PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN

PROYECTO DE TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE MASTER EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN

"ANÁLISIS DE FACTIBILIDAD PARA BRINDAR SERVICIOS ADMINISTRADOS DE SEGURIDAD PERIMETRAL DE REDES PARA GRANDES EMPRESAS DE COMERCIO AL POR MENOR"

CALDERÓN VALAREZO PABLO SEBASTIÁN

ULLOA MÁRQUEZ JULIO ALEXANDER

DIRECTOR:

MTR. JAVIER CÓNDOR

Quito, 05 2014

RESUMEN

En los últimos 20 años, el uso del Internet en las empresas, además de ser una ventaja de negocio, se ha convertido en una preocupación, debido a los riesgos que se generan al exponer la información de redes privadas al público. Esto ha llevado a que las empresas dediquen tiempo, esfuerzo y dinero en implementar y administrar esquemas de seguridad en las diferentes capas dentro de sus infraestructuras, siendo la capa perimetral la más vulnerable al acceso de intrusos. Por esta misma razón han aparecido en el mercado un sinnúmero de empresas orientadas a desarrollar y fabricar equipamiento dedicado a la seguridad perimetral de redes; cada uno de estos fabricantes con sus diferentes ofertas de equipos pretende mitigar determinadas amenazas de seguridad que se han venido presentando en el tiempo.

Las empresas están conscientes de la importancia de proteger la información, ya que es su activo más valioso, por lo que cada vez invierten más para conseguir ambientes seguros y parte de esta inversión se destina a la administración de estos esquemas de seguridad perimetral de redes con personal in-house, personal que muchas de las ocasiones no es especializado en el tema o que comparte su tiempo realizando otras actividades. El invertir en personal para administrar equipos que no forman parte de la cadena de valor de las empresas puede derivar en gastos excesivos, por lo que los servicios administrados aparecen como una alternativa en la forma de operar la seguridad perimetral de red de una empresa.

En la presente investigación se van a desarrollar estos temas de manera detallada, empezando por los conceptos y la teoría, con lo que se tendrá un mayor

entendimiento de los servicios administrados y la seguridad de la información. A continuación se analizará las implicaciones de ofrecer servicios administrados de seguridad perimetral a empresas de comercio al por menor desde el punto de vista legal, operativo y tecnológico, para luego continuar con una investigación de mercado que permitirá la evaluación económica-financiera de este proyecto de inversión. Adicionalmente se definirá un portafolio de servicios para poder comercializarlo y se presentará un análisis del ahorro que puede representar a una empresa el invertir en este tipo de servicios. Finalmente se detallarán los resultados de la presente investigación con sus correspondientes recomendaciones y las posibles investigaciones que pueden derivarse de este análisis.

DEDICATORIA

JULIO

A mis hermanos Nadia, Vladimir y Jorge por todo el esfuerzo y dedicación que imprimen cada día de sus vidas

PABLO

Dedico el presente trabajo a mi esposa Cindy Romero por el apoyo y ánimo que siempre me brindó para poder culminarlo.

AGRADECIMIENTOS

JULIO

A mi esposa Lorena Medina por brindarme su amor y su apoyo en la consecución de este objetivo. A mis padres Janneth Márquez y Segundo Ulloa por brindarme día a día su amor incondicional.

PABLO

Agradezco a todos los que nos colaboraron para poder culminar este proyecto, principalmente a Dios y a la Virgen María.

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CAPÍTULO 1. MARCO TEÓRICO

En este capítulo se revisarán los conceptos que conforman la base teórica del tema elegido para su análisis, los cuales son seguridad de la información, servicios administrados y clasificación de las empresas. En la primera parte se presentan conceptos clave para entender de manera general que es lo que la empresa pretende lograr al manejar seguridad de la información, cuales son las áreas más críticas dentro de una infraestructura de red que necesitan ser protegidas y cuáles son los equipos que se utilizan para implementar estas protecciones. La segunda parte trata los servicios administrados, definiéndolos en base a la comparación con otros términos populares que se manejan en el mercado como lo son el *outsourcing*[1] y el *cloud computing*[2]. Finalmente, en la tercera parte se muestra cual es la clasificación que da el ente regulatorio local a las empresas del Ecuador para tener claro cuál es el mercado que se quiere cubrir con el servicio que se está proponiendo.

1.1. Seguridad de la Información

Conforme las empresas han visto la necesidad de apoyarse en la tecnología no solo para manejar sus procesos operativos sino más bien para lograr la innovación que les permite seguir existiendo, la seguridad de la información ha ido cobrando cada vez un mayor protagonismo, tanto así que se ve que está presente en todo tipo de empresas, independiente de la actividad de negocio principal de las mismas.

[1] Subcontratación, externalización.
[2] Computación en la nube.

Uno de los activos de mayor valor que posee cualquier tipo de empresa es la información. Esta información es generada a través del procesamiento de un conjunto de datos que son usados como entradas o salidas de los procesos empresariales. El gran valor que tiene la información dentro de una empresa radica en que esta genera conocimiento, el cual, desde un punto de vista de negocio, puede ser usado por ejemplo por las empresas privadas para generar una ventaja competitiva frente al resto de empresas de su misma rama y de esta manera aumentar las ventas de su producto o servicio. De ahí que es tan importante que existan los mecanismos necesarios para proteger esta información.

La información y los datos están alojados en sistemas tecnológicos que hacen posible que los usuarios que los necesiten pueden acceder a ellos. Sin embargo, debido a esta característica de permitir el acceso a la información que tienen los sistemas tecnológicos, se crea una exposición de esta misma información a usuarios no deseados. Es ahí donde entra la seguridad de la información, la cual puede ser definida como "todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma" [1].

Las últimas características mencionadas en la definición de la seguridad de la información son conocidas como la triada CIA[3] por sus siglas en inglés (Figura 1.1). El primer componente de la triada, la confidencialidad, trata acerca de la privacidad y hace referencia a la habilidad de proteger los datos de aquellos que no están

[3] Confidentiality, Integrity, Availability

autorizados para verlos. El segundo componente, la integridad, hace referencia a la habilidad de prevenir que los datos sean cambiados de una manera no autorizada o no deseada además de poder reversar cambios no deseados hechos por personas autorizadas. El último componente es la disponibilidad, la cual hace referencia a la habilidad de acceder a los datos cuando se necesite hacerlo. Como una alternativa a la triada CIA se creó el sexteto de Parkerian, el cual introduce tres componentes adicionales: posesión o control, autenticidad y utilidad (Figura 1.2).

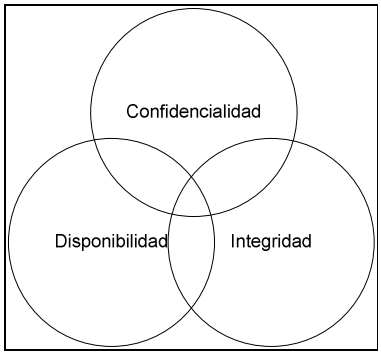

Figura 1.1. Triada CIA [A]

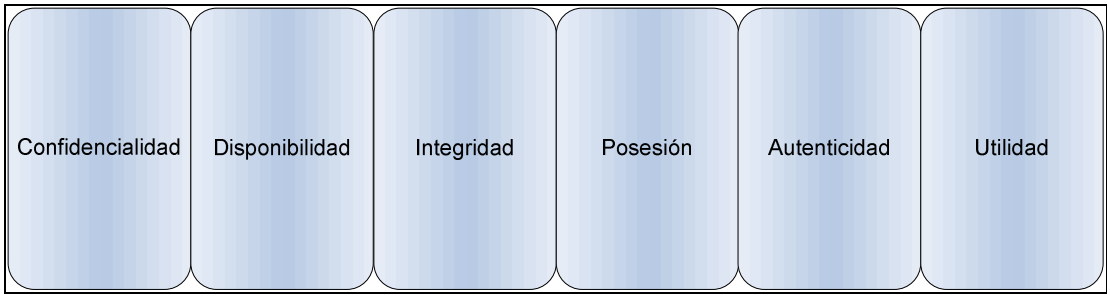

Figura 1.2. Sexteto de Parkerian [A]

En resumen, la seguridad de la información busca proteger los datos y los sistemas de aquellos que buscan su mal uso.

La relación entre los niveles de seguridad de la información que maneja una empresa y su productividad es inversamente proporcional, es decir mientras el nivel de seguridad de la información sea más alto, menor será el nivel de productividad. En base a esto, es necesario realizar un análisis costo-beneficio cuando se quiera implementar un nuevo mecanismo de seguridad de la información, teniendo en cuenta que el costo del mecanismo a implementar nunca debe exceder el valor de aquello que está protegiendo.

Para que las empresas puedan tener un referente de que mecanismos deben adoptar para manejar la seguridad de la información existen varias organizaciones que han creado estándares o que han definido mejores prácticas en base a la experiencia de la implementación de seguridad de la información en muchas empresas. Algunos de estos estándares son:

- ISO 27000 de la ISO[4] y la IEC[5].
- Standard of Good Practice del ISF[6].
- PCI[7] Data Security Standard del Consejo de estándares de Seguridad PCI.
- RFCE-2196 de The Internet Society.

Como se puede apreciar en la mayoría de los estándares que tratan la seguridad de la información, esta no hace referencia a una tecnología en particular sino que más bien define un marco de trabajo que engloba varias áreas, cada una de la cual está compuesta de capas de seguridad. Mientras más elementos de seguridad o capas

[4] International Organization for Standardization
[5] International Electro-technical Commission
[6] Information Security Forum
[7] Payment Card Industry.

tenga un área, más segura estará la información contenida en esa área. No existe una sola tecnología implementada sobre una capa que pueda resolver todos los problemas de seguridad de una empresa. Es ahí donde nace el concepto de defensa en profundidad, el cual dice que para cada una de las áreas se debe tener una variedad de defensas independientes. Esta división en áreas hace que, en caso de que se presente un ataque por parte de un intruso, este tenga que sortear cada una de las áreas para poder llegar finalmente a la información o a los datos y que en cada una de la áreas se encuentre con una variedad de defensas independientes lo que va a hacer que el ataque se vuelva más lento y que probablemente el atacante desiste de su propósito.

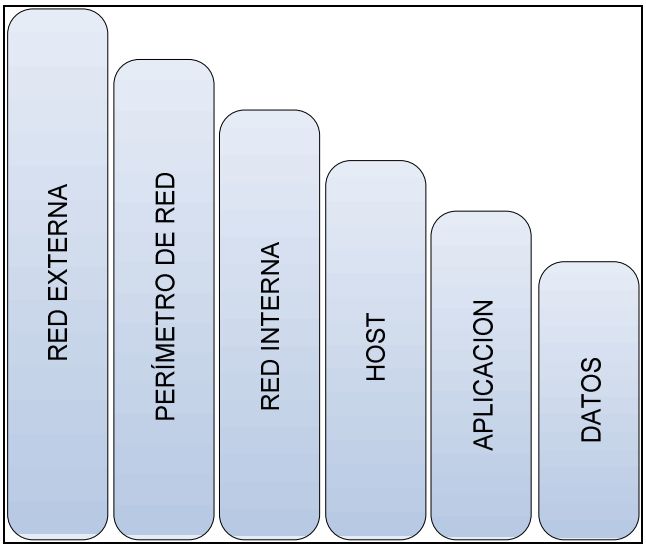

Figura 1.3. Áreas del modelo de defensa en profundidad [A]

Entre las áreas que se pueden definir para manejar seguridad de la información se encuentran la de operación, la física, la de sistema operativo, la de aplicación y el área de seguridad de red. En la siguiente sección se profundiza más en esta última

área, la cual nos permitirá llegar a definir, en conjunto con la sección de arquitectura de redes, que es la seguridad perimetral de redes.

1.1.1. *Seguridad de red*

La seguridad de red es el mecanismo para proveer acceso apropiado y consistente a información confidencial en una organización mientras se asegura la integridad de la misma. Como se mencionaba cuando se definía la seguridad de la información, la seguridad de red es un área que se maneja con una arquitectura de capas la cual se basa en un apropiado diseño de red.

Para comenzar con la seguridad de redes, el acercamiento más acertado es preguntarse qué es lo que la empresa necesita proteger y plasmarlo en una política de seguridad. Con esto, todos los actores que participan de la seguridad de red estarán conscientes de que es lo que la empresa necesita de ellos para lograr mantener una red segura además de minimizar el impacto de las acciones del eslabón más débil que tiene el ecosistema de una empresa, el ser humano, ya que este incorpora un variable de incertidumbre al lenguaje binario que manejan los sistemas de seguridad de red.

Lo que generalmente ocurre en una empresa es que se piensa en la seguridad de red como un departamento o equipo de trabajo que va a ser el responsable de dar este servicio. Aquí el sistema de seguridad de red se limita a lo que el equipo puede ofrecer y no a lo que la empresa necesita. Una vez que se tenga clara la política de seguridad se puede proseguir elaborando el modelo de seguridad, el cual define el hardware, software y las pautas de las configuraciones que hagan cumplir la política

de seguridad establecida. Mientras que la política de seguridad de red es un enunciado de alto nivel que describe la filosofía, el ambiente laboral y las metas de la organización en el área de seguridad de red, el modelo es una serie de pasos a seguir para implementar estas metas y se basa en estándares y procedimientos. Como complemento al modelo existen las guías de configuración, las cuales llegan al detalle de que se debe configurar y con qué valor.

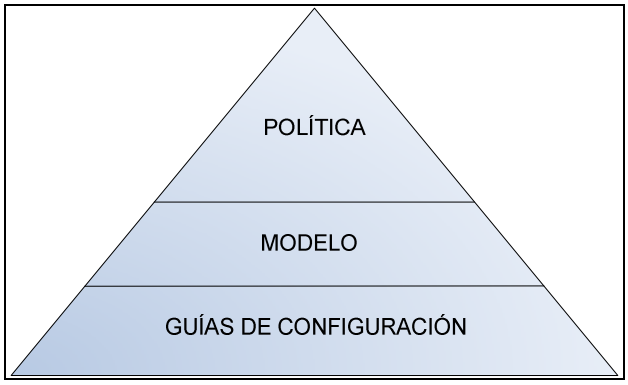

Figura 1.4. Capas de modelo de seguridad de red [A]

1.1.2. *Arquitectura de redes*

La arquitectura de redes es el diseño de una red de comunicaciones. Esta tiene como objetivo lograr un diseño modular y que dentro de cada módulo o área se tenga una jerarquía definida entre sus componentes. Entre las áreas que generalmente se definen en una arquitectura de redes se encuentran el perímetro del proveedor de servicios, el perímetro empresarial, el campus empresarial, las sucursales y el centro de datos. Estas áreas no definen ubicaciones físicas dentro de la infraestructura de red de una empresa sino más bien son áreas lógicas que pueden estar dispersas en toda la infraestructura. Es así que pueden existir varios

campus empresariales dispersos, cada uno de los cuales pueden estar localizados en una diferente ubicación física.

Desde el punto de vista de arquitectura, cada área es importante ya que cumple un papel o rol en particular. Sin embargo, desde el punto de vista de seguridad de red, el área más crítica es el perímetro empresarial por las razones que se expondrán en la siguiente sección.

1.1.2.1. Perímetro empresarial

El perímetro empresarial está definido como el área que concentra las conexiones entregadas por el perímetro de los proveedores de servicios. Las conexiones entregadas por el proveedor de servicios pueden ser el Internet, la *WAN*[8] y las conexiones de acceso remoto.

Las conexiones de Internet son dadas por proveedores conocidos como *ISPs*[9]. El Internet es la red de comunicaciones más grande del mundo debido en gran parte al uso estándar de protocolos *TCP/IP*[10] sin importar que red física esté por debajo. El Internet es usado por las empresas principalmente para permitir que los usuarios accedan a la información contenida en esta red. Adicionalmente, la empresa usa el Internet para publicar servicios al mundo como por ejemplo su página web. Otro servicio muy importante que utiliza el Internet es el correo electrónico empresarial, el cual en porcentaje puede llegar a ocupar la mayoría del ancho de banda del

[8] Wide Area Network
[9] Internet Service Providers
[10] Transport Control Protocol / Internet Protocol

enlace de Internet provisto por el ISP. La gran mayoría de las empresas cuentan por lo menos con un ISP. Existen empresas que manejan más de un ISP en una misma localidad y otras que tienen un ISP por cada localidad donde se encuentran presentes. Debido a su naturaleza de multiacceso y de cobertura global, la entrada del Internet de una empresa es la zona más expuesta a amenazas que pueden ser tan básicas como un escaneo de puertos o más elaboradas como un ataque dinámico de negación de servicio. Al igual que los niveles de las amenazas, los motivos de los atacantes son variados y generalmente no son claros.

La WAN es definida como una red de largo alcance geográfico. En el mundo de las redes y las telecomunicaciones, la WAN hace referencia a la zona que recibe las conexiones de los socios de negocios de las empresas, ya sean estos clientes o proveedores. El costo de estas conexiones o enlaces varía dependiendo del tipo de tecnología que se use y el ancho de banda o capacidad requerida. Las tecnologías que generalmente se utilizan en la WAN son *MPLS*[11], *Frame-Relay*, *ATM*[12] o fibras obscuras.

El acceso remoto se identifica como la zona que recibe una conexión hacia la *PSTN*[13] dada por el perímetro del proveedor de servicios. Tiene como funcionalidad permitir el establecimiento de un enlace para acceder a los servicios de la empresa desde lugares remotos utilizando una línea telefónica. El equipo que maneja este tipo de conexiones se lo conoce como RAS[14]. Debido a la penetración del Internet y

[11] Multiprotocol Label Switching
[12] Asynchronous Transfer Mode
[13] Public Switched Telephone Network
[14] Remote Access Server

la facilidad de implementación de las *VPN*s[15] cliente-servidor, esta zona ha ido perdiendo importancia y en muchos casos ha desaparecido. En la mayoría de las empresas donde aún existe se la considera una zona de acceso de contingencia, utilizada en caso de que las conexiones de las otras zonas fallen.

En resumen el perímetro empresarial concentra las conexiones de Internet, de telefonía y de enlaces que salen del perímetro del proveedor de servicios. Desde el punto de vista de seguridad de red, esta área es la más crítica debido a que es la puerta que separa la red segura administrada por la empresa de las redes inseguras que no están bajo la administración de la empresa. El presente trabajo se concentra en la administración de servicios de seguridad para esta área.

1.1.3. *Seguridad perimetral de redes*

La seguridad perimetral de redes es la seguridad de redes aplicada a un área en particular considerada la de más alto riesgo, el perímetro empresarial. Si se define al riesgo como la probabilidad de que una amenaza afecte a una vulnerabilidad, el perímetro empresarial es de alto riesgo ya que está expuesto a una gran variedad de amenazas, más que ninguna otra área, al ser la puerta de entrada de redes inseguras a la red segura de la empresa. Las medidas que se toman para mitigar los riesgos se los conoce como controles. Estos pueden ser de tipo físico, lógico y administrativo. Un control de tipo físico para mitigar los riesgos a los que está expuesto el perímetro de la red podría consistir en controlar el acceso a la ubicación física donde se encuentran instalados los equipos que protegen el perímetro. Un

[15] Virtual Private Networks

ejemplo de control de tipo lógico son las reglas de control de acceso configurados en un firewall. Por último, el control de tipo administrativo está más relacionado con la política manejada por la empresa en relación a la seguridad de la información y podría consistir en la obligatoriedad de llenar un documento de control de cambios antes de realizar una nueva configuración en un equipo.

Los ataques a los cuales está expuesto el perímetro de la red y que deben ser mitigados se los puede agrupar en cuatro categorías: intercepción, interrupción, modificación y fabricación. Los ataques de intercepción permiten a usuarios no autorizados acceder a los datos, aplicaciones o ambientes. Los de interrupción hacen que los bienes no estén disponibles para el uso de manera temporal o permanente. Los ataques de modificación manipulan los bienes. Por último, los de fabricación están relacionados con la generación de datos, procesos, comunicaciones u otras actividades similares con un sistema. Algunos ejemplos de ataques que generalmente se observan en el perímetro empresarial son la negación de servicio, generación de spam y el escaneo de puertos.

Los controles que se implementan para lograr una seguridad en el perímetro de la red son manejados por varios tipos de equipos, cada uno de los cuales tiene su función particular. A continuación se presentan los equipos más populares utilizados para asegurar el perímetro de la red.

1.1.3.1. Firewalls

Los firewalls son los equipos principales utilizados para prevenir ataques y van ubicados en la periferia de las redes. Existen dos tipos de firewalls: firewalls de

filtrado de paquetes y firewalls de filtrado de paquetes con información de estado. Los firewalls de filtrado de paquetes analizan las direcciones IP y los protocolos de los paquetes que lo atraviesan para luego comparar esta información con un conjunto de criterios o reglas definidas por el administrador del firewall y en base a esta comparación tomar la decisión de dejar pasar o no dicho tráfico. Las reglas pueden ser aplicadas de entrada o de salida. Los firewalls de filtrado de paquetes con información de estado utilizan el concepto de sesiones, las cuales se pueden definir como varias conexiones entre dos hosts que comparten la misma información de dirección IP y puerto origen y dirección IP y puerto destino. Basándose en esto, el firewall con información de estado puede rastrear las sesiones al monitorear el tráfico de los usuarios y configurar de manera automática las reglas de regreso del tráfico, facilitando de esta manera la administración del equipo.

Los firewalls delimitan tres tipos de zonas: la interna, la externa y la DMZ[16]. La zona interna o segura está asociada con la LAN[17]. La zona externa o insegura es la que recibe el enlace de Internet. La DMZ aloja a los servidores como los web, DNS, de archivos, de correo electrónico, entre otros. La DMZ posee restricciones de acceso que son más estrictas que las manejadas en la zona interna pero menos que las que se encuentran configuradas para la zona externa.

Otra tarea generalmente atribuida al firewall es la de realizar la traducción de direcciones de red (NAT[18]), que consiste en convertir en tiempo real direcciones IP. Generalmente esta conversión se la realiza entre direcciones IP privadas a

[16] Demilitarized zone
[17] Local Area Network
[18] Network Address Translation

direcciones IP públicas. Existen tres tipos de NAT: estático, dinámico y de sobrecarga. El NAT estático es un NAT uno a uno, es decir, una dirección IP es convertida en otra dirección IP distinta. El NAT dinámico convierte un conjunto de direcciones IP en otro conjunto de direcciones IP distintas. El NAT de sobrecarga convierte un conjunto de direcciones IP a una sola dirección IP pero con diferentes puertos.

1.1.3.2. IDS[19] / IPS[20]

El IDS/IPS es un equipo que monitorea la actividad de la red para detectar tráfico malicioso. Es ubicado en línea con la red entre el router externo y el firewall con la finalidad de que pueda detectar ataques antes de que estos sean procesados por el firewall. A diferencia de los firewalls, los IDS/IPSs no solamente revisan las cabeceras de los paquetes sino también su contenido.

Existen dos tipos de IDS/IPS, los basados en firmas y los basados en estadísticas. Los primeros poseen una base de datos de firmas, las cuales tienen información de patrones de ataque y utilizan estas firmas para compararlas con el tráfico que atraviesa el equipo y de esta forma determinar si es que este tráfico de red corresponde a tráfico normal o es un ataque. Los equipos basados en estadísticas se dividen a su vez en basados en comportamiento y basados en tráfico. El primer tipo crea una línea de referencia en base al monitoreo del comportamiento del usuario sobre el tiempo y genera una alerta cuando algo fuera de esta línea base

[19] Intrusion Detection System
[20] Intrusion Prevention System

ocurre. El segundo tipo crea una línea base al monitorear el tráfico de red en el tiempo y dispara una alerta cuando se detecta tráfico de red anormal.

Los ataques de día cero son aquellos para los cuales todavía no existen firmas liberadas por los fabricantes debido a que acaban de salir. Para este tipo de ataques, los IDS/IPSs basados en firmas no son útiles ya que no tienen manera de reconocer el ataque debido a que no tienen una firma con la cual emparejarlo. Para este escenario, los IDS/IPS basados en estadísticas son los ideales ya que no manejan un método estático de detección de anomalías.

Es importante mencionar que todos los IDS/IPSs requieren de una etapa de afinamiento después de que son puestos en producción, ya que al inicio habrá un sinnúmero de falsos positivos, los cuales se producen cuando tráfico normal de usuarios es detectado como ataque.

1.1.3.3. Equipo de filtrado web

El Internet permite realizar varias actividades, como por ejemplo utilizar aplicaciones para descargar contenido, realizar videollamadas, manejar mensajería instantánea, pero la más popular de todas es la navegación web. Los equipos de filtrado web hacen que la navegación dentro de la empresa esté orientada a cumplir con los objetivos de negocio, evitando de esta manera la pérdida de productividad de los empleados y la exposición de la red segura debido a: navegación a sitios web que no están relacionados con el negocio, incremento en el consumo del ancho de banda del enlace de Internet por aplicaciones web no legítimas, exposición de información confidencial a través de sitios web para chat, incremento

de la exposición de la red empresarial a amenazas web como virus, gusanos, troyanos y spyware e infringir los derechos de autor debido a la descarga de multimedia desde sitios webs ilegales.

Los equipos que manejan el filtrado web son también conocidos como proxies de aplicación, control de contenido o gateways de web seguros. Los equipos de filtrado web están compuestos por aplicaciones de software que generalmente corren en equipos dedicados que se encuentran en el perímetro empresarial y que tienen como objetivo permitir o bloquear el contenido web que llega a través de Internet.

Los equipos de filtrado web pueden estar ubicados en medio o a un lado del paso del tráfico hacia Internet. La ubicación de los equipos de filtrado web tiene incidencia sobre las configuraciones que requieren los navegadores web de los usuarios. Para el caso en el cual el equipo de filtrado web se encuentra en medio del tráfico hacia el Internet, el administrador tiene la opción de hacer que los navegadores web de los usuarios requieren una configuración en la cual apunten al proxy para poder navegar o también tiene la opción de que no se requiera ninguna configuración en el navegador web. En el segundo caso, en el cual el equipo de filtrado web no está en el camino del tráfico hacia el Internet, el navegador web de los usuarios necesariamente debe tener la información del equipo de filtrado web, el cual se convierte en un proxy. Dependiendo del navegador web que se utilice en la empresa, la información del proxy puede ser enviada de manera automática o requerir que sea ingresada manualmente.

Los métodos más populares que existen para manejar el filtrado web son listas de palabras prohibidas, bloqueo por URLs[21], bloqueo por categorías y más recientemente el filtrado basado en imágenes. Los equipos de filtrado web pueden manejar uno de los métodos mencionados o varios de ellos de manera simultánea. El método de listas de palabras prohibidas consiste en la comparación del contenido de las URLs o de la página web con las de un diccionario formado por palabras o frases de una lista negra, la cual puede ser dada en un inicio por el fabricante del equipo y que posteriormente debe ser actualizada por el administrador del equipo. El bloque de URLs consiste en la configuración estática de una lista de páginas web que se quieren permitir o bloquear. Finalmente, para el bloqueo por categorías el administrador del equipo de filtrado web selecciona las categorías que son permitidas o restringidas para un usuario. Cada categoría abarca un grupo de URLs, haciendo que la administración de estos equipos sea mucho más fácil que con los otros métodos mencionados. Entre las categorías más comunes que se encuentran están contenido ilegal, contenido sexual explícito, contenido violento, networking social, de potencial alto consumo de ancho de banda, de interés general, no categorizado entre otros.

1.1.3.4. Gateway antivirus

Los virus son programas de computadora que se replican al ser copiados o al copiarse ellos mismos a otro programa, un sector de arranque del sistema o a un documento. Estos programas causan daño al alterar archivos o datos. Los costos que representan para una empresa el ataque de un virus son enormes, ya que

[21] Uniform Resource Locators

generalmente se habla de un impacto de varias horas en la operatividad de red así como dedicar recursos y tiempo para realizar una limpieza de los sistemas después de sufrir el ataque.

