UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE INGENIERIA
CARRERA INGENIERIA EN SISTEMAS COMPUTACIONALES

TÍTULO:

DIAGNÓSTICO DE LA SEGURIDAD QUE OFRECEN LOS FIREWALLS PARA LAS AGENCIAS PRODUCTORAS Y ASESORAS DE SEGUROS DE LA CIUDAD DE GUAYAQUIL

AUTOR:
CORONEL SUAREZ VICTOR HUGO

Trabajo de Titulación Previo a la Obtención del Título de:
INGENIERO EN SISTEMAS COMPUTACIONALES

TUTOR:
ING. GILBERTO FERNANDO CASTRO, MGS

Guayaquil, Ecuador
2014

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE INGENIERIA
CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por **Coronel Suárez Víctor Hugo**, como requerimiento parcial para la obtención del Título de **Ingeniero en Sistemas Computacionales.**

TUTOR

_____
Ing. Gilberto Fernando Castro, Mgs

REVISORES

_____
Ing. Edison José Toala Quimi, Mgs

_____
Ing. Adela Zurita Fabre, Mgs

DIRECTOR DE LA CARRERA (e)

_____
Ing. Beatriz Guerrero Yépez, Mgs

Guayaquil, a los 30 del mes de marzo de 2014

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE INGENIERIA
CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Víctor Hugo Coronel Suárez**

DECLARO QUE:

El Trabajo de Titulación **Diagnóstico de la Seguridad que ofrecen los Firewalls para las Agencias Productoras y Asesoras de Seguros de la ciudad de Guayaquil** previa a la obtención del Título de **Ingeniero en Sistemas Computacionales**, ha sido desarrollado en base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan en las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del Trabajo de Titulación referido.

Guayaquil, a los 30 días del mes de marzo de 2014

EL AUTOR

_____
Víctor Hugo Coronel Suárez

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE INGENIERIA
CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

AUTORIZACIÓN

Yo, **Víctor Hugo Coronel Suárez**

Autorizo a la Universidad Católica de Santiago de Guayaquil, la **publicación** en la biblioteca de la institución del Trabajo de Titulación: **Diagnóstico de la Seguridad que ofrecen los Firewalls para las Agencias Productoras y Asesoras de Seguros de la ciudad de Guayaquil**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 30 del mes de marzo de 2014

EL AUTOR:

_____
Víctor Hugo Coronel Suárez

AGRADECIMIENTO

Agradecimiento especial a las empresas que colaboraron con el trabajo de investigación realizado, proporcionando valiosa información, transformándola en un aporte para la sociedad.

Gracias al Ing. Fernando Castro, al Ing. Edison Toala, y a la Ing. Zurita tutor y lectores respectivamente que con su apoyo se ha logrado presentar un trabajo que aportará positivamente a la sociedad.

Gracias a Ecuaprimas y al personal que labora en la empresa por darme todas las facilidades para poder realizar el presente trabajo.

A Dios por darme la vida y el don del amor y la perseverancia ya que sin ello no habría logrado conseguir logros muy importantes en mi vida.

VICTOR HUGO CORONEL SUÁREZ

DEDICATORIA

El presente trabajo está dedicado a Dios por darme la fuerza e inteligencia necesaria para poder llevar a cabo la realización de esta investigación. A Grace Suárez mi madre que con amor espero incansablemente el momento en que finalice mi carrera profesional, a Víctor Coronel mi padre que me ayuda a demostrarme que cada vez puedo ser mejor, a mi hermana Grace Coronel por sus consejos y a mi novia Yajaira Vera por su apoyo y cariño incondicional, a todos ellos va dedicada la consecución de esta alegría que es una de las muchas que se vendrán.

Dedicado también al resto de mi familia y a los que de una u otra forma decidieron creer o no en todo el potencial que tenemos cada una de las personas en este mundo, todo es imposible hasta que alguien demuestre lo contrario.

VÍCTOR HUGO CORONEL SUÁREZ

TRIBUNAL DE SUSTENTACIÓN

_____

Ing. Gilberto Fernando Castro, Mgs
PROFESOR TUTOR

_____

Ing. Edison José Toala Quimi, Mgs
PROFESOR DELEGADO

_____

Ing. Adela Zurita Fabre, Mgs
PROFESOR DELEGADO

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERIA

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

CALIFICACIÓN

_____

ING. GILBERTO FERNANDO CASTRO
PROFESOR TUTOR

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

RESUMEN

Los avances tecnológicos que han marcado tendencia en la última década hacen que las personas tengan recelo al momento de compartir su información y sienten la necesidad de proteger la misma, más aún si son los encargados de alguna organización que tiene como principal objetivo mantener satisfechos a los clientes.

Es fundamental mencionar que se debe entender todo lo relacionado a la seguridad informática, su importancia y elementos que facilitan su investigación, además de recordar que muchas de las organizaciones públicas y privadas manejan sus propias políticas de seguridad cuando de confiar su información se trata, y entre sus políticas se puede conocer que antes de confiar sus datos, toman en cuenta si la empresa de seguros en este caso, tiene un departamento de tecnología capaz de garantizar confiabilidad y por ende cuente con una infraestructura que respalde los servicios que ofrece. Con esto empieza el interés de *Diagnosticar la seguridad que ofrecen los firewall para las agencias productoras y asesoras de seguros de la ciudad de Guayaquil,* y para conseguir lo propuesto se utilizó el método cuantitativo, el cual nos permite evaluar las necesidades de los bróker y haciendo uso de las encuestas a las compañías se determinó la obligación de buscar alternativas para la seguridad informática y reuniones con proveedores ayudaron a generar opciones ajustables a este tipo de negocios.

En conclusión, se propone una solución referencial que facilita la implementación de seguridad informática en las agencias productoras y asesoras de seguros para que estén protegidos de las amenazas que se puedan presentar.

Palabras clave: Firewall, Seguridad, Políticas, Seguros, Agencias de Seguros, Información.

ABSTRACT

The technological advances that have set the trend in the last decade make people have misgivings when sharing your information and feel the need to protect it, even if they are responsible for an organization whose main objective is to maintain satisfied the customers.

It is essential to mention that you should understand everything related to computer security, importance and elements that facilitate research in addition to remember that many public and private organizations manage their own security policies when it comes to trust your information , and between policies can be found that before trusting your data, taking into account whether the insurance company in this case has a department of technology to ensure reliability and therefore count with an infrastructure to support the services offered . With this begins the interest of the security afforded Diagnose the firewall for the producing agencies and insurance advisory Guayaquil, and proposed for the quantitative method, which allows us to assess the needs of the broker and was used by use of surveys companies the obligation to seek alternatives to computer security and vendor meetings helped generate adjustable options to this type of business was determined.

In conclusion, a reference solution that facilitates the implementation of information security in the producing agencies and insurance advisors to be protected from threats that may arise is proposed.

Keywords: Firewall, Security, Policies, Insurance, Insurance Agency, Information.

INTRODUCCIÓN

El presente trabajo de titulación tiene como propósito demostrar las bondades que ofrecen los firewall frente a las necesidades de seguridad de las pequeñas y medianas empresas, las cuales son conscientes de los riesgos informáticos a las que su información empresarial está expuesta, y sienten preocupación por los ataques cibernéticos a los que son propensos, y es por ello que la seguridad es el principal punto a tratar cuando una organización desea mantener conectada su red privada a Internet.

Sin considerar el giro de negocio de las organizaciones, se puede notar que se han incrementado los servicios que puede ofrecer el internet y a su vez el número de usuarios que hacen uso de los mismos. Adicional a lo expuesto, las empresas buscan las ventajas que ofrece el Internet como el compartir archivos de forma ágil y rápida.

En la actualidad las empresas corren el riesgo de sufrir ataques externos y también los podrían sufrir internamente, es por ello que se debe precautelar y controlar los accesos dentro de la organización con el fin de evitar la fuga de información importante para la compañía. Los administradores de red son los llamados a cuidar lo concerniente a la seguridad de sus sistemas, debido a que se expone la red de la organización a posibles ataques que afecten la integridad y evolución de la compañía.

Con el fin de superar el temor de ser atacado tecnológicamente y proveer el nivel de protección requerida, la organización necesita implementar seguridad en todo su perímetro de red para prevenir el acceso no-autorizado de usuarios a los recursos de la red privada, y protegerse contra la fuga de información. Inclusive si alguna organización no está conectada al Internet, ésta se encuentra con el deber de establecer políticas de seguridad interna para administrar el acceso de usuarios a porciones de red y proteger de manera adecuada la información privada.

Una de las razones que motivó a realizar esta investigación, es la necesidad de realizar un diagnóstico para ayudar a las compañías aseguradoras a elegir un firewall adecuado con un estándar en sus políticas de seguridad informática, esperando de esta manera evitar caídas de servicios informáticos y pérdidas de información. Cabe mencionar que se busca prevenir ser víctimas de ataques por temas de seguridad debido a las falencias que se pudieran detectar por no tener definido a que pueden acceder cada uno de los usuarios dentro organización y hasta donde pueden llegar cuando necesiten realizar tareas en concreto.

Este trabajo de titulación está orientado, principalmente, a proponer soluciones de seguridad informática para solventar situaciones de riesgo que puedan afectar a las pequeñas y medianas compañías con un enfoque preferente en las agencias productoras y asesoras de seguros, para ello se plantea los siguientes objetivos:

Objetivo General

- Identificar el firewall que más se ajuste a las necesidades de las empresas productoras y asesoras de seguros que permita precautelar su negocio y la productividad del mismo.

Objetivos Específicos

- Hacer un diagnóstico de la vulnerabilidad a la que están expuestas las compañías productoras y asesoras de seguros.
- Identificar las necesidades reales de las compañías productoras y asesoras de seguros para la implementación de las seguridades.
- Diseñar políticas de seguridad aplicable a los firewalls y basadas en el ethical hacking.

- Presentar plan de implementación de las políticas diseñadas en un firewall identificado.

Los propósitos planteados determinan la siguiente hipótesis:

> Si se realiza un adecuado análisis de las características de los firewalls y las necesidades del manejo confiable de la información de las empresas asesoras y productoras de seguros, entonces se podrá instaurar una solución referencial que será aplicable a este tipo de organizaciones.

La metodología de investigación a aplicar se realizará bajo el método cuantitativo, debido a su enfoque en los siguientes aspectos:

Se puede definir y limitar el número de elementos, saber dónde se inicia el problema, en qué dirección va y que tipo de incidencia existe entre los elementos.

CAPÍTULO I

MARCO TEÓRICO

Este capítulo definirá conceptos relacionados al tema en donde se involucra la seguridad informática en el mundo de los seguros, con la intención de tener claras las definiciones relacionadas al objeto de estudio.

1.1 FUNDAMENTACIÓN TEÓRICA CONCEPTUAL

En la actualidad son ya muchas las organizaciones que tratan de diferenciarse en sus mercados y de obtener ventajas competitivas con una óptima y adecuada utilización de las Tecnologías de la Información y las Comunicaciones (TIC). Desde muchas perspectivas la utilización de la Informática y/o de las TIC puede establecer una diferencia importante en una materia de calidad en los procesos tanto internos como externos de una organización (López-Hermoso Agus, y otros, 2000, pág. 13)

Firewall o cortafuegos, herramienta encargada de la protección de los medios informáticos que hacen posible el desarrollo de la organización, tanto en lo económico como en su competencia comercial. El enfoque de la importancia de este tipo de herramientas es el conocimiento previo de la necesidad y de los riesgos, pero la palabra clave es protección, la cual las organizaciones aspiran a tener la mejor y la indicada. De allí se encuentra la primera necesidad que es conocer lo más relevante acerca de seguridad informática y su enfoque hacia la necesidad de protección de las organizaciones.

La seguridad informática orientada a proteger la infraestructura tecnológica y computacional y todo aquello que se relacione con este campo, sobre todo la información y datos que ella contiene. Para responder a esta necesidad de protección, hay todo un conjunto de métodos, reglas, políticas, estándares y leyes que han sido diseñadas específicamente para minimizar los riesgos a

los que puede estar expuesta la infraestructura tecnológica o la información. La seguridad informática involucra al software tal es el caso de los programas que se usan en el día a día, el hardware que en términos simples es el que hace posible el funcionamiento del software y todo lo que la importante que la organización considere y signifique un riesgo. La seguridad de la información no debe ser confundida con seguridad informática, tienen relación pero se enfocan en diferentes escalas de protección porque la seguridad informática se encarga de lo relacionado a los medios informáticos, pero no se puede olvidar que la información es posible que se encuentre en formas y medios diferentes, no solamente en medios informáticos y para ello es necesario la seguridad de la información. La seguridad informática se preocupa de conseguir un sistema de información seguro y confiable.

La información se define como toda percepción que permita adquirir cualquier tipo de conocimiento; por tanto, existirá información cuando se da a conocer algo que se desconoce (Desongles Corrales & Moya Arribas, 2006, pág. 13)

Se concluye, definitivamente, que el encargado de guardar y cuidar la información de la empresa es el personal informática, y debe ofrecer soluciones confiables de hardware y software, que así mismo, respondan con toda su capacidad a las exigencias del quehacer diario, y que sean escalables con el fin de que ofrezcan un beneficio de inversión que dé seguridad y frutos a largo plazo y se convierta en un beneficio general para toda la organización.

Las empresas, de forma consciente o inconsciente, han volcado sus procesos de negocio netamente a los sistemas de información. Siempre con el fin de volverse más productivas, ahorrar costos y poder realizar negocios en todas partes del mundo, cada una de las operaciones de una empresa se ha transformado en parte de una aplicación informática. La información que años atrás era almacenada en papel (el cual podía guardarse en un lugar conocido, leerse, copiarse y destruirse a mano), ahora se encuentra dispersa

en forma de ceros y unos, dentro de varios medios de almacenamiento, como memorias USB, discos duros, dispositivos ópticos, y otros. Esto ha creado una amplia diversidad de fuentes de información, que nosotros estamos encargados de proteger. Dentro de las filas de una organización que se rige por un presupuesto, nuestros recursos para brindar protección y seguridad serán limitados. Algunas empresas asignan más capital a la seguridad informática que otras, pero lo cierto es que todos, en mayor o menos medida, nos encontramos limitados en cuanto a los recursos de que podamos disponer para realizar nuestras tareas (Portantier, 2012, pág. 26)

La información tiende a hacerse uno de los bienes más preciados de la empresa y su destrucción, su copia o su pérdida de integridad pueden traer consigo consecuencias graves para las organizaciones.

Si les demostramos a nuestros clientes un compromiso con la seguridad de sus datos y con brindar un servicio de primer nivel, estaremos ganando más dinero porque atraeremos más clientes y mantendremos contentos a los que ya tenemos (Portantier, 2012, pág. 27)

Cabe recalcar el párrafo anterior porque es la información la que se busca proteger y para ello se determinará cual es el firewall idóneo para las compañías asesoras y productoras de seguros, y partiendo de estos lineamientos básicos podemos aspirar a tener segura la red empresarial.

Como se observa la necesidad de que las empresas de computación o las compañías que emplean bienes o servicios informáticos recurran a los contratos de seguros para que estos cubran o respalden la gama de riesgos informáticos existentes se convierte en imperioso menester. En materia informático-contractual se denomina agente de transformación a la compañía aseguradora. Entre los agentes de transformación más conocidos están los aseguradores, los especuladores sobre mercados a término, los agentes de seguros, los banqueros, etc. Las consecuencias financieras de un siniestro informático se aprecian según se trate de un daño al equipo, pérdida de control de confiabilidad en los tratamientos, o perjuicios causados

a terceros. En este sentido, el perjuicio financiero se analiza según se trate de un perjuicio directo (costo del material destruido), un perjuicio consecutivo (el monto del margen beneficiario no realizado) o perjuicio indirecto (la pérdida del mercado o del cliente) (Téllez Valdés, 2009, pág. 175)

El mundo de los seguros es eso, protección preventiva sin esperar a que suceda el percance o siniestro, no esperar a perder para que ese momento se convierta en el punto de partida para comenzar a protegerse. Al momento que se pierde información la organización no solo se expone a la perdida de la mismas dado que en el ámbito financiero y en el ámbito empresarial también causaría repercusiones porque se pierde dinero y en muchos casos empieza la desconfianza del cliente, la posible pérdida del mismo y con el posibles buenas referencias futuras que por lo general desencadenan en negocios importantes para la organización entonces si no se los cuida es posible encontrarse con pérdidas irreparables.

El mundo informático colabora con grandes soluciones cuando de manejar información se trata y expande sin número de posibilidades para cuidar la misma. Conservar la información intacta es primordial y cuidarla es labor del departamento de sistemas inmerso en cada una de las empresas o del personal externo encargado de dar servicios de protección de la información.

Entre las protecciones que aparecen en la órbita del término seguridad informática se encuentran los firewall centro del presente estudio los mismos que pueden estar implementados como Hardware o Software, para proteger la información que se encuentra dentro de la compañía y que no debería estar expuesta y tener acceso desde fuera de ella sin antes contar con los permisos necesarios, inclusive cuando se haga uso de herramientas que utilicen servicios web, en los cuales se sigue el modelo cliente/servidor. En el modelo cliente/servidor de un sistema distribuido hay un cliente que solicita un determinado servicio a través de un computador y un servidor que proporciona ese servicio desde otro computador (Arnedo Moreno, y otros, 2010, pág. 50)

Soluciones antivirus, endpoint para empresas y otros ofrecen protección dentro de la organización puesto que por ningún motivo se debe descuidar en ambiente interno pues también representa un punto frágil al momento de presentarse algún tipo de ataque.

AIG Metropolitana presentó en noviembre el producto Cyber Edge que cubre a las empresas de fraudes informáticos. AIG conocida aseguradora internacional tiene cobertura en 192 países y el seguro Cyber Edge ya está operando en toda América (Revista Lideres.ec, 2013)

En la actualidad, las nuevas tecnologías establecen facilidad en el uso por parte del mundo empresarial, en todas las áreas y disciplinas. La información proveniente de bases de datos, redes sociales, las cuentas bancarias, entre otra, se encuentra en plataformas virtuales. Ya la práctica de archivos y estantes para ubicar documentación física ha sido reemplazada por la “nube” lo que facilita la obtención de la información y agilidad en los procesos; sin embargo de estas ventajas, los riesgos y nuevas formas de delinquir aumenta, por lo que las compañías aseguradoras deben adelantarse a estos riesgos y diseñar mecanismos que permitan proteger a sus clientes.

1.2 FUNDAMENTACIÓN TECNOLÓGICA

A continuación se presentan conceptos modulares que permitirán a hacer referencia a la tecnología que se utilizará en el presente proyecto.

1.2.1 Hardware

Es el equipo físico el cual se conoce como el elemento que se puede tocar en el área de la informática ya que se lo puede manipular y mover en caso de que sea necesario. A lo largo del tiempo han existido varios tipos de hardware que son parte de la tecnología, y se los puede clasificar en dispositivos de entrada como el teclado, el mouse, lector de códigos de

barra, etc., y también están los dispositivos de salida como el monitor, proyector, impresora, parlantes entre otros.

El hardware se clasifica en básico y complementario. El básico es todo aquel dispositivo, o aparato, necesario para iniciar el funcionamiento de la computadora, y el complemento realiza funciones específicas o más allá de las básicas (Ibañez Carrasco & García Torres, 2009, pág. 7)

Los switch, router, satélites, y antenas, equipos que se usan en el área de las telecomunicaciones, los dispositivos de procesamiento y almacenamiento también están dentro de los equipos considerados como hardware entre los que se puede mencionar a los procesadores de diferentes marcas como Intel, AMD, entre otros, y también disco duro, pendrive, tarjeta madre, memoria, etc.

También conocidos como la tecnología sensorial que se utiliza para introducir información y comandos a la computadora. Estos dispositivos capturan la información del medio ambiente y la convierten a una forma entendible por la computadora (González Martínez, y otros, 2010, pág. 4)

Hardware es la plataforma fisica para la infraestructura de los sistemas de informacion integrada con los siguientes componentes.

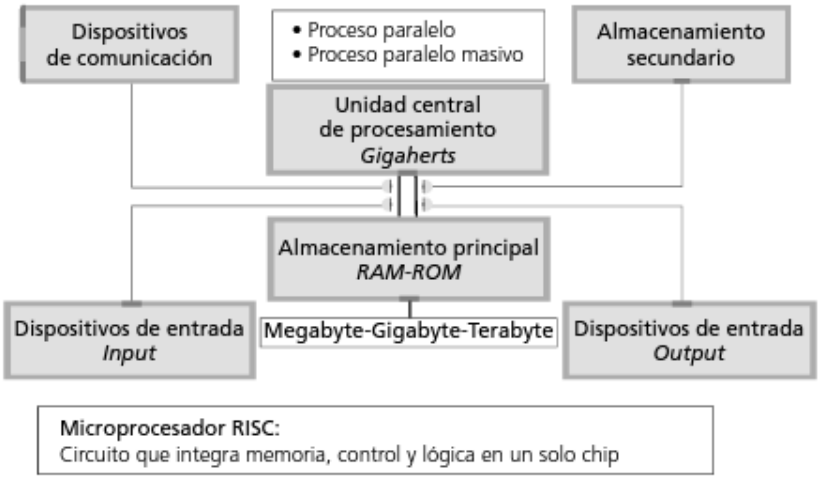


Figura de acuerdo con los conceptos de Parsons, J., Oja, D., 2004.

Gráfico # 1. Hardware como plataforma para integración de componentes

Fuente: (González Martínez, y otros, 2010, pág. 7)

Para mayor claridad conceptual, hardware se refiere a todas las partes tangibles de un sistema informático, en el cual se pueden establecer diferencias entre hardware básico y sofisticado, cuál es el estrictamente necesario para el funcionamiento normal de un equipo y el complementario que sería el encargado de cumplir funciones específicas.

1.2.2 Software

Herramienta lógica de un sistema informático ejecutada gracias a la ayuda del hardware, el software reúne a todos los componentes lógicos necesarios los cuales ayudan a cumplir funciones previamente establecidas y definidas. Software es también conocido como programa, que por ejemplo se usa en la emisión de reportes, facturas, estados de cuenta, etc., entonces se puede asegurar que son todo tipo de programas en general, aplicaciones, juegos, sistemas operativos, utilitarios, antivirus, entre otros y es todo lo que se pueda ejecutar en la computadora.

El software es necesario para que el hardware adquiera la importancia que se merece, y es por ello que se los utiliza para inicializar cualquier tipo de sistemas y se puede citar por ejemplo los sistemas operativos de las computadoras como Windows, Mac, Linux, Solaris, también están los software para automatización industrial, programas educativos, juegos, los que sirven para programar que tienen incluidas librerías y herramientas editoras de texto, y con ellos se crean más programas, que pueden de igual manera someterse a procesos de depuración o corrección mediante software especializado.

Realiza tareas específicas para administrar la tecnología de información y coordina la interacción de los dispositivos. El más conocido es el sistema operativo que controla al software de aplicación y administra el trabajo conjunto de los dispositivos (González Martínez, y otros, 2010, pág. 8)

- Controla las acciones de la computadora.

- Calendariza y asigna los recursos del sistema de acuerdo con las solicitudes.
- Da seguimiento a las actividades y trabajos en proceso.

1.2.3 Red Computacional

Es cuando hay varios equipos conectados entre sí a través de equipos físicos con el fin de transmitir, compartir y ofrecer datos o servicios. Una red computacional conocida a nivel mundial es el internet pero también se puede privatizar las redes para que sean de exclusividad de una organización determinada. Como en toda red en la que va a haber una interacción se debe tener el sujeto emisor y el receptor sin olvidar lo que se va a transmitir, y en este tipo de acciones se busca la confiabilidad en la transmisión y la completa disponibilidad en el momento que se lo requiera utilizando diversos tipos de protocolos.

1.2.4 Internet

Medio mundialmente utilizado a diario para compartir o buscar información utilizando diversos tipos de protocolos los cuales ayudan a acortar distancias entre la comunidad mundial, tal es el caso de una comunicación entre familiares que se encuentren en diferentes partes del mundo, o tan solo jugar en línea. Con los avances que ha tenido este medio ahora se puede obtener telefonía o televisión a través de protocolos de internet utilizados exclusivamente para tener este tipo de servicios, o conectarse remotamente a otro equipo es tan fácil como ir de un punto a otro dentro de la sala del hogar y es imposible olvidar los millones de correos electrónicos que son enviados minuto a minuto, y que también usan sus protocolos específicos.

