de dónde se encuentre el usuario.
- Implementar y configurar las aplicaciones en base a las mejores prácticas para brindar el máximo de seguridad.
- Implementar un esquema de seguridad donde se restringa el acceso a los programas y archivos.
- Implementar mecanismo de cifrado y respaldo de la información.
- Implementar, configurar e instalar un antivirus de última generación que este en capacidad de detectar los últimos tipos de amenazas informáticas.
- Implementar procedimientos para el uso de contraseñas seguras y educar a los empleados en las distintas tácticas de ingeniería social.

- Implementar mecanismos de socialización y formación a los empleados en cuestiones de seguridad informática, para que eviten conductas de riesgo al utilizar su email corporativo.

Tabla 5. Actividades Fase II Paso 2

Fase II Paso 2	Actividades Generales	
Implementación	Implementar esquema de segmentación	
	Implementar equipos de conectividad	
	Implementar las aplicaciones a las mejores prácticas	
	Implementar un esquema de seguridad donde se restringa el acceso a los programas y archivos.	
	Implementar, configurar e instalar un antivirus de última generación	
	Implementar, configurar e instalar un antivirus de última generación que este en capacidad de detectar los últimos tipos de amenazas informáticas.	
	Implementar procedimientos para el uso de contraseñas seguras.	

7.4. PROTECCIÓN DE LA INFORMACIÓN DE DAÑOS POR VIRUS Y OTROS CÓDIGOS MALICIOSOS.

Teniendo en cuenta los últimos tipos de malware y que continuamente se liberan nuevos virus es necesario tener en cuenta los siguientes aspectos que debe cumplir la solución de Antivirus para las Pymes el cual debe estar en capacidad de:

- Detener los ataques dirigidos y las amenazas persistentes avanzadas mediante la protección en capas en el endpoint.

- Separar los archivos que están en peligro de los archivos seguros para realizar una detección más rápida y precisa.
- Supervisar en tiempo real el comportamiento de las aplicaciones y detener las amenazas de día cero.
- Mantener una carga de red reducida con flexibilidad para controlar la cantidad de conexiones de red y el ancho de banda.
- Soportar plataformas físicas y virtuales.
- Controlar políticas de forma granular con bloqueo de sistemas, control de aplicaciones y dispositivos, y reconocimiento de ubicación.
- Limitar los posibles efectos de un ataque y proporciona una identificación temprana de los ataques.
- Evitar los exploits de los últimos ataques contra vulnerabilidades.

Tabla 6. Aspectos que debe cumplir el antivirus en las Pyme.

Aspectos	Aspecto que debe cumplir el antivirus en las Pyme.	
Aspectos específicos	Detener los ataques dirigidos y las amenazas persistentes avanzadas mediante la protección en capas en el endpoint.	
	Separar los archivos que están en peligro de los archivos seguros para realizar una detección más rápida y precisa.	
	Supervisar en tiempo real el comportamiento de las aplicaciones y detener las amenazas de día cero.	
	Mantener una carga de red reducida con flexibilidad para controlar la cantidad de conexiones de red y el ancho de banda.	

	Soportar plataformas físicas y virtuales.	
	Controlar políticas de forma granular con bloqueo de sistemas, control de aplicaciones y dispositivos, y reconocimiento de ubicación.	
	Limitar los posibles efectos de un ataque y proporciona una identificación temprana de los ataques	
	Evitar los exploits de los últimos ataques contra vulnerabilidades.	

7.5. CONFIGURACIÓN EQUIPO FIREWALL DE NUEVA GENERACIÓN.

Los firewalls de nueva generación, Next-Generation Firewall (NGFW), surgieron para revolucionar la seguridad de la red tal y como la conocíamos hasta ahora. Los firewalls tradicionales se limitan a la inspección de paquetes por estado y a reglas de control de acceso, pero a medida que los hackers se hacen más sofisticados, las amenazas son más avanzadas y este sistema ha dejado de ser eficaz es necesario tener en cuenta en las Pymes los siguientes criterios para la adquisición e implementación de los firewall de nueva generación.