Los virus pueden acceder a la red empresarial desde fuera de la misma como desde adentro. Las herramientas que se utilizan en la detección de los virus dependen de a qué sector de posible ingreso se quiera resguardar. Si lo que se quiere es evitar que los virus ingresen a través de la red interna, es necesario utilizar un software antivirus instalado en todas las máquinas que se conectan a la LAN empresarial. Si es que se necesita evitar el ingreso de virus a través de las redes inseguras como el Internet se necesita un equipo que se encuentre en el perímetro empresarial. Este equipo es conocido como gateway antivirus. Si bien las aplicaciones antivirus instaladas en las máquinas de los empleados de las empresas pueden ayudar a detener un virus que ya haya ingresado por la red insegura, lo que pretende el gateway antivirus es evitar que el virus llegue siquiera a ser visto por al antivirus de máquina.

1.1.3.5. Gateway anti-spam

Al spam se lo puede definir como como correo electrónico no deseado, también como correo electrónico comercial no solicitado o correo electrónico basura pero la definición que abarca todo lo que se puede evidenciar como spam en la actualidad es la de correo electrónico masivo no solicitado. El spam en la empresa hace que las bandejas de entrada de correos electrónicos se llenen con correo no solicitado y

que generalmente contiene malware[22] o spyware como archivos adjuntos o links a páginas web potencialmente peligrosas. Los gateways anti-spam son la primera defensa contra la lucha de este tipo de correos electrónicos.

Los métodos utilizados por los gateways anti-spam son listas negras, listas blancas, filtrado heurístico, desafío/respuesta, entre otras. Las listas negras son un listado de direcciones IP con su dominio que son catalogados como generadores de spam. Las listas blancas por el contrario son listas incluyentes que recopilan un conjunto de direcciones IP con sus dominios y los catalogan como no generadores de spam. El filtrado heurístico utiliza un conjunto de reglas que pretenden identificar características específicas de spam así como características de correo electrónico legítimo. Con el método de desafío/respuesta, cada vez que alguien fuera de la empresa envía por primera vez un correo electrónico a alguien dentro de la empresa, la persona fuera de la empresa recibe un correo en el cual se pide que confirme su identidad; una vez confirmada la identidad, el correo electrónico inicial es liberado a su destino original.

Los métodos mencionados pueden ser implementados en una variedad de formas como por ejemplo en software, en un equipo, en el lado del proveedor de servicios y en el lado del cliente. El Gateway anti-spam es considerado un equipo dedicado al control de spam.

[22] Malicious Software

1.1.3.6. Concentrador de VPNs

Como una forma de garantizar la confidencialidad de los datos al igual que su integridad y disponibilidad se utilizan las VPNs las cuales funcionan sobre redes inseguras como es el caso del Internet. Los clientes y los proveedores de las empresas generalmente usan VPNs como una forma costo-efectiva de intercambiar servicios sin la necesidad de contratar enlaces dedicados para la interconexión.

Un concentrador de VPN es un equipo que transforma texto plano a texto cifrado, lo envía sobre un canal de comunicaciones inseguro a través de un túnel y al otro lado es recibido por un dispositivo que transforma el texto cifrado nuevamente a texto plano.

Los algoritmos de encriptación que puede usar un dispositivo como este pueden ser simétricos, los cuales usan una misma llave para encriptar y desencriptar los datos, o asimétricos, los cuales usan una llave para encriptar y otra para desencriptar. Los algoritmos simétricos generalmente son usados para la encriptación de los datos mientras que los asimétricos son usados para el intercambio de las llaves. Algunos ejemplos de algoritmos simétricos que existen son: DES[23], 3DES[24], IDEA[25], RC4[26] y AES[27]. Los algoritmos asimétricos más usados son Diffie-Hellman y RSA.

Además de las llaves, los equipos VPN pueden también utilizar certificados digitales, los cuales son piezas de información emitidas por una autoridad

[23] Data Encryption Standard
[24] Triple Data Encryption Standard
[25] International Data Encryption Algorithm
[26] Rivest Cipher 4
[27] Advanced Encryption Standard

certificadora pública reconocida, lo que hace que cualquier sistema confié en este certificado.

Otro concepto muy importante dentro del mundo de las VPNs es el término hashing, el cual es usado para proveer integridad a los datos. La manera como funciona es la siguiente: datos con un tamaño arbitrario son colocados como la entrada de una función de hash y luego procesados a través de esta función. Como salida se obtiene un hash de longitud fija. Este hash de longitud fija se lo conoce como digest.

Los equipos que se conecten a un concentrador VPN tienen dos opciones, enviar todo su tráfico por el túnel seguro o solamente parte de todo su tráfico. La funcionalidad que permite manejar esta diferenciación del lugar por el cual se debe enviar el tráfico se la conoce como *split tunneling*.

La mayoría de las VPNs son de uno de dos tipos. El primer tipo es la llamada VPN de acceso remoto. Es usada por los usuarios que requieren conectar sus dispositivos a la red corporativa a través de una red insegura como el Internet. Para esto el equipo del usuario debe tener una aplicación instalada, conocida como el cliente VPN, la cual se conectará a un servidor que se encuentra en el lado de la empresa conocido como el concentrador VPN. Mediante configuraciones se puede hacer que todo el tráfico generado por el usuario pase por el túnel VPN o solamente aquel tráfico que tiene como destino alguna red existente en el lado de la empresa.

Generalmente se configura el cliente VPN para que todo el tráfico generado por el equipo del usuario pase a través del túnel hacia el concentrador VPN, evitando de

esta forma que el usuario pueda llegar a infectar la red corporativa si es que tuviera la posibilidad de navegar a Internet por su conexión insegura mientras está conectado de manera segura a la red de la empresa. El segundo tipo se lo conoce como VPN de sitio a sitio. El principio de operación es básicamente el mismo que el descrito para el primer tipo de VPN. La diferencia es que la VPN se establece ya no desde un cliente a un servidor, sino entre un servidor y otro servidor. Se lo utiliza cuando no es solo un host el que necesita acceder a una red remota de forma segura sino toda una red o varias redes.

Los protocolos más usados para la creación de VPNs son: PPTP, L2TP, IPSEC y SSL. En la actualidad el más usado a nivel empresarial es IPSEC, el cual en realidad es un conjunto de protocolos conformado de dos elementos: el AH[28] y el ESP[29]. El AH fue diseñado para integridad, autenticación y no repudiación mientras que el ESP maneja la confidencialidad.

1.2. Servicios Administrados

En este documento se pretende definir los servicios administrados como modelo de negocio, haciendo una comparación con otros modelos similares pero que a su vez pueden resultar complementarios.

[28] Authentication Header
[29] Encapsulating Security Payload

1.2.1. *Definición*

De manera general, los servicios administrados son un esquema de negocio que tiene como objetivo centralizar o consolidar un conjunto de funciones o servicios de una empresa de tal manera que una empresa externa pueda tomar el control total o parcial de la operación de los mismos.

Los servicios administrados son una "forma de *outsourcing*[30] sin la transferencia de bienes y/o personal" [3], entendiéndose como outsourcing un acuerdo contractual entre dos empresas en la cual se involucra el intercambio de servicios (que pueden incluir personal y/o activos) por dinero. Partiendo de este punto se puede llegar a la siguiente definición:

Los servicios administrados son un acuerdo contractual entre dos empresas, una de ellas empresa proveedora de servicios administrados, en la cual se involucra el intercambio de servicios por dinero pero sin la transferencia de activos y/o personal. Estos servicios son brindados por personal en cierta manera especializado en el tema, y todo el conjunto es llevado a través de una metodología de gerencia de proyectos y de gestión de servicios.

1.2.2. *Características*

Los servicios administrados pueden compartirse entre varias áreas de negocio como es el caso de los servicios de tecnologías de la información (TI), inventarios,

[30] Externalización

compras, mensajería, entre otras. Generalmente existe un contrato de por medio para este tipo de modelo y está orientado a la contratación de empresas especializadas en las áreas a operar. En general, las áreas o funciones a contratar no son parte del núcleo del negocio sino que son áreas de apoyo o áreas de soporte.

Los servicios administrados permiten a las empresas enfocar todos sus esfuerzos a la parte más importante del negocio, lo cual les lleva a tener un mejor control de los procesos de la empresa, así como también permite la reducción de costos. El adecuado manejo de los recursos de una empresa es un componente vital para el éxito, y lo que pretende los servicios administrados es optimizar dichos recursos utilizando únicamente el tiempo efectivo de los mismos, o compartiendo estos en varios clientes.

Por lo general, la empresa que recibe el servicio sigue siendo responsable de la funcionalidad, de los resultados y de su administración y no renuncia a la responsabilidad de la gestión global de la organización o sistema, es decir que a pesar de que determinada actividad ya no es manejada internamente, el control y supervisión de la misma sigue siendo parte fundamental del proceso. En este caso el cliente pasa de ser un ente ejecutor a un ente de control y seguimiento.

La visión que se debe tener para el éxito de la contratación de servicios administrados debe ser a futuro y a largo plazo, siendo un pilar importante entender las etapas que son parte de la ejecución de los servicios, de tal manera que se los pueda manejar utilizando las mejores prácticas que se encuentren vigentes. Los resultados a nivel de costos no se ven reflejados de manera inmediata ya que toda

contratación a largo plazo requiere inversiones iniciales que al corto plazo no se pueden justificar; sin embargo luego de que ha pasado un tiempo de operación los costos se van estabilizando y la operación de igual manera. Es necesario tener claro que existen etapas de transición en las cuales las empresas, tanto la proveedora del servicio como el cliente, deben estar preparadas para el cambio y deben ajustarse a las nuevas exigencias. Es importante además tener claro que para un nuevo esquema de servicios administrados se deben levantar procesos y procedimientos específicos para cada tarea; algunos procesos van a ser propios de cada empresa y otros se tendrán que realizar en conjunto.

1.2.3. *Servicios administrados de tecnologías de la información*

Las tareas específicas que realizan los departamentos de Tecnología de la Información calzan de manera perfecta en el modelo de negocio de servicios administrados, ya que son tareas especializadas, que sirven de apoyo a la empresa y que pueden ser brindadas de manera externa sin generar impacto a la organización.

Los servicios administrados de TI, como su nombre lo indica ofrecen un servicio de TI, el cual es el la “combinación de tecnologías de la información, personas y procesos” [Q]; estos componentes en general no son tangibles para el cliente, sin embargo debido a este punto se tiene que definir los factores a medir para que se generen políticas de cumplimiento de servicio.

Los servicios administrados de Tecnologías de la Información es una idea que se ha venido fortaleciendo con el paso del tiempo debido a la necesidad de las

empresas de optimizar recursos y mejorar sus procesos internos, generando áreas de control que estén más alineadas al negocio y no directamente la operación.

En el ambiente de TI, se suelen utilizar los términos outsourcing y servicios administrados de la misma manera a pesar de que no son lo mismo ya que los servicios administrados de TI son altamente especializados en funciones particulares y pretenden gestionar de mejor manera el equipamiento de TI que la empresa dispone; es decir que la empresa proveedora de servicios administrados no provee el equipamiento a administrar sino que solo brindará servicios de gestión o administración puntual de determinada plataforma o servicio; de igual manera, los servicios administrados en general no tienen personas en sitio que administran las plataformas o servicios, sino que generalmente la administración es remota, brindando mucho más valor a la empresa que contrata los servicios pues no necesita adecuar espacio físico para recibirlos.

Los servicios administrados de TI tienen una característica muy particular que los diferencian de los servicios de outsourcing, que es la capacidad de generar servicios a escala debido a que con la misma infraestructura, el mismo personal y los mismos recursos se pueden atender a varios clientes a la vez, obviamente va a depender de la distribución de los recursos y la clara delimitación de funciones internas dentro de la empresa que provee el servicio. Esto genera beneficio colectivo ya que el tiempo de productividad de los recursos aumenta, y la especialización de los mismos es mucho más completa debido a los diferentes escenarios y casos que pueden manejar.

Los servicios administrados de TI son una solución puntual que se brinda de tal manera que agrega valor a los componentes de TI de la empresa, sacando el mayor provecho y beneficio de los mismos; adicional a esto se consigue una optimización y/o reducción de los gastos operativos del departamento de TI (OPEX[31]) y una optimización de los gastos de capital (CAPEX[32]), así como también permite el acceso a competencias técnicas especializadas, que en cierta manera agrega mucho más valor a la empresa debido a que los tiempos de respuesta pueden disminuir y la administración de los servicios o plataformas es mucho más especializada. La especialización de los recursos puede además optimizar de manera adecuada los componentes de hardware y software involucrados, pudiendo en cierta manera mejorar tareas productivas dentro de la empresa beneficiada.

Los servicios administrados de TI son hechos a medida, siendo muy complicado definir una clasificación específica de los mismos ya que las realidades, necesidades y arquitecturas de TI de cada empresa pueden variar. Generalmente estos se dimensionan de acuerdo a necesidades particulares de una empresa; sin embargo si se pueden enmarcar de acuerdo a las tecnologías y áreas de acción de los servicios, por ejemplo se pueden tener servicios administrados de LAN, servicios administrados de WAN, servicios administrados de control de acceso, servicios administrados de hosting[33] y storage[34] o servicios administrados de comunicaciones unificadas. El presente documento se enfocará en los servicios administrados de seguridad perimetral de redes.

[31] Operating Expense
[32] Capital Expenditure
[33] Alojamiento
[34] Almacenamiento

Al ser un modelo hecho a medida no se puede hablar de las características particulares que tendrá dicho servicio o el alcance que podrá tener el mismo, sin embargo se pueden tener definiciones generales para poder realizar la entrega del servicio como son los acuerdos de niveles de servicio (SLAs[35]) y las líneas base de los servicios.

Los acuerdos de niveles de servicio de manera general es un contrato que formaliza la relación de negocio entre dos componentes que son el cliente y el proveedor de servicio. Los niveles de servicio se establecen dentro de los ambientes de TI para medir y administrar la calidad del servicio entregada. Los SLAs definen que niveles de servicio son considerados aceptables por los usuarios y son realizables por los proveedores de servicio. Los niveles de servicio además permiten definir cómo se van a medir los servicios para garantizar calidad y cumplimiento. Los SLAs que se definan entre las partes permiten evidenciar los costos que podrá tener determinado servicio, ya que dependiendo de la exigencia del acuerdo de nivel de servicio se podrá saber de manera estimada los recursos necesarios para poder brindar dicho servicio.

Las líneas base son valores muy claros de acuerdo al servicio que se esté brindando, por ejemplo puede ser número de atenciones por semana, o número de horas de trabajo por día, número de minutos al teléfono, número de visitas en sitio, etc. Estas líneas base de servicios son sumamente importantes ya que de cierta manera permiten dimensionar la cantidad de esfuerzo necesaria de ambas partes y permiten dimensionar los costos y el precio que pueden tener los servicios.

[35] Service Level Agreement

Para garantizar el éxito de la entrega del servicio se deben utilizar metodologías de gestión del servicio como ITSM[36], las cuales utilizan determinados marcos de trabajo o mejores prácticas, como es el caso de ITIL[37], para poder realizar una adecuada entrega del servicio.

1.2.3.1. Servicios administrados de seguridad perimetral de redes

En la actualidad todo lo que tiene que ver con seguridad de la información se ha convertido en prioridad para los departamentos de TI, siendo este un punto crítico y de vital importancia a tomar en cuenta el momento de invertir o de definir los presupuestos anuales. Los múltiples fabricantes y la falta de recursos especializados en todas las tecnologías generan un bajo desempeño en la administración de estos servicios, provocando riesgos de suma importancia a la empresa, riesgos que pueden ser desde la pérdida de servicios de productividad hasta la pérdida de información vital para el negocio. Los servicios administrados de seguridad perimetral de redes se enfocan en la administración de los equipos, servicios y tecnologías que se encuentran en el perímetro empresarial; la idea de este servicio es garantizar el buen manejo y control de los componentes de red que conforman el perímetro.

1.2.3.1.1.Determinación de alcances

Para poder trasladar la administración de la seguridad perimetral a determinada empresa proveedora de servicios es necesario definir claramente los alcances del

[36] IT Service Management
[37] IT Infrastructure Library

servicio. Las empresas deben tener políticas bien definidas en lo que se refiere a la seguridad. Este punto es muy importante ya que la empresa de servicios se convierte en un ente ejecutor de las políticas, que tiene determinada empresa.

El punto de partida para poder llegar a definir el servicio parte de las necesidades específicas del cliente. En el caso de que una empresa no disponga de dichas políticas, es necesario levantarlas de manera general, ya que estas formarán parte del marco de trabajo de la empresa de servicio.

El segundo punto a evaluar es la identificación de la infraestructura de red que dispone el cliente en la zona perimetral, a nivel de software y hardware, ya que puede presentarse el caso de que las políticas de seguridad de la empresa no estén cubiertas con la infraestructura de seguridad perimetral que dispone la empresa. En este punto se debe especificar de manera detallada el equipamiento con sus modelos específicos y sus versiones de sistemas operativos sobre los cuales se tendrá acción.

Con toda esta información es necesario definir los procesos de ejecución de los requerimientos, es decir cuál es el flujo de trabajo para ejecutar determinada tarea, no está por demás recalcar que los procesos deben estar alineados a las políticas de la empresa. Estos procesos son el marco de trabajo de las personas que ejecutan el servicio, siendo este el punto de partida inicial ante cualquier solicitud.

El siguiente punto que se debe evaluar son los horarios de dicha administración, es decir cuándo y en qué momento se ejecutarán las tareas; por ejemplo se puede definir que todos los requerimientos se ejecuten al final de la jornada laboral de

cada día de lunes a viernes, o que los requerimientos se ejecuten apenas sean solicitados. Aquí se involucran los horarios de atención, cantidad de personas y los tiempos de respuesta. Este punto también es importante ya que con este se puede dimensionar la cantidad de personas y recursos necesarios para ofrecer el servicio.

Luego de esto, se debe definir el número de requerimientos o solicitudes a ejecutar dentro de un periodo claramente determinado; por ejemplo puede ser número de reglas en el Firewall a crear en la semana, número de VPNs creadas dentro de un año, etc. Aquí se debe evidenciar claramente cómo se procederá si se excede el número de requerimientos contratados o definidos, se debe especificar rangos de tolerancia y los costos específicos por requerimientos adicionales.

1.2.3.1.2.Etapas del servicio

Cuando se contratan servicios administrados se evidencian varias etapas del servicio, la primera es la etapa inicial en la cual se define la estrategia de la transición, la segunda etapa es la etapa de transición en la cual se tiene un rol compartido con la empresa para poder tomar la operación de manera completa; la duración de esta etapa se la define en la etapa inicial, e inclusive debe estar plasmada en el contrato de servicios. La etapa de transición también sirve como piloto para evaluar si los parámetros del servicio como tal fueron bien dimensionados y si es necesario hacer ajustes, por ejemplo los niveles de servicio y las líneas base de servicio, o más aún el alcance de determinada tarea.

Posterior a la etapa de transición se encuentra la etapa de operación en la cual la empresa proveedora de servicio toma control absoluto de la operación definida en

el acuerdo contractual. En esta etapa no se deberían modificar los niveles de servicio y líneas base de los servicios ya que en la etapa de transición se debieron haber evaluado los mismos, sin embargo eso no limita a que se hagan modificaciones por cambios internos de la empresa o por comportamientos no evidenciados en la etapa de transición. Todo cambio debería ser documentado y debe estar atado a una modificación del acuerdo contractual.

Luego de un periodo de trabajo en operación normal se deben realizar evaluaciones constantes del servicio para validar las mejoras al mismo, tanto en SLAs, en líneas base y en procesos de ejecución. La idea de esta etapa es la mejora continua del servicio. En el caso de que se tengan modificaciones que no se encuentren alineadas a lo definido en el acuerdo contractual, es necesario hacer una revisión de contrato para ajustar dichos cambios.

En el caso de que se llegue a una terminación de servicios, ya sea unilateral o por una culminación de contrato, se debe especificar una nueva etapa de transición, que no es la misma que la inicial, ya que el objetivo de esta es devolver la operación al cliente o a otra empresa de servicios.
Por último se encuentra la etapa de fin del servicio en la cual se culmina cualquier relación de ejecución del servicio del acuerdo antes definido.

1.2.4. *Outsourcing*

En la actualidad el modelo de outsourcing está enfocado principalmente a servicios de primer nivel orientados al usuario, como son las mesas de ayuda (help desk), servicios de impresión, los centros de atención de llamadas (call center), etc. En

este modelo es necesaria la presencia del personal en sitio, lo que impide al proveedor de servicios hacer economía de escala con el negocio ya que no se pueden compartir recursos o personas en varios clientes al mismo tiempo. Generalmente en este modelo las personas en sitio no son personas con conocimientos especializados, pero si con habilidades particulares para resolución de problemas de TI. En este modelo es necesario el manejo del personal, la adecuada coordinación de tareas y el seguimiento de las mismas.

Al igual que los servicios administrados el modelo de outsourcing debería utilizar modelos de gestión de servicio como ITIL, de la misma manera se aplican SLAs y líneas base de servicio. Por otro lado, los servicios de outsourcing al ser servicios que se dan dentro de la empresa del cliente, deben preocuparse de otros aspectos como por ejemplo la cultura organizacional del cliente, ya que al formar parte de la interacción diaria del personal con la empresa se debe también formar parte de la cultura empresarial.

En este modelo a diferencia de los servicios administrados los componentes de hardware, por ejemplo computadores de escritorio, o impresoras, pueden ser provistos por la empresa proveedora de servicios, y la renovación, mantenimiento y gestión de garantías son responsabilidad de la empresa propietaria de los equipos. La ventaja de este aspecto es que la renovación tecnológica de infraestructura es mucho más ágil ya que se encuentra plasmada de manera específica y clara en los contratos de servicio.

1.2.5. *Cloud computing*[38]

En la actualidad ha venido tomando fuerza la idea de los servicios en la Nube o *Cloud*, siendo este un punto a analizar debido a que parte de los servicios administrados se pueden suplir con este modelo, o a su vez pueden ser complementarios.

Basados en la definición del Instituto Nacional de Estándares y Tecnología NIST[39] se puede definir a Cloud Computing de manera simple como un modelo que permite el acceso a un conjunto compartido de recursos computacionales configurables como son por ejemplo redes, servidores, aplicaciones, datos, almacenamiento y servicios; este modelo puede ser brindado de manera ágil con una mínima interacción del proveedor del servicio. Un ejemplo muy claro de cloud computing es Google Apps que brinda herramientas y aplicaciones enfocadas a la productividad de las empresas como por ejemplo correo electrónico o procesador de palabras. Para brindar estos servicios no es necesario que la empresa disponga de equipamiento para sostener la plataforma brindada por el proveedor, sino que solo basta con una conexión a Internet para el acceso.

El modelo de cloud computing brinda una gran flexibilidad ya que el cliente, de acuerdo a sus necesidades, puede transmitir a su proveedor de servicio la cantidad exacta de procesamiento, almacenamiento o aplicaciones que necesita.

[38] Computación en la Nube
[39] National Institute of Technology and Standards

De manera general el concepto de nube, en tecnología, se lo utiliza para describir algo que para el cliente es oculto, que desconoce a detalle y que no tienen ni interés ni necesidad de conocer las particularidades de su funcionamiento. En el concepto de cloud computing, el cliente no tiene la necesidad de conocer a detalle cómo se encuentra conformada la nube ni las particularidades técnicas que se presenten dentro de la nube; de lo que el cliente si se preocupa es de velar por los recursos contratados y los niveles de servicio de los mismos. Basados en esta premisa los proveedores de cloud computing apalancan su negocio generando recursos compartidos de un mismo equipo, tratando de aprovechar dichos equipos al máximo; para conseguir este propósito se valen de la virtualización. Esta compartición de recursos es transparente para el usuario final, el cliente no se llega a enterar de cuantos otros usuarios comparten el mismo componente de hardware.

1.2.5.1. Características

El modelo de Cloud Computing tiene varias características esenciales como son el auto servicio bajo demanda, donde el servicio es aprovisionado de manera unilateral por el usuario de los servicios en la nube para servidores, red y almacenamiento sin interactuar con los proveedores de servicio; escalabilidad y elasticidad, en donde se puede mover las capacidades de cómputo hacia arriba o hacia abajo de una manera flexible en la que se pueda mantener la eficiencia de los costos; pago por uso, característica a través de la cual solo se paga por el uso de los recurso de acuerdo a la demanda; acceso desde cualquier lugar y en cualquier momento, siendo un punto importante la independencia de la plataforma de uso; asignación dinámica de recursos por comportamiento, en este caso los servicios

son medidos por el proveedor para asignar o reasignar recursos físicos y virtuales de manera dinámica independiente de la ubicación de dichos recursos.

1.2.5.2. Modelos de entrega del servicio

Dentro del cloud computing se pueden tener varios modelos de entrega del servicio (cloud delivery model) dentro de los cuales se tiene el modelo de *nube pública* la cual cuenta con una infraestructura que en esencia está constituida para que el público en general pueda acceder a la misma; también se encuentra el modelo de *nube privada* la cual está diseñada solo para el acceso de una única organización o empresa; en este caso esta nube puede ser administrada por la misma empresa o administrada por un empresa externa. Se puede tener también una combinación de los dos modelos anteriores llamada *nube híbrida*, en la cual la infraestructura de las nubes privadas y públicas operan entre sí. Como último modelo se tiene la *nube comunitaria* en la cual la infraestructura de la nube es compartida por varias organizaciones soportando a una comunidad específica.

1.2.5.3. Modelos de servicio

Cuando se habla de cloud computing se tiene que distinguir claramente los modelos de servicio que se ofrecen en la nube. De acuerdo al NIST[40] se tienen tres modelos de servicio: *Software as a Service, SaaS*, donde el cliente accede a las aplicaciones del proveedor que se encuentran ejecutando en la infraestructura del proveedor; *Platform as a Service, PaaS*, donde el cliente ejecuta sus aplicaciones en la

[40] National Institute of Standards and Technology

infraestructura del proveedor, usando los sistemas operativos del mismo proveedor; *Infrastructure as a Service, IaaS*, en el cual el cliente usa, administra y controla sus sistemas operativos y aplicaciones ejecutándose sobre la infraestructura del proveedor; aquí también se puede incluir la tecnología de virtualización utilizada para administrar los recursos de la infraestructura.

En la Figura 1.5 se puede observar los elementos posibles de modelos de entrega de servicio y los modelos de servicio:

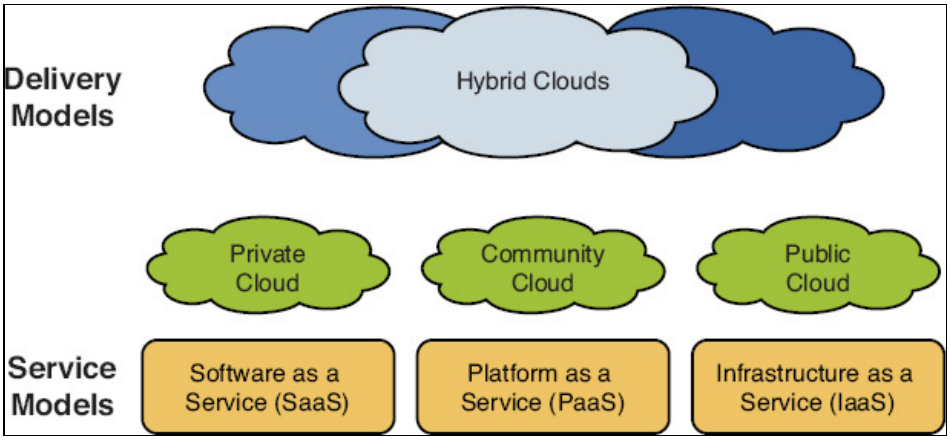

Figura 1.5. Modelos de Cloud Computing [N]

1.2.5.4. Ventajas

El modelo de cloud computing está enfocado al alojamiento de la información y aplicaciones en un espacio remoto (nube) que tiene todas las prestaciones de seguridad, confiabilidad, disponibilidad y escalabilidad, lo que genera que el cliente prescinda de la adquisición de infraestructura dedicada para sus aplicaciones y sus datos. Este modelo permite que las empresas disminuyan sus inversiones en equipamiento costoso y que a la larga con el avance de la tecnología llega a ser

obsoleto en el corto tiempo. El proveedor de servicios en la nube corre con toda la actualización de equipamiento, y con la renovación tecnológica de ser el caso, siendo transparente para el cliente ya que al contratar este tipo de servicios se establecen valores mínimos de procesamiento, memoria, disponibilidad, almacenamiento, y anchos de banda de acceso. La ventaja que tiene el proveedor de servicios es que la inversión tecnológica que realice puede servir a varios clientes a la vez ya que este modelo permite la compartición de recursos a través de esquemas de virtualización.