1.2.5 Familia de Protocolos de Internet

El modelo OSI divide y especifica las funciones propias de la comunicación a través de siete capas informáticas. Concretamente, la descomposición del modelo en funciones se organizó en forma de protocolos. Un protocolo constituye un conjunto de estándares de comunicación que precisan el formato siguiente correspondiente a los datos que se transmiten a través de la red (Atelin & Dordoigne, 2007, pág. 47)

El internet se centra en diversos protocolos de red para poder llevar a cabo la comunicación o transmisión de datos, y entre los primeros que se crearon son el TCP y el IP los cuales significan Protocolo de Control de Transmisión y Protocolo de Internet respectivamente y son la base del mismo. Existen muchos protocolos entre los que se pueden mencionar el HTTP, para la navegación web, el SMTP, IMAP y POP3 que son para el uso de correo electrónico, el FTP y P2P para la transferencia de archivos, y el protocolo telnet para el uso de conexiones remotas entre equipos.

IP versión 4 consiste en asignar una dirección de 4 porciones de números separadas por un punto que sirven para identificar un equipo y enlazar varios computadores en una red pequeña dándole por nombre red LAN, y si es una red extensa se le asigna el nombre de red WAN. Las IPs pueden llegar a ser públicas y privadas.

IP versión 6 creada principalmente para en un futuro muy próximo ser la reemplazante de IP versión 4 debido a la demanda de direcciones IP que existe en la actualidad, es destinada a mejorar el servicio de comunicación de tal manera que asignara direcciones permanentes a los dispositivos móviles y su diferencia radica en la longitud de la dirección ya que en IP v4 se representan como un entero de 32 bits y en IP v6 se representan como un entero de 128 bits, por lo cual la dirección está conformada por 8 grupos de 4 dígitos hexadecimales cada uno.

1.2.6 Seguridad Informática

En lo que se refiere a la seguridad en la red, debe entenderse que se trata de la habilidad que deben desarrollar las empresas para identificar y eliminar toda posibilidad de que se vulnere la información, buscando salvaguardar tanto la identidad de la empresa, sus datos, equipos y hasta los mismos computadores. Además es importante destacar que el nivel de seguridad varía de empresa a empresa, puesto que lo que es factible y necesario para una organización no necesariamente va a beneficiar a otra; lo que sí es determinante es que cualquier empresa que maneje en red su información debe tener políticas de seguridad que pueda adaptarla a sus necesidades y conveniencia.

Prever un riesgo es controlar el perjuicio financiero que viene aparejado a su realización, de aquí que toda empresa deba controlar sus riesgos de acuerdo con su capacidad financiera, al hacer frente a las variaciones de dichos riesgos y cuidar que no exceda su presupuesto o activo si el siniestro llegara a suceder. Si se estudian los riesgos que pueden convertirse en siniestros o desastres informáticos en una compañía, se puede cuantificar su rentabilidad para solventarlos o añadir a una cobertura de seguro que proteja esa incertidumbre (Téllez Valdés, 2009, pág. 174)

La seguridad informática tiene como función principal la protección de archivos e información contenida en su infraestructura computacional, entre los que destacan se detalla a continuación:

- Infraestructura tecnológica: Esencial para el manejo de la información, el trabajo y desarrollo de la compañía. El objetivo es cuidar que los equipos trabajen correctamente y tener planes de contingencia al momento de reportar algún tipo de daños, que pueden ser provocados o presentarse de forma imprevista y natural o cualquier problema que atente contra la infraestructura tecnológica.
- Usuario: personas que se sirven de la estructura tecnológica, medios de comunicación y son quienes administran la información; por ello,

se debe determinar las condiciones de protección en el sistema de manera que el uso de los datos por parte de los usuarios no ponga en riesgo la marcha normal de la empresa. La información, parte importante de la empresa y es la que se vulnera si no se cuenta con un sistema de seguridad adecuada; esta información se encuentra en la infraestructura computacional y es usada, alimentada y gestionada por los usuarios.

- La información: el factor más importante a cuidar en todas las organizaciones. Hace uso y se encuentra en la infraestructura tecnológica y el usuario dispone de la misma a su conveniencia en la mayoría de los casos.

1.2.7 Amenazas informáticas

Son las que atentan contra la infraestructura tecnológica o la información, o de manera combinada, con el afán de obtener algún tipo de beneficio o por el simple hecho de causar daño, en caso de las organizaciones tratar de eliminar la competencia, y eso tiende a convertirse en una lucha desleal que aunque parezca mentira se presenta en muchas partes del mundo y en el país no se lo considera como excepción.

Las amenazas pueden ser inevitables y no se las puede llegar a prevenir y es esa la escena en la que tiene que entrar en acción los diversos recursos de protección como la replicación de la información y no tenerla ubicada en un solo sitio, comúnmente a esto se le llama respaldos. Y es que se debe tener claro que las amenazas no solo son las creadas por personas que programan códigos con el ánimo de causar daño, o se presente por la falla de algún equipo de transmisión de datos que causan perdidas de datos irreparables, es por esto que se debe estar consciente que las amenazas que rodean los diferentes ambientes informáticos se presentan de diversas formas y maneras, provocadas, sin intención o premeditadas.

Tal es el ejemplo del espionaje industrial, algunos piratas persiguen un objetivo concreto, trabajan para una empresa de la competencia, incluso un país extranjero. Su objetivo es extorsionarle con datos estratégicos (su fichero de clientes, los contratos de los clientes, los datos sobre sus empleados, etc.) o paralizar su empresa para ayudar a la competencia (Royer, 2004, pág. 13)

La amenaza se puede dar inclusive a la interna de la organización, de manera inconsciente con el simple hecho de copiar información en algún medio extraíble y que la misma caiga en manos equivocadas y es este uno de los puntos que muy poco se trata por la confianza que se brinda al personal que se contrata en cada una de las organizaciones, y es imposible no mencionar los medios externos en la cuales entran en escena los programas maliciosos, errores intencionales en las programación, las intrusiones, etc., entonces dicho esto se podría clasificarlas según su origen por el daño que podrían causar a quien es objeto del ataque.

En su comunicación Seguridad de las redes y de la información propuesta para un enfoque político europeo, la Comisión de las Comunidades Europeas propuso la siguiente descripción de las amenazas contra los sistemas informáticos (Téllez Valdés, 2009, págs. 191-192)

- Acceso no autorizado a sistemas de información.
- Perturbación de los sistemas de información.
- Ejecución de programas informáticos perjudiciales que modifican o destruyan datos.
- Intercepción de comunicaciones.
- Declaraciones falsas.

Se debe añadir que, el ser parte de una amenaza informática directa o indirectamente incurre en el cometimiento de un delito informático en donde se puede llegar a violar el derecho a la privacidad y da pie al cometimiento de fraudes. Las amenazas se las puede clasificar por la gravedad que representan y de esta manera podemos presentar los más conocidos:

- Phishing**,** conocido como el envío de mails malicioso haciéndose

pasar como enviados por algún tipo de organización importante valiéndose de enlaces o direcciones que re direccionan al perjudicado a sitios falsos en los que se intenta adquirir información de cuentas bancarias, como claves y demás datos importantes que pueden derivar en pérdidas cuantiosas para el objeto del ataque.

- Falsificación de datos o tampering, conocido como modificar, borrar o alterar sin autorización los datos dentro de un programa.
- Scanning, es la búsqueda en diferentes medios escritos o digitales contenido especial para un interés en específico.
- Pharming o cambiazo, es cuando ingresando a través de los servidores de dominio de la organización se realiza un cambio en el direccionamiento cuando el usuario ingresa y los envía a sitios falsos similares al original.
- Skimming, en lo negativo conocido como la clonación de las tarjetas que se usan en los cajeros colocando dispositivos especiales encargados de obtener la información de las tarjetas usadas lo que permite crear tarjetas similares con las claves incluidas, el infractor procede a instalarlo en momentos de poca afluencia de público y se acerca a retirarlo cuando ya ha obtenido la información que desea, este tipo de casos ha disminuido por el hecho de la seguridad que se ha implementado en los cajeros como la instalación de cámaras a su alrededor para evitar el trabajo fraudulento en los mismos.
- Sniffing, técnica para robar información de una red o de un sitio en específico, utilizando técnicas de espionaje y camuflaje para poder ocultar su verdadera ubicación utilizando servidores que evitan se divulgue su punto exacto y la alteran la IP desde donde se está realizando el ataque para así desviar la atención del investigador del delito.

Como se lo menciono en párrafos anteriores existe el elemento externo que se encarga de causar el daño informático a las personas u organizaciones y también son sujetos que tienen como trabajo cometer delitos informáticos, y se los clasifica según el tipo actividad que desempeñan en cada ataque,

estos conocidos como los Hackers, Crackers, o simplemente intrusos, aprovechan sus conocimientos en tecnología para hallar las falencias de un sistema con el fin de dañar información u obtenerla y usarla para su conveniencia, pero así mismo existen malos con el ánimo de ser buenos encontrando falencias y alertando y malos con el ánimo de ser verdaderamente malos atacando con el único objetivo de dañar y se los puede clasificar así:

- Cracker, persona que sabe programar para hacer daño, sujetos que conocen el talón de Aquiles de muchos de los ambientes informáticos, y usan ese conocimiento para invadir cualquier tipo de sistemas, apropiándose de información privilegiada, de acceso exclusivo, para borrarla o hacer de ella lo que mejor les convenga y son personas muy inteligentes que tratan de causar daños morales y demostrar que muchas organizaciones no se preocupan por la protección de datos.
- Pirata informático, persona que obtiene, copia y distribuye información que no le pertenece de forma masiva con fin de obtener beneficios de tipo económicos sin el permiso de su autor o creador perjudicando al creador original de lo que ha sido objeto de copia, y este caso se presenta en lo que son los programas que usan las computadoras, música, videos y otros usando una computadora para cometer su delito.
- Spammer, son los que se encargan de distribuir correos comúnmente conocidos como no deseados a usuarios u organizaciones para hacer llegar algún tipo de promociones o estafas, por lo general es difícil detectar desde donde son enviados ya que utilizan diferentes tipos de servidores que pueden estar ubicados en cualquier parte del mundo los cuales pueden tener replicación en diferentes sitios.

1.2.8 Firewall

El concepto de firewall ha cambiado mucho en los últimos años, y ha dejado de ser algo tan simple como filtrado por origen, destino y puertos, para pasar

a abarcar equipos o aplicaciones muchísimo más granulares, que, incluso llegan a inspeccionar el contenido de los paquetes que pasan a través de ellos e interpretan los protocolos utilizados para la comunicación. Es por eso que debemos aprovechar al máximo estas nuevas capacidades, para incluirlas dentro de nuestras medidas de protección (Portantier, 2012, pág. 84)

El firewall es el equipo o programa que interactúa con los equipos de una organización para evitar las intrusiones o accesos no permitidos a un servidor o equipos dentro de una red privada, ayudando también a controlar y asignar accesos permitidos previamente definidos. El mismo permite poner límites en los accesos, controlar tráfico de información, usuarios, y a su vez emite informes con el fin de tener un control general de la o las redes que puede manejar una compañía.

Se denomina cortafuegos a un sistema de seguridad desarrollado para ubicarse entre una red pública, generalmente Internet, y una red interna perteneciente a una organización, o bien entre diferentes secciones de una red interna. El cortafuegos está compuesto de una colección de elementos (equipos, programas…) que controlan el tráfico entre dos redes, autorizando o impidiendo su tránsito de una a otra, según la serie de criterios de seguridad que se hayan definido (España Boquera, 2003, pág. 295)

Los Firewalls se los pueden implementar en soluciones de hardware o software o la combinación de los 2 y se lo usa en las organizaciones para proteger la información privada de la empresa a la cual los usuarios del internet no deben de tener libre acceso. El firewall se encarga de revisar todo lo que entra y sale de la organización en relación a paquetes de datos transmitidos y también es común utilizar la red llamada zona desmilitarizada en la cual se ubican los servidores de la organización que ofrecen servicios y necesitan tener comunicación sin interrupción con el exterior.

Tener configurado correctamente un firewall da una protección necesaria a la red mas no se debe de considerar suficiente, y para ello se debe realizar pruebas de vulnerabilidad periódicamente.

El firewall es una de las herramientas que existen para defenderse de los ataques, pero el sentido común también desempeña un papel fundamental para ganar la batalla a los atacantes. Para comenzar, es necesario saber en realidad que se necesita y se desea compartir, y a partir de allí si surge algún tipo de amenaza, será fácil detectarla debido a la comprobación rápida que se podrá realizar debido a lo que inicialmente pudo haber designado el encargado de la protección.

Muchos de los sistemas operativos, como Windows, incluyen algunos firewall de software de tipo básico. Estas soluciones “gratuitas” sólo ofrecen una protección mínima y no se deben confundir con las soluciones de firewall de hardware o software integrales con varias funciones de seguridad sofisticadas. Por ejemplo, estos firewall básicos no impiden ni verifican las transmisiones de datos desde un disco duro o medio extraíble de almacenamiento de información.

Firewall es un dispositivo de hardware (que puede ser una computadora configurada para esta tarea en particular, que corra software de firewall o un dispositivo dedicado de firewall que contenga una computadora dedicada) que se instala entre las dos redes y refuerza las políticas de seguridad (Hallberg, 2007, pág. 76)

Así como el firewall evita y bloquea el acceso de personas o aplicaciones a la red privada, se le hace difícil e imposible combatir varios puntos que salen fuera de su alcance, tales como el espionaje interno que va de la mano con las personas que están dentro de la organización, las configuraciones erróneas en los servicios, el tráfico que no pasa a través de la herramienta de firewall, o los virus que pueden infectar los equipos de la organización.

1.2.8.1 Firewall de hardware

Es el equipo físico que tiene un software especializado y configurable el cual es instalado entre la red interna y el exterior. Si se configura correctamente el equipo de firewall físico constituye una pared que protege y mantiene ocultos los equipos de una compañía con respecto al exterior. También se puede utilizar como pantalla entre las dependencias o departamentos de una misma organización.

Los firewall de hardware son soluciones idóneas para organizaciones que desean que un mismo techo de protección cuide varios espacios informáticos.

El aspecto negativo de este tipo de equipos es que como se trata de herramientas especializadas, los cortafuegos de hardware suelen ser costosos, complejos, difíciles de escalar y algo complicados a la hora de configurarlos. En otras palabras, están orientados para administradores de TI que cuentan con el conocimiento necesario para administrar este tipo de equipos.

Los proveedores de internet ofrecen una especie de firewall de hardware de bajo costo, que están incluidos dentro del ruteador que ofrecen para el hogar pero al igual que los de alto costo poseen sus limitantes como dejar de proteger un equipo portátil que se aleja del radio de cobertura del firewall.

1.2.8.2 Firewall de Software

Los firewall de software están orientados al uso personal o para las pequeñas organizaciones que poseen conexiones de banda ancha no muy amplias. En lugar de adquirir un equipo de hardware personalizado y caro, se opta por conseguir firewall de software el mismo que se implementa en cada equipo de la red organizativa, y esto incluye equipos servidores, equipos de escritorio o equipos móviles.

Actualmente, todos los sistemas operativos cuentan con sistemas de firewall, ya sea para servidores o para estaciones de trabajo. Tanto Windows Firewall (sistemas Windows), como IPTables (sistemas GNU/Linux) y PF (sistemas OpenBSD) son excelentes herramientas para bloquear los puertos de nuestros sistemas a los que se puede acceder desde la red. En el caso de las plataformas Microsoft, podemos encontrar varias soluciones que intentan reemplazar al firewall incluido por defecto. En este caso deberemos analizar qué ventajas y desventajas podría traernos implementarlas. En los sistemas Windows, es posible realizar excelentes configuraciones a través de Active Directory, para mantener un estándar de puertos permitidos. Con esto nos aseguramos de bloquear algunos de los ataques más comunes realizando un esfuerzo mínimo (Portantier, 2012, págs. 122-123)

Inclusive se podría contar con una protección combinada en el caso que una organización disponga de firewall de hardware, ya que sería una buena opción que los usuarios tengan firewall de software instalado en cada uno de sus equipos. Esto resulta verdaderamente útil para los usuarios que usan laptop o algún otro equipo móvil, que necesitan seguridad digital cuando trabajan fuera de la red corporativa. Cabe mencionar otra de las ventajas importantes de los firewall de software y es que se pueden escalar de una forma ágil debido a que los usuarios de los equipos sólo deberían descargar los parches, soluciones, actualizaciones y mejoras desde el sitio web del proveedor del software de protección o bien el distribuidor de la herramienta se encargaría de hacer llegar la información acerca de las novedades con respecto al producto adquirido.

1.2.9 Antivirus

Un antivirus es un programa de computación que tiene como propósito detectar y eliminar virus y otros programas que pueden causar daño antes o después de ingresar a los equipos de la organización.

Otro medio de defensa frente a las invasiones a través de las conexiones de red es el denominado software antivirus, que se utiliza para detectar y eliminar virus conocidos y otras infecciones (en la práctica, el software antivirus representa una amplia clase de productos de software, cada uno de ellos diseñado para detectar y eliminar un tipo específico de infección. Por ejemplo, mientras que muchos productos se especializan en el control de virus, otros están especializados en la protección frente al software espía). Es importante que los usuarios de estos paquetes entiendan que, al igual que en el caso de los sistemas biológicos, continuamente están apareciendo en escena nuevas infecciones de computadora, las cuales requieren vacunas actualizadas. Por tanto, el software antivirus debe de contar con un mantenimiento periódico, consistente en descargar actualizaciones proporcionadas por el fabricante del software. Sin embargo, ni siquiera esto garantiza la seguridad de una computadora. Después de todo, cada nuevo virus que aparece debe primero infectar algunas computadoras antes de ser descubierto y antes de que se pueda crear una vacuna. Por tanto, los usuarios inteligentes nunca abren adjuntos de correo electrónico procedentes de fuentes desconocidas, ni tampoco descargan software sin confirmar antes su fiabilidad, ni responden a los anuncios que aparecen en ventanas emergentes, ni dejan un PC conectado a Internet cuando esa conexión no es necesaria (Brookshear, Smith, & Brylow, 2012, págs. 211-212)

Un antivirus puede complementarse con otras aplicaciones de seguridad como firewalls o anti-spyware que cumplen funciones complementarias para evitar el ingreso de virus.

Los mejores programas antivirus o, mejor dicho, antimalware, no solamente cubren el código malicioso sino también la acción de los intrusos informáticos, el spam y los intentos de phishing. Algunos incorporan utilidades específicas para la navegación, como por ejemplo cortafuegos (Aguilera López, 2010, pág. 130)

1.2.10 Ética Hacker

Concepto conocido como el acceso libre a la información por medio de técnicas y procedimientos para vulnerar todo tipo de seguridades impuestas en un sector determinado, por parte de una persona o personas que usan sus conocimientos avanzados en informática y seguridad, para luego de esto reportar cada una de las vulnerabilidades encontradas con el objetivo de que se tomen medidas en un lapso corto de tiempo, y este tipo de pruebas no causan ningún tipo de daño a la organización.

La idea de este tipo de técnicas es conocer que elementos dentro de una red son vulnerables con el fin de corregir antes de que se presenten intrusiones o acceso no autorizado y esto derive por ejemplo en el robo de información. A este tipo de pruebas se las llama como "pruebas de penetración", en donde se intenta de múltiples formas burlar la seguridad de la red para intentar obtener información que es exclusiva de la organización a la que se le realiza la prueba, para luego elaborar un reporte y enviarlo a dicha organización y de esta manera contribuir de una manera responsable al cuidado de la información que posee cada compañía.

Se sugiere a las empresas contratar servicios de pruebas de hacking ético de forma periódica ya que en la tecnología todo evoluciona y la forma de atacar hace lo propio. Hay compañías especializadas en este tipo de pruebas que poseen certificaciones emitidas por entidades u organizaciones reconocidas a nivel mundial. Las personas que hacen estas pruebas pueden llegar a ver información confidencial, por lo que se necesita de total profesionalismo por parte del consultor.

Existen numerosas técnicas de ataque, que se aplican a diferentes entornos (como SQL Injection y Cross Site Scripting); y diversos conceptos que debemos de tener en mente, como la evasión de medidas de seguridad (firewalls, IDS, etc.). Por lo tanto es necesario que nos mantengamos constantemente capacitados y leyendo acerca de las nuevas técnicas y

herramientas que aparecen en el mercado. El Ethical Hacking debe ser bien conocido por todo buen profesional de la seguridad informática (Portantier, 2012, pág. 181)

En el centro de nuestra era tecnológica se hallan unas personas que se autodenominan hackers. Se definen a sí mismos como personas que se dedican a programar de manera apasionada y creen que es un deber para ellos compartir la información y elaborar software gratuito. No hay que confundirlos con los crackers, los usuarios destructivos cuyo objetivo es el de crear virus e introducirse en otros sistemas: un hacker es un experto o un entusiasta de cualquier tipo que puede dedicarse o no a la informática. En este sentido, la ética hacker es una nueva moral que desafía la ética protestante del trabajo, tal como la expuso hace casi un siglo Max Weber en su obra La ética protestante y el espíritu del capitalismo, y que está fundada en la laboriosidad diligente, la aceptación de la rutina, el valor del dinero y la preocupación por la cuenta de resultados. Frente a la moral presentada por Weber, la ética del trabajo para el hacker se funda en el valor de la creatividad, y consiste en combinar la pasión con la libertad. El dinero deja de ser un valor en sí mismo y el beneficio se cifra en metas como el valor social y el libre acceso, la transparencia y la franqueza (Pekka, 2002, pág. 2)

1.3 FUNDAMENTACIÓN LEGAL

Cuando se realiza el diagnóstico de la seguridad que ofrecen los firewall no se debe de obviar las implicaciones legales que se podrían presentar al momento de vulnerar la protección de los mismos y las leyes ecuatorianas contemplan sanciones para las infracciones que podrían cometerse por medio por medio del computador.

En la ley orgánica de comunicación publicada en el registro oficial # 22 tercer suplemento del 25 de junio del 2013, no se encuentra referencia relacionada con el objeto de estudio del presente trabajo. Sin embargo, en el artículo 202, 353, 415 y 553 del código penal ecuatoriano vigente a febrero del 2014

se puede evidenciar la severidad de la ley que castiga la difusión de datos personales sin autorización, la pena puede llegar acarrear hasta 2 años de prisión.

En el siguiente cuadro se describe las infracciones, la pena carcelaria y pecuniaria si se llega a determinar el cometimiento de delitos informáticos de cualquier índole:

	Sanción Carcelaria	**Sanción Pecuniaria**
Art. …: Delitos Contra La Información Protegida (Art. 202 Cp): 1.- Violentando claves o sistemas.	6 meses a un año	US$500 a US$1.000
2.- Información obtenida sobre la seguridad nacional, secretos comerciales o industriales.	3 años	US$1.000 a US$1.500
3.- Divulgación o utilización fraudulenta de los rubros anteriores.	3 a 6 años	US$2.000 a US$10.000
4.-Divulgación o utilización por funcionarios a cargo de dicha información.	6 a 9 años	US$2.000 a US$10.000
5.- Obtención y uso no autorizados de datos personales para cederla o utilizarla.	2 meses a 2 años	US$1.000 a US$2.000
Art. …: Falsificación Electrónica (Art. 353 Cp): 1.- Alterar un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial; 2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad; 3.- Suponiendo en un acto de intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieran hecho.	Serán juzgados de acuerdo a lo que se dispone en este capítulo, 6 a 9 años de reclusión menor	Xxx
Art. …: Daños Informáticos (Art. 415 Cp) Según: 1.- Daño doloso de información contenida en un sistema.	6 meses a 3 años	US$60 a US$150
2.- Programas, datos, base de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculado a la defensa nacional.	3 a 5 años	US$200 a US$600

3.- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de infraestructura para la transmisión.	8 meses a 4 años	US$200 a US$600
Art. …: Apropiación Ilícita (Art. 553 Cp) Según Lo Siguiente: 1.- Los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de esta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensaje de datos.	6 meses a 5 años	US$500 a US$1.000

Tabla # 1. Fuente.- (Procuraduria General del Estado, 2013)

La o las personas que abren una cuenta falsa en Twitter de otra persona con el fin de causar daño o mal informar a los seguidores pudieran estar en problemas legales, porque aquello podría tipificarse como usurpación o plagio de identidad. Los que abren una cuenta en cualquier red social que no es la suya y sin permiso de su verdadero creador, también están incurriendo en el delito mencionado anteriormente. Inclusive los que intercambian mensajes en correos electrónicos particulares podrían ser sometidos a juicio por injurias, si se detecta que en alguna parte de la comunicación hubo frases que puedan afectar directa o indirectamente la integridad moral de una persona.