- Identificación de aplicaciones, no de puertos.
- Vinculación del uso de la aplicación a la identidad del usuario, no a la dirección IP, independientemente de la ubicación o del dispositivo.
- Prevención de todas las amenazas, tanto conocidas como desconocidas.
- Simplificación de la administración de políticas.
- Habilitación segura de aplicaciones.
- Identificación de hosts infectados por bots.
- Limitación de transferencias de datos y archivos no autorizados.
- Control de la navegación web.
- Generación de informes y logs.

Tabla 7. Aspectos de los FWNG

Aspectos	**Aspecto que debe cumplir el FWNG en las Pyme.**	
Aspectos específicos	Identificación de aplicaciones, no de puertos.	
	Vinculación del uso de la aplicación a la identidad del usuario, no a la dirección IP, independientemente de la ubicación o del dispositivo.	
	Prevención de todas las amenazas, tanto conocidas como desconocidas.	
	Simplificación de la administración de políticas.	
	Habilitación segura de aplicaciones.	
	Identificación de hosts infectados por bots.	
	Limitación de transferencias de datos y archivos no autorizados	
	Control de la navegación web.	
	Generación de informes y logs.	

Sin importar cuál sea la guía de implementación que una empresa determine usar, es imprescindible que la gestión de incidentes sea la base para iniciar un proceso de gestión integral de la seguridad de la información, un valor muy importante para los objetivos empresariales y la mejora continua de la organización, la guía se debe basar e implementar bajo la norma ISO27002. Lo anterior teniendo en cuenta que la norma puede ser aplicada a cualquier tipo de empresa u organización, ya sea privada o pública, sin importar el tamaño de la misma.

8. BENEFICIOS EN LA IMPLEMENTACIÓN DE LA GUÍA.

La implementación de la guía permite gestionar incidentes de seguridad de forma más eficiente y tener un soporte sólido para sustentar ante la alta gerencia un plan de inversión en seguridad de la información, donde con evidencias y cálculos claros de los impactos económicos que se pueden presentar ante la materialización de un incidente, es posible presentar de forma clara las posibles soluciones para la mitigación correctiva o preventiva de estos eventos no deseados, y de esta forma poder garantizar que la inversión cubra las brechas de seguridad más importantes y una medición de la eficacia de sus controles.

Un beneficio importante en el aspecto comercial es que se genera credibilidad y confianza en los clientes que tenga la organización. En el ámbito funcional, se desarrolla una adecuada gestión de los riesgos. La empresa conoce de forma exhaustiva su organización y los sistemas de información que aplican, los problemas que se producen y los medios de protección que se aplican, para así terminar garantizando la mejor disponibilidad de los materiales y datos, y asegurando su continuidad.

Otra de los beneficios que se tiene al gestionar incidentes son las evidencias, lo cual para casos de fraudes internos o externos nos permite entregar al área legal una prueba válida ante un posible proceso administrativo interno o judicial, para lo cual es conveniente que esta recopilación de evidencias se realicen cumpliendo las normas legales para este procedimiento.

9. CONCLUSIONES

Todos los proyectos orientados a la seguridad de la información corporativa empiezan con el mismo paso, determinar cuál es la información sensible, descubrir dónde está alojada además del centro de datos, si está diseminada en computadoras de escritorio, dispositivos móviles y en la nube, y revisar cómo y quién accede a ella.

Tras identificar la información sensible, se debe determinar cómo se utiliza, quién accede a ella, quién la utiliza, quién la crea, dónde se envía, y así identificar los procesos del negocio en los cuales participan estos datos, para poder asegurarlos y plasmarlos en políticas corporativas, e incluir algunos casos de excepción que sean necesarios como en el caso de los socios de negocios.