1.2.5.5. Desventajas

Uno de los puntos más controversiales del manejo de servicios en la nube es la seguridad, ya que en cierta manera los datos, y la información se encuentran en equipamiento que no es propiedad de la empresa, sino que es propiedad de un proveedor. De igual manera, al ser una nube no se sabe cómo se maneja dicha información, ya que como se mencionó anteriormente los componentes de hardware pueden ser compartidos por varios usuarios o clientes.

Un reto que tienen los proveedores de cloud computing es el manejo adecuado de la seguridad de la información, y las garantías que deben dar a sus clientes de que dicha información se encuentra segura.

Otra desventaja que tienen los servicios en la nube son las velocidades de acceso, ya que para poder acceder a los diferentes servicios localizados en la nube ya sea a través del Internet o de enlaces dedicados se necesitan anchos de banda adecuados. Estos anchos de banda tienen que ser adecuadamente dimensionados

y más allá de eso se deben hacer los análisis de costo beneficio de la contratación de los mismos.

1.2.6. *Interrelación entre servicios administrados, outsourcing y cloud computing*

Se puede llegar a pensar que Cloud Computing puede reemplazar a los Servicios Administrados y al Outsourcing, sin embargo es importante definir que cada uno tiene su rol en el ambiente de TI.

Los servicios de Outsourcing están enfocados de mayor manera hacia el usuario final como son el caso de las mesas de ayuda o los servicios de impresión y generan una alta demanda del personal en sitio para resolución de problemas. Este no puede ser reemplazado por el modelo de Servicios Administrados ya que una de las premisas esenciales de este modelo es que los servicios administrados no dispongan personal en sitio. Los servicios de outsourcing son esenciales para tareas del día a día y son un modelo de negocio que hasta el momento sigue dando resultados positivos para las empresas, ya que han dejado de enfocar sus esfuerzos en resolver problemas con usuarios y lo han trasladado a empresas de servicios dedicadas a este propósito, permitiendo que las empresas dediquen sus esfuerzos a tareas de la cadena de valor.

Los servicios de Cloud Computing están concentrados en brindar servicios de infraestructura, plataforma y software en la nube para que los usuarios puedan acceder a determinada información o aplicaciones específicas. Los servicios de Cloud computing no intervienen en la solución de problemas de acceso de usuario

final, ya que la información se encuentra en la nube; es aquí donde intervienen los servicios de Outsourcing, ya que ante cualquier problema de acceso local, se puede brindar soporte en sitio para resolución de problemas locales. Los proveedores de servicio de Cloud Computing brindarán soluciones de problemas en la nube.

Los Servicios Administrados se encuentran enfocados en determinadas tareas especializadas, como son la gestión remota de enlaces, de seguridad, de infraestructura LAN, de comunicaciones unificadas, etc., en las cuales no es necesaria la presencia en sitio para solucionar un requerimiento, y no tienen, en la mayoría de los casos, impacto directo con el usuario final. Los servicios administrados no se relacionan directamente con el usuario final sino que interactúan con la persona responsable de TI de la empresa.

Con el concepto de Cloud Computing se pensaría que no se tiene nada que administrar y que el modelo de servicios administrados pierde valor. Sin embargo, los Servicios Administrados han tomado mucha más fuerza ya que hay elementos de la infraestructura que no se pueden trasladar a la nube y que son importantes de tomar en cuenta, como por ejemplo la administración de la infraestructura LAN, o por ejemplo la telefonía, o los enlaces de datos que son esenciales para el acceso a la nube.

Se puede decir que los Servicios Administrados son complementarios a los servicios de Outsourcing y de Cloud Computing. Referente a los de Outsourcing ya que son mucho más especializados que estos y no tienen interacción directa con el usuario final; por otro lado con relación a los servicios de Cloud Computing ya que

trabajan directamente con la infraestructura sobra la cual el Cloud Computing no actúa.

Los servicios administrados de seguridad perimetral calzan de manera perfecta en la tendencia del mercado, ya que lo que pretenden es asegurar el perímetro empresarial para el acceso a la nube (en el caso de Cloud Computing) o viceversa, complementan ciertas falencias de seguridad que pueden tener las empresas proveedoras de servicios de Cloud Computing. La tendencia actual es contratar empresas dedicadas a determinadas tareas especializadas, para no dedicar esfuerzos en tareas que no le brindan valor a su centro de producción o de generación de ingresos.

1.3. Clasificación de las empresas en el Ecuador

Instituciones como la Superintendencia de Compañías utilizan la CIIU[41] como la referencia para clasificar las actividades económicas productivas dentro del Ecuador. La CIIU presenta un conjunto de categorías de empresas, las cuales están relacionadas con la actividad económica que realizan, entendiéndose como actividad a un proceso formado por una combinación de acciones cuyo resultado es un conjunto de productos o servicios determinados.

Para la CIIU una empresa es una entidad institucional en su calidad de productora de bienes y servicios. Para su clasificación, la CIIU en su revisión número 4 utiliza

[41] Clasificación Industrial Internacional Uniforme de todas las actividades económicas

una lista de secciones, cada una de las cuales posee divisiones. En la Tabla 1.1 se muestran las secciones utilizadas por la CIIU con sus respectivas divisiones.

La sección y la división a la que pertenecen las empresas relacionadas con la presente investigación son la G-47, la cual corresponde a comercio al por menor, excepto el comercio de vehículos automotores y motocicletas.

La sección G comprende todo lo referente a la venta al por mayor y al por menor de todo tipo de productos, con sus servicios accesorios asociados. La sección 47 comprende "*la reventa de productos nuevos y usados, principalmente al público en general, para el consumo o uso personal o doméstico, realizada por tiendas, grandes almacenes, puestos de venta, empresas de venta por correo, buhoneros y vendedores ambulantes, cooperativas de consumidores, casas de subasta, etcétera*" [W] .

La clasificación en grupos que se encuentra en la división 47 está dada en primer lugar por el tipo de lugar de venta: comercio al por menor en comercios (va desde el grupo 471 al grupo 477) y comercio al por menor no realizado en comercios (va desde el grupo 478 al grupo 479). Dentro del grupo de comercio al por menor realizada en comercios se encuentra otra división: venta al por menor en comercios especializados (grupo 472 a 477) y venta al por menor en comercios no especializados (grupo 471).

Sección	Divisiones	Descripción
A	01-03	Producción agropecuaria, forestación y pesca
B	05-09	Explotación de minas y canteras
C	10-33	Industrias Manufactureras
D	35	Suministro de electricidad, gas, vapor y aire acondicionado
E	36-39	Suministro de agua; alcantarillado, gestión de desechos y actividades de saneamiento
F	41-43	Construcción
G	45-47	Comercio al por mayor y al por menor; reparación de los vehículos de motor y de las motocicletas
H	49-53	Transporte y almacenamiento
I	55-56	Alojamiento y servicios de comida
J	58-63	Información y comunicación
K	64-66	Actividades financieras y de seguros.
L	68	Actividades inmobiliarias
M	69-75	Actividades profesionales, científicas y técnicas
N	77-82	Actividades administrativas y servicios de apoyo
O	84	Administración pública y defensa; planes de seguridad social de afiliación obligatoria
P	85	Enseñanza
Q	86-88	Servicios sociales y relacionados con la Salud humana.
R	90-93	Artes, entretenimiento y recreación
S	94-96	Otras actividades de servicio

Sección	Divisiones	Descripción
T	97-98	Actividades de los hogares en calidad de empleadores, actividades indiferenciadas de producción de bienes y servicios de los hogares para uso propio.
U	99	Actividades de organizaciones y órganos extraterritoriales.
V		Anexo al manual de Clasificación Industrial Internacional Uniforme, revisión 4

Tabla 1.1. Clasificación de las empresas según la CIIU [A]

CAPÍTULO 2. ANÁLISIS TECNOLÓGICO, OPERATIVO Y LEGAL

En este capítulo se realizará el análisis de todos los componentes que forman parte de un servicio, comenzando por el componente tecnológico, en donde se presenta lo que se requiere desde el punto de vista tecnológico para ofrecer el servicio administrado de seguridad perimetral de redes a las empresas de comercio al por menor. A continuación se analizan los componentes necesarios para la operación del servicio. Finalmente, en el componente legal se presentará una descripción del marco legal que rige a la empresa de servicios administrados dentro del país y los requisitos para constituirla.

2.1. Análisis tecnológico

Para realizar el análisis de la tecnología que se necesita para poder dar el servicio administrado de seguridad perimetral de redes se definirán los lugares involucrados en el servicio y sobre cada lugar sus requerimientos tecnológicos. Adicionalmente, se establecerá la forma de comunicación entre estos lugares.

Los lugares o sitios involucrados en el servicio administrado de seguridad perimetral de redes son: instalaciones del cliente y el centro de operaciones.

2.1.1. *Instalaciones del cliente*

Las instalaciones del cliente son el lugar físico donde se encuentran instalados los equipos de seguridad perimetral de redes que van a ser administrados desde el centro de operaciones. Los lugares que se pueden considerar como instalaciones del cliente son sus oficinas matrices, las sucursales, agencias o dependencias e inclusive los espacios rentados por el cliente a proveedores que administran centros de cómputo especializados.

Para poder dar el servicio de administración de la seguridad perimetral de redes, los equipos que conforman esta seguridad y que fueron definidos en la sección *1.1.3 Seguridad perimetral de redes* deberán tener la funcionalidad de ser administrados a través de una interfaz de usuarios gráfica (GUI[42]), una interfaz de línea de comandos (CLI[43]) o ambos tipos de interfaces. A diferencia de otros equipos de comunicaciones, como por ejemplo los switches, se podría decir que todos los equipos que forman parte de la seguridad perimetral de redes poseen al menos uno de los dos tipos de interfaces de administración mencionados.

Además, el direccionamiento IP de la interfaz de administración que permite el acceso al GUI o al CLI deberá estar correctamente configurado. Es decir, las interfaces de administración deberán tener su dirección IP, máscara y *gateway* correctamente configurados. El cliente deberá prestar especial atención a la adecuada configuración del gateway, ya que este servirá para que el equipo pueda comunicarse con otros dispositivos que se encuentran en una red diferente. Esto

[42] Graphical User Interface
[43] Command Line Interface

cobra una mayor importancia en los servicios administrados ya que los equipos a ser administrados y los dispositivos que harán esta función van a encontrarse en redes diferentes. Dependiendo del equipo, la dirección IP de la interfaz de administración puede estar configurada sobre un puerto dedicado exclusivamente a la administración o podría ser la dirección IP de un puerto del equipo utilizado para el procesamiento de datos.

Finalmente, es necesario que la interfaz de administración de los equipos se encuentre correctamente conectada a la red LAN del cliente. Haciendo referencia a lo explicado en el párrafo anterior, si la dirección IP de administración del equipo se encuentra configurada sobre el puerto dedicado a esta función, se hablaría de una administración *Out-of-Band*[44]. En contraste, si es que la dirección IP se encuentra configurada sobre un puerto que se utiliza para procesar datos, la administración sería *In-Band*[45]. Los dos tipos de administración tienen sus ventajas y desventajas. Entre las ventajas del esquema In-Band se pueden mencionar una mayor simplicidad para su implementación, mientras que una desventaja es la susceptibilidad a una pérdida de la administración remota cuando exista congestión en la red de datos debido a que el tráfico de administración y datos comparten el mismo medio. Por el contrario, la implementación del esquema Out-of-Band implica una mayor complejidad pero su disponibilidad es más alta ya que el tráfico de administración se encuentra separado del tráfico de datos.

[44] Fuera de banda
[45] En banda

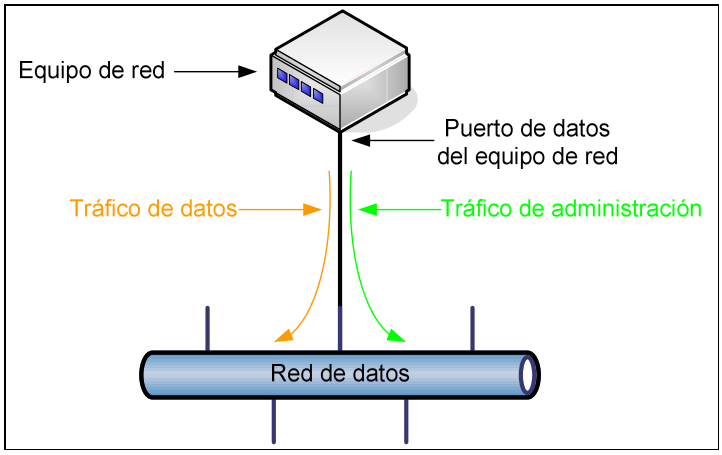

Figura 2.1. Administración In-Band [A]

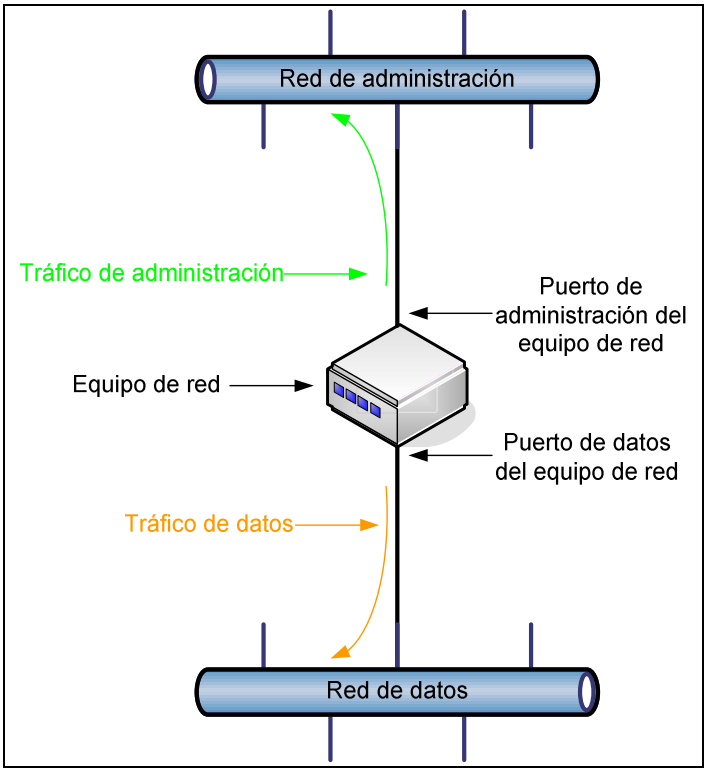

Figura 2.2. Administración Out-of-Band [A]

Una vez que se cumplan los requerimientos básicos para poder administrar los equipos de seguridad perimetral de redes, el cliente deberá preocuparse de tener

listos y configurados los accesos, entendiéndose como accesos a lo relacionado con la aplicación de los conceptos del marco de trabajo AAA[46] a los equipos. Es decir, los equipos deberán tener creados usuarios de administración con sus respectivos niveles de acceso para que puedan ser administrados desde el centro de operaciones de acuerdo al alcance del servicio definido en el contrato entre ambas partes y, de ser posible, el cliente también deberá configurar el equipo para que registre las actividades de los usuarios que accedan al mismo.

Lo expuesto en esta sección hasta este punto son los requerimientos tecnológicos indispensables en las instalaciones del cliente para poder dar el servicio administrado de seguridad perimetral de redes. Sin embargo, existen consideraciones adicionales que el cliente podría tomar en cuenta y que serían beneficiosas para el servicio. Entre estas consideraciones se encuentran tener un cableado estructurado certificado, ubicar los equipos en sitios cuyos accesos sean controlados y monitoreados, conectar los equipos a tomas de corriente respaldadas con UPSs[47] y poseer sistemas de enfriamiento para los equipos.

2.1.2. *Centro de operaciones*

El centro de operaciones será el lugar desde el cual se realizará el control de los equipos de seguridad perimetral de redes de acuerdo a los requerimientos del cliente. Entre las principales funciones del personal que trabaja en el centro de operaciones se encuentran: monitoreo de la red, atención de requerimientos y

[46] Authentication, Authorization y Accounting.
[47] Uninterruptible Power Supply

generación de reportes [9]. El centro de operaciones deberá poseer toda la tecnología para poder realizar las funciones mencionadas.

El monitoreo de la red se refiere al monitoreo de la conectividad entre el centro de operaciones y las instalaciones del cliente donde se encuentran los equipos a ser administrados. Esto con el fin de saber con certeza que la conectividad desde el centro de operaciones a las instalaciones del cliente va a estar disponible para poder atender algún requerimiento de configuración solicitado por el cliente. Para esto se necesita tener una aplicación instalada sobre una máquina con características de alta disponibilidad, como un servidor, que monitoree la conectividad entre los sitios mencionados utilizando protocolos de monitoreo como ICMP[48] o SNMP[49]. Lo mencionado corresponde a una de las tareas de un NMS[50].

La función de atención de requerimientos realizada por el centro de operaciones consiste en recibir el requerimiento de configuración de los equipos de seguridad perimetral de redes del cliente e implementar este requerimiento. El detalle de este proceso se lo presentará en la sección correspondiente al análisis operativo. Para realizar esta función principalmente se necesita tener conectividad desde el centro de operaciones hacia las instalaciones del cliente. El tema de la conectividad se lo tratará en la siguiente sección. Adicionalmente se necesita tener una herramienta para hacer el seguimiento del estado de atención de los requerimientos. Este tipo de herramienta tendrá la información del historial del requerimiento, desde que fue

[48] Internet Control Message Protocol
[49] Simple Network Management Protocol
[50] Network Management System

enviado por parte del cliente hasta que uno de los operadores lo atendió y fue cerrado con el consentimiento del cliente.

Finalmente, para la generación de reportes se necesitan aplicaciones de ofimática en donde se procesará la información almacenada en la herramienta de manejo de incidentes, para el seguimiento de los requerimientos y su presentación al cliente.

Como tecnologías adicionales que deben estar presentes y que van a ser usadas por todo el personal, no solo por el dedicado a brindar el servicio de atención de requerimientos, se encuentran el servicio telefónico, correo electrónico, computadoras personales con sus debidas aplicaciones, Internet y un repositorio de archivos, que podrá ser usado por ejemplo para almacenar las plantillas de configuración que se pueden aplicar a los equipos del cliente.

Con respecto a la tecnología que será utilizada para dar el servicio al cliente, en la medida de lo posible esta deberá estar separada o aislada de la tecnología utilizada por el resto de la empresa; por ejemplo, la red en la que se encuentran los operadores que atenderán los requerimientos de cambios de configuración de los equipos de seguridad perimetral de redes de los clientes debe estar concentrada en una VLAN[51] con su correspondiente segmento de red, la cual será diferente al resto de VLANs donde se están los equipos del personal de la empresa. Esto con el fin de garantizar la integridad, confidencialidad y disponibilidad de la información del cliente.

[51] Virtual Local Area Network

2.1.3. *Canal de comunicación entre los sitios*

El canal de comunicación entre los sitios se vuelve crítico debido a que es el medio utilizado para poder atender los requerimientos de configuraciones de los clientes. Si es que no existe un canal de comunicación entre las instalaciones del cliente y el centro de operaciones, el servicio no podrá ejecutarse.

Este medio de comunicación está formado por equipos que se encuentran tanto en las instalaciones del cliente como en el centro de operaciones. Los equipos que se encuentran en el centro de operaciones deberán ser alojados en un espacio con sistema de enfriamiento, correctas instalaciones de cableado estructurado y de tendido eléctrico y un acceso controlado como en un centro de cómputo. En el lado del cliente esto no es indispensable para dar el servicio pero si es recomendable.

Los principales medios que existen para establecer un canal de comunicaciones entre los sitios son: enlaces de datos dedicados y el Internet.

Los enlaces de datos dedicados utilizan tecnologías como Frame-relay, ATM, MPLS o el mismo estándar utilizado en las redes LAN llamado Ethernet. Este último se utiliza en el caso de que exista una conexión directa entre los sitios a través de una fibra óptica, lo cual se lo conoce como una fibra obscura. También es posible enlazar dos sitios utilizando enlaces de radio. Las tecnologías Frame-relay, ATM y MPLS comparten muchas características, diferenciándose principalmente en que MPLS es independiente de los protocolos utilizados en capa 2, de ahí que es tan usado por los proveedores de enlaces en la actualidad. Estas tecnologías de caminos conmutados tienen la ventaja de que pueden ser utilizadas por los

proveedores de enlaces para dar servicio a más de un cliente y de esta forma optimizar el uso de la infraestructura física que implementaron, lo que se traduce en un menor costo para el cliente final. En el caso de utilizar una fibra obscura para enlazar dos sitios, los costos son mayores porque generalmente esta fibra es solamente utilizada para dar el servicio a un cliente. Como una última opción se tienen los enlaces de radio, los cuales pueden llegar a tener una relación de costo beneficio muy alta pero que tienen como desventaja las bajas tasas de transferencia que pueden manejar, la latencia y la inestabilidad debido a factores externos como las condiciones climáticas.

En este tipo de enlaces se tiene un equipo en cada uno de los sitios interconectados. A este equipo se lo conoce como CPE[52] y puede ser provisto por la empresa que ofrece el servicio del enlace de comunicaciones o por el cliente. Generalmente, este equipo es dado por el proveedor del enlace y consiste en un router que tiene dos interfaces, una que se conecta a la red del cliente y la otra a la red del proveedor.

El otro tipo de medio de comunicación además de los enlaces dedicados es el Internet. Al ser un medio de acceso público, se necesita utilizar una tecnología que permita brindar las mismas funcionalidades de los enlaces privados; para esto se utilizan VPNs. Los equipos que se necesitan para levantar una VPN dependen del tipo de VPN que se pueda establecer contra la red del cliente desde el centro de operaciones. Las opciones que se tienen son: VPN de acceso remoto o VPN sitio a sitio. Para el primer tipo de VPN se necesita instalar un cliente VPN en una

[52] Customer Premises Equipment

máquina en el centro de operaciones para que esta pueda acceder a las redes del lado del cliente. Para la VPN sitio a sitio se necesita tener un concentrador VPN tanto en el lado del cliente como en el centro de operaciones. Generalmente el concentrador VPN viendo embebido como una funcionalidad manejada por los firewalls.

De lo expuesto anteriormente, se cuenta con todos los elementos tecnológicos necesarios para brindar el servicio administrado de seguridad perimetral de redes.

2.2. Análisis operativo

Es importante definir de manera adecuada los componentes necesarios para poder brindar el servicio; esto quiere decir que hay que detallar cada uno de los componentes que intervienen en la operación del mismo. Luego de detallar dichos componentes se podrá evaluar si es posible ejecutar el servicio mencionado.

A nivel de la operación del servicio se puede definir de manera clara lo siguiente:

- El organigrama, que enmarca a las personas, quienes deben tener un rol específico y funciones claras.
- Los procesos, que permiten realizar la ejecución del servicio de manera ordenada y transparente.
- La línea base de servicio y los SLAs, los cuales permiten medir el servicio en base a indicadores.

El objetivo del análisis operativo es definir si se cuenta con los componentes necesarios en lo que se refiere a la operación diaria para ejecutar los servicios planteados en la presente investigación.

2.2.1. *Organigrama*

Es necesario definir la estructura de la organización que permitirá brindar el servicio, para esto se ha generado un organigrama de funciones en el cual se evidencian los roles dentro de la organización.

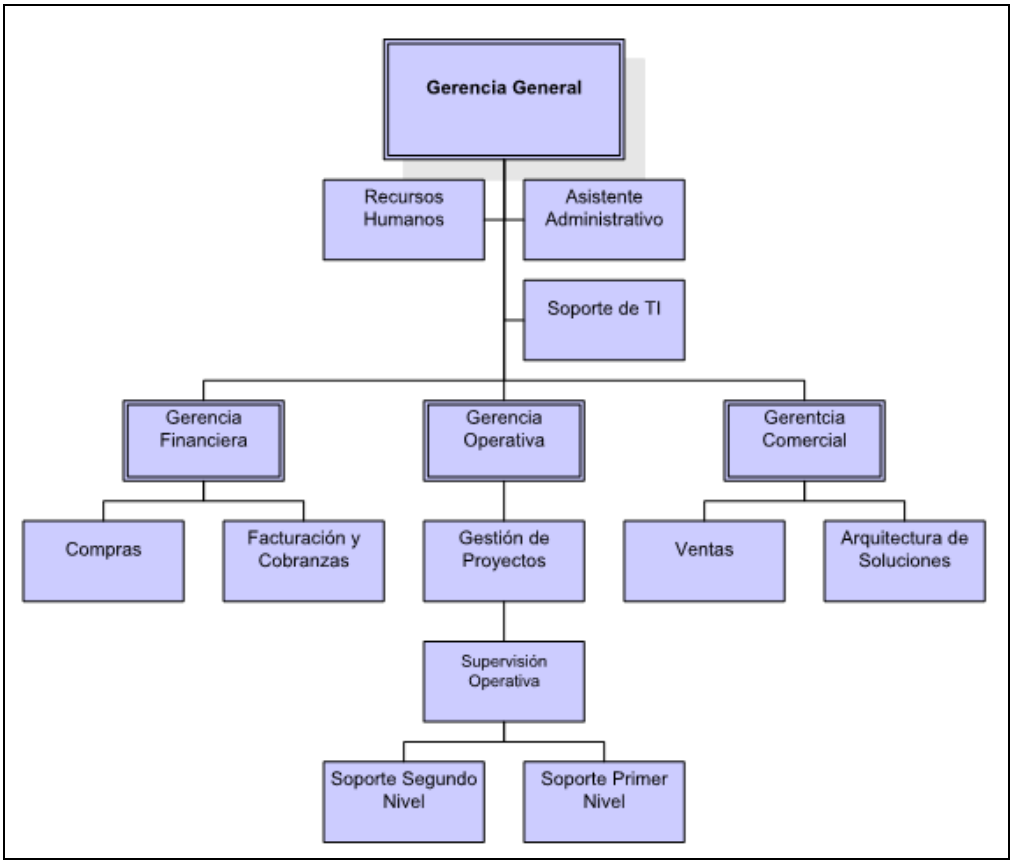

Figura 2.3. Organigrama [A]

A continuación se detalla cada uno de los roles descritos en el organigrama. El objetivo del detalle de roles es validar si los recursos que se necesitan se podrían conseguir dentro del mercado Ecuatoriano.

Rol	Descripción
GERENCIA GENERAL	La Gerencia General tiene como función planear y desarrollar los objetivos del negocio, socializar los mismos a las diferentes áreas y evaluar de manera periódica el cumplimiento de los objetivos. Los objetivos que se plantean deben estar alineados con la planificación estratégica de la empresa. En este rol se necesita una persona con habilidades administrativas con un alto entendimiento de tecnologías de la información.
Recursos Humanos	Se encarga de la gestión del talento humano dentro de la organización. En este rol debe estar una persona con perfil de recursos humanos, con cualidades de gestión de talento humano.
Soporte de TI	Se encarga de dar soporte de tecnologías de la información a los usuarios internos para que puedan ejecutar sus tareas adecuadamente. En este rol se necesita una persona con conocimiento de tecnología, además de tener habilidades comunicativas.
Asistente administrativo	Este rol brinda apoyo administrativo a la organización en todo lo que tiene que ver con la operación de la empresa. Se apoya en los procesos de la empresa para ejecutar tareas claras. Brinda un descargo de tareas administrativas a los departamentos como por ejemplo la gestión de correspondencia, el manejo de órdenes de

Rol	Descripción
	compra, actualización de documentación, manejo de archivos y comunicaciones. Este rol está diseñado para personas con un perfil administrativo, comercial, con habilidades comunicativas.
GERENCIA FINANCIERA	El objetivo principal de la Gerencia Financiera es maximizar el valor de la empresa, por lo que en este rol se encuentra la planeación y administración del flujo de caja, administración de activos y pasivos, compras e inversiones. La elaboración de los estados financieros de la empresa es responsabilidad de este rol, así como también el análisis de los mismos. En este rol también se definen presupuestos de trabajo para cada área de acuerdo a los objetivos de la empresa y a las prioridades de la misma. Para este rol se necesita una persona con alto entendimiento de finanzas y administración de empresas.
Compras	El rol de compras en una empresa es maximizar los beneficios en la compra de los insumos necesarios para la operación diaria y para poder brindar los servicios, ya sea a través de mayores descuentos o mejores beneficios. En este rol se necesita una persona con entendimiento técnico que tenga habilidades de negociación.
Facturación y Cobranzas	El rol de Facturación y Cobranzas tiene como objetivo generar la factura con los valores correctos de los productos o servicios que una empresa comercializa. Los valores indicados en la factura deben ser cobrados o recuperados por la empresa de acuerdo a los acuerdos de cobro que se establezcan. En este rol se necesita una persona con perfil administrativo y financiero.
GERENCIA	Este rol tiene como fin asegurar que la operación de los diferentes

Rol	Descripción
OPERATIVA	proyectos se realice adecuadamente y se garantice la satisfacción de los clientes con miras a la generación de nuevos negocios. En este rol se necesita una persona con perfil de administración y gestión de proyectos.
Gestión de Proyectos	En esta rol se encuentra la administración de los contratos o proyectos producto de la venta; aquí se debe gestionar el cumplimiento del alcance del contrato y brindar al pie de la letra los entregables descritos en el mismo. En este rol se necesita una persona con conocimientos de administración de proyectos de tecnologías de la información.
Supervisión Operativa	Se encarga de la operación propiamente dicha, donde se valida el cumplimiento de los servicios. En este rol se necesita una persona con un perfil especializado en administración y resolución de problemas. Esta persona debe tener habilidades comunicativas y de documentación.
Soporte Segundo Nivel	Se encarga de la ejecución de tareas de mayor complejidad, producto del escalamiento de los requerimientos que no pueden ser solventados por el primer nivel. En este rol se necesita una persona con un perfil especializado en resolución de problemas con equipos de seguridad de red. Esta persona debe tener habilidades comunicativas y de documentación.
Soporte Primer Nivel	Es el primer nivel de la operación, donde se analizan de primera mano los requerimientos del servicio para ejecutarlos o escalarlos. En este rol se necesita una persona con conocimientos en administración de

Rol	Descripción
	equipos de seguridad de red, adicional a esto debe tener cualidades comunicativas y de documentación.
GERENCIA COMERCIAL	Este rol permite generar las estrategias para que el equipo de ventas desarrolle nuevos negocios. Adicional a esto, este rol sirve como apoyo para el cierre efectivo de los negocios. En este rol se necesita una persona con un perfil de administración de negocios, con habilidades de negociación y con un entendimiento de tecnologías de la información.
Ventas	En este rol se recopilan o se crean las necesidades de los potenciales clientes para generar un acuerdo comercial de beneficio compartido. En este rol se necesita una persona con perfil comercial con habilidades de negociación y de documentación.
Arquitectura de soluciones	En este rol se plasman las ideas o las necesidades del cliente en soluciones tecnológicas con el fin de proporcionar un beneficio claro y de valor. En este rol se necesita una persona con alto entendimiento de soluciones de tecnologías de la información, así como de diseño de soluciones y documentación.

Tabla 2.1. Roles del organigrama [A]

Para brindar el servicio dentro de la empresa se necesitan tener todos los roles indicados en la Tabla 2.1., sin embargo esto no quiere decir que debe existir una persona por rol, pueden existir personas que manejen más de un rol dentro de la organización. Esto va a depender del crecimiento de la empresa y como se va conformando el equipo de trabajo.

En el organigrama se pueden evidenciar roles que generalmente se encuentran en todas las empresas así como también roles técnicos especializados. Para estos últimos se deben buscar perfiles que se adapten lo mejor posible a estos roles. Es muy probable que existan brechas de conocimiento técnico que deberán ser solventadas con capacitación.

Lo más importante es saber incorporar el talento adecuado para el ofrecimiento de los servicios y también para la ejecución de los mismos, así como también para la administración de los recursos de la organización. En el caso de los servicios administrados de seguridad perimetral, es necesario identificar las habilidades de cada persona asociada a cada rol para poder involucrarse en el objetivo esencial del negocio. Por ejemplo la persona de ventas debe conocer a detalle soluciones de seguridad perimetral para poder ofrecer determinado servicio o solución. Otro ejemplo es que las personas de la operación como tal (soporte de nivel 1 y nivel 2) deben conocer como configurar los equipos de seguridad que estén involucrados en los servicios. Es por esto que para el proceso de reclutamiento se debe generar un perfil del recurso a contratar en el cual se debe detallar las actividades esenciales que debe ejecutar en el rol, se deben identificar cuáles son los resultados esperados de la persona dentro del rol y el perfil de la persona donde se indiquen las habilidades y formación que este debe tener. Es necesario tener claro el propósito del rol dentro de la organización y el aporte que este va a dar a la misma.

2.2.2. *Procesos*

Los procesos dentro de una empresa de servicios permiten ejecutar de manera adecuada las actividades o el alcance definidos en los acuerdos contractuales. Los procesos se basan en conjuntos de actividades que pueden ser secuenciales o paralelas y que permiten llegar a un fin específico.

En el caso de los servicios administrados de seguridad perimetral de redes de la información es necesario incluir procesos específicos para la ejecución del servicio y es necesario además identificar aquellos componentes que permiten dar inicio al proceso. En el caso particular de los servicios administrados lo que da inicio al proceso es el requerimiento del cliente, que de manera específica es una solicitud de ejecución de determinada actividad en sus componentes de seguridad perimetral. Un ejemplo claro es la inclusión de un permiso de acceso a un determinado servicio en un firewall.

Es importante mencionar que cada actividad dentro de los procesos tiene un responsable quien vela por el cumplimiento de las tareas. Las partes involucradas son el cliente, quien inicia el proceso con una solicitud o un requerimiento, y los que ejecutan las acciones, que son los soportes de primer y segundo nivel, dependiendo de la complejidad de la ejecución. Como resultado del proceso se deben tener notificaciones de culminación del mismo y se debe tener un resultado ya sea de cumplimiento del requerimiento en función del alcance del acuerdo contractual, o de imposibilidad de ejecutarlo ya sea por alguna limitación técnica o por una limitante contractual. En el Anexo 1 se puede ver un ejemplo del flujo del

proceso de ejecución de un requerimiento; este flujo del proceso formaría parte del conjunto de procesos de la empresa como tal.

Los procesos permiten ejecutar de manera ordenada las actividades de ejecución del servicio lo que a la larga se puede traducir en ahorro de tiempo y en ahorro de recursos. Los procesos se los debe ir desarrollando en función a lo que se defina contractualmente en los acuerdos de servicio. Estos procesos no son estáticos, sino que pueden irse optimizando, mejorando o modificando de acuerdo a las necesidades del servicio o a las necesidades de un determinado control. Los procesos, al poner orden en la ejecución, permiten generar puntos de control y de observación, dando como resultado métricas de servicio.

Las métricas pueden servir como indicadores de la eficiencia del servicio y permiten llevar un nivel de cumplimiento de los acuerdos contractuales en el caso de que estos lo indiquen. Las métricas permiten ajustar la operación para que esta se pueda ejecutar de manera adecuada con la optimización de los recursos.

Con todo lo que se ha descrito anteriormente se ha podido evidenciar que es posible armar un conjunto de procesos para la ejecución de los servicios; esto hace notar que se dispone de las herramientas necesarias para poder ejecutar dichas tareas.

2.2.3. *Líneas Base de Servicio*

Las Líneas Base del Servicio permiten cuantificar el servicio, por ejemplo permiten poner un número mínimo o máximo de atenciones al mes, también podrían definir

un máximo de atenciones resueltas por mes o un mínimo de reportes mensuales. El objetivo de las líneas base es evitar el desborde de las atenciones, o requerimientos definidos en un acuerdo contractual que puede ser perjudicial para una de las partes. Normalmente se suelen definir líneas base de atención, en las cuales el cliente paga por un número determinado de atenciones mensuales y cualquier atención que sobrepase ese número será rechazada, o cobrada con un costo adicional al contrato.

Para la operación del servicio con cada cliente se deben definir las líneas base. El tamaño o la cantidad de la línea base no es impedimento para que se pueda operar el servicio, ya que en función de la cantidad de atenciones o requerimientos se deben dimensionar los recursos. Los recursos para poder operar el servicio adecuadamente van a depender del buen dimensionamiento de la solución.

No se puede especificar un listado de cuantificadores de línea base ya que los servicios administrados de equipos de seguridad perimetral son personalizables de acuerdo a las necesidades del cliente; normalmente estas definiciones se las establece en la etapa de diseño.

2.2.4. *SLAs*

Para los servicios administrados de seguridad perimetral un SLA representa el nivel de cumplimiento de determinado servicio. Cuando se miden los SLAs y no se cumplen los valores esperados en función del acuerdo contractual se puede incurrir en multas, sanciones o penalidades. La ventaja de definir adecuadamente los SLAs es que establece claramente lo que el cliente espera recibir, por lo cual es

importante contar con indicadores medibles o cuantificables incorporados dentro del contrato. Tales medidas deben ser determinadas fácilmente por ambas partes en el acuerdo contractual, y las sanciones que resulten de un nivel de servicio que cae por debajo de un nivel especificado deben ser examinadas cuidadosamente por las partes.

La mejor manera de establecer un nivel de servicio es especificar un indicador fácil de medir, como por ejemplo el tiempo de respuesta máximo de una atención en horas, el tiempo de respuesta máximo que un requerimiento puede estar sin resolver en días, el número de incidentes sin resolver dentro de un mismo día, horas de atención del servicio, horarios de atención del servicio, etc. Estos niveles de servicio deben ser claramente acordados contractualmente y deben estar documentados. Es importante recalcar que entre más altas sean las exigencias de los niveles de servicio a especificarse en un acuerdo, más alto es el riesgo de llegar al incumplimiento, por lo que es necesario cuantificar claramente en el dimensionamiento de la solución todos los componentes que permitan alcanzar dichas exigencias, como por ejemplo más personal para atender el servicio.

Así como las líneas base de servicio, los SLAs son hechos a medida de acuerdo a la necesidad de quien recibe el servicio, y la asignación de los recursos necesarios para poder atenderlo va a depender del dimensionamiento adecuado en la etapa de diseño de la solución. El rol que cumplen los procesos para el correcto cumplimiento de los SLAs se convierte en algo vital para la operación del servicio.

2.3. Análisis legal

En esta sección se presentará el marco legal que rige a las empresas que brindan servicios administrados de seguridad perimetral de redes, tanto en su regulación como en su constitución. El objetivo del análisis será la confirmación de que una empresa de servicios administrados puede ser conformada y puede operar en el país.

2.3.1. *Regulación de las telecomunicaciones en el Ecuador*

La Ley Especial de Telecomunicaciones Reformada, como norma legal superior del sector de Telecomunicaciones en la República, establece como Organismos Estatales de Regulación y Control a las siguientes entidades:

- Consejo Nacional de Telecomunicaciones (CONATEL). Es el ente de administración y regulación de las telecomunicaciones en el país. Entre las principales facultades tiene las siguientes: “dictar las políticas del estado con relación a las telecomunicaciones, aprobar el Plan Nacional de Desarrollo de las Telecomunicaciones, aprobar el plan de frecuencias y de uso del espectro radioeléctrico, aprobar los pliegos tarifarios de los servicios de telecomunicaciones abiertos a la correspondencia pública, así como los cargos de interconexión que deban pagar obligatoriamente los concesionarios de servicios portadores, incluyendo los alquileres de circuitos, establecer términos, condiciones y plazos para otorgar las concesiones y autorizaciones del uso de frecuencias así como la autorización de la explotación de los servicios finales y portadores de

telecomunicaciones, autorizar a la Secretaría Nacional de Telecomunicaciones la suscripción de contratos de concesión para la explotación de servicios de telecomunicaciones" [AA].

- Secretaría Nacional de Telecomunicaciones (SENATEL). Es el ente encargado de la ejecución de la política de Telecomunicaciones en el país. Entre sus principales facultades se encuentran: "cumplir y hacer cumplir las resoluciones del CONATEL, ejercer la gestión y administración del espectro radioeléctrico, elaborar el Plan Nacional de Desarrollo de las Telecomunicaciones y someterlo a consideración y aprobación del CONATEL, suscribir los contratos de concesión para la explotación de servicios de telecomunicaciones autorizados por el CONATEL, suscribir los contratos de autorización y/o concesión para el uso del espectro radioeléctrico autorizados por el CONATEL, otorgar la autorización necesaria para la interconexión de las redes" [AA].

- Superintendencia de Telecomunicaciones (SUPERTEL). Este ente está "encargado de cumplir y hacer cumplir las resoluciones del CONATEL, del control y monitoreo del espectro radioeléctrico, el control de los operadores que exploten los servicios de telecomunicaciones, supervisar el cumplimiento de los contratos de concesión para la explotación de los servicios de telecomunicaciones" [AA], entre otras funciones.

La Ley Especial de Telecomunicaciones Reformada clasifica los servicios de Telecomunicaciones en servicios finales y servicios portadores. También existen los servicios públicos, los cuales son servicios abiertos a la correspondencia pública y

son garantizados por el Estado debido a la importancia que tienen para la colectividad.

Los servicios finales dan la capacidad completa para la comunicación entre usuarios mientras que los servicios portadores dan la capacidad necesaria para la transmisión de señales entre puntos de red definidos y se dividen en servicios portadores que utilizan redes de telecomunicaciones conmutadas y aquellos que utilizan redes de telecomunicaciones no conmutadas. Los servicios de valor agregado son servicios finales de telecomunicaciones que incorporan aplicaciones para transformar el contenido de la información que se transmite. Los servicios finales y portadores se prestan a través de redes públicas de telecomunicaciones.

Por otro lado, existen las redes privadas, las cuales son utilizadas por personas naturales o jurídicas en su exclusivo beneficio, con el propósito de conectar distintas instalaciones de su propiedad o bajo su control. Las redes privadas no podrán prestar servicios de telecomunicaciones en el territorio nacional o en el extranjero.

La SENATEL otorga concesiones para la prestación de servicios finales y portadores y otorga permisos para la prestación de servicios de valor agregado y la instalación y operación de redes privadas.

En la Ley Especial de Telecomunicaciones Reformada no se define normativa alguna que aplique a los servicios administrados. Si bien para dar el servicio administrado de seguridad perimetral de redes se podría utilizar un servicio de un portador para conectar cada uno de los clientes con el centro de operaciones, el

servicio no pretende interconectar los clientes sino tener acceso a sus redes para poder administrar sus equipos.

2.3.2. *Constitución de la empresa*

La empresa es una organización compuesta por personas asociadas las cuales desarrollan actividades para cubrir una demanda de bienes o servicios. La constitución de una empresa está definida en un contrato de compañía, el cual se rige fundamentalmente en el contenido de la Ley de Compañías.

El organismo que vigila y controla las actividades de una empresa es la Superintendencia de Compañías, basándose en leyes y reglamentos definidos. Trabaja en conjunto con el Registro Mercantil y el Registro de la Propiedad.

La constitución de la empresa es un requisito indispensable para comenzar con el ofrecimiento de los bienes o los servicios que esta maneja. El proceso para constituir la empresa consta de varios pasos que involucran a la Superintendencia de Compañías, al Municipio, al Registro Mercantil y al Servicio de Rentas Internas (SRI). En resumen, los pasos que se deben seguir son los siguientes:

1. Aprobación del nombre o la razón social.
2. Apertura de la cuenta de integración del capital.
3. Elevar a escritura pública la constitución de la empresa en una notaría.
4. Presentación de 3 escrituras de constitución de la empresa en la Superintendencia de Compañías.

5. Publicar en un periódico el domicilio de la empresa.
6. Sentar razón de la resolución de constitución en la escritura.
7. Obtener patente municipal en la administración zonal correspondiente.
8. Inscribir las escrituras en el Registro Mercantil.
9. Obtener el Registro Único de Contribuyentes (RUC) en el SRI.

La información detallada de los pasos anteriormente expuestos se encuentra en el Anexo 2, el cual es un documento que fue provisto por la Superintendencia de Compañías.

Como parte del último paso se necesita identificar la actividad económica de la empresa de acuerdo al clasificador de actividades CIIU. La empresa que ofrezca el servicio que se está proponiendo en el presente documento debería tener el indicativo J6202.10 cuya descripción es: Actividades de planificación y diseño de sistemas informáticos que integran equipo y programas informáticos y tecnología de las comunicaciones.

En conclusión, para constituir la empresa que pueda brindar servicios administrados de seguridad perimetral de redes se debe seguir el procedimiento determinado para la constitución de la empresa manejado por la Superintendencia de Compañías.

CAPÍTULO 3. ANÁLISIS DE MERCADO

El análisis de mercado estudia la situación actual al identificar las oportunidades que existen para un producto o servicio así como los problemas asociados a los mismos. Finalmente lo que hará el análisis de mercado será definir cuáles son las necesidades del cliente y como se debe estructurar el producto o servicio para cubrir estas necesidades.

Para el caso del servicio objeto de este estudio, el análisis determinará la existencia de un mercado para el servicio de seguridad perimetral de redes dentro del sector de grandes empresas de comercio al por menor. Producto de este análisis se determinarán las formas de comercialización idóneas para el servicio propuesto.

Como fuentes primarias para el análisis de mercado se utilizarán datos de primera mano obtenidos de encuestas realizadas a las empresas que caen dentro del segmento meta. Como fuentes secundarias se utilizarán datos de estudios realizados por organizaciones acerca de la seguridad de la información.

3.1. Análisis de servicio

El objetivo de este análisis es definir de manera clara el servicio que se va a comercializar, así como también describir los factores que pueden llegar a influir en la comercialización del servicio.

3.1.1. *Definición del servicio*

Para poder ejecutar el servicio administrado de seguridad perimetral de redes es necesario definir claramente de que se trata esta actividad, cuál es su alcance y sus limitantes, por lo cual es de mucho valor diferenciar los términos implementación y operación para evitar confusiones.

Según la Real Academia de la Lengua Española, implementar es "poner en funcionamiento, aplicar métodos, medidas, etc., para llevar algo a cabo" [10]. Si se utiliza esta definición y se la lleva al ambiente de equipamiento de seguridad de redes, se puede decir que implementar es poner en funcionamiento estos equipos; es aplicar una metodología para que este equipamiento cumpla una tarea específica; en otras palabras es hacer que este funcione como debería funcionar.

Por otro lado, según la Real Academia de la Lengua Española, "operar es obrar, trabajar, ejecutar diversos menesteres u ocupaciones" [10]. Si se utiliza esta definición y se la lleva al ambiente de equipamiento de seguridad de redes, operar es ejecutar tareas específicas sobre dicho equipamiento, no es poner en funcionamiento este equipamiento desde cero, solo se trata de ejecutar tareas del día a día o tareas administrativas específicas.

Dada esta diferenciación, el servicio descrito en la presente investigación se basa en la ejecución de tareas específicas producto o resultado de las necesidades diarias de las empresas. No se trata de implementar algo nuevo o desde cero. Las implementaciones generalmente necesitan una planificación previa, mientras que la operación forma parte de un proceso definido con tareas conocidas y específicas.

Es necesario definir cuáles son las tareas que forman parte de este servicio, para que sobre ellas se pueda realizar el análisis de mercado. Las tareas que podrían forman parte de los servicios administrados de seguridad perimetral de redes se describen en la siguiente tabla en la que se muestra una clasificación por equipos.

El servicio final que se brindará al usuario no necesariamente tendrá todas las tareas que se van a enlistar; esto dependerá de las capacidades de los equipos que posea y de las necesidades particulares del cliente.

Equipo	Tareas
Firewall	creación/modificación/eliminación de objetos
	creación/modificación/eliminación de ACL
	creación/modificación/eliminación de NAT
	creación/modificación/eliminación de VPN Site to Site
	creación/modificación/eliminación de VPN Remote Access
	creación/modificación/eliminación de usuario
IDS / IPS	creación/modificación/eliminación de firma
	creación/modificación/eliminación de política de inspección
	creación/modificación/eliminación de usuario
	verificación de estado firmas
Equipo de Filtrado Web	creación/modificación/eliminación de objetos
	creación/modificación/eliminación de política de filtrado web
	creación/modificación/eliminación de política de límite de ancho de banda
	creación/modificación/eliminación de usuario

Equipo	Tareas
Gateway Antivirus	creación/modificación/eliminación de objetos
	creación/modificación/eliminación de política de antivirus
	verificación del estado de la base de datos de antivirus
	creación/modificación/eliminación de usuario
Gateway Anti-spam	creación/modificación/eliminación de dominios o IPs en listas negras
	creación/modificación/eliminación de dominios o IPs en listas blancas
	creación/modificación/eliminación de usuario
Concentrador VPNs	creación/modificación/eliminación de VPN Site to Site
	creación/modificación/eliminación de VPN Remote Access
	creación/modificación/eliminación de usuario

Tabla 3.1. Equipos de seguridad perimetral de redes y tareas asociadas [A]

3.1.2. *Análisis del entorno*

En la hipérbola de Gartner[53] para Infraestructura de TI y Servicios de Outsourcing (Figura 3.1), los servicios administrados de seguridad se encuentran subiendo la pendiente de la iluminación, con una oferta muy madura y en menos de 2 años tendrá una adopción generalizada. Gartner ubica a los servicios administrados de seguridad como parte de los servicios de Outsourcing de Seguridad conjuntamente

[53] Gartner Inc. es una empresa consultora considerada líder en investigación de tecnologías de la información y en asesoramiento tecnológico con sede en Stamford, Connecticut, Estados Unidos.

con los servicios de seguridad en la nube y con los servicios de alojamiento externo del equipamiento de seguridad.

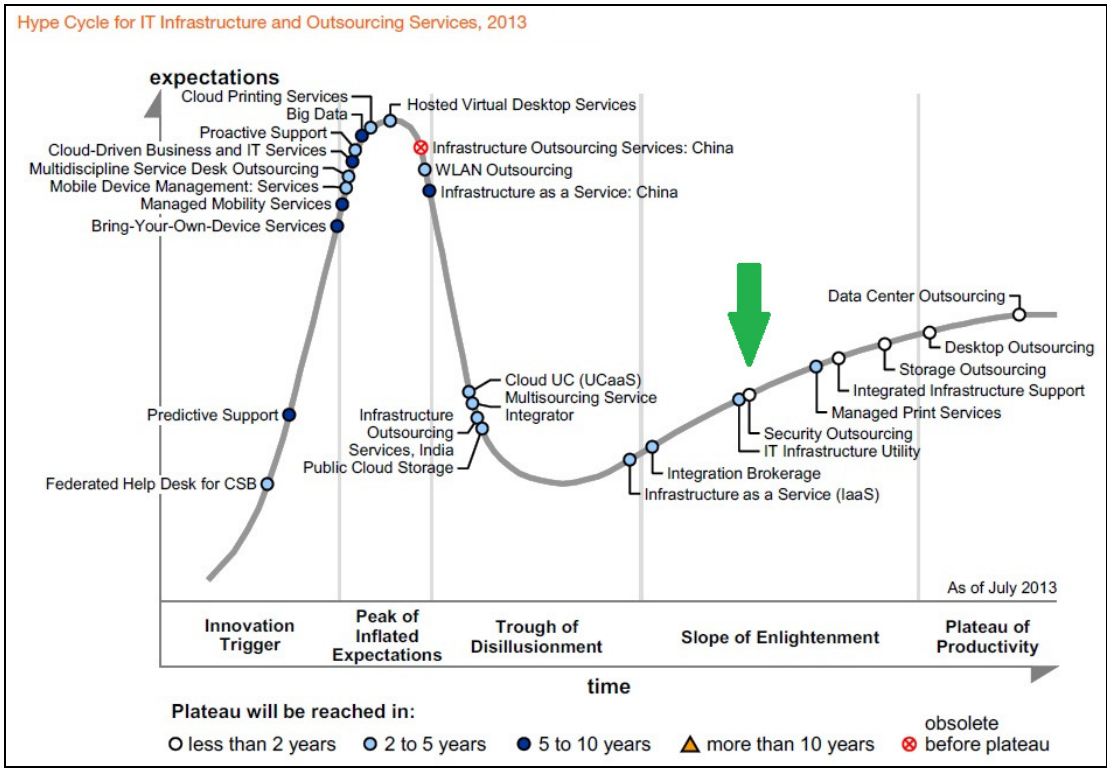

Figura 3.1. Hipérbola de Gartner - Infraestructura de TI y Servicios de Outsourcing [AE]

De acuerdo al análisis que realiza Gartner, los servicios administrados de seguridad son los únicos con una alta tasa de beneficios en comparación con aquellos que se encuentran en la misma porción de la hipérbola, indica además que sigue siendo una necesidad de inversión dentro de las empresas.

Gartner menciona además que los servicios administrados de seguridad crecerán dando a las empresas una reducción de costos y solventando los problemas de la falta de habilidades y experiencia en el manejo de plataformas; además la adopción

de servicios administrados de seguridad abrirá el camino hacia la adopción de servicios basados en la nube. Gartner también menciona que las organizaciones que participan en una amplia externalización deben planificar inversiones adicionales en las herramientas y servicios de gestión de seguridad y evaluación de vulnerabilidades para asegurar que los proveedores cumplen con los requisitos de seguridad.

La utilización de los servicios administrados de seguridad, puede ser eficaz en la mejora de la ejecución de las políticas de seguridad de la empresa así como también colabora en la reducción de costos. Sin embargo, hay que tener en cuenta que los servicios administrados de seguridad no transfieren la responsabilidad, o la reemplaza en lo que tiene que ver con la seguridad de la empresa.

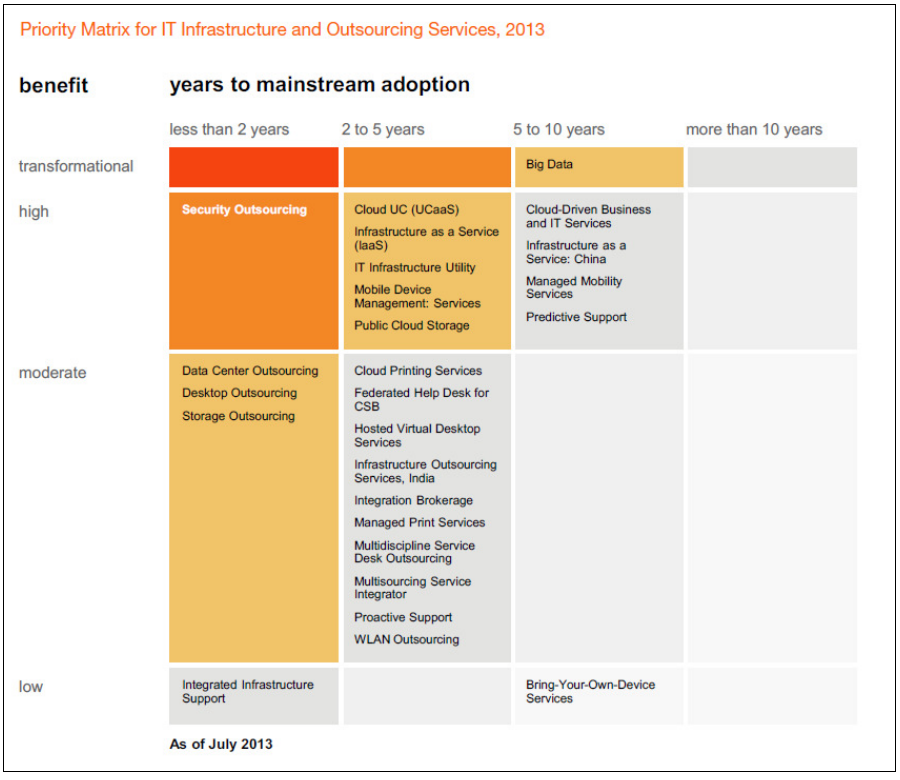

Figura 3.2. Matriz de prioridades para Infraestructura de TI - Infraestructura de TI y Servicios de Outsourcing [AE]

En la matriz de la Figura 3.2 se puede apreciar que los servicios administrados de seguridad presentan un alto beneficio y que su adopción generalizada tendrá lugar en menos de dos años, llegando en este tiempo a su periodo de madurez.

Uno de los factores que permiten la ejecución de este servicio es el acceso a las plataformas del cliente, ya sea por enlaces de datos dedicados o a través del Internet. En Ecuador, existen proveedores que tienen cobertura a nivel nacional para proporcionar enlaces de datos dedicados o enlaces de servicio de Internet.
Lo expuesto anteriormente corresponde al análisis del macroentorno del servicio. A continuación se describirán los elementos que forman parte del microentorno.

3.2. Proveedores

Como parte del análisis del microentorno en esta sección se analizarán a los proveedores del servicio de seguridad perimetral de redes.

Los proveedores son aquellos que entregan los recursos necesarios para producir el servicio. La relación que se tiene con los proveedores es sumamente importante ya que la calidad, el precio, y el tiempo de entrega de sus bienes o servicios impactan directamente al servicio que se brindará al cliente final. Principalmente, el aspecto de los proveedores que se analizará será la disponibilidad. El precio de los bienes o servicios de los proveedores se analizará en el siguiente capítulo.

Como se definió en la sección correspondiente al análisis tecnológico del servicio administrado de seguridad perimetral de redes, los bienes y servicios que se

necesitan y que están relacionados directamente con la cadena de valor son los siguientes:

- Internet
- Enlaces de datos
- Aplicación para monitoreo de Internet y enlaces de datos
- Computadoras personales con aplicaciones de ofimática
- Aplicación para seguimiento de casos
- Servicio de correo electrónico
- Servicio telefónico
- Repositorio de archivos
- Equipos de comunicaciones

Para cada uno de los bienes y servicios que se acaban de presentar se determinará la existencia de proveedores y se detallará cuál es su oferta.

Con respecto al Internet, se requiere un Internet que sea dedicado (que no sea compartido con otros usuarios) y que además sea simétrico, es decir que la velocidad de carga sea igual a la velocidad de descarga. El tráfico que pasaría por el enlace de Internet sería de administración y monitoreo, además de correo electrónico. Estos tipos de tráfico no necesitan un excesivo ancho de banda, por lo que una velocidad de mínimo 1 Mbps sería suficiente. Algunos de los proveedores locales que ofrecen este tipo de Internet corporativo son Telconet, Level3 y CNT.

En caso de que el cliente opte por una conexión a través de un enlace de datos para administrar sus equipos, este deberá ser provisto por el cliente, por lo que la

empresa que brinde los servicios administrados de seguridad perimetral de redes no necesitará proveedores de enlaces de datos.

La aplicación para el monitoreo de los enlaces de datos e Internet servirá para verificar la disponibilidad de la conexión hacia el cliente, usando principalmente el protocolo ICMP y el protocolo SNMP. Existen aplicaciones de este tipo que tienen costo y otras que no tienen costo. Entre las aplicaciones que tienen costo se encuentran WhatsUpGold, PRTG Network Monitor, IBM Tivoli Network Manager y HP Network Node Manager. Como ejemplos de las aplicaciones que no tienen costo están Cacti, Nagios y MRTG. Cabe mencionar que la mayoría de las aplicaciones que tienen costo pueden ser usadas sin necesidad de adquirir una licencia cuando el número de enlaces a ser monitoreado es menor a 10. Las aplicaciones con costo pueden ser adquiridas a través de canales en el país o directamente a la empresa desarrolladora de la aplicación utilizando el Internet.

Para las computadoras personales con aplicaciones de ofimática se necesitan equipos portátiles, con sistema operativo de tipo empresarial, que puedan conectarse en red a través de puertos RJ45 a 1 Gbps o de manera inalámbrica con soporte mínimo del estándar 802.11n y navegar por Internet utilizando un navegador web. Además deben poseer aplicaciones de editores de texto y hojas de cálculo. Este tipo de equipos con las características mencionadas se pueden encontrar en proveedores locales tales como TecnoMega, Computrón y Cinticomp. Con respecto a la aplicación para el seguimiento de casos, existen aplicaciones especializadas que realizan esta tarea; sin embargo esta misma función puede ser realizada utilizando un formato realizado en una aplicación de hoja de cálculo

El servicio de correo electrónico tiene un papel muy relevante en el servicio administrado de seguridad perimetral de redes, ya que el cliente enviará su requerimiento a través de este medio. Todos los miembros de la empresa deberán tener una cuenta de correo electrónico. Este servicio se lo puede proveer de dos maneras, a través de servidores que se encuentran localmente instalados en la empresa o como un servicio en la nube. Para la primera opción se tienen aplicaciones como por ejemplo Exchange de Microsoft o Lotus Notes de IBM. Para el segundo tipo se tienen las versiones en la nube de las aplicaciones mencionadas y también la opción de Google llamada Google Apps. Esta última opción también trae un repositorio de archivos conocido como Google Drive, que podría ser usado para el repositorio que se necesita para guardar la información generada por el servicio administrado. Para el servicio soportado en servidores locales se puede adquirir estas aplicaciones a través de proveedores locales como por ejemplo Binaria y Akros. Para adquirir la opción de correo electrónico en la nube se lo puede hacer directamente a través de Internet.

Para el servicio telefónico se tienen las opciones de telefonía fija y telefonía móvil. Para contratar telefonía fija en el país, algunas de las opciones de operadoras son CNT, Ecuadortelecom y Setel mientras que la telefonía móvil puede ser provista por Claro, Movistar y CNT.

Los equipos de comunicaciones como firewall y switches que servirán para la interconexión del centro de operaciones con las redes de los clientes podrán ser adquiridos a canales de marcas como Cisco, HP o Juniper. Entre los canales que manejan estas marcas se encuentran IBM, Logicalis, Desca, Dos.

En resumen, existen los proveedores que pueden dar los bienes y los servicios necesarios para que una empresa de servicios administrados de seguridad perimetral de redes pueda operar.

3.3. Clientes

El mercado del servicio administrado de seguridad perimetral de redes son las grandes empresas de comercio al por menor. Es necesario segmentar el mercado para definir cuál es el mercado meta.

Para la segmentación del mercado se utilizarán las siguientes variables de segmentación: ubicación geográfica, tipo de organización, tamaño del cliente y uso del servicio.

El mercado meta tendrá las siguientes características:

- Con respecto a la variable ubicación geográfica, el análisis se enfocará en las grandes empresas de comercio al por menor ubicadas en Ecuador.

- En lo referente al tipo de organización, dentro de las grandes empresas de comercio al por menor existe una gran diversidad de empresas que comercializan diferentes tipos de productos, como por ejemplo alimentos, medicinas, combustibles, prendas de vestir, electrodomésticos, artículos cosméticos, productos para la agricultura, etc. En el presente estudio se seleccionarán todos los tipos de empresas que se encuentren enmarcadas dentro de las grandes empresas del comercio al por menor.

- El tamaño de la empresa se lo define de acuerdo a lo indicado por la CAN[54], quien indica que se lo debe hacer por el volumen de ventas y el número de personas ocupadas; de estos dos criterios el que prevalece será el valor de las ventas sobre el personal ocupado. La clasificación dada por la CAN se la pude apreciar en la Tabla 3.2. De esta clasificación se puede observar que las grandes empresas son aquellas que tienen volúmenes de ventas anuales superiores a 5'000.000 USD y en la presente investigación se han seleccionado dichas empresas.

Clasificación de las empresas	Volumen de ventas anuales	Personal ocupado
Micro empresa	Menor a 100.000	1 a 9
Pequeña empresa	De 100.001 a 1´000.000	10 a 49
Mediana empresa "A"	De 1´000.001 a 2´000.000	50 A 99
Mediana empresa "B"	De 2´000.001 a 5´000.000	100 A 199
Grande empresa	De 5´000.001 en adelante	200 en adelante

Tabla 3.2. Clasificación de las empresas emitida por la CAN [11]

- Finalmente, con respecto al uso del servicio, las empresas a analizar serán aquellas que sean clientes finales del servicio administrado de seguridad perimetral de redes, y no aquellas que se presenten como intermediarias del servicio a ofrecer.

[54] Comunidad Andina de Naciones

El listado de empresas se lo ha obtenido del Ranking de Empresas del 2012 publicado por la Superintendencia de Compañías del Ecuador [12], listado que proviene de un cálculo realizado en función de los ingresos, activos y patrimonio de las empresas que presentaron a dicha institución su información financiera. De este listado, 53 empresas cumplen con los requisitos antes mencionados.

Como fuente primaria para obtener la información del mercado objetivo que servirá para definir las características del servicio y en general la factibilidad del mismo se utilizó la técnica de la encuesta.

Debido a la cantidad de empresas que se encuentran en el segmento meta, la muestra de la población de este mercado objetivo sobre la cual se aplicó la encuesta fue igual a la totalidad de las empresas.

La aplicación de la encuesta se la realizó a personas responsables de los departamentos de Sistemas, Tecnología, Infraestructura o Seguridad de la Información de las empresas seleccionadas debido a que estas personas son aquellas que pueden influir o tomar la decisión de implementar un servicio administrado de seguridad de redes.

El formato del formulario web de la encuesta que se utilizó se lo puede encontrar en el Anexo 3, el mismo que fue enviado a través de correo electrónico a las empresas del mercado meta. La información de contacto (correo electrónico) de las personas a las cuales se les envió la encuesta se la obtuvo a través de llamadas telefónicas.

3.3.1. *Resultados de la encuesta*

Del listado de 53 empresas seleccionadas se identificó que 3 de ellas pertenecen al mismo grupo empresarial; esto se identificó el momento de obtener la información de contacto vía telefónica. Debido a esto el número de empresas del segmento meta se redujo a 51.

De las 51 empresas a las cuales se les envió la encuesta, 39 de ellas enviaron sus respuestas. La localización de las 39 empresas que contestaron la encuesta se la puede observar en la Figura 3.3.

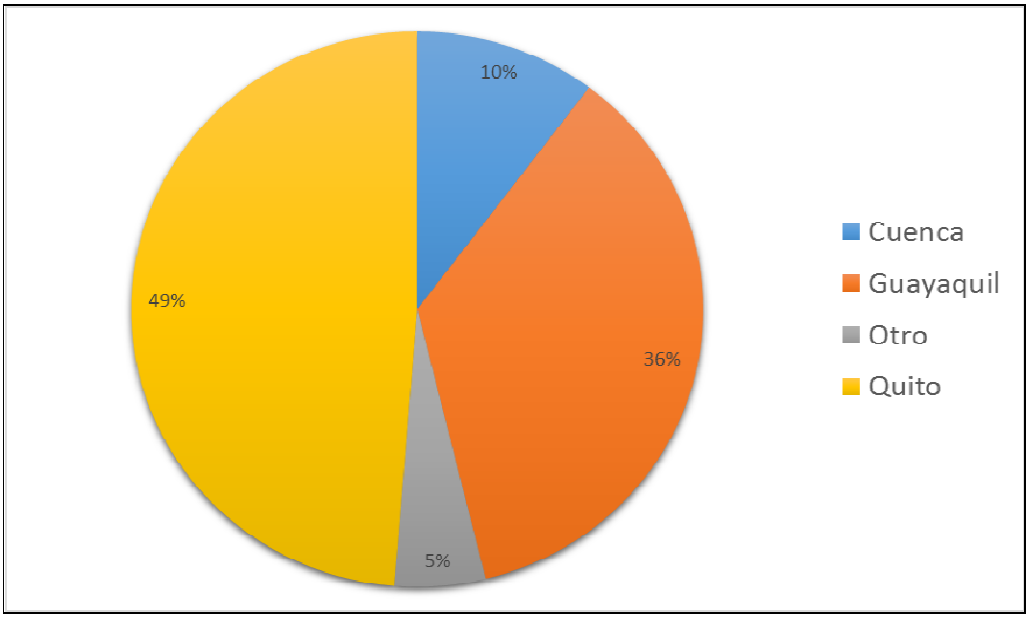

Figura 3.3. Ciudad donde está ubicada la matriz de las empresas encuestadas [A]

En la Figura 3.4 se observa que los Firewalls son los equipos que tienen mayor presencia en las empresas, seguidos por los Gateways Antivirus y los concentradores VPN. Esta información es de gran valor para la presente

investigación pues permitirá definir de manera clara el portafolio de servicios. También se observa en la Figura 3.5 que la marca predominante en las empresas es Cisco seguida por Symantec y McAfee.

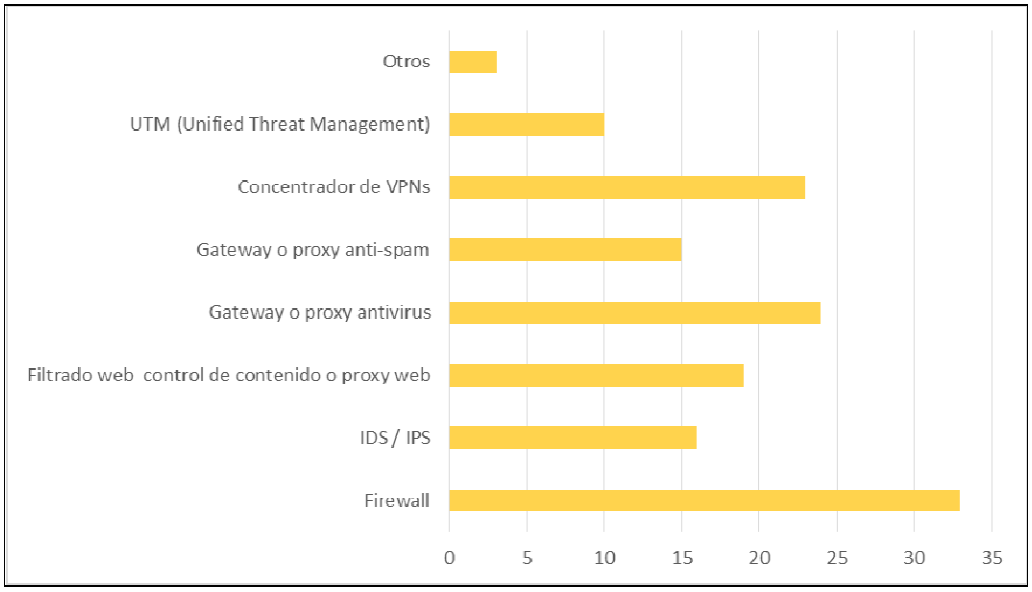

Figura 3.4. Equipos de seguridad de las empresas encuestadas [A]

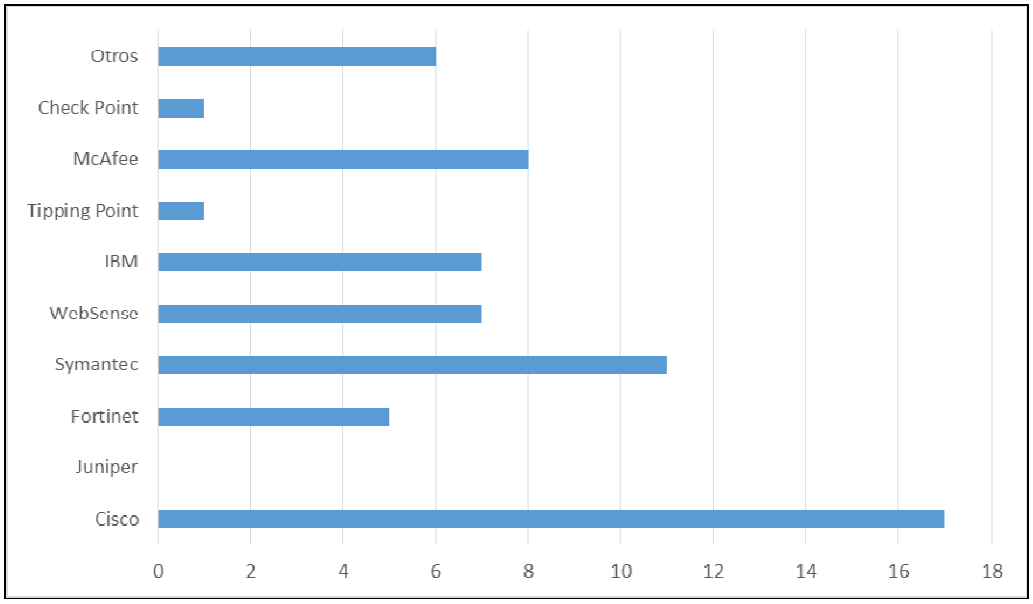

Figura 3.5. Marcas de equipos de seguridad de las empresas encuestadas [A]

Las empresas consideran que la seguridad de la información es importante; ninguna de las empresas encuestadas consideró que preocuparse de la seguridad de la información no es importante. Esto se lo puede observar en la Figura 3.6.

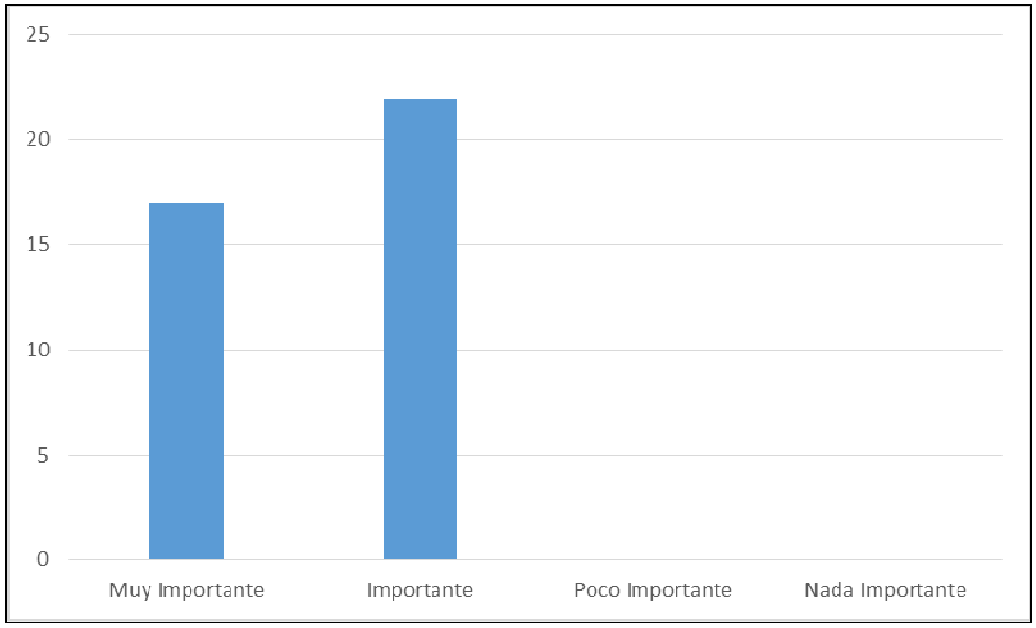

Figura 3.6. Importancia de la seguridad de la información en las empresas encuestadas [A]

Las empresas tienen personal que administra la infraestructura de red y dentro de este grupo de personas se encuentran las dedicadas a administrar los equipos de seguridad de red. El resultado de la encuesta nos indica que la mayoría de empresas de comercio al por menor tienen entre 2 y 3 personas dedicadas a administrar la infraestructura de red y 1 a 2 personas dedicadas exclusivamente a administrar los equipos de seguridad de red. En la intersección de los campos de la Tabla 3.3 se puede apreciar el número de empresas, lo cual ratifica lo mencionado.

		Personas dedicadas a seguridad				
		1	**2**	**3**	**4**	**10+**
Total de personas de infraestructura	**1**	5	-	-	-	-
	2	12	5	-	-	-
	3	7	3	-	-	-
	4	-	2	-	-	-
	5	-	1	1	-	-
	7	-	-	-	1	-
	10	-	-	1	-	-
	10+	-	-	-	-	1

Tabla 3.3. Cantidad de personas dedicadas a administrar equipos de seguridad [A]

Una de las preguntas de la encuesta permitió determinar de manera cuantitativa la cantidad de cambios que se realizan en los equipos de seguridad y se evidenció que de las empresas encuestadas un 5% realiza muchos cambios en sus equipos de seguridad, el 67% que representa la mayoría de las empresas ejecuta algunos y pocos cambios y un 28% de las empresas no realiza casi ningún cambio. En la Figura 3.7 se puede evidenciar este resultado.

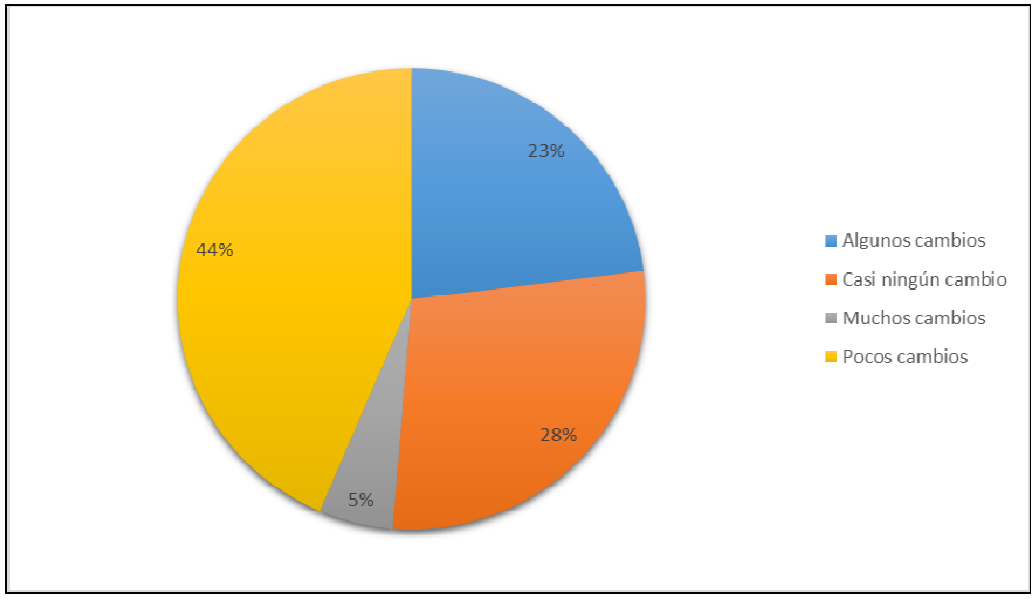

Figura 3.7. Cantidad de cambios en los equipos de seguridad de redes [A]

Continuando con los resultados de las encuestas, se evidenció que la mayoría de las empresas no poseen procesos de gestión de cambios en los equipos de seguridad de redes (Figura 3,8). Con esta información se puede concluir que para implementar servicios administrados de seguridad perimetral de redes es necesario trabajar previamente con los clientes en la definición de los procesos para la ejecución de cambios. Además esta falta de manejo de procesos en las empresas servirá como punto de partida para poder posicionar el servicio, indicando las ventajas que tiene la implementación de un servicio cómo el propuesto en lo que se refiere a la implementación de procesos claros y que generen valor.

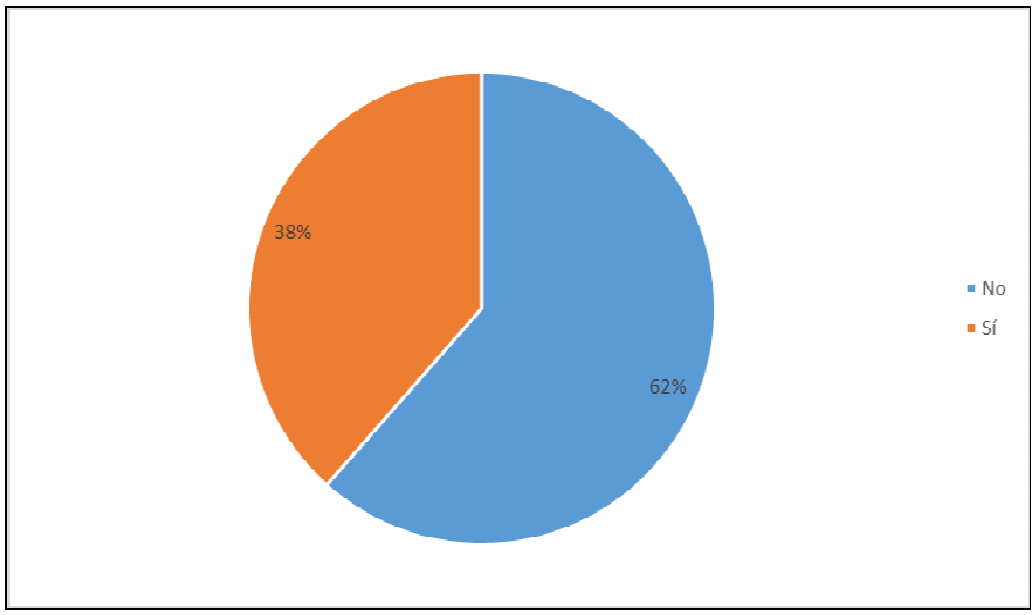

Figura 3.8. Existencia de procesos de control de cambios en equipos de seguridad [A]

Los resultados de las encuestas también permitieron evidenciar que las empresas buscan principalmente como beneficio la reducción de los costos de operación, así como también el dedicar sus esfuerzos hacia la cadena de valor de la empresa. Esta información es de mucha importancia dentro del análisis ya que permitirá definir una estrategia de promoción del servicio, indicando estos criterios como sus principales beneficios. El detalle de los beneficios marcados por las empresas encuestadas se lo puede observar en la Figura 3.9.

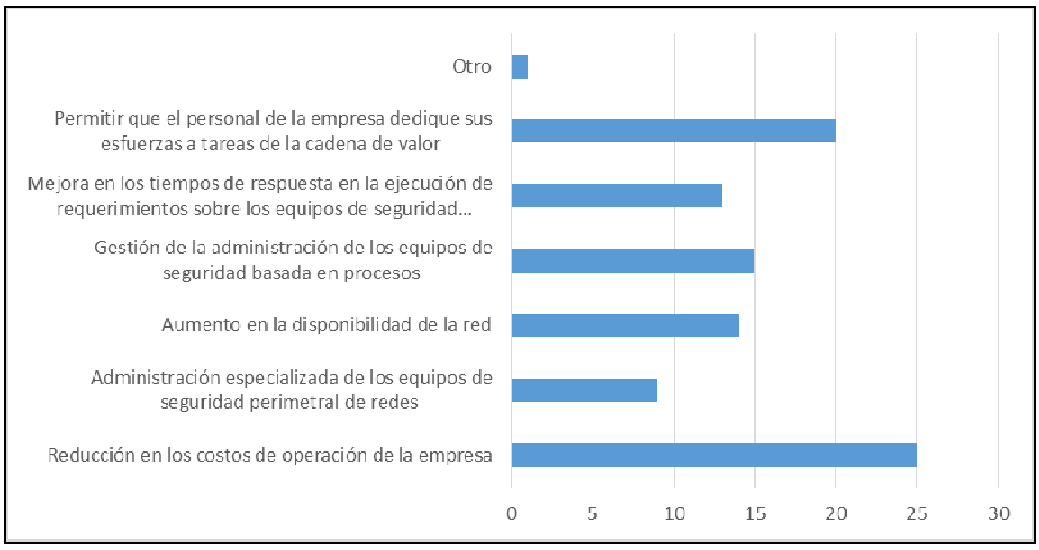

Figura 3.9. Beneficios de implementar servicios administrados de seguridad [A]

El 82% de las empresas indican que los factores clave para que las empresas del segmento meta adquieran un servicio administrado de seguridad perimetral son la confidencialidad de la información (44%), la rapidez en la ejecución (23%) y la experiencia de la empresa que ofrece el servicio (15%). Esta información también deberá ser usada dentro de las características del servicio. El factor experiencia es una limitante al ser un proyecto nuevo, sin embargo se puede cubrir este factor potencializando los anteriores y con un manejo adecuado de los procesos en la ejecución del servicio. El detalle de los factores se lo aprecia en la Figura 3.10.

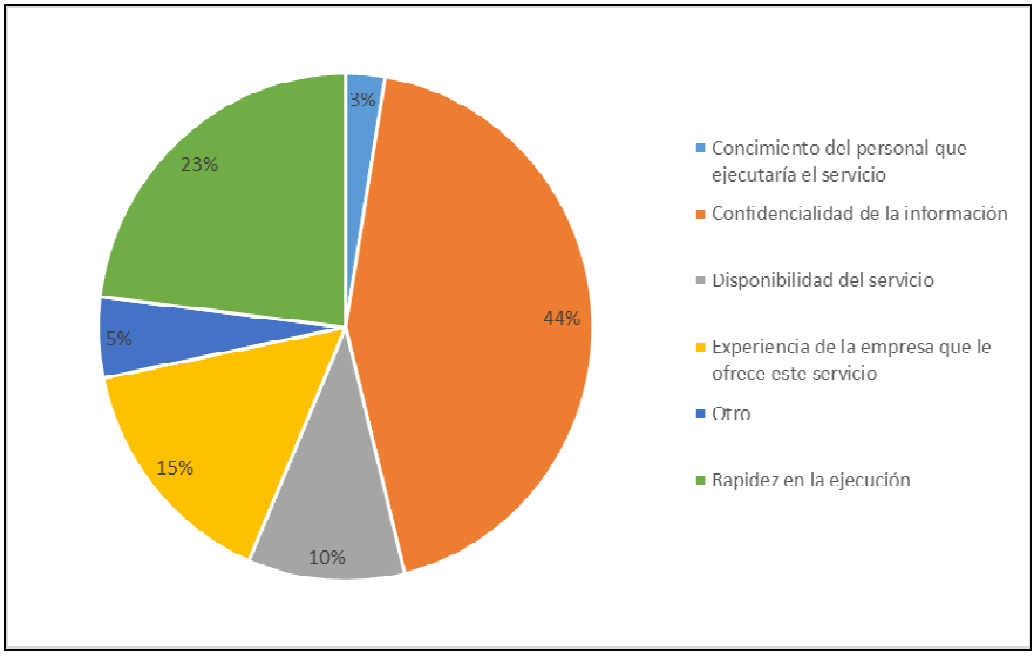

Figura 3.10. Factores para adquirir un servicio administrado se seguridad de redes [A]

Del grupo de empresas encuestadas se llegó a establecer que el número de empresas que estaría interesado en el servicio y que probablemente lo adquiera es 10, lo que representa aproximadamente un 25% del segmento meta. Esto se lo puede observar en Tabla 3.4.

		Probabilidad de adquirir el servicio		
		Muy probable	**Probable**	**TOTAL**
Interés en el servicio	**Interesado**	0	6	6
	Muy interesado	3	1	4
	TOTAL	3	7	**10**

Tabla 3.4. Cantidad de empresas interesadas que adquirirían el servicio [A]

De este grupo de empresas se tabuló el tiempo en el cual adquirirían el servicio y se lo presenta en la Figura 3.11.

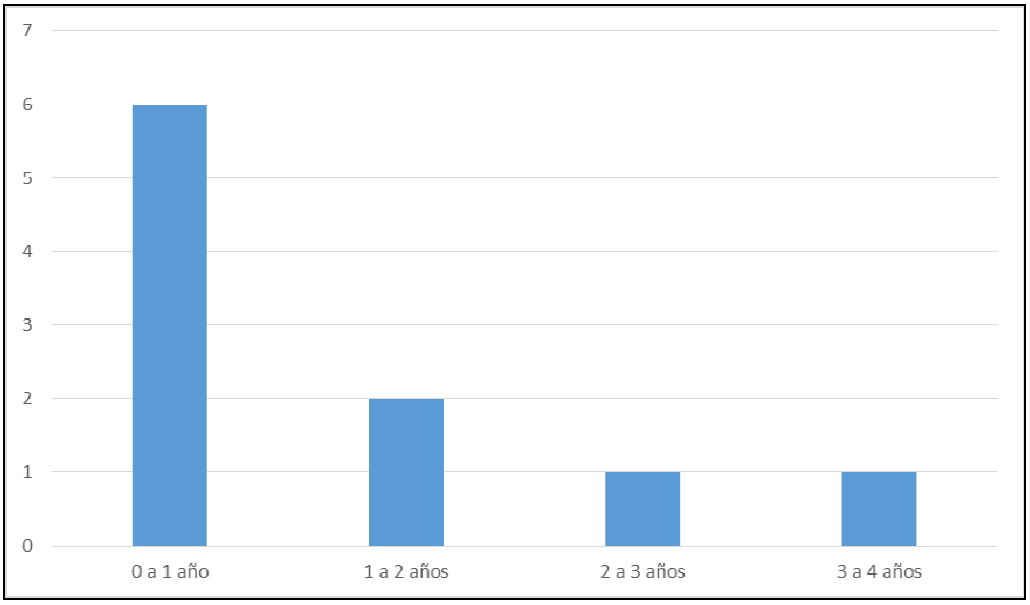

Figura 3.11. Tiempo en el que las empresas interesadas adquirirían el servicio [A]

De la misma manera, de las encuestas de las empresas interesadas y que adquirirían el servicio se obtuvo la información de cuanto estarían dispuestas a invertir. En la Figura 3.12 se observan los valores que las empresas están dispuestas a invertir. La mayoría de empresas estarían dispuestas a pagar en promedio un valor mensual de 2000 USD por este servicio.

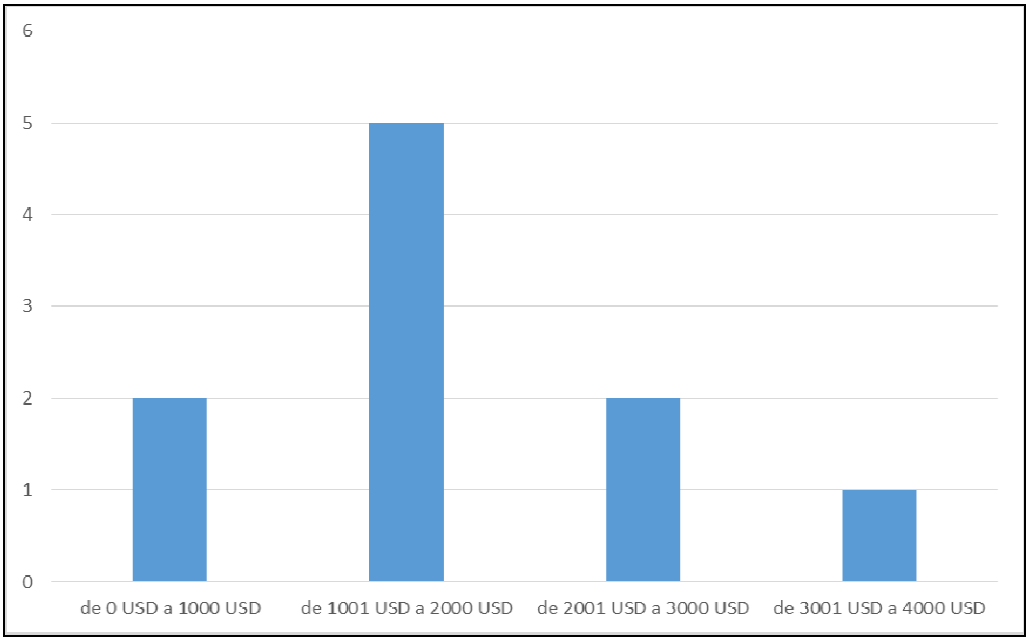

Figura 3.12. Dinero que invertirían mensualmente las empresas interesadas en el servicio administrado de seguridad perimetral de redes [A]

3.4. Competencia

En el mercado se pueden encontrar productos similares a los servicios administrados de seguridad perimetral, como son el outsourcing de los servicios de seguridad y los servicios de seguridad en la nube; sin embargo se ha indicado que cada uno de estos servicios tiene sus particularidades y se adaptan a diferentes modelos de negocio. El outsourcing de los servicios de seguridad, se adapta más a un modelo de outsourcing más complejo, donde la empresa contratante tiene algunos otros servicios de tecnología a ser atendidos. Los servicios administrados de seguridad perimetral en cambio, son el paso intermedio entre los otros tipos de servicio, siendo un esquema puntual especializado, y que al mediano o largo plazo será el que de paso a servicios más complejos como los servicios en la nube. Es

importante mencionar que los servicios de seguridad en la nube no son reemplazo de los servicios administrados de seguridad perimetral, sino que más bien son complementarios.

Los tipos de empresas que podrían brindar servicios de administración de seguridad perimetral son las siguientes [AE]:

- Proveedores de servicios de Internet y de enlaces de datos
- Grandes integradores de servicios de tecnologías de la información
- Proveedores de servicios de Outsourcing
- Vendedores de servicios específicos de seguridad

Los proveedores de servicio de Internet y de enlaces de datos tienen muchas ventajas para brindar servicios administrados de seguridad ya que disponen de lo que se mencionó en el Capítulo 1, como por ejemplo el centro de operaciones, que es el lugar donde se puede ejecutar dicho servicio. Además de ello disponen de la logística necesaria para poder brindar un servicio con determinados SLAs adaptados a la realidad del cliente. El brindar este tipo de servicios a estas empresas permite diversificar su portafolio, teniendo en cuenta que este servicio no es la razón de ser de su negocio. En este grupo de empresas se puede encontrar a Telconet, Level3, CNT como las más grandes en el Ecuador. Actualmente de estas empresas, en el Ecuador solo Telconet brinda servicios administrados de seguridad. [13]

Las empresas integradoras de servicios de tecnologías de la información son empresas que tienen muchas líneas de negocio y cuyo objetivo es brindar

soluciones integrales en lo que se refiere a tecnologías de la información. Una ventaja de estas empresas es la facilidad de incluir cualquier tipo de tecnología o producto dentro de una solución lo que permite que se puedan adaptar a cualquier necesidad particular que tenga el cliente; otra ventaja es que estas empresas disponen del personal especializado para la implementación de determinado servicio, y en caso de no tener dicha especialización, subcontratan recursos o empresas que lo hagan. Así mismo esa ventaja de poder integrar, puede convertirse en una desventaja el momento de analizar el precio, ya que estas empresas por su estructura de integradores tienen altos costos operativos. En el Ecuador existen grandes empresas integradoras como son IBM, Sonda y TATA en cuyo portafolio de servicios se encuentran los servicios administrados de seguridad; estas empresas arman soluciones a medida, y normalmente están atadas a situaciones más integrales.

Las empresas proveedoras de servicios de outsourcing tienen dentro de su portafolio de servicios la administración de la tecnología y específicamente se puede encontrar la administración de la seguridad de la información; sin embargo como se mencionó en el Capítulo 1 existe diferencia entre los servicios administrados y los servicios de outsourcing, diferencia que normalmente se basa en el esquema de la operación de dichos servicios. Las empresas de servicios de outsourcing generalmente brindan soluciones integrales asociadas a una gestión más amplia de la tecnología, y no limitadas a la seguridad de la información. La ventaja que tienen las empresas de servicios de outsourcing está en los procesos definidos y la experiencia que tienen en la operación, y se posicionan muy bien sobre todo en las empresas en las que ya operan; de manera general la administración de la seguridad es consecuencia de la administración de otros

servicios como la telefonía IP, la administración de las Redes LAN y WAN, y servidores. Una desventaja de este tipo de servicio es que no suele ser de alta especialización ya que la diversificación de los servicios limita la especialización de la ejecución por los costos que esto puede generar. En el Ecuador existen empresas que brindan servicios de Outsourcing como son IBM, Sonda, TATA y Huawei y que dentro de su portafolio de servicios de outsourcing se encuentra la administración de seguridad de la información.

Las empresas que venden servicios específicos de seguridad pueden ofrecer dentro de su portafolio servicios administrados de seguridad de redes. Estas empresas por su naturaleza de ser específicas, brindan servicios especializados que frente a las descritas anteriormente tienen ventaja en la ejecución debido a la especialización. En la actualidad las empresas tienen infraestructuras complejas, es por esto que se han creado estas empresas dedicadas a brindar servicios específicos de seguridad. En el Ecuador existen empresas de servicios específicos de seguridad como son Digiware, Inforc, y GMS las cuales están más orientadas a consultoría y resolución de problemas específicos; no se ha encontrado que estás empresas brinden servicios administrados de seguridad de redes en el país.

El éxito de un servicio administrado de seguridad perimetral de redes es la mezcla de todas las bondades que puedan tener los tipos de empresas antes detalladas como son la experiencia, la logística, la utilización de procesos claros, y la especialización en el área; el factor diferenciador justamente viene de la aplicación de las mejores prácticas de todas ellas.

3.5. Canales de comercialización

Un canal de comercialización está definido por todos los actores que participan en la comercialización de un producto o servicio, desde el productor que es el encargado de fabricar o crear el producto o servicio hasta el consumidor o usuario final. Los actores que se encuentran en el medio se los conoce como intermediarios. Dependiendo de la existencia de intermediarios entre el productor y el consumidor final existen canales de distribución directos e indirectos. En el canal directo no existen intermediarios. El canal indirecto puede ser corto si es que solo existe un intermediario o largo si es que existen varios intermediarios.

Para la comercialización del servicio administrado de seguridad perimetral de redes el canal de comercialización será principalmente directo, ya que el servicio se lo brindará directamente a los usuarios finales. Esto debido a que el proceso de comercialización de este servicio implica un trabajo previo con el usuario final para personalizarlo, en el cual se define el alcance particular para la situación del cliente.

Sin embargo, también se podrá ofrecer el servicio a través de un canal de comercialización indirecto corto, que servirá de intermediario para establecer el contacto inicial con el usuario final. Este intermediario comercial puede ser una empresa de tecnología que no tenga en su portafolio los servicios administrados y cuyo negocio sea la venta de equipos de seguridad perimetral de redes. De esta forma, la empresa de servicios administrados de seguridad perimetral de redes podría posicionar el servicio a través de un intermediario que venda equipos de seguridad perimetral de redes a clientes que no tengan personal calificado para administrarlos.

Estas dos serían las principales formas de comercialización del servicio administrado de seguridad perimetral de redes.

Después de haber realizado el análisis del entorno, teniendo en cuenta las variables del macroentorno y los elementos del microentorno, se presentará el análisis FODA[55] de la situación de la empresa que brindará servicios administrados de seguridad perimetral de redes.

3.6. Análisis FODA

Debido a que la empresa que ofrecerá los servicios administrados de seguridad perimetral de redes aún no existe, se realizará el análisis de las oportunidades y de las amenazas.

3.6.1. *Oportunidades*

- Tendencia generalizada a nivel mundial de adquisición de servicios administrados por parte de las empresas.
- Complementariedad entre los servicios administrados y la tecnología que se encuentra de moda en la actualidad, la computación en la nube.
- Inexistencia de un servicio especializado de administración de seguridad de redes en el país.
- Necesidad por parte de las empresas de reducir los costos operativos y dejar de manejar actividades no relacionadas con su cadena de valor.

[55] Fortalezas, Oportunidades, Debilidades y Amenazas.

- Escasez de personal calificado para la administración de equipos de seguridad que esté dispuestos a trabajar en empresas no relacionadas con tecnología.
- Las empresas consideran que la seguridad de la información es importante dentro de su organización.

3.6.2. *Amenazas*

- Existencia de grandes empresas a nivel mundial que están en la capacidad de dar servicios administrados de seguridad perimetral de redes en el país.
- El brindar el servicio administrado de seguridad perimetral de redes depende de la conectividad brindada por un proveedor hacia las localidades de los clientes. Si es que esta conectividad falla, no se puede dar el servicio.
- Se requiere una base mínima de políticas de seguridad y procesos asociados para brindar el servicio administrado de seguridad perimetral de redes. La mayoría de las empresas no poseen estos elementos.
- Cuando se trata el tema de servicios administrados con las empresas, estas muestran una gran preocupación acerca de la confidencialidad de su información.

CAPÍTULO 4. ANÁLISIS ECONÓMICO – FINANCIERO

En este capítulo se analizará la factibilidad económica-financiera del proyecto al definir los ingresos, el capital de trabajo, el estado de pérdidas y ganancias y finalmente el flujo de efectivo, con lo cual se podrán calcular el Valor Actual Neto (VAN) y la Tasa Interna de Retorno (TIR) del proyecto. Estos indicadores definirán si el proyecto es viable o no.

Como punto de partida del análisis se tomarán los datos de la demanda por parte de los clientes y el precio del servicio, valores que se obtuvieron de las encuestas realizadas. Con respecto al precio del servicio, las empresas encuestadas lo definieron en 2,000 USD mensuales. En lo referente a la demanda, el total de clientes que se tendrá cada año durante 4 años se lo muestra en la Tabla 4.1.

	Año 1	Año 2	Año 3	Año 4
Total de clientes	6	8	9	10

Tabla 4.1. Número total de clientes por año [A]

El precio anual del servicio es igual al precio mensual multiplicado por 12 meses, lo que da un resultado de 24,000 USD. El resultado del producto de la demanda anual y el precio anual es el ingreso anual:

	Año 1	Año 2	Año 3	Año 4
Ingreso anual	$ 144,000.00	$ 192,000.00	$ 216,000.00	$ 240,000.00

Tabla 4.2. Ingresos anuales [A]

La información del ingreso anual será utilizada más adelante en la generación del estado de pérdidas y ganancias.

4.1. Inversión

La inversión es el uso de un determinado capital en una actividad empresarial cuyo fin es incrementar dicho capital. Para determinar la cantidad de dinero que se requiere para la inversión inicial que permitiría la puesta en marcha del negocio de servicios administrados de seguridad perimetral de redes, es necesario definir los activos tangibles e intangibles de este proyecto empresarial. Adicionalmente se requiere determinar el valor del capital de trabajo, el cual se lo definirá como lo que necesita una empresa para operar con normalidad en un período corto de tiempo, como por ejemplo durante un mes.

Una vez que se haya determinado el valor de la inversión inicial en base a los activos tangibles e intangibles y al capital de trabajo, se presentará la información del préstamo requerido para poder solventar la inversión inicial.

4.1.1. *Gastos operativos y capital de trabajo*

En esta sección se calculará el valor anual de los gastos operativos durante 4 años. Los gastos operativos están compuestos de lo siguiente:

- Salarios
- Servicios básicos
- Egresos técnicos y marketing

- Arriendo del local
- Mantenimiento del local
- Suministros de oficina
- Egresos

Para el cálculo del capital de trabajo, se tomara el valor anual de los gastos operativos y se lo dividirá para el número de meses en un año.

Empezando con el primer gasto que forma parte de los gastos operativos, el salario, se tomó en cuenta el mínimo número de personas que se necesitarían para empezar con la operación de la empresa, teniendo como base el organigrama que se había definido. Se tendrá una persona para cada uno de los roles que se muestran en la Tabla 4.3. En la misma tabla también se muestra el salario y lo que la empresa debe provisionar para cada rol, considerando que el valor que la empresa paga al IESS mensualmente es el 11.15% del salario [14], los fondos de reserva son el 8.33% del salario, la provisión del décimo tercer sueldo es el salario mensual dividido para 12 meses y la provisión del décimo cuarto sueldo es el salario básico (340 USD) dividido para 12 meses. También se debe considerar que el rol de contador es ejercido por un profesional que no se encuentra en la nómina de la empresa y trabaja bajo la figura de servicios profesionales.

Rol	**Salario**	**IESS**	**Fondos de reserva**	**Provisión 13er sueldo**	**Provisión 14to sueldo**
Presidente	$2,000.00	$ 223.00	$ 166.60	$ 166.67	$ 28.33

Rol	Salario	IESS	Fondos de reserva	Provisión 13er sueldo	Provisión 14to sueldo
Gerente General	$2,000.00	$ 223.00	$ 166.60	$ 166.67	$ 28.33
Vendedor	$1,400.00	$ 156.10	$ 116.62	$ 116.67	$ 28.33
Soporte segundo nivel	$1,300.00	$ 144.95	$ 108.29	$ 108.33	$ 28.33
Soporte primer nivel	$1,100.00	$ 122.65	$ 91.63	$ 91.67	$ 28.33
Asistente	$450.00	$ 50.18	$ 37.49	$ 37.50	$ 28.33
Contador	$500.00	$ 0.00	$ 0.00	$ 0.00	$ 0.00

Tabla 4.3. Detalle salarios mensual [A]

Teniendo en cuenta la información mensual presentada con respecto a los salarios y que en el primer año de trabajo los fondos de reserva no deben ser cancelados, el gasto de los salarios por año es el siguiente:

	Año 1	Año 2	Año 3	Año 4
Salarios	$ 126,328.50	$ 134,575.20	$ 134,575.20	$ 134,575.20

Tabla 4.4. Salarios anual [A]

Para los servicios básicos, los costos mensuales son los siguientes:

Servicio básico	Costo mensual
Internet	$145.60
Luz	$30.00

Servicio básico	Costo mensual
Agua	$10.00
Telefonía fija	$30.00
Telefonía celular para 6 personas	$180.00
Total	$395.60

Tabla 4.5. Detalle servicios básicos [A]

Considerando que el primer año se debe cancelar 168 USD por la inscripción al servicio de Internet, el gasto de servicios básicos por año es el siguiente:

	Año 1	Año 2	Año 3	Año 4
Servicios básicos	$ 4,915.20	$ 4,747.20	$ 4,747.20	$ 4,747.20

Tabla 4.6. Servicios básicos anual [A]

Los egresos técnicos y de mercadeo en los que se incurrirá anualmente son los siguientes:

Servicio	Costo anual
Hosting corporativo	$50.00
Mantenimiento página web	$50.00
Google Apps para 6 personas	$300.00
Total	$400.00

Tabla 4.7. Detalle egresos técnicos y de mercadeo [A]

El primer año se pagará 400 USD por el desarrollo de la página web empresarial. Con este valor, los egresos técnicos y de mercadeo por año son:

	Año 1	Año 2	Año 3	Año 4
Egresos técnicos y mercadeo	$ 800.00	$ 400.00	$ 400.00	$ 400.00

Tabla 4.8. Egresos técnicos y de mercadeo anual [A]

Con respecto al arriendo del local, se cancelará mensualmente un valor de 450 USD. En la Tabla 4.9 se muestra el valor a cancelar anualmente por concepto de arriendo.

	Año 1	Año 2	Año 3	Año 4
Arriendo	$ 5,400.00	$ 5,400.00	$ 5,400.00	$ 5,400.00

Tabla 4.9. Arriendo anual [A]

Para el mantenimiento del local arrendado, se destinará mensualmente 100 USD para la alícuota y 50 USD para la limpieza del mismo. Por año, los gastos de mantenimiento serían los siguientes:

	Año 1	Año 2	Año 3	Año 4
Mantenimiento local	$ 1,800.00	$ 1,800.00	$ 1,800.00	$ 1,800.00

Tabla 4.10. Mantenimiento del local anual [A]

Para los suministros de oficina se gastará 60 USD mensuales. En la Tabla 4.11 se indica el gasto anual.

	Año 1	Año 2	Año 3	Año 4
Suministros	$ 720.00	$ 720.00	$ 720.00	$ 720.00

Tabla 4.11. Suministros anual [A]

Al ser una empresa puramente servicios, los egresos que se generan en función de la demanda tienen relación con el número de ingenieros de soporte de primer nivel. Mientras más demanda exista, se necesitará un mayor número de ingenieros de soporte de primer nivel. Por cada nuevo ingeniero que ingrese a la empresa, se requerirá contemplar por una sola vez una laptop y sus respectivos muebles. Además se deberá contemplar el pago mensual de los servicios que la empresa le debe proveer al nuevo empleado para que este pueda desempeñar su función. Todo esto se le encuentra detallado en la Tabla 4.12 con sus respectivos costos.

Elemento	Costo
Servicio Google apps mensual para 1 persona	$ 4.17
Servicio telefonía celular mensual para 1 persona	$ 30.00
Servicios básicos mensual para 1 persona	$ 11.67
Suministros mensual para 1 persona	$ 10.00
1 laptop	$ 970.00
1 juego de muebles	$ 373.00

Tabla 4.12. Detalle gastos adicionales por ingreso de nueva persona [A]

El número de ingenieros de soporte adicionales que se requiere, considerando que un ingeniero de soporte puede atender a un máximo de cuatro clientes, es de 0 para el primer año, 1 para el segundo año y 1 más para el tercer año. Los egresos

generados en función de la contratación de este personal adicional año tras año se muestran a continuación:

	Año 1	**Año 2**	**Año 3**	**Año 4**
Total ingenieros adicionales	0	1	2	2
Salarios	$ 0.00	$ 16,111.80	$ 33,323.16	$ 34,422.72
Servicios y suministros	$ 0.00	$ 670.00	$ 1,340.00	$ 1,340.00
Egresos	$ 0.00	$ 16,781.80	$ 34,663.16	$ 35,762.72

Tabla 4.13. Egresos anual [A]

Adicionalmente, se deberá contemplar la adquisición de 1 laptop (970 USD) y 1 juego de muebles (373 USD) en los años en los cuales ingrese una nueva persona. El valor total de estos elementos es de 1,343 USD, valor que deberá ser contemplado como inversión en el año 2 y el mismo valor en el año 3 cuando se realice el flujo de efectivo más adelante.

Con toda esta información, los gastos operativos anuales son:

	Año 1	**Año 2**	**Año 3**	**Año 4**
Salarios	$ 126,328.50	$ 134,575.20	$ 134,575.20	$ 134,575.20
Servicios básicos	$ 4,915.20	$ 4,747.20	$ 4,747.20	$ 4,747.20
Egresos técnicos y mercadeo	$ 800.00	$ 400.00	$ 400.00	$ 400.00
Arriendo	$ 5,400.00	$ 5,400.00	$ 5,400.00	$ 5,400.00
Mantenimiento local	$ 1,800.00	$ 1,800.00	$ 1,800.00	$ 1,800.00

	Año 1	Año 2	Año 3	Año 4
Suministros	$ 720.00	$ 720.00	$ 720.00	$ 720.00
Egresos	$ 0.00	$ 16,781.80	$ 34,663.16	$ 35,762.72
Gastos operativos	$ 139,963.70	$ 164,424.20	$ 182,305.56	$ 183,405.12

Tabla 4.14. Gastos operativos [A]

Para obtener el capital de trabajo, dividimos el valor del gasto operativo para el número de meses de un año:

	Año 1	Año 2	Año 3	Año 4
Capital de trabajo	$ 11,663.64	$ 13,702.02	$ 15,192.13	$ 15,283.76

Tabla 4.15. Capital de trabajo [A]

4.1.2. *Activos tangibles e intangibles*

Los activos están compuestos por los equipos, el mobiliario y los gastos de constitución de la empresa. El detalle de estos elementos se muestra a continuación.

Activo	Descripción	Costo unitario	Cantidad	Sub-total
Switch	8 puertos de 1 Gbps.	$ 20.00	1	$ 20.00
Servidor monitoreo/firewall	Procesador Intel Core i5, 8GB de RAM, 500 GB de disco duro,	$ 900.00	1	$ 900.00

Activo	Descripción	Costo unitario	Cantidad	Sub-total	
	sistema operativo CentOS.				
Laptop	Procesador Intel Core i5, 4GB de RAM, 350 GB de disco duro, sistema operativo Windows 7 Professional.	$ 970.00	6	$ 5,820.00	
Escritorio	Para 1 persona	$ 179.00	6	$ 1,074.00	
Silla	Para 1 persona	$ 39.00	6	$ 234.00	
Archivador	Para 1 persona	$ 155.00	6	$ 930.00	
				$ 8,978.00	**Total**

Tabla 4.16. Equipos de cómputo y mobiliario en el año 0 [A]

Lo que se muestra en la Tabla 4.16 corresponde a la inversión inicial que se debe realizar en lo que respecta a equipos de cómputo y mobiliario en el año 0. Para el año 2 y el año 3 se debe considerar la laptop y el mobiliario para el nuevo personal que ingresaría a la empresa. Como se detalló anteriormente, el valor que se debería tener en cuenta es de 1,343 USD en cada uno de estos años:

	Año 0	Año 1	Año 2	Año 3	Año 4
Equipos de cómputo y mobiliario	$ 8,978.00	$ 0,00	$ 1,343.00	$ 1,343.00	$ 0,00

Tabla 4.17. Equipos de cómputo y mobiliario en 4 años [A]

En la Tabla 4.18 se encuentran los gastos asociados con la constitución de la empresa:

Gasto	Descripción	Costo	
Asesoría Legal	Honorarios de abogado para asesoría en la constitución de la empresa.	$1,000.00	
Registro IEPI	Registro del nombre de la empresa en el Instituto Ecuatoriano de Propiedad Intelectual.	$116.00	
		$ 1,116.00	**Total**

Tabla 4.18. Gastos de constitución [A]

4.1.3. *Inversión inicial y préstamo*

Como se había mencionado, la inversión inicial estará compuesta por la suma de los equipos de cómputo, el mobiliario, los gastos de constitución y el capital de trabajo del primer año.

Elemento	Valor
Capital de trabajo	$ 11,663.64
Equipos de cómputo y mobiliario	$ 8,978.00
Gastos de constitución	$ 1,116.00
Inversión inicial	$ 21,757.64

Tabla 4.19. Inversión inicial [A]

Del valor total que se necesita como inversión inicial, el 55.15% (12,000 USD) se lo cubrirá con capital propio y el restante 44.85% (9,757.64 USD) con un préstamo

bancario que se lo sacará a 36 meses (3 años) con una tasa de interés anual referencial del 11.83%, que es la tasa máxima para un préstamo productivo para pequeñas y medianas empresas referenciado por el Banco Central del Ecuador [15]. A continuación se presenta la tabla de amortización de dicho préstamo:

Cuota N°	Saldo Capital	Capital	Interés	Cuota
0	$ 9,757.64			
1	$ 9,530.53	$ 227.11	$ 96.19	$ 323.30
2	$ 9,301.19	$ 229.35	$ 93.96	$ 323.30
3	$ 9,069.58	$ 231.61	$ 91.69	$ 323.30
4	$ 8,835.69	$ 233.89	$ 89.41	$ 323.30
5	$ 8,599.49	$ 236.20	$ 87.11	$ 323.30
6	$ 8,360.97	$ 238.52	$ 84.78	$ 323.30
7	$ 8,120.09	$ 240.88	$ 82.43	$ 323.30
8	$ 7,876.84	$ 243.25	$ 80.05	$ 323.30
9	$ 7,631.19	$ 245.65	$ 77.65	$ 323.30
10	$ 7,383.12	$ 248.07	$ 75.23	$ 323.30
11	$ 7,132.60	$ 250.52	$ 72.79	$ 323.30
12	$ 6,879.62	$ 252.99	$ 70.32	$ 323.30
13	$ 6,624.14	$ 255.48	$ 67.82	$ 323.30
14	$ 6,366.14	$ 258.00	$ 65.30	$ 323.30
15	$ 6,105.60	$ 260.54	$ 62.76	$ 323.30
16	$ 5,842.49	$ 263.11	$ 60.19	$ 323.30
17	$ 5,576.78	$ 265.70	$ 57.60	$ 323.30

Cuota N°	Saldo Capital	Capital	Interés	Cuota
18	$ 5,308.46	$ 268.32	$ 54.98	$ 323.30
19	$ 5,037.49	$ 270.97	$ 52.33	$ 323.30
20	$ 4,763.85	$ 273.64	$ 49.66	$ 323.30
21	$ 4,487.51	$ 276.34	$ 46.96	$ 323.30
22	$ 4,208.45	$ 279.06	$ 44.24	$ 323.30
23	$ 3,926.64	$ 281.81	$ 41.49	$ 323.30
24	$ 3,642.04	$ 284.59	$ 38.71	$ 323.30
25	$ 3,354.65	$ 287.40	$ 35.90	$ 323.30
26	$ 3,064.42	$ 290.23	$ 33.07	$ 323.30
27	$ 2,771.32	$ 293.09	$ 30.21	$ 323.30
28	$ 2,475.34	$ 295.98	$ 27.32	$ 323.30
29	$ 2,176.45	$ 298.90	$ 24.40	$ 323.30
30	$ 1,874.60	$ 301.85	$ 21.46	$ 323.30
31	$ 1,569.78	$ 304.82	$ 18.48	$ 323.30
32	$ 1,261.95	$ 307.83	$ 15.48	$ 323.30
33	$ 951.09	$ 310.86	$ 12.44	$ 323.30
34	$ 637.17	$ 313.93	$ 9.38	$ 323.30
35	$ 320.15	$ 317.02	$ 6.28	$ 323.30
36	($ 0.00)	$ 320.15	$ 3.16	$ 323.30

Tabla 4.20. Tabla de amortización del préstamo [A]

Un resumen del total por año de los valores de capital e interés del préstamo se muestra en la Tabla 4.21.

	Año 1	Año 2	Año 3	Año 4
Capital	$ 2,878.02	$ 3,237.57	$ 3,642.04	$ 0.00
Interés	$ 1,001.60	$ 642.05	$ 237.58	$ 0.00

Tabla 4.21. Capital e interés del préstamo por año [A]

4.2. Análisis de rentabilidad

Como parte del análisis del presente trabajo, el cual se lo puede considerar como un proyecto de inversión, es necesario determinar si el proyecto es rentable o no lo es. Para determinar esto en primer lugar se realizará el estado de pérdidas y ganancias en donde se muestran los ingresos de la empresa así como sus egresos para finalmente poder calcular el valor de la utilidad neta en cada uno de los años que forman parte del análisis. En segundo lugar se procederá con la realización del estado de flujo de efectivo, que utilizará como entrada el valor de la utilidad neta en cada año y obtendrá de resultado el valor del flujo neto de efectivo para cada año del análisis. Finalmente los valores del flujo neto de efectivo serán utilizados para realizar el cálculo del VAN y el TIR, que son los indicadores financieros que permitirán definir si el proyecto es rentable o no.

4.2.1. *Estado de pérdidas y ganancias*

Para realizar el estado de pérdidas y ganancias se utilizarán los valores de ingresos y gastos operativos que ya se obtuvieron. Adicionalmente, se necesitan calcular los valores de depreciación y amortización de los activos tangibles e intangibles respectivamente.

Con respecto a la depreciación, las instalaciones, maquinarias, equipos y muebles se deprecian al 10% anual mientras que los equipos de cómputo y software al 33% anual [16]. Es decir, los primeros se deprecian totalmente en 10 años y los segundos en 3 años.

Tipo de activo	Activo	Costo	Depreciación anual
Muebles	Escritorio	$ 179.00	$ 17.90
	Silla	$ 39.00	$ 3.90
	Archivador	$ 155.00	$ 15.50
Equipos de cómputo	Laptop	$ 970.00	$ 323.33
	Switch	$ 20.00	$ 6.67
	Servidor monitoreo/firewall	$ 900.00	$ 300.00

Tabla 4.22. Valor depreciación activos [A]

A cada empleado que ingrese a la empresa se le dará un escritorio, una silla, un archivador y una laptop. La suma del valor de depreciación del escritorio (17.90 USD), de la silla (3.90 USD), del archivador (15.50 USD) y de la laptop (323.33 USD) da como resultado 360.63 USD. Teniendo en cuenta esto, los tiempos de depreciación de los activos y que en el año 2 ingresará 1 empleado y en el año 3 otro empelado más, la depreciación de los activos año por año y el valor de salvamento se muestran a continuación:

	Año 1	Año 2	Año 3	Año 4	Valor Salvamento
Total empleados	6	7	8	8	
Activos empleado 1	$ 360.63	$ 360.63	$ 360.63	$ 37.30	$ 223.80
Activos empleado 2	$ 360.63	$ 360.63	$ 360.63	$ 37.30	$ 223.80

	Año 1	Año 2	Año 3	Año 4	Valor Salvamento
Activos empleado 3	$ 360.63	$ 360.63	$ 360.63	$ 37.30	$ 223.80
Activos empleado 4	$ 360.63	$ 360.63	$ 360.63	$ 37.30	$ 223.80
Activos empleado 5	$ 360.63	$ 360.63	$ 360.63	$ 37.30	$ 223.80
Activos empleado 6	$ 360.63	$ 360.63	$ 360.63	$ 37.30	$ 223.80
Activos empleado 7	$ 0.00	$ 360.63	$ 360.63	$ 360.63	$ 261.10
Activos empleado 8	$ 0.00	$ 0.00	$ 360.63	$ 360.63	$ 621.73
Switch	$ 6.67	$ 6.67	$ 6.67	$ 0.00	$ 0.00
Servidor	$ 300.00	$ 300.00	$ 300.00	$ 0.00	$ 0.00
Total Depreciación	$ 2,470.47	$ 2,831.10	$ 3,191.73	$ 945.07	$ 2,225.63

Tabla 4.23. Depreciación anual y salvamento [A]

Para la amortización de las inversiones que son necesarias para constituir la empresa se tomará como referencia el valor del 25% anual, es decir se amortizará en 4 años. Como inversión de constitución de la empresa se considerará la asesoría legal con un costo de 1000 USD y el registro del nombre de la empresa en el IEPI por 116 USD como ya se había mencionado.

	Año 1	Año 2	Año 3	Año 4	Valor Salvamento
Amortización asesoría legal	$ 250.00	$ 250.00	$ 250.00	$ 250.00	$ 0.00
Amortización registro IEPI	$ 29.00	$ 29.00	$ 29.00	$ 29.00	$ 0.00
Total Amortización	$ 279.00	$ 279.00	$ 279.00	$ 279.00	$ 0.00

Tabla 4.24. Amortización anual y salvamento [A]

Teniendo los valores de los ingresos, los gastos operativos y los intereses del préstamo y habiendo calculado los valores de depreciación y amortización, en la Tabla 4.25 se muestra el estado de pérdidas y ganancias. Para el cálculo de la

participación de las utilidades se consideró un porcentaje del 15% de acuerdo a lo dictado por el Código del Trabajo en su Artículo 97. Para el cálculo del impuesto a la renta se consideró un porcentaje del 22% de acuerdo a lo establecido en la reforma al Artículo 37 de la Ley de Régimen Tributario Interno.

	Año 1	**Año 2**	**Año 3**	**Año 4**
Ingresos por ventas	$ 144,000.00	$ 192,000.00	$ 216,000.00	$ 240,000.00
Salarios	($ 126,328.50)	($ 150,687.00)	($ 167,898.36)	($ 168,997.92)
Servicios básicos	($ 4,915.20)	($ 4,747.20)	($ 4,747.20)	($ 4,747.20)
Egresos técnicos y mercadeo	($ 800.00)	($ 400.00)	($ 400.00)	($ 400.00)
Arriendo	($ 5,400.00)	($ 5,400.00)	($ 5,400.00)	($ 5,400.00)
Mantenimiento	($ 1,800.00)	($ 1,800.00)	($ 1,800.00)	($ 1,800.00)
Suministros	($ 720.00)	($ 720.00)	($ 720.00)	($ 720.00)
Otros egresos	$ 0.00	($ 670.00)	($ 1,340.00)	($ 1,340.00)
Depreciación	($ 2,470.47)	($ 2,831.10)	($ 3,191.73)	($ 945.07)
Amortización	($ 279.00)	($ 279.00)	($ 279.00)	($ 279.00)
Total egresos	($ 142,713.17)	($ 167,534.30)	($ 185,776.29)	($ 184,629.19)
Utilidad operacional	$ 1,286.83	$ 24,465.70	$ 30,223.71	$ 55,370.81
Intereses	($ 1,001.60)	($ 642.05)	($ 237.58)	$ 0.00
Utilidad antes de participación	$ 285.24	$ 23,823.65	$ 29,986.13	$ 55,370.81
15% de participación	($ 42.79)	($ 3,573.55)	($ 4,497.92)	($ 8,305.62)

	Año 1	Año 2	Año 3	Año 4
Utilidad antes de impuestos	$ 242.45	$ 20,250.11	$ 25,488.21	$ 47,065.19
22% de impuesto a la renta	($ 53.34)	($ 4,455.02)	($ 5,607.41)	($ 10,354.34)
Utilidad neta	$ 189.11	$ 15,795.08	$ 19,880.80	$ 36,710.85

Tabla 4.25. Estado de pérdidas y ganancias [A]

4.2.2. *Estado de flujo de efectivo*

El estado de flujo de efectivo permite identificar el movimiento de los recursos año tras año. Para calcularlo se utilizará toda la información que se ha obtenido hasta el momento. Además, se utilizarán los valores anuales del pago de capital del préstamo, en los años 2 y 3 se incluirá en la inversión los equipos y mobiliario del nuevo personal que ingresará y en el año 4 se incluirán los valores de salvamento y de recuperación del capital de trabajo.

		Año 0	Año 1	Año 2	Año 3	Año 4
Inversión	Equipos	($ 6,740.00)	$ 0.00	($ 970.00)	($ 970.00)	$ 0.00
	Mobiliario	($ 2,238.00)	$ 0.00	($ 373.00)	($ 373.00)	$ 0.00
	Constitución	($ 1,116.00)	$ 0.00	$ 0.00	$ 0.00	$ 0.00
	Capital de trabajo	($ 11,663.64)	$ 0.00	$ 0.00	$ 0.00	$ 0.00
	Préstamo	$ 9,757.64	$ 0.00	$ 0.00	$ 0.00	$ 0.00
Flujo del proyecto	Utilidad neta	$ 0.00	$ 189.11	$ 15,795.08	$ 19,880.80	$ 36,710.85
	Depreciación	$ 0.00	$ 2,470.47	$ 2,831.10	$ 3,191.73	$ 945.07

	Año 0	Año 1	Año 2	Año 3	Año 4
Amortización	$ 0.00	$ 279.00	$ 279.00	$ 279.00	$ 279.00
Valor Salvamento	$ 0.00	$ 0.00	$ 0.00	$ 0.00	$ 2,225.63
Recuperación KT	$ 0.00	$ 0.00	$ 0.00	$ 0.00	$ 11,663.64
Pago de capital	$ 0.00	($ 2,878.02)	($ 3,237.57)	($ 3,642.04)	$ 0.00
Flujo neto efectivo	($ 12,000.00)	$ 60.56	$ 14,324.61	$ 18,366.49	$ 51,824.19

Tabla 4.26. Estado de flujo de efectivo [A]

4.2.3. *Indicadores financieros*

Finalmente, para evaluar la rentabilidad del proyecto de inversión se utilizarán los indicadores financieros VAN y TIR. El VAN mide los flujos de ingresos y egresos en el período de análisis, con lo cual se puede definir, luego de restar la inversión inicial, si el proyecto de inversión generará una ganancia. También se lo utiliza para determinar cuál es el proyecto más rentable entre un grupo de opciones que se pudieran tener. Para calcular el VAN se utilizará el valor de la inversión, el flujo neto efectivo y una tasa comparativa. La fórmula es la siguiente:

$$\mathrm{VAN} = \sum_{t=1}^{t=n} \frac{V_t}{(1+k)^t} - I_0$$

Figura 4.1. Fórmula VAN [17]

Donde:

- V_t es el flujo neto de efectivo en un determinado año
- I_O es el valor de la inversión inicial.
- n es el número de años considerados en el análisis
- k es el valor de la tasa de descuento

En la siguiente tabla se muestra el VAN resultante para varios valores de tasa:

Tasa	VAN
0.00%	$ 72,575.85
5.00%	$ 59,552.07
10.00%	$ 49,089.21
12.99%	$ 43,802.13
15.00%	$ 40,591.04
20.00%	$ 33,619.24
30.00%	$ 23,027.58
40.00%	$ 15,535.32
50.00%	$ 10,085.66
60.00%	$ 6,025.15
70.00%	$ 2,935.51
80.00%	$ 540.84
82.64%	$ 0.00
90.00%	($ 1,345.71)
100.00%	($ 2,853.75)
110.00%	($ 4,075.00)

Tabla 4.27. VAN [A]

La tasa de descuento que se utilizará para la comparación es el resultado de la adición de la tasa libre de riesgo, la inflación anual y el riesgo país. De acuerdo con datos manejados por el Banco Central del Ecuador [18], la tasa libre de riesgo en Abril 2014 es del 4.53%, la inflación anual en Marzo 2014 es del 3.11% y el riesgo país en Marzo 2014 es del 5.35%. Esto da como resultado una tasa de descuento del 12.99%.

Elemento	Valor
Tasa libre de riesgo	4.53%
Inflación anual	3.11%
Riesgo país	5.35%
Tasa de descuento	**12.99%**

Tabla 4.28. Tasa de descuento [A]

De acuerdo a lo mostrado en la Tabla 4.27, el valor del VAN con la tasa de descuento del 12.99% es mayor que cero, por lo que el proyecto es rentable. También se puede apreciar que el valor del TIR (tasa cuando el VAN es igual a cero), es igual a 82.64%.

4.3. Análisis de sensibilidad

Para realizar el análisis de la sensibilidad se calculará el VAN y TIR al variar la demanda y los costos.

En el primer escenario se variará la demanda, es decir el número de clientes que adquirirían el servicio año tras año. En la Tabla 4.29 se observan los resultados de las variaciones de la demanda al hacerla crecer y decrecer en un 5% y en un 10%.

Demanda	Costos	VAN (12.99%)	TIR
Crece 10%	Se mantiene	$ 81,912.89	149.98%
Crece 5%	Se mantiene	$ 62,857.51	115.65%
Se mantiene	Se mantiene	$ 43,802.13	82.64%
Decrece 5%	Se mantiene	$ 24,746.75	51.20%
Decrece 10%	Se mantiene	$ 5,691.37	21.51%

Tabla 4.29. Sensibilidad al variar demanda [A]

En el siguiente escenario se variarán los costos, en particular se variará el costo resultante del pago de salarios. Debido a que los salarios solo podrían crecer y no disminuir, se hará el cálculo cuando estos crezcan desde el 5% hasta el 20%.

Demanda	Costos	VAN (12.99%)	TIR
Se mantiene	Crece 20%	($ 15,461.60)	-7.28%
Se mantiene	Crece 15%	($ 645.67)	12.10%
Se mantiene	Crece 10%	$ 14,170.27	33.53%
Se mantiene	Crece 5%	$ 28,986.20	57.07%
Se mantiene	Se mantiene	$ 43,802.13	82.64%

Tabla 4.30. Sensibilidad al variar costos [A]

Finalmente, en el último escenario de análisis se variará tanto la demanda como los costos.

Demanda	Costos	VAN (12.99%)	TIR
Crece 10%	Crece 5%	$ 67,096.96	121.18%
Crece 10%	Crece 10%	$ 52,281.02	93.90%
Crece 5%	Crece 5%	$ 48,041.58	88.32%
Se mantiene	Se mantiene	$ 43,802.13	82.64%
Crece 5%	Crece 10%	$ 33,225.64	62.80%
Decrece 5%	Crece 5%	$ 9,930.82	27.61%
Decrece 5%	Crece 10%	($ 4,885.11)	6.15%
Decrece 10%	Crece 5%	($ 9,124.56)	-0.02%
Decrece 10%	Crece 10%	($ 23,940.49)	-19.54%

Tabla 4.31. Sensibilidad al variar demanda y costos [A]

Como se puede apreciar en las tablas, el proyecto es sensible principalmente al crecimiento de los costos, aunque si es que este crecimiento de costos está acompañado de un crecimiento de la demanda de por lo menos un 5%, el proyecto sigue siendo rentable.

CAPÍTULO 5. PORTAFOLIO DE SERVICIOS

El presente capítulo pretende describir como se estructurará el servicio para la comercialización y la ejecución. Además, se detalla el alcance de los servicios a ser ofertados para que se pueda acoplar a las necesidades de los clientes y tenga una estructura modular en el momento de personalizarlo. También se detalla el precio base del servicio así como también se define como se calculan las atenciones extra, que se encuentran fuera del alcance del servicio base.

Adicional a todo esto, se definirá la manera de comercializar el servicio y se presentará la forma económica-comercial de justificarlo ante el cliente a través de un análisis de retorno de inversión.

5.1. Servicios

En esta sección se detallará el alcance del servicio con sus niveles de cumplimiento, su duración y sus etapas para la operación.

5.1.1. *Alcance*

Luego de haber realizado el análisis de mercado se identificó que las empresas disponen de diferentes tipos de equipos de seguridad así como también diferentes marcas, lo que hace difícil enmarcar o encasillar el servicio a un solo tipo de equipo o marca; más bien se puede notar que se debe plantear el servicio de una manera modular en la cual se abarquen todas las tecnologías y todos las marcas. Para ello

se ha definido un esquema de requerimientos de servicios, siendo el requerimiento de servicio una unidad descrita en el contrato acordado con el cliente para poder definir las atenciones realizadas. Cada requerimiento de servicio, como unidad de medida, tiene una duración de 1 hora, y esta información solo servirá para poder dimensionar el servicio, es decir que no se hablará de número de horas de atención sino de número de requerimientos de servicio atendidos, ya que el tiempo de atención de un requerimiento puede variar uno con otro.

Los requerimientos de servicio representan las solicitudes de los clientes para realizar determinados cambios en sus equipos de seguridad de acuerdo a la Tabla 3.1 del Capítulo 3. El ejecutar dichas tareas no toma necesariamente el mismo tiempo por lo que se ha establecido un esquema de descuento de requerimientos el cual se lo puede observar en la Tabla 5.1.

Equipo	**Tareas**	**Descuento de requerimiento de servicio**
Firewall	creación/modificación/eliminación de objetos	1
	creación/modificación/eliminación de ACL	1
	creación/modificación/eliminación de NAT	1
	creación/modificación/eliminación de VPN Site to Site	2
	creación/modificación/eliminación de VPN Remote Access	2
	creación/modificación/eliminación de usuario	0.5

Equipo	Tareas	Descuento de requerimiento de servicio
IDS / IPS	creación/modificación/eliminación de firma	1
	creación/modificación/eliminación de política de inspección	1
	creación/modificación/eliminación de usuario	0.5
	verificación de estado firmas	1
Equipo de Filtrado Web	creación/modificación/eliminación de objetos	1
	creación/modificación/eliminación de política de filtrado web	1
	creación/modificación/eliminación de política de límite de ancho de banda	1
	creación/modificación/eliminación de usuario	0.5
Gateway Antivirus	creación/modificación/eliminación de objetos	1
	creación/modificación/eliminación de política de antivirus	1
	verificación del estado de la base de datos de antivirus	1
	creación/modificación/eliminación de usuario	0.5
Gateway Anti-spam	creación/modificación/eliminación de dominios o IPs en listas negras	1
	creación/modificación/eliminación de dominios o IPs en listas blancas	1
	creación/modificación/eliminación de usuario	0.5

Equipo	Tareas	Descuento de requerimiento de servicio
Concentrador VPNs	creación/modificación/eliminación de VPN Site to Site	2
	creación/modificación/eliminación de VPN Remote Access	2
	creación/modificación/eliminación de usuario	0.5

Tabla 5.1. Esquema de descuento por tipo de atención [A]

Las atenciones se las dimensiona para realizarlas en horario laboral, es decir de lunes a viernes de 8h30 a 17h30, por lo que cualquier atención o solicitud a realizarse fuera de este horario por petición del cliente se la deberá descontar con un factor de fuera de horario que se lo ha definido como un 50% adicional de una atención normal. El detalle del descuento por actividad se lo puede observar en la Tabla 5.2.

Equipo	Tareas	Descuento horario laboral	Descuento fuera de horario
Firewall	creación/modificación/eliminación de objetos	1	1.5
	creación/modificación/eliminación de ACL	1	1.5
	creación/modificación/eliminación de NAT	1	1.5

Equipo	Tareas	Descuento horario laboral	Descuento fuera de horario
	creación/modificación/eliminación de VPN Site to Site	2	3
	creación/modificación/eliminación de VPN Remote Access	2	3
	creación/modificación/eliminación de usuario	0.5	0.75
IDS / IPS	creación/modificación/eliminación de firma	1	1.5
	creación/modificación/eliminación de política de inspección	1	1.5
	creación/modificación/eliminación de usuario	0.5	0.75
	verificación de estado firmas	1	1.5
Equipo de Filtrado Web	creación/modificación/eliminación de objetos	1	1.5
	creación/modificación/eliminación de política de filtrado web	1	1.5
	creación/modificación/eliminación de política de límite de ancho de banda	1	1.5
	creación/modificación/eliminación de usuario	0.5	0.75

Equipo	Tareas	Descuento horario laboral	Descuento fuera de horario
Gateway Antivirus	creación/modificación/eliminación de objetos	1	1.5
	creación/modificación/eliminación de política de antivirus	1	1.5
	verificación del estado de la base de datos de antivirus	1	1.5
	creación/modificación/eliminación de usuario	0.5	0.75
Gateway Anti-spam	creación/modificación/eliminación de dominios o IPs en listas negras	1	1.5
	creación/modificación/eliminación de dominios o IPs en listas blancas	1	1.5
	creación/modificación/eliminación de usuario	0.5	0.75
Concentrador VPNs	creación/modificación/eliminación de VPN Site to Site	2	3
	creación/modificación/eliminación de VPN Remote Access	2	3
	creación/modificación/eliminación de usuario	0.5	0.75

Tabla 5.2. Esquema de descuento de requerimientos de servicio en horario laboral y no laboral [A]

Adicional a esto, las atenciones fuera de horario no pueden exceder el 25% del número de requerimientos de servicio mensuales, esto es 7.5 requerimientos fuera de horario, en el caso de que se necesiten más atenciones fuera de horario habrá un cargo de 0.5 requerimiento de servicio por atención adicional. Para poder solicitar atenciones fuera de horario es necesario notificar telefónicamente la solicitud.

Como resultado del análisis de mercado y el análisis financiero se identificó que el precio base para el servicio es de 2000 USD, por lo que es importante definir como establecer el alcance para el servicio base. Para lograr esto es necesario basarse en lo ya definido anteriormente: tareas a ejecutar, equipos involucrados y número de requerimientos de servicio disponibles.

En un servicio base se incluyen 30 requerimientos de servicio que incluyen todas las tareas descritas en la Tabla 5.2, con el detalle del descuento descrito. Es importante aclarar que no todos los clientes disponen de todos los equipos detallados, por lo que el servicio se limitará a los equipos que el cliente disponga. El listado de equipos sobre los cuales se ejecutarán los servicios debe indicarse claramente en el contrato.

Los 30 requerimientos de servicio mensual no son acumulables mes a mes. Adicional a esto el cliente dispondrá de un paquete de 10 requerimientos de servicio anuales extra que se descontarán en caso de que los requerimientos en algún mes sobrepasen la línea base de requerimientos. En el caso de que el cliente exceda el número de requerimientos de servicio base mensual y no disponga más requerimientos se facturará como extra el número de requerimientos adicionales.

Estos 10 requerimientos extra también servirán como requerimientos de emergencia, es decir que si el cliente necesita un soporte con un mejor tiempo de respuesta, se descontará dicho soporte de este paquete de 10 requerimientos extra.

Es necesario destacar que el detalle de descuento de requerimientos está definido de acuerdo a un escenario base, sin embargo, si hay necesidades particulares de los clientes, estas se las puede ajustar, tanto en número de requerimientos y precio para poder brindar un soporte a medida, teniendo en cuenta que no se podrá brindar valores menores al escenario base.

5.1.2. *Niveles de Servicio*

La forma más adecuada de establecer las líneas base de un servicio es conversar con el cliente y armar un paquete ajustado a su realidad y necesidad. Sin embargo esto no se lo puede ajustar totalmente sino hasta el momento de la operación, para esto es necesario establecer los SLOs[56] del servicio, y determinar un periodo de monitoreo en el cual se validará exactamente el comportamiento del servicio, para luego realizar un ajuste a los mismos.

Los SLAs se los debe establecer de acuerdo al alcance definido con el cliente y de acuerdo a las necesidades del cliente; sin embargo se han definido los niveles de servicio para el servicio base, los cuales se los puede observar en la Tabla 5.3 y Tabla 5.4.

[56] Service Level Objective, Objetivo de nivel de servicio

Indicador	Especificaciones	Nivel Objetivo
Tiempo de respuesta máximo para comenzar a atender una solicitud regular.	Tiempo desde que se solicita algo hasta que se confirma que comienza la atención.	120 minutos
Tiempo de respuesta máximo para comenzar a atender una solicitud emergente.	Tiempo desde que se solicita algo hasta que se confirma que comienza la atención.	30 minutos
Tiempo máximo que un requerimiento puede estar sin resolver.	Tiempo desde la confirmación del inicio de la atención hasta que se confirma que ha sido atendido.	30 horas
Número de solicitudes sin resolver al final de un mismo día.	Número máximo de solicitudes acumuladas sin resolver en un mismo día.	4 solicitudes

Tabla 5.3. SLAs en horario laboral [A]

Indicador	Especificaciones	Nivel Objetivo
Tiempo de respuesta máximo para comenzar a atender una solicitud regular.	Tiempo desde que se solicita algo hasta que se confirma que comienza la atención.	180 minutos
Tiempo de respuesta máximo para comenzar a atender una solicitud emergente.	Tiempo desde la confirmación del inicio de la atención hasta que se confirma que ha sido atendido.	45 minutos

Tabla 5.4. SLAs fuera de horario laboral [A]

El incumplimiento de los acuerdos de niveles de servicio puede generar multas que se verán impactadas en los costos del proyecto, es por eso que se han establecido niveles de servicio que se ajustan a la realidad de la operación del servicio con el personal que se ha definido para que pueda operar.

5.1.3. *Duración del Servicio y Etapas de Operación*

Se ha establecido que para poder brindar este servicio con el fin de que sea beneficioso para las dos partes, es necesario definir un periodo mínimo razonable de duración del servicio o contrato. Este periodo de duración permitirá establecer de manera adecuada el comportamiento de la operación del servicio y permitirá que ambas empresas puedan obtener un beneficio tangible ya sea económico o de operación. Para esto se ha establecido que el periodo de duración del contrato con los parámetros de servicio base deberá ser de 3 años.

Durante el periodo de validez del servicio que se indica contractualmente se deben especificar las etapas de ejecución del servicio, estas etapas deben estar claramente definidas para que dicho servicio pueda entrar a operar sin problemas. Las etapas propuestas para el servicio son establecimiento del servicio, transición, operación y renovación o cierre del servicio.

5.1.3.1. Etapa de establecimiento del servicio

Esta etapa del servicio se inicia con la firma del contrato y se realiza un levantamiento detallado de la información técnica de la situación del cliente y de los procesos internos de la empresa. En el caso de que el cliente no disponga de

procesos para los cambios en sus equipos de seguridad se necesita trabajar en conjunto para la generación de los procesos mínimos para poder operar el servicio. Adicional a esto es necesario generar los procesos comunes para poder brindar el servicio como el proceso de requerimiento de servicio. En esta etapa se definen los responsables de las tareas dentro de la operación del servicio y los mecanismos de escalamiento. Esta etapa no debe durar más de 15 días ya que la idea es iniciar con el servicio lo más pronto posible.

5.1.3.2. Etapa de transición del servicio

En esta etapa el servicio empieza a ejecutarse, las tareas de administración de los equipos de seguridad empiezan a ser tomadas por la empresa de servicios de acuerdo a los procesos definidos en la etapa de establecimiento del servicio.

El objetivo de esta etapa es evaluar si los procesos definidos son los adecuados, sirven para mejorar dichos procesos y para evaluar si las líneas base de servicio son adecuadas. En esta etapa se podrán hacer ajustes a las líneas base de servicio y a los niveles de servicio para optimizar la ejecución de los requerimientos. En el caso que los niveles de servicio y las líneas base aumenten es necesario evaluar el impacto en los costos y revisar los mismos con el cliente. Esta etapa de transición no debe tomar más de 2 meses ya que el objetivo es estabilizar el servicio lo más pronto posible.

5.1.3.3. Etapa de operación del servicio

En esta etapa se brinda el servicio tal como indica el contrato firmado entre las partes. En esta etapa se busca cumplir con los requerimientos solicitados por el cliente en los tiempos definidos en los acuerdos de niveles de servicio. En esta etapa además se debe realizar una mejora continua, es decir se debe medir el servicio para tratar de optimizarlo sin que esto involucre costos adicionales o cambios en el servicio. En el caso de que exista un cambio que pueda afectar a los costos del servicio con el afán de mejorarlo es necesario trabajar sobre un control de cambios al contrato. Esta etapa tiene una duración no menor a 2 años y 8 meses.

5.1.3.4. Etapa de renovación o cierre del servicio

En esta etapa dependiendo de los acuerdos que se hayan llegado con el cliente se debe proceder a tomar una decisión sobre el futuro del servicio, es decir se debe llegar a acuerdos para mantenerlo en un periodo prolongado de tiempo; sin embargo existe la posibilidad que no se lleguen a acuerdos referente a la continuidad del mismo; en este caso se debe proceder con la finalización del servicio y cierre de contrato. En el caso de renovación del servicio se debe trabajar en esta etapa en la elaboración y revisión del contrato de renovación, sin detener el servicio brindado; en esta etapa además se deben definir los cambios a realizar en el servicio, en el caso de que existan, para ser ejecutados luego de la firma de dicho contrato. Por otro lado en el caso de que haya el cierre del servicio por no llegar a acuerdos de extensión del mismo se debe definir como se realizará la etapa de cierre, es decir se deben realizar las actividades necesarias para que el cierre no

sea de gran impacto para el cliente y que permita salir de la operación de una manera adecuada sin extender el plazo de la ejecución del servicio y sin que esto involucre costos a la empresa. Este periodo no debe durar más de 1 mes 15 días.

5.2. Precios y formas de comercialización

5.2.1. *Catálogo de precios*

Como resultado del análisis de mercado se definió un precio mínimo para ofrecer el servicio; este precio mínimo se lo estableció en 2000 USD como se lo había indicado anteriormente; sin embargo, este servicio tiene cierta flexibilidad y adaptación a las necesidades del cliente por lo cual es necesario definir cómo se puede armar una solución en función de los cambios o variaciones que pueda tener determinado cliente y como esto impactaría al precio del servicio. Para esto se ha definido un catálogo de precios del servicio que se lo puede observar en la Tabla 5.5.

N°	Componente	Cantidad de requerimientos regulares mensuales	Cantidad de requerimientos VIP anuales	Precio mensual (USD)
1	Servicio Base	30	10	$ 2,000.00
2	Paquete Bronce	5	0	$ 280.00
3	Paquete Plata	10	0	$ 550.00
4	Paquete Oro	20	0	$ 1,050.00

N°	Componente	Cantidad de requerimientos regulares mensuales	Cantidad de requerimientos VIP anuales	Precio mensual (USD)
5	Paquete Bronce VIP	0	5	$ 65.00
6	Paquete Plata VIP	0	10	$ 120.00
7	Paquete Oro VIP	0	20	$ 220.00
N°	**Componente**	**Cantidad de requerimientos anuales**	**Precio requerimiento (USD)**	
1	Requerimiento bajo demanda	Bajo demanda	$ 170.00	

Tabla 5.5. Catálogo de precios de requerimientos de servicio [A]

El Servicio Base es lo mínimo que se puede contratar y en función de este se puede ajustar el paquete a las necesidades del cliente. Los paquetes Bronce, Plata y Oro tienen requerimientos regulares que se suman a los 30 del Servicio Base, es decir son del tipo de requerimiento que expiran mensualmente y que están definidos para ser utilizados con los niveles de servicio estándar, estos paquetes se pueden adquirir con un periodo mínimo de 1 año. Por otro lado se encuentran los paquetes Bronce VIP, Plata VIP y Oro VIP, que son requerimientos de servicio adicionales que se suman a los 10 VIP del Servicio Base y pueden ser utilizados en el caso de que los requerimientos de servicio regulares se terminen o en caso de emergencias para mejorar los niveles de servicio estándar; estos paquetes se pueden adquirir con un periodo mínimo de 1 año. Adicional a esto encontramos los requerimientos de servicio bajo demanda que sirven para adquirirlos por solicitud

del cliente en momentos en que los requerimientos disponibles por contrato se hayan terminado.

Con respecto al incumplimiento de los niveles de servicio, para evitar la definición a nivel contractual de un esquema de multas económicas si es que se llegara a presentar esta situación, se establecerá un esquema de compensación. Este esquema establecerá que no se descontará el número de requerimientos de servicio correspondientes a la solicitud que se encuentre fuera de los parámetros del SLA. Además indicará que de darse el caso que dentro de un mismo mes el 25% de las atenciones estén fuera del SLA, se acreditarán 3 requerimientos VIP a la bolsa de requerimientos de servicio anual.

5.2.2. *Formas de comercialización*

La comercialización del servicio administrado de seguridad perimetral de redes se la realizará a través de una asesoría personalizada con las empresas que forman el grupo de posibles clientes. A través de esta asesoría se desarrollará un servicio personalizado que satisfaga las necesidades de la empresa, teniendo como base el catálogo de precios definido en la sección anterior. Adicionalmente, se mostrará el beneficio de contratar un servicio administrado a través de un análisis de retorno de inversión, el cual arrojará como resultado cuanto ahorro se producirá si es que se llegara a tener un servicio administrado.

El análisis de retorno de inversión permitirá que las empresas que estén interesados en adquirir el servicio puedan comparar entre tener el servicio de

manera in-house[57] o de manera administrada. Para poder realizar esta comparación en primer lugar se deben definir los costos asociados a tener el servicio administrado en cada una de estas dos modalidades. Para definir estos costos se identificarán aquellos que deben ser cancelados una sola vez (cargo único) y aquellos costos recurrentes que tienen un valor mensual (cargo mensual). Como referencia también se mostrará el total anual de estos costos recurrentes (cago anual), que resulta de la multiplicación del cargo mensual por 12 meses.

Para el primer caso, en donde la administración de los equipos de seguridad perimetral de red es realizada por personal dentro de la misma empresa, los costos asociados a esta actividad son los siguientes:

Tipo	**Componente**	**Cargo único**	**Cargo mensual**	**Cargo anual**
Hardware	Laptop	$970.00	$0.00	$0.00
Software	Ofimática y correo electrónico.	$0.00	$20.00	$240.00
Servicios y otros	Administrador de seguridad de red.	$0.00	$1,965.78	$23,589.36
	Horas de soporte con proveedor de seguridad de red.	$0.00	$300.00	$3,600.00
	Capacitación /Actualización tecnológica.	$0.00	$208.33	$2,500.00

[57] Dentro de casa. Esté término hace referencia a una actividad que es desarrollada por la propia empresa.

Tipo	Componente	Cargo único	Cargo mensual	Cargo anual
	Servicios básicos, suministros y espacio de trabajo.	$0.00	$60.00	$720.00

Tabla 5.6. Componentes de administración seguridad modalidad in-house [A]

Para el segundo caso, en el cual los servicios son brindados por un tercero en la modalidad de servicios administrados y de acuerdo a lo definido en capítulos anteriores, los costos asociados del servicio base son los siguientes:

Tipo	Componente	Cargo único	Cargo mensual	Cargo anual
Servicio	Servicio administrado de seguridad perimetral de redes	$0.00	$2,000.00	$24,000.00

Tabla 5.7. Componentes de administración seguridad modalidad servicio administrado [A]

En la siguiente tabla se muestra una comparativa durante 3 años (tiempo mínimo de contratación del servicio administrado) entre la modalidad in-house y la modalidad de servicio administrado. El año 0 representa la inversión inicial que se debería realizar.

Servicio	Año 0	Año 1	Año 2	Año 3
In-house	$970.00	$30,649.36	$30,649.36	$30,649.36
Administrado	$0.00	$24,000.00	$24,000.00	$24,000.00

Tabla 5.8. Costo total de propiedad modalidad in-house y servicio administrado [A]

Si sumamos los costos asociados a cada modalidad y los restamos entre sí, el resultado indica que con el servicio administrado la empresa ahorraría en 3 años 20,918.08 USD, que equivale a un 23% de ahorro.

	Valor	**Porcentaje**
Ahorro en 3 años	$ 20,918.08	23%

Tabla 5.9. Valores de retorno de inversión [A]

CAPÍTULO 6. CONCLUSIONES, RECOMENDACIONES Y LÍNEAS DE INVESTIGACIÓN

6.1. Conclusiones

- El activo más valioso que existe dentro de una empresa es la información, por lo que resulta imprescindible protegerlo de accesos no autorizados.
- La seguridad de la información debe aplicarse como un modelo de capas, siendo la seguridad perimetral de la información el componente más vulnerable dentro de este modelo.
- El modelo de negocio conocido como servicios administrados no debe ser considerado como un reemplazo de otros modelos que se encuentran en el mercado, como el outsourcing y el cloud computing, sino más bien como un complemento.
- En lo referente a la tecnología, para poder brindar un servicio administrado de seguridad perimetral de redes es necesario contar un centro de operaciones, el mismo que se interconectará a través de un enlace de comunicaciones a las instalaciones del cliente, lugar donde se encuentran los equipos de seguridad a ser administrados.
- Con respecto a la operación, es necesario que la empresa que brinde servicios administrados de seguridad perimetral de redes defina claramente los roles de sus colaboradores así como un proceso para manejar los requerimientos provenientes de sus clientes. Como complemento, también se debe definir una línea base del servicio así como SLAs entre la empresa que brinda los servicios administrados y la empresa contratante.

- En el campo de lo legal, no existe ninguna restricción que impida dar servicios administrados de seguridad perimetral de redes a las empresas de comercio al por menor.
- La totalidad de las empresas encuestadas poseen equipos de seguridad de redes, siendo el firewall el equipo que tiene mayor presencia dentro del segmento de mercado que se consideró.
- El 62% de las empresas encuestadas no poseen procesos de control de cambios establecidos para la operación de los equipos de seguridad de red.
- El 100% de las empresas que respondieron a la encuesta coinciden en que la seguridad de la información es importante.
- Las empresas creen que los beneficios que ganarían al adquirir un servicio administrado de seguridad perimetral de redes son la reducción en los costos de operación de la empresa y el permitir que el personal de la empresa pueda dedicarse a otras tareas de mayor injerencia con su cadena de valor.
- La mayor preocupación que tienen las empresas cuando analizan el contratar servicios administrados de seguridad perimetral de redes es la confidencialidad de su información.
- El 25% del segmento meta seleccionado está interesado en adquirir un servicio administrado de seguridad perimetral de redes.
- En una empresa de servicios como la que brindaría los servicios administrados de seguridad perimetral de redes, el componente que más aporta a los gastos operativos es el salario del talento humano.
- El proyecto de inversión descrito como servicios administrados de seguridad perimetral de redes para grandes empresas de comercio al por menor es rentable ya que los resultados del análisis económico-financiero en un

período de tiempo de 4 años indican que tiene una tasa de retorno de inversión del 82.64%.

- Se generó un catálogo de precios del servicio administrado, el cual tiene una línea base y opciones que permitirán la personalización del servicio dependiendo de las necesidades puntuales de los clientes.
- En resumen, después de haber realizado el análisis tecnológico, operativo, legal, de mercado, económico y financiero, se concluye que es factible brindar servicios administrados de seguridad perimetral de redes a grandes empresas de comercio al por menor del Ecuador.
- Referente a la Maestría, la relación que han tenido los contenidos administrativos y financieros con los contenidos tecnológicos ha permitido tener una mejor visión de la forma cómo se maneja el ambiente de las Tecnologías de la Información dentro de las empresas; sobre todo ha permitido aprender y mejorar las habilidades administrativas y financieras que generalmente no se las trata en las carreras de ingeniería.
- La experiencia de esta Maestría ha permitido interactuar con otros colegas relacionados con el campo de las Tecnologías de la Información, donde cada uno ha aportado con sus experiencias laborales y personales enriqueciendo mucho más el contenido impartido en las clases.
- La Pontificia Universidad Católica del Ecuador, con la Maestría de Gerencia de las Tecnologías de la Información, ha impartido a los estudiantes los conocimientos necesarios para la generación de nuevas fuentes de trabajo, lo que resultaría en un gran beneficio para la sociedad.

6.2. Recomendaciones

- Cuando se posicione el servicio administrado de seguridad perimetral de redes en una empresa, se debe enfatizar que el alcance del servicio ofertado no representa una garantía de poseer una infraestructura de red totalmente asegurada. Esto debido a que existen otros elementos que constituyen la seguridad de la información, como por ejemplo el aseguramiento de los equipos de los usuarios finales.
- Las empresas deberían tener definida una política de seguridad de la información, la cual es un enunciado de alto nivel de las aspiraciones de la empresa con respecto a la seguridad de la información. Si una empresa no tiene esta política, adoptar un servicio administrado podría resultar más complejo.
- Debido a que la confidencialidad de la información es la principal preocupación de una empresa cuando se trata de servicios administrados, se deben manejar acuerdos de confidencialidad con los clientes para que tengan una garantía de que no existirá ningún inconveniente con respecto a este tema. La verificación del cumplimiento de estos acuerdos deberá formar parte del proceso de operación del servicio.
- Para posicionar un servicio administrado de seguridad perimetral de redes en una empresa se debe realizar un trabajo de pre-venta de tipo consultoría, en el cual se debe determinar de manera precisa cuál es la situación actual de la empresa en lo referente a la seguridad perimetral de redes con el objetivo de recomendar las mejores opciones del servicio.
- La generación del proyecto de titulación es un paso muy importante dentro de la Maestría por lo que se recomienda que en las futuras promociones se

incluya una materia de guía y preparación del proyecto de titulación en la cual se pueda trabajar el proyecto de manera más ágil y con una guía presencial; esto permitirá que los estudiantes culminen sus proyectos de titulación en menor tiempo.

- Se recomienda hacer seguimiento a los proyectos de titulación presentados para evaluar el impacto positivo y el nivel de incidencia que ha tenido la Maestría en las actividades laborales de cada uno de los maestrantes, y sus aportes a la sociedad.
- Se recomienda a la Pontificia Universidad Católica del Ecuador continuar brindado este tipo de maestrías que se enfocan en complementar las habilidades de Ingenierías Tecnológicas con temas administrativos-financieros.

6.3. Líneas de investigación

El presente trabajo analiza la interrelación de tres temas particulares: los servicios administrados, la seguridad perimetral de redes y las grandes empresas de comercio al por menor. El modificar uno de estos temas y mantener la interrelación con los otros dos, podría generar un conjunto de posibles temas de trabajos de investigación. Con respecto al primer tema, los servicios administrados, se lo podría cambiar por el modelo de outsourcing o cloud computing. En relación al segundo tema, la seguridad perimetral de redes, el posible trabajo podría considerar el análisis de comunicaciones unificadas, comunicaciones inalámbricas o comunicaciones alámbricas. Para el último tema, se podría cambiar el segmento meta de grandes empresas de comercio al por menor por otro tipo de empresas, como por ejemplo empresas de gobierno, de salud, manufactureras, entre otras.

Teniendo esto en cuenta, las líneas de investigación más trascendentes que se podrían generar a partir del presente trabajo serían las siguientes:

- Servicio de seguridad perimetral de redes utilizando un modelo de cloud computing.
- Servicios administrados de otras áreas de la tecnología de red, como por ejemplo comunicaciones unificadas, comunicaciones inalámbricas, LAN.
- Servicios administrados de otras capas del espectro de la seguridad de la información, como por ejemplo aquella capa destinada al aseguramiento del usuario final.
- Servicios administrados de seguridad perimetral de redes a otro tipo de empresas, como por ejemplo empresas del sector financiero.

Adicional a estos posibles trabajos que se pueden generar, también se podría profundizar acerca de la evaluación de los requerimientos necesarios para que una empresa pueda adoptar el modelo de servicios administrados de manera satisfactoria sin que esto produzca un gran impacto en su operación normal.

REFERENCIAS BIBLIOGRÁFICAS

[A] Análisis de factibilidad para brindar servicios administrados de seguridad perimetral de redes para grandes empresas de comercio al por menor, Julio Ulloa y Pablo Calderón, 2013, PUCE.

[B] The Basics of Information Security, Jason Andress, Editorial Elsevier, 2011.

[C] Network Security Bible, Segunda Edición, Eric Cole, Editorial Wiley Publishing Inc., 2009.

[D] Access Denied: The Practice and Policy of Global Internet Filtering, Ronald Deibert. The MIT Press, 2008.

[E] Blocking Spam & Spyware For Dummies, Peter Gregory y Michael A. Simon, John Wiley & Sons, 2005.

[F] Computer and Information Security Handbook, John R. Vacca, Morgan Kaufmann Publishers, 2009.

[G] Email Security & Spam, Books24x7, 2006.

[H] E-Mail Virus Protection Handbook, Brian Bagnall, Chris O. Broomes, Ryan Russell y James Stanger, Syngress Publishing, 2000.

[I] Ending Spam - Bayesian Content Filtering and the Art of Statistical Language Classification, Jonathan A. Zdziarski, Starch Press, 2005.

[J] How to Protect your Enterprise from Viruses, Kevin McCarthy, Laura J. Ciavola y Craig A. Bickel, Books24x7, 2005.

[K] Network perimeter security – Building Defense In-depth, Cliff Riggs, Auerbach Publications, 2004.

[L] Information Security Management Handbook, Sexta Edición, Volumen 1, Harold F. Tipton y Micki Krause, Auerbach Publications, 2007.

[M] Information Security Management Handbook, Sexta Edición, Volumen 2, Harold F. Tipton y Micki Krause, Auerbach Publications, 2008.

[N] Cloud Computing - Automating the Virtualized Data Center, Venkata Josyula, Malcolm Orr, Greg Page, © 2012 Cisco Systems, Inc. Cisco Press, ISBN: 9781587204340.

[O] Security as a Service, June 2010, An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) Research Report Written by Scott Crawford.

[P] Perspective in Brief , The Managed IT Services Market (A Report) , Books24x7, Inc. ©, 2007.

[Q] ITIL Service Design, 2011 Edition by Office of Government Commerce (OGC) TSO ©, 2011.

[R] Manager Services and Outsourcing, White Paper, Motorola, 2004.

[S] What You Should Know About Managed Security Services, Ed Eskew, Geoffrey Fite, Paul Q. Judge and Greg Baumgardner, Books24x7 ©, 2008.

[T] Infrastructure Outsourcing and Managed Services (Market Focus): Solid Overall Growth Masks Sub-market Variations, Datamonitor plc ©, 2006.

[U] Integrating Service Level Agreements: Optimizing Your OSS for SLA Delivery, John J. Lee and Ron Ben-Natan, John Wiley & Sons ©, 2002, ISBN:9780471210122.

[V] Service Level Agreements: A Legal and Practical Guide, Jimmy Desai, Service Level Agreements: A Legal and Practical Guide, Jimmy Desai,IT Governance © 2010, ISBN:9781849280693.

[W] Clasificación Industrial Internacional Uniforme de todas las actividades económicas (CIIU), Departamento de Asuntos Económicos y Sociales de las Naciones Unidas, Revisión 4, 2009.

[X] Service Level Agreements: Winning a Competitive Edge for Support & Supply Services, Andrew Hiles, Rothstein Associates ©, 2000, ISBN:9780964164840.

[Y] ITIL Service Operation, Office of Government Commerce (OGC), TSO ©, 2011, ISBN:9780113313075.

[Z] Network Management: Know it all, Adrian Farrel, Morgan Kaufmann Publishers © 2009, ISBN:9780123745989.

[AA] Ley Especial de Telecomunicaciones Reformada, Congreso Nacional del Ecuador, 2004.

[AB] Ley de Compañías, Congreso Nacional del Ecuador, 2012.

[AC] Gerencia de Marketing, Sexta Edición, Joseph P. Guiltinan, Gordon W. Paul y Thomas J. Madden, McGraw-Hill, 2004, ISBN: 958-600-828-2.

[AD] Proyectos de inversión, Nassir Sapag Chaín, Prentice Hall, 2007, ISBN: 9789702609643.

[AE] Hype Cycle for IT Infrastructure and Outsourcing Services, Christine Tenneson, 31 de Julio de 2013.

[AF] Código Orgánico de la producción, Asamblea Nacional, 2010.

[1] http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

[2] http://en.wikipedia.org/wiki/Web_filtering

[3] http://www.bpovoice.com/profiles/blogs/managed-services-its-much

[4] http://www.addictware.com.mx/index.php/blog/511-ipor-que-adoptar-los-servicio-administrados

[5] http://www.cgi.com/files/white-papers/cgi_whpr_81_out-tasking_vs_outsourcing_e.pdf

[6] http://www.spendmatters.com/index.cfm/2012/8/9/Contract-Procurement-Managed-Services-or-Outsource

[7] http://www.businesscomputingworld.co.uk/outsource-managed-service-or-cloud/

[8] http://www.mspnews.com/msp/articles/302855-outsourcing-versus-managed-services-which-you-prefer.htm

[9] http://en.wikipedia.org/wiki/Network_operations_center

[10] http://www.rae.es/recursos/diccionarios/drae

[11] http://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Economicas/DirectorioEmpresas/140210%20DirEmpresas%20final3.pdf

[12] http://www.supercias.gob.ec/

[13] http://www.telconet.net/images/archivos/portafolio.pdf

[14] http://www.iess.gob.ec/documents/13718/54965/Tasasdeaportacion.pdf

[15] http://contenido.bce.fin.ec/docs.php?path=/documentos/Estadisticas/SectorMonFin/TasasInteres/Indice.htm

[16] http://www.sri.gob.ec/web/guest/depreciacion-acelarada-de-activos-fijos

[17] http://es.wikipedia.org/wiki/VAN

[18] http://www.bce.fin.ec/index.php/indicadores-economicos

GLOSARIO

AAA

Authentication, Authorization & Accounting (Autenticación, Autorización y Contabilización. Este término hace referencia a un conjunto de protocolos que ofrecen los servicios de probar la identidad de un ente (autenticación), concederle sus privilegios (autorización) y registrar sus acciones (contabilización).

Call center

Centro de llamadas. Es un lugar conformado por agentes y sus supervisores en donde se realizan o reciben interacciones con clientes a través de distintos medios de comunicación como por ejemplo llamadas telefónicas o correos electrónicos.

CIIU

Clasificación Internacional Industrial Uniforme. Clasifica la actividad económica de las empresas y ofrece una codificación de esta clasificación. Estos códigos tienen alcance mundial y son utilizados generalmente para agrupar datos de acuerdo a la actividad económica principal de las empresas.

DMZ

Demilitarized zone (Zona Desmilitarizada). Es el nombre de una zona de seguridad definida en un firewall, cuyo nivel de seguridad es menor que el de la zona interna pero mayor que el de la zona externa. En esta zona van

los equipos que albergan los servicios que necesitan ser accedidos tanto de la zona interna como de la zona externa.

Help desk

Mesa de ayuda. Es un servicio en el que se agrupan componentes tecnológicos y de talento humano para dar soporte a una parte del área de tecnología de la información de una empresa o a su totalidad. Este servicio se lo puede dar con personal que se encuentre dentro de la empresa que recibe el servicio o fuera de la misma.

Hipérbola de Gartner

Es una herramienta gráfica desarrollada por la empresa Gartner que representa la madurez y la visibilidad de las tecnologías en un determinado período de tiempo.

ICMP

Internet Control Message Protocol (Protocolo de Mensajes de Control de Internet). Es un protocolo que pertenece a la capa de red del modelo OSI que se utiliza para el envío de notificaciones relacionadas con el protocolo IP. La forma más usada de ICMP es la herramienta ping, que sirve para verificar el estado de un elemento de red que posee una dirección IP.

LAN

Local Area Network (Red de Área Local). Es una red que interconecta equipos computacionales y está limitada a un área geográfica pequeña. El

estándar que generalmente se maneja dentro de esta red es Ethernet (IEEE 802.3).

NMS

Network Monitoring System (Sistema de Monitoreo de Red). Este término hace referencia a un sistema compuesto por servidores y agentes, que permite comprobar la salud de los elementos que constituyen una red. Estos sistemas utilizan protocolos como ICMP y SNMP para realizar esta actividad.

SNMP

Simple Network Management Protocol (Protocolo Simple de Administración de Red). Es un protocolo que permite realizar tareas de administración o lectura de información en dispositivos de red. Para ello se necesita que el servidor que vaya a realizar estas acciones tenga instalada una aplicación que maneje SNMP y que los dispositivos tengan instalados agentes SNMP.

Tecnologías de la información

Este término hace referencia a todas las tecnologías que se utilizan para administrar y procesar la información.

TIR

Tasa Interna de Retorno. Es la tasa con la que el Valor Actual Neto es igual a cero y se lo utiliza como un indicador financiero de la rentabilidad de un proyecto.

VAN

Valor Actual Neto. Es un indicador financiero que da como resultado el valor presente de un número de flujos neto de efectivo determinados que tienen como origen una inversión.

VLAN

Virtual Local Area Network (Red de Área Local Virtual). Es una tecnología de virtualización que permite la creación de varias redes lógicas dentro de un mismo dispositivo físico conocido como un Switch.

WAN

Wide Area Network (Red de Área Amplia). Es una red que interconecta equipos computacionales que se encuentran dispersos geográficamente. También puede ser definida como una red que interconecta varias redes LAN dispersas.