De hecho, se conoce que ya se han presentado casos de injurias a través de medios informáticos y es por ello que la secretaria de comunicación ha está tomando medidas en contra de la divulgación y emisión de mensajes ofensivos hacia personas naturales o jurídicas pero a su vez existen trabas por el hecho de la mala interpretación del derecho a la libre expresión. Todo esto constituye una porción de la variedad de delitos informáticos que contempla el código penal del Ecuador y que ya están siendo sancionados

por la fiscalía del Guayas, con lo que hay una nueva legislación en un área que es muy importante en la actualidad a nivel mundial.

Se ha podido conocer a través de la prensa de televisión y escrita que son muchas las denuncias presentadas por el cometimiento de los delitos informáticos en donde el robo de claves, y estafas electrónicas tienen el principal protagonismo. Existen organizaciones delictivas dedicadas a este tipo de ilícitos con el fin de obtener un lucro económico. En el país operan hackers procedentes de distintas partes del mundo que colaboran al crecimiento antisocial de las personas del país.

Actualmente existe una poderosa organización de hackers autodenominada Anonymous que se desarrolla en varias partes del mundo, la cual está en contra de varias organizaciones en general y su lucha supuestamente es a favor de la libertad de expresión, inicio sus operaciones como un simple juego pero luego se expandió tanto que muchos hackers tratan de formar parte de esa organización y utilizan su figura o imagen en el cometimiento de delitos. No se conoce su creador ni quienes la componen pero gozan de vastos conocimientos para realizar ataques a través de la red y fuera de ella.

CAPÍTULO II

MARCO METODOLÓGICO

“Ya que las ciencias particulares dejan sin tratar algunas cosas que necesitan investigación, se hace necesaria la existencia de una ciencia universal y primera que estudie esas cuestiones de las que no se ocupan las ciencias particulares.” (Santo Tomas de Aquino).

Para llevar a cabo una investigación confiable se debe aplicar la metodología de acuerdo a las características del trabajo y el entorno en el que será realizado para para cumplir con los objetivos planteados.

2.1 TIPO DE INVESTIGACIÓN

Este trabajo se lo realizará en base al método cuantitativo usando la recolección de datos por medio de las encuestas para conocer la posición de las compañías asesoras y productoras de seguros y de los proveedores frente a las necesidades de seguridad que pueden presentar, para probar la hipótesis, con base en la medición numérica y el análisis estadístico, para establecer patrones de uso y poder probar la teoría de que en algún momento puede ser atacado (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2010, pág. 4)

Para obtener resultados que ayuden con los objetivos de esta investigación se inicia con un análisis de los problemas en seguridad informática que se pueden presentar a diario en las empresas con los cuales se podrá identificar las características necesarias de los equipos de firewall que existen en el mercado ecuatoriano para luego analizar las necesidades en común que presentan las agencias productoras y asesoras de seguros de Guayaquil utilizando encuestas de los puntos a tomar en cuenta por parte del tipo de empresas antes mencionadas y luego de los resultados que se obtuvieron de dichas encuestas realizar las consultas y cuestionamientos necesarios a los proveedores de firewall para finalmente elaborar una

propuesta o modelo que sirva como solución básica y general a los problemas de seguridad de los bróker de seguros.

Se puede destacar, rápidamente, que los análisis cuantitativos son más exactos y más fáciles de entender por la gerencia, pero requiere un trabajo muchísimo mayor y una gran cantidad de cálculos (Portantier, 2012, pág. 37)

Dicho esto se puede determinar que este método permite un mejor análisis costo-beneficio, es más entendible a para las altas gerencias y puede automatizarse.

Las investigaciones se originan por ideas, sin importar qué tipo de paradigma fundamente el estudio ni el enfoque que se habrá de seguir. Para iniciar una investigación siempre se necesita una idea; todavía no se conoce el sustituto de una buena idea. Las ideas constituyen el primer acercamiento a la realidad objetiva (desde la perspectiva cuantitativa), a la realidad subjetiva (desde la perspectiva cualitativa) o a la realidad intersubjetiva (desde la óptica mixta) que habrá de investigarse (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2010, pág. 26)

2.1.1 Variables

Las variables se establecen de acuerdo a la influencia de unas sobre otras siendo las mismas dependientes e independientes y se las detalla a continuación:

Variables independientes:

- Análisis: Se realizará estudio minucioso de lo que pueden llegar a ofrecer los firewalls.
- Firewall: Objeto a evaluar con el fin de obtener un beneficio.
- Manejo confiable: Lo que se espera con la ayuda del objeto a revisar.

Cumpliendo las variables independientes se busca satisfacer las variables dependientes propuestas a continuación:

Variables dependientes:

- Solución referencial: Lo que se desea obtener de la investigación a realizar.
- Aplicable: Solución que pueda servir a las organizaciones que forman parte del universo que se ha designado.

2.2 DELIMITACION DE ESTUDIO

La ciudad de Guayaquil cuenta con aproximadamente 120 agencias productoras y asesoras de seguros según el registro la Superintendencia de Bancos y Seguros del Ecuador.

El diagnóstico de la seguridad que ofrecen los firewalls se realizará en un lapso de 4 meses tiempo en el cual se realizarán encuestas para conocer la necesidad de estas empresas y qué punto consideran como esencial proteger ante posibles ataques para de esta manera tener claro el fin de la mencionada investigación. No sólo ayudará a prevenir intrusiones sino también a tener control total centralizado y organizado de la red empresarial.

En este trabajo no se incluirá el estudio de la ingeniería social como parte de las amenazas actuales, el correcto uso de VPN, no se implementará nuevas soluciones antivirus, o herramientas que estén relacionadas a la seguridad física del sitio, como la seguridad perimetral que se pueda implementar en las instalaciones de la organización, el enfoque está direccionado a la información como tal y los medios que se usan para su difusión y compartición. No se realizarán manuales ni guías para usuarios pero las políticas de seguridad básicas que se formulen en esta investigación servirán como referencia en la implementación del firewall que cada organización esté dispuesta a realizar, y serán documentadas como puntos a tomar en consideración para los Departamentos de T.I. de las diferentes

organizaciones con el fin de que puedan tener un control total de la red empresarial y que pueda ser administrado de una forma ágil y segura.

2.3 POBLACION Y MUESTRA

La población objeto de esta investigación está constituida por 120 compañías asesoras y productoras de seguros de la ciudad de Guayaquil a la cual esa orientada esta investigación y 5 proveedores de firewall de Guayaquil y Quito.

Para esta investigación se realizará un muestreo intencional en el cual se seleccionará 40 compañías de las 120 registradas en la Superintendencia de Bancos y Seguros del Ecuador en la ciudad de Guayaquil, y las mismas se encuentran entre las mejores posicionadas según el ranking de comisiones del 2012 que se publica en la página web del ente regulador. (Superintendencia de Bancos y Seguros del Ecuador, 2014)

Con respecto a los proveedores de Firewall se consultará a los 5 mencionados los cuales tienen sus oficinas en Guayaquil o Quito y son los más reconocidos por no solo ofrecer el producto puesto que también ofrecen el servicio de soporte y capacitaciones. Hay otros proveedores que venden los equipos pero no dan capacitaciones e indican que se debe comunicar directamente al fabricante en caso de presentarse algún inconveniente con el equipo.

En el muestreo intencional todos los elementos muestréales de la población serán seleccionados bajo estricto juicio personal del investigador. En este tipo de muestreo el investigador tiene previo conocimiento de los elementos poblacionales. Aunque este muestreo es subjetivo, requiere que el investigador conozca los elementos muestréales, lo que permite que el muestreo sea representativo. (Namakforoosh, 2005, pág. 189)

Se puede concluir que es una muestra con propósito, entonces se decide elegir un grupo específico de personas u objetos dentro de una población para realizar el análisis por parte del investigador. El grupo elegido a menudo es el que ofrece la mayor parte de la información a la investigación.

Se utiliza este tipo de muestreo dado que en el muestreo aleatorio simple toda la población que compone el universo tiene la misma probabilidad de ser elegido pero en este caso se elige a las empresas más representativas de la ciudad y en las cuales posiblemente se podrían centrar ataques informáticos. El negocio de las compañías asesoras y productoras de seguros es actuar como intermediario la aseguradora y el cliente de tal forma que pesa sobre este tipo de empresas la responsabilidad de llegar a un acuerdo entre las dos partes, con el fin de que el cliente llene sus expectativas en cuanto a las necesidades que presenta por medio de un programa de seguros propuesto por la aseguradora.

El bróker cumple la función de asesorar al cliente que quiere asegurar sus bienes proporcionándole información acerca de los beneficios que puede ofrecer cada una de las aseguradoras, es por ello que la compañía productora y asesora de seguros es la que realiza la inspección de los riesgos que se pudieran presentar, ya que con esta información puede llegar al cliente y notificarle cual es el producto que se ajusta al tipo de riesgo que presenta y necesidades descritas inicialmente, contemplando todo lo que respecta un contrato de seguros entre ellos coberturas y clausulas.

La agencia productora y asesora de seguros es la llamada a confirmar que los reclamos sean pagados acorde a las clausulas determinadas inicialmente en el contrato con el objetivo de que cliente este conforme con el seguro que firmo.

2.4 TÉCNICAS E INSTRUMENTOS PARA OBTENER LA INFORMACIÓN

Se utilizarán técnicas cuantitativas en las cuáles se hará uso de las encuestas y las entrevistas.

La entrevista será semiestructurada puesto que se desea semejar un encuentro tipo charla donde la persona entrevistada (proveedor) pueda explayarse con libertad acerca de los Firewall, exponer sus características y todos los servicios que puede ofrecer en el mercado guayaquileño. Luego de la misma se entregará al proveedor una lista de necesidades básicas que se derivan del resultado del análisis previo de las encuestas a las compañías productoras y asesoras de seguros y el proveedor emitirá su mejor propuesta de firewall en la cual se expondrán cuantos de los requerimientos cumple su equipo o propuesta.

De la entrevista se determinará si los firewalls que ofrecen los proveedores siguen los lineamientos que desean las compañías asesoras y productoras de seguros y se ajustan a los mismos, con el fin de alcanzar un nivel de satisfacción en las organizaciones luego de los resultados a presentarse.

Las encuestas están realizadas con preguntas de opción múltiple y se enfocan en lo que piensan y opinan los administradores de las compañías asesoras y productoras de seguros, y la realidad actual que presentan las mismas en su infraestructura tecnológica para de allí partir con la investigación, análisis y propuesta base de solución o mejoras a problemas de seguridad informática.

Para la realización de la entrevista se contará con los puntos principales a tomar en cuenta al momento que un bróker de seguros desea elegir un firewall por ejemplo precio, características, certificaciones, mantenimiento, instalación, etc.

2.5 TRATAMIENTO DE LA INFORMACION

En esta etapa se refiere al procesamiento de la información recolectada por medio de los instrumentos mencionados en el punto anterior.

Los datos serán recogidos en papel e información de tipo digital. La organización de la información será realizada a través de Excel para realizar gráficos estadísticos que ayuden a realizar el análisis cuantitativo de la información mediante la categorización de las variables y el análisis del contenido obtenido.

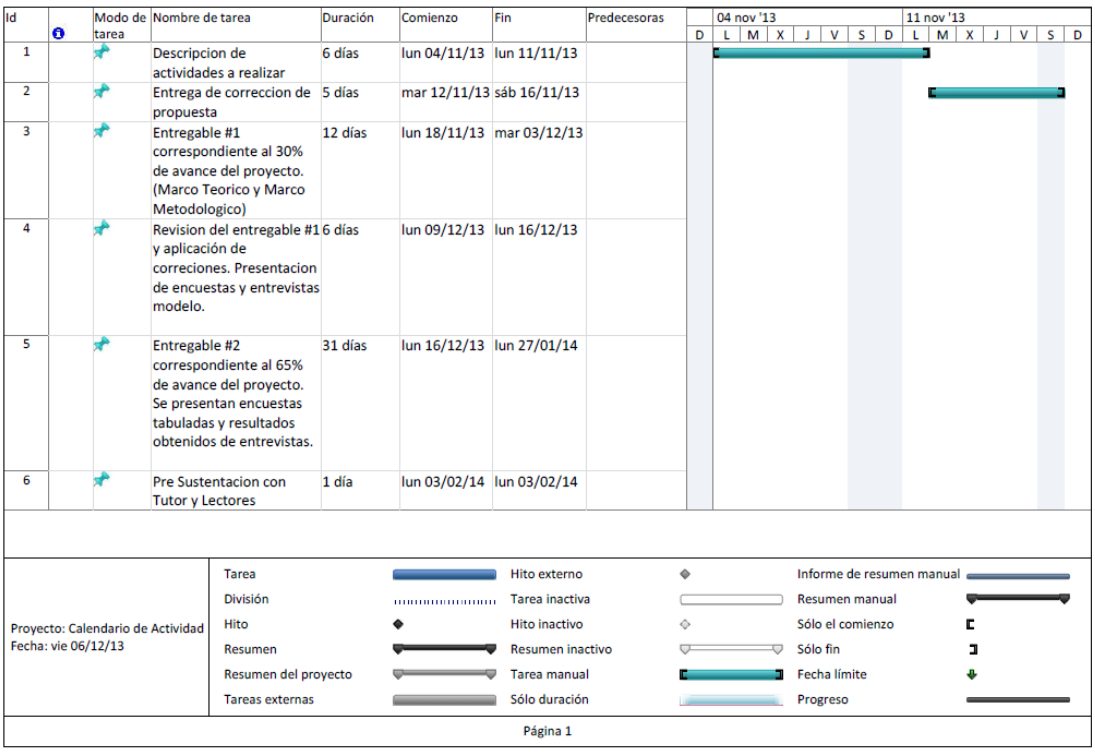
La información que se desea obtener está enmarcada en el nivel de facilidad que necesitan tener las compañías asesoras y productoras de seguros al momento de adquirir un nuevo firewall, realizar pruebas, y establecer un estándar en políticas de seguridad.

2.6 PLAN DE TRABAJO

Con el fin de organizar el desarrollo de este proyecto, se estableció las medidas de tiempo y cumplimiento de manera que se obtenga la finalización del trabajo. La distribución del cronograma de actividades con su tiempo aproximado se presenta en el diagrama de Gantt.

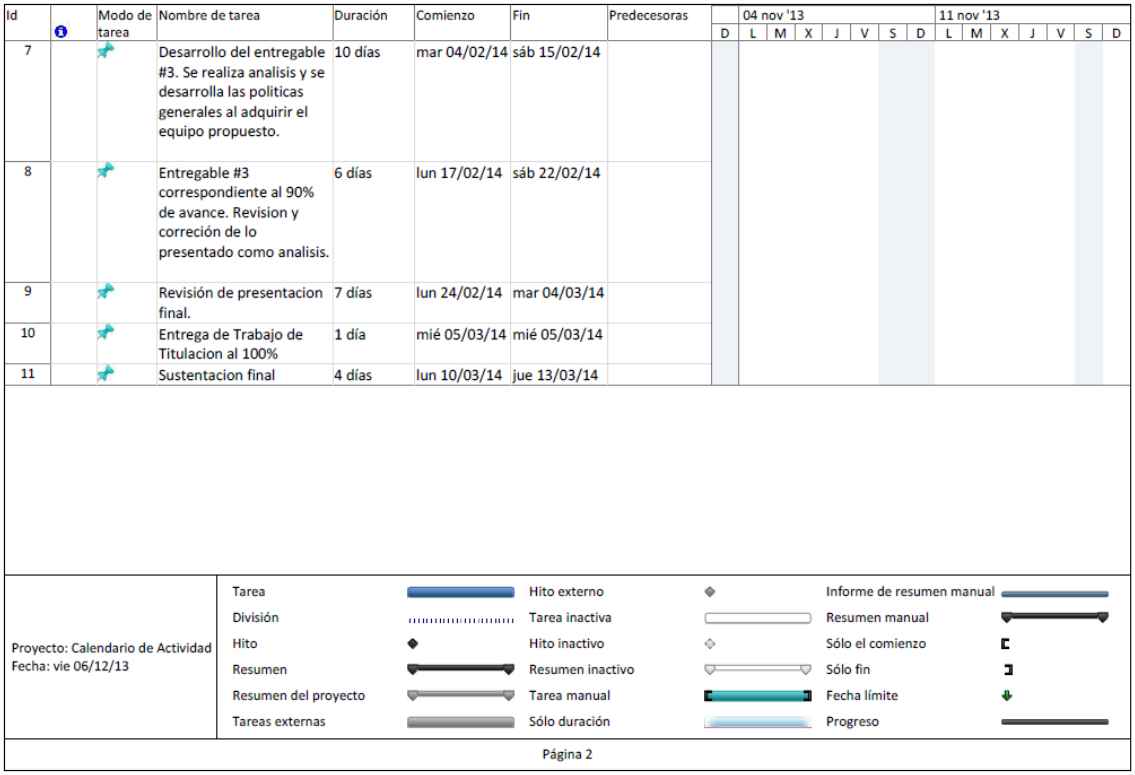
La realización de la investigación tomó aproximadamente 4 meses en el cual se toma en cuenta las fechas de entrega estipuladas al inicio del proceso de titulación. No se consideró las variaciones y modificaciones que tuvo el calendario ya que la fecha de culminación del proceso de titulación no llevo consigo ninguna alteración.

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1		Descripcion de actividades a realizar	6 días	lun 04/11/13	lun 11/11/13	
2		Entrega de correccion de propuesta	5 días	mar 12/11/13	sáb 16/11/13	
3		Entregable #1 correspondiente al 30% de avance del proyecto. (Marco Teorico y Marco Metodologico)	12 días	lun 18/11/13	mar 03/12/13	
4		Revision del entregable #1 y aplicación de correciones. Presentacion de encuestas y entrevistas modelo.	6 días	lun 09/12/13	lun 16/12/13	
5		Entregable #2 correspondiente al 65% de avance del proyecto. Se presentan encuestas tabuladas y resultados obtenidos de entrevistas.	31 días	lun 16/12/13	lun 27/01/14	
6		Pre Sustentacion con Tutor y Lectores	1 día	lun 03/02/14	lun 03/02/14	

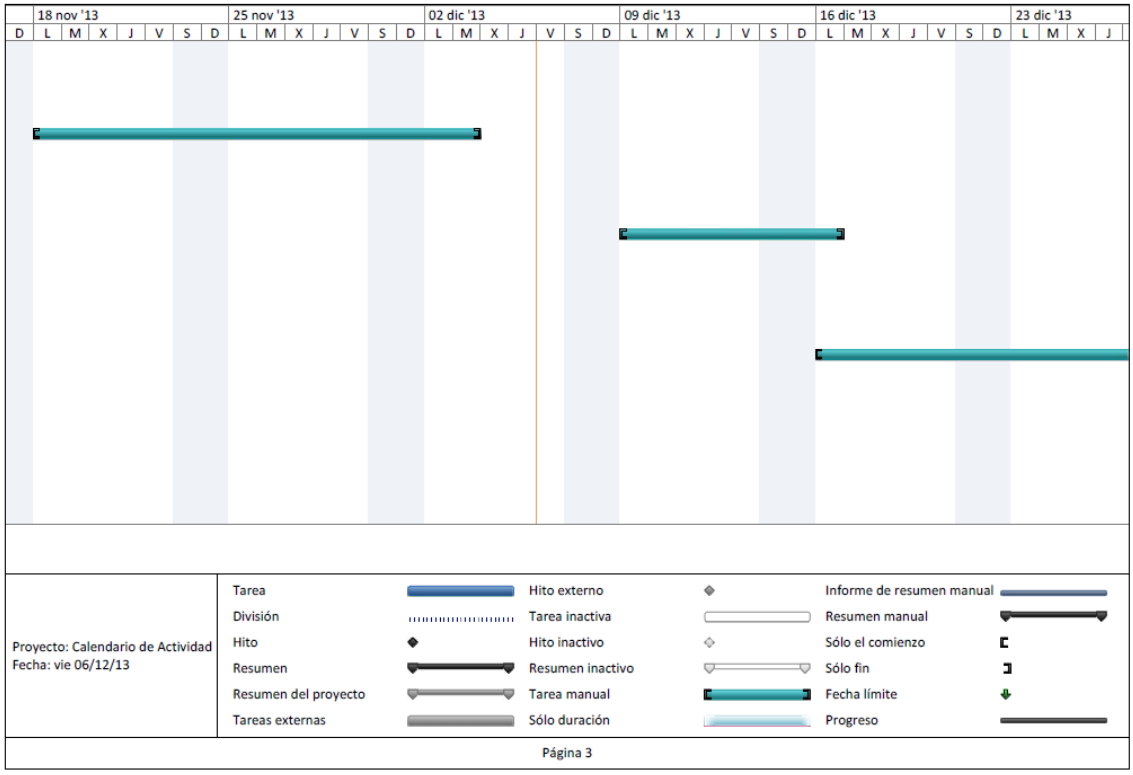


Página 1

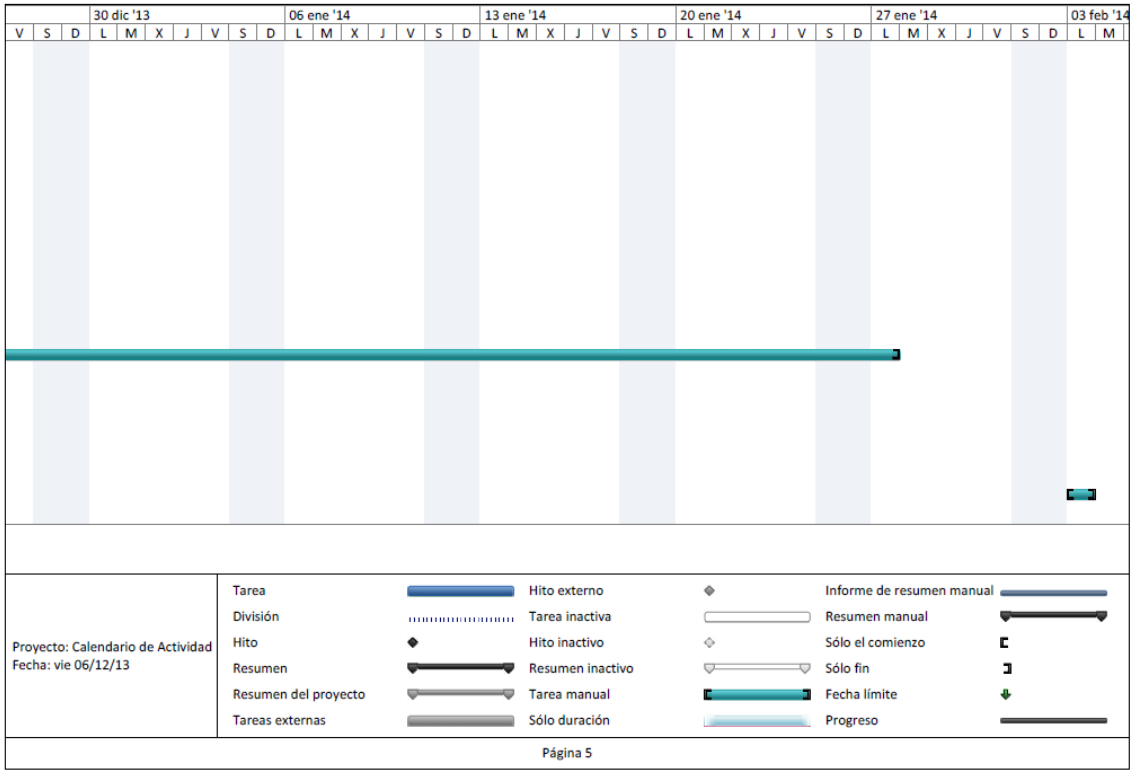
Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
7		Desarrollo del entregable #3. Se realiza analisis y se desarrolla las politicas generales al adquirir el equipo propuesto.	10 días	mar 04/02/14	sáb 15/02/14	
8		Entregable #3 correspondiente al 90% de avance. Revision y correción de lo presentado como analisis.	6 días	lun 17/02/14	sáb 22/02/14	
9		Revisión de presentacion final.	7 días	lun 24/02/14	mar 04/03/14	
10		Entrega de Trabajo de Titulacion al 100%	1 día	mié 05/03/14	mié 05/03/14	
11		Sustentacion final	4 días	lun 10/03/14	jue 13/03/14	



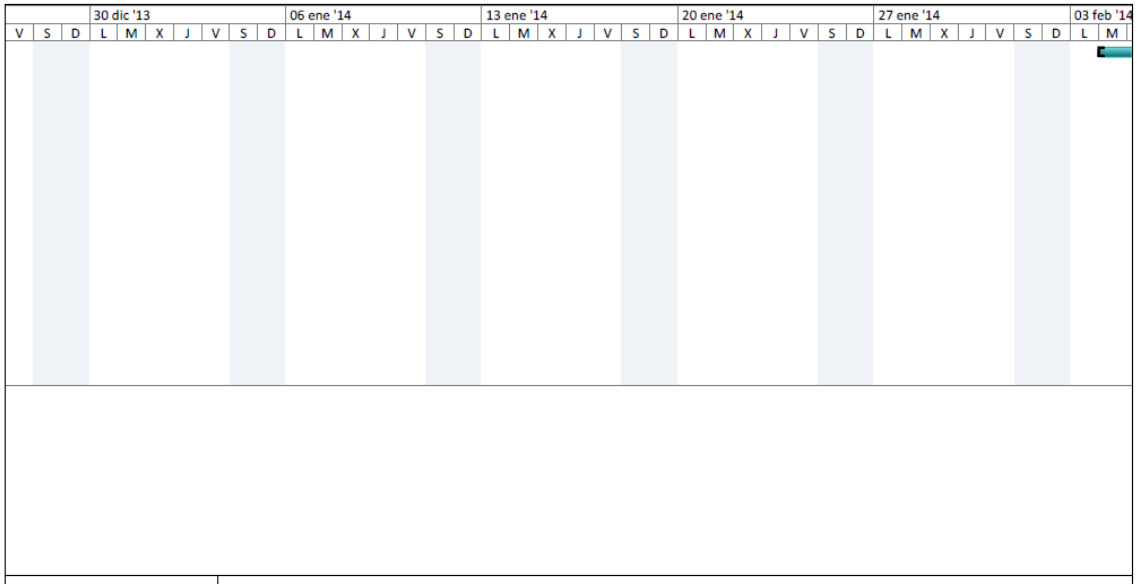
Página 2



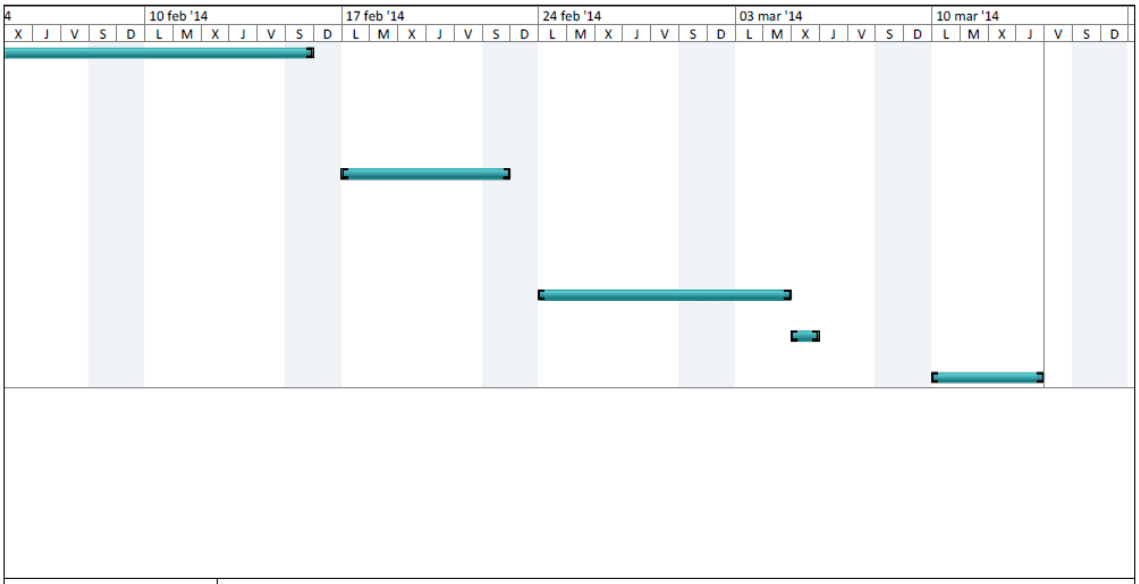
Página 3



Página 5



Página 6



Página 8

CAPÍTULO III

ANÁLISIS DE LOS RESULTADOS

En este capítulo se presenta el resultado de las encuestas realizadas al personal encargado de las compañías productoras y asesoras de seguros y a los que administran o se encargan del departamento de tecnología.

También se presenta los resultados de las entrevistas a los proveedores en las que los mismos presentan sus respectivas propuestas para equipamiento de los bróker de seguros en el ámbito de seguridad informática.

La importancia de los resultados radica en la información obtenida gracias a los instrumentos y técnicas de investigación utilizados que permiten elaborar un análisis concreto de las necesidades que presentan las organizaciones y con ello tener claro el panorama para la presentación de una solución que logre satisfacer dichas necesidades y poder proteger la información que es lo primordial para las compañías.

En relación a las encuestas dirigidas a los bróker de seguros se puede destacar la siguiente información:

- Número de personas que laboran en la organización.
- Información importante a proteger.
- Conocimiento de amenazas e intención de mejoras para la seguridad informática de la organización a la que pertenecen.
- Presupuesto para la inversión en el área de informática.
- Equipamiento actual en lo que respecta a seguridad informática.
- Soluciones tecnológicas que emplean en la actualidad y con cuales les gustaría contar.
- Como se realiza el análisis de las vulnerabilidades.
- Planes de protección ante situaciones que se presentan a diario.
- Presencia o ausencia de políticas de seguridad.

Y con respecto a las entrevistas a los proveedores se pudo conocer y determinar lo siguiente:

- Equipos con los que cuentan y pueden llegar a ofrecer a las organizaciones.
- Servicios que incluyen sus propuestas.
- Ventajas de los equipos en comparación a la competencia que existe en el mercado.
- Costos de inversión con respecto a las necesidades presentadas.

3.1 RESULTADOS DE LAS ENCUESTAS ORIENTADAS AL PERSONAL DE LAS AGENCIAS PRODUCTORAS Y ASESORAS DE SEGUROS DE LA CIUDAD DE GUAYAQUIL

Administradores de compañías.

1.- ¿Cuantas personas laboran actualmente en la organización?

Personas	Cantidad de Empresas
5 a 30	35
31 a 60	4
61 a 100	0
101 a 150	1
151 o mas	0

Tabla # 2. Fuente.- Autor

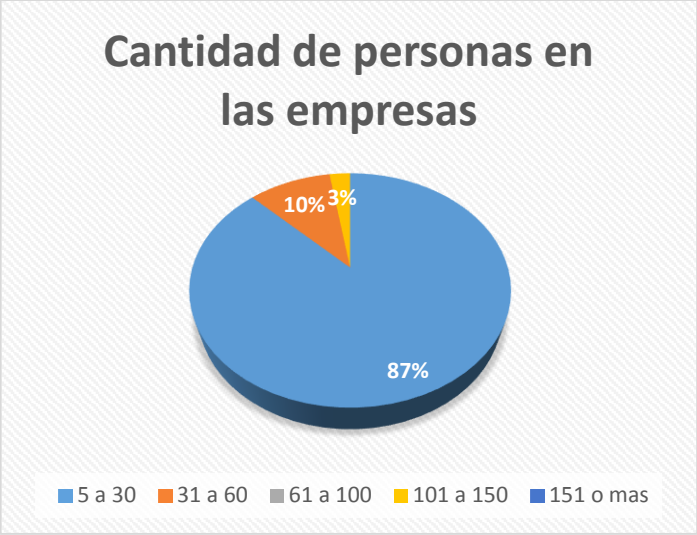


Gráfico # 2. Cantidad de personas en las empresas. Fuente.- Autor

Análisis.- En las compañías productoras y asesoras de seguros de Guayaquil se puede observar que la mayor cantidad de empresas encuestadas manejan el rango de "5 a 30 empleados" (35), es importante indicar que esta variable no considera la cantidad de clientes o cuentas que maneja cada una de ellas, pero representa un dato importante para asignar el tipo de seguridad en el ámbito informático que requieren para proteger la información que es manipulada.

2.- ¿Cómo considera usted a su ambiente de seguridad?

Pregunta 2	Insuficiente	Medio Suficiente	Suficiente	Ideal	Se podría mejorar
Ambiente de seguridad	0	3	20	2	15

Tabla # 3. Fuente.- Autor

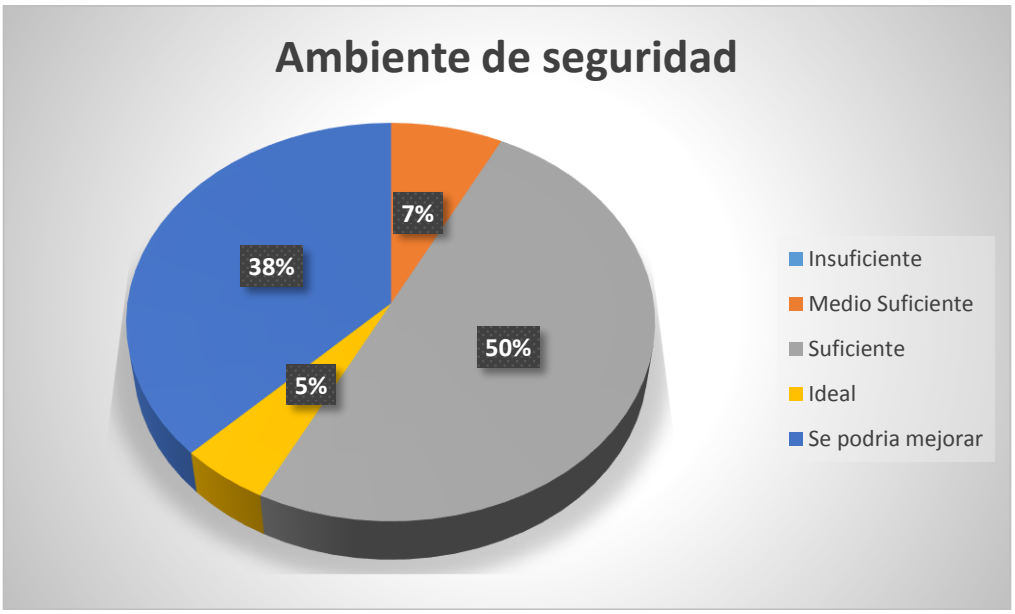


Gráfico # 3. Ambiente de seguridad. Fuente.- Autor

Análisis.- Muchas de las compañías encuestadas consideran que su ambiente de seguridad es suficiente para la actividad que realizan, sin embargo, el concepto "suficiente" (20) se encasilla en tener antivirus, tener alguien que revise los equipos cada cierto tiempo, o que sus equipos sean de última tecnología. Si bien consideran estar alertas a cualquier ataque, no los excluye de los mismos, por lo menos hasta que se ponga a prueba su seguridad actual y demuestren que tienen probabilidades de resistir las amenaza, aun cuando cuenten con equipos de seguridad especializados, pues solo 11 compañías de las encuestadas cuentan con personal de sistemas de planta y se ha podido conocer que están al pendiente de la seguridad informática de la organización. Sin embargo un valor nada despreciable indica que "se podría mejorar" (15) su seguridad ya que si bien la protección mejora también lo hacen las amenazas y la manera de atacar.

3.- Para la realidad actual de su compañía, considera usted que necesita tener un ambiente informático más seguro.

Pregunta 3	SI	NO
Mejorar ambiente informático	17	23

Tabla # 4. Fuente.- Autor

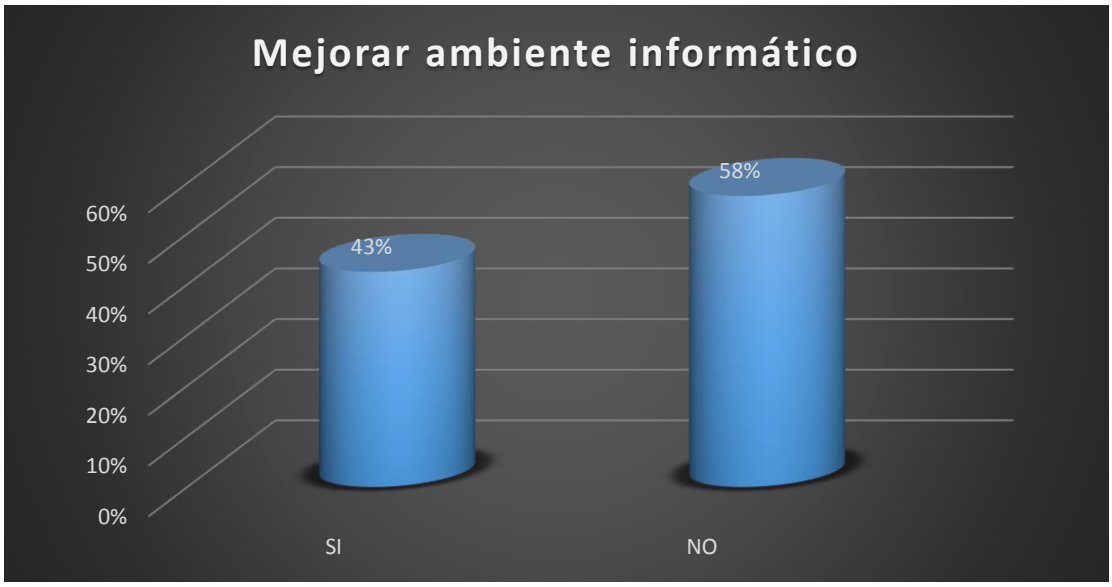


Gráfico # 4. Mejorar ambiente informático. Fuente.- Autor

Análisis.- Como se lo indica en esta pregunta muchas de las empresas consideran que la protección actual de su ambiente informático es suficiente y sustentan sus posturas a diversos factores, tales como:

- Consideran que se encuentran bien protegidos.
- La compañía no tiene un gran número de personal.
- El presupuesto asignado a ese rubro es muy pequeño.
- Consideran que no son un blanco directo de los piratas informáticos.

Sin embargo hay muchas empresas que consideran que podría mejorar su ambiente informático a corto plazo ya que tienen altas posibilidades de crecimiento empresarial, porque por cada negocio que ganan tienen más información y cliente que proteger.

4.- De acuerdo al grado de importancia clasifique ¿Que datos considera usted como sensibles y que no quisiera perder?

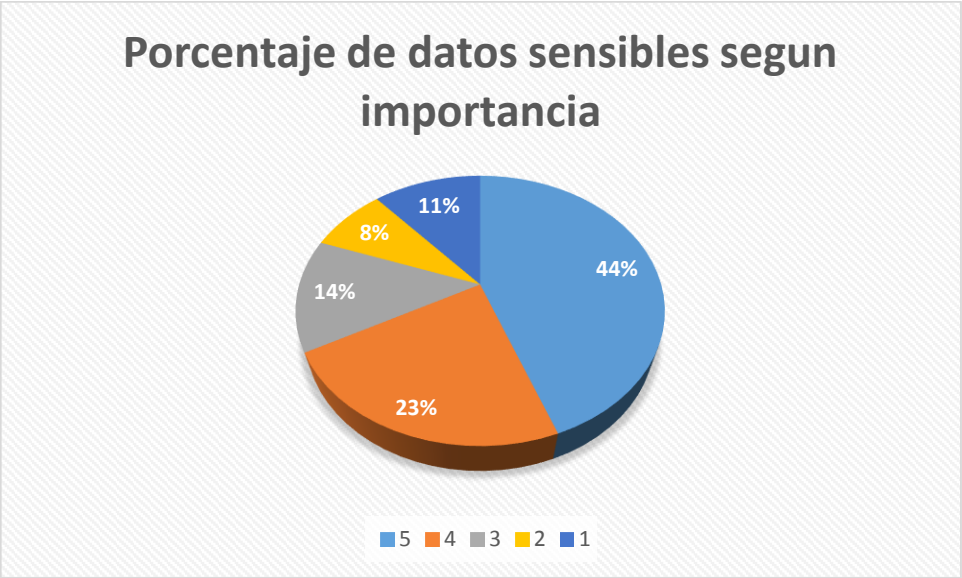


Gráfico # 5. Porcentaje de datos sensibles según importancia. Fuente.- Autor

Análisis.- Se puede observar que en las empresas productoras y asesoras de seguros encuestadas tienen un aproximado de 6 tipos de datos que consideran valiosos e imprescindibles para la evolución del negocio, tales como:

- Pólizas
- Clientes
- Contabilidad
- Administración
- Comercial
- Siniestros

Los cuales no deben ser accesibles a ninguna persona ajena a la compañía por el hecho de que pueden causar pérdidas irreparables. Cabe recalcar todos los datos presentados en la encuesta tienen su grado de importancia pero existen aquellos que afectan en diferente grado la productividad y afectan a la organización.

5.- ¿Conoce las amenazas a las que se encuentra expuesta su organización en temas referentes a la seguridad informática?

Gráfico # 6. Conocimiento de amenazas. Fuente.- (Olimpia, 2013)

Sus respuestas se las analiza de la siguiente manera:

Análisis.- Los administradores de las compañías concuerdan en que los spyware, virus, y estafas son las amenazas más comunes ya que escuchan hablar de ellas a diario, pero cada uno de ellos está consciente que a medida de que la tecnología evoluciona, los hackers también están evolucionando para poder entrar a esa tecnología.

Conocen que pueden encontrarse con amenazas combinadas que atentan contra la información y cada uno de los procesos del negocio, y esto incluye desde el robo físico de documentos y archivos, hasta la copia de bases de datos y almacenamiento de información en dispositivos externos.

6.- ¿Cuánto estaría dispuesto a invertir por equipos de seguridad informática (FIREWALL) y capacitaciones al personal que será el encargado de administrarlo?

Pregunta 6	1k a 3.5k	3.5k a 6k	6k a 8k	8k a 10k	Más de 10k
Cuanto a invertir	23	13	3	0	1

Tabla # 5. Fuente.- Autor

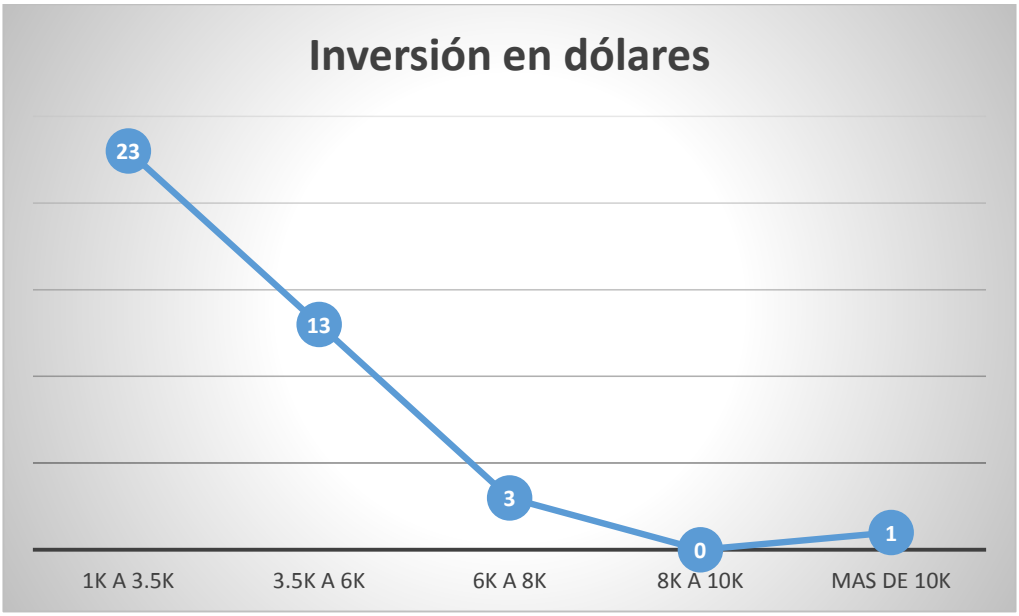


Gráfico # 7. Inversión en miles de dólares. Fuente.- Autor

Análisis.- Se consultó acerca de la inversión en relación a seguridad informática para su compañía y el resultado es que la inversión de la mayoría (23) de las empresas encuestadas no corresponde a un valor representativo (Entre 1000 y 3500 dólares) en comparación al valor en dólares que reportan como comisiones en 1 año.

De la premisa anterior surge una incógnita que será representada en el siguiente ejemplo: "Si una empresa es atacada y pierde clientes por algún tipo de delito informático, lo cual representa un ingreso aproximado de 10000 dólares al año, el valor mencionado es significativo en comparación a la protección que deberían implementar". Limitar la inversión también limita la seguridad y limita la importancia de la información.

7.- Su organización ofrece algún tipo de seguro que contribuya a la protección de los clientes ante los delitos informáticos.

Pregunta 7	SI	NO
Seguro ante delitos informáticos	0	40

Tabla # 6. Fuente.- Autor

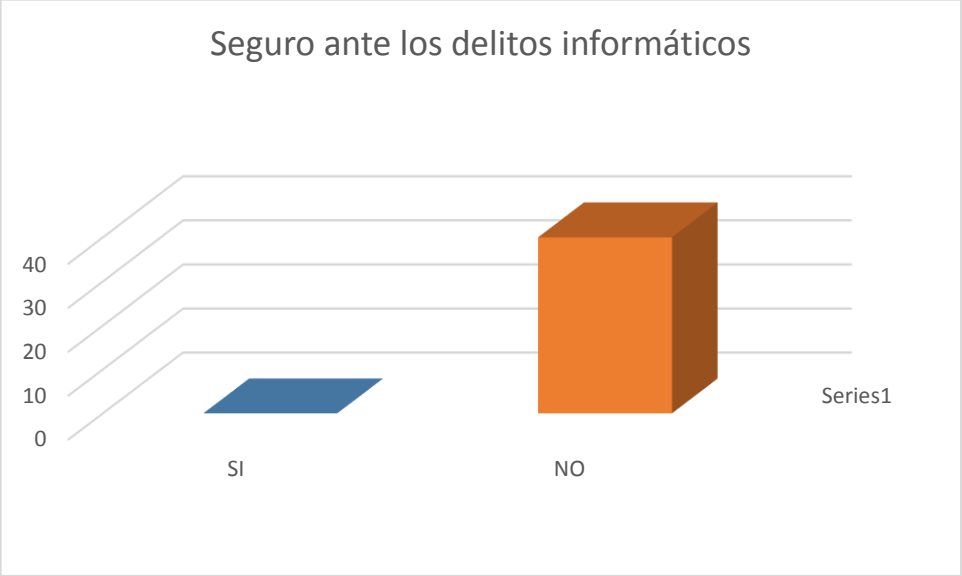


Gráfico # 8. Seguro ante delitos informáticos. Fuente.- Autor

Análisis.- Ninguna (40) de las compañías encuestadas pudo dar información referente a algún tipo de seguro ante los delitos informáticos, se puede interpretar que la compañía de seguros opta por promocionar el producto directamente y no por medio de las productoras y asesoras de seguros, ya que se pudo conocer que una reconocida compañía internacional de seguros lanzo un producto que protege a las empresas de los fraudes informáticos y en caso de que los tuvieran ayudan a que la marca no sufra quebrantos y mala imagen ocasionando cuantiosas pérdidas económicas.

8.- Con respecto a la información que se maneja en su compañía, conoce usted si los datos de cualquier tipo tienen opción a salir de la organización por algún medio tecnológico.

Pregunta 8	Extremadamente improbable	Improbable	Algo probable	Probable	Muy probable
Salida de datos	0	5	24	10	1

Tabla # 7. Fuente.- Autor

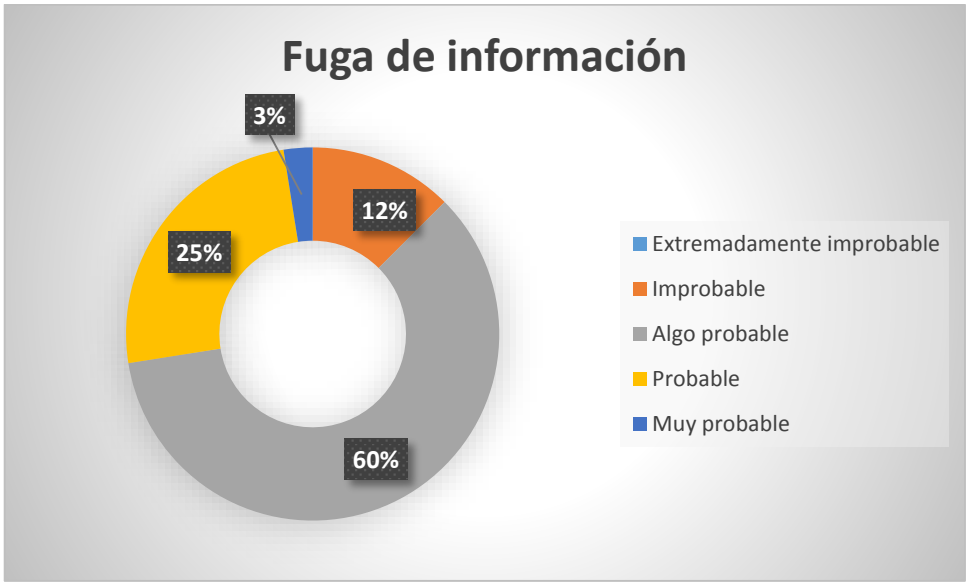


Gráfico # 9. Fuga de información. Fuente.- Autor

Análisis.- El mundo de la informática ofrece un sin número de opciones al momento de transportar información de un lado a otro, como olvidar la época en la que el único medio para trasladar la información era en papel o medios de almacenamiento pequeños pero los medios actuales permiten llevar carpetas completas de información de un lado a otro. En la totalidad de las compañías se maneja el correo electrónico y a pesar de que ofrece una cantidad limitada de información para compartir no es impedimento para pensar en algún tipo de fuga de información. Y de ello están conscientes las empresas encuestadas ya que el 88% considera que la fuga de información está dentro del rango de lo probable y que se debería tomar en cuenta al momento de implementar seguridad en la compañía.

9.- ¿Su empresa posee políticas de seguridad informática?

Pregunta 9	SI	NO	NO CONTESTA
Políticas de seguridad	7	24	9

Tabla # 8. Fuente.- Autor

Gráfico # 10. Políticas de seguridad. Fuente.- Autor

Análisis.- ¿Qué tanto conoces a tu compañía? ¿Sabes realmente que son las políticas de seguridad informática? ¿Prefieres no brindar esa información? Son preguntas que surgen al momento de realizar esta investigación, pero el decir que no tienen políticas de seguridad informática implementadas (60%) no significa que realmente no las tengan, puede ser que no las tienen definidas por escrito y se rigen a lo que diga el personal de sistemas en caso de que lo tuvieran o al agente externo que los visita cada cierto tiempo o tiene contrato. Otros prefieren no contestar (23%) y dejar a consideración del encuestador el pensamiento correcto o incorrecto de la existencia de las mismas por la infraestructura visualizada o por el trato que se le da a la información. Así mismo existen compañías que realmente tienen definidas las políticas porque realmente lo consideran importante.

10.- El riesgo al que se exponen los bróker de seguros en referencia a los delitos informáticos lo considera:

Pregunta 10	No severo	Poco severo	Medianamente Severo	Severo	Muy severo
Riesgo ante delitos	0	0	10	28	2

Tabla # 9. Fuente.- Autor

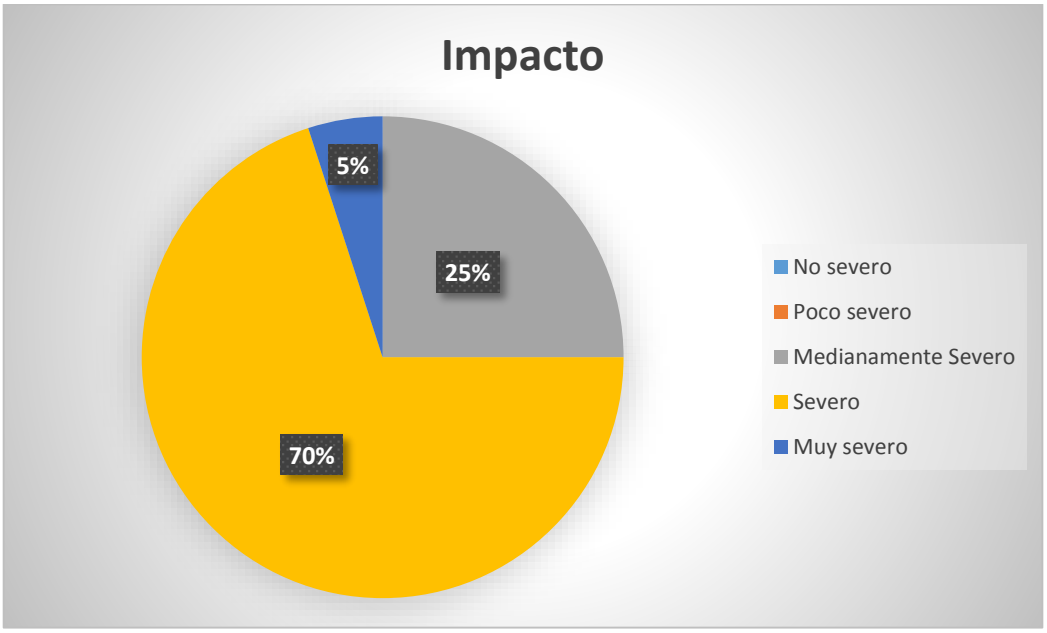


Gráfico # 11. Impacto para las empresas. Fuente.- Autor

Análisis.- Ninguna de las compañías resta importancia al impacto que podría sufrir ante algún tipo de fraude informático más bien consideran que les traería perjuicios importantes ya que se pone en juego la imagen y nombre de la compañía y podrían llegar a perder futuros clientes por no estar debidamente protegidos, aun cuando crean que si lo están el riesgo está latente debido a que manejan miles de dólares que se podrían convertir en miles de problemas. Para algunas compañías si llega a pasar será ese el preciso momento en el que se sentirán obligados a reforzar su seguridad o recién implementarla. Es así como el 70% de las empresas encuestadas consideran que el riesgo es "Severo".

Personal de sistemas de las compañías.

1.- En lo referente al área de tecnología, ¿con que tipo de seguridad cuenta actualmente?

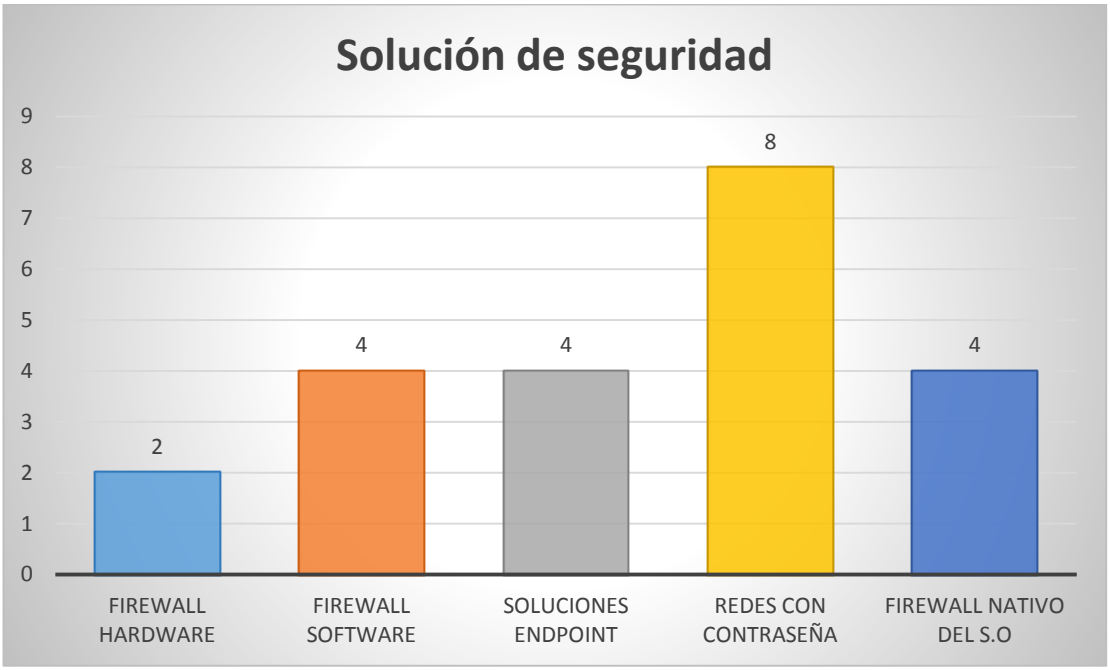


Gráfico # 12. Solución de seguridad. Fuente.- Autor

Análisis.- De las compañías que cuentan con alguna(s) persona(s) de sistemas se pudo conocer que en gran número tienen implementado algún tipo de seguridad informática y el factor común y básico que se encuentra es tener sus redes con contraseña (8) en el caso de las redes Wireless adicional a la protección antivirus que poseen sus equipos, sin embargo también hay compañías que ya cuentan con Firewall sea este en versión Hardware o Software en combinación con las soluciones EndPoint. De estos resultados se puede observar que hay compañías las cuales pueden resultar blanco fácil de las amenazas informáticas y las cuales pueden mejorar su infraestructura de seguridad.

2.- En el último año, ¿Ha sufrido algún tipo de ataque o se ha presentado alguna amenaza de consideración?

	SI	NO	NO CONTESTA
Empresas	1	10	**0**

Tabla # 10. Fuente.- Autor

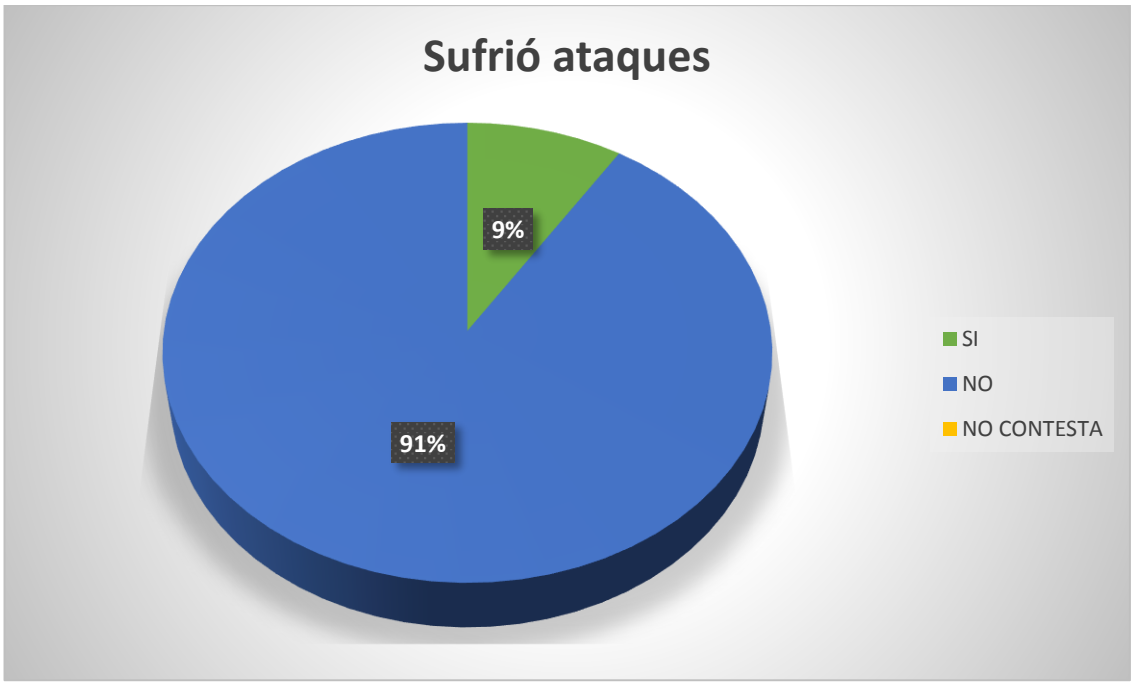


Gráfico # 13. Sufrió ataques. Fuente.- Autor

Análisis.- Si bien en el último año no todas las empresas reportan ataques de consideración fuera de los virus a los que se está expuesto a diario, ya existe el precedente que una de ellas fue atacada y a partir de eso hay que comenzar a preocuparse de que si existen personas que tienen como blanco a las empresas productoras y asesoras de seguros, por la información importante y relevante que manejan de cada uno de los usuarios y compañías que requieren sus servicios.

3.- Indique por favor el número aproximado de amenazas presentadas en el último año.

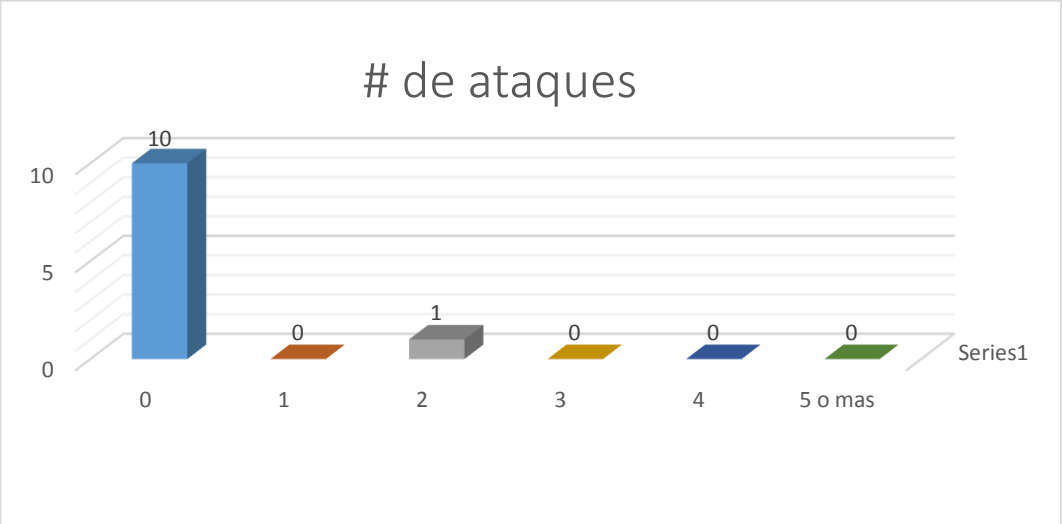


Gráfico # 14. Número de ataques. Fuente.- Autor

Análisis.- Una empresa tuvo 2 amenazas en el último año, y el resto indica que no presento amenaza alguna, se presentan las siguientes incógnitas:

- Prefieren evitar brindar dicho tipo de información.
- La empresa atacada no tiene la seguridad suficiente.
- Realmente están protegidas y pueden contrarrestar los ataques.

O simplemente todavía no son un blanco llamativo para los atacantes.

Sea o no uno de los puntos mencionados anteriormente se pudo conocer que ninguna de las compañías se ha sometidos a pruebas de penetración para comprobar si en realidad están protegidas y de ahí se puede partir para pensar que pudieron ser víctimas de ataques sin poder darse cuenta de los mismos.

4.- ¿La totalidad de sus servidores se encuentran físicamente dentro de su organización?

	SI	NO
Empresas	9	2

Tabla # 11. Fuente.- Autor

Gráfico # 15. Servidores dentro de la organización. Fuente.- Autor

Análisis.- Con esta información se busca conocer cuánto se puede proteger y si los servidores que en un 82% están dentro de las empresas realmente hay mucha información por cuidar ya que la misma tiene un solo punto de concentración el cual debe estar fuera del acceso no autorizado. Con esto se conoce que están al tanto que no pueden proteger algo que no tienen cerca y que físicamente no lo pueden ver. En la actualidad se suelen usar contratos de nubes informáticas que son las encargadas de brindar protección y respaldo de la información y cuentan con el equipo tecnológico suficiente para contrarrestar cualquier eventualidad.

5.- Tomando en cuenta que las compañías de seguros tienen puntos de servicio fuera de su organización, ¿Cómo esos equipos se interconectan con los servicios de su compañía? Puede seleccionar una o varias alternativas.

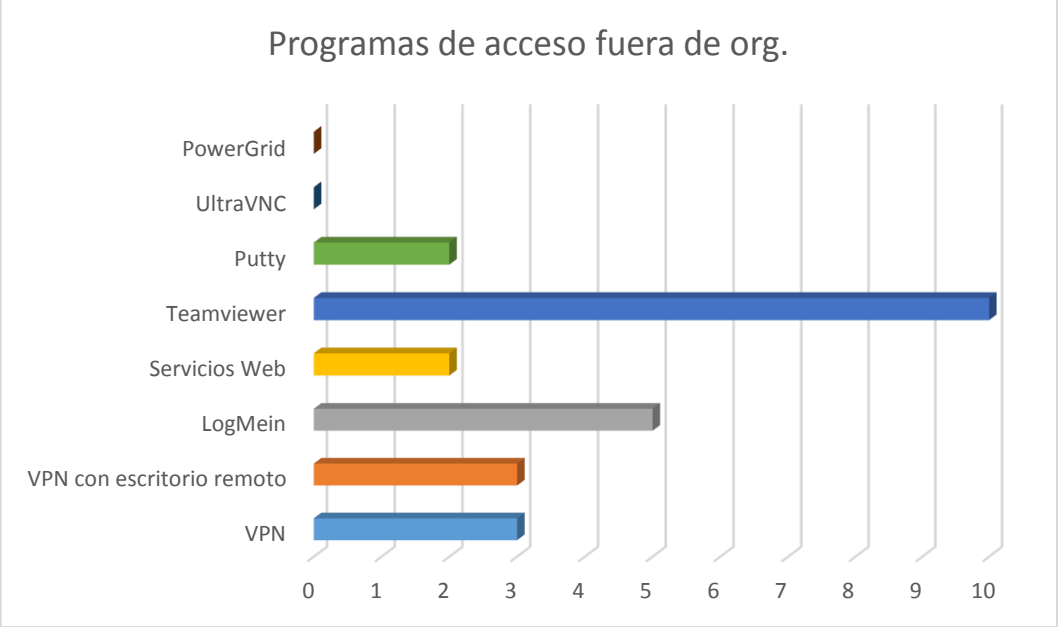


Gráfico # 16. Programas para acceder fuera de la organización. Fuente.- Autor

Análisis.- El Teamviewer es la opción con mayor acogida para las empresas encuestadas pero no se puede dejar de mencionar que es la versión gratuita la cual después de la sospecha de uso comercial comienza a presentar inconvenientes en el tiempo de conexión y demás mensajes de alerta. Inclusive los costos comerciales de Teamviewer son un poco elevados y las compañías consideran otra variedad de posibilidades para establecer conexiones. Otra de las alternativas más usadas es LogMein un servicio vía web que depende mucho del ancho de banda disponible para que la conexión sea buena y eficaz, y luego vienen las conexiones seguras VPN que permiten tener un acceso más controlado a los servicios empresariales y son parte de los beneficios de un firewall.

6.- ¿Cómo se interconectan las sucursales de las diferentes ciudades en caso de que las tuvieran?

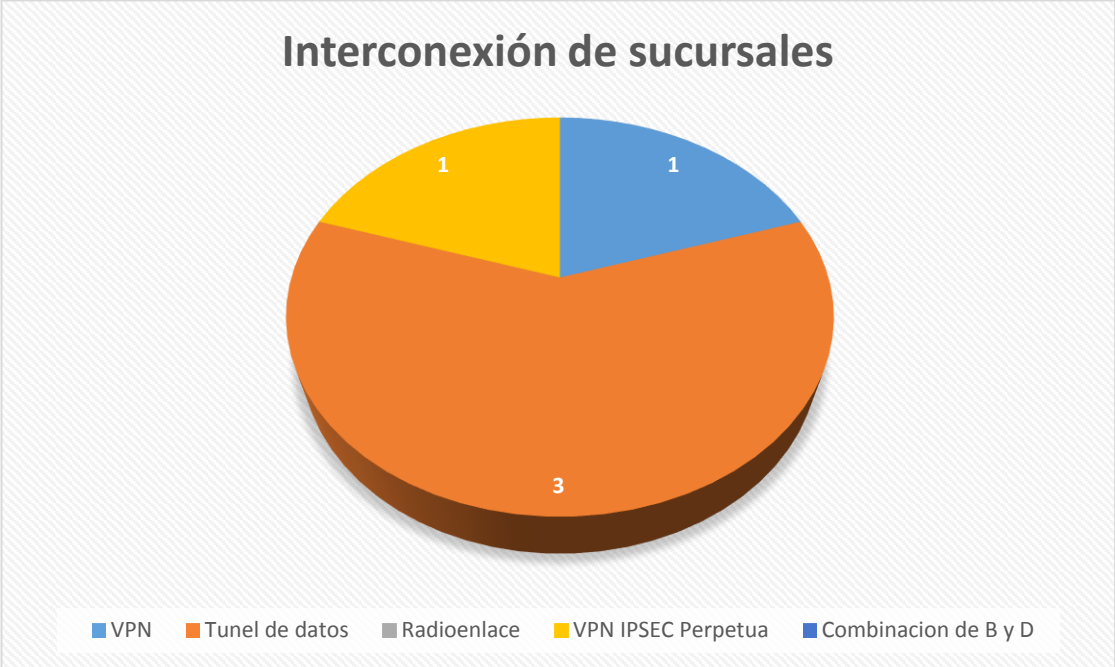


Gráfico # 17. Interconexión de sucursales. Fuente.- Autor

Análisis.- Se pudo conocer que las empresas que cuentan con sucursales en otras ciudades cuentan con un equipo o software de firewall y realizan sus conexiones entre ciudades por medio del túnel de datos que ofrece Telconet y adicional realizan la configuración de la VPN para así reforzar la seguridad. También es común utilizar la VPN IPSEC perpetua con el fin de garantizar la comunicación y de esta manera pueden compartir el uso del internet, acceder a servicios de telefonía IP, y sin número de beneficios que se pueden obtener de acuerdo a las configuraciones implementadas. Cabe recalcar que no todas las agencias productoras y asesoras de seguros tienen sucursales en otras ciudades del país.

7.- ¿Su compañía posee políticas de seguridad para proteger su red empresarial de ataques tanto internos como externos?

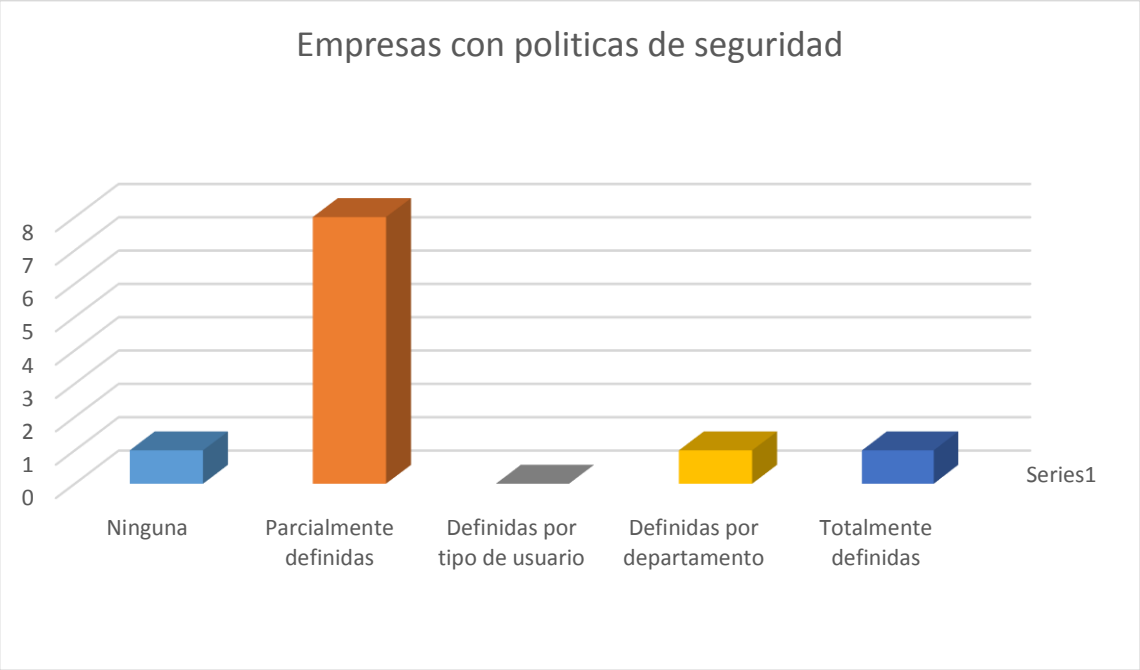


Gráfico # 18. Empresas con políticas de seguridad. Fuente.- Autor

Análisis.- Las departamentos de sistemas encuestados han podido confirmar que gran parte de ellos tienen por lo menos "parcialmente definidas" (8) las políticas de seguridad informática y las hacen conocer al personal de la empresa y con ello buscan tener el control de la seguridad para su organización, pero al momento de mencionar que están parcialmente definidas da la pauta para aseverar que falta normas y políticas por definir y de allí viene la pregunta, ¿Que ha pasado para que no estén totalmente definidas? y la respuesta es que a medida de que se presente algún riesgo se definen las mismas y esto solo con las empresas que si tienen un departamento de tecnología preocupado de los riesgos informáticos, y las compañías que no tienen área de sistemas en realidad no tienen definidas sus políticas de seguridad informática.

8.- El ancho de banda contratado con su ISP (Internet Service Provider) ¿satisface las necesidades de su compañía?

Gráfico # 19. Satisfacción con internet. Fuente.- Autor

Análisis.- Se puede observar que el nivel de satisfacción es bastante bueno para la mayoría de los departamentos de sistemas (6) dado a la cantidad de empleados que maneja la compañía y las transacciones que se realizan de manera simultánea sin embargo también hay empresas que indican que se podría mejorar por la concurrencia que tienen al momento de la navegación y no dudaran en mejorarlo muy pronto ya que es importante para la productividad de la organización. También hay empresas que reportan y consideran ideal su ancho de banda ya que no han recibido reportes de lentitud o caídas en el servicio de internet.

9.- ¿Qué ancho de banda posee actualmente en su organización?

	1 a 2 Mbps	3 a 5 Mbps	6 a 9 Mbps	10 a 12 Mbps	13 Mbps o mas
Empresas	4	6	1	0	0

Tabla # 12. Fuente.- Autor

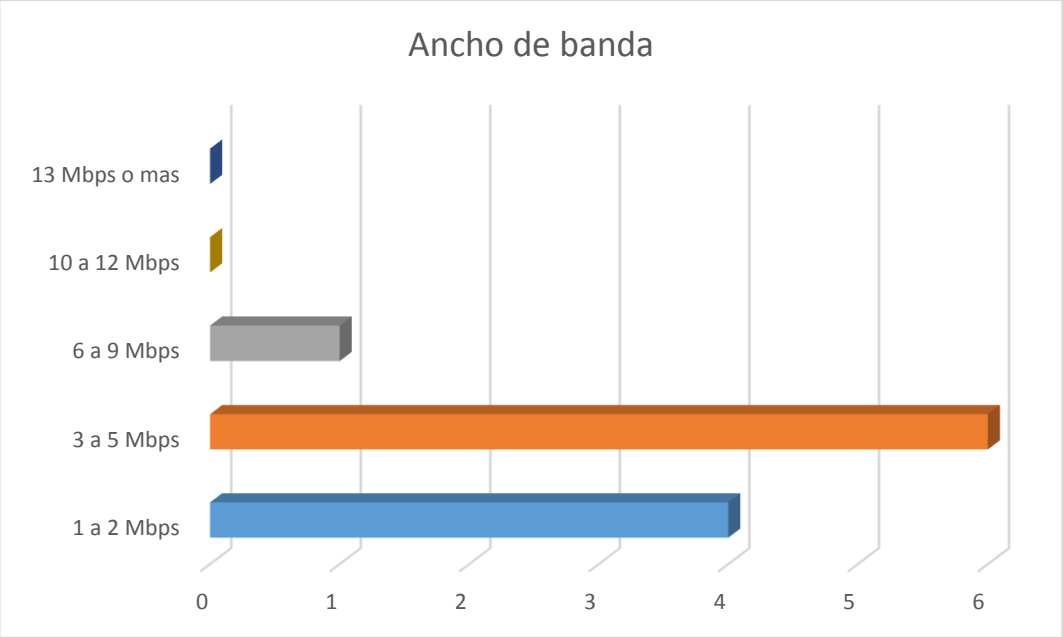


Gráfico # 20. Ancho de banda. Fuente.- Autor

Análisis.- Se puede observar que los departamentos de sistemas se preocupan de que la conexión a internet de las empresas que supervisan sea la que realmente satisface sus necesidades aun así no descartan las futuras mejoras que se puedan realizar a medida que sea necesario para mejorar la productividad del negocio, es por eso que la velocidad promedio que se maneja es de 3 a 5 mbps.

Los proveedores de Internet (ISP) continuamente realizan mejoras y mantenimientos en cada uno de los nodos que proveen la conexión a internet y tratan de no sobrecargar los mismos para que no se presente saturación y la muy conocida lentitud en la navegación.

10.- ¿Cuál es el nivel de compartición que tiene su contrato de internet?

	Sin compartición	2:1	4:1	6:1	8:1
Empresas	3	5	1	0	2

Tabla # 13. Fuente.- Autor

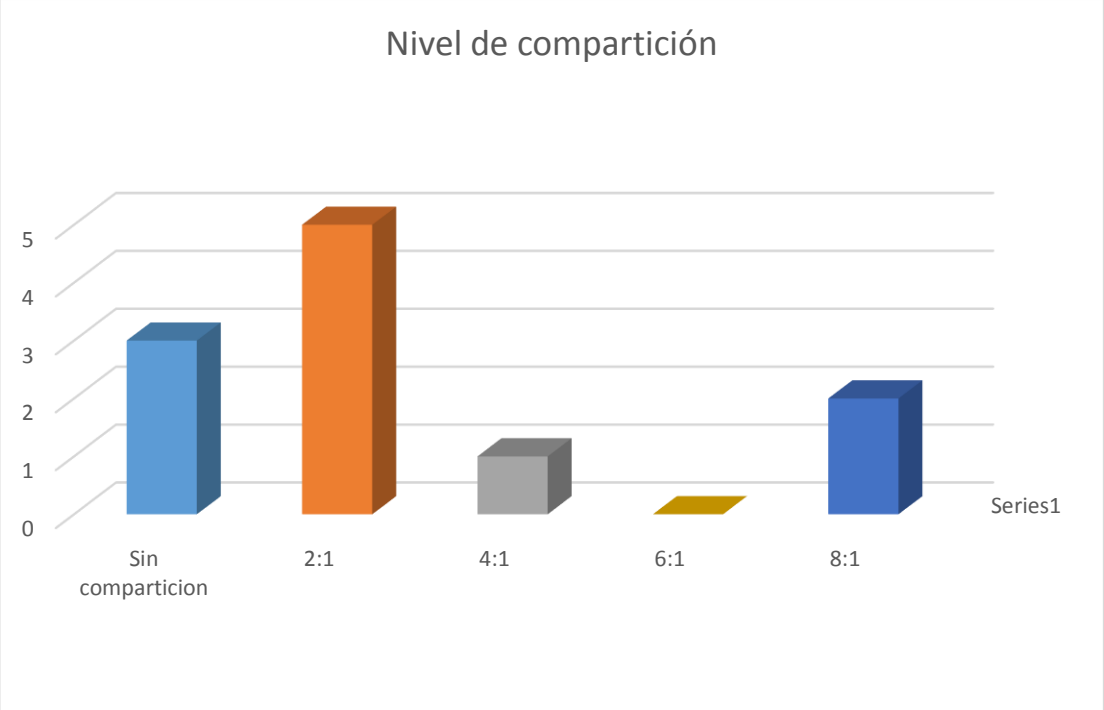


Gráfico # 21. Nivel de compartición. Fuente.- Autor

Análisis.- El nivel de compartición al que aspiran las organizaciones es realmente no tenerlo, no compartir su señal de internet para no disminuir el performance al momento de cargar o descargar cualquier clase de archivo es el objetivo, y poco a poco se está logrando el mismo debido a la reducción del costo por el servicio pero al momento la tendencia es tener una compartición 2:1.

11.- ¿Con cuál de los siguientes proveedores tiene contratado su internet?

	Telconet	TV Cable	Claro	CNT	NETLIFE	Otro
Empresas	5	3	2	0	1	2

Tabla # 14. Fuente.- Autor

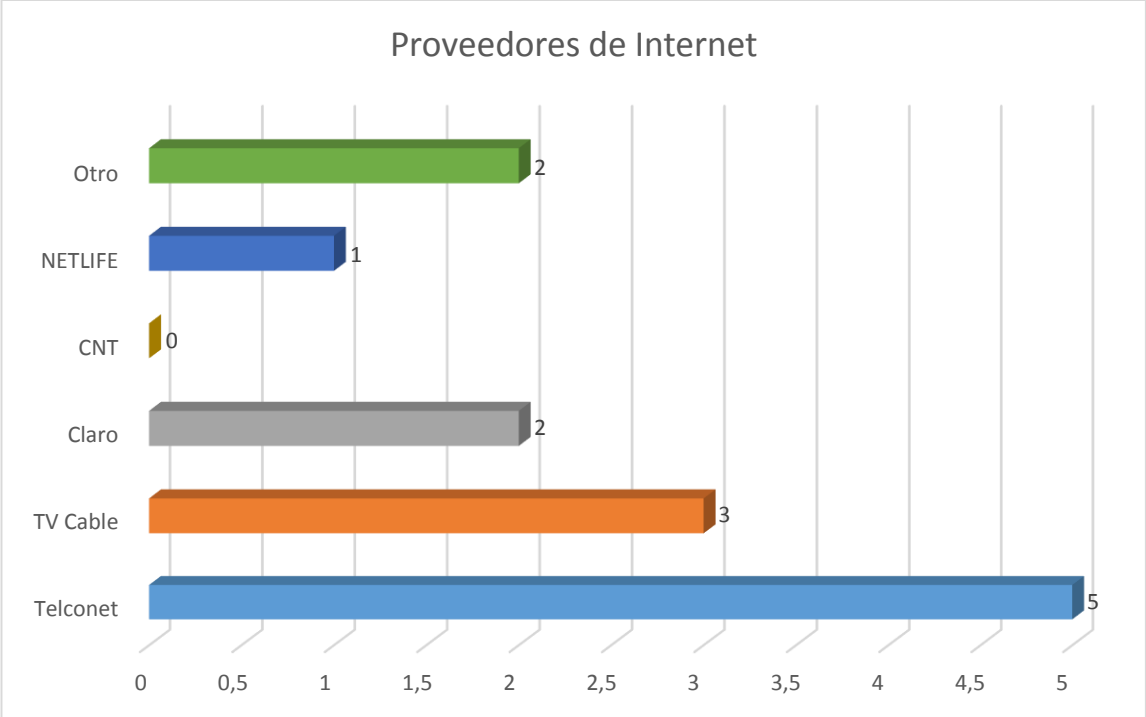


Gráfico # 22. Proveedores de internet. Fuente.- Autor

Análisis.- Proveedores de internet hay muchos y cada uno de ellos ofrecen servicios de tipo empresarial. Las empresas al momento de elegir proveedor no solo de internet sino de cualquier otro tipo de servicio, buscan calidad, precio y buenas referencias y ese es el caso de Telconet que en telecomunicaciones es una de las empresas líderes del mercado y lo ratifica la elección de la mayoría de empresas productoras y asesoras de seguros ya que no solo contratan el servicio de internet sino lo que traen como valor agregado.

12.- ¿Cómo distribuye el consumo de ancho de banda entre los usuarios de su organización?

	Todos acceso por igual	Se asigna según redes disponibles	Jefaturas deciden accesos a internet	Lo define Sistemas	Según transacciones por departamento
Empresas	7	1	1	0	2

Tabla # 15. Fuente.- Autor

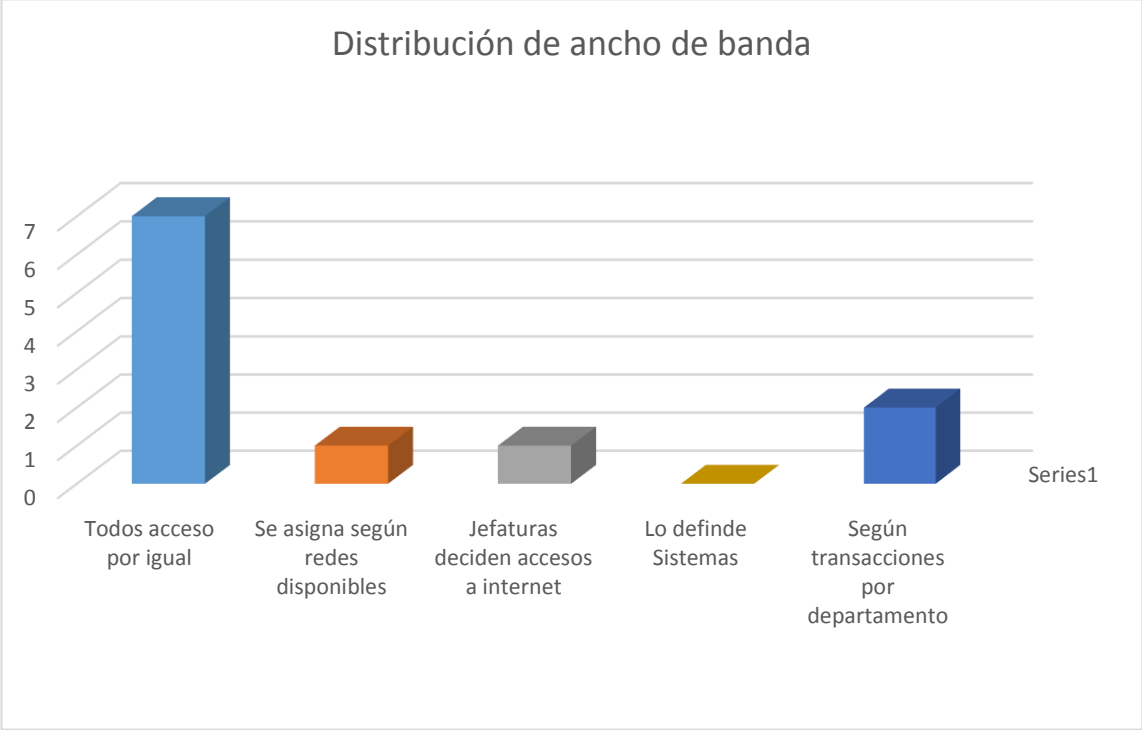


Gráfico # 23. Distribución de ancho de banda. Fuente.- Autor

Análisis.- La mayoría de los encuestados concuerdan en que todos tienen acceso por igual y en realidad podría ser un gran tema de discusión debido al control que se debería aplicar, por el hecho de que se debe recordar que el consumo del internet se distribuye equitativamente según el número de usuarios y disminuye según las transacciones que realice cada uno de ellos ya que consumen más recursos de los que en realidad necesitan.

13.- El recurso humano destinado a velar por la seguridad informática de su compañía cumple con capacitaciones periódicas para estar al día con la información de las nuevas amenazas y prevención, ¿cuál es la frecuencia de estas capacitaciones?

	Diariamente	Semanalmente	Mensualmente	Semestralmente	Anualmente	Nunca
Empresas	0	0	2	1	8	0

Tabla # 16. Fuente.- Autor

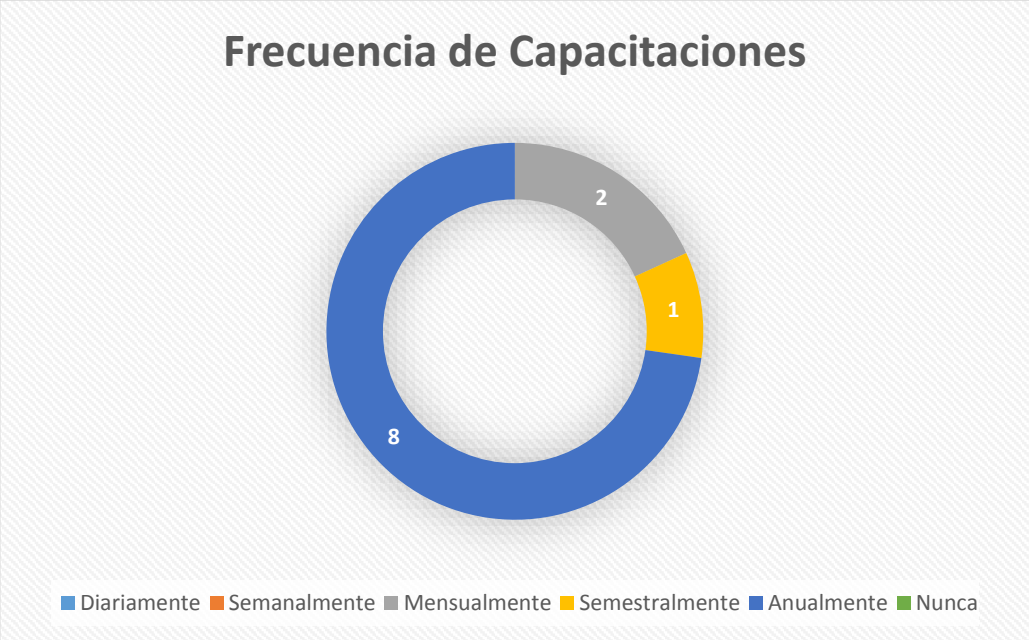


Gráfico # 24. Frecuencia de capacitaciones. Fuente.- Autor

Análisis.- Las capacitaciones con respecto a las amenazas que diariamente se presentan no son directamente proporcionales, y es lógico cuando una organización considera que esta bien protegida y que no necesita capacitaciones constantes para su personal, más aun cuando no han sido víctimas de ataque alguno, pero se debe tener en cuenta que no es del todo beneficioso recibir capacitaciones anualmente lo cual es tendencia ya que ceden bastante terreno a las acciones que deben de tomar en caso de algún imprevisto, queda a consideración del personal de sistemas ser autodidacta.

14.- ¿Cómo analiza la vulnerabilidad de su red empresarial?

	Herramienta de Auditoria Informática	Revisión periódica de permisos de accesos	Logs o Reportes	Pruebas de Ethical Hacking	Otros
Empresas	1	5	5	0	3

Tabla # 17. Fuente.- Autor

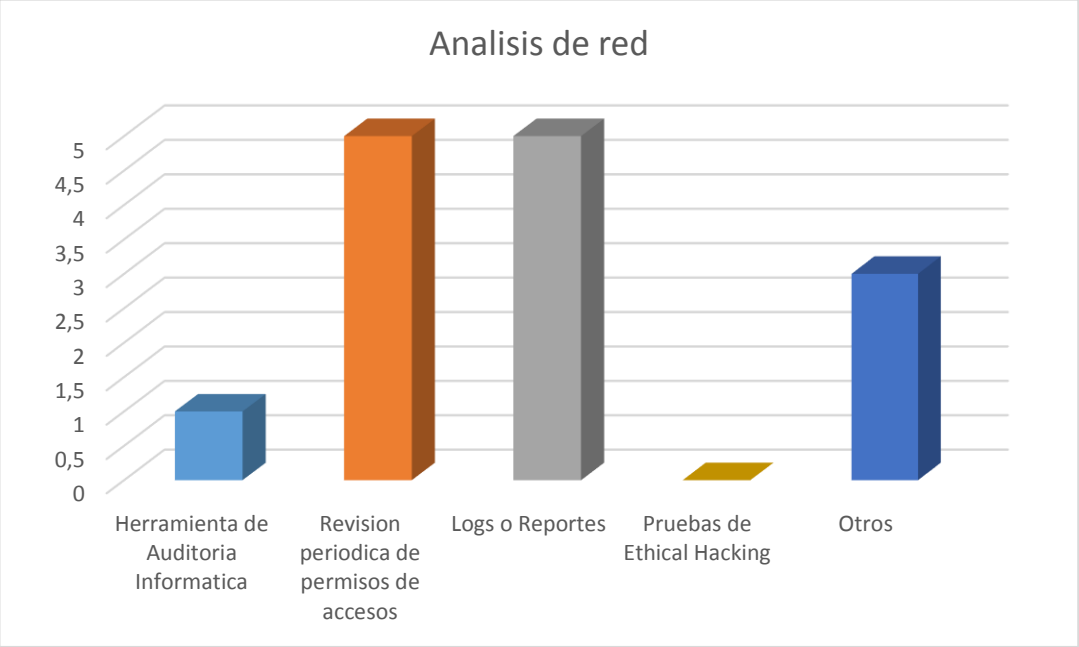


Gráfico # 25. Análisis de red. Fuente.- Autor

Análisis.- Para analizar la vulnerabilidad de la organización existen varias maneras y en el caso de las empresas encuestadas domina la revisión periódica de los permisos de acceso junto con los reportes o logs que pueden generar programas instalados que evalúan el tráfico, transacciones tanto exitosas o errores en las mismas y diversos procesos extras, pero hay un punto a tomar en cuenta y que llama mucho la atención y es que no se realizan pruebas de ethical hacking, lo cual ayudaría mucho más para descubrir sectores o puntos flacos por donde se podrían presentar filtraciones o intrusiones en caso de que se presente algún tipo de amenaza.

15.- Cuando un usuario renuncia o es separado de la compañía, ¿Cómo protege la información a la cual tuvo acceso?

	Eliminación de usuario	Eliminación de correo	Cambio de claves de acceso	Anulación de permisos	Otros
Empresas	0	4	9	7	0

Tabla # 18. Fuente.- Autor

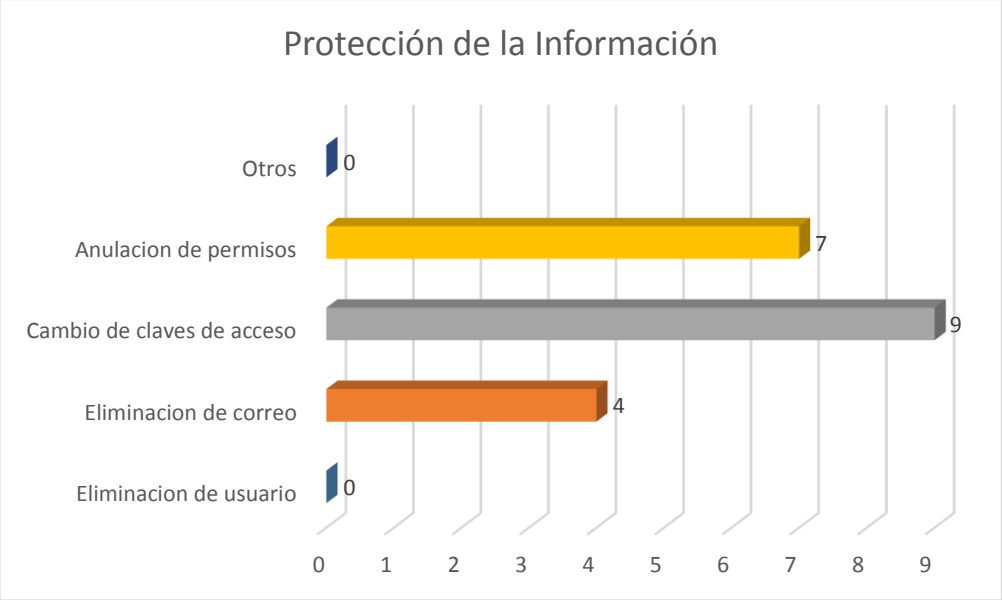


Gráfico # 26. Protección de la información. Fuente.- Autor

Análisis.- Cuando un usuario abandona la compañía por cualquier tipo de novedad que se presente, es un verdadero problema porque conoce información valiosa de la compañía que ayuda a la generación de negocios y también podría ser la causa de la perdida de los mismos y es por ella que las empresas toman precauciones al momento de que suceda este tipo de situaciones, y es así como predomina el cambio de claves de acceso y la anulación de permisos y puede surgir la incógnita de porque no se elimina el usuario directamente, y es porque los clientes que ya conocen al mismo seguirán reportando sus dudas, sugerencias e inconvenientes a esa persona y se necesita informar del cambio de asesor de la manera más adecuada sin que se presenten malos entendidos y se pueda mantener la relación con el cliente.

De la encuesta realizada a cada uno de los 2 actores de las agencias productoras y asesoras de seguros de Guayaquil se pudo conocer su necesidad primordial de cuidar la información importante para la compañía por medio de conexiones seguras dentro y fuera de la organización, detección y bloqueo de amenazas, navegación en internet que pueda restringirse en cada departamento según lo que puedan solicitar las jefaturas, y con un equipo que ofrezca servicio de comunicaciones para enlace entre ciudades, logs de status en cada uno de sus módulos o componentes, logs de sitios visitados por parte de los usuarios, reportes ejecutivos acerca de bloqueos, amenazas detectadas, puertos admitidos y denegados, base de datos sobre listas blancas y listas negras, actualizaciones periódicas sobre protección contra nuevas amenazas y soporte las 24 horas del día con garantía que pueda solventar eventualidades que se puedan presentar durante la operación y funcionamiento de la solución adquirida.

3.2 RESULTADOS DE ENTREVISTAS A PROVEEDORES DE FIREWALL

La entrevista se la realizó a 4 proveedores que dieron la debida apertura a la investigación tomando en cuenta que posiblemente es un sector el cual no han realizado el estudio de mercado necesario para poder situar sus productos dentro de las agencias productoras y asesoras de seguros de la ciudad de Guayaquil teniendo como resultado lo siguiente:

- Los proveedores entrevistados fueron:
    - GMS, con sucursal en la ciudad de Guayaquil en el edificio Blue Towers, proveedor de diversos servicios informáticos tiene entre sus productos el Firewall de marca Sophos el cual expone en su propuesta, el contacto fue el Ing. Mario Triviño.
    - Pentasec, empresa situada en el norte de la ciudad de Quito especialista en seguridad informática ofrece su producto de marca McAfee, el contacto fue el Ing. Favio Estévez.

    - CEMPAZ, empresa que provee soluciones informáticas ubicada al norte en la ciudad de Guayaquil, revendedor de importantes marcas como Microsoft, HP, IBM, D-Link ofrece el firewall de esta última marca, y el contacto fue el Ing. Jorge Game.
    - Synergy, compañía encargada de la prestación de servicios tecnológicos, tiene sus oficinas en el edificio World Trade Center al norte de Guayaquil, pudo dar a conocer que promocionan el firewall de marca CheckPoint, el contacto fue la Ing. María Verónica Baquerizo.
- GMS, PENTASEC, CEMPAZ fueron los proveedores que enviaron propuestas técnicas y económicas para equipar a las agencias productoras y asesoras de seguros de Guayaquil con sus soluciones de firewall dentro del área de seguridad informática.
- SYNERGY manifestó que su solución no podía presentarse como solución al mercado de seguros porque el costo de la misma no estaba dentro del rango de inversión que pueden tener las organizaciones mencionadas.

Luego de la reunión mantenida con los proveedores se realizó un boceto de características básicas que debería tener un firewall para poder satisfacer la necesidad de seguridad que tienen las agencias productoras y asesoras de seguros de la ciudad de Guayaquil, el cual fue enviado a los proveedores, y ellos respondieron el mismo con su debida propuesta.

La lista de características básicas enviada a los proveedores y La respuesta por parte de los mismos es representada en la siguiente tabla de cumplimiento en donde se especifican los equipos de firewall con sus respectivas marcas y modelo:

CARACTERISTICAS	CUMPLIMIENTO DE PROVEEDORES CON EQUIPO MARCA / MODELO		
	GMS *Sophos - ASG 320*	**PENTASEC McAFEE - NGF 1035 C2**	**CEMPAZ D-Link DFL 1660**
El firewall UTM deberá permitir acceso exterior del cliente y opción de acceso por medio de SSH externo a través de internet con configuraciones de denegación de acceso, acceso por VPN y la de permitir acceso en general. Activación y desactivación del protocolo ICMP (ping) directamente al firewall.	SI	SI	SI
Tiene que contar con módulo de autenticación de usuarios.	SI	SI	SI
Deberá contar con un editor de reglas basado en las siguientes condicionales como mínimo: - Servicio (Especificando puerto y protocolo) - Acción (Dirección de la conectividad) - Deberá permitir loggear el evento de conectividad (Log event) - Deberá poder asignar proxy para funcionalidades e inspección especifica (dependiendo de la necesidad) - Deberá permitir configurar NAT's / BiNAT / PNAT's y SNAT's - Deberá permitir asignar inspección a nivel aplicativo para: o DNS o FTP o HTTP	SI	SI	SI

○ POP3 ○ SMTP			
Deberá contar con un panel específico donde se pueda monitorear en tiempo real el status de las conexiones en donde se pueden realizar filtros específicos para obtener datos importantes durante la resolución de problemas.	SI	SI	SI
Deberá contar con la posibilidad de ser administrado por una herramienta gráfica y como segunda opción vía consola.	SI	SI	SI
Deberá contar con la certificación Common Criteria EAL 4+	SI	SI	SI
Deberá gestionar backups automáticos de manera interna sobra la plataforma que se vaya a configurar.	SI	SI	SI
Deberá poder generar backups que se envíen por correo electrónico a una(s) dirección (es) especifica(s)	SI	SI	SI
Deberá contar con al menos 4 interfaces Gigabit Ethernet RJ45.	SI	SI	SI
Deberá permitir al menos 500000 (Quinientos mil) de sesiones concurrentes	SI	SI	SI
Deberá contar con la posibilidad de realizar bridges (transparentes) entre tarjetas reales dando la funcionalidad de firewalling, ips, ids, content filter y traffic shapping.	SI	SI	SI
Deberá permitir generar túneles SSL entre interfaces de bridge con fines de realizar VPN’s en modo transparente.	SI	SI	SI

Deberá contar con la posibilidad de manejar ruteo estático, donde se especifique la interfaz, destino, mascara de red y Gateway.	SI	SI	SI
La solución deberá poder administrar como mínimo 2 enlaces diferentes de internet.	SI	SI	SI
Cada tipo de conexión a internet deberá poder ser de tipo RDSI, PPPoE o conexión a router común.	SI	SI	SI
Deberá permitir asignar DNS's específicos por conexión a internet o DNS's específicos de manera global.	SI	SI	SI
Deberá ser rackeable en caso de ser hardware.	SI	SI	SI
Las reglas de calidad de servicio (QoS) deberán poder asignarse a túneles de VPN (PPTP), IPSec y SSL.	SI	SI	SI
Deberá contar con el servicio de replicación de DNS's para usuarios finales del UTM	SI	SI	SI
Deberá contar con un servidor DHCP.	SI	SI	SI
Deberá permitir el envío de notificaciones sobre el status del firewall.	SI	SI	SI
Deberá funcionar autenticando usuarios de manera local y en función de un directorio LDAP (openldap, active directory, etc.)	SI	SI	SI
Deberá poder integrar relación de confianza con active directory de Windows.	SI	SI	SI

Deberá contar con la posibilidad de segmentar actualizaciones de funcionalidad, de seguridad, hotfixes y firmware con fines de poder aplicarlos de manera automatizada algunos y otros no, dependiendo del nivel de riesgo del firewall.	SI	SI	SI
Deberá contar con un log de actualizaciones aplicadas y actualizaciones pendientes.	SI	SI	SI
Deberá ser una solución que incluya todos los módulos como por ejemplo anti spam, antivirus, filtrado url, entre otros.	SI	SI	SI
Deberá contar con la posibilidad de realizar listas negras y listas blancas basadas en expresiones regulares.	SI	SI	SI
Deberá permitir bloquear ciertos sitios para navegación en formato https.	SI	SI	SI
Deberá permitir ancho de banda específico.	SI	SI	SI
Deberá poder proteger los datos personales del usuario tales como enlaces y consultas donde se incluyan logins, passwords, etc.	SI	SI	SI
Deberá poder bloquear extensiones de archivo y meta caracteres.	SI	SI	SI
Deberá funcionar en modo completamente transparente en función del proxy SMTP sin necesidad de configurar nada en la plataforma de SMTP que manejara el correo electrónico.	SI	SI	SI

Deberá permitir realizar exclusiones basadas en listas blancas para hosts, urls o ips.	SI	SI	SI
Deberá contar con la posibilidad de inicializar túneles de tipo PPTP - Donde se señale pool de direcciones IP que serán utilizadas - Gateway asignado - Transferencia automática de DNS - Transferencia automática de WINS	SI	SI	SI
Deberá contar con la posibilidad de negociar túneles de tipo IPSEC de tipo client to site (C2S) y site to site (S2S) con las siguientes características mínimas - Se deberá poder asignar un nombre significativo al túnel - Asignación a interfaz - Tipo de conexión - Red local que será ruteada automáticamente en el túnel. - Red remota que será automáticamente ruteada en el túnel. - Posibilidad de iniciar automáticamente los túneles. - Se podrán utilizar las credenciales de usuarios específicos vía el directorio activo.	SI	SI	SI
Deberá contar con la posibilidad de mostrar información sobre las visitas a sitios de internet.	SI	SI	SI
Deberá generar reportes ejecutivos sobre ataques, top de amenazas, etc.	SI	SI	SI
Deberá poder generar filtros para obtener información con los	SI	SI	SI

siguientes parámetros como mínimo. - Filtro por usuario, objeto o nombre. - Filtro por intervalos de tiempo. - Filtro de plazo especifico de horario.			
Deberá mostrar status de hardware en consola (uso de disco, memoria, etc.)	SI	SI	SI
Deberá mostrar estadísticas de errores.	SI	SI	SI
En caso de daño del hardware, se deberá contar con equipo de backup.	SI	SI	SI
Tiempo de garantía	1 año	1 año	1 año
Licenciamiento	Anual	Anual	Anual
Costo aproximado de inversión	$11,000	$9,500	$8,900

Tabla # 19. Requerimientos de características básicas de firewall. Fuente.- Autor

Según la tabla se puede determinar que en especificaciones técnicas los 3 equipos cumplen con la mayoría de requerimientos pero el factor determinante para conseguir una solución a esta investigación es la inversión económica que está dispuesta a realizar las agencias productoras y asesoras de seguros de la ciudad de Guayaquil.

El factor económico es un punto determinante en esta investigación debido al costo de los equipos y la suscripción anual de sus servicios, ya que la licencia tiene un periodo limitado de duración, y a partir de la fecha límite de licencia se tiene que proceder con la negociación de la renovación de los servicios que puede ofrecer el equipo.

Se ha desarrollado un diagrama de flujo explicativo en el cual se detalla cada proceso para realizar el diagnóstico del firewall indicado tomando en cuenta

todos los aspectos a considerar, como características técnicas y la inversión que se tendría que realizar.

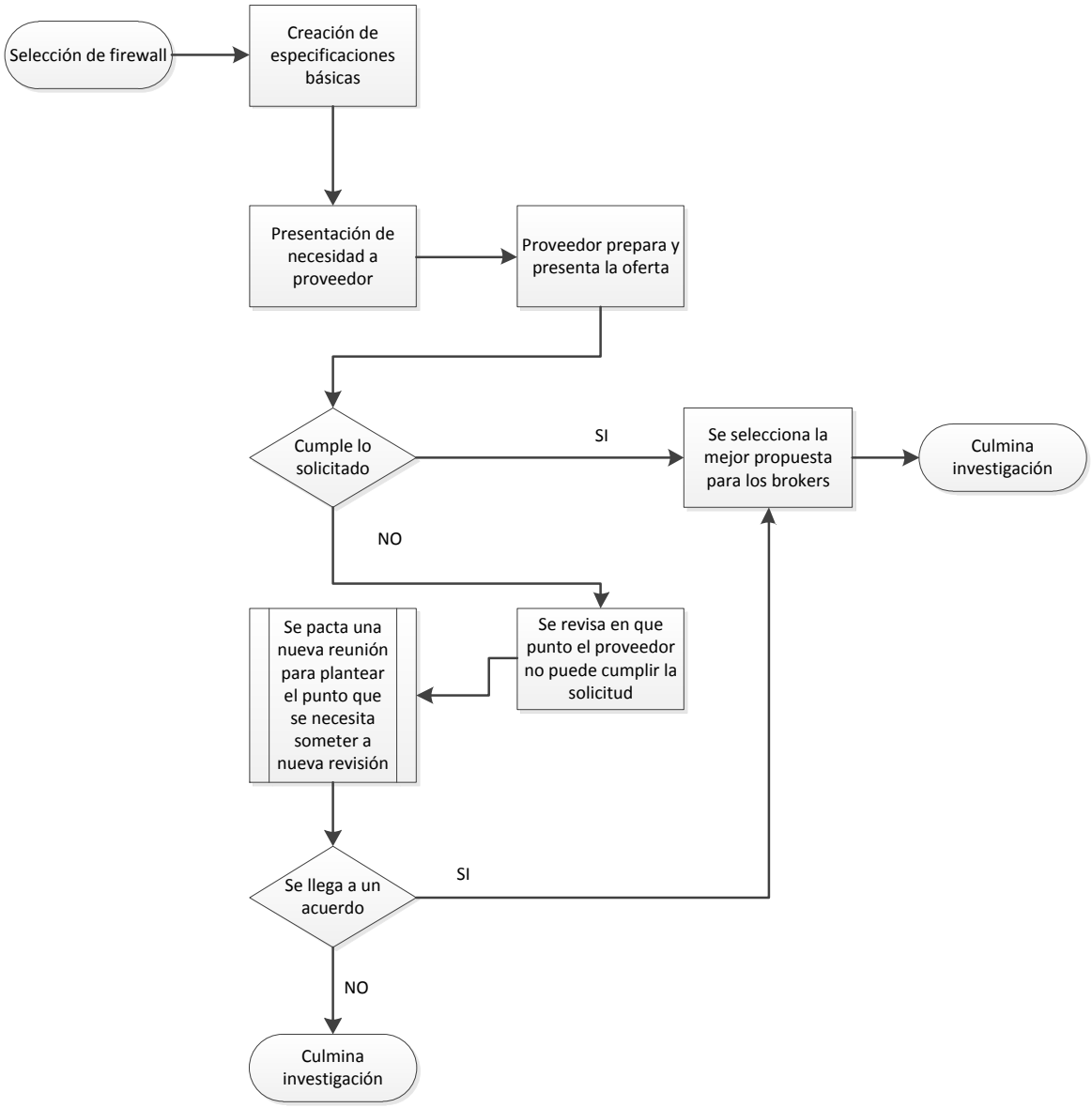


Gráfico # 27. Diagrama de proceso de selección de firewall. Fuente.- Autor

La investigación cuenta con varias etapas importantes para la obtención de la solución, la cual tenía 2 caminos posibles para poder llegar a finalizar el presente trabajo y se lo detalla de la siguiente manera:

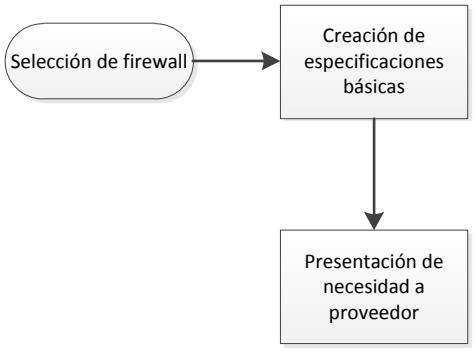


Gráfico # 28. Creación de especificaciones y presentación a proveedor. Fuente.- Autor

Para la selección correcta del firewall se cumplió con el proceso de indagación de necesidades y requerimientos de las agencias productoras y asesoras de seguros de la ciudad de Guayaquil, y para su efecto se realizaron las encuestas, creando a partir de ellas las especificaciones básicas que debe de tener un firewall para ser considerado idóneo en la operación de las empresas mencionadas y sean el arma de protección que sirva para cuidar la información. En la reunión que se tuvo con el proveedor luego de escuchar las especificaciones y beneficios del producto que ofrece, se procedió a entregar las especificaciones básicas con las que debería contar el firewall para la elaboración de la propuesta.

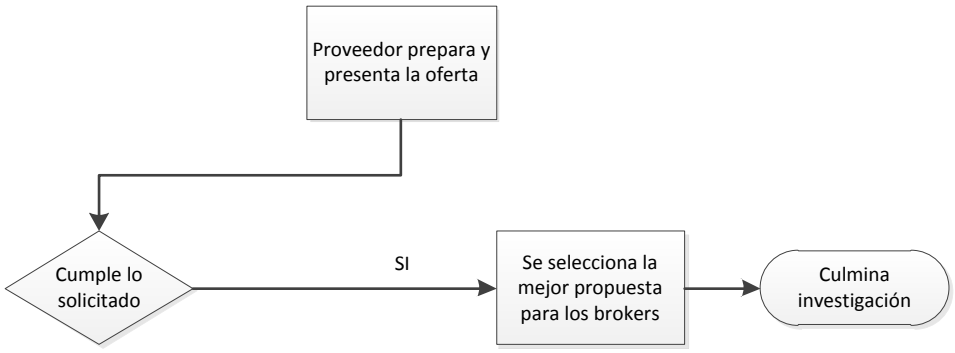


Gráfico # 29. Presentación de oferta por parte del proveedor (Parte 1). Fuente.- Autor

En esta parte el proveedor preparó y presentó la oferta de equipo que se adapta a las especificaciones solicitadas, con su respectiva propuesta económica la cual fue evaluada por el investigador y si se daba el caso de que se acogiera a todos los lineamientos se daba por culminada la investigación determinando el firewall idóneo para este tipo de

organizaciones con lo cual podrán tener protegida la información que consideran realmente importante.

En el caso de que el proveedor no pueda cumplir con algún punto detallado en los requerimientos básicos iniciales enviados al mismo, se presenta el siguiente escenario:

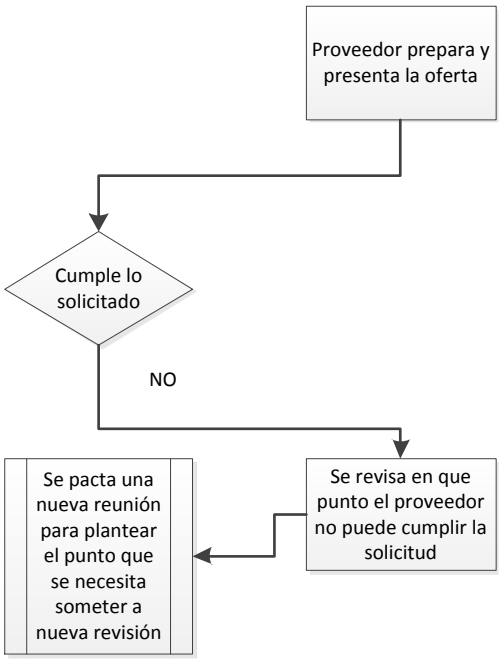


Gráfico # 30. Presentación de oferta por parte del proveedor (Parte 2). Fuente.- Autor

Si el proveedor no cumple uno de los puntos en este caso el económico se acordó una nueva reunión, en la que se presentó las características del firewall de las que se podría prescindir tales como ser rackeable, presentar status en consola, que no se cuente con algún modulo en específico, presentación de informes detallados, con menos puertos, etc., para de esta manera tratar de mejorar la oferta económica que se presentó inicialmente.

En dicha reunión el investigador propuso que se presente algún tipo de servicio con el equipo de tal modo que el bróker tenga que realizar el pago a largo plazo y no tenga que realizar un desembolso fuerte de dinero por con lo cual se podría ver afectado el presupuesto anual por un rubro que consideran se podría analizar posteriormente, cuando se presente un equipo o servicio que requiera menor inversión.

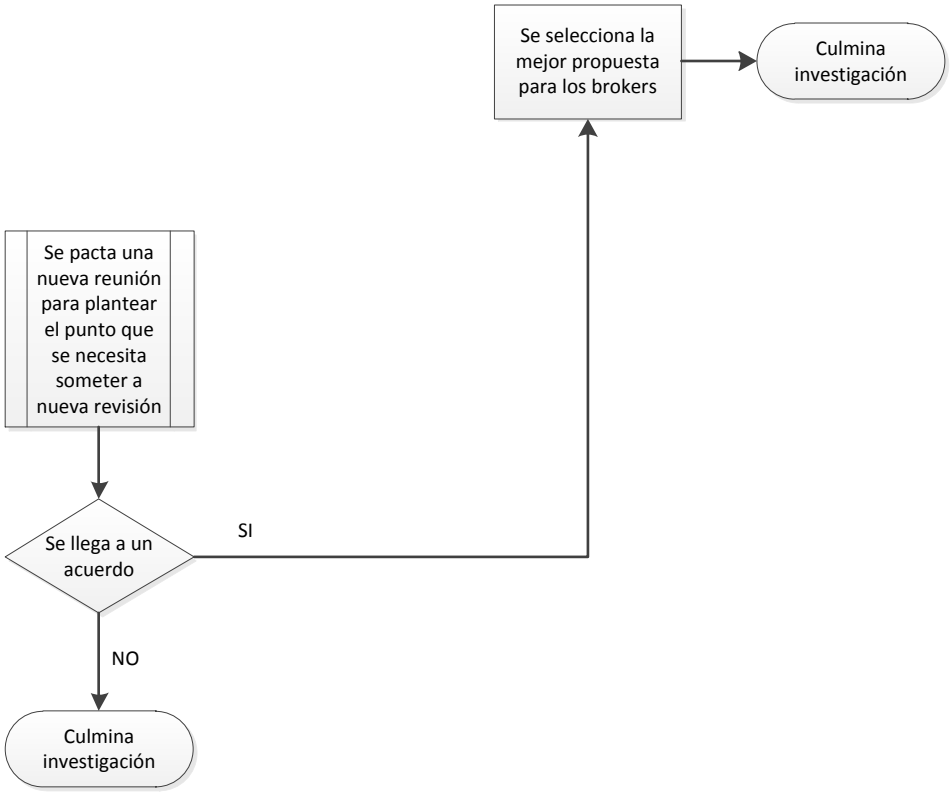


Gráfico # 31.Revisión del porque no aplica la propuesta. Fuente.- Autor

En la presente investigación no se obtiene una propuesta favorable para seleccionar un firewall idóneo para las agencias productoras y asesoras de seguros por el factor económico que es determinante, debido a que este tipo de organizaciones que están ubicadas entre las pymes del mercado ecuatoriano no están dispuestas a realizar grandes inversiones en el área de informática hasta que se dan cuenta que el área es un punto importante si se aspira al crecimiento de la organización.

CAPITULO IV
PRESENTACIÓN DE SOLUCIONES TECNOLÓGICAS

Se puede indicar que los firewall mencionados (Sophos, McAfee, D-Link) son muy buenas opciones en el mercado ecuatoriano, por sus características y por las buenas referencias de muchas empresas importantes del sector público y privado reconocidas en el país que cuentan con alguno de estos equipos en su infraestructura tecnológica. Es por ello que a pesar de que no se pudo seleccionar un firewall específico en el cual se desarrollaría y propondría un plan de implementación para las políticas de seguridad informática de los bróker de seguros se presenta a continuación las políticas básicas de seguridad informática que deberían tener todas las organizaciones entre estas las agencias productoras y asesoras de seguros de la ciudad de Guayaquil y si se presenta la oportunidad de realizar la adquisición de un firewall se presentan políticas básicas para implementar dentro del firewall.

4.1 POLÍTICAS BÁSICAS DE SEGURIDAD INFORMÁTICA

Debido al avance tecnológico que se ha presentado en los últimos años principalmente con el uso del internet, las organizaciones a nivel mundial se ven inmiscuidas en ambientes poco favorables para mantener segura la información que manejan, y se presentan como las próximas víctimas de los hackers que buscan cometer sus delitos con el fin de perjudicar a terceros.

Según se presenten los avances tecnológicos, también se presenta un avance continuo en los riesgos, los cuales obligan a todas las compañías a implementar planes de emergencia y políticas de seguridad para protegerse de posibles ataques. Vale mencionar que en muchas compañías del país en este caso las agencias productoras y asesoras de seguros de la ciudad de Guayaquil se percibe un poco de falta de concientización, poca disposición para la inversión en recursos que beneficien a la seguridad informática lo

cual retrasa el plan de seguridad que debería implementarse en cada una de estas organizaciones.

A nivel mundial la información que poseen las empresas en su poder se ha convertido en el principal punto a cuidar, por ello es importante establecer políticas de seguridad informática que ayuden a proteger cada uno de los activos de la compañía. Las mismas colaboran como instrumento para concientizar al personal de las empresas con respecto a la sensibilidad e importancia de la información que manejan y tienen al alcance de sus manos.

A continuación se presenta las políticas básicas de seguridad informática creadas a partir de puntos clave a tomar en consideración en una organización.

Cuando se realiza la instalación de equipos de computación se toma en cuenta lo detallado a continuación:

1. Toda herramienta tecnológica que esté conectada a la red corporativa y sea propiedad de la compañía deberá regirse a los lineamientos establecidos por el departamento de tecnología.
2. Toda herramienta tecnológica que tenga una labor específica, requiere contar con las condiciones idóneas para su correcto funcionamiento y cuidado, tales como las condiciones ambientales, seguridad física incluyendo su respectiva alimentación eléctrica adecuada.
3. Los colaboradores del departamento de tecnología debe encargarse de hacer cumplir a cabalidad los lineamientos establecidos por el departamento y de que se realicen las notificaciones correspondientes concernientes a cambios de ubicación de los equipos, actualización de los mismos, asignación del mismo a otro usuario, y todo lo que implique cambios en las herramientas tecnológicas.
4. El cuidado de las herramientas tecnológicas corresponde a la persona a la que fue asignada, y la misma está en la obligación de

informar al departamento de tecnología algún tipo de cambio o novedad que se presente en la herramienta que se le asigno.

5. El departamento de tecnología será el responsable de llevar un control de los equipos que sean propiedad de la compañía con la colaboración del departamento encargado del manejo de los activos fijos de la compañía.
6. Cuando un usuario sufra la pérdida o robo de la herramienta tecnológica proporcionada por la organización el departamento de tecnología se encargará de informar al departamento encargado del activo fijo para tener el respectivo registro de la novedad.
7. Si se necesita reubicar alguna herramienta tecnológica que pertenece o esté dentro de la empresa se realizará bajo previo análisis y autorización del departamento de tecnología que se encargara de certificar que el sitio de reubicación cumple con las medidas necesarias para la instalación.

Cuando se necesite realizar mantenimiento o actualización de los equipos de computación se recomienda lo siguiente:

1. El mantenimiento preventivo y correctivo de las herramientas tecnológicas que pertenecen a la organización son de expresa obligación del departamento de tecnología y si esto conlleva una actualización en los equipos se debe procurar conservar o mejorar la calidad de servicio que ofrece.
2. Si las herramientas tecnológicas de la organización presentan inconvenientes en su funcionamiento o simplemente su respectivo mantenimiento, el departamento de tecnología es el encargado de decidir si las mismas serán atendidas por terceros.
3. Si las herramientas tecnológicas tienen que ser atendidas por terceros, el departamento de tecnología será el encargado de coordinar y cuidar de las mismas.

En relación al acceso de las herramientas tecnológicas se considera lo siguiente:

1. Todas las herramientas tecnológicas son asignadas a una persona responsable, la cual se encarga de hacer el correcto uso y cuidado de la misma.
2. Todas las herramientas tecnológicas que se encuentren en las áreas de acceso general incluso las que reúnan características de imprescindibles se sujetaran a los lineamientos que establezca el departamento de tecnología.
3. Si en la organización existen herramientas tecnológicas que no pertenecen a la misma que estén conectadas a la red corporativa, el departamento de tecnología tendrá la facultad de acceder a las mismas en el momento que consideren conveniente.

Cuando se trata de supervisar el acceso a la red local se toma en cuenta lo que se presenta a continuación:

1. El departamento de tecnología es el encargado de asignar a los usuarios el acceso a los recursos informáticos según lo requieran sus funciones.
2. El departamento de tecnología es el encargado de difundir los lineamientos con respecto al uso de red y los permisos que se asignan para el acceso a la misma.
3. El acceso a servidores conectados a la red local estará permitido o denegado según lo estipule el departamento de tecnología.
4. Toda herramienta tecnológica que no pertenezca a la organización y que esté conectado a la red corporativa deberá someterse a los lineamientos establecidos por el departamento de tecnología con relación a los permisos de acceso.

Cuando se necesite acceso remoto a la organización se debe considerar lo siguiente:

1. El departamento de tecnología será el encargado de proveer el servicio de acceso remoto a los colaboradores con acceso limitado a los recursos informáticos y con previa autorización de la jefatura correspondiente.
2. Para el acceso especifico a los servidores o recursos que no se encuentran dentro del acceso limitado el colaborador tendrá que tener

autorización de la jefatura, recursos humanos y la gerencia de la compañía para que el departamento de tecnología proceda con la habilitación del acceso remoto a recursos específicos.

Si existe un sistema administrativo el acceso estará limitado por:

1. El acceso a los sistemas que maneje la organización para su administración o contabilidad que son de acceso restringido es de uso exclusivo del personal que labore en las áreas mencionadas.
2. El departamento de tecnología deberá proteger con algún tipo de contraseña el acceso a los archivos que contenga información administrativa para poder garantizar la integridad del mismo.
3. Solo el departamento de tecnología podrá tener acceso a los servidores de base de datos que contengan información del sistema administrativo.

Cuando se requiera revisar la vulnerabilidad de la red corporativa se determina lo siguiente:

1. Capacitar al personal del departamento de tecnología semestralmente en pruebas de hacking ético.
2. Someter a la red a test de penetración conocidos como el ciego, informado, interno o externo.
3. Contratar anualmente a diferentes empresas externas especializadas en seguridad informática para que realicen pruebas de hacking ético y según informe emitido por la compañía seleccionada proceder a las correcciones.
4. Revisar periódicamente los accesos que posee cada uno de los usuarios para verificar que tengan los correctos.
5. Cambio de claves de acceso cada 180 días.
6. Cuando un usuario deje de laborar en la organización se deberá cambiar sus claves de acceso, claves de correo electrónico, eliminar acceso remoto, y emitir mensaje de auto respuesta cada vez que envíen correo electrónico al ex colaborador informando que dejo de aportar con sus servicios a la compañía y detallar la persona que se hará cargo de las funciones que realizaba.

7. Cuando un usuario sufra la pérdida o robo se deberá cambiar sus claves de acceso, claves de correo electrónico, eliminar acceso remoto.

Y considerando normas básicas de cuidado de la información:

1. Cada área de la compañía se encargará de tener su plan de contingencia en referencia a las actividades importantes que realicen a diario.
2. El departamento de tecnología tendrá que sujetarse a códigos de ética profesional debido a toda la información que pueden manejar y tener acceso.

Cabe recalcar que la violación de alguna de las políticas básicas de seguridad informática establecidas, se regirá a sanciones que determine la compañía, las cuales pueden ir desde un llamado de atención hasta la separación del usuario dependiendo de la falta cometida o del grado de daño o perjuicio ocasionado a la organización.

Todo caso en el que se vea afectada la seguridad de la compañía y que no esté estipulada en las políticas antes mencionadas, la gerencia tendrá que resolver la sanción y el departamento de tecnología revisar en que ámbito se puede agregar alguna nueva política una vez autorizada por la gerencia.

4.2 POLÍTICAS BÁSICAS PARA IMPLEMENTAR DENTRO DE UN FIREWALL

1. El departamento de tecnología será el encargado de definir qué puertos agregará al firewall para la comunicación entre un sector y otro, los que no estén definidos se denegará la comunicación.
2. En caso de tener la red DMZ, esta deberá tener acceso a internet seleccionando puertos específicos o habilitando todos los puertos según se requiera.
3. La red interna deberá tener comunicación a la DMZ por todos los puertos.

4. En el caso de la red interna se deberá habilitar puertos HTTP para la navegación en la organización.
5. Se definirá accesos por parte de las aplicaciones externas que se necesite usar y requieran conexión a la red de la organización.
6. Se definirá accesos por parte de la organización que necesite usar y requiera conexión a través de aplicaciones externas.
7. Si algún equipo necesita tener habilitados todos los puertos se realizará la solicitud al departamento de tecnología y será el encargado de evaluar la necesidad y su posible impacto.
8. Se deberá definir y asignar ancho de banda específico para todas las subredes en caso de que las posea con el fin de tener un control del consumo.
9. Se deberá definir subredes en caso que se necesite conectar un gran número de equipos.
10. En caso de implementar alguna subred para el acceso a internet por parte de personas ajenas a la organización se deberá denegar el acceso por cualquiera de los puertos a la red de la organización.
11. En caso de implementar alguna subred para el acceso a internet por parte de personas ajenas a la organización se deberá denegar el acceso por cualquiera de los puertos a la red DMZ de la organización.
12. En caso de implementar alguna subred para el acceso a internet por parte de personas ajenas a la organización se permitirá el acceso a la web por todos los puertos con un ancho de banda definido.
13. La red de la organización tendrá acceso a todas las subredes de la organización a través de todos los puertos.
14. En caso de implementar una red VPN se establecerá el pool de usuarios los cuales tienen acceso a través de puertos definidos para el envío y recepción de correos, tales como el 143, 993, 110, 995 etc.
15. En caso de implementar una red VPN se establecerá el pool de usuarios los cuales tienen acceso a través de puertos definidos para mensajería instantánea, tales como el 5222, 1863, etc.
16. En caso de implementar una red VPN se establecerá el pool de usuarios los cuales tienen acceso a través de puertos definidos para navegación web, tales como el 80, 8080, 443, etc.

17. Se podrá acceder desde cualquier lugar del mundo a los servidores de la organización a través de los puertos DNS y viceversa si se lo considera necesario.
18. El departamento de tecnología deberá definir horarios de navegación permitida y restringida.
19. Se deberá elaborar una lista de URL a las cuales se les permitirá el acceso sin restricción alguna y una lista de URL a las cuales se les restringirá completamente el acceso.
20. Se deberá definir grupos de usuarios definiendo para cada uno de ellos listas de acceso.
21. De ser necesario se deberá agregar excepciones en relación a dominios de correos electrónicos que han caído en listas negras.
22. Dentro de la red DMZ se ubicará solo servidores y solo se permite lo que los servidores necesiten como actualizaciones y control remoto.
23. Se deberá realizar reserva de IPs por medio de la MAC para todos los equipos que pertenecen o estén dentro de la red corporativa.
24. Se deberá definir por cual interfaz entrará la conexión a internet y por cual estará la conexión a la red corporativa.
25. El departamento de tecnología deberá apoyarse con los reportes del firewall para la evaluación e implementación de mejoras en caso de ser necesario en la red corporativa.
26. Se deberá establecer conexiones VPN IP Sec entre sucursales para tener un mejor control de seguridad entre sucursales en lugar de usar túneles de datos proporcionados por el proveedor de servicios de internet.
27. Se deberá realizar test de penetración semestralmente para oportunamente poder cubrir las falencias que se puedan generar a partir de nuevas amenazas.

4.3 PLAN DE IMPLEMENTACIÓN DE POLÍTICAS

El plan de implementación de las políticas básicas de seguridad informática y de las políticas básicas para implementar dentro de un firewall detalladas puede darse a partir de que se organicen los siguientes detalles:

- Tener claro por parte del departamento de tecnología acerca de cuantas herramientas tecnológicas posee la organización, a quien están asignadas y en qué departamento se encuentran.
- Una vez estén definidas las normas y lineamientos de tipo tecnológico por el departamento de tecnología.
- Cuando se establezcan las sanciones al no cumplimiento de las políticas por parte de la gerencia y recursos humanos para que el departamento de tecnología pueda difundir las mismas antes y después de implementar las políticas.
- Una vez adquirido el equipo de firewall con los servicios que sean necesarios para la organización.

Una vez cumplidos los detalles mencionados, se puede cumplir con una implementación periódica de las políticas para cumplir con un periodo de adaptación entre el personal que está llamado a cumplirlas y el personal que está encargado de hacer cumplir las mismas, el cual no debería durar más allá de mes y medio.

CONCLUSIONES

A través de la investigación realizada, del estudio de campo realizado, de la comparación de todas las variables y el análisis resultante de todo el estudio se llega a las siguientes conclusiones:

El presente estudio permitió conocer el papel que desempeña la información en las organizaciones y se determinó que es el punto de mayor vulnerabilidad y el cual representaría en muchos casos un daño irreparable en caso de ser violentado.

Los bróker de seguros son susceptibles pero no han hecho conciencia de la vulnerabilidad a la que están expuestos, considerando que su activo radica en la información de los clientes, dado que el activo no es el archivo físico que pueden llegar a poseer. El poder analizar la información que poseen es indispensable para poder ofrecer nuevos productos a toda su cartera de clientes y las nuevas cuentas que desean obtener, por ello la información debe estar protegida y la investigación dilucida un punto que no se está tomando en consideración y es que se le está dedicando valores por debajo de los costos reales que tienen las empresas proveedoras de firewall en soluciones tanto en software como en hardware para la seguridad informática.

Las agencias productoras y asesoras de seguros de la ciudad de Guayaquil se encuentran en general desprotegidas inicialmente por no contar con personal de sistemas dentro de las organizaciones, lo cual no beneficia empezando por la seguridad informática interna, apenas 11 de las 40 empresas encuestadas cuentan con por lo menos 1 persona que se encarga de cuidar la integridad de la información y de los activos de la compañía en relación a tecnología.

Por lo cual se presenta la imperiosa necesidad de contar con al menos una persona que sepa de sistemas que esté al tanto de las amenazas que se presentan día a día, y pueda solventar las falencias que se pudieran

presentar ya que esta investigación permite evidenciar una realidad que no han visto hasta ahora.

Dado que la mayoría de este tipo de empresas no cuenta con un estándar de seguridad informática con el cual podrían cubrir necesidades básicas de protección, se procedió a diseñar políticas básicas de seguridad informática aplicables a este tipo de negocios con el fin de aplicarlas periódicamente y con ello empezar a protegerse ante cualquier eventualidad, y en caso de lograr un acuerdo para aumentar la inversión en equipos o software de seguridad informática como firewall se presentan políticas que se podrían implementar dentro del firewall para con ello proteger el acceso al bien más preciado que es la información.

El implementar políticas de seguridad informática en una organización no es una tarea fácil y para cual se necesita implementar un proceso y cumplir pasos y necesidades previas con el objetivo de que la implementación sea un éxito y no sea un obstáculo en el desarrollo de las actividades de la organización.

RECOMENDACIONES

Se recomienda tomar en cuenta los siguientes puntos:

- Se recomienda tener reuniones periódicas con la gerencia y recursos humanos para revisar las políticas de seguridad en caso de que se desee agregar, actualizar o eliminar alguna de las políticas en vigencia con el fin de tener mejores soluciones tecnológicas, para preservar la infraestructura existente en la organización y la información valiosa que se maneja diariamente. También es recomendable poseer planes de contingencia para los casos críticos que pongan en riesgo la seguridad informática y que afecten al correcto desarrollo de la compañía.
- Las personas encargadas de manejar la tecnología que forman parte de las agencias productoras y asesoras de seguros son las encargadas de concientizar a todas las áreas de este tipo de compañías especialmente en las áreas directivas para que reconsideren el valor a invertir en soluciones de protección, por medio de demostraciones de los daños que pueden causar las distintas amenazas que se pudieran presentar y con esto puedan ser testigo de la vulnerabilidad que presentan y los valores que consideran en su presupuesto no alcanzan para cubrir las necesidades de seguridad.
- A los proveedores de firewall que no han considerado a los bróker como cliente potencial deberían plantear varias alternativas de negocio como la de servicios asistidos, con el fin de obtener un nuevo cliente, muy aparte de los ingresos que pueden llegar a generar y poder ubicar sus equipos o soluciones dentro de otro sector con giro de negocio distinto a los que pudieran estar acostumbrados.
- Se recomienda evaluar semestralmente la opción de someter a este tipo de compañías a pruebas de ethical hacking por parte de empresas especializadas en este tipo de servicios con el objetivo de obtener una visión más clara en relación a la seguridad que necesitan.

BIBLIOGRAFÍA

Referencias

Aguilera López, P. (2010). *Seguridad Informática.* Madrid: Editex.

Arnedo Moreno, J., Cabot Sagrera, J., Guitart Hormigo, I., Noguera Otero, F. J., Macau Nadal, R., Marco Galindo, M. J., . . . Segret Sala, R. (2010). *Escaneando la informática.* Barcelona: UOC.

Atelin, P., & Dordoigne, J. (2007). *TCP/IP y protocolos de internet.* Barcelona: ENI.

Brookshear, J., Smith, D., & Brylow, D. (2012). *Introducción a la Computación.* Madrid: Pearson Educación.

Desongles Corrales, J., & Moya Arribas, M. (2006). *Conocimientos Básicos de Informática.* España: Mad, S.L.

España Boquera, M. C. (2003). *Servicios Avanzados de Telecomunicación.* Madrid: Díaz de Santos, S.A.

González Martínez, M., Lankenau Caballero, D., Lankenau Caballero, M. L., Valdez Salazar, M. I., Almaguer Flores, A., Dieck Assad, M. E., . . . Garza Leal, M. E. (2010). *Tecnologías de la información.* México: McGraw-Hill.

Hallberg, B. (2007). *Fundamentos de redes.* México: McGraw-Hill.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2010). *Metodología de la Investigación.* Mexico: McGraw-Hill.

Ibañez Carrasco, P., & García Torres, G. (2009). *Informática I.* México: Cengage Learning Editores, S.A.

López-Hermoso Agus, J., Martín-Romo Romero, S., Izquierdo Loyola, V., Montero Navarro, A., De Pablos Heredero, C., & Nájera Sánchez, J. (2000). *Informática Aplicada a la Gestión de Empresas.* Madrid: ESIC.

Namakforoosh, M. N. (2005). *Metodología de la Investigación.* Mexico: Limusa. Recuperado el 11 de Diciembre de 2013

Olimpia, B. (8 de Julio de 2013). *Amenazas Informaticas: Como preparar su empresa*. Obtenido de http://seguridadexpertos.com/?p=1006&doing_wp_cron=1394001290.9637870788574218750000

Pekka, H. (2002). *La etíca del hacker y el espíritu de la era de la información.* Destino.

Portantier, F. (2012). *Seguridad Informática.* Buenos Aires: Fox Andina.

Procuraduria General del Estado. (Mayo de 2013). *Código Penal.* Obtenido de www.pge.gob.ec/es/documentos/doc_download/226-codigo-penal.html

Revista Lideres.ec, R. (2 de Diciembre de 2013). *Revista Lideres.ec*. Obtenido de http://www.revistalideres.ec/tecnologia/Sebastian_Uzcategui-tecnologia-virtual-Cyber_Edge_0_1040295975.html

Royer, J.-M. (2004). *Seguridad en la informática de empresa.* Barcelona: ENI.

Superintendencia de Bancos y Seguros del Ecuador. (9 de Febrero de 2014). *Superintendencia de Bancos y Seguros del Ecuador.* Obtenido de http://www.sbs.gob.ec/practg/pk_ranking_comision.p_asesores_reporte?vp_cod_tip_instt=33&vp_cod_provincia=09&vp_fecha=31/12/2012

Téllez Valdés, J. (2009). *Derecho Informático.* México: McGraw-Hill.

ANEXOS

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

ENCUESTA PARA DESARROLLO DE TRABAJO DE TITULACIÓN

Tema: *Diagnóstico de la Seguridad que ofrecen los Firewalls para las Agencias Productoras y Asesoras de Seguros de la ciudad de Guayaquil.*

COMPAÑÍA: _____

NOMBRE: _____

1.- ¿Cuantas personas laboran actualmente en la organización?

5 a 30 personas ☐

31 a 60 personas ☐

61 a 100 personas ☐

101 a 150 personas ☐

151 personas o más ☐

2.- ¿Cómo considera usted a su ambiente de seguridad?

A.- Insuficiente ☐

B.- Medio Suficiente ☐

C.- Suficiente ☐

D.- Ideal ☐

E.- Se podría mejorar ☐

3.- Para la realidad actual de su compañía, considera usted que necesita tener un ambiente informático más seguro.

SI ☐ NO ☐

¿Porque?

_____

_____

_____

_____

4.- De acuerdo al grado de importancia clasifique ¿Que datos considera usted como sensibles y que no quisiera perder?

5 muy importante		4 importante		3 medianamente importante		2 poco importante		1 nada importante	
Pólizas	☐	Clientes	☐	Empleados	☐	Cobranzas	☐		
Administración	☐	Mercadeo	☐	Noticias internas	☐	Inventario	☐		
Instaladores	☐	Comercial	☐	Contabilidad	☐	Aplicaciones adquiridas	☐		
Siniestros	☐	Digitalizaciones	☐						

5.- ¿Conoce las amenazas a las que se encuentra expuesta su organización en temas referentes a la seguridad informática? Mencione 4.

1.- _____

2.- _____

3.- _____

4.- _____

6.- ¿Cuánto estaría dispuesto a invertir por equipos de seguridad informática (FIREWALL) y capacitaciones al personal que será el encargado de administrarlo?

A.- Entre 1000 y 3500 dólares ☐

B.- Entre 3500 y 6000 dólares ☐

C.- Entre 6000 y 8000 dólares ☐

D.- Entre 8000 y 10000 dólares ☐

E.- Más de 10000 dólares ☐

7.- Su organización ofrece algún tipo de seguro que contribuya a la protección de los clientes ante los delitos informáticos.

SI ☐ NO ☐

¿Con que nombre se lo solicita?_____

_____

8.- Con respecto a la información que se maneja en su compañía, conoce usted si los datos de cualquier tipo tienen opción a salir de la organización por algún medio tecnológico.

A.- Extremadamente Improbable ☐

B.- Improbable ☐

C.- Algo probable ☐

D.- Probable ☐

E.- Muy probable ☐

9.- ¿Su empresa posee políticas de seguridad informática?

SI ☐ NO ☐ NO CONTESTA ☐

10.- El riesgo al que se exponen los bróker de seguros en referencia a los delitos informáticos lo considera:

A.- No severo ☐

B.- Poco severo ☐

C.- Medianamente severo ☐

D.- Severo ☐

E.- Muy severo ☐

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

ENCUESTA PARA DESARROLLO DE TRABAJO DE TITULACIÓN

Tema: *Diagnóstico de la Seguridad que ofrecen los Firewalls para las Agencias Productoras y Asesoras de Seguros de la ciudad de Guayaquil.*

COMPAÑÍA: _____

NOMBRE: _____

1.- En lo referente al área de tecnología, ¿con que tipo de seguridad cuenta actualmente?

Firewall Hardware ☐

Firewall Software ☐

Soluciones EndPoint ☐

Redes con contraseña ☐

Firewall Nativo del S.O. ☐

2.- En el último año, ¿Ha sufrido algún tipo de ataque o se ha presentado alguna amenaza de consideración?

SI ☐ NO ☐ NO CONTESTA ☐

3.- Indique por favor el número aproximado de amenazas presentadas en el último año.

0 ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 o mas ☐

4.- ¿La totalidad de sus servidores se encuentran físicamente dentro de su organización?

SI ☐ NO ☐

5.- Tomando en cuenta que las compañías de seguros tienen puntos de servicio fuera de su organización, ¿Cómo esos equipos se interconectan con los servicios de su compañía? Puede seleccionar una o varias alternativas.

VPN ☐ Logmein ☐ Teamviewer ☐ UltraVNC ☐

VPN con ESC. REMOTO ☐ Servicios WEB ☐ Putty ☐ Power Grid ☐

6.- ¿Cómo se interconectan las sucursales de las diferentes ciudades en caso de que las tuvieran?

A.- VPN ☐

B.- TUNEL DE DATOS ☐

C.- RADIOENLACE ☐

D.- VPN IPSEC PERPETUA ☐

C.- COMBINACION DE B y D ☐

7.- ¿Su compañía posee políticas de seguridad para proteger su red empresarial de ataques tanto internos como externos?

Ninguna ☐

Parcialmente definidas ☐

Definidas por tipos de usuario ☐

Definidas por departamento ☐

Totalmente definidas ☐

8.- El ancho de banda contratado con su ISP (Internet Service Provider) ¿satisface las necesidades de su compañía?

A.- Insuficiente ☐

B.- Medio Suficiente ☐

C.- Suficiente ☐

D.- Ideal ☐

E.- Se podría mejorar ☐

9.- ¿Qué ancho de banda posee actualmente en su organización?

A.- 1 a 2 Mbps ☐

B.- 3 a 5 Mbps ☐

C.- 6 a 9 Mbps ☐

D.- 10 a 12 Mbps ☐

E.- 13 Mbps o más ☐

10.- ¿Cuál es el nivel de compartición que tiene su contrato de internet?

A.- Sin compartición ☐

B.- 2:1 ☐

C.- 4:1 ☐

D.- 6:1 ☐

E.- 8:1 ☐

11.- ¿Con cuál de los siguientes proveedores tiene contratado su internet?

A.- Telconet ☐

B.- TV CABLE ☐

C.- Claro ☐

D.- CNT ☐

E.- NETLIFE ☐

Otro: _____

12.- ¿Cómo distribuye el consumo de ancho de banda entre los usuarios de su organización?

A.- Todos tienen acceso por igual ☐

B.- Se asigna ancho de banda según las redes disponibles ☐

C.- Jefaturas deciden los accesos a internet de sus usuarios ☐

D.- Lo define el departamento de T.I. ☐

E.- Se define según las transacciones por departamento ☐

13.- El recurso humano destinado a velar por la seguridad informática de su compañía cumple con capacitaciones periódicas para estar al día con la información de las nuevas amenazas y prevención, ¿cuál es la frecuencia de estas capacitaciones?

A.- Diariamente ☐

B.- Semanalmente ☐

C.- Mensualmente ☐

D.- Semestralmente ☐

E.- Anualmente ☐

F.- Nunca ☐

14.- ¿Cómo analiza la vulnerabilidad de su red empresarial?

A.- Herramientas de auditoria informática ☐

B.- Revisión periódica de los permisos de acceso ☐

C.- Logs o reportes emitidos por equipo o software de seguridad empresarial ☐

D.- Pruebas anuales de Ethical Hacking ☐

E.- Otros: _____ ☐

15.- Cuando un usuario renuncia o es separado de la compañía, ¿Cómo protege la información a la cual tuvo acceso?

A.- Eliminación de usuario ☐

B.- Eliminación de correo ☐

C.- Cambios de claves de acceso ☐

D.- Anulación de permisos ☐

E.- Otra: _____ ☐