La falta de recursos provoca a veces que muchas PYMES cuenten con una seguridad insuficiente o no sepan exactamente cuáles son las medidas que tienen que adaptar para estar protegidos, además no invierten en seguridad informática porque no creen que esa inversión les traiga algún costo beneficio, al contrario lo ven como algo que va hacer efectivo, pero que no les generará muchos beneficios. Cuando deciden hacerlo es cuando ven un crecimiento en su compañía, pero les cuesta más sí nunca han invertido.

Los cambios radicales en el ámbito de las aplicaciones y de las amenazas, el comportamiento de los usuarios y la infraestructura de la red han ido deteriorando la seguridad tradicional, actualmente la seguridad de datos empresariales involucra a todos en la empresa desde el dueño y los ejecutivos más altos, hasta los proveedores y socios. Desde la parte cultural, hasta la parte tecnológica.

En su trabajo diario los usuarios acceden a todo tipo de aplicaciones utilizando una amplia gama de dispositivos. Mientras tanto la expansión de los centros de datos, la virtualización, la movilidad y las iniciativas basadas en la nube, están obligando a rediseñar los permisos de acceso de las aplicaciones sin afectar a la protección de la red.

No todas las pequeñas y medianas empresas tienen la experiencia necesaria para la gestación de sistema de seguridad informática de nueva generación, es necesario tener guías prácticas adaptables a cada necesidad que les ayude a tener una línea base para el aseguramiento de sus herramientas tecnológicas, de forma ágil, reduciendo costos y minimizando los riesgos de sufrir ataques informáticos.

Al final los objetivos básicos de una arquitectura de seguridad corporativa, siguen siendo evitar que personas no deseadas o programas computarizados entre a la red empresarial; si entra, evitar que tome control de los recursos informáticos, si toma control del sistema, evitar que extraiga información.

10. BIBLIOGRAFIA

Cisco, (2015). *Pymes colombianas deben mejorar inversión en tecnología.* Colombia: el empleo. Recuperado de: http://www.elempleo.com/colombia/formacion_desarrollo/pymes-colombianas-deben-mejorar-inversin-n-en-tecnolognua/6587747

Caracol, (2014). *Colombia es el país de habla hispana que genera más ataques informáticos.* Colombia: Kaspersky. Recuperado de http://caracol.com.co/radio/2014/10/16/tecnologia/1413470760_465076.html

Certicamara, (2015). El *2015 fue un año de "altas y bajas" para la seguridad Informática.* Colombia: Certicamara. Recuperado de https://web.certicamara.com/media/158090/el-2015-fue-un-ano-de-altas-y-bajas-para-la-seguridad-informatica.pdf

Dinero, (2015). *EL 43% de las empresas colombianas no están preparadas contra los ciberataques.* Colombia: Dinero. Recuperado de http://www.dinero.com/pais/articulo/colombia-tuvo-perdidas-de-1-billon-por-ciberataques/224404

El Universal, (2016). *La cibercriminalidad será la mayor amenaza para 2016.* Colombia: El Universal. Recuperado de http://www.eluniversal.com/noticias/estilo-vida/cibercriminalidad-sera-mayor-amenaza-para-2016_83918

Evilfingers, (2010). *Ataques informáticos Debilidades de seguridad comúnmente explotadas.* Colombia: Evilfingers Recuperado de https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf

Itil, (2013). *Introducción a Itil.* Colombia: Itil. Recuperado de http://itil.osiatis.es/

Lopez, A. (2014). *¿Qué es un Firewall de Nueva Generación?* Colombia: Firewall.

Recuperado de http://noticias.gti.es/fabricantes/que-es-firewall-de-nueva-generacion/

PaloAlto, (2011). *Paloaltonetworks.* Colombia: Firewall. Recuperado de https://media.paloaltonetworks

Portafolio, (2015). *Cuatro de cada diez empresas en el país no están preparadas para un ciberataque.* Colombia: Telefonica. Recuperado de http://www.portafolio.co/negocios/empresas/ciberataque-empresas-preparadas-colombia-